U.S. Department
of Transportation
**National Highway
Traffic Safety
Administration**

www.nhtsa.dot.gov
nhtsa
people saving people

DOT HS 810 591 **April 2006**

Vehicle Safety Communications Project

Final Report

TABLE OF CONTENTS

Executive Summary i

1 Introduction 1

1.1 Background 1

1.2 Focus and Organization of the VSC Project 1

1.3 Report Organization 2

2 Vehicle Safety Application Scenarios 4

2.1 Preliminary Analysis 4

2.1.1 Safety-Related Application Categories 4

2.1.2 Non-Safety Application Categories 5

2.2 Secondary Analysis 5

2.3 Vehicle Safety Application Summary 7

3 Potential Safety Benefits 8

3.1 Overview 8

3.2 Analysis Ranking Attributes 8

3.3 Relative Ranking 9

3.4 Application Ranking 10

3.5 Potential Safety Benefits Summary 11

4 Communication Requirements and Technologies 12

4.1 Overview 12

4.2 Assumptions 13

4.3 Communication Parameters 14

4.4 Comparison of Wireless Communication Technologies 15

4.5 Preliminary Application Communication Scenario Requirements 17

4.6 Preliminary Communications Requirements Summary 18

5 Field and Simulation Testing 20

5.1 Overview 20

5.2 Field Testing and Evaluation 20

5.2.1 Transmission Characteristics at Intersections 21
5.2.2 Intersection Controller Data Exchange 21
5.2.3 Vehicle Data Exchange 22

5.3 Simulation Testing and Evaluation 23

5.3.1 High Priority Emergency Messages 23
5.3.2 Routine Safety Messages 23
5.3.3 Intersection RSU Rebroadcast of Routine Messages 24

5.4 Field and Simulation Testing Summary 24

6 DSRC Communication and Security Standards 25

6.1 Overview 25

6.2 Communications Standards 25

6.3 Standards Support for Vehicle Safety Requirements 26

6.4 Security Standards 27

6.4.1 Threats 27
6.4.2 Defense 27

6.5 Standards and Security Summary 28

7 Conclusions 29

7.1 Summary of Project Accomplishments 29

7.2 VSC Findings 30

7.2.1 Applications 30
7.2.2 Communications 30
7.2.3 Standards 32

7.3 Remaining Needs 33

7.4 Potential Next Steps 33

Appendix A: VSC Project Goals and Tasks

Appendix B: Vehicle Safety Applications

Appendix C: Refinement of Communication Requirements

Appendix D: Antennas

Appendix E: WAVE Radio Modules

Appendix F: Testing System

Appendix G: Field Testing and Evaluation of WAVE DSRC

Appendix H: WAVE DSRC Security

Appendix I: Simulation Testing Results

Appendix J: WAVE DSRC Standards

LIST OF TABLES

Table 2-1: Safety-Related Application Scenarios 6
Table 2-2: Non-Safety-Related Application Scenarios 7
Table 3-1: High-Potential-Benefit Near-Term Applications 10
Table 3-2: High-Potential-Benefit Mid-Term Applications 10
Table 3-3: High-Potential-Benefit Long-Term Applications 10
Table 4-1: Representative Vehicle Safety Application Scenarios 12
Table 4-2: Comparison of Wireless Technologies 16
Table 4-3: Preliminary Application Scenario Communication Requirements 17

Executive Summary

The Vehicle Safety Communications (VSC) project was established to evaluate vehicle safety applications enabled or enhanced by communications. This project determined initial communication requirements for each application, performed some Dedicated Short-Range Communications (DSRC) vehicle testing, and helped to develop the DSRC standards so that the requirements of the safety applications were considered. In 2002, seven automotive manufacturers—BMW, DaimlerChrysler, Ford, GM, Nissan, Toyota, and VW—formed the VSC Consortium (VSCC) to participate in this project with the U.S. Department of Transportation (USDOT).

The goals of the VSC project were to:

- evaluate the potential safety benefits of communication-based vehicle safety applications in terms of reductions in vehicle crashes and functional productive years saved;
- define and evaluate the communications requirements of selected vehicle safety applications;
- work with standards development organizations to ensure that proposed DSRC communications protocols meet the needs of vehicle safety applications; and
- investigate specific technical issues that may affect the ability of DSRC to support deployment of vehicle safety applications, estimate the deployment feasibility of communications-based vehicle safety applications, and assess the ability of proposed DSRC communications protocols to meet the needs of safety applications.

Safety Applications

Initially, the VSCC complied and evaluated a comprehensive list of potential vehicle safety application scenarios. From this list, 34 vehicle safety application scenarios enabled or enhanced by wireless communications were identified. The VSCC estimated potential safety benefits for the identified vehicle safety application scenarios using available crash statistics, as well as assumptions regarding deployment, market penetration, and cooperation with infrastructure or other vehicles. These potential safety benefits appear to be significant for a number of the application scenarios.

From the 34 application scenarios, the VSCC identified 8 scenarios as high-priority and selected for further research based on the estimated potential safety benefits. Of these 8 application scenarios, 4 involve vehicle-to-vehicle communications and 4 involve communications between vehicles and the infrastructure. Three of the vehicle-infrastructure communication applications involve intersections.

Communications Requirements

The VSCC determined preliminary communications requirements for the 8 high-priority vehicle safety application scenarios. Most of these application scenarios required periodic transmission of one-way, point-to-multipoint broadcast messages. The message packet size was 200 to 500 bytes with a communications range of 50 to 300 meters. The VSC project team evaluated communications requirements through both field and simulation testing.

For field testing, the VSC project team developed and conducted evaluations on a test system based on the lower-layer DSRC standard. During the testing, the team implemented a preliminary, common safety-message set developed by the Society of Automotive Engineers (SAE) for vehicle-to-vehicle safety applications. The SAE's DSRC safety-message set includes vehicle size, position, speed and acceleration data, and braking, steering and throttle information. Actual vehicle bus data in a standard format was exchanged between vehicles from different manufacturers. The field testing confirmed the functionality of DSRC communications at real intersection locations under typical traffic conditions and demonstrated the technical feasibility of the current DSRC technology.

Through simulation, the VSC project team studied the effect of large-scale deployment of DSRC-equipped vehicles and roadside units on communications capacity. Based on the simulation testing, the VSC project team suggested the need for a high-availability, low-latency channel for latency-critical safety applications. The simulation testing also showed that emergency message prioritization consistently improved the reception probability over routine messages by 5 percent to 40 percent, and reduced the communications latency across a wide-range of simulation scenarios. The simulation results further illustrated that channel capacity is an issue that will need to be addressed for large-scale deployment in stressed traffic environments.

Standards Development

As active participants in the DSRC standards development process, the VSCC evaluated existing and proposed DSRC standards. VSCC identified specific technical issues, presented vehicle safety requirements and a proposed security solution, and secured necessary revisions in eight major areas of the standards. To ensure message authentication, the proposed security architecture requires that all vehicle and roadside units be issued certificates and that safety-relevant messages be digitally signed. In addition, compromised units need to be revoked through a certificate revocation list that is distributed to all units. The SAE developed a common vehicle-to-vehicle DSRC safety message set that includes vehicle size, position, speed, and acceleration data, and braking, steering, and throttle information.

The vehicle safety communications requirements and proposed security solution are currently being considered in the development of upper-layer and security standards in Institute of Electrical and Electronic Engineers (IEEE) committees. The preliminary vehicle safety communications requirements appear to be supported by the FCC Report and Order, and the current lower-layer DSRC standards mandated by the FCC. However,

the high-availability, low-latency DSRC channel required for particular vehicle safety applications was not designated in the FCC Report and Order.

DSRC Deployment Issues

The VSC project evaluated proposed DSRC standards, identified specific technical issues, and presented vehicle safety requirements. A test system based on the current lower-layer DSRC standard was developed and field-tested. As a result of the testing, the functionality of DSRC communications for vehicle safety application scenarios at real intersections was confirmed. In addition, the project successfully demonstrated the exchange of messages for vehicle-to-vehicle safety applications, identified channel capacity in high-penetration traffic environments as a deployment issue, and determined that 5.9 GHz DSRC wireless technology appears to be able to support the communications requirements of the majority of vehicle safety applications.

Potential Next Steps

Based on the VSC project accomplishments, and the remaining needs that have been identified, VSCC envisions that the following steps be undertaken:

- Develop prototype cooperative intersection collision avoidance safety applications.
- Develop prototype communication-based vehicle-to-vehicle safety applications.
- Develop adaptive DSRC protocols to improve communication reliability in stressful traffic environments.
- Continue to influence and contribute to DSRC standards development from a vehicle safety communication requirements standpoint.
- Implement and test upper-layer and communications protocol, when available.

1 Introduction

1.1 Background

The Vehicle Safety Communications (VSC) project was established to evaluate vehicle safety applications enabled or enhanced by communications. This project determined initial communication requirements associated with each application and promoted their accommodation in developing communications standards. The VSC project consists of a set of tasks and subtasks. A summary of the project goals and tasks has been included in Appendix A.

The VSC Consortium (VSCC) was formed to participate in this project with the U.S. Department of Transportation (USDOT). The VSCC consists of participants from seven automotive manufacturers—BMW, DaimlerChrysler, Ford, GM, Nissan, Toyota, and VW. Since May 2002, VSCC has identified and evaluated vehicle safety applications enhanced or enabled by external communications, determined their respective communications requirements, and worked with standards development organizations to ensure that the proposed 5.9 GHz Dedicated Short Range Communications (DSRC) protocols support vehicle safety applications.

1.2 Focus and Organization of the VSC Project

The VSC project goals were to:

- estimate the potential opportunity for safety benefits of communication-based vehicle safety applications in terms of reductions in vehicle crashes and functional productive years saved;
- clearly define the communications requirements of selected vehicle safety applications;
- work with standards development organizations to ensure that proposed DSRC communications protocols meet the needs of vehicle safety applications;
- investigate specific technical issues that may affect the ability of DSRC (as defined by the standards) to support deployment of vehicle safety applications;
- estimate the deployment feasibility of communications-based vehicle safety applications; and
- assess the ability of proposed DSRC communications protocols to meet the needs of safety applications.

The following questions illustrate the focus and organization of the VSC project research, analysis, testing, and evaluation carried out to achieve the project goals. Discussions related to the questions are included in the chapters listed.

- What vehicle safety applications have the potential to be improved or made possible with external vehicle communications? (Chapter 2)
- Are there significant potential safety benefits for communication-based vehicle safety applications? (Chapter 3)
- What are the communication requirements for communications-based vehicle safety applications? (Chapter 4)
- Will the proposed DSRC communications protocols (as defined by the standards) meet the needs of vehicle safety applications? (Chapter 5)
- What is the preliminary estimate of technical feasibility for deployment of communications-based vehicle applications? (Chapter 6)

The report concludes with a summary of the VSC project accomplishments, findings, and suggestions for potential next steps (Chapter 7).

1.3 Report Organization

This report identifies the vehicle safety application scenarios evaluated for potential safety benefits and describes the preliminary communications requirements necessary to support a selected set of representative application scenarios. Included in this report is an assessment of the applicability of available wireless technologies to the preliminary requirements of the selected application scenarios. The capabilities of DSRC wireless technology were evaluated in field tests (test tracks and public roadways) and in model simulation tests. This report describes the results of those tests. Further, the report outlines DSRC security requirements and a proposed security architecture, and discusses VSCC's activities working with the SDOs to ensure that developed standards adequately support the anticipated safety applications.

This report consists of the introduction and the following chapters:

- **Chapter 2, Vehicle Safety Application Scenarios**
  Describes the vehicle safety application scenarios that may be improved by or made possible with external vehicle communications. More than 75 applications were identified in the preliminary analysis and 45 applications were selected for further review.
- **Chapter 3, Potential Safety Benefits**
  Discusses the estimated near-, mid-, and long-term benefits that might be realized by implementing wireless communications systems enabling vehicle-to/from-infrastructure and vehicle-to-vehicle transfer of vehicle safety information.
- **Chapter 4, Communications Requirements and Technologies**
  Presents the operational characteristics and preliminary communications requirements of eight representative potential near- and mid-term vehicle

safety application scenarios. Compares the wireless communication technologies available to address the preliminary requirements of vehicle safety application scenarios.

- **Chapter 5, Field and Simulation Testing**
  Describes the field-testing program carried out on test track facilities and public roadways to evaluate vehicle safety communications, including vehicle-to-vehicle and vehicle-to/from infrastructure transmissions. Discusses the simulation model testing of vehicle safety communications in scaled environments based on proposed DSRC systems.
- **Chapter 6, DSRC Communication and Security Standards**
  Discusses the work of the VSCC to ensure that the proposed DSRC communications protocols, as defined in standards, meet the needs of vehicle safety applications. Describes the progress achieved in resolving specific technical issues that may have affected the ability of DSRC to support deployment of vehicle safety applications. Presents the DSRC security requirements for vehicle safety applications that need to be addressed in the DSRC standards. Describes the security threat model, and outlines a potential design for a comprehensive security architecture and protocol.
- **Chapter 7, Conclusions**
  Provides a summary of the accomplishments of the VSC project. Sumarizes the key findings of the project, and describes the remaining vehicle safety communications needs that have not yet been met. Identifies potential next steps that might be undertaken to build on the knowledge gained from the VSC project and address the remaining needs.

2 Vehicle Safety Application Scenarios

2.1 Preliminary Analysis

An initial goal of the VSC project was to identify safety application scenarios that might be improved or made possible by external vehicle communications. The vehicle safety applications were initially compiled by reviewing existing literature under Task 1 as a starting point. The initial list of vehicle safety applications and the review of existing literature is presented in the VSC project *Task 1 & 2 Final Report.*[1]

In Task 3 of the VSC project, a comprehensive list of communications-based vehicle safety and non-safety application scenarios was compiled. The VSCC participants identified safety applications that may benefit or be enabled by wireless communications (either vehicle-vehicle or vehicle-infrastructure). In addition, brainstorming sessions between all members of the VSCC were organized to expand the list of potential safety applications, and group the safety applications with respect to complexity and when they may become commercially feasible for light vehicles. This list represents the best efforts of the participants at the time of publication. It may not contain all vehicle safety applications (due to similarity) but does contain, at a minimum, examples and brief descriptions of representative safety applications. More than 75 application scenarios were identified and analyzed resulting in 34 safety and 11 non-safety application scenario descriptions. Details of this study are presented in the VSC project *Task 3 Final Report.*[2]

The VSCC grouped the vehicle safety application scenarios by level of complexity. A time estimate of when applications might be commercially available in light vehicles, based upon deployment assumptions relevant in 2002, was developed. More than 75 potential application scenarios were identified and classified in two groups: safety-related and non-safety-related application categories.

2.1.1 Safety-Related Application Categories

- **Intersection Collision Avoidance (ICA)**
  Uses infrastructure-to-vehicle communication to warn the driver of potentially unsafe situations occurring at intersections, including traffic signal violations, left-turn assistance, blind-merge warnings, and imminent-collision warnings.
- **Public Safety**
  Improves general public safety by providing the driver with warnings related to current or up-coming traffic situations such as approaching emergency vehicles, disabled vehicles in traffic lanes, and emergency message transmissions.

---

[1] *Task 1 & 2 Final Report* - Literature Review and Analysis of DSRC Standards Process, Public Document, Vehicle Safety Communications Project, Crash Avoidance Metrics Partnership, 2003.

[2] *Task 3 Final Report - Identify Intelligent Vehicle Safety Applications Enabled by DSRC*, Public Document, Vehicle Safety Communications Project, Crash Avoidance Metrics Partnership, 2004.

- **Sign Extension**
  Warns the driver of road signs, road curves, structures, work zones, wrong-way vehicles, and amber alerts.
- **Vehicle Diagnostics and Maintenance**
  Uses infrastructure-to-vehicle communication to improve safe vehicle operation through distributed safety recall information and interaction with service and maintenance providers.
- **Information From Other Vehicles**
  Uses vehicle-to-vehicle communications to determine and warn the driver of hazardous conditions such as other vehicles braking for emergency stops, merging traffic, vehicles in a driver's blind spot, and an imminent collision.

2.1.2 Non-Safety Application Categories

- **Traffic Management**
  Uses vehicle-to-vehicle communication to improve traffic flow.
- **Free-Flow Tolling**
  Uses infrastructure-to/from-vehicle communication to reduce congestion and improve traffic flow of toll roads by toll collection without the need for toll plazas along the roadway.
- **Information From Other Vehicles**
  Uses infrastructure-to-vehicle and vehicle-to-vehicle communication to improve driver navigation and enhance safe vehicle operation.

2.2 Secondary Analysis

From the comprehensive list of scenarios, additional analysis resulted in the identification of 45 vehicle safety application scenarios for further study (Task 3). Of these 45 scenarios, 34 were judged to be safety-related. Table 2-1 and Table 2-2 list the scenarios in each category that were selected for further review.

See Appendix B for a descriptive overview of these scenarios. See the VSC project Task 3 Final Report[3] for additional descriptions and details of the vehicle safety applications summarized in Table 2-1 and Table 2-2.

[3] *Task 3 Final Report - Identify Intelligent Vehicle Safety Applications Enabled by DSRC*, Public Document, Vehicle Safety Communications Project, Crash Avoidance Metrics Partnership, 2004.

Table 2-1: Safety-Related Application Scenarios

Category	Application Scenario
Intersection Collision Avoidance	• Traffic Signal Violation Warning • Stop Sign Violation Warning • Left Turn Assistant • Stop Sign Movement Assistant • Intersection Collision Warning • Blind Merge Warning • Pedestrian Crossing Information Warning
Public Safety	• Approaching Emergency Vehicle Warning • Emergency Vehicle Signal Preemption • SOS Services • Post-Crash Warning
Sign Extension	• In-Vehicle Signage Warning • Curve Speed Warning • Low Parking Structure Warning • Wrong Way Driver Warning • Low Bridge Warning • Work Zone Warning • In-Vehicle Amber Alert Warning
Vehicle Diagnostics and Maintenance	• Safety Recall Notice • Just-in-Time Repair Notification
Information from Other Vehicles	• Cooperative Forward Collision Warning • Road Condition Warning • Emergency Electronic Brake Lights • Lane Change Warning • Blind Spot Warning • Highway Merge Assistant • Visibility Enhancer • Cooperative Collision Warning • Cooperative Vehicle-Highway Automation System (Platoon) • Cooperative Adaptive Cruise Control • Road Condition Warning • Pre-Crash Sensing • Highway/Railroad Collision Warning • Vehicle-to-Vehicle Road Feature Notification • Cooperative Glare Reduction • Adaptive Headlamp Aiming

Table 2-2: Non-Safety-Related Application Scenarios

Category	Application Scenario
Traffic Management	• Intelligent On-Ramp Metering • Intelligent Traffic Flow Control
Tolling	• Free-Flow Tolling
Information from Other Vehicles	• Instant Messaging • Adaptive Drive-Train Management • Enhanced Route Guidance and Navigation • Point-of-Interest Notification • Map Downloads and Updates • GPS Correction

2.3 Vehicle Safety Application Summary

As part of the initial VSC project activities, a comprehensive list of potential vehicle safety application scenarios was compiled and evaluated. Of these, 34 vehicle safety application scenarios potentially enabled or enhanced by wireless communications were identified. It is likely that additional vehicle safety application scenarios enabled or enhanced by wireless communications will be identified in the future, especially as advances in wireless technology become available.

3 Potential Safety Benefits

3.1 Overview

For each vehicle safety application scenario discussed in Chapter 2, initial estimates of potential safety benefits were derived. These estimates were based on a crash statistic loss metric called "Functional Years Lost" from the General Motors 44 Crashes report.[4] In addition to this crash statistic loss metric, assumptions available in late 2002 and early 2003 regarding deployment, market penetration, and cooperation between infrastructure and/or other vehicles were used to estimate potential safety benefits. High-priority safety applications were identified for further evaluation based on estimates of potential safety benefits.

The VSCC and the USDOT jointly selected a subset of safety applications of mutual interest from the comprehensive list. Safety applications were selected based on potential safety benefit and were representative of the range of identified safety applications. Refer to the VSC project Task 3 Final Report[5] for additional descriptions and details on the process followed in the selection of vehicle safety applications based on potential safety benefit.

3.2 Analysis Ranking Attributes

The VSC project team defined a set of analysis categories by which the potential safety benefits of application scenarios could be compared. The team used a methodology for analysis and ranking that included consideration of:

- **Estimated Deployment Time Frame**
  Defines the estimated time frame before the application may be available on light duty vehicles in the United States. Estimated deployment time frame depends on technical factors such as additional sensor requirements, vehicle position plus map accuracy requirements, communication requirements, and cost. Near-term application systems were considered to be potentially deployable in the U.S. market between 2007 and 2011; mid-term applications deployable between 2012 and 2016; and long-term applications deployable beyond 2016.
- **Estimated Effectiveness**
  Defines the effectiveness of an application in terms of the reduction of three crashed-related factors: (i) direct dollar expenditures related to the damage and injury caused by a crash, (ii) functional years lost to fatal injury plus years lost of functional capacity to nonfatal injury, and (iii) number of vehicles involved in various crash types in the United States.

---

[4] General Motors (1997). *44 Crashes, v.3.0.* Warren, MI: NAO Engineering, Safety & Restraints Center, Crash Avoidance Department.

[5] *Task 3 Final Report - Identify Intelligent Vehicle Safety Applications Enabled by DSRC*, Public Document, Vehicle Safety Communications Project, Crash Avoidance Metrics Partnership, 2004.

- **Estimated Market Penetration**
  Estimates the number of light-duty vehicles in the U.S. market that would be equipped with each vehicle safety application in each year after initial deployment. Also estimates the number of vehicles equipped with safety applications after the fifth year of deployment
- **Estimated Cooperation from Infrastructure and/or Other Vehicles**
  Estimates the probability of securing infrastructure cooperation and/or other vehicle cooperation in fifth year after deployment. Cooperation required by the applications is in the form of relevant safety-related data exchange using infrastructure-to/from-vehicle communication and vehicle-to-vehicle communication.

3.3 Relative Ranking

Relative ranking was done separately for near-, mid-, and long-term application scenarios. Application scenarios were evaluated based on benefits derived with respect to 44 Crashes. For each application system, the VSC team used engineering judgment in estimating the application ranking attributes. The methodology used to estimate the safety benefits and the relative ranking of the application scenarios is presented in the VSC project Task 3 Report.[6] It is important to stress that the VSC application safety benefits analysis was for the purpose of relative ranking of communications-enabled application scenarios. In the Addendum to the VSC project Task 3 Report,[7] the estimates for the evaluation attributes used for the application safety benefits analysis and application ranking are presented.

For each of the relevant crash types that benefit from an application scenario, the VSC team estimated the percent effectiveness of the application system to that particular crash type. The benefit distributions of an application system were computed based on two perspectives:

- **Benefit Opportunity**
  Estimate of the potential benefits derived by deployment of an application scenario in all new vehicles for each year after initial deployment.
- **Estimated Benefits**
  Estimate of the potential benefits derived by deployment of an application scenario using the VSC estimates for market.

---

[6] *Task 3 Final Report - Identify Intelligent Vehicle Safety Applications Enabled by DSRC*, Public Document, Vehicle Safety Communications Project, Crash Avoidance Metrics Partnership, 2004.

[7] *Addendum to the Task 3 Final Report - Identify Intelligent Vehicle Safety Applications Enabled by DSRC*, Public Document, Vehicle Safety Communications Project, Crash Avoidance Metrics Partnership, 2004.

The percent effectiveness of the application scenario with respect to 44 Crashes, and the probability that a vehicle equipped with an application will get cooperative communication from other vehicles and/or the infrastructure is also based on the VSC team estimates.

3.4 Application Ranking

The following tables summarize estimated near-, mid-, and long-term safety benefits (functional years saved) for vehicle safety applications with the highest potential. The ranking is based on benefit opportunity for the fifth year after deployment.

Table 3-1: High Potential Benefit Near-term Applications

Application System	Benefit Opportunity (functional years saved)	Estimated Benefits (functional years saved)
Traffic Signal Violation Warning	17,627	364
Curve Speed Warning	11,189	116
Emergency Electronic Brake Lights	4,284	66

Table 3-2: High Potential Benefit Mid-term Applications

Application System	Benefit Opportunity (functional years saved)	Estimated Benefits (functional years saved)
Pre-Crash Sensing	34,172	523
Cooperative Forward Collision Warning	19,160	294
Left Turn Assistant	8,534	113
Lane Change Warning	7,354	113
Stop Sign Movement Assistant	7,217	95

Table 3-3: High Potential Benefit Long-term Applications

Application System	Benefit Opportunity (functional years saved)	Estimated Benefits (functional years saved)
Cooperative Collision Warning	59,336	5,453
Intersection Collision Warning	52,804	4,911

3.5 Potential Safety Benefits Summary

The potential safety benefits for identified vehicle safety application scenarios were estimated according to effectiveness toward known crash statistics, as well as assumptions regarding deployment, market penetration, and cooperation between infrastructure and/or other vehicles. These potential safety benefits appear to be significant for a number of the application scenarios, based on the deployment and other assumptions available in late 2002 and early 2003. As a result, eight application scenarios were identified as high priority for further research.

4 Communication Requirements and Technologies

4.1 Overview

Thirty-four vehicle safety application scenarios were analyzed and ranked. The result of this evaluation was a subset of eight representative near- and mid-term safety applications suitable to be used as a basis for establishing preliminary communication requirements. The requirements were described in terms of communications parameters defined in this chapter and key assumptions about the operational characteristics of the application scenarios.

Table 4-1: Representative Vehicle Safety Application Scenarios

Near-term	Mid-term
Traffic Signal Violation Warning	Pre-Crash Sensing
Curve Speed Warning	Cooperative Forward Collision Warning
Emergency Electronic Brake Lights	Left Turn Assistant
	Lane Change Warning
	Stop Sign Movement Assistance

- **Traffic Signal Violation Warning**
  Traffic signal violation warning uses infrastructure-to-vehicle communication to warn the driver to stop at the legally prescribed location if the traffic signal indicates a stop and it is predicted the driver will be in violation.
- **Curve Speed Warning – Rollover Warning**
  Curve speed warning aids the driver in negotiating curves at appropriate speeds.
- **Emergency Electronic Brake Lights**
  When a vehicle brakes hard, the emergency electronic brake light application sends a message to other vehicles following behind.
- **Pre-Crash Sensing**
  Pre-crash sensing prepares the driver for imminent, unavoidable collisions.
- **Cooperative Forward Collision Warning**
  Cooperative forward collision warning system aids the driver in avoiding or mitigating collisions with the rear end of vehicles in the forward path of travel through driver notification or warning of the impending collision. The application does not attempt to control the host vehicle to avoid an impending collision.

- **Left Turn Assistant**
  The left turn assistant application informs the driver about oncoming traffic to assist in making a left turn at a signalized intersection without a phasing left turn arrow.
- **Lane Change Warning**
  The lane change warning application warns the driver if an intended lane change may cause a crash with a nearby vehicle.
- **Stop Sign Movement Assistance**
  The stop sign movement application warns the driver that the vehicle is about to pass through an intersection after having stopped at a stop sign.

4.2 Assumptions

Several assumptions about operational characteristics were used to define the communication requirements of the representative safety applications, including:

- The rapid evolution of wireless technologies provides opportunities to use these technologies in support of advanced vehicle safety applications. In particular, DSRC at 5.9 GHz offers the potential to effectively support wireless data communications between vehicles and between vehicles and infrastructure.
- A standardized DSRC message set and data dictionary would be established for safety applications that use vehicle-to-vehicle and/or vehicle-to-infrastructure communications. The message set would require agreement by all public and private sector organizations involved in this aspect of DSRC.
- Some applications would require periodic broadcasts (e.g., every 100 msec.) from vehicles in order to identify the roadway position. The transmitted data would need to be based on a location-referencing standard accepted by DSRC stakeholders.
- Many of the preliminary communication requirements call for an on-board unit with a communication range between 100 to 1,000 meters. The practicality of these requirements in light of transmission characteristics such as multipath and interference with other DSRC applications should be studied before such requirements are finalized.
- Many of the applications require communications in multiple directions from the vehicle. Conceptually, this could be achieved through an on-board unit using an omnidirectional antenna, although transmission characteristics should be considered when evaluating the performance of such a system. The use of a directional antenna (especially for roadside units) should be considered for those applications in which data need only be transmitted or received in a specific direction.

- Security is an open issue for all of the applications. Potential security measures could include a method for assuring that packet/data was generated by a trusted source and that the packet/data was not tampered with or altered after it was generated. Any application that involves a financial transaction (such as tolling) requires the capability to perform a secure transaction.

4.3 Communication Parameters

The application scenarios require cooperation from the infrastructure, other vehicles, or both in the form of relevant safety-related data exchange using infrastructure-to/from-vehicle communication and/or vehicle-to-vehicle communication. The proposed operational characteristics and preliminary communication requirements for the eight vehicle safety applications are described in terms of the following parameters:

- **Type of Communication**
  Considers the (a) source-destination of the transmission (infrastructure-to-vehicle, vehicle-to-infrastructure, or vehicle-to-vehicle communications), (b) direction of the transmission (one-way or two-way), and DSRC communication, and (c) source reception of the communication (point-to-point or point-to-multipoint).
- **Transmission Mode**
  Describes whether the transmission is triggered by an event (event-driven) or sent automatically at regular intervals (periodic).
- **Minimum Frequency**
  Defines the minimum rate at which a transmission should be repeated (e.g., 1 Hz).
- **Allowable Latency**
  Defines the maximum duration of time allowable between when information is available for transmission and when it is received (e.g., 100 msec).
- **Data to Be Transmitted and/or Received**
  Describes the contents of the communication (e.g., vehicle location, speed, and heading). Design considerations include whether or not vehicles make periodic broadcasts to identify their positions on the roadway and how privacy is best maintained.
- **Maximum Required Range of Communication**
  Defines the communication distance between two units that is required to effectively support a particular application (e.g., 100 m).

4.4 Comparison of Wireless Communication Technologies

Currently available wireless communications technologies that could possibly be applied to the representative vehicle safety applications identified earlier in this chapter included:

- 5.9 GHz DSRC
- 2.5-3G PCS and Digital Cellular
- Bluetooth
- Digital Television (DTV)
- High-Altitude Platforms
- IEEE 802.11 Wireless LAN
- Nationwide Differential Global Positioning System (NDGPS)
- Radar
- Remote Keyless Entry (RKE)
- Satellite Digital Audio Radio Systems (SDARS)
- Terrestrial Digital Radio
- Two-Way Satellite
- Ultra-Wideband (UWB)

Table 4-2 summarizes the capabilities of these wireless technologies. A detailed discussion is presented in the VSC Task 3 Final Report.

Table 4-2: Comparison of Wireless Technologies

Wireless Technology	5.9 GHz DSRC	2.5-3G PCS and Digital Cellular	Bluetooth	Digital Television(DTV)	High Altitude Platforms	IEEE 802.11 Wireless LAN	Nationwide Differential Global Positioning System	Radar	Remote Keyless Entry (RKE)	Satellite Digital Audio Radio Systems (SDARS)	Terrestrial Digital Radio	Two-Way Satellite	Ultrawideband (UWB)
Capabilities: Range	1000 m	~4-6 km	10 m	~40 km	120 km	1000 m	300-400 km	2 km	30 m	US 48 States	30-50 km	N/A	15-30 m
One-Way To Vehicle	X			X	?		X	X	X	X	X		?
One-Way From Vehicle	X				?			X					?
Two-Way	X				?							X	?
Point-To-Point	X	X	X		?	X			X			X	?
Point-To-Multipoint	X	X	X	X	?	x	X	X		X	X		?
Latency	200 µsec	1.5-3.5 sec	3-4 Sec	10-30 sec	?	3-5 sec	N/A	N/A	N/A	10-20 sec	10-20 sec	60+sec	?

4.5 Preliminary Application Communication Scenario Requirements

Wireless technologies are rapidly evolving. This evolution provides opportunities to use these technologies in support of advanced vehicle safety applications and crash avoidance countermeasures. For example, DSRC offers the potential to support low-latency wireless data communications between vehicles and between vehicles and infrastructure. Low-latency data communications within the immediate vicinity of a vehicle potentially enable a large number of vehicle safety applications including crash avoidance countermeasures.

Table 4-3 summarizes the preliminary communication requirements in terms of the previously defined parameters.

Table 4-3: Preliminary Application Scenario Communication Requirements

	Comm Type	Trans Mode	Min. Freq (Hz)	Latency (msec)	Data to Be Transmitted and/or Received	Max. Req'd Comm Range (m)
Traffic Signal Violation Warning	• Infrastructure -to-vehicle • One-way • Point-to-multipoint	Periodic	~10	~100	• Traffic signal status • Timing • Directionality • Position of the traffic signal stopping location • Weather condition (if available) • Road surface type	~250
Curve Speed Warning	• Infrastructure -to-vehicle • One-way • Point-to-multipoint	Periodic	~1	~1000	• Curve location • Curve speed limits • Curvature • Bank • Road surface condition	~200
Emergency Electronic Brake Lights	• Vehicle-to-vehicle • One-way • Point-to-multipoint	Event-driven	~10	~100	• Position • Heading • Velocity • Deceleration	~300
Pre-Crash Sensing	• Vehicle-to-vehicle • Two-way • Point-to-point	Event-driven	~50	~20	• Vehicle type • Position • Velocity • Acceleration • Heading • Yaw-rate	~50
Cooperative Forward Collision Warning	• Vehicle-to-vehicle • One-way • Point-to-multipoint	Periodic	~10	~100	• Position • Velocity • Acceleration • Heading • Yaw-rate	~150

	Comm Type	Trans Mode	Min. Freq (Hz)	Latency (msec)	Data to Be Transmitted and/or Received	Max. Req'd Comm Range (m)
Left Turn Assistant	• Vehicle-to-infrastructure and infrastructure-to-vehicle • One-way • Point-to-multipoint	Periodic	~10	~100	• Traffic signal status • Timing • Directionality; • Road shape and intersection information; • Vehicle position • Velocity • Heading	~300
Lane Change Warning	• Vehicle-to-vehicle • One-way • Point-to-multipoint	Periodic	~10	~100	• Position • Heading • Velocity • Acceleration • Turn signal status	~150
Stop Sign Movement Assistance	• Vehicle-to-infrastructure and infrastructure-to-vehicle • One-way • Point-to-multipoint	Periodic	~10	~100	• Vehicle position • Velocity • Heading; • Warning	~300

For each high-priority application that ranked high in potential safety benefits, the VSC project team defined system level architecture and concepts of operation. The definitions included development of initial system architecture block diagrams, illustrations and information flowcharts, identification of sensors and other system needs, data message sets, and message size. Communications parameter values for the application scenarios were specified based on evaluation of the proposed system concept, engineering judgment, and industry experience. See the VSC project Task 3 Report[8] for details.

4.6 Preliminary Communications Requirements Summary

The VSC project team analyzed the eight high-priority vehicle safety applications scenarios and determined preliminary communications requirements for these scenarios, including:

- Message packet size of 200 to 500 bytes (all 8 scenarios)
- Maximum required range of communications of 50 to 300 meters (all 8 scenarios)
- One-way, point-to-multipoint broadcast messages (7 of 8 scenarios)

[8] *Task 3 Final Report - Identify Intelligent Vehicle Safety Applications Enabled by DSRC*, Public Document, Vehicle Safety Communications Project, Crash Avoidance Metrics Partnership, 2004.

- Two-way, point-to-point messages (1 of 8 scenarios)
- Periodic transmission mode (6 or 7 of 8 scenarios)
- Event-driven transmission mode (1 or 2 of 8 scenarios)
- Allowable latency of 100 milliseconds (6 of 8 scenarios)
- Allowable latency of 20 milliseconds (1 of 8 scenarios)
- Allowable latency of 1 second (1 of 8 scenarios)

If additional high-priority applications scenarios are identified, or if alternative scenarios are developed for identified vehicle safety applications, it will likely become necessary to reexamine these preliminary communications requirements.

It is expected that the communications requirements will need further refinement as prototype vehicle safety applications are developed from a safety-systems design perspective.

5 Field and Simulation Testing

5.1 Overview

VSCC tested the communications functionalities and potential technical feasibility of using DSRC to enable and enhance vehicle-safety systems and applications. Two levels of testing were performed:

- **Field Testing and Evaluation**
  Test track and public roadway evaluations to establish technical feasibility and to enable the future design and development of potential vehicle safety applications.
- **Simulation Testing and Evaluation**
  Evaluation of simulated DSRC performance in an urban intersection environment densely populated with DSRC-equipped vehicles and infrastructure.

5.2 Field Testing and Evaluation

VSCC assessed the viability of DSRC relevant to potential safety applications in real-world environments through field testing on test tracks and public roadways. This was accomplished through the testing and evaluation of communication functionalities started in Task 4 and continued in Task 10, using both vehicle-vehicle and vehicle-infrastructure wireless data transfer. Various antenna configurations also were evaluated to determine the most realistic and deployable physical structure that would meet technical requirements.

For the initial field testing, VSCC designed and developed 20 first-generation communications DSRC test kits. The kits enabled engineering testing in a number of different locations and configurations using different vehicles in test track and public roadway environments. The field testing did not require the procurement of dedicated test vehicles as individual manufacturers used their own vehicles with proprietary on-board systems.

The simulations and test results for the antenna design activity are presented in detail in Appendix D. The design details and test results for the WAVE radio modules are provided in Appendix E.

The anticipated communications parameters for two potential vehicle-safety application scenarios were tested in detail: Traffic Signal Violation Warning and Emergency Electronic Brake Lights. Testing focused on three areas:

- Collecting and analyzing data in real-world intersection environments to determine communications characteristics.
- Intersection testing using an interface with a traffic-signal controller to transmit actual traffic signal data.

- Vehicle-to-vehicle testing using test track and public roadway environments to send actual common message set data between vehicles.

5.2.1 Transmission Characteristics at Intersections

One goal of the testing was to evaluate the potential technical feasibility of deploying future intersection-based safety systems, like traffic signal violation warning. Testing focused on the capability of a DSRC on-board unit (OBU) to receive packets sent from a dedicated roadside unit (RSU) stationed near an intersection. A key issue investigated by VSCC was the degree to which a test vehicle could move through different types of intersections while maintaining communications with the RSU when variables such as buildings, terrain, roadway geometry and traffic conditions were presented.

The equipment used during initial phases of this evaluation consisted of test kits, radio modules, and 5.9 GHz antennas developed under VSC Tasks 4, 6A, and 6C. Fifteen intersection test sites were selected based on a broad range of characteristics. A comprehensive visualization approach involving aerial photos was used to illustrate how well packet reception is maintained as a test vehicle approaches, passes through, and moves away from an intersection.

The findings from tests conducted at a representative intersection demonstrated an 85 percent successful transmission ratio while the test vehicle was approaching the RSU from 250 m, and a 99 percent success ratio while approaching from 100 m. The results were derived with an inverted OBU roof-mount antenna serving as the RSU antenna (clearly not optimized for RSU conditions), and with the antenna situated at a less-than-optimal position (intersection corner, 10 feet high above the ground).

The transmission success ratios vary from intersection to intersection based on factors such as the density of traffic between the RSU and the OBU antennas, and whether or not the line-of-sight is blocked by objects alongside a curving roadway. Implementing an intersection-based safety application will need to address similar types of obstructions, but aside from these particular situations, the ability of a vehicle to receive packets from an RSU positioned at an intersection under realistic traffic conditions was proven.

5.2.2 Intersection Controller Data Exchange

In addition to testing transmission characteristics at intersections, arrangements were made to send test data from a roadside location in one, real-world intersection using a programmed traffic-signal-controller box. The objective was to work toward developing implementation requirements for interfacing with existing traffic control equipment to support potential vehicle safety applications effectively. Rather than connecting the test equipment to the traffic signal controller that actually controlled the traffic lights, the VSC team opted to connect the equipment to a second, independent controller.

The later phase field testing conducted at this location used test equipment developed in Tasks 6D and 9, consisting of WAVE radio modules (WRMs) and associated interface software. This new equipment was necessary in order to support the data connection from the traffic signal controller and the transmission of the resultant dynamic data. The test runs were similar to the intersection evaluations with an OBU-equipped test vehicle traveling through the test intersection.

The VSC team successfully synchronized the traffic-signal controller with the installed controller at the intersection. The OBU correctly received the traffic controller data, consisting of the signal state and the time remaining. The resolution of the time remaining (1 sec) available with the test setup was deemed not adequate. To satisfy the 100 msec safety applications update rate requirement for the RSU message, the signal controller software and serial protocol would require more elaborate modifications for improving the 200 msec update rate achieved with the controller.

For a safety application such as Traffic Signal Violation Warning, no major communications issues were uncovered in Task 10 testing that conflicted with the preliminary requirements from Task 3. DSRC 5.9 GHz wireless communication at the test intersection was characterized overall with a 93 percent successful transmission ratio over the range of interest of 250 m. Power control tests were performed to verify the capability to control the maximum range of communication at a real world intersection. The test results showed that some level of maximum transmission range control could be achieved with the proper selection of transmission power. The results show that this current test equipment, which is representative of the currently approved lower layer DSRC standard, can likely support communications for application scenarios like Traffic Signal Violation Warning.

5.2.3 Vehicle Data Exchange

Vehicle-to-vehicle testing was conducted to evaluate the performance of the WRMs and associated interface software developed in Tasks 6D and 9, and to demonstrate the wireless exchange of dynamic data between different vehicle makes.

Depending upon vehicular configuration (e.g., available sensors, vehicle-specific CAN output), various amounts of information were contained in the vehicle-to-vehicle messages sent and received between vehicles. Some vehicles exchanged full sensor data based upon the proposed SAE Common Vehicle-to-Vehicle Message Set; others provided only basic information. All messages, however, contained vehicle location (i.e., GPS) information and were typically forced to 200 bytes in size.

Results showed 100 percent reception and no packet loss between two vehicles up to ranges that exceed 200 m in a vehicle following scenario, and up to ranges exceeding 600 m in both directions of travel. Reducing the transmit power from 20 dBm to 5 dBm reduced the maximum range to approximately 250 m in both directions of travel. Increasing the data rate from 6 Mbps to 27 Mbps resulted in higher packet losses and a reduction in communication range.

Testing was conducted on an interstate freeway and a State highway. Seven test vehicles formed a caravan with information shared among all. In general, the results showed that in a freeway environment, there was communication between vehicles to 180 m range with transmission power of 20 dBm. In a freeway ramp environment, there was communication between vehicles to a 100-meter range with a reduced transmit power of 16 dBm.

Based on the vehicle-to-vehicle testing, it is clear that the performance of the WRMs is adequate for future vehicle-safety application development. The field testing suggests that safety systems using DSRC communications show promise. VSCC encourages the

next stages of development be undertaken to proceed toward the timely deployment of these potential vehicle safety applications.

5.3 Simulation Testing and Evaluation

VSCC tested and evaluated simulated DSRC performance in an urban intersection environment densely populated with DSRC-equipped vehicles and infrastructure. This was done to assess simulation test scenarios of high volume, signalized intersections. A simulation test environment was configured, containing both a high traffic volume intersection with a freeway nearby. Both environments were filled with dense vehicle traffic. Great care was taken so that both the environment and the vehicle traffic patterns reflected realistic, though stressing conditions.

The results of the simulation testing in this stressing environment showed that channel capacity will need to be preserved for effective, large-scale deployment of vehicle safety applications. Adaptive protocols for scaled situations should be developed based on the potential for temporarily or intermittently reducing update rate, transmission power, or both while recognizing congested channel conditions. These adaptive protocols for congested conditions could then be incorporated into future real-world and simulation testing to ensure that the desired application performance could be realized.

5.3.1 High Priority Emergency Messages

In Tasks 4 and 6A, the proposed priority mechanism for DSRC was found to enhance a high-priority message's likelihood of successful reception. In Task 12, this same conclusion was reached for an urban environment where high-priority emergency message prioritization consistently improved reception probability over routine messages by 5 percent to 40 percent and reduced latency across a wide-range of simulation scenarios. Overall simulation test results showed that emergency message reception probability in a city environment dropped 25 percent to 50 percent when the DSRC channel was stressed with 134 to 230 cars/lane mile transmitting 200 byte routine messages every 100 msec with a 200 m range. This suggested a requirement for a high-availability, low-latency channel for latency-critical safety applications.

To further study the support of high-priority emergency messages for critical safety applications, simulated cascading emergency messages were evaluated. This was done to emulate the expected communication pattern/protocol of a class of safety applications from Task 3 that might benefit from message cascading. The simulation test results indicated that even in a saturated channel, high-priority messages cascaded through a traffic lane of 70 vehicles within one or two repetitions per node in 0.2 to 1.2 sec. However, an in-depth analysis of safety application protocol design is needed before more meaningful insights into these results can be drawn.

5.3.2 Routine Safety Messages

The reception probability rate for routine safety messages was found to be more sensitive than emergency messages to channel loading. This sensitivity was of significant interest since the channel is expected to be occupied primarily by this class of message, due to the anticipated routine transmission of the common vehicle-to-vehicle safety message.

The simulation test environment was configured to represent a high-traffic volume intersection environment with commensurately heavy communication levels due to DSRC message density. Within this simulation context, routine message latencies at particular confidence levels were insensitive to changes in routine message transmission rates from 6 to 10 Hz. These simulation results for routine safety messages further illustrate that channel capacity is an issue that will need to be addressed adequately for large-scale deployment in stressing traffic environments.

5.3.3 Intersection RSU Rebroadcast of Routine Messages

The simulation tests demonstrated that using an intersection RSU to rebroadcast routine safety messages to improve vehicle communications around a corner causes internal queue overflow in the RSU even in an otherwise moderately loaded channel. This method did, however, improve emergency message performance around a corner since these messages were far less plentiful and at higher priority than routine messages generated from all vehicles.

5.4 Field and Simulation Testing Summary

The field testing conducted under the VSC project confirmed the viability of DSRC communications for vehicle safety applications at real intersection locations under typical traffic conditions. The field testing results also demonstrated the successful exchange of the preliminary SAE common safety message set needed for vehicle-to-vehicle safety applications between vehicles from different manufacturers. These favorable field testing results demonstrated the apparent technical feasibility of the current DSRC technology, based upon the preliminary communications requirements of vehicle safety applications. This favorable evaluation enables the future development and testing of prototype vehicle safety applications.

The simulation testing completed during the VSC project implied the requirement for a high-availability, low-latency channel for latency-critical safety applications. The simulation testing also showed that emergency message prioritization consistently improved the reception probability over routine messages by 5 percent to 40 percent, and reduced the communications latency across a wide range of simulation scenarios. The simulation results further illustrated that channel capacity is an issue that will need to be adequately addressed for large-scale deployment in stressing traffic environments.

6 DSRC Communication and Security Standards

6.1 Overview

VSCC participated in the development of the DSRC standards recently underway through standards organizations such as the American Society for Testing and Materials (ASTM), the Institute of Electrical and Electronic Engineers (IEEE), and the Society of Automotive Engineers (SAE). The goal of VSCC's participation was to ensure that the communications requirements of vehicle safety applications were addressed adequately.

VSCC worked with the standards development organizations to ensure that WAVE/DSRC standard protocols meet the needs of anticipated vehicle safety applications. This work included upper-layer WAVE standards development and WAVE/DSRC security standard development through IEEE, lower-layer standards refinement and approval through IEEE 802.11, and DSRC testing and validation standard through ASTM. It also included safety message sets and data dictionary standards development in the SAE. The direct participation of the VSCC in DSRC standards development appears to be a highly efficient way to understand, analyze, and influence the development of the majority of DSRC standards.

The DSRC communications system is based on well known wireless networking principles. The system relies on a carrier sense scheme to determine when the wireless channel is free, and uses a random time interval delay or "back off" to separate simultaneous users. This contention based scheme has proven effective in dynamic multi user wireless communications situations. Upper layers of the protocol rely on a combination of established Internet protocols and some new low latency short messaging schemes. For a more complete description of the underlying technologies, refer to the *Computer Networks* by A. S. Tannenbaum[9].

6.2 Communications Standards

The VSCC presented and interpreted the communications requirements of vehicle safety applications through active participation at DSRC standards meetings. As a result, the standards were modified or developed in a number of areas to better support the communications requirements of vehicle safety applications.

Specific areas that the VSCC addressed at standards meetings included:

- Broadcast-type messages
- Random Medium Access Control (MAC) addresses
- Short header for vehicle safety messages
- Antenna characteristics
- Vehicle safety messages on control channel

[9] Tannenbaum, Andrew S. *Computer Networks*, 3rd Edition, Prentice Hall, 1996.

- High-availability, low-latency channel
- Priority for vehicle safety applications
- Message set standardization
- Security

6.3 Standards Support for Vehicle Safety Requirements

The FCC DSRC Report and Order (FCC Document FCC 03-324 in regard to WT Docket No. 01-90 and ET docket No. 98-95, Final rule and Order Adopted December 17, 2003, and Released on February 10, 2004) went into effect in October 2004, and mandated the use of the ASTM E2213-03 lower-layer standard. The Report and Order contained a majority of features that were favorable to the potential deployment of vehicle safety applications. However, it did not mandate the high-availability, low-latency channel (ch172) suggested by the VSCC.

The ASTM E2213-03 standard mandated by the FCC appears to facilitate lower-layer interoperability. Test equipment based on this standard provided support for vehicle safety communications during the VSC field testing. This standard is currently undergoing a revision process within the ASTM committee. Plans are underway to replace the ASTM E2213-03 standard in the FCC mandate with the emerging IEEE 802.11p lower-layer standard, once it is completed. IEEE 802.11p is based on the anticipated revisions in ASTM E2213-03, and is expected to provide on-going synergies with IEEE 802.11a chipset designs.

The IEEE P1609 committee was tasked through the IEEE Project Authorization Request (PAR) for the development of the upper-layer DSRC standards. The upper-layer protocols are being planned as a complement to the lower-layer standard, and will depend upon lower layer standards for implementation. Through active participation in the IEEE P1609 committee the VSC team presented and promoted the communications requirements for vehicle safety applications. As of November 2004, a smaller technical drafting group was preparing updated draft standards for subsequent consideration by the IEEE P1609 committee. Although previous drafts of IEEE P1609 standards appeared to support vehicle safety communications requirements, the newly updated upper layer standards will need to be thoroughly analyzed and evaluated as soon as they are available. In addition, testing and validation of the DSRC standards is expected to begin as soon as software that implements the DSRC upper-layer standard protocols on generic host computers, and/or standards-compliant prototype equipment, becomes available. Revisions to the standards are likely to be required as a result of this testing and validation by various stakeholders.

A common vehicle-to-vehicle safety message set was developed in the SAE DSRC technical committee. A preliminary version of this message set was successfully sent and received using fields populated with actual CAN data between vehicles from two different manufacturers during VSC field testing. As of November 2004, a common intersection-to-vehicle safety message set was under development in the SAE committee.

A vehicle-to-vehicle safety message set to support pre-crash scenarios was also under development.

6.4 Security Standards

Security is an important consideration for DSRC vehicle safety applications. For the system to be secure, the applications must be able to trust that the communication has been received unaltered and from a known source. In addition, the communication must be anonymous, at least to passive listeners. It must require a low amount of computational and communications overhead and must be robust in the event of individual units being compromised.

There are unique DSRC security requirements for vehicle safety applications. Most of the vehicle safety application scenarios studied in the VSC project broadcast messages to all receivers, rather than directed to a given peer. This creates additional security challenges.

Vehicle safety requirements and potential solution suggestions have been presented and promoted by the VSC team to the IEEE P1556 standards development process. As of November 2004, a technical drafting group was integrating the requirements of other stakeholders with the vehicle safety requirements and proposed solutions. The result will be an updated draft standard for consideration by the IEEE P1556 committee.

6.4.1 Threats

The VSCC described a threat model, listed the constraints, and discussed these with the DSRC standardization groups. Four types of threats of increasing empowerment related to vehicle safety communication systems' endangerment were identified:

- Type 1: Attackers with a programmable radio transmitter/receiver
- Type 2: Attackers with access to an un-modified VSC unit
- Type 3: Attackers with access to a modified VSC unit who have obtained the keying material
- Type 4: Attackers inside manufacturing or security programming with full access

The capabilities of each attacker were evaluated and documented in Task 6B. System constraints in the categories of network characteristics, environmental characteristics, cost of goods, and management costs were estimated.

6.4.2 Defense

The threat model and constraints led to the core of the task—an architecture design that the VSCC believes may adequately address the identified threats while meeting the estimated constraints within this task.

- All on-board units and roadside units (RSUs) are issued certificates (OBUs are issued multiple certificates) in a special, compact format.

- The certificates for RSUs contain authorization information such as the area in which the unit is permitted to operate and the type of information it is allowed to broadcast.
- OBU certificates do not contain the permanent vehicle-identity information.
- All messages are digitally signed. Any units suspected of being compromised are put on a revocation list that is flooded to all other units.

Security comes at a price. Even with the currently proposed architecture, which includes many optimizations, each message transmitted would include significant overhead, and the message signatures would take time to process once they are received. Management of a public key infrastructure for RSUs would be necessary, according to the proposed scheme. In addition, there are piece costs, administrative costs, maintenance costs, and enforcement costs.

6.5 Standards and Security Summary

During the VSC project, a test system based on the lower-layer DSRC standard was developed and used to conduct extensive communication field testing. The preliminary SAE common safety message set needed for vehicle-to-vehicle safety applications was successfully implemented in VSCC field testing. This message set allowed the exchange of actual vehicle bus data in a standard format between vehicles from different manufacturers.

As a result of active participation in the DSRC standards development process, the VSCC evaluated proposed DSRC standards, identified specific technical issues, presented vehicle safety requirements and a proposed security solution, and secured necessary revisions in eight major areas. The IEEE committee is currently considering vehicle safety communications requirements and proposed security solution presented by the VSCC. Testing and validation of these emerging DSRC standards should be initiated as soon as the standards become available. As these standards become available for deployment, upper-layer DSRC standards enforcement will be necessary to ensure interoperability of vehicle safety applications.

The preliminary vehicle safety communications requirements appear to be well-supported by the FCC Report and Order, and the current lower-layer DSRC standards mandated by the FCC. However, the high-availability, low-latency DSRC channel that is likely required for particular vehicle safety applications was not mandated in the FCC Report and Order. Future technical work will be required to justify fully the need for the high-availability, low-latency channel, but it is important to reserve a DSRC channel at this time for this potential usage.

7 Conclusions

7.1 Summary of Project Accomplishments

The VSC project began in May 2002. The purpose of this project was to evaluate vehicle safety applications potentially enabled or enhanced by wireless communications, identify associated communications requirements, and promote the accommodation of these requirements in developing communications standards. As a result of work on this project, VSCC has:

- Prepared a comprehensive list of thirty-four potential vehicle safety application scenarios enabled or enhanced by wireless communications.
- Developed preliminary communications requirements for the potential application scenarios.
- Estimated potential safety benefits resulting from the deployment of vehicle safety applications.
- Identified eight high-priority vehicle safety applications based on estimated potential safety benefits.
- Conducted extensive communication testing on scenarios representative of the eight high-priority applications with promising results.
- Developed the first lower-layer DSRC standard compliant test system (hardware and software) with vehicle and infrastructure interfaces to enable potential prototyping of prospective communication-based vehicle safety applications.
- Conducted extensive testing at 15 intersections and confirmed the successful functioning of DSRC communications for potential vehicle safety applications at a real intersection.
- Synchronized a traffic controller unit to an existing intersection unit to transmit actual signal timing and phase for future intersection collision avoidance applications.
- Confirmed reception of signal timing and state by on-board units.
- Implemented and demonstrated successful exchange of preliminary SAE common message set needed for vehicle-to-vehicle safety applications.
- Identified channel capacity issues in traffic density scenarios through simulations and recommended development of an adaptive DSRC protocol to improve communication reliability in stressful traffic environments.
- Determined that 5.9 GHz DSRC represents the wireless technology most likely to support the communications requirements of the majority of vehicle safety applications.

7.2 VSC Findings

7.2.1 Applications

A variety of safety applications are feasible using wireless communications between the vehicle and the roadside and between vehicles. The full safety improvement impact of these applications generally depends on the extent of penetration of the systems in the vehicle fleet and the availability of supporting infrastructure systems. Therefore, conditions required for rapid and thorough infrastructure deployment across the country, and rapid penetration in to the annual vehicle build, must be established in order to fully exploit the potential safety benefits of the assessed applications.

From the 34 application scenarios potentially enabled or enhanced by wireless communications, eight were identified as high-priority and selected for further research based on the estimated potential safety benefits.

- High Potential Benefit Near-term Applications
  - Traffic Signal Violation Warning
  - Curve Speed Warning
  - Emergency Electronic Brake Lights
- High Potential Benefit Mid-term Applications
  - Pre-Crash Sensing
  - Cooperative Forward Collision Warning
  - Left Turn Assistant
  - Lane Change Warning
  - Stop Sign Movement Assistant

7.2.2 Communications

Preliminary communications requirements were determined for the eight high-priority vehicle safety application scenarios. Most of these application scenarios required periodic transmission of one-way, point-to-multipoint broadcast messages. The message packet size was 200 to 500 bytes with a communications range of 50 to 300 meters.

Several assumptions about operational characteristics are necessary to assure the functionality of the proposed/evaluated applications:

- The rapid evolution of wireless technologies will provide opportunities to use these technologies in support of advanced vehicle safety applications.
- A standardized DSRC message set and data dictionary will be established for safety applications that use vehicle-to-vehicle and/or vehicle-to-infrastructure communications. The message set would require agreement by all public and private sector organizations involved in this aspect of DSRC.

- Some applications will require vehicles periodic broadcasts (e.g., every 100 msec.) from vehicles in order to identify the roadway position. The transmitted data would need to be based on a location-referencing standard accepted by DSRC stakeholders.
- On-board units will be capable of supporting a communication range between 100 to 1000 meters.
- Suitable technical processes and supporting administrative infrastructures will be established to support secure and authenticated transactions. This includes assumptions about certificate generation and distribution, as well as OBU lifecycle management and the secure retirement of terminal equipment.

The preliminary vehicle safety communications requirements appear to be supported by the FCC Report and Order, and the current lower-layer DSRC standards mandated by the FCC. However, the high-availability, low-latency DSRC channel required for particular vehicle safety applications was not. It is expected that the communications requirements will need further refinement as prototype vehicle safety applications are developed from a safety-systems design perspective.

- Functionality of DSRC communications for vehicle safety application scenarios at real intersections was confirmed. The findings from tests conducted at a representative intersection demonstrated an 85 percent successful transmission ratio while the test vehicle was approaching the RSU from 250 m, and a 99 percent success ratio while approaching from 100 m.
- The transmission success ratios vary from intersection to intersection. Implementing an intersection-based safety application will need to address specific structural aspects of the intersection, but the ability of a vehicle to receive packets from an RSU positioned at an intersection under realistic traffic conditions was proven
- For a safety application such as Traffic Signal Violation Warning, no major communications issues were uncovered. DSRC 5.9 GHz wireless communication at the test intersection was characterized overall with a 93 percent successful transmission ratio over the range of interest of 250 m. The results show that the current test equipment, which is representative of the currently approved lower layer DSRC standard, can likely support communications for application scenarios like Traffic Signal Violation Warning.
- Simple isotropic antennas appear to meet OBU communication needs for the studied applications.

Based on the vehicle-to-vehicle testing, it is clear that the performance of the WAVE radio modules is adequate for future vehicle-safety application development. The field testing suggests that safety systems using DSRC communications show promise. VSCC encourages the next stages of development be undertaken to proceed toward the timely deployment of these potential vehicle safety applications.

Simulation testing showed that channel capacity will be a critical issue for effective, large-scale deployment of vehicle safety applications. Adaptive protocols for scaled situations should be developed based on the potential for temporarily or intermittently reducing update rate, transmission power, or both while recognizing congested channel conditions. These adaptive protocols for congested conditions could then be incorporated into future real world and simulation testing to ensure that the desired application performance could be realized.

7.2.3 Standards

The preliminary vehicle safety communications requirements appear to be well-supported by the FCC Report and Order, and the current lower-layer DSRC standards mandated by the FCC. However, the high-availability, low-latency DSRC channel that is likely required for particular vehicle safety applications was not designated in the FCC Report and Order. Future safety application prototyping will justify fully the need for the high-availability, low-latency channel, but it is important to reserve a DSRC channel at this time for this potential usage.

Plans are underway to replace the ASTM E2213-03 standard in the FCC mandate with the emerging IEEE 802.11p lower-layer standard, once it is completed. IEEE 802.11p is based on the anticipated revisions in ASTM E2213-03, and is expected to provide on-going synergies with IEEE 802.11a chipset designs.

As of November 2004, smaller technical drafting groups were preparing updated draft standards for subsequent consideration by the IEEE P1609 and P1556 committees. Although previous drafts of IEEE P1609 standards appeared to support vehicle safety communications requirements, the newly updated upper layer standards, and the P1556 security standard will need to be thoroughly analyzed and evaluated as soon as they are available.

7.3 Remaining Needs

At the present time, there are no complete, detailed safety systems designs or detailed communications requirements for specific vehicle-safety applications. DSRC communications protocols need to be identified and tested, specifically for any proposed revisions to the lower-layer standards in ASTM or IEEE 802.11p as well as upper-layer DSRC standards under development in IEEE P1609. There is a need to actively participate in the development of DSRC standards that have not yet been completed, as well as those that are anticipated to be developed in the future.

Further, there is a need to focus on complete systems designs for specific prototypes for a number of vehicle safety applications. It is not yet certain if vehicle safety applications can be designed to effectively mitigate the effects of potential channel overloading in high-traffic environments. Communications requirements need to be refined to the detailed protocol level through the design of several representative prototypes for vehicle safety applications. There is also a need to aid in the development and testing of additional vehicle safety message sets to support infrastructure-to/from-vehicle safety applications and specific applications with potentially unique message requirements.

7.4 Potential Next Steps

Based on the VSC project accomplishments, and the remaining needs that have been identified, VSCC envisions that the following steps be undertaken:

- Develop prototype cooperative intersection collision-avoidance safety applications.
- Develop prototype communication-based vehicle-to-vehicle safety applications.
- Develop adaptive DSRC protocols to improve communication reliability in stressful traffic environments.
- Continue to influence and contribute to DSRC standards development from a vehicle safety communication requirements standpoint.
- Implement and test upper-layer and security standards, when available.

DOT HS 810 591
April 2006

U.S. Department
of Transportation
**National Highway
Traffic Safety
Administration**

www.nhtsa.dot.gov
nhtsa
people saving people

Appendix A:
VSC Project Goals and Tasks

TABLE OF CONTENTS

1 Goals **2**

2 Tasks **2**

2.1 Task 1: Review of Literature and Ongoing Activities 2

2.2 Task 2: Analysis of the DSRC Standards Development Process 3

2.3 Task 3: Identify Intelligent-Vehicle Applications Enabled by DSRC 3

2.4 Task 4: Refinement of Vehicle Safety Application Communication Requirements 3

2.5 Task 5: Participation in, and Coordination with, DSRC Standards Committees and Groups 4

2.6 Task 6A: Test and Validation of DSRC Capabilities 4

2.7 Task 7: Summary of Project Results From Tasks 1 Through 6 5

2.8 Task 8: Program Management 5

2.9 Task 9: Development of Next-Generation Testing System 5

2.10 Task 10: Testing and Evaluation of WAVE/DSRC Communications Functionalities for Potential Vehicle Implementations 6

2.11 Task 11: WAVE/DSRC Security Extension 7

2.12 Task 12: Intersection and Intervehicle Safety Messaging Effectiveness Evaluation 7

2.13 Task 13: Continued Participation in WAVE/DSRC Standards Development 8

2.14 Task 14: Project Extension Program Management 8

1 Goals

The VSC project consists on a set of tasks and subsets. In general, the VSC project goals are to:

- Estimate the potential opportunity for safety benefits of communication-based vehicle safety applications in terms of reductions in vehicle crashes and functional productive years saved.
- Clearly define the communications requirements of selected vehicle safety applications.
- Work with standards development organizations to ensure that proposed DSRC communications protocols meet the needs of vehicle safety applications.
- Investigate specific technical issues that may affect the ability of DSRC (as defined by the standards) to support deployment of vehicle safety applications.
- Estimate the deployment feasibility of communications-based vehicle safety applications.
- Assess the ability of proposed DSRC communications protocols to meet the needs of safety applications.

2 Tasks

The current VSC project consists of fourteen tasks. A brief description of each task completed follows.

2.1 Task 1: Review of Literature and Ongoing Activities

Task 1 focused on defining vehicle safety applications and their communication requirements. The VSCC reviewed the results from research sponsored by USDOT, automotive OEMs, and others to support the development of a DSRC standard. Specific task outcomes included:

- Review of existing research results used to develop DSRC standards.
- Definition of vehicle safety applications and their communications requirements.
- Determination of benefits of 5.9 GHz DSRC to OEMs.
- Assessment of communications requirements of safety applications supported by current DSRC standards.

2.2 Task 2: Analysis of the DSRC Standards Development Process

Task 2 reviewed the DSRC Standards development process to determine the most effective means for light vehicle manufacturers to provide input on, and influence the details of, DSRC standards in North America. The existing DSRC standards were assessed to evaluate their impact on the future deployment of vehicle safety applications and to recommend actions to address critical issues concerning already completed standards. Specific task outcomes included:

- Assessment of current DSRC standards and evaluate their impact on future deployment of vehicle safety applications.
- Identification of standards necessary for DSRC-based vehicle safety systems applications.
- Definition of the requisite input and analysis from vehicle OEMs to support development of these DSRC standards.
- Establish a plan for developing DSRC standards.

2.3 Task 3: Identify Intelligent-Vehicle Applications Enabled by DSRC

Task 3 developed a list of vehicle safety applications that may benefit from or be enabled by DSRC. Preliminary communication requirements and potential incremental safety benefits estimates, in terms of reductions in vehicle crashes and functional productive years lost, were developed for safety applications jointly selected with the USDOT. Specific task outcomes included:

- Development of a list of vehicle safety applications that may benefit from or be enabled by DSRC.
- Analysis of the communications requirements and safety benefits of the intersection collision avoidance concepts studied by the USDOT, Infrastructure Consortium, and Virginia Tech.
- Identification of other available communication paths that may enable each safety application.

2.4 Task 4: Refinement of Vehicle Safety Application Communication Requirements

Task 4 refined the communications requirements for vehicle safety applications jointly selected with the USDOT from the preliminary requirements developed in Task 3. Applications were selected based on potential incremental safety benefit. Possible weaknesses and issues within the DSRC standards that may limit the ability to support vehicle safety applications identified in Task 3 were analyzed. In addition, test hardware was identified and assembled to provide prototype DSRC evaluation units for testing

specific implementations of communications. More extensive testing was conducted in Task 6. Specific Task 4 outcomes were:

- Analysis of possible weaknesses and issues within DSRC standards that may limit supporting the vehicle safety applications identified in Task 3.
- Assembly of test hardware to provide each VSCC member with prototype DSRC evaluation units for basic testing.

2.5 Task 5: Participation in, and Coordination with, DSRC Standards Committees and Groups

Task 5 involved the participation of VSCC in the definition and development of the DSRC standards currently underway through organizations such as the American Society for Testing and Materials (ASTM) and the Institute of Electrical and Electronic Engineers (IEEE). VSCC worked to ensure that vehicle safety applications requirements are being addressed, including planning for and implementing steps necessary to accomplish the activities described in Task 2. Specific task outcomes included:

- Participation in the development of DSRC standards in accordance with recommendations developed in Task 2.
- Providing regular status updates at DSRC standards group writing meetings.

2.6 Task 6A: Test and Validation of DSRC Capabilities

VSCC conducted tests and evaluated various aspects of DSRC performance measures to support the characterization of prototype hardware. This effort supported the layers of standards development by characterizing DSRC capabilities relative to anticipated vehicle safety applications' needs. Tests under this task were initiated through approved work orders (Tasks 6A, 6B, 6C, and 6D). The testing was based upon results from Task 4, as well as ongoing developments in the DSRC standards development process.

- Specific Task 6A, DSRC Communication Simulation Test and Protocol Research, outcomes included:
  - Development or enhancement of tools to gather empirical data and investigate performance at and near DSRC frequencies for a small numbers of vehicles.
  - Development of a DSRC simulator to focus on supporting large-scale and realistic simulation tests of generic safety applications in arbitrary complex roadway configurations at the basic radio communications level.
  - Interpretation of simulator results.
- Specific Task 6B, Security Subproject, outcomes included:
  - Description of the threat model for which a security scheme will be designed and outline the security service provided.

  - Definition of a security architecture and protocol that could meet the VSCC's needs for DSRC.
  - Development of a test plan and corresponding criteria for success for implementation and testing of the protocol.
  - Development of detailed requirements to the DSRC standards writing group.
- Specific Task 6C, Antenna Subproject, outcomes included:
  - Build and test OBU antennas in an anechoic chamber, on a test range, and atop test vehicles.
  - Summary of simulation and chamber test results.
- Specific Task 6D, WAVE Radio Module, outcomes included:
  - Development of a wireless access in vehicular environments (WAVE) radio module to support and enable future VSCC activities.
  - Build and test 20 second-generation WAVE radio module units.
  - Summary of test results.

2.7 Task 7: Summary of Project Results From Tasks 1 Through 6

VSCC assembled a final report summarizing the project results from Tasks 1 through 6. The report reviewed the current status and projected outlook of DSRC standards relative to enabling potential vehicle safety applications and identified any obstacles to deployment of DSRC enabled/enhanced vehicle safety applications.

2.8 Task 8: Program Management

Task 8 encompassed project management activities of the principal investigator. These activities include ensuring that milestones are met, revising the project plan in response to program findings, preparing materials for progress review meetings, coordinating with other organizations engaged in related activities, facilitating communication of project results within the VSCC partner companies, and preparing reports and briefings for the USDOT.

2.9 Task 9: Development of Next-Generation Testing System

Task 9 focused on developing the next generation testing system necessary to interface the Task 6D WAVE radio module with automotive network, traffic signal controllers, and research computers. Included in the system is the ability to support enhanced data acquisition capabilities, both for recording pertinent test-related information, and for acquiring and recording automotive network data pertinent to the testing in Task 10. Due to the wide range of anticipated testing uses, the next generation test system was designed

to function as a portable system with flexible system interfaces to plug into relevant automotive networks, traffic signal controllers, and research computers. The next generation test system was able to reuse laptop computers with Windows operating system installed that were previously used as part of the initial VSCC communication test kits. The software that was developed in Task 9 was configured to operate on these laptop computers and was suitable for Task 10 testing and evaluation. Specific Task 9 outcomes included:

- Establish an interface between the WAVE radio module and existing vehicle networks and between the WAVE radio module and traffic signal controllers.
- Development of software to allow transmission and reception of messages between vehicles and between vehicle and infrastructure, and to collect, log, and analyze test data on the common platform and/or existing on-board systems.
- Establish testing system requirements and architecture for common computing platform.
- Design Roadside Unit (RSU) test application to be used near a roadway infrastructure device and to broadcast traffic signal information.
- Design On-Board Unit (OBU) test application to be used in a vehicle and to wirelessly broadcast vehicle parameters and decode incoming packets containing surround parameters.

2.10 Task 10: Testing and Evaluation of WAVE/DSRC Communications Functionalities for Potential Vehicle Implementations

Task 10 tested and evaluated communications functionalities for potential vehicle safety implementations, in order to continue pre-competitive research into the feasibility of using 5.9 GHz DSRC to enable and enhance vehicle safety systems and applications. The focus of the testing was to establish feasibility and to enable future design and development of two potential vehicle safety applications—traffic signal violation warning and emergency electronic brake lights. VSCC developed communication scenarios (transmissions between a RSU and an OBU) that would support early prototype vehicle safety applications in order to evaluate communications requirements. The activities focused on data collection and analysis in preparation for the full functionality prototype development of prospective vehicle safety applications. Specific Task 10 outcomes included:

- Assessment of the viability of DSRC communications in real-world conditions and collection of raw data as a basis for future safety application algorithm development in a situation environment.
- Development of communication warning and emergency electronic brake lights.

- Development of communication scenarios to support early prototype vehicle safety applications in order to evaluate communications requirements.
- Determine implementation requirements for interfacing with existing infrastructure traffic control equipment to effectively establish vehicle safety applications.
- Evaluate available DSRC standards for communications reliability, update rate, and range.
- Conduct evaluations on test track and public roadway environments.

2.11 Task 11: WAVE/DSRC Security Extension

Task 11 addressed implementation prototyping and testing of the security approach identified in Task 6B. This task included regular technical interaction with the Task 12 protocol development activities so that security prototyping and testing results could be incorporated into the protocol development. Interactions with other VSC project extension tasks were also performed under this task, including technical coordination with the next generation testing system developments, applications prototyping activities, and standards participation task.

This task also described the threat model needed to serve as a basis for designing a security scheme and defining the security services needed, including the constraints for the security scheme (e.g., cost, bandwidth) and described the security architecture and protocol that would meet VSCC's needs for DSRC. In addition, Task 11 developed a plan and criteria for success to implement and test the protocol. Specific Task 11 outcomes included:

- Complete testing, analysis, and documentation of the results of the third-party prototyping and testing of the proposed security solution.
- Review the proposed architecture, produce a reference implementation, and create a simulation to evaluate the performance impact of the security overhead.
- Provide support to promote the VSC security solution for inclusion into the IEEE P1556 DSRC security standard.

2.12 Task 12: Intersection and Intervehicle Safety Messaging Effectiveness Evaluation

Task 12, an extension of DSRC protocol development beyond Task 6A, investigated broadcast effectiveness for VSC applications at varying communication densities, and link layer mechanisms to enhance such effectiveness. In particular, feedback oriented broadcast enhancement was examined in more depth, and additional dimension of non-uniform transmission power (i.e., aggressive power control according to the vehicle's speed) was simulated in an urban intersection environment densely populated with DSRC-equipped vehicles. The simulation environment contained a high-volume

intersection with a nearby freeway, each with dense traffic. Specific Task 12 outcomes included:

- Development, simulation, and testing of the unicast selective acknowledgement protocol techniques to mitigate channel loading and/or improve broadcast effectiveness.
- Simulate and test the effectiveness of aggressive power control schemes in a mixed traffic environment.
- Provide results and comments to the DSRC standards development process.

2.13 Task 13: Continued Participation in WAVE/DSRC Standards Development

Task 13 continued VSCC's active participation in standards development organizations to effectively influence further WAVE/DSRC standards developments to support vehicle-safety communications requirements. This task included further upper layer WAVE standards developments in IEEE, WAVE/DSRC security standard development in IEEE, lower layer standards refinement and approval in IEEE 802.11, and DSRC testing and validation standard in ASTM. Specific Task 13 outcomes included:

- Description of the current status of WAVE/DSRC standards development including an updated Task 2 roadmap.
- Identification of areas where ability to deploy vehicle safety applications based on the status of WAVE/DSRC standards development is a concern, such as broadcast-type messages, medium access control addresses, short header for vehicle safety messages, antenna characteristics, vehicle safety messages on control channel, high-availability, low-latency channel, priority for vehicle safety applications, message set standardization, and security.
- Status of incorporating VSCC positions into standards and consequences of any failures to achieve agreement on incorporation.
- Preliminary test and validation of DSRC standards.

2.14 Task 14: Project Extension Program Management

Task 14 is a continuation of Task 7 technical management of VSC project including management of daily project operation of the project, completion and review of deliverables, development and maintenance of a project plan, and coordination within and between the VSC technical and management teams.

Appendix B:
Vehicle Safety Applications

TABLE OF CONTENTS

1 Introduction 1

2 Safety-Related Applications 1

2.1 Intersection Collision Avoidance (ICA) 1

2.1.1 Traffic Signal Violation Warning 1
2.1.2 Stop Sign Violation Warning 1
2.1.3 Left-Turn Assistant 2
2.1.4 Stop Sign Movement Assistant 2
2.1.5 Intersection Collision Warning 2
2.1.6 Blind Merge Warning 2
2.1.7 Pedestrian Crossing Information at Designated Intersections Warning 3

2.2 Public Safety 3

2.2.1 Approaching Emergency Vehicle Warning 3
2.2.2 Emergency Vehicle Signal Preemption 3
2.2.3 SOS Services 3
2.2.4 Post-Crash Warning 4

2.3 Sign Extension 4

2.3.1 In-Vehicle Signage Warning 4
2.3.2 Curve Speed Warning – Rollover Warning 4
2.3.3 Low-Parking-Structure Warning 4
2.3.4 Wrong-Way-Driver Warning 5
2.3.5 Low-Bridge Warning 5
2.3.6 Work Zone Warning 5
2.3.7 In-Vehicle Amber Alert Warning 5

2.4 Vehicle Diagnostics and Maintenance 5

2.4.1 Safety Recall Notice 5
2.4.2 Just-in-Time Repair Notification 5

2.5 Information from Other Vehicles 6

2.5.1 Cooperative Forward Collision Warning 6
2.5.2 Road Condition Warning 6
2.5.3 Emergency Electronic Brake Lights 6
2.5.4 Lane Change Warning 6
2.5.5 Blind Spot Warning 7
2.5.6 Highway Merge Assistant 7
2.5.7 Visibility Enhancer 7
2.5.8 Cooperative Collision Warning 7

2.5.9 Cooperative Vehicle-Highway Automation System (Platoon) 7
2.5.10 Cooperative Adaptive Cruise Control 8
2.5.11 Road Condition Warning 8
2.5.12 Pre-Crash Sensing 8
2.5.13 Highway/Railroad Collision Warning 8
2.5.14 Vehicle-to-Vehicle Road Feature Notification 8
2.5.15 Cooperative Glare Reduction 9

3 Non-Safety Applications 9

3.1 Traffic Management 9
3.1.1 Intelligent On-Ramp Metering 9
3.1.2 Intelligent Traffic Flow Control 9
3.1.3 Free-Flow Tolling 9

3.2 Information from Other Vehicles 10
3.2.1 Instant Messaging 10
3.2.2 Adaptive Headlamp Aiming 10
3.2.3 Adaptive Drive Train Management 10
3.2.4 Enhanced Route Guidance and Navigation 10
3.2.5 Point-of-Interest Notification 10
3.2.6 Map Downloads and Updates 11
3.2.7 GPS Correction 11

1 Introduction

This appendix provides a general description of each selected vehicle safety application. The applications are classified as safety-related and non-safety-related.

- Safety-Related Applications
  - Intersection Collision Avoidance
  - Public Safety
  - Sign Extension
  - Vehicle Diagnostics and Maintenance
  - Information from Other Vehicles
- Non-Safety-Related Applications
  - Traffic Management
  - Tolling
  - Information from Other Vehicles

2 Safety-Related Applications

2.1 Intersection Collision Avoidance (ICA)

The following ICA applications were evaluated based on their ability to reduce traffic accidents at intersections.

2.1.1 Traffic Signal Violation Warning

The traffic signal violation warning application uses infrastructure-to-vehicle communication to warn the driver to stop at the legally prescribed location if the traffic signal indicates a stop and the system predicts that the driver will be in violation. The in-vehicle system uses information communicated from infrastructure located at traffic signals to determine if a warning should be given to the driver.

2.1.2 Stop Sign Violation Warning

The stop sign violation warning application uses infrastructure-to-vehicle communication to warn the driver if the distance to the legally prescribed stopping location and the speed of the vehicle indicate that a relatively high level of braking is required for a complete stop. The in-vehicle system uses information communicated from the infrastructure to provide the warning to the driver. Digital maps and GPS could be used as an alternative to DSRC communications.

2.1.3 Left-Turn Assistant

The left-turn assistant (LTA) application provides information about oncoming traffic to assist in making a left turn at a signalized intersection without a phasing left-turn arrow. Information is obtained by the infrastructure system, which uses sensors and/or DSRC communications to detect vehicles approaching from the opposite direction. This information is then used in the turning vehicle to provide gap information to the driver to assist in deciding when to turn.

One potential application is an in-vehicle system that determines a need for information about approaching traffic near an intersection based upon the driver's activation of the left-turn signal. The traffic data is gathered automatically by the infrastructure system, which detects the location and movement patterns of oncoming vehicles using vehicle detection sensors. The infrastructure system transmits the data to vehicles at regular intervals via DSRC, and the in-vehicle system provides the relevant information to the driver.

2.1.4 Stop Sign Movement Assistant

The stop sign movement assistant application provides a warning to a vehicle about to cross through an intersection after having stopped at a stop sign. Information is obtained from the infrastructure system, which uses sensors or DSRC communications to detect vehicles moving through an intersection. The application warns the driver when proceeding through the intersection is unsafe because traffic is approaching the intersection.

2.1.5 Intersection Collision Warning

The intersection collision warning application warns drivers when a collision at an intersection is probable. Infrastructure sensors and/or DSRC communications can be used to detect all vehicles, their positions, velocity, acceleration, and turning status when approaching an intersection. The infrastructure unit or the in-vehicle unit determines when a collision is imminent and issues a warning to either a specific vehicle or all drivers in the vicinity, depending on the warning strategy.

One potential application is an infrastructure system that determines the location of vehicles through infrastructure sensors (radar, cameras, etc.) and transmits this information to vehicles in the vicinity. If the in-vehicle application determines that a collision is imminent, it provides a warning to the driver.

2.1.6 Blind Merge Warning

The blind merge warning application provides a warning to the driver if a vehicle is attempting to merge from a location with limited visibility and another vehicle is approaching and is predicted to occupy merging space. Vehicles notify the roadside infrastructure unit of their velocity, acceleration, heading, and location. Based on the information sent from the vehicles and knowledge of the road, the roadside unit calculates whether a collision is imminent. The roadside unit notifies both the merging traffic and the right-of-way traffic of potential collisions. The roadside unit provides an all-clear signal when there is no approaching traffic.

2.1.7 Pedestrian Crossing Information at Designated Intersections Warning

The pedestrian crossing application provides an alert to vehicles if there is danger of a collision with a pedestrian in a designated crossing. The presence of a pedestrian is detected through infrastructure sensing equipment, including the “walk” button that pedestrians press before crossing an intersection. A broadcast message with information regarding the pedestrian is transmitted from roadside units to vehicles approaching the crossing area.

2.2 Public Safety

The following applications were evaluated based on their ability to improve general public safety.

2.2.1 Approaching Emergency Vehicle Warning

The approaching emergency vehicle warning application provides a warning to the driver to yield the right-of-way to an approaching emergency vehicle. The emergency vehicle broadcast message could include information regarding its position, lane information, speed, and intended path. The in-vehicle system uses this information to alert the driver.

2.2.2 Emergency Vehicle Signal Preemption

The emergency vehicle signal preemption warning application permits an emergency vehicle to request right-of-way from traffic signals in its direction of travel. This application allows the emergency vehicle to override intersection signal controls. An intersection-mounted roadside unit verifies that the request was made by an authorized source and alters the traffic signal and timing to provide right-of-way to the emergency vehicle. This application may need to be integrated with the approaching emergency vehicle warning application.

2.2.3 SOS Services

The SOS services application is an in-vehicle system that send emergency (SOS) messages after airbags are deployed, and a rollover or other life-threatening emergency is sensed. An occupant could also initiate the message for a non-crash-related medical or other emergency.

- ***Vehicle-to-infrastructure:*** The emergency message is sent from the vehicle to a roadside unit and then forwarded to the nearest local authority for immediate assistance.
- ***Vehicle-to-vehicle****:* The emergency message is sent from the vehicle to a passing vehicle, which stores and then relays the message when in range of a roadside unit. The message is then forwarded to the nearest local authority for immediate assistance.

2.2.4 Post-Crash Warning

The post-crash warning application is an in-vehicle system that warns approaching traffic of a disabled vehicle stuck in or near traffic lanes, as determined using map information and GPS. The application assumes communication, digital map, and GPS are still operable and may require a bottom-mounted antenna for rollover situations. This application will have the greatest benefit in poor visibility and inclement weather situations and may reduce the potential for a secondary crash.

- ***Vehicle-to-infrastructure**:* The disabled vehicle transmits its position, heading, and status to a nearby roadside unit. The unit broadcasts a warning message to vehicles approaching the accident scene and discontinues broadcast when the accident is cleared.
- ***Vehicle-to-vehicle:*** A disabled vehicle warns approaching vehicles of its position.

2.3 Sign Extension

The following sign extension applications were evaluated based on their ability to reduce traffic accidents and improve general safety.

2.3.1 In-Vehicle Signage Warning

The in-vehicle signage application provides the driver with information typically conveyed by traffic signs. Roadside units mounted at key points along the roadway send messages to approaching vehicles. In-vehicle signage features safety-critical information such as:

- ***School zone warning**:* alerts drivers that they are near a school.
- ***Animal crossing zone information**:* alerts drivers that animals tend to cross the road in the near vicinity.
- ***Sign information**:* provides information concerning dips, rough road, sudden turns, and other roadway and infrastructure characteristics.
- ***Keep clear warning**:* warns drivers that the vehicle is parked or standing in an area that should be kept clear.

2.3.2 Curve Speed Warning – Rollover Warning

The curve speed warning application aids the driver in negotiating curves at appropriate speeds using information communicated from roadside units located ahead of approaching curves. On-board vehicle information such as speed and acceleration are used to determine if the driver needs to be alerted.

2.3.3 Low-Parking-Structure Warning

The low-parking-structure warning is an in-vehicle system that provides drivers with information concerning the clearance height of a parking structure. A unit mounted on or near the parking facility provides clearance height information and location to vehicles in

the area. The in-vehicle system uses this information to decide whether to provide the driver with a warning before entering the parking structure.

2.3.4 Wrong-Way-Driver Warning

The wrong-way-driver warning application warns drivers that a vehicle is driving or about to drive against the flow of traffic. The vehicle senses its own right-of-way violation through precise positioning technology and map database data. If a right-of-way violation is sensed, the driver of the errant vehicle receives a warning, and that vehicle broadcasts information regarding its location, direction, speed, etc., to vehicles near the at-risk area.

2.3.5 Low-Bridge Warning

The low-bridge warning application provides drivers, especially of commercial vehicles, with warning messages when approaching a bridge of low height. The application is implemented with roadside units close to the bridge. Each vehicle determines whether a warning is issued to its driver.

2.3.6 Work Zone Warning

The work zone safety warning application refers to the detection of a vehicle in an active work zone area and the indication of a warning to its driver. Roadside units broadcast the warning data to vehicles as they approach a work zone or construction zone.

2.3.7 In-Vehicle Amber Alert Warning

The amber alert warning application sends alert information to the in-vehicle unit. The amber alert response program uses law enforcement and media resources to notify the public when children are suspected of being kidnapped. A sought-after vehicle could be excluded from receiving the message.

2.4 Vehicle Diagnostics and Maintenance

The following diagnostic and maintenance applications were evaluated based on their ability to improve safe vehicle operation.

2.4.1 Safety Recall Notice

The safety recall notice application distributes safety recalls through DSRC communications sent directly to vehicles via roadside units and/or in-home PCs. A safety recall reminder requiring immediate attention can be provided through a warning lamp or other methods.

2.4.2 Just-in-Time Repair Notification

The just-in-time repair notification application communicates in-vehicle diagnostics to the infrastructure and advises the driver of nearby available services. The roadside unit can pass information to an OEM technical support center for assessment. This information could be used to advise the driver of potential maintenance required.

2.5 Information From Other Vehicles

The following applications were evaluated based on their ability to reduce traffic accidents and improve public safety.

2.5.1 Cooperative Forward Collision Warning

The cooperative forward collision warning application is designed to aid the driver in avoiding or mitigating collisions with the rear end of vehicles in the forward path of travel through driver notification or warning of the impending collision. The system does not attempt to control the host vehicle in order to avoid an impending collision. This application is an enhancement of the radar-based forward collision warning system and would use information communicated from neighboring vehicles via vehicle-to-vehicle communication.

Using data regarding position, velocity, heading, yaw rate, and acceleration of other vehicles in the vicinity along with its own position, dynamics, and roadway information, the vehicle determines whether a rear-end collision with the lead vehicle is likely. The host vehicle also transmits position, velocity, acceleration, heading, and yaw rate to other vehicles.

2.5.2 Road Condition Warning

The road condition warning application is an in-vehicle system that uses on-board systems and sensors to detect marginal road conditions and transmit a road condition warning to other vehicles via broadcast. Road condition information can be used by vehicle safety applications in the receiving vehicle. The application can be designed calculate maximum speed recommendations based on road conditions and upcoming road features and notify the driver appropriately.

2.5.3 Emergency Electronic Brake Lights

The emergency electronic brake lights application is an in-vehicle system that sends a message to vehicles following behind the vehicle that brakes hard. This application helps the drivers of following vehicles by giving an early notification of the lead vehicle braking hard even when visibility is limited. This information could also be integrated into an adaptive cruise control system.

2.5.4 Lane Change Warning

The lane change warning application is an in-vehicle system that provides a warning to the driver if an intended lane change may cause a crash with a nearby vehicle. The application receives periodic updates of the position, heading and speed of surrounding vehicles via vehicle-to-vehicle communication. When the driver signals a lane change intention, the system determines and predicts the presence or absence of adequate gap between vehicles in the adjacent lane that will permit a safe lane change. If the gap between vehicles in the adjacent lane will not be sufficient, the system warns the driver that a safe lane change is not possible.

2.5.5 Blind Spot Warning

The blind spot warning application provides a warning when a driver intends to make a lane change and the driver's blind spot is occupied by another vehicle. The application receives periodic updates of the position, heading and speed of surrounding vehicles via vehicle-to-vehicle communication. When the driver signals a lane change intention, the application determines the presence or absence of other vehicles in his blind spot, and warns the driver appropriately.

2.5.6 Highway Merge Assistant

The highway merge assistant application warns a vehicle on a highway on-ramp if another vehicle is in its merge path (and possibly in its blind spot). The merging vehicle uses its navigation information to recognize that it is on an on-ramp. The in-vehicle system monitors information received from other vehicles in the area regarding their position, speed, and heading. The system warns the driver if one of the vehicles is in the merge path and is considered a potential collision threat.

2.5.7 Visibility Enhancer

The visibility enhancer application senses poor visibility situations such as fog, glare, and heavy rain either automatically or via user command. Vehicle-to-vehicle communication is used to obtain position, velocity, and heading of nearby vehicles. The application uses this information with its own GPS and map database for visibility enhancement that may range from simple to complex implementations.

2.5.8 Cooperative Collision Warning

The cooperative collision warning application collects surrounding vehicle locations and dynamics and warns the driver when a collision is likely. The vehicle receives data regarding the position, velocity, heading, yaw rate, and acceleration of other vehicles in the vicinity. Using this information along with its own position, dynamics, and roadway information (map data), the system determines whether a collision with any vehicle is likely. In addition, the system transmits position, velocity, acceleration, heading, and yaw rate to other vehicles.

2.5.9 Cooperative Vehicle-Highway Automation System (Platoon)

The platoon application provides both positional and velocity control of vehicles to operate safely as a platoon on a highway. Platooning requires vehicle-to-vehicle communication and may include vehicle-to/from-infrastructure communication. Functioning only in a control role, the application improves highway traffic flow and capacity by allowing short-range headway distance following in platoon architecture. The application combines vehicle data with position and map data. By reducing the amount of time a human controls the vehicle, the application reduces opportunities for driver error. Vehicles with this application may be required to use dedicated highway lanes. Longitudinal control of the vehicle is provided in order to maintain the short-range headway following within a platoon (similar to adaptive cruise control). Lateral control via automated steering provides lane-keeping and lane change maneuvers of platoon vehicles in a coordinated manner.

2.5.10 Cooperative Adaptive Cruise Control

The cooperative adaptive cruise control (ACC) application uses vehicle-to-vehicle communication to obtain lead vehicle dynamics and enhance the performance of ACC. Enhancements that could be made to ACC include stopped-vehicle detection, cut-in vehicle detection, shorter headway distance following, improved safety, etc. The application can be enhanced by communication from the infrastructure, which could include intelligent speed adaptation through school zones, work zones, off-ramps, etc.

2.5.11 Road Condition Warning

The road condition warning application provides warning messages to nearby vehicles when the road surface is icy, or when traction is otherwise reduced. Road condition warning may be implemented with roadside units mounted along the road at points where the road condition could change rapidly, such as bridges, low points, weather-related high frequency accident areas. The road surface condition would need to be determined by using infrastructure sensors for moisture, temperature, etc. A warning message is sent to nearby vehicles when the road surface traction is considered low enough to constitute a driving hazard.

2.5.12 Pre-Crash Sensing

The pre-crash sensing application provides a warning to prepare the vehicle and occupants for imminent, unavoidable collisions. This application could use DSRC communication in combination with other sensors to mitigate the severity of a crash. Countermeasures may include: pre-tightening seatbelts, air bag pre-arming, front bumper extension, etc.

2.5.13 Highway/Railroad Collision Warning

The highway/railroad collision warning application aids in preventing collisions between vehicles and trains on intersecting paths.

- ***Infrastructure-to-vehicle:*** This application uses information communicated from roadside units located near railroad crossings. The communicated information from roadside units would include data about approaching trains such as position, heading, and velocity.
- ***Vehicle-to-vehicle****:* This application will use information communicated from a train. The communicated information would include data about the approaching train such as position, heading, and velocity.

2.5.14 Vehicle-to-Vehicle Road Feature Notification

The road feature notification application is in-vehicle system that senses the road features such as grade, curve, etc. that exceed pre-set limits and transmits the information to other vehicles via broadcast. All vehicles within a certain area of the same road feature will be notified. The road feature information can be used by vehicle safety applications in the receiving vehicle. An application can be designed to work in the vehicle to calculate maximum speed recommendations based on road features such as road curvature ahead and notify the driver appropriately.

2.5.15 Cooperative Glare Reduction

The cooperative glare reduction application is an in-vehicle system that uses DSRC to automatically switch from high beams to low beams when trailing another vehicle. Each vehicle broadcasts its position and heading in low-light situations. If one vehicle calculates that another vehicle in front of it is within a specified range, it will switch from high to low beams.

3 Non-Safety Applications

3.1 Traffic Management

The following applications were evaluated based on their ability to improve traffic flow.

3.1.1 Intelligent On-Ramp Metering

The intelligent on-ramp metering application is infrastructure system that uses vehicle-to-infrastructure communication to measure real-time traffic density on the highway and dynamically alters on-ramp metering signal phasing. It is assumed that the infrastructure will make periodic point-to-multipoint broadcasts requesting the information from nearby vehicles. Vehicle-to-infrastructure communication from nearby highway traffic permits the ramp meter controller to adjust the signal timing based on real-time traffic flow and thereby improves traffic flow.

3.1.2 Intelligent Traffic Flow Control

The intelligent traffic flow control application is an infrastructure system that uses vehicle-to-infrastructure communication and thereby facilitates traffic light signal phasing based on real-time traffic flow. It is assumed that the infrastructure will make periodic broadcasts requesting the information from nearby vehicles. Vehicles send a message regarding their position, heading, and speed to the traffic signal infrastructure, which processes the information from each direction and determines the optimal signal phasing based on the real-time information.

3.1.3 Free-Flow Tolling

The free-flow tolling application is designed to reduce congestion and improve traffic on toll roads. The application uses communications for toll collection without the need for toll plazas along the roadway. The application can be designed to eliminate the need for vehicles to stop at toll plazas, thereby reducing stop-and-go traffic near toll collection areas.

3.2 Information from Other Vehicles

The following applications were evaluated based on their ability to improve driver comfort and enhance safety vehicle operation.

3.2.1 Instant Messaging

The instant messaging application is an in-vehicle system that enables a driver to send an instant message to another vehicle. A driver can send a message to a corresponding vehicle if the driver notices any problem such as a flat tire, missing gas cap, open trunk, etc. The message could be chosen from a list of pre-defined or customized messages. The interface for the sender of the message (i.e., how to identify the target vehicle) is not defined.

3.2.2 Adaptive Headlamp Aiming

The adaptive headlamp aiming application allows vehicles to aim their headlights in the direction of travel and more effectively illuminate the road ahead. Roadside units communicate road features that enable vehicles to appropriately aim their headlights. As an alternative to DSRC, digital maps could be used.

3.2.3 Adaptive Drive Train Management

The adaptive drive train management application is designed to improve fuel economy, emissions, and transmission shifting performance. This system uses information provided by the infrastructure regarding road features ahead to assist the engine management system of a vehicle in stabilizing its transmission. Roadside units communicate road features that enable the vehicles to anticipate appropriate shift patterns. As an alternative to DSRC, digital maps and GPS could be used.

3.2.4 Enhanced Route Guidance and Navigation

The enhanced route guidance and navigation application sends up-to-date and localized navigation information to vehicles via roadside units. Information that could be sent includes construction advisories, detours, right and left turn restrictions, and parking restrictions. This information may be temporary or too recent to appear in published navigation maps. Roadside units send enhanced route guidance and navigation information to the vehicle, which processes it and possibly merges it with its navigation system.

3.2.5 Point-of-Interest Notification

The point-of-interest notification application is a roadside unit system that provides information to passing vehicles periodically via broadcast. The information can describe features about the local area or services that are provided in the near vicinity. This application would relieve the driver from searching for a specific type of service.

3.2.6 Map Downloads and Updates

The map application downloads maps to a vehicle. A roadside unit can update a vehicle's existing maps. The kind of information provided varies with the type of roadside unit. Other units could allow entirely new maps to be bought and downloaded. If specific queries can be made from the vehicle or if a transaction is performed, two-way communication is required.

3.2.7 GPS Correction

The GPS correction application is a roadside unit that is pre-programmed with its precise location and gives this information to passing vehicles. Based on GPS coordinates and the time stamp of the message from the roadside unit to the vehicle, the vehicle can calculate its position more accurately using DGPS techniques. This application is particularly useful when the vehicle is far from a commercial DGPS station or when the differential signal is difficult to receive.

Appendix C:
Refinement of Communication Requirements

TABLE OF CONTENTS

1 Background 1-1

1.1 Communication Test Kits (CTKs) 1-1

1.2 Test Plan 1-6

2 Field Test Results 2-1

2.1 Dynamic Vehicle-Roadside Communications 2-1

2.2 Dynamic Vehicle-Vehicle Communications 2-6

2.3 Stationary Vehicle Communications 2-11

2.4 Multiple Sender Communications 2-14

2.5 Multipath Considerations 2-20

3 Simulation Architecture and Test Results 3-1

3.1 Simulation Architecture 3-1

3.2 Simulation Test Results 3-6

4 Dynamic Vehicle-to-Vehicle Communications 4-1

4.1 Test Scenario 4-1

5 Dynamic Vehicle-Vehicle Communication 5-1

5.1 Test Scenarios 5-1

6 Stationary Vehicle Communications 6-1

6.1 Test Scenarios 6-1

6.2 Multiple Senders Communications 6-35

TABLE OF FIGURES

Figure 1. Typical Antenna Mounting Configurations 1-3
Figure 2. CTK Features 1-3
Figure 3. Test Kit Diagramming Key 1-4
Figure 4. Multisender Diagramming Key 1-5
Figure 5. Evaluation Flow Overview for Task 4 1-6
Figure 6. Technical and Environmental Effects 1-7
Figure 7. Test Scenario Design 1-9

Figure 8. Test Matrix and Vehicle Configuration 1-10
Figure 9. Summary Development..... 1-10
Figure 10. Test 1-2 Results..... 2-2
Figure 11. Test 1-12 Results..... 2-2
Figure 12. Test 1-14 Results..... 2-3
Figure 13. Test 1-4 Results..... 2-3
Figure 14. Test 1-15 Results..... 2-4
Figure 15. Test 1-17 Results..... 2-4
Figure 16. Test 1-22 Results..... 2-5
Figure 17. Test 1-10 Results..... 2-5
Figure 18. Test 2-2 Results..... 2-6
Figure 19. Test 2-3 Results..... 2-6
Figure 20. Test 2-28 Results..... 2-7
Figure 21. Test 2-24 Results..... 2-7
Figure 22. Test 2-27 Results..... 2-8
Figure 23. Test 2-25 Results..... 2-8
Figure 24. Test 2-6 Results..... 2-9
Figure 25. Test 2-14 Results..... 2-9
Figure 26. Test 2-25 Results..... 2-10
Figure 27. Test 2-11 Results..... 2-10
Figure 28. Test 3-4 Results..... 2-11
Figure 29. Test 3-14 Results..... 2-11
Figure 30. Test 3-12 Results..... 2-12
Figure 31. Test 3-3 Results..... 2-12
Figure 32. Test 3-9 Results..... 2-13
Figure 33. Test 3-9 Vehicle Configuration..... 2-13
Figure 34. Test 4-4 Results..... 2-14
Figure 35. Test 4-6 Results..... 2-15
Figure 36. Test 4-1 Results..... 2-15
Figure 37. Test 4-2 Results..... 2-16
Figure 38. Test 4-9 Results..... 2-16
Figure 39. Test 4-7 Results..... 2-17
Figure 40. Test 4-3 and 4.5 Results 2-17
Figure 41. Test 4-11 Results..... 2-18
Figure 42. Test 4-12 Results..... 2-19
Figure 43. Slow Rolling Test in a Multipath Zone..... 2-20
Figure 44. Simulator Components..... 3-2
Figure 45. Traffic Trace Configuration Window 3-3
Figure 46. Graphical User Interface 3-4
Figure 47. Test Number 1-1 Results..... 4-2
Figure 48. Test Number 1-2 Results..... 4-4
Figure 49. Test Number 1-3 Results..... 4-6
Figure 50. Test Number 1-4 Results..... 4-8
Figure 51. Test Number 1-5 Results..... 4-10
Figure 52. Test Number 1-6 Results..... 4-12
Figure 53. Test Number 1-9 Results..... 4-14

Figure 54. Test Number 1-10 Results 4-16
Figure 55. Test Number 1-11 Results 4-18
Figure 56. Test Number 1-12 Results 4-20
Figure 57. Test Number 1-13 Results 4-22
Figure 58. Test Number 1-14 Results 4-24
Figure 59. Test Number 1-15 Results 4-26
Figure 60. Test Number 1-17 Results 4-28
Figure 61. Test Number 1-18 Results 4-30
Figure 62. Test Number 1-19 Results 4-32
Figure 63. Test Number 1-20 Results 4-34
Figure 64. Test Number 1-21 Results 4-36
Figure 65. Test Number 1-2 Results 4-38
Figure 66. Test Number 1-23 Results 4-40
Figure 67. Test Number 1-24 Results 4-42
Figure 68. Test Number 1-25 Results 4-44
Figure 69. Test Number 1-26 Results 4-46
Figure 70. Test Number 1-27-1 Results 4-48
Figure 71. Test Number 1-28-1 Results 4-50
Figure 72. Test Number 2-1 Results 5-2
Figure 73. Test Number 2-2 Results 5-4
Figure 74. Test Number 2-3 Results 5-6
Figure 75. Test Number 2-4 Results 5-8
Figure 76. Test Number 2-5 Results 5-10
Figure 77. Test Number 2-6 Results 5-12
Figure 78. Test Number 2-8 Results 5-14
Figure 79. Test Number 2-9 Results 5-16
Figure 80. Test Number 2-10 Results 5-18
Figure 81. Test Number 2-11 Results 5-20
Figure 82. Test Number 2-12 Results 5-22
Figure 83. Test Number 2-13 Results 5-24
Figure 84. Test Number 2-14 Results 5-26
Figure 85. Test Number 2-15 Results 5-28
Figure 86. Test Number 2-16 Results 5-30
Figure 87. Test Number 2-17 Results 5-32
Figure 88. Test Number 2-18 Results 5-34
Figure 89. Test Number 2-20-3 Results 5-36
Figure 90. Test Number 2-21 Results 5-38
Figure 91. Test Number 2-22 Results 5-40
Figure 92. Test Number 2-23 Results 5-42
Figure 93. Test Number 2-24-1 Results 5-44
Figure 94. Test Number 2-25 Results 5-46
Figure 95. Test Number 2-26 Results 5-48
Figure 96. Test Number 2-27 Results 5-50
Figure 97. Test Number 2-28-5 Results 5-52
Figure 98. Test Number 2-29 Results 5-54
Figure 99. Test Number 2-30 Results 5-56

Figure 100. Test Number 2-31 Results 5-58
Figure 101. Test Number 2-32-2 Results 5-60
Figure 102. Test Number 3-33 Results 5-62
Figure 103. Test Number 3-1 Results 6-2
Figure 104. Test Number 3-2 Results 6-4
Figure 105. Test Number 3-3 Results 6-6
Figure 106. Test Number 3-4 Results 6-8
Figure 107. Test Number 3-5 Results 6-10
Figure 108. Test Number 3-6 Results 6-12
Figure 109. Test Number 3-7 Results 6-14
Figure 110. Test Number 3-8 Results 6-16
Figure 111. Test Number 3-9 Results 6-18
Figure 112. Test Number 3-10 Results 6-20
Figure 113. Test Number 3-11 Results 6-22
Figure 114. Test Number 3-12 Results 6-24
Figure 115. Test Number 3-13 Results 6-26
Figure 116. Test Number 3-14 Results 6-28
Figure 117. Test Number 3-15 Results 6-30
Figure 118. Test Number 3-16 Results 6-32
Figure 119. Test Number 4-1 Results 6-36
Figure 120. Test Number 4-2 Results 6-38
Figure 121. Test Number 4-3 Results 6-40
Figure 122. Test Number 4-4 Results 6-42
Figure 123. Test number 4-5 Results 6-44
Figure 124. Test Number 4-6 Results 6-46
Figure 125. Test Number 4-7 Results 6-48
Figure 126. Test Number 4-8 Results 6-50
Figure 127. Test Number 4-9 Results 6-52
Figure 128. Test Number 4-10 Results 6-54
Figure 129. Test Number 4-11 Results 6-56
Figure 130. Test Number 4-12 Results 6-58

TABLE OF TABLES

Table 1. Test Scenario 1-1 4-1
Table 2. Test Scenario 1-2 4-3
Table 3. Test Scenario 1-3 4-5
Table 4. Test Scenario 1-4 4-7
Table 5. Test Scenario 1-5 4-9
Table 6. Test Scenario 1-6 4-11
Table 7. Test Scenario 1-9 4-13
Table 8. Test Scenario 1-10 4-15
Table 9. Test Scenario 1-11 4-17

Table 10. Test Scenario 1-12 4-19
Table 11. Test Scenario 1-13 4-21
Table 12. Test Scenario 1-14 4-23
Table 13. Test Scenario 1-15 4-25
Table 14. Test Scenario 1-17 4-27
Table 15. Test Scenario 1-18 4-29
Table 16. Test Scenario 1-19 4-31
Table 17. Test Scenario 1-20 4-33
Table 18. Test Scenario 1-21 4-35
Table 19. Test Scenario 1-22 4-37
Table 20. Test Scenario 1-23 4-39
Table 21. Test Scenario 1-24 4-41
Table 22. Test Scenario 1-25 4-43
Table 23. Test Scenario 1-26 4-45
Table 24. Test Scenario 1-27 4-47
Table 25. Test Scenario 1-28 4-49
Table 26. Test Scenario 2-1 5-1
Table 27. Test Scenario 2-2 5-3
Table 28. Test Scenario 2-3 5-5
Table 29. Test Scenario 2-4 5-7
Table 30. Test Scenario 2-5 5-9
Table 31. Test Scenario 2-6 5-11
Table 32. Test Scenario 2-8 5-13
Table 33. Test Scenario 2-9 5-15
Table 34. Test Scenario 2-10 5-17
Table 35. Test Scenario 2-11 5-19
Table 36. Test Scenario 2-12 5-21
Table 37. Test Scenario 2-13 5-23
Table 38. Test Scenario 2-14 5-25
Table 39. Test Scenario 2-15 5-27
Table 40. Test Scenario 2-16 5-29
Table 41. Test Scenario 2-17 5-31
Table 42. Test Scenario 2-18 5-33
Table 43. Test Scenario 2-20 5-35
Table 44. Test Scenario 2-21 5-37
Table 45. Test Scenario 2-22 5-39
Table 46. Test Scenario 2-23 5-41
Table 47. Test Scenario 2-24 5-43
Table 48. Test Scenario 2-25 5-45
Table 49. Test Scenario 2-26 5-47
Table 50. Test Scenario 2-27 5-49
Table 51. Test Scenario 2-28 5-51
Table 52. Test Scenario 2-29 5-53
Table 53. Test Scenario 2-30 5-55
Table 54. Test Scenario 2-31 5-57
Table 55. Test Scenario 2-32 5-59

Table 56. Test Scenario 2-33 5-61
Table 57. Test Scenario 3-1 6-1
Table 58. Test Scenario 3-2 6-3
Table 59. Test Scenario 3-3 6-5
Table 60. Test Scenario 3-4 6-7
Table 61. Test Scenario 3-5 6-9
Table 62. Test Scenario 3-6 6-11
Table 63. Test Scenario 3-7 6-13
Table 64. Test Scenario 3-8 6-15
Table 65. Test Scenario 3-9 6-17
Table 66. Test Scenario 3-10 6-19
Table 67. Test Scenario 3-11 6-21
Table 68. Test Scenario 3-12 6-23
Table 69. Test Scenario 3-13 6-25
Table 70. Test Scenario 3-14 6-27
Table 71. Test Scenario 3-15 6-29
Table 72. Test Scenario 3-16 6-31
Table 73. Test Scenario 3-17 6-33
Table 74. Test Scenario 4-1 6-35
Table 75. Test Scenario 4-2 6-37
Table 76. Test Scenario 4-3 6-39
Table 77. Test Scenario 4-4 6-41
Table 78. Test Scenario 3-14 6-43
Table 79. Test Scenario 4-6 6-45
Table 80. Test Scenario 4-7 6-47
Table 81. Test Scenario 4-8 6-49
Table 82. Test Scenario 4-9 6-51
Table 83. Test Scenario 4-10 6-53
Table 84. Test Scenario 4-11 6-55
Table 85. Test Scenario 4-12 6-57

1 Background

In order to refine the initial communication requirements that were established in Task 3 for potential 5.9 GHz safety applications, the Vehicle Safety Communications Consortium (VSCC) developed a specialized Communications Test Kit (CTK) and a mobile communications network simulator. The test kits and simulator were used to validate the Task 3 communications parameters and provide informed input to the Dedicated Short Range Communications (DSRC) standards development efforts. All VSCC member-companies were provided with two CTKs for investigations within the VSC project, particularly the Task 4 testing activity.

1.1 Communication Test Kits

Though the DSRC standards were incomplete, it was feasible to use and modify existing 802.11a equipment to simulate performance in the DSRC band. In order to use the equipment for test purposes, original software had to be written to integrate the various components and provide the necessary test environment to configure, conduct, record, analyze, and display generated test results. The VSCC agreed to have DaimlerChrysler define, develop, and assemble the CTKs based on their past experience with similar equipment. The next step was to define essential CTK features required for baseline functionality.

The CTKs were intended to support testing of multiple vehicles' communications on roadways at normal driving speeds. In order to accomplish anticipated tests in a vehicular environment, the VSCC derived the following CTK functional requirements:

- Communications based on a representative 802.11a radio.
- Mobile computing platform interfaced with the radio to support test configuration, operation, and documentation.
- Measurable and recordable communications performance data.
- Optimized communication paths between radios.
- Accurate and recordable position knowledge of test vehicles that is synchronized with test data and updated frequently.
- A minimum of two test kits for performing wireless communication testing.
- Post-processing for data analysis.

A further requirement was that the 802.11a device should be able to connect directly with a host computer, and that the computer should be portable to allow easy transition between vehicles. External antennas for the 802.11a frequency should be mounted on the vehicle exterior, and a Differential Global Positioning System (DGPS) receiver would be needed for relatively accurate vehicle position readings.

1.1.1 Test Kit Hardware

Given the preceding requirements, DaimlerChrysler, with VSCC participation, assembled the following components to create the baseline CTK:

Item	Brand and Model	Comments
802.11a radio	Atheros model AR5211, mini-PCI format (MB23 board)	The mini-PCI format supports external antennas (note antenna connectors and cables on top right of photo). This format also provides a higher maximum transmit power than the PC card version.
GPS receiver	DGPS Max from Communications Systems International, Inc.	This differential GPS receiver determines position accuracy to 1 - 3 meters 95 per cent of the time. It also has a 5 Hz update rate.
Laptop	IBM T23 laptop	IBM T series laptops have a mini-PCI slot in the base that is user accessible. They also have a serial port for the DGPS interface. Note the installed 802.11a card and attached pigtail RF coaxial cables.
Antenna	Atheros Access Point antennas (AP21 antenna)	These strip antennas are optimized for 802.11a operation in the 5.1-5.3 and 5.8 GHz range. They also allow for mounting away from the 802.11a radio, but came as bare units with only an RF connector on the base.
Antenna enclosure	Hayes, custom design	Clear polycarbonate enclosures with magnetic mounts were designed and built specifically for the Atheros antennas. These were essential for tests with external antennas at vehicle speeds.
RF coaxial cables	Talley Communications, custom build	These low loss cables were custom built to remotely connect the antenna to the radio card. They also allow for the anticipated distance between the external antenna and the rest of the test kit inside the vehicle.

A custom antenna housing and mount were needed to protect the 802.11a antennas at freeway speeds and to secure it to the vehicle exterior. Examples of the typical antenna mounting configurations on different vehicle types are shown below:

Figure 1. Typical Antenna Mounting Configurations

1.1.2 Test Kit Software

Test kit software for the host laptop computers needed to be developed. Initial testing was conducted with Version 2.3 software, and subsequent revisions were made to more closely resemble the anticipated DSRC standard and to improve the capabilities of the CTK. The latest revision used in formal evaluation (shown in the table below as Version 3.0) accommodated multi-sender testing.

CTK S/W v2.3	CTK S/W v3.0	DSRC Standard
25/50 mW default antenna input power settings	Programmable antenna input power (100 mW spec.)	Up to 750 mW variable antenna input power
5.15-5.35, 5.725-5.825 GHz	5.15-5.35, 5.725-5.825, 5.85-5.925 GHz	5.85-5.925 GHz
20 MHz channel	10 MHz channel	10/20 MHz channels
Single-sender capable	Multi-sender capable	Multi-sender capable
Real-time range	Real-time range/RSSI	N/A
Pre-set channel	Selectable channel	Channel switching
Diversity antennas	Diversity with manual override	N/A
IEEE 802.11 Ad hoc	DSRC Ad hoc	DSRC Ad hoc
6-54 Mbps	3-27 Mbps	3-27 Mbps

Figure 2. CTK Features

The software has several components, each with specific functions:

- GPS library for converting the DGPS receiver data to a compatible format within the test kit laptop.
- VSC Test Kit Sender for configuring communication and test parameters, recording sending vehicle position, and transmitting test data packets from a single CTK.
- VSC Test Kit Receiver for configuring communication and test parameters and recording received data packets and vehicle position.
- VSC Test Kit Notation for annotating specific events during testing.
- VSC Test Kit Diagram for post-processing and displaying the test data results.

1.1.3 Test Kit Diagramming Function

The CTK diagramming function provides a means to display the test data results in a graphical format. A sample diagram from the Version 2.3 software is shown below. In this test, 236 packets were sent, 206 packets were received, and 30 packets were lost over a 26 second test duration and vehicle separation distances ranging from 85 to 105 meters. The test was conducted on a test track with one vehicle slowly moving away from the other.

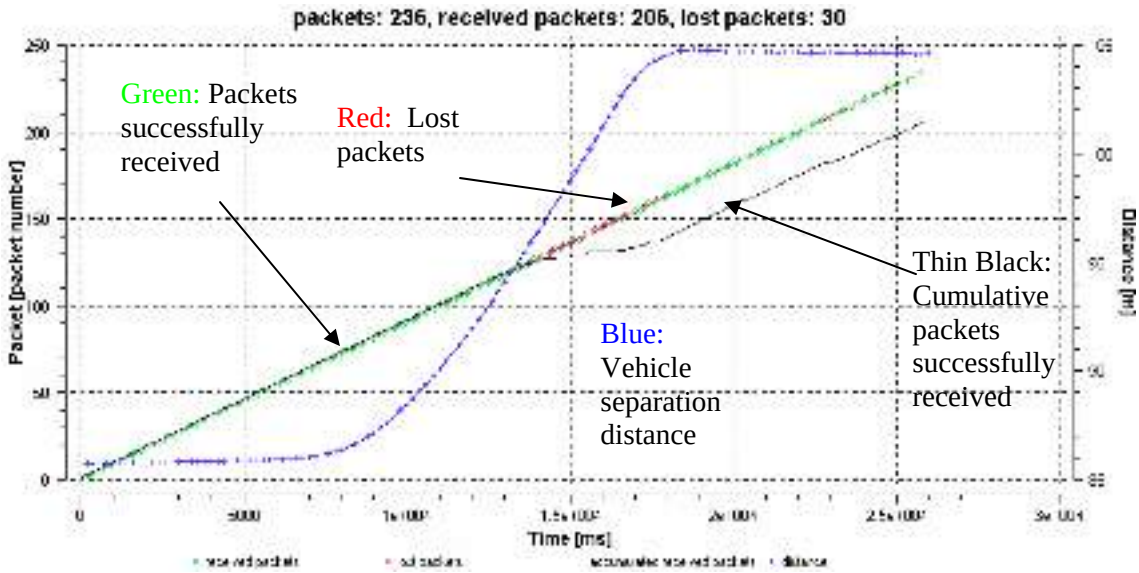


Figure 3. Test Kit Diagramming Key

Additional data capture capabilities were added during the course of the project. One of the major improvements was the addition of the received signal strength indication (RSSI). The RSSI is not plotted against specific values shown on an axis, but it provides an indication of the received power (sensitivity between –96 dBm and –36 dBm). This allows for more detailed analyses of the correlations between packet loss and

obstructions, for example. A significant convenience feature has also been added to the test kits: a dynamic display of the distance between test vehicles in field test situations. This feature made field-testing much more precise, by allowing separation distances between moving vehicles to be maintained within the desired scenario values.

The diagram below shows the RSSI feature along with the addition of the multiple sender functionality. In order to clearly show the data received from both sending vehicles, note that the data from Sender 1 is offset from that of Sender 2. The use of offsets is evidenced by the negative values that appear on the Y-axis of the graph. The range and packet offset levels for Sender 1 are 50 meters and 200 packets.

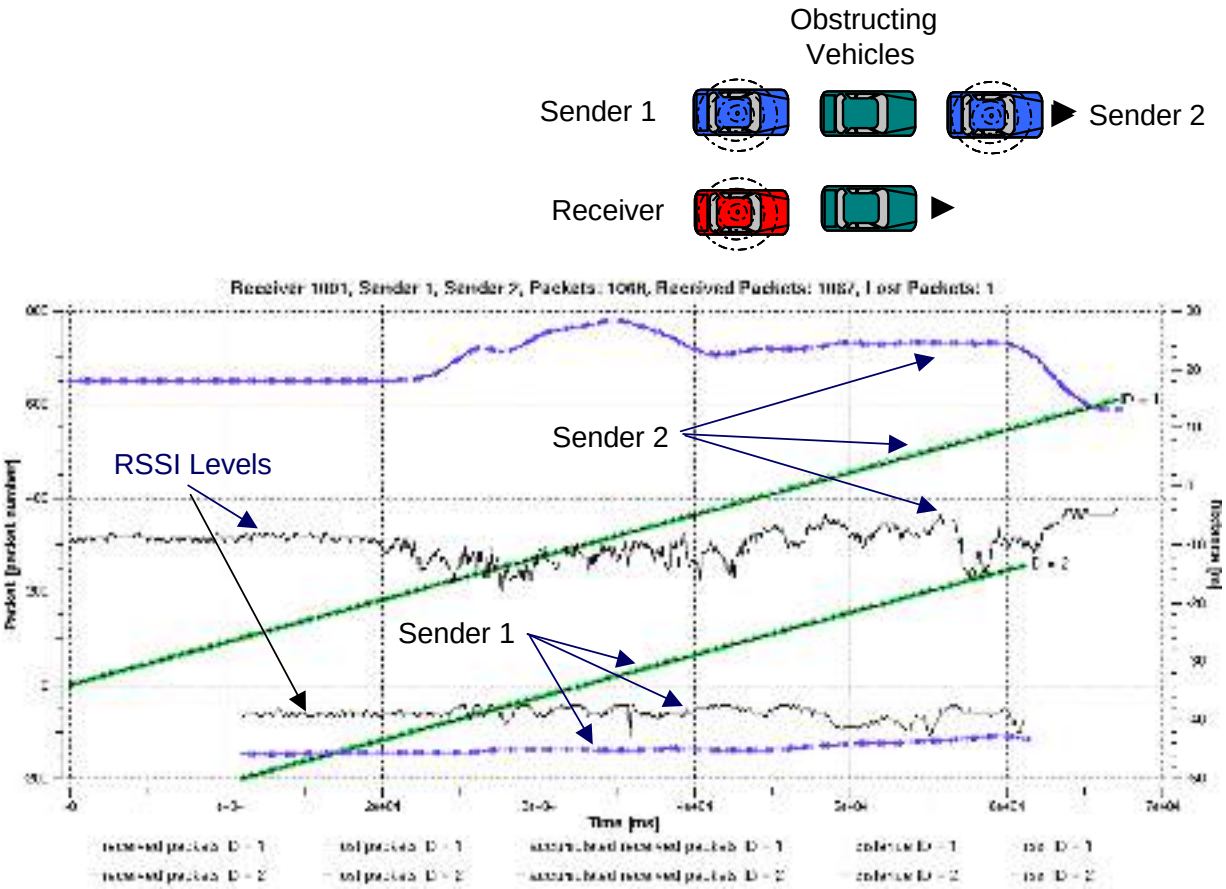


Figure 4. Multi-Sender Diagramming Key

1.2 Test Plan

Test scenarios have been defined by delineating the Technical Parameters and Environment Effects required to create the Requirements Summary (see the figure below). This has led to the definition of evaluation items within each application, scenario, and associated tests, and subsequently scripting the example test scenarios to address those areas of focus. The goals of the Task 4 example test scenarios were to create a testing procedure that could evaluate the test kits' development and provide timely feedback to the DSRC Standards development.

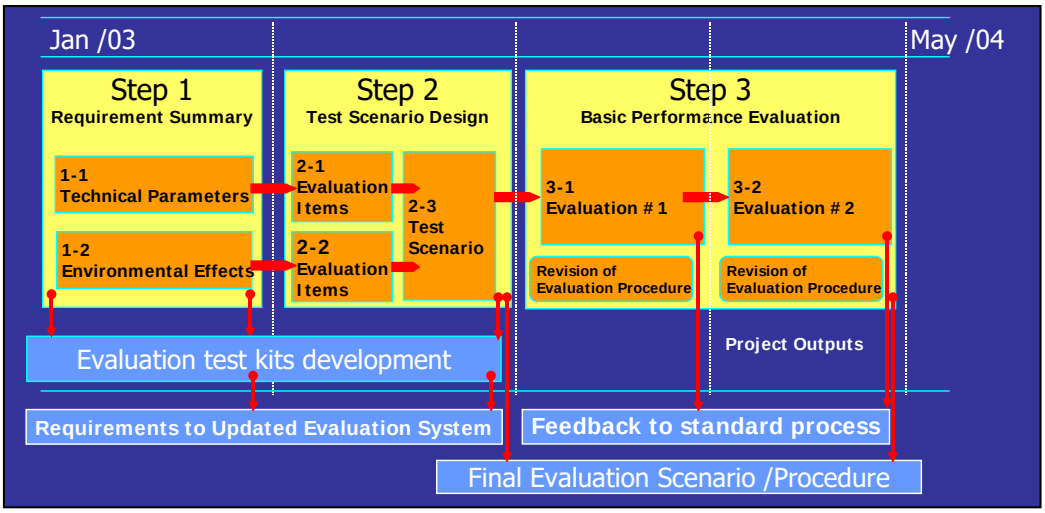


Figure 5. Evaluation Flow Overview for Task 4

1.2.1 Scenario Definition

The word "scenario" could have multiple meanings since every unique variable change within an environment creates a different scenario. After evaluating the aforementioned factors, VSCC grouped blocks of similar situations by the quantity of "sending" antennas required (*the eight priority applications from Task 3 require, at times, multiple sending antennas) and their relative movement, and described each assemblage with a "base scenario." To this base scenario, other technical parameters and environmental effects were added to define various test situations and sketches.

1.2.2 Technical Parameters

Technical parameters are defined herein as a subset of the overall variables within or between the test kits that may be considered when given a sterile or laboratory environment. Those variables that are introduced once the test kits and vehicles are introduced into "real-world" conditions are deemed environmental effects and are described in section 1.2.3.

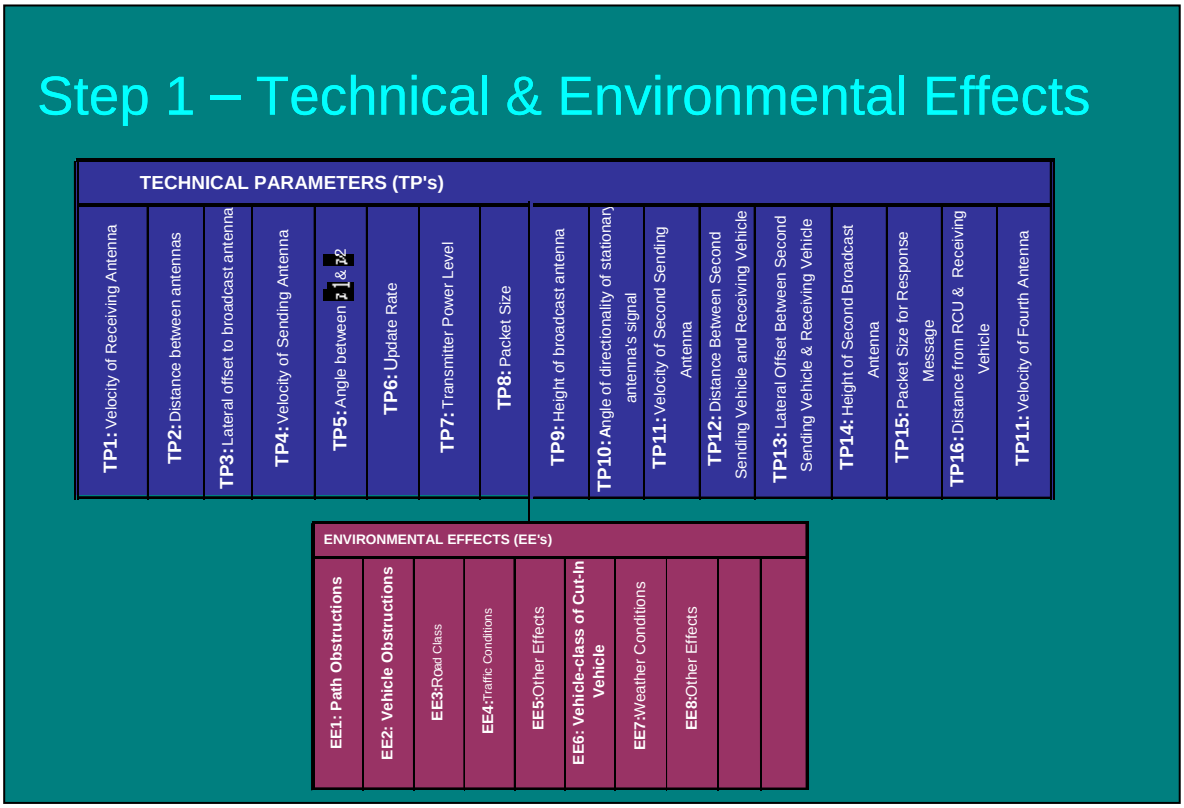


Figure 6. Technical and Environmental Effects

The variables shown below are the technical parameters that will be varied during Task 4 and, mostly likely, future tests:

- **v_1: Velocity of Receiving Antenna** – This value represents the speed (in miles per hour) of the receiving antenna; coupled with the sketch creates the velocity. The receiving antenna may be stationary in some tests (v_1 = 0 mph), thereby simulating an RSU.
- **d_{y1}: Distance Between Antennas** – This represents the distance (in meters) between the receiving antenna and the first sending vehicle along the y-axis.
- **d_{x1}: Distance Between Antennas** – This represents the distance (in meters) between the receiving antenna and the first sending vehicle along the x-axis. Four meters is meant to simulate one car lane.
- **v_2: Velocity of Sending Antenna** – This value represents the speed (in miles per hour) of the sending antenna; coupled with the sketch creates the velocity. The sending antenna may be stationary in some tests (v_2 = 0 mph), thereby simulating an RSU.
- **α: Angle Between v_1 & v_2 –** This angle describes the difference in direction between the sending & receiving antenna's velocity, and serves simply as a numerical reinforcement of the test sketches' velocities.

- **ξ: Update Rate –** This represents the inverse of the number of times per second the test kits are sending the packets of information, and is expressed in milliseconds.
- **P_t: Transmitter Power Level –** This percentage describes at what relative level the sender is broadcasting the communication with respect to full potential power.
- **s_1: Packet Size** – The test kits broadcast a message of specified packet size (in bytes) wirelessly to the receiving antenna which may be varied by the engineer.
- **d_{z1}: Distance Between Antennas** – This represents the distance (in meters) between the receiving antenna and the first sending vehicle along the z-axis (see sketches). The z-axis height for all antennas will be fixed throughout Task 4 for testing simplicity.
- **d_{x2}, d_{y2}, & d_{z2},: Distance Between Antennas** – This represents the distance (in meters) between the receiving antenna and the second sending vehicle along all three axes.
- **ϕ: Angle of Directionality of Stationary Antenna's Signal–** This angle designates the directionality of the sending antenna.
- **v_3: Velocity of Second Sending Antenna** – This value represents the speed (in miles per hour) of the second sending antenna; coupled with the sketch creates the velocity. The sending antenna may be stationary in some tests (v_2 = 0mph), thereby simulating an RSU.
- **v_4: Velocity of Fourth Antenna** – This value represents the speed (in miles per hour) of the fourth antenna; coupled with the sketch creates the velocity. The sending antenna may be stationary in some tests (v_2 = 0mph), thereby simulating an RSU.

1.2.3 Environmental Effects

Environmental effects are defined herein as the variables that are introduced once the test kits and vehicles are introduced into “real-world” conditions. The variables shown below are the environmental effects that will be varied during Task 4 and, mostly likely, future tests:

- **Path Obstructions** – This is a reference indicator of whether a building or roadside structure shall be within the intended path of communications.
- **Vehicular Obstruction(s)** – This is a reference indicator of whether a vehicle shall be within the intended path of communications. This vehicle may be designated as a “cut-in” (temporary) or “sustained” (continuous) obstruction.
- **Road Class** – This designates the general category of road design (arterial, highway, test track) that shall be used for the specified test.

- **Traffic Conditions** – This loosely designates the relative volume of uncontrolled traffic desired while conducting the test (e.g., light, heavy).
- **Vehicle Class Of Cut-in Vehicle –** This loosely describes the size of vehicular obstruction (e.g., sedan, SUV, truck).
- **Weather** – This variable loosely describes the ambient conditions (e.g., raining, snowing, sunny) required to run the test.
- **Other** – Other variables which should be considered once Task 4 evaluations have shed light on conditions beyond the vehicle's design.

1.2.4 Scenario Definition

The figure below shows four test scenarios with their representative vehicle configurations. Testing for the first three scenarios was conducted using CTK v2.3 software, while tests for Scenario 4 were conducted with CTK v3.0 software.

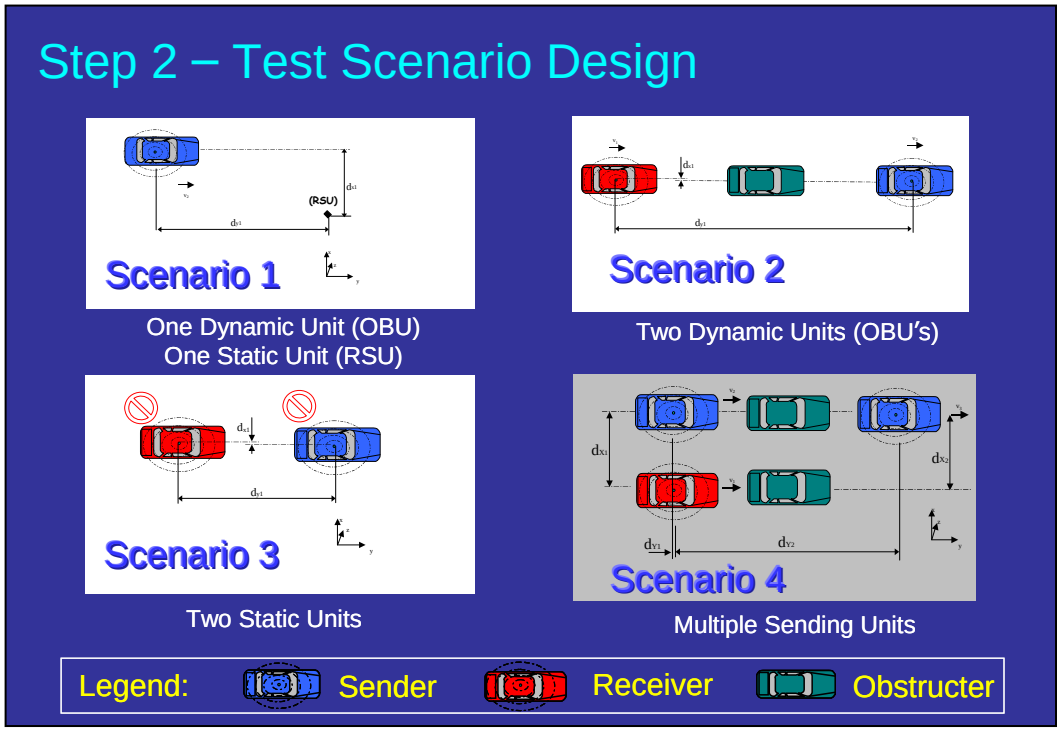


Figure 7. Test Scenario Design

1.2.5 Basic Performance Evaluation

The test plan was constructed based upon multiple field trials under each of the Task 4 test scenarios described in a test matrix. These test scenarios were chosen by the technical team to allow thorough field-testing and validation of the communications requirements for the eight high-priority application scenarios identified in Task 3.

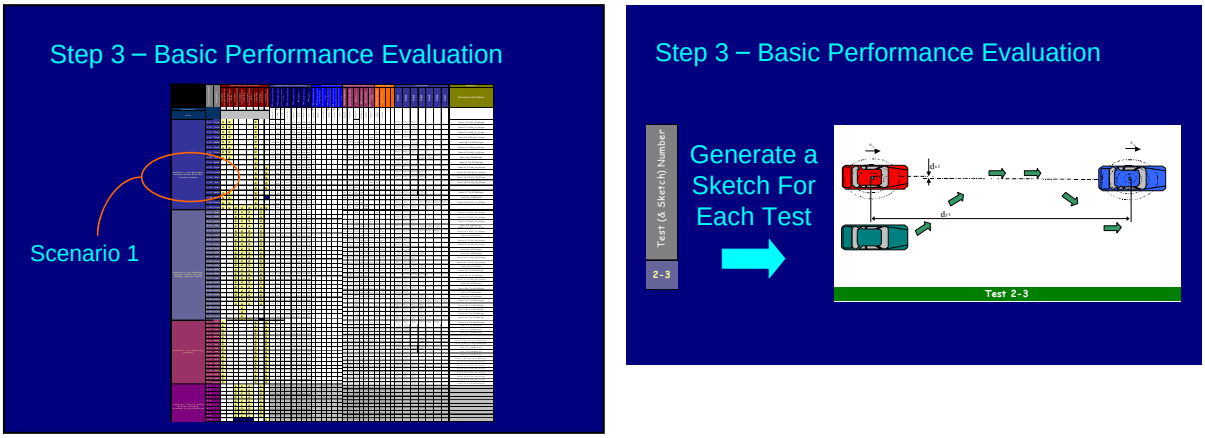


Figure 8. Test Matrix and Vehicle Configuration

The test data was collected during the field-testing. After analysis of multiple trials for each test scenario, a summary was prepared to illustrate the test results.

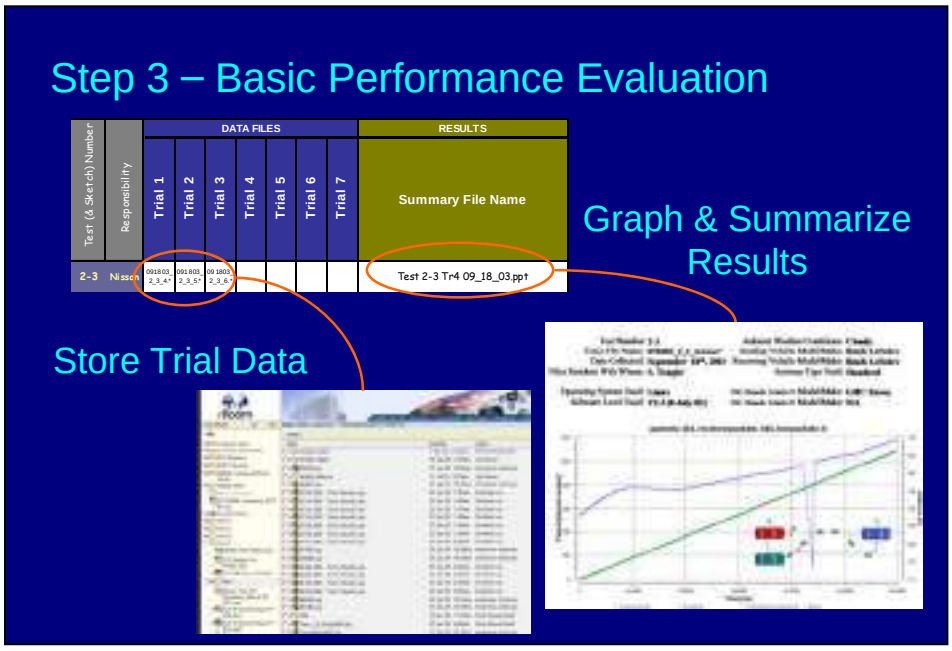


Figure 9. Summary Development

2 Field Test Results

The field-testing program was conducted using test track facilities at GM's Milford Proving Ground as well as testing on public roadways. The testing was conducted in accordance with the test scenarios described in the test plan, as well as detailed explorations of several factors that emerged from the initial test results.

Since DSRC equipment was not yet available, 802.11a was used to approximate DSRC operations. The general conditions throughout all the field-testing (with the exception of several tests with power control and multiple sender scenarios), included: broadcast of repetitive small packets (100-400 bytes), update rates of 50-100 milliseconds, ranges exceeding 300 meters, 5.15-5.25 GHz (802.11a) transmission frequencies, 20 MHz channel width, around 50 milliwatt transmission power (at the output port of the radio card), dry weather, and 6 Mbps data rate.

In general, multiple test runs were completed for each test scenario. After the test runs were completed for each scenario, the test data were analyzed and evaluated. A summary of the test results was then prepared for each of the test scenarios.

The test scenarios can be divided into five main categories:

- Dynamic Vehicle-Roadside Communications
- Dynamic Vehicle-Vehicle Communications
- Stationary Vehicle Communications
- Multiple Sender Communications
- Multipath Considerations

The following sections summarize the test results in each category by presenting examples of the test results on a scenario-by-scenario basis within each of the main categories. Further details of each particular test can be found at the end of this appendix. An illustration of each scenario graphically portrays the test result summary for the examples shown.

2.1 Dynamic Vehicle-Roadside Communications

The testing of dynamic vehicle-roadside communications within the scope of Task 4 consisted of using a stationary test vehicle located beside the roadway as a surrogate for the roadside unit (RSU). The main limitations that were imposed by this arrangement were the constraints on antenna height and placement.

Tests performed in a test track environment showed excellent communication performance for transmissions having both direct line-of-sight (LOS), and also a single vehicle obstructing the LOS between the sending and receiving antennas. The following diagrams illustrate the results found during these tests. The diagram below (Test 1-2) shows a receiving vehicle traveling at 60 mph with no packet loss 300 meters before passing the stationary sending antenna, and 300 meters after.

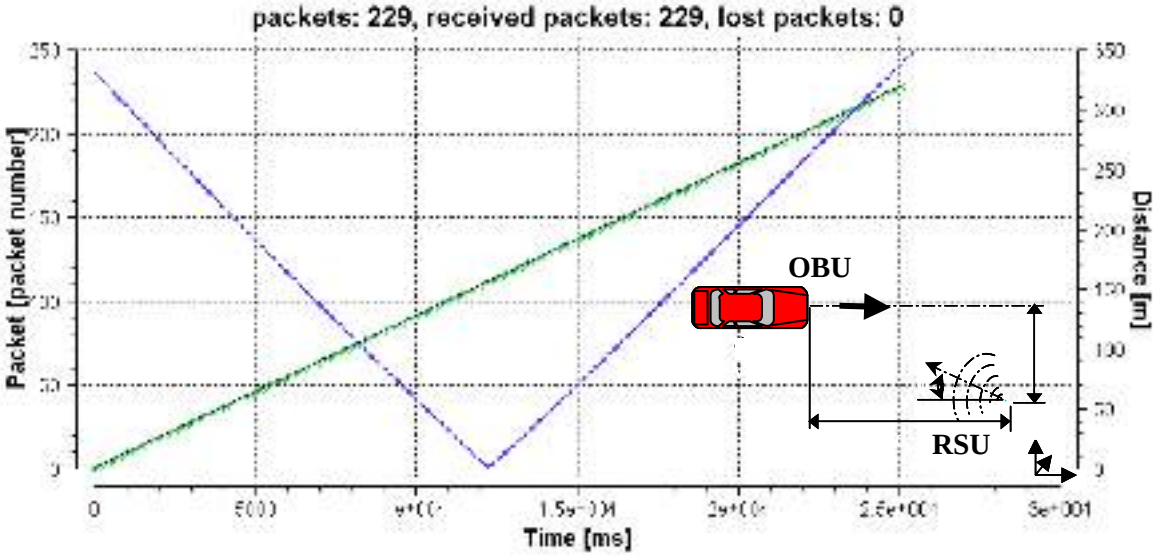


Figure 10. Test 1-2 Results

A similar test was conducted in which the moving vehicle transmits packets instead of receiving them (Test 1-12). In this trial, a few packets were lost at a range of about 90 meters, but over 99 percent of the packets were still received.

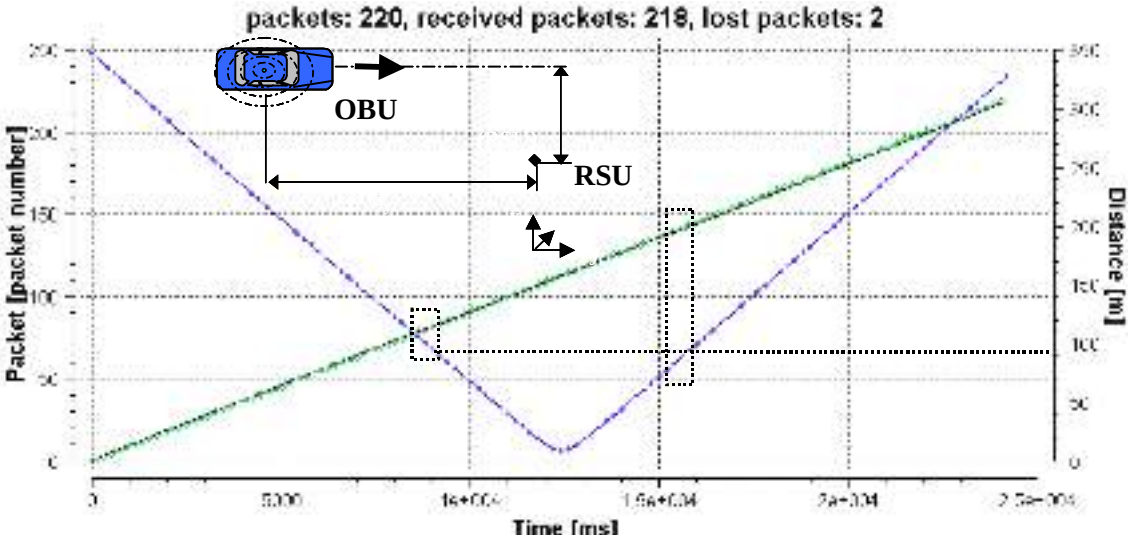


Figure 11. Test 1-12 Results

Similar results were found in a test in which the moving vehicle slows down to 20 mph (Test 1-14). In this case, a few packets are lost at a range close to 80 meters both before and after the transmitting vehicle passes the stationary antenna.

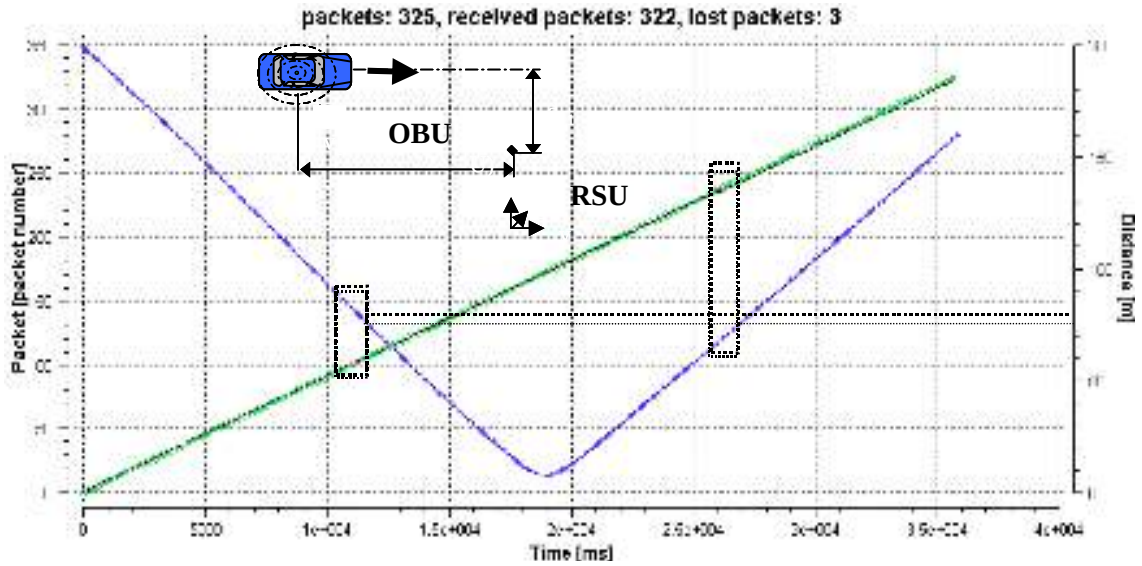
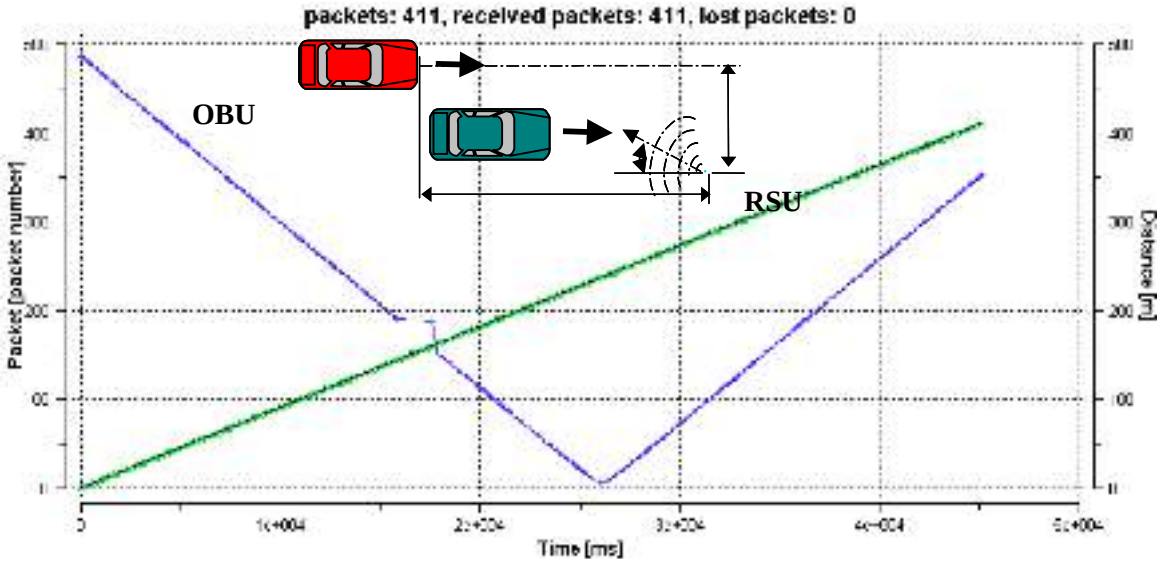


Figure 12. Test 1-14 Results



This pattern of lost packets at distances close to 80-90 meters was investigated further, and the findings are described in Section 2.5: Multipath Considerations. The results were similar when an obstructing SUV moving at the same speed as the receiving sedan blocked the direct line-of-sight to the stationary antenna (Test 1-4). There were no lost packets with the vehicles moving at 40 mph.

Figure 13. Test 1-4 Results

The same was true when the moving vehicle changed its role from the receiver to the transmitter (Test 1-15). There were no lost packets while traveling at 40 mph.

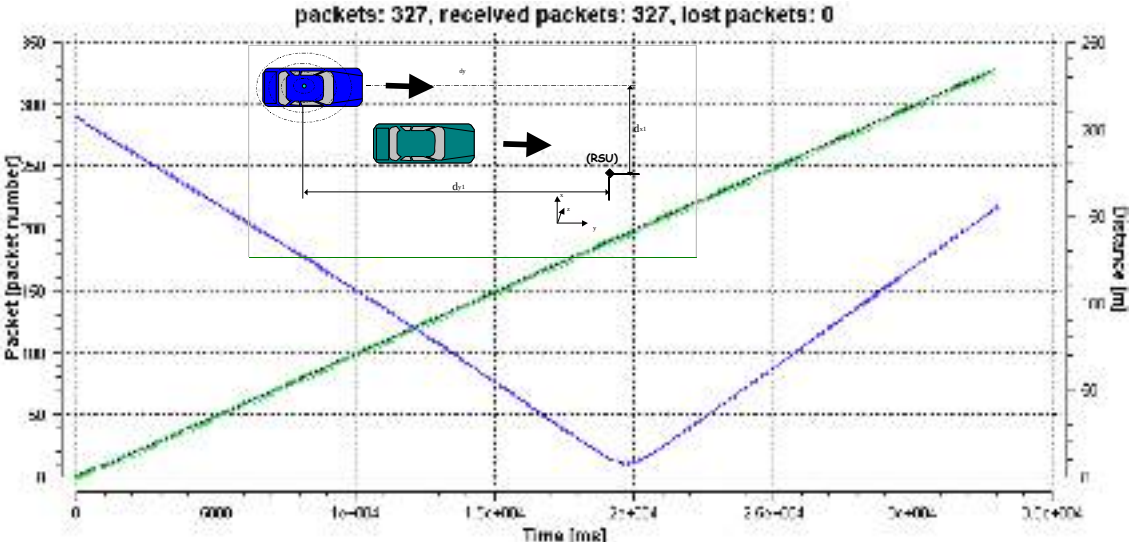


Figure 14. Test 1-15 Results

The public road tests featured results with passing vehicles, cut-in vehicles, and other variables to complicate the transmission environment. The diagram below shows a receiving vehicle passing a stationary sending antenna at 60 mph along a highway with light traffic conditions (Test 1-17). Almost no packets were lost on the straight-away for the middle section of the test. There was no reception before and after the straight-away where the road makes sharp bends and obstruction blocked the antennas.

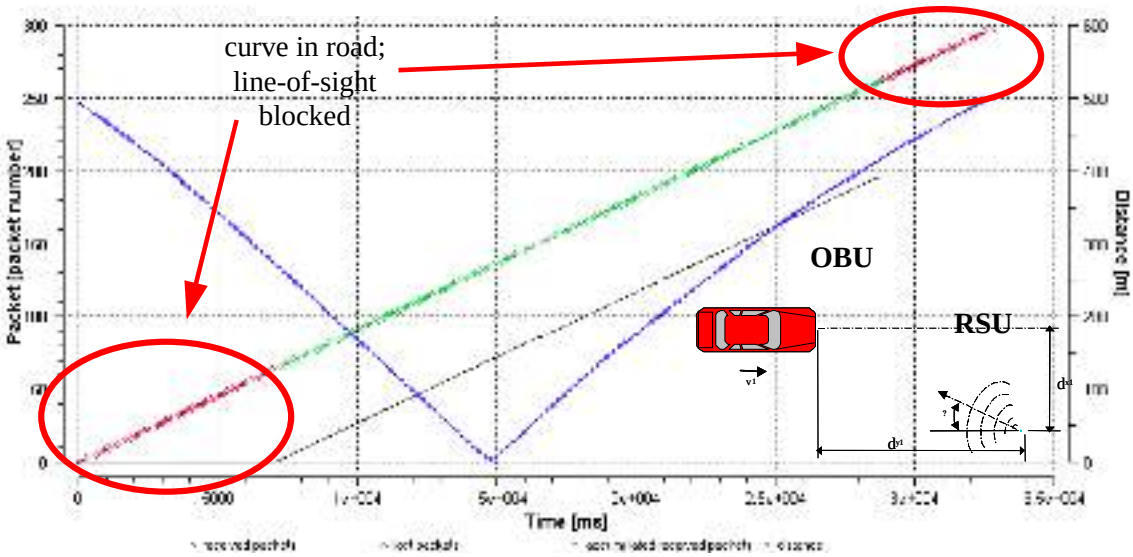


Figure 15. Test 1-17 Results

More packets were lost in heavier vehicle traffic, as the diagram below illustrates (Test 1-22). This test took place on an arterial road in a rural environment at 30 mph, and heavy traffic periodically blocked the line-of-sight while the receiving vehicle approached the roadside unit. After the vehicle passed the RSU, it went over a hill and out of line-of-sight.

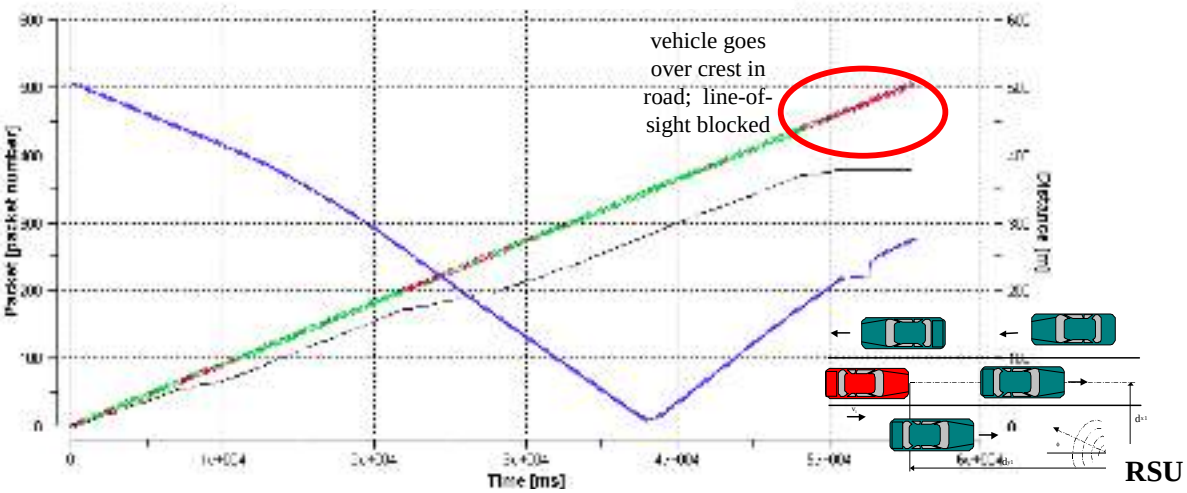


Figure 16. Test 1-22 Results

Another test showed similar results with the line-of-sight being blocked by a truck in addition to the SUV used for the trial (Test 1-10). As the sender goes out of line-of-sight, the RSU started losing packets.

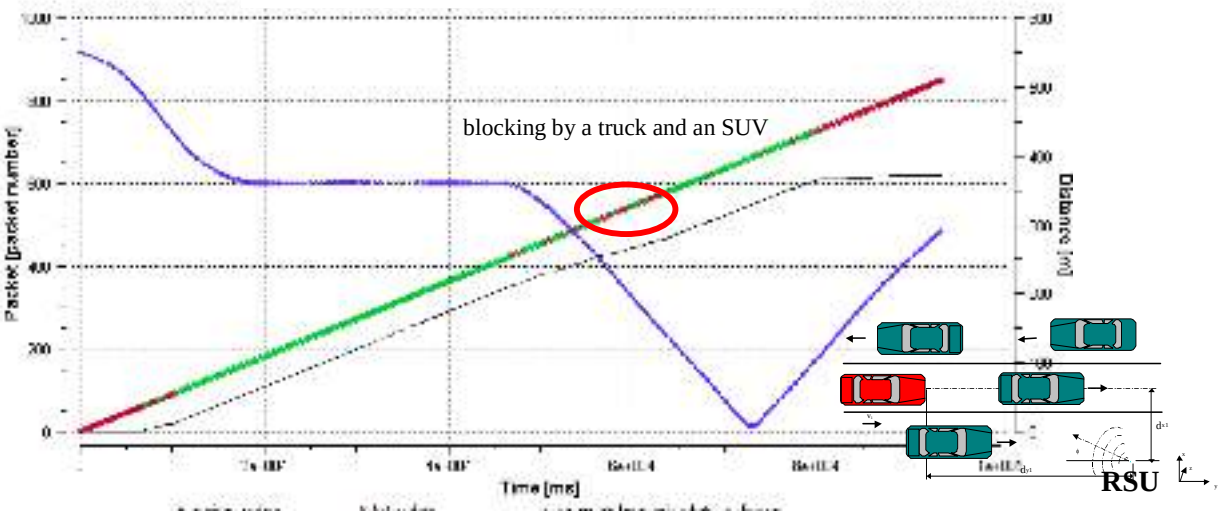


Figure 17. Test 1-10 Results

2.2 Dynamic Vehicle-Vehicle Communications

This section discusses the results with two dynamic antennas representing vehicle-to-vehicle communications. In the diagram shown below, there were no lost packets with two vehicles traveling in the same direction with a distance between them of about 150 m (Test 2-2). The test was conducted on a test track at speeds up to 60 mph.

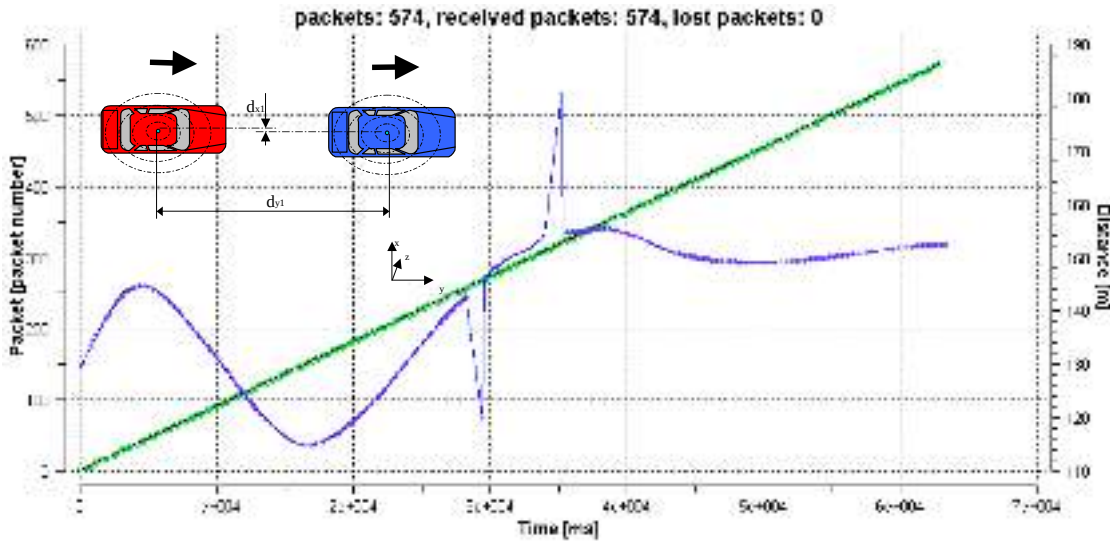


Figure 18. Test 2-2 Results

In a similar test track trial, there were also no packets lost when an SUV temporarily cut in between the vehicles (Test 2-3).

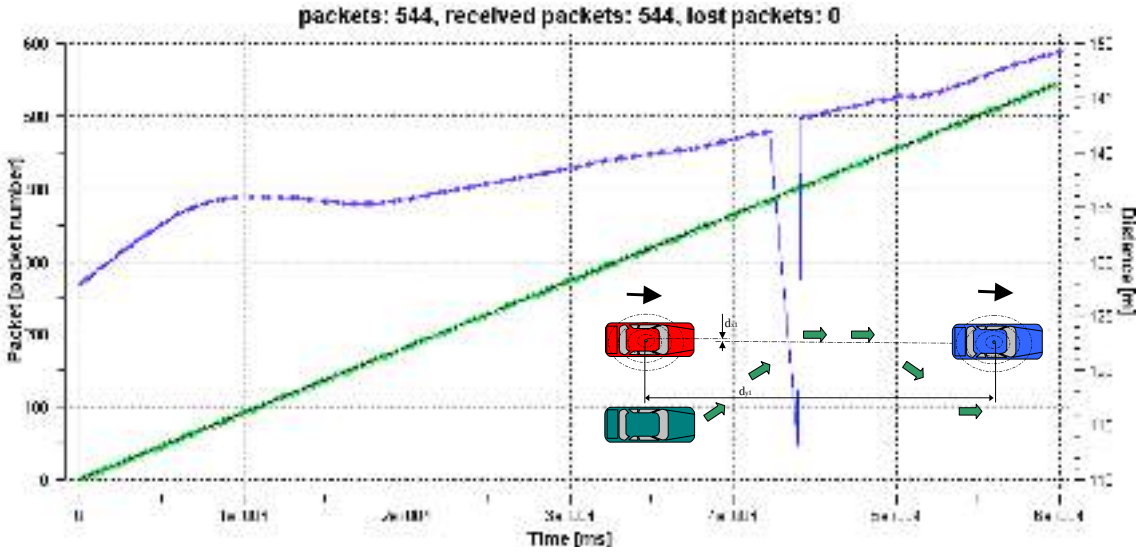


Figure 19. Test 2-3 Results

The test below approximates the driving characteristics of an application like Emergency

Electronic Brake Lights (Test 2-28). The sender vehicle and an obstructing SUV brake to a stop while the receiving vehicle passes them at 50 mph. In this particular trial about 5 percent of the packets were lost, and this packet loss appeared to be due to the obstructing SUV. The test results were repeatable over several trials.

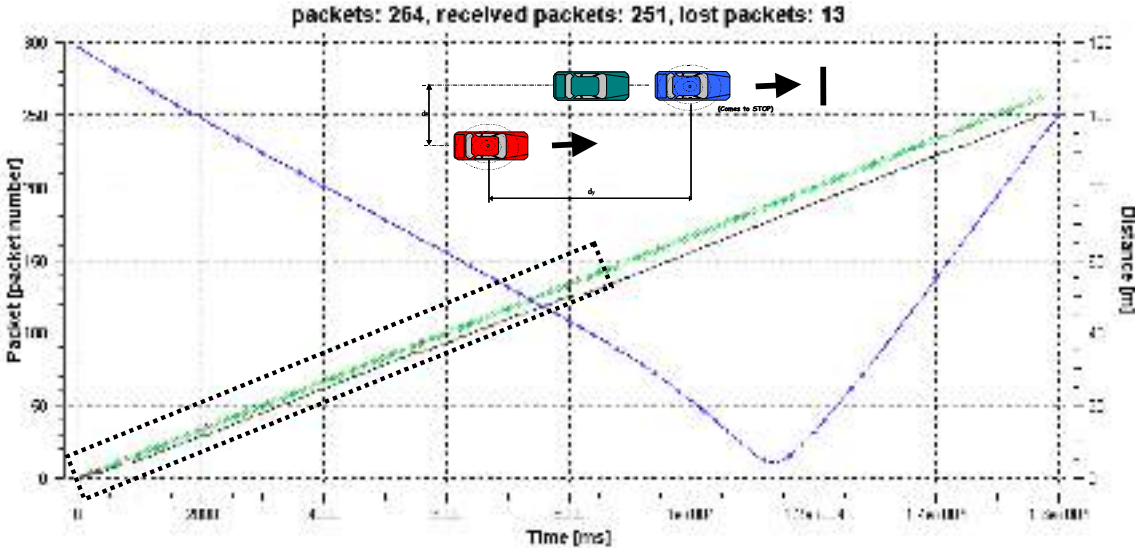


Figure 20. Test 2-28 Results

In this next test the obstructing vehicle was removed. The results improved significantly with only a few lost packets occurring at a range of about 90 meters (Test 2-24).

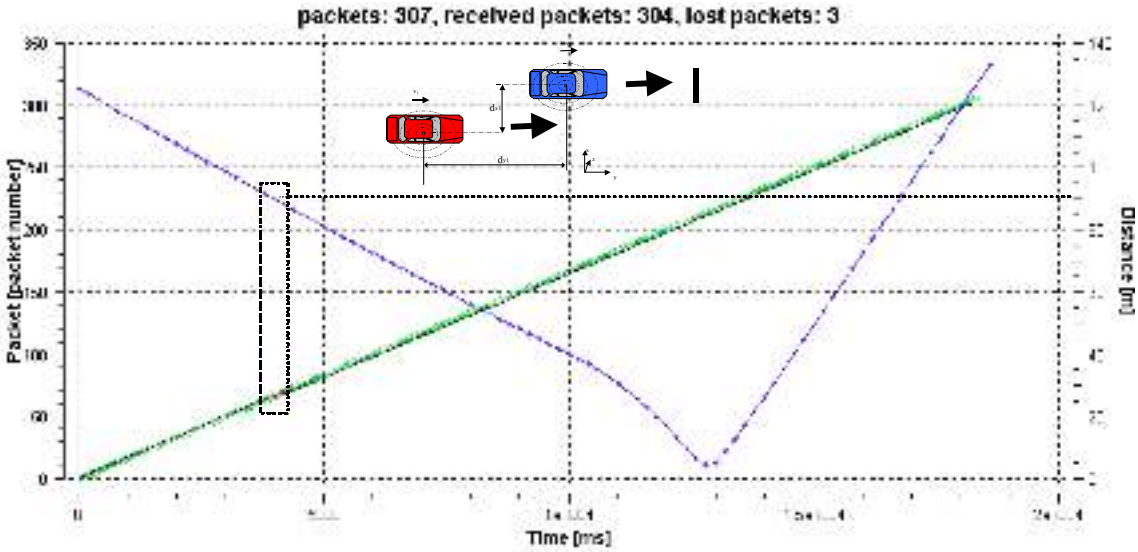


Figure 21. Test 2-24 Results

The next test approximates the driving characteristics of an application like Pre-Crash Sensing by having the sending and receiving vehicles pass by each other at 50 mph, simulating a head-on collision (Test 2-27). The test also was meant to stress the system with a high delta-velocity and a 50 msec update rate. Even at distances up to 400 m, there was no packet loss.

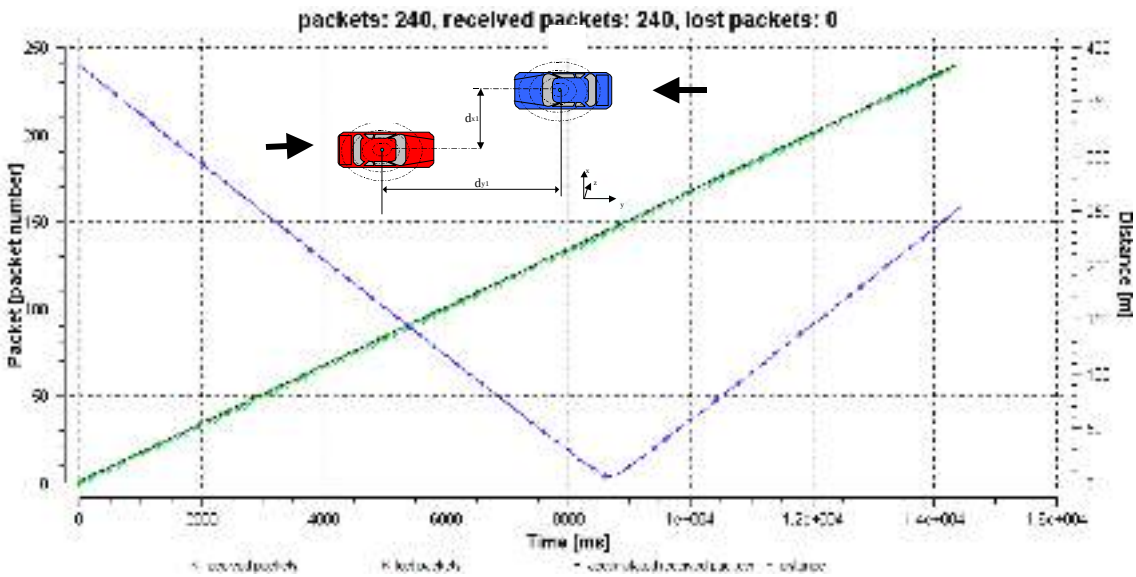


Figure 22. Test 2-27 Results

Interestingly, there was packet loss during a less stressful test with the vehicles traveling at 30 mph (Test 2-25). Once again the packet loss occurred when the vehicles were at a distance of about 90 m.

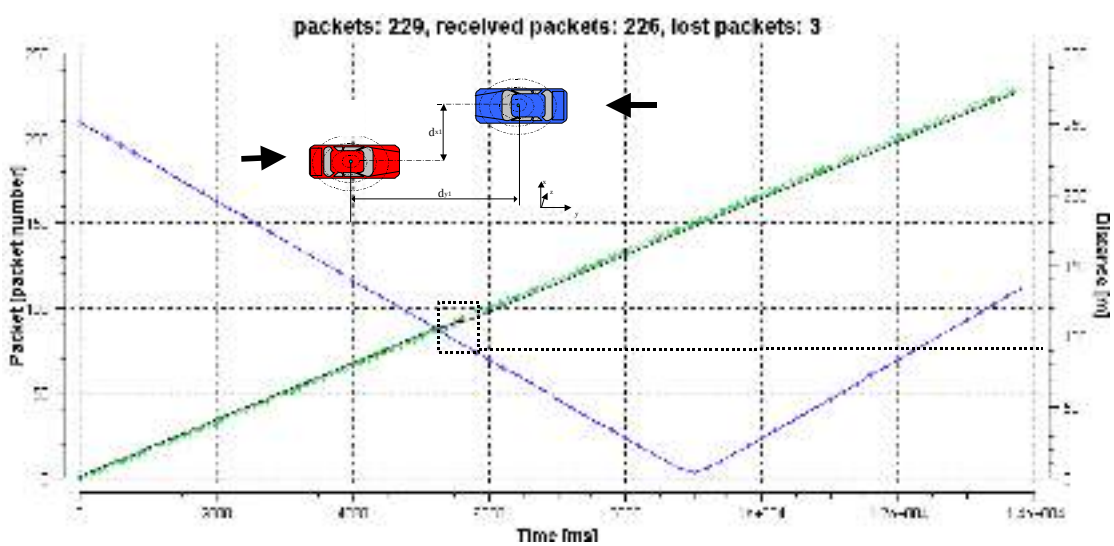


Figure 23. Test 2-25 Results

In the public road testing, basic communication at separation distances of around 100 meters experienced less than 3 percent packet loss (Test 2-6). The vehicles were traveling on a highway at 60 mph in light vehicle traffic conditions. The packet loss in this case is most likely due to a truck moving in between the two cars and blocking the line-of-sight.

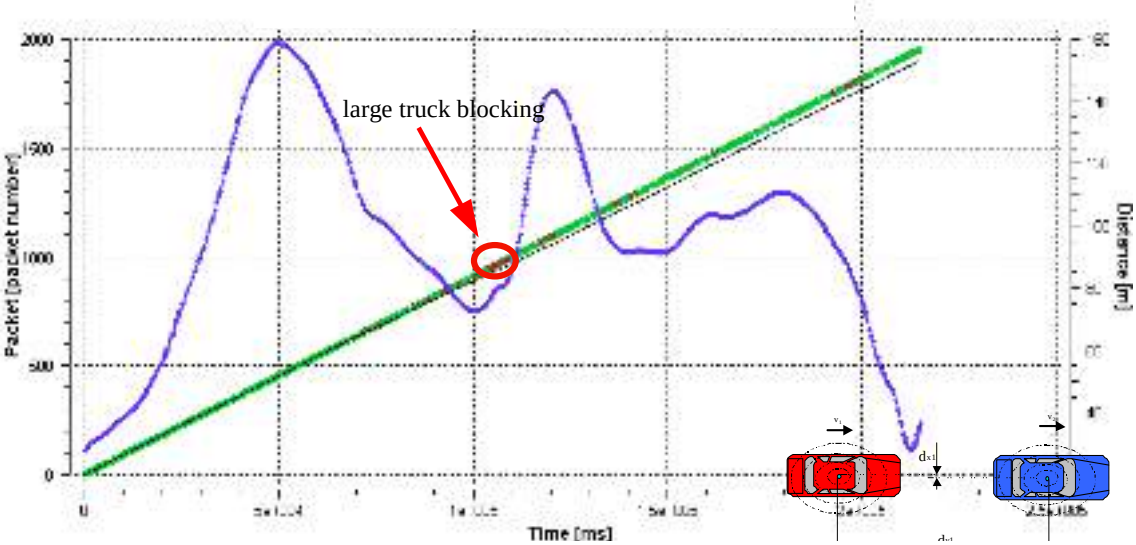


Figure 24. Test 2-6 Results

Similar results were found when the vehicles had a two-highway lane offset while traveling at 60 mph (Test 2-14). There was noticeable packet loss due to line-of-sight blockage between the test vehicles while driving on opposite sides of a hillcrest.

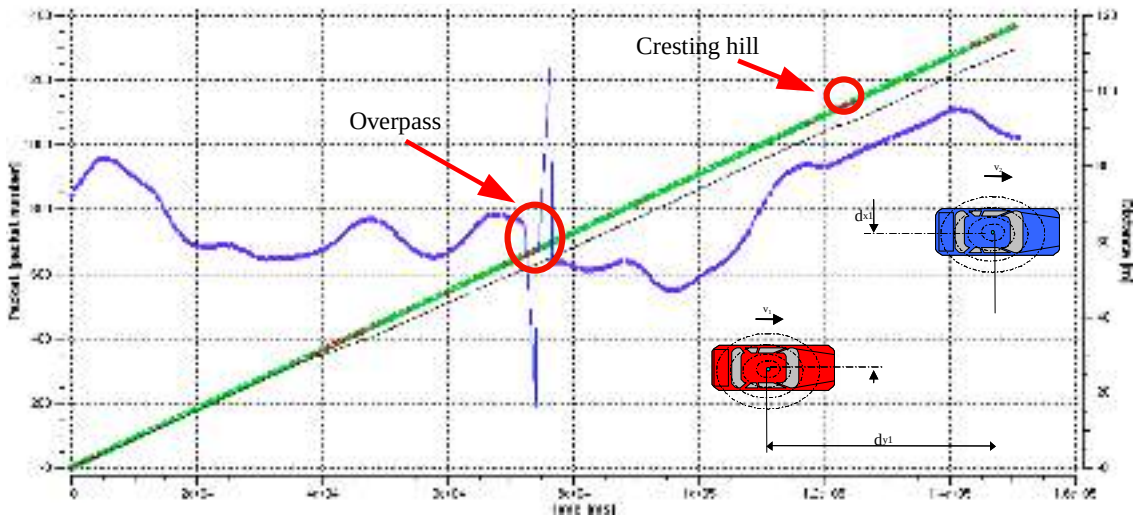


Figure 25. Test 2-14 Results

Momentary packet losses were also experienced with blocking sedans between the sending and receiving vehicles while traveling at 40 mph in light traffic conditions, as shown below (Test 2-25). The GPS outages were due to many thick overhanging trees.

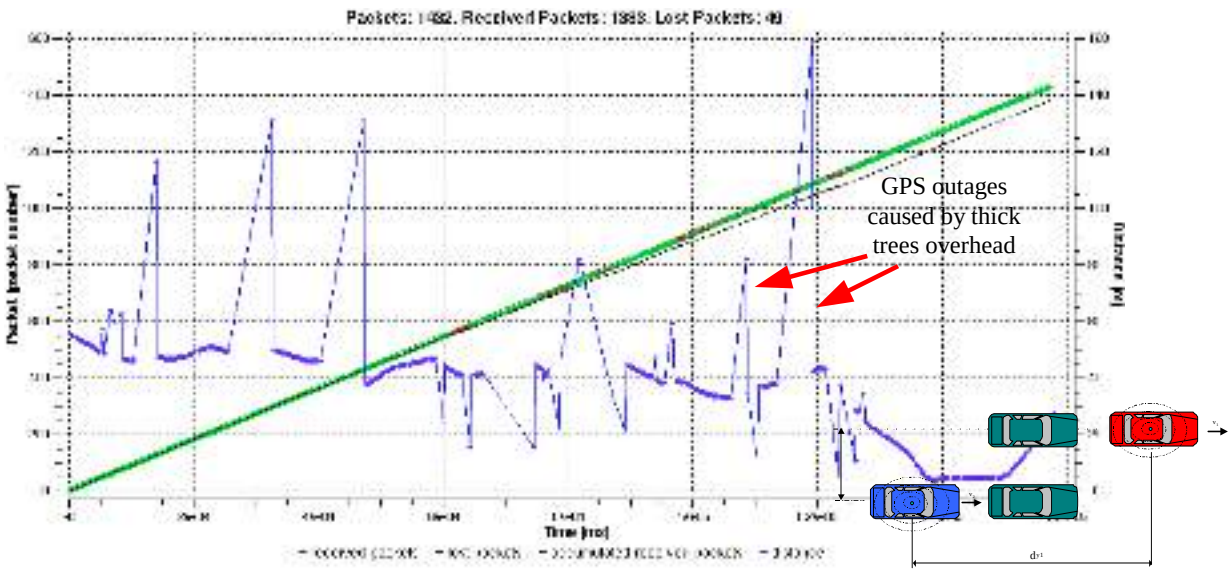


Figure 26. Test 2-25 Results

Two blocking SUVs between the sending and receiving vehicles caused more significant packet losses as shown in the trial below (Test 2-11). The vehicle formation was traveling at 60 mph in light traffic conditions. Packet transfer seemed more successful at longer distances, possibly due to reduced field of view blockage compared to that of a tightly packed formation.

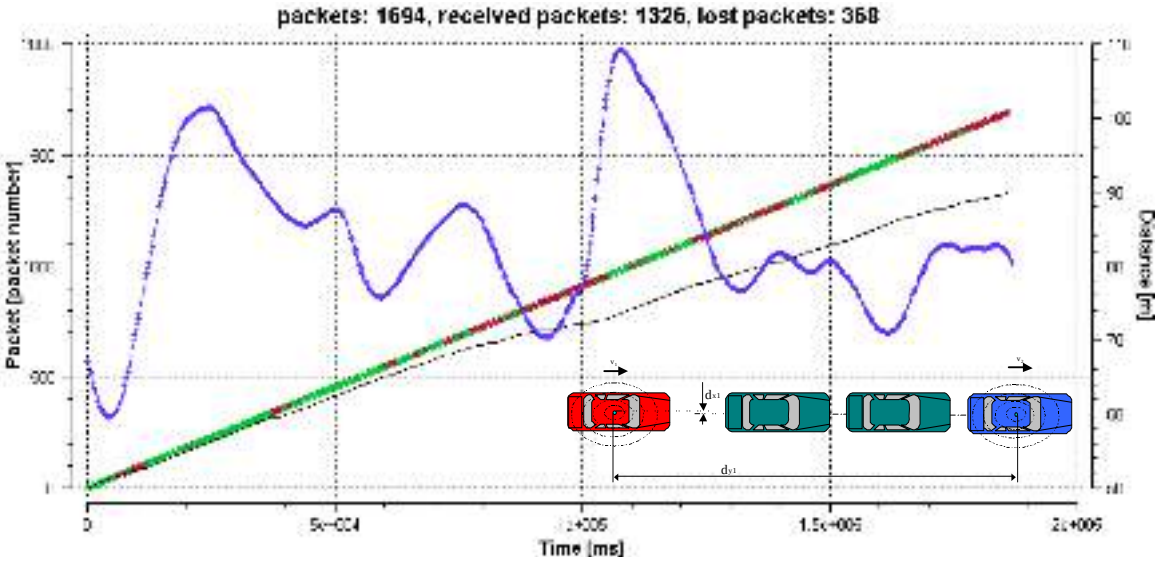


Figure 27. Test 2-11 Results

2.3 Stationary Vehicle Communications

The static tests considered communication range and the effect of other vehicles obstructing the line-of-sight between the antennas. The test below shows that no packets were lost at a distance of 200m with the vehicles in direct line-of-sight (Test 3-4). The message size was 200 bytes with a 100 msec update rate.

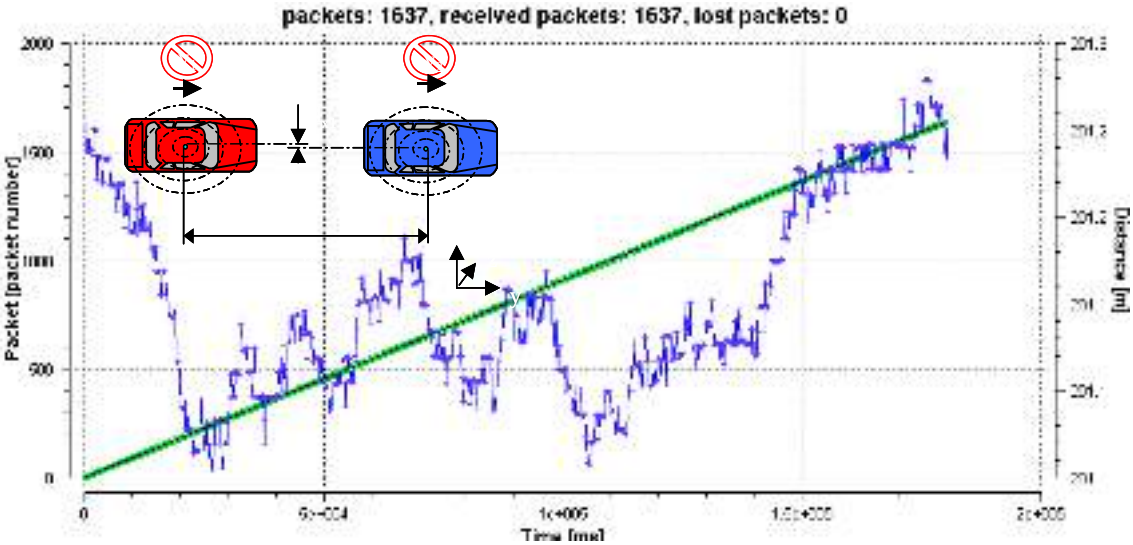


Figure 28. Test 3-4 Results

Another test considered a large, box-type truck parked laterally between the test vehicles (Test 3-14). There were no lost packets with this arrangement.

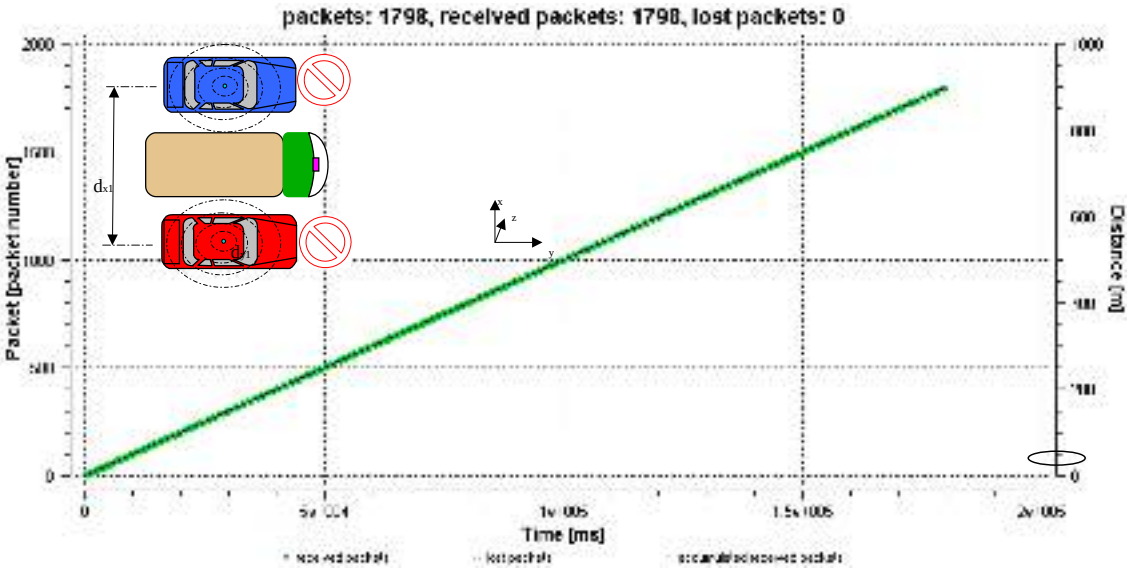


Figure 29. Test 3-14 Results

A similar test where the vehicles were parked longitudinally at a distance of 39 meters with the truck between them found some packet losses, though 93 percent of the packets were still received (Test 3-12).

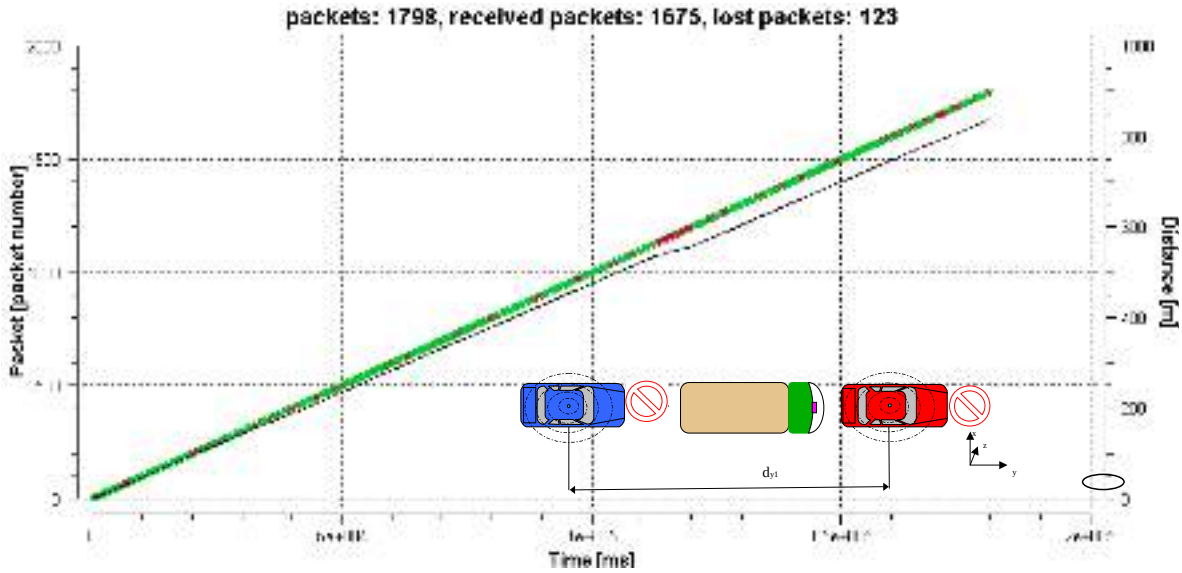


Figure 30. Test 3-12 Results

Transmissions were excellent between two stationary vehicles in a public parking lot (Test 3-3). No packets were lost at a distance of 148 meters.

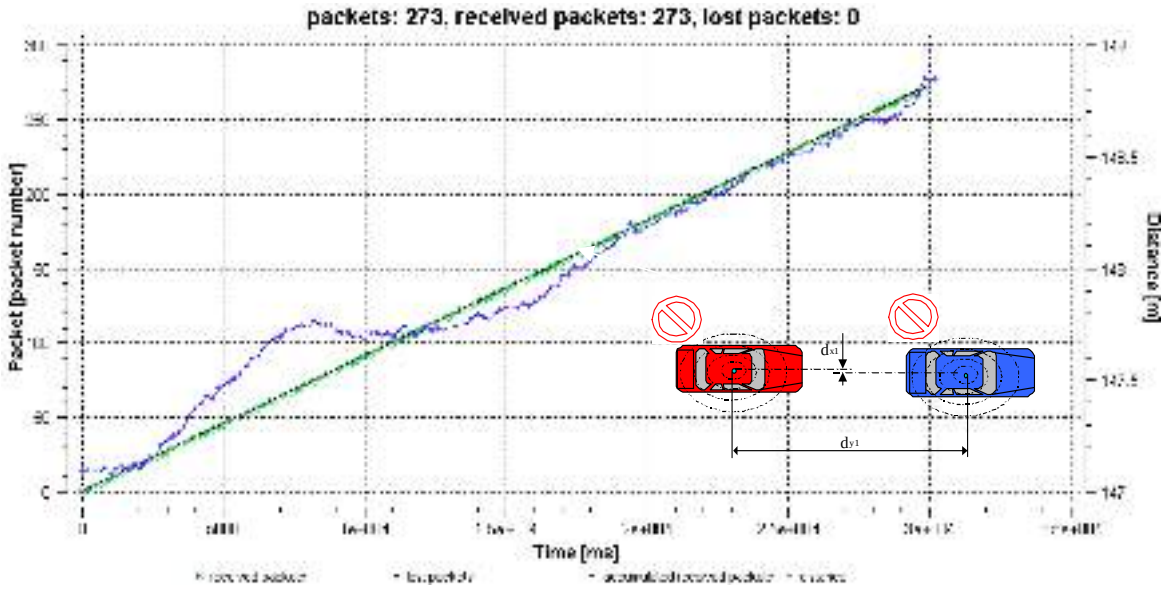


Figure 31. Test 3-3 Results

Another test conducted in a parking lot had the sending and receiving vehicles separated by an SUV parked between them (Test 3-9). No packets were lost during the test. The distance between the test vehicles based on GPS data fluctuated from ~9 ~10 meters.

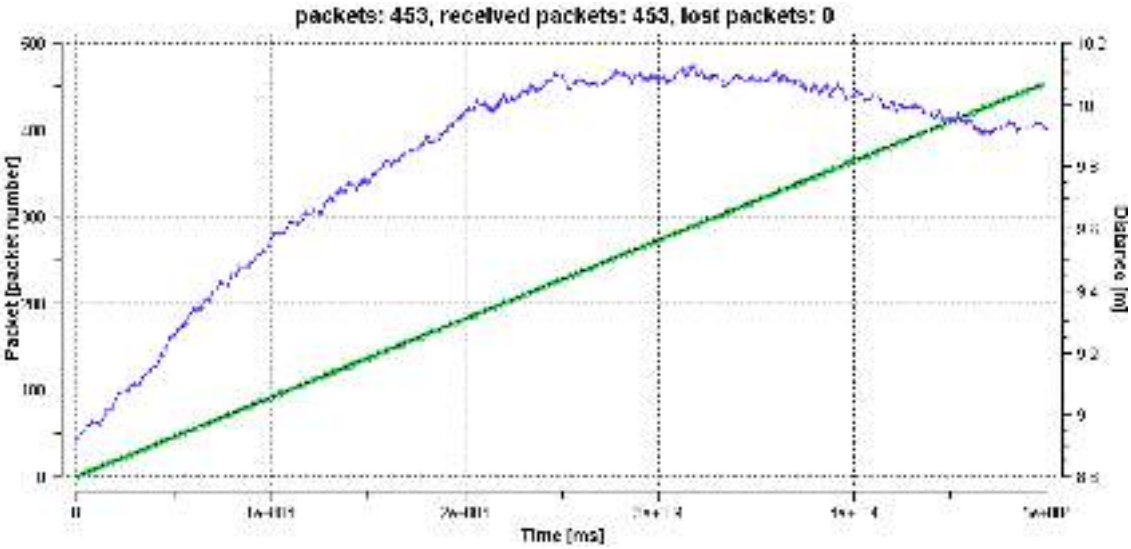


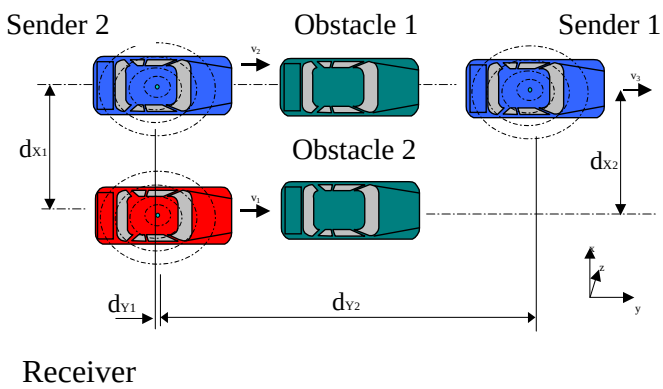
Figure 32. Test 3-9 Results

Figure 33. Test 3-9 Vehicle Configuration

2.4 Multiple-Sender Communications

Tests that included both three and four CTKs were conducted to evaluate multi-sender capabilities in various driving configurations. In order to differentiate the data that was received from more than one sender unit, the respective data plots for different senders are often shifted to a lower location on the diagram, with negative values on the Y-axis indicating the amount of the offsets.

The test below was conducted at arterial speeds close to 25 mph (Test 4-4). A tight formation was maintained with distances of less than 20 m between Sender 1 and the Receiver. Two obstructing vehicles were sustained throughout the test (Obstacle 1 was an SUV, and the other vehicles in the test were sedans). Overall, over 99 percent of the packets sent during all three trials of the test were received. The obstructing vehicles did not cause any significant loss of reception from Sender 1. The Sender 2 values are shifted on the diagram from those of Sender 1 with packet and range offsets of 200 packets and 50 meters.



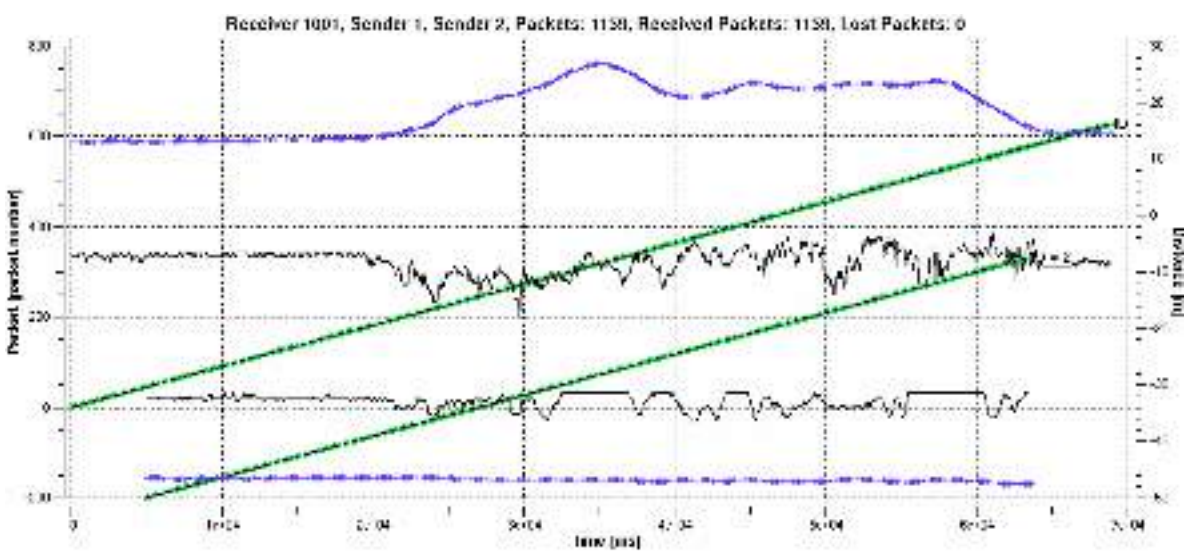


Figure 34. Test 4-4 Results

The same test was performed with the SUV driving directly in front of the receiver sedan (Test 4-6). Similar results were found and no more than one packet was lost out of the thousand packets that were sent during each of the three trials.

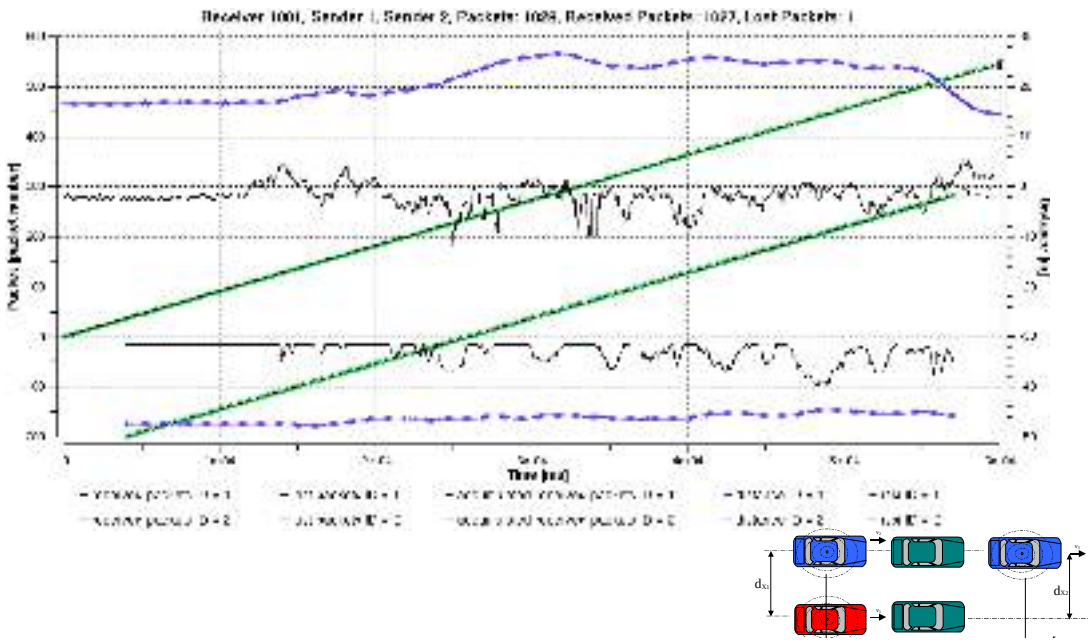


Figure 35. Test 4-6 Results

Another test on an arterial road in light traffic conditions specified the sending vehicles moving slightly faster than the receiving vehicle (Test 4-1). The band of lost packets shown on the diagram below was due to a number of vehicles that came in between the receiver and lead sender vehicle. The offsets used for the graph are 20 packets, 200 meters, and 200 RSSI.

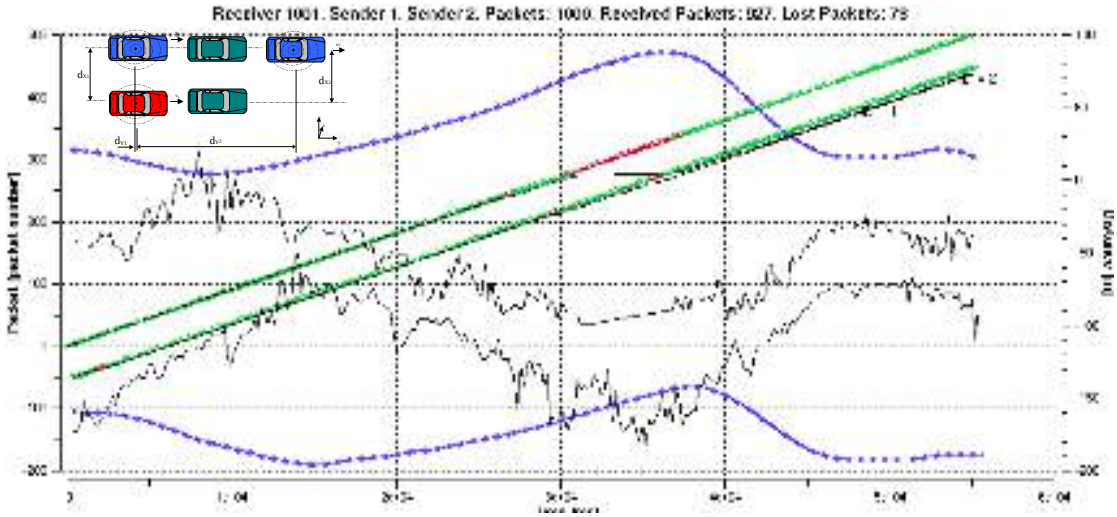


Figure 36. Test 4-1 Results

In testing conducted at highway speeds with the senders slowly passing a receiver (one-lane separation), non-test vehicles occasionally entered the test pattern and blocked some packets, as shown in the diagram below (Test 4-2).

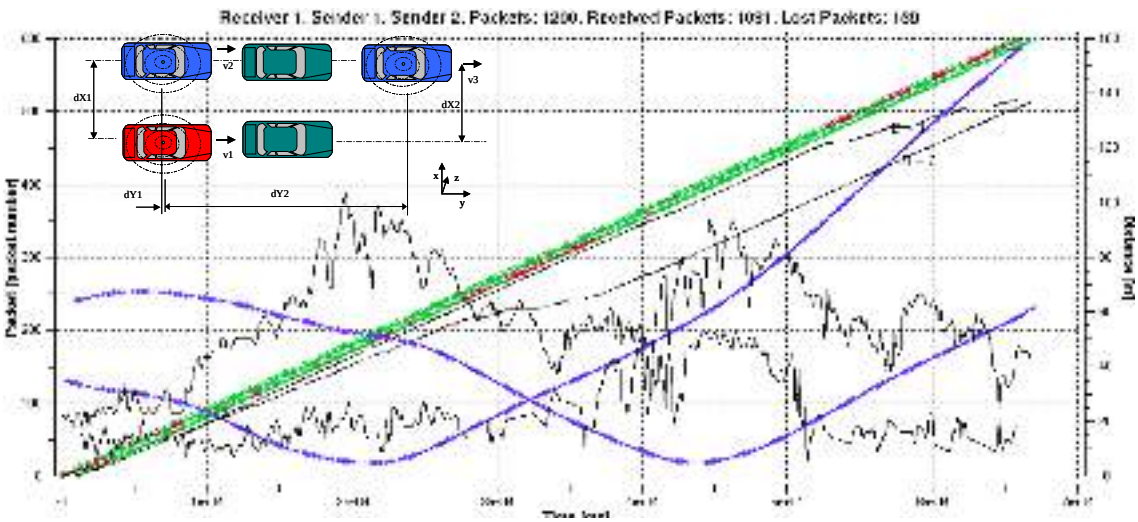


Figure 37. Test 4-2 Results

In a similar test with a two-lane separation between the senders and the receiver there was substantial packet loss due to a large truck passing between test vehicles and blocking the senders' line-of-sight to receiver (Test 4-9). There was also occasional line-of-sight blockage by obstructing SUVs.

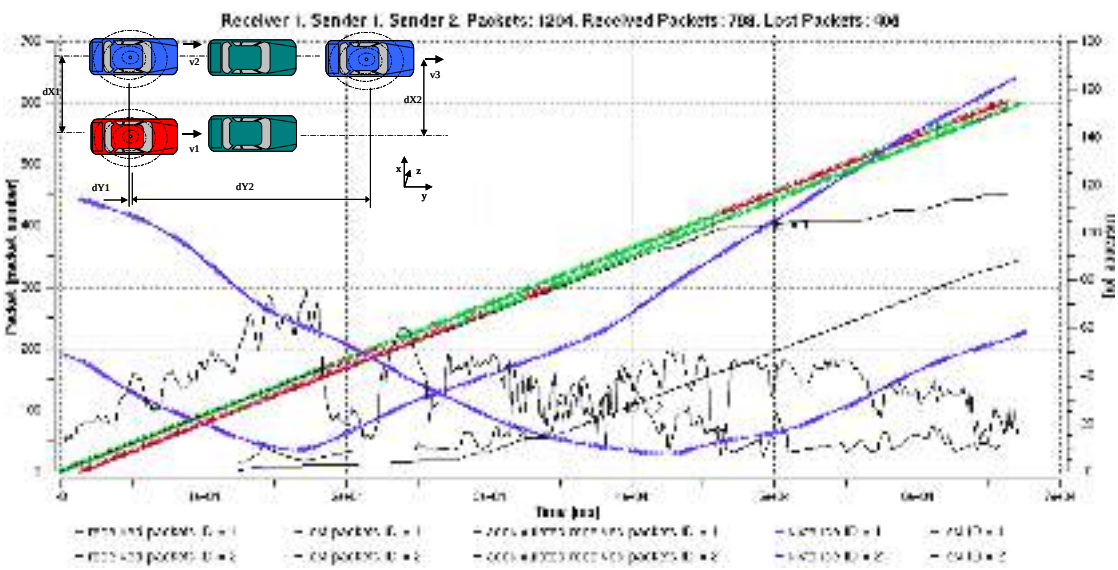


Figure 38. Test 4-9 Results

In a highway test that showed the effect of distance upon packet reception, there was approximately 100 meters of separation between the front sender (Sender 1) and the Receiver, while Sender 2 and the Receiver remained side-by-side (Test 4-7). Almost all packets from Sender 2 were received, but many packets from Sender 1 were lost.

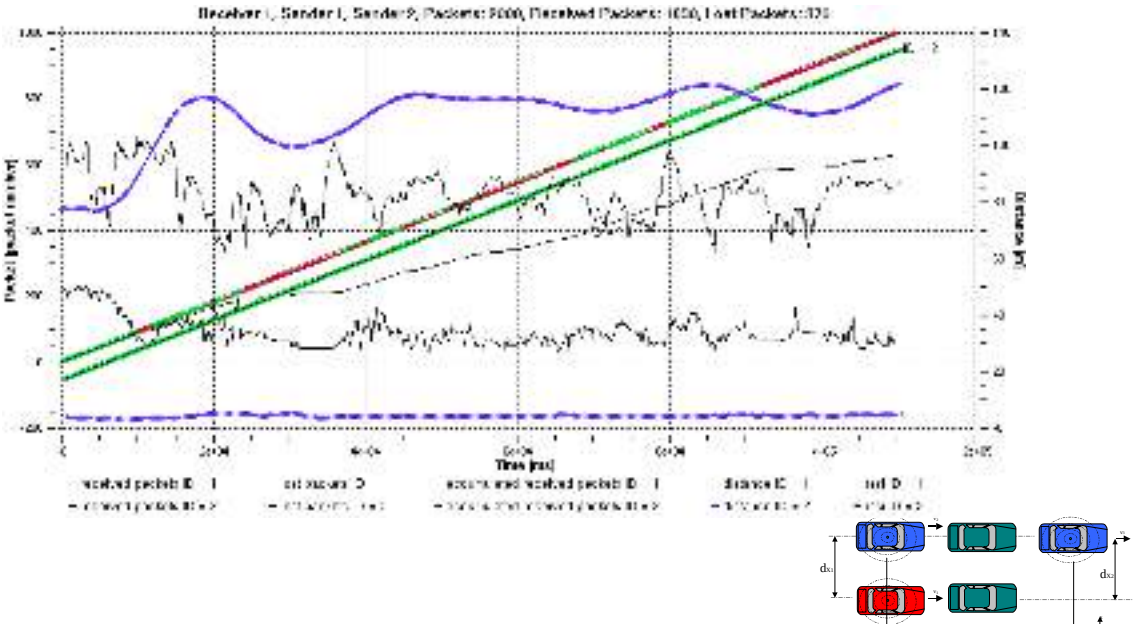


Figure 39. Test 4-7 Results

A longer duration test conducted at highway speeds found that 96 percent of the packets sent during the test were received (Tests 4-3 and 4-5). The majority of the lost of packets (circle 1) were caused by an obstacle 18-wheeler in close proximity (under 25 m).

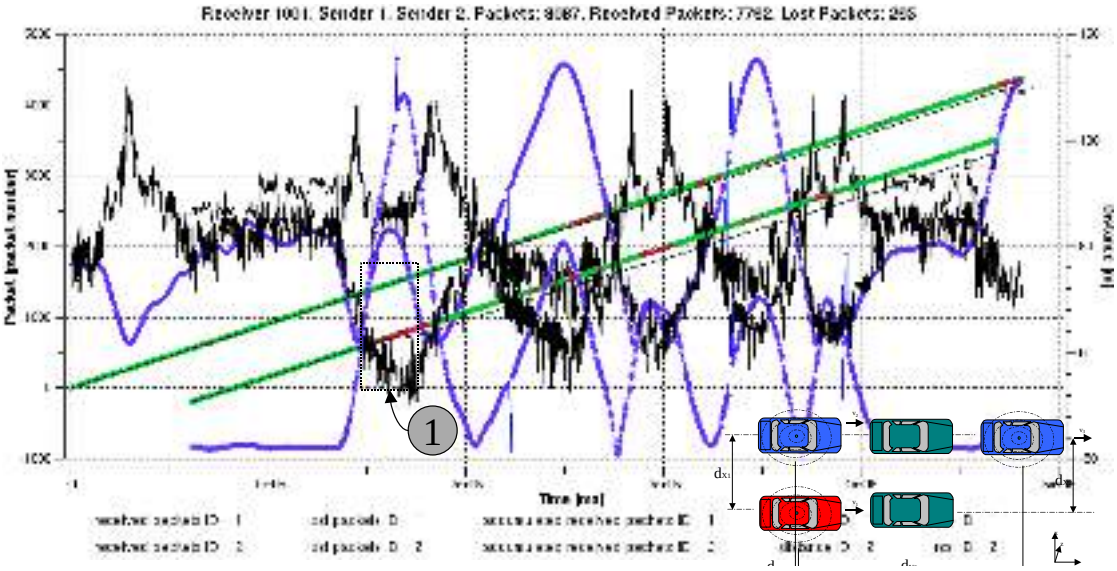
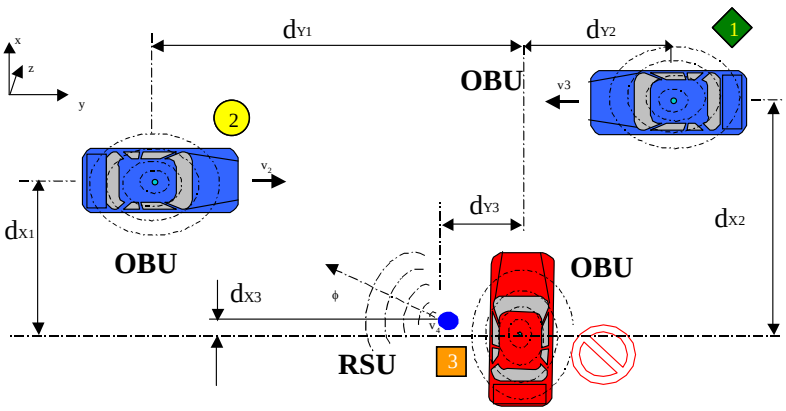


Figure 40. Test 4-3 and 4.5 Results

Tests were also conducted to simulate an intersection environment with both on-board units and a roadside unit simultaneously transmitting data. In the test shown below, the sender OBUs (triangle 1 and circle 2) were traveling at 25 mph while the receiving vehicle was parked next to another sender vehicle (square 3) that represented the RSU (Test 4-11). The distance between the stationary sender and the receiver was about 10 m, and moving senders were one lane apart.

Overall, over 99 percent of the packets sent during all three trials of the test were received. The test shows that having 3 senders in an intersection type scenario has no effect on packet loss of reception. The Sender 2 values are offset from the Sender 1 values by 200 packets, 50 meters, and 500 RSSI. The Sender 3 values are offset from the Sender 2 values by 200 packets, 50 meters, and 500 RSSI.



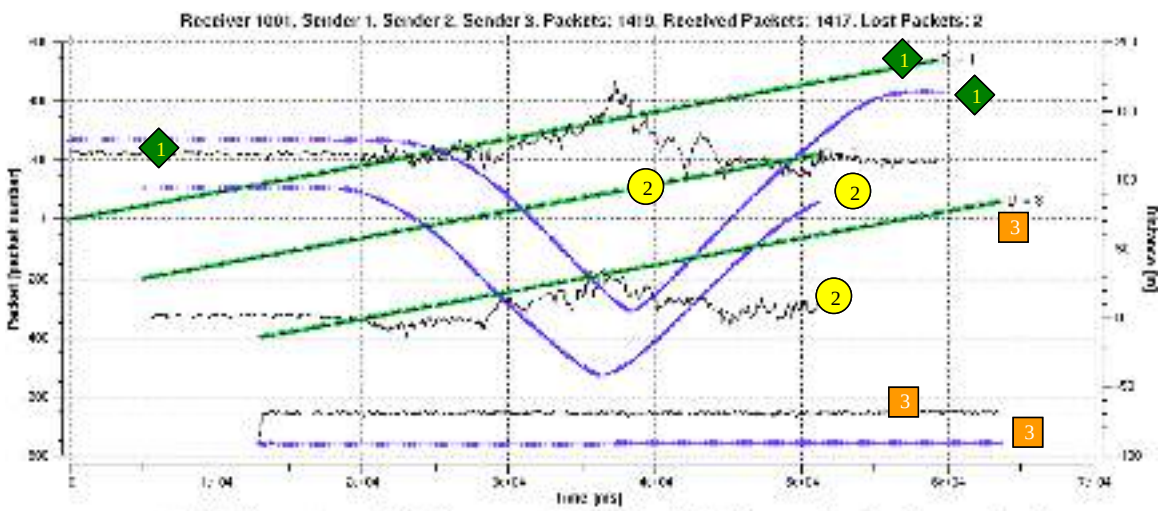
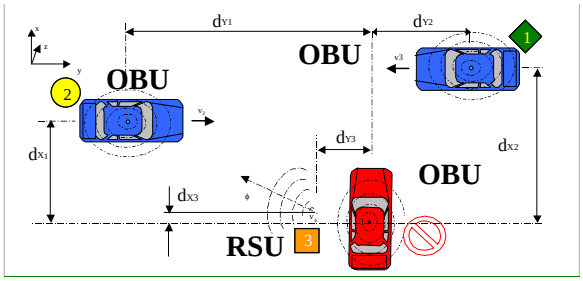


Figure 41. Test 4-11 Results

The same test was conducted with Senders 1 and 2 traveling at speeds close to 50 mph (Test 4-12). The distance between (stationary) Sender 3 and the Receiver was ~10 m, and Senders 1 and 2 were initially stationary for a significant period of time while waiting for unexpected traffic to clear from the test zone. Also, Sender 2 began well beyond the line-of-sight of the Receiver. Aside from this, very few packets were lost during the actual drive by. It should be further noted that there was significant roadside clutter in the form of trees and parked cars, which may have partially contributed to the few lost packets. Note that the data curves are offset for clarity, with a shift of 200 packets, 50 meters, and 500 RSSI units between each.



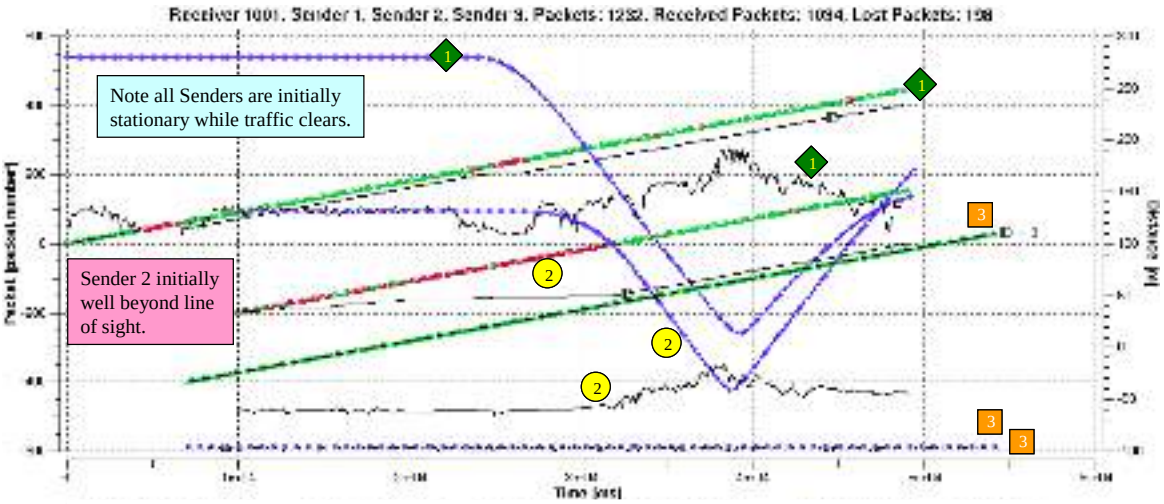


Figure 42. Test 4-12 Results

2.5 Multipath Considerations

During analysis of the test scenario results incorporating a moving vehicle or vehicles, a zone of minor packet loss was identified at around 90 meters separation. This anomaly was further investigated by placing two vehicles approximately 90 meters apart, then slowly moving one vehicle forward and backward while monitoring the packet reception indication on the CTK screen. Using this "Slow Rolling Test" (see figure below), a specific point could generally be found where nearly all packets would be lost, but moving forward or backward as little as one meter would re-establish reliable communications. This result was repeatable on subsequent trials.

The Two-Ray Model was used to predict multipath interference at the frequencies and antenna heights being used in the field-testing. In general, this model predicted a large degree of interference in the approximate range of 90 meters. Based upon this prediction and the results of the field-testing, the high packet loss zone is presumed to be due to multipath interference between the direct line-of-sight transmission and a reflection of the transmission from the roadway surface. Further testing will be necessary to determine if the antenna mounting location on the vehicle can be optimized to minimize this presumed multipath interference.

This multipath packet loss has been a very small percentage of packets in test scenarios between moving vehicles, or between moving vehicles and stationary roadside units. Even in slow speed test scenarios, only two or three packets were generally lost (out of hundreds of sent packets). Further testing is required to determine the potential impact on the operation of vehicle safety applications.

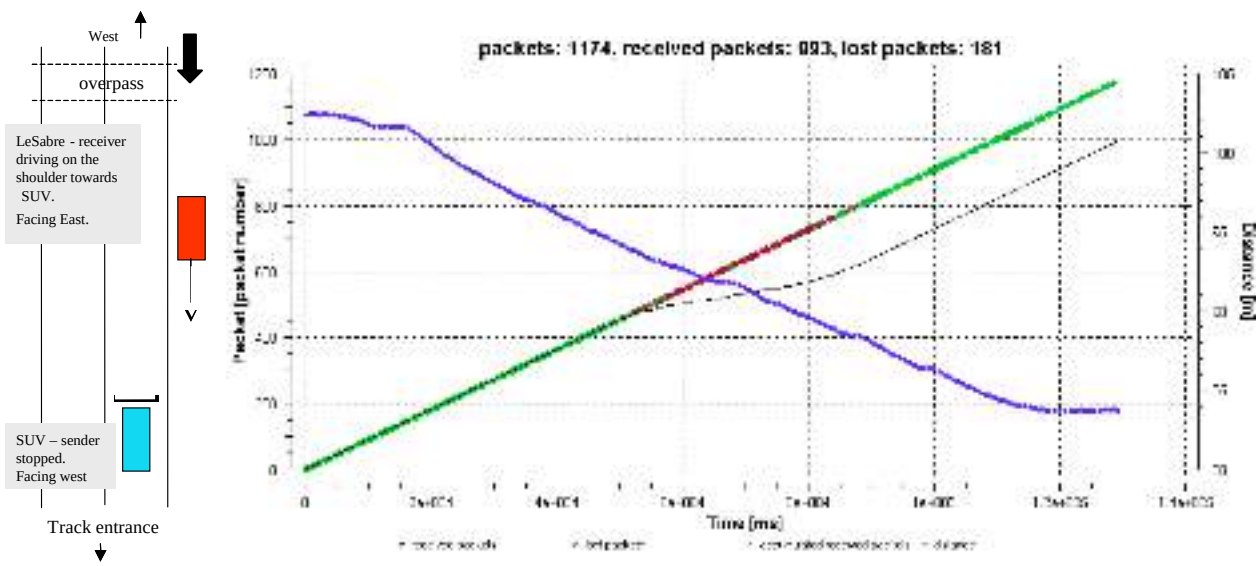


Figure 43. Slow Rolling Test in a Multipath Zone

3 Simulation Architecture and Test Results

Task 4 included simulation studies in vehicle communications. A DSRC simulator was therefore developed to perform the required simulation testing. The simulator architecture was designed to focus on research topics that are readily addressed through a simulation environment, but difficult, if not impossible, to replicate in a real world vehicle environment. Therefore, areas such as scalability and potential channel capacity constraints, multichannel operations, prioritization schemes, and dynamic power control were primary simulation topics.

3.1 Simulation Architecture

The VSC DSRC simulator was designed to be used for research in various subjects, including the following:

- **Scalability.** This is an obvious and major challenge in using DSRC for vehicle safety communications. When the DSRC penetration level becomes high, it is important to ensure that the system will still effectively support safety applications even in very dense traffic environments. A simulator is particularly useful for this work, since there are few, if any, alternative evaluation tools for the analysis of VSC protocol designs.
- **Multi-Channel Operation.** DSRC is an explicitly multichannel oriented design. RSUs advertise their services on the control channel, while potentially providing the content and/or interaction on service channels. On the other hand, safety messages are constantly transmitted on the control channel. So there is a conflict between safety applications' need to stay in the control channel for safety message monitoring, and private applications' need to provide value in service channels.
- **Safety Application Evaluation.** The design of the simulator is such that it could mimic the communication channel for safety application communications. This would incorporate various protocol mechanisms and constraints such as dynamic power control, multichannel operations, and other real-world variables.

3.1.1 Simulator Design

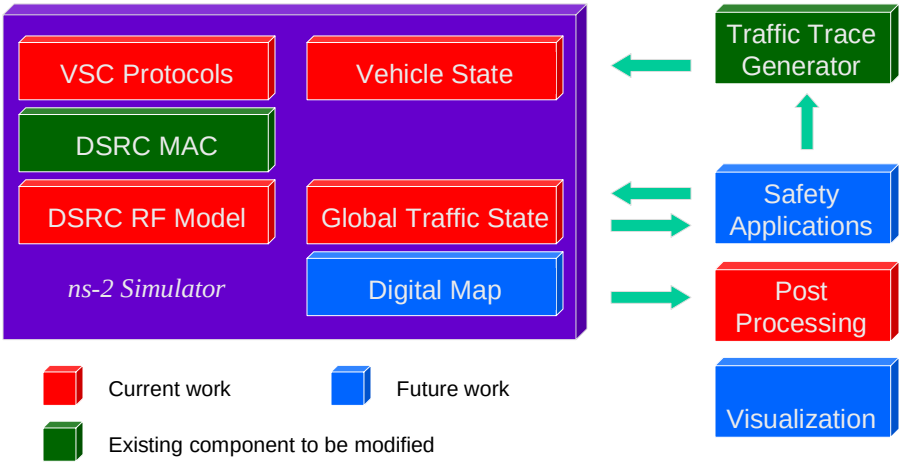


Figure 44. Simulator Components

As shown in the figure above depicting the simulator architecture, this DSRC simulator was built on top of the NS-2 simulation platform. NS-2 is a C++ based network communication simulator developed at the University of California at Berkeley. It was historically used in computer network research for many years and is widely distributed and respected among researchers. A support forum exists in the form of a mailing list, through which a huge archive of solutions and helpful comments are available. Additionally, NS-2 is "open source" software and is continuously updated. Its independence from a commercial source makes it a no-cost and flexible solution. NS-2 works well on various UNIX systems, including Linux. The Win32 platform is also supported.

NS-2 is a basic and non-graphical tool. The input to NS-2 is provided by an OTcl (Object Oriented Tcl) script, which contains all topology and node information. These scripts are, depending on the scale of the scenario, very complex and large input sources. The output NS-2 provides is very detailed. It can give per packet information at MAC, agent, or router levels.

3.1.1.1 Vehicle Traffic Trace as Input for Simulator

The simulator is designed to take external input for the vehicle traffic movement during the simulation. This traffic movement input could be a file, TCP/IP socket connection, or even an actual safety application implementation that generates vehicle movements dynamically.

In comparison, Carnegie Mellon University's Monarch Group added a mobility extension to NS-2, which allows mobile nodes to move within the boundaries of a predefined scenario. This extension, however, is not sufficiently flexible for a

vehicle safety communication simulation tool. Before starting the simulation, the movements of all nodes must be set up. It is not possible to interactively adjust the movement in the simulation as a result of communications among nodes.

The figure below shows a screen shot of the traffic trace configuration window. The design and implementation of the simulator allows for traffic traces in a very flexible format. For example, any delimited text file with necessary (but arbitrarily ordered and formatted) data fields could be used in this simulator.

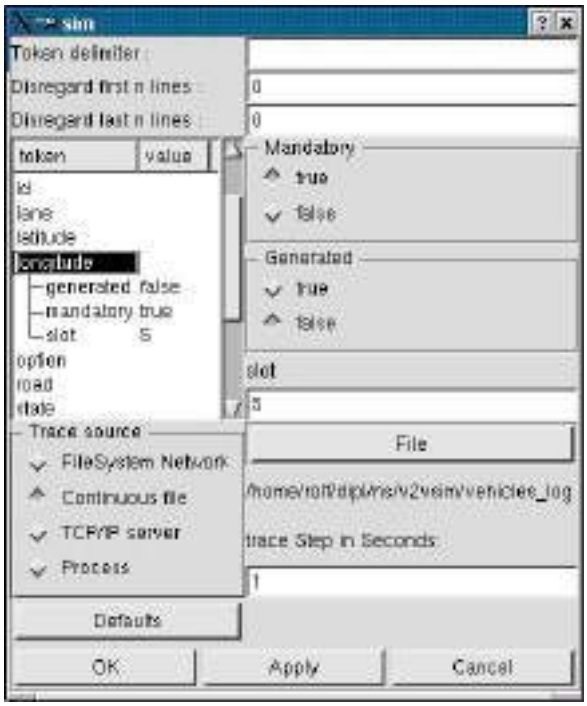


Figure 45. Traffic Trace Configuration Window

3.1.1.2 Simulation Configuration and Operation

The usage of the simulator is generally an iterative process, an example of which follows:

1. Design and implement components for protocols and agents at various layers in the NS-2 system.
2. Match up particular instances of components in each layer.
3. Configure and adjust parameter values in each component.
4. Run simulation and produce output traces.
5. Repeat from step 1 or 2.

A GUI (graphic user interface) was implemented to simplify configuration in steps 2 to 5. As shown in the screen capture below, one could pick any instance of a component in any layer and adjust the parameters arbitrarily. All such configurations can be saved in an XML formatted file. Batch operation of several simulation sessions is also supported.

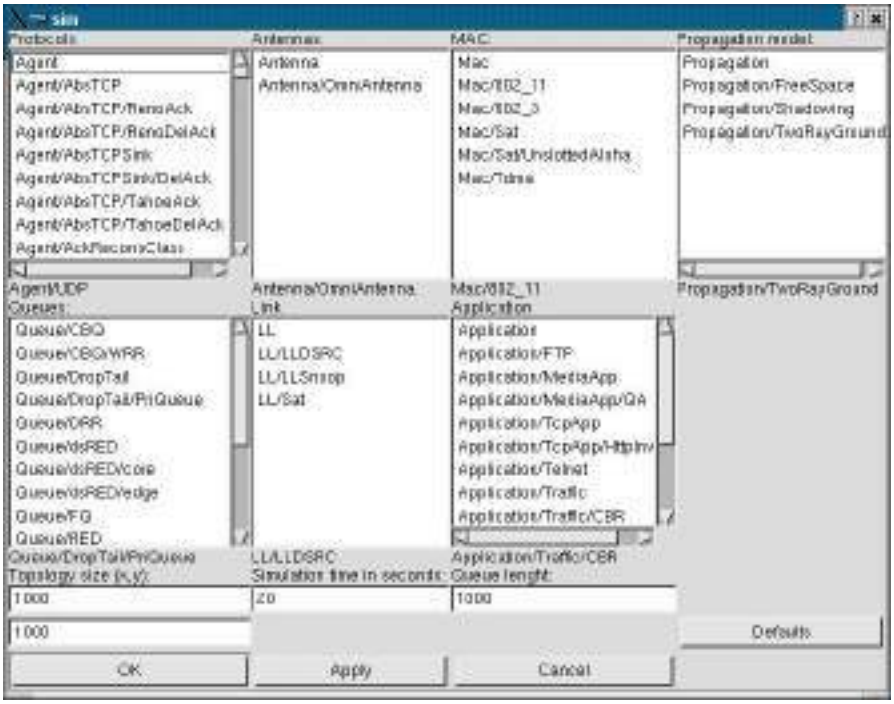


Figure 46. Graphical User Interface

3.1.2 Channel Capacity Evaluations

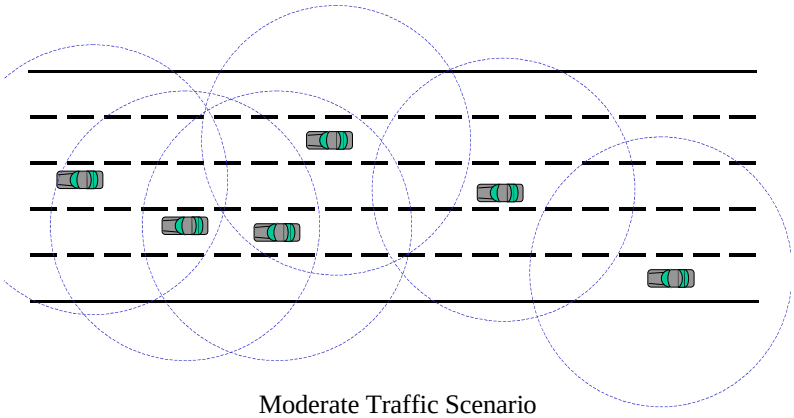
Simply put, channel capacity could be described as how often and how loud can vehicles transmit, at what packet size, in what traffic density, and environment while preserving certain tolerable levels of reliability and channel access delay. Given the complexities of interrelating so many parameters, it is important to use limited but representative values for the simulations. The following list describes the parameters in more detail.

- **Packet Size**. Most safety messages are expected to contain some minimum amount of information such as position, velocity, time stamp, etc. So a very simple message may have a packet size of 64 bytes at the low end of the scale. Beyond this, packets at 128, 256 and 512 bytes are examined. In particular, such simple variations of large packet sizes could provide some first order evaluation of the impact created by some form of security mechanism overhead.
- **Transmission Frequency.** It seems that 100 ms is a reasonable time interval since it is often mentioned in various safety application

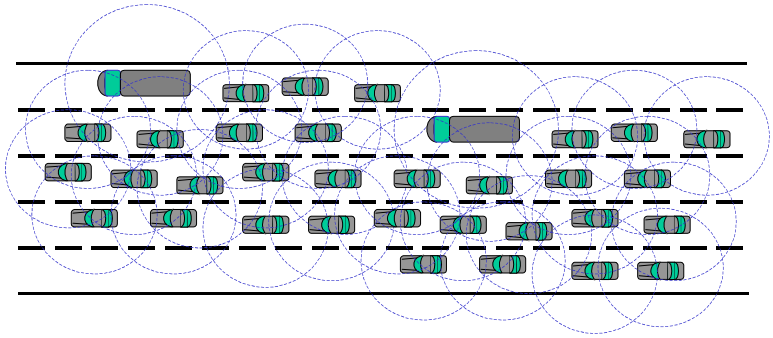
communication requirements. Values at 150 and 200 ms may also be of some relevance.

- **Transmission Power**. Transmission power determines both the reach of expected communication reception and the interference range at which others are prevented from transmitting. Since Task 4 simulations depend on detailed testing and modeling in Task 6A to provide an understanding of actual power level versus communication reach, transmission power variations are simplistically simulated to adjust the range of communication and interference.

There are innumerable ways to model traffic densities and environments. Since this is a high level study of channel capacity, the initial simulation focuses on simple scenarios with traffic densities that range from “moderate” to “heavy,” as shown in the following figures. The actual figures of traffic flow are based on typical statistics collected from representative major commuting highways for non-rush and rush hours. The actual traffic trace will be synthetically generated, since only the average flow and vehicle separation are important for the high level capacity evaluations.



Moderate Traffic Scenario



Heavy Traffic Scenario

Conceptually, an obvious evaluation metric in the simulation is channel occupancy. However, it is not exactly clear how such a figure should be computed. The roadway environment is large and by definition is not an enclosed system in which everyone can hear everyone. If two cars far apart can talk at the same time, should this be counted twice? If so, the channel occupancy could easily exceed 100 percent, given a large enough area of simulation.

For this reason, the simulator uses other evaluation parameters. In particular, it tracks the average channel access delay and packet loss rate.

3.1.3 Power Control Evaluations

Simulation results in channel capacity evaluations are likely to show that naïve usage of the channel will cause problems in congested situation. The next step will be the evaluation of proposed techniques to resolve the capacity concern in these situations. In general, power control is expected to be an important approach in any solution. However, there may be some hidden limitations in this approach.

The general concept for power control is the following:

- If there are many vehicles around, they will move slowly as in a traffic jam. In this case, scaling back each vehicle's transmission power would work well since in slowly moving traffic, there is no great need for safety messages to reach beyond one's immediate neighbors.
- If vehicles are moving fast, they should be reasonably far apart. Therefore, capacity is less of a concern, even if all of them need to transmit at higher power for the longer ranges.

Problems arise if these two scenarios are merged into one, as shown above. The slow moving vehicles on one side of the freeway could be working quite well with each other using low power, whereas the fast moving vehicles on the other side communicate effectively among themselves at high power. However, if both scenarios coexist as in the figure, then there is the danger that high-powered transmissions, even though low in number, could interfere with a disproportionate number of low powered transmissions.

3.2 Simulation Test Results

Initial simulation testing focused on a significant concern for the proper support of message prioritization. This is critical for the effectiveness of vehicle safety applications, and especially so when channel loading is high. Consequently, simulation testing was conducted to evaluate the DSRC priority mechanism in increasingly stressful communication contexts.

3.2.1 Simulation Test Setup

The basic configuration assumed for the purpose of the simulation test was ten concentric roadway lanes (see illustration below). The innermost lane was set with an inner radius of

150 meters. This circular configuration was chosen to allow full vehicle motion within the roadway lanes, without entering and leaving the simulation.

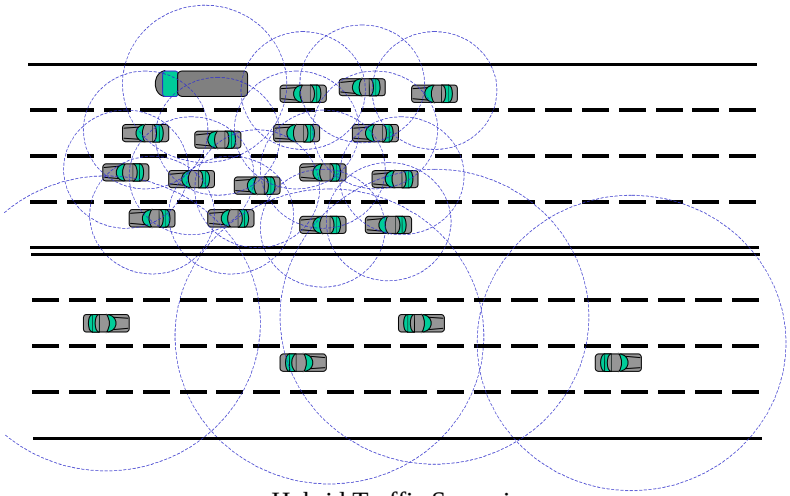
Simulation test runs were conducted with three different vehicle density assumptions. These vehicle density assumptions were: 20, 30, and 40 meters per car per lane.

The simulation test runs assumed the communication range at three different levels: 50, 100, and 200 meters. This provided a simplified surrogate for power control (see Section 1.1.3).

In the simulation test runs, the packet size was varied. The three packet sizes used were: 100, 200, and 500 Bytes.

The simulation test assumption of transmission frequency was consistent with the communications requirements expected for many of the identified vehicle safety applications: 1 message per car per 100 ms.

Illustration of Simulation Test Setup



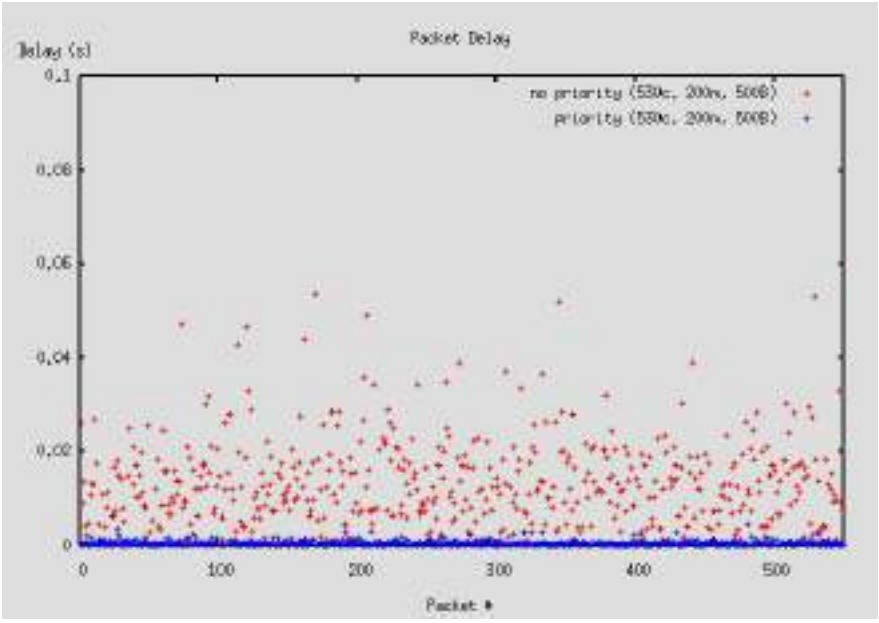
Hybrid Traffic Scenario

3.2.2 Priority Process

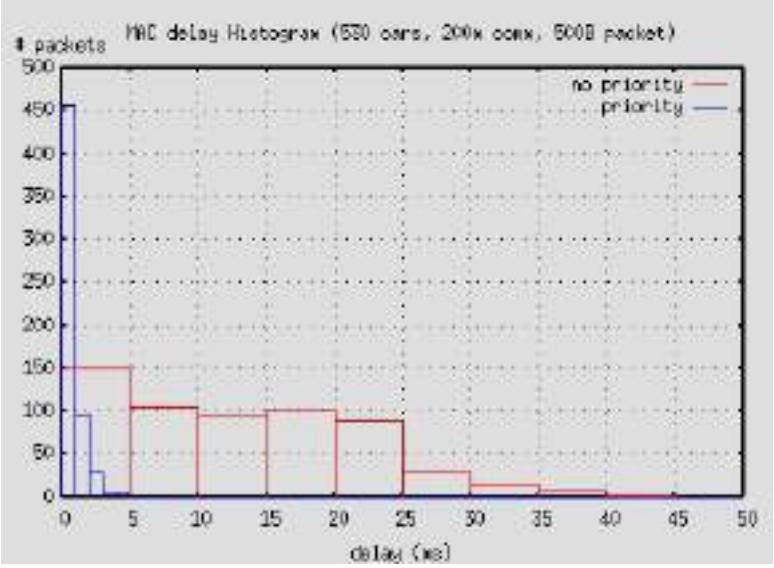
For the purpose of this simulation testing, the VSC used the Enhanced Distributed Coordination Function (EDCF) as the priority mechanism for DSRC. The EDCF was introduced as a part of the IEEE 802.11e Quality of Service standardization effort. EDCF is designed to prevent collisions between packets in the communications medium. The process can be described in the following, basic way:

- Listen: each transmitter listens for the channel to become idle
- Wait: based on priority, then wait a random, but again prioritized back-off time
- Talk: after the wait times expire and if no other transmissions are heard, the packet is sent

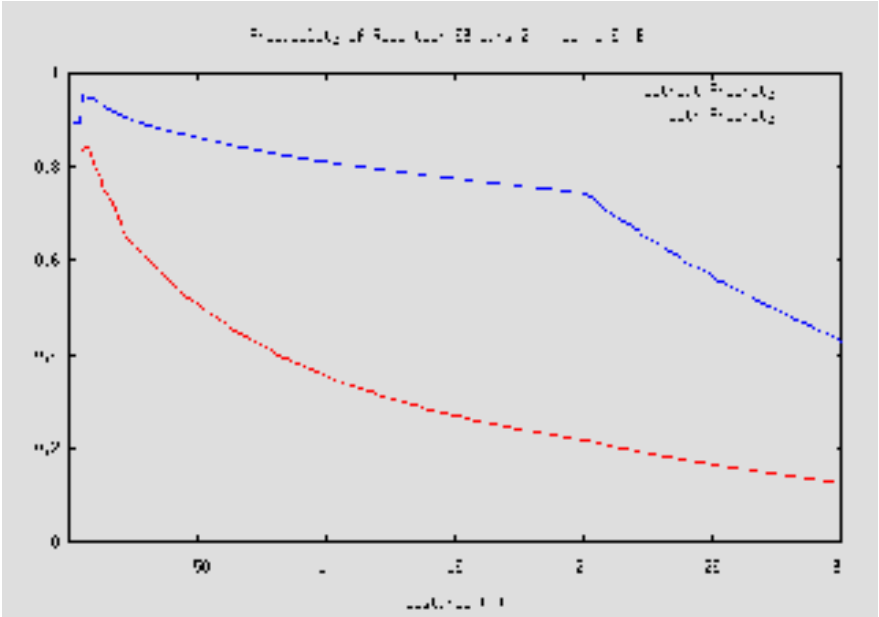
EDCF is designed to specify the random back-off time according to the message priority. This means that lower-priority messages should have a longer back-off time. By using this process, high-priority messages should have much better chances to get on the channel before messages with lower priority. The following results illustrate the potential benefits to safety applications from such a prioritization mechanism.



The EDCF priority mechanism is illustrated in the above simulation test result. In this case, there are 530 cars in the simulation with 20 m separation distance per car per lane. Transmission power is set for a distance of 200 m and packet size is 500 bytes. Out of the 530 cars, one car (blue data points) is given high priority while all others have no priority. The red data points show results for a representative car with no priority. Virtually all of the high-priority messages are sent with less than 5 ms delay. Conversely, non-priority messages encounter delays of up to approximately 50 ms.



In another perspective, the same data is shown below. It is very clear in this perspective that priority for this particular case significantly reduces message transmission delays. This result has apparent implications for high-priority vehicle safety applications.



The final graph above shows the same results, but now depicts broadcast effectiveness. It specifically shows the percentage of cars at various ranges that successfully receive the priority and non-priority messages. This simulation test result demonstrates significant potential impact to safety messaging success rates through the application of a single protocol mechanism, message prioritization.

Field Test Scenarios

4 Dynamic Vehicle-to-Vehicle Communications

4.1 Test Scenario

4.1.1 Test Scenario 1-1

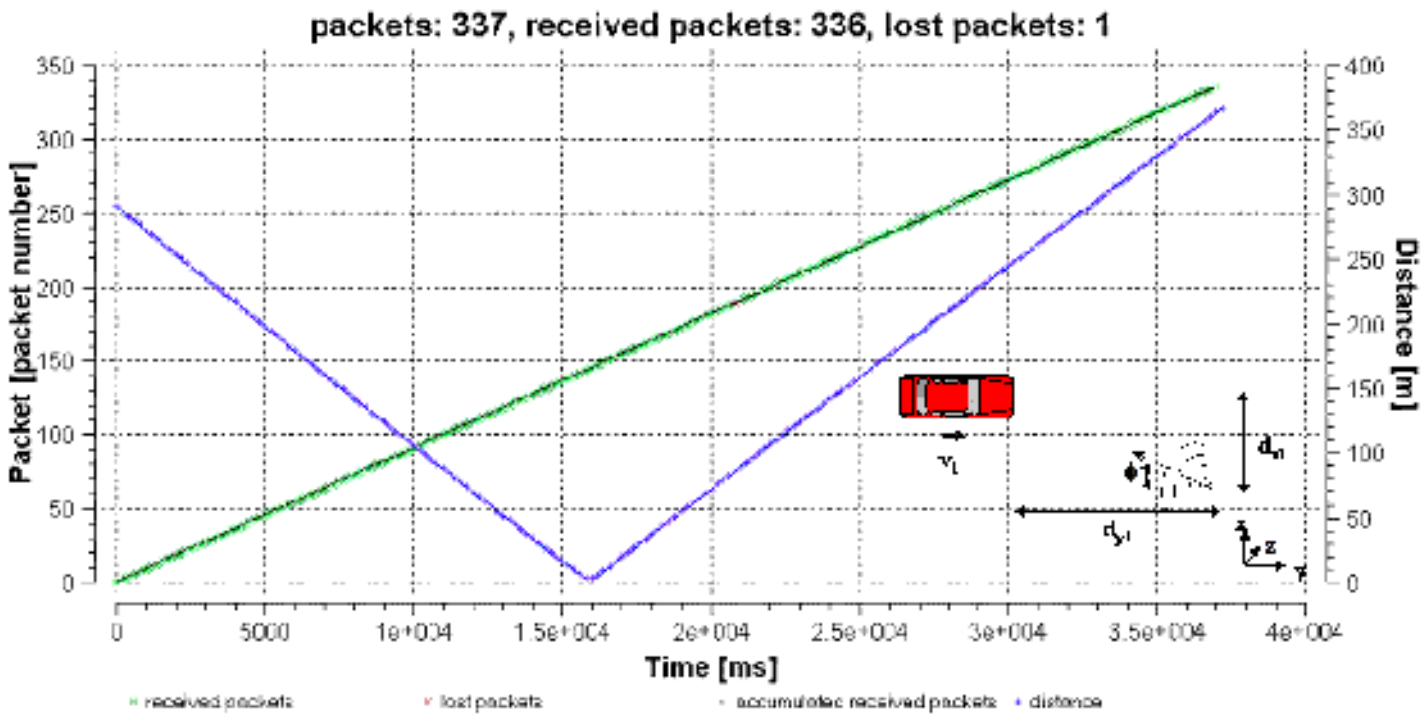
Test Scenario	**1-1**
Relevant Applications	Traffic Signal Violation Warning Curve Speed Warning / Rollover Warning Left-Turn Assistant
Velocity of Receiving Antenna (miles/hour)	40
Distance Between Antennas (meters)	< 300
Lateral Offset to Broadcast Antenna (meters)	4
Velocity of Sending Antenna (miles/hour)	0
Angle Between Vehicle 1 & Vehicle 2 (degrees)	N/A
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	200
Path Obstructions	None
Vehicle Obstructions	None
Road Class	Test Track
Traffic Conditions	N/A
Other Effects	None
Vehicle-Class of Cut-In Vehicle	N/A

Table 1. Test Scenario 1-1

Test Comments: In this test, the RSU (GMC Envoy) sends messages (200 bytes) every 100 msec. The receiving vehicle (LeSabre) is traveling at 40 mph in a lane adjacent to the RSU. Both units are constantly in a clear line-of-sight. The communication link was very reliable since in all trials of this test, at the most, only one packet was lost per run.

Figure 47. Test Number 1-1 Results

Test Number:	**1-1**	**Ambient Weather Conditions:**	**Sunny**
Trace File Name:	**061403_1_1_1.trace***	**Sending Vehicle Model/Make:**	**GMC Envoy**
Date Collected:	**August 14, 2003**	**Receiving Vehicle Model/Make:**	**Buick LeSabre**
Files Resident With Whom:	**F. Ahmed-Zaid**	**Antenna Type Used:**	**Standard**
Operating System Used:	**Linux**	**VSC Obstacle Vehicle #1 Model/Make:**	**N/A**
Software Level Used:	**V1.3 (8-July-03)**	**VSC Obstacle Vehicle #2 Model/Make:**	**N/A**



4.1.2 Test Scenario 1-2

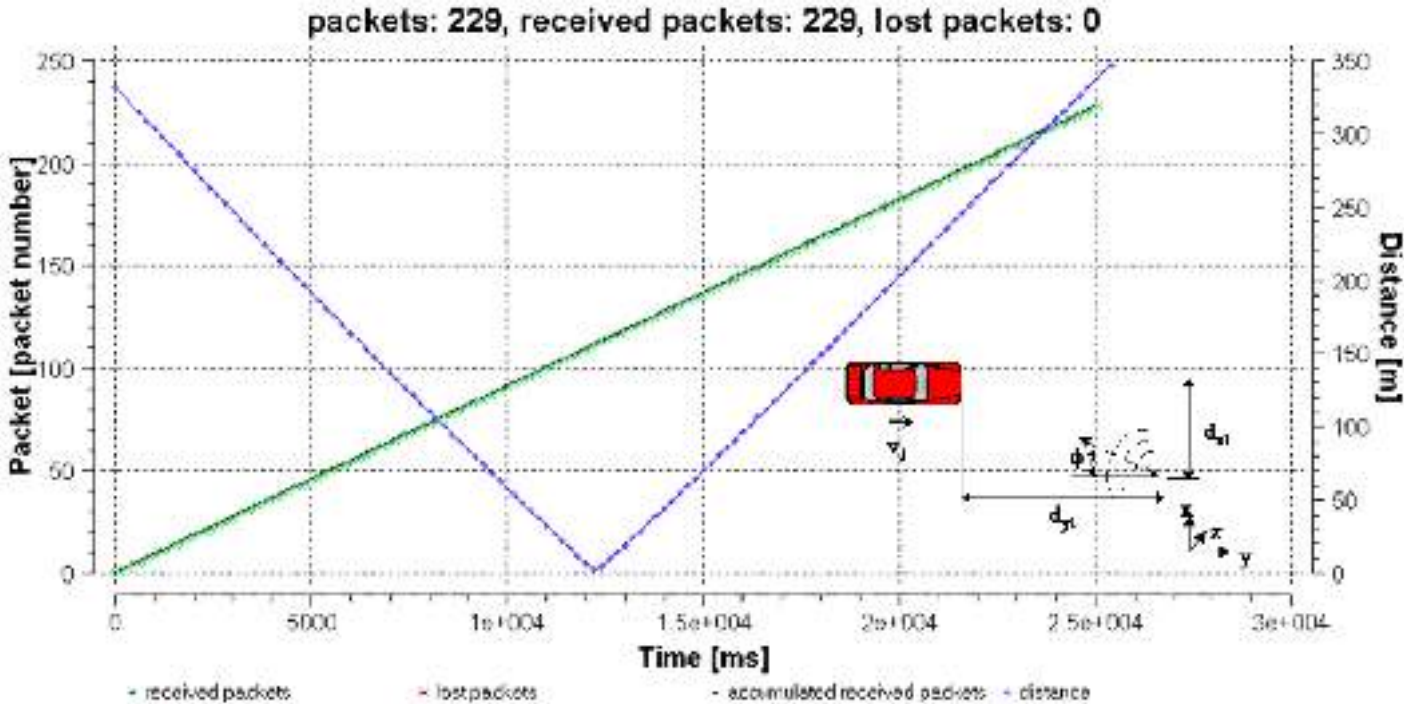
Test Scenario	**1-2**
Relevant Applications	Traffic Signal Violation Warning Curve Speed Warning / Rollover Warning Left-Turn Assistant
Velocity of Receiving Antenna (miles/hour)	60
Distance Between Antennas (meters)	< 300
Lateral Offset to Broadcast Antenna (meters)	4
Velocity of Sending Antenna (miles/hour)	0
Angle Between Vehicle 1 & Vehicle 2 (degrees)	N/A
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	200
Path Obstructions	None
Vehicle Obstructions	None
Road Class	Test Track
Traffic Conditions	N/A
Other Effects	None
Vehicle-Class of Cut-In Vehicle	N/A

Table 2. Test Scenario 1-2

Test Comments: In this test the RSU (GMC Envoy) sends messages (200 bytes) every 100 msec. The receiving vehicle (LeSabre) is traveling at 60 mph in a lane adjacent to the RSU. Both units are constantly in a clear line-of-sight. The communication link was very reliable since in all trials of this test, at the most, only 5 packets were lost per run.

Figure 48. Test Number 1-2 Results

Test Number:	1-2	Ambient Weather Conditions:	Sunny
Trace File Name:	001403_1_2_1.trace*	Sending Vehicle Model/Make:	GMC Envoy
Date Collected:	August 14, 2003	Receiving Vehicle Model/Make:	Buick LeSabre
Files Resident With Whom:	F. Ahmed-Zaid	Antenna Type Used:	Standard
Operating System Used:	Linux	VSC Obstacle Vehicle #1 Model/Make:	N/A
Software Level Used:	V2.3 (8-July-03)	VSC Obstacle Vehicle #2 Model/Make:	N/A



4.1.3 Test Scenario 1-3

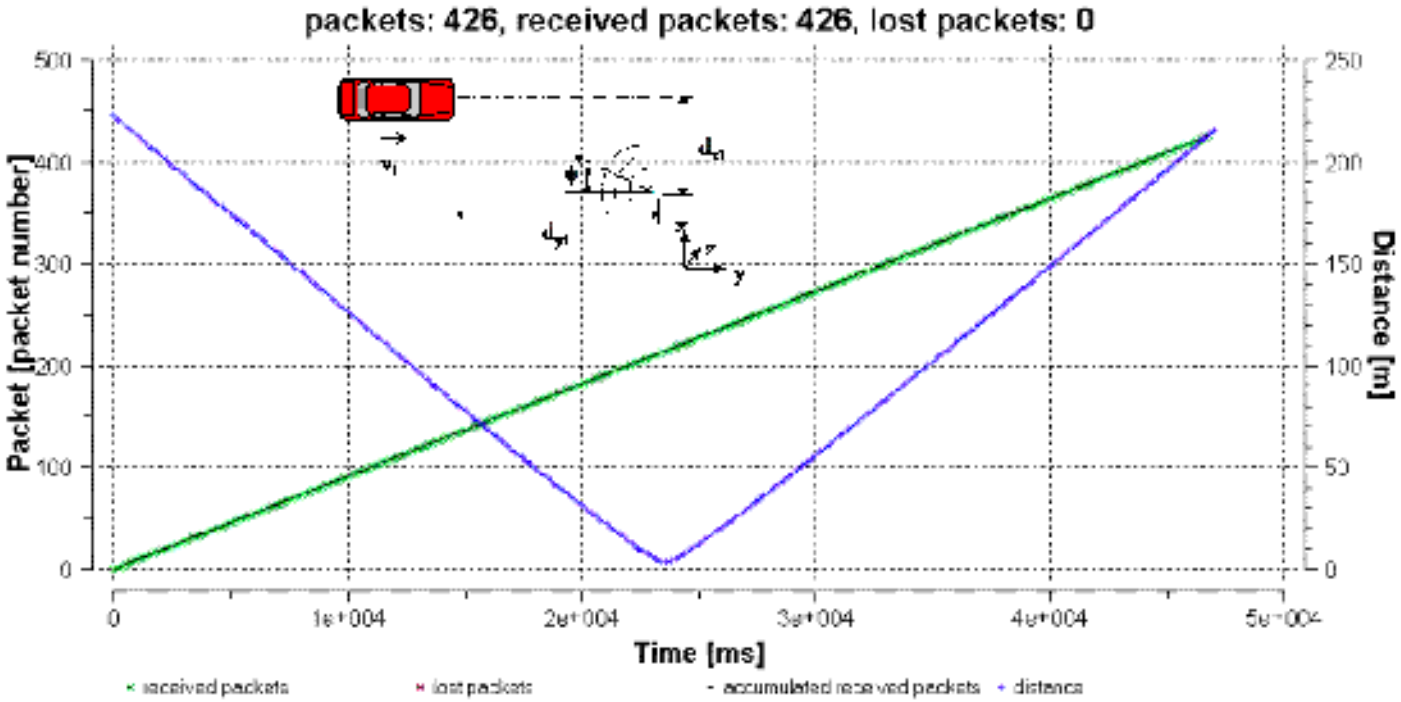
Test Scenario	**1-3**
Relevant Applications	Traffic Signal Violation Warning Curve Speed Warning / Rollover Warning Left-Turn Assistant
Velocity of Receiving Antenna (miles/hour)	20
Distance Between Antennas (meters)	< 100
Lateral Offset to Broadcast Antenna (meters)	4
Velocity of Sending Antenna (miles/hour)	0
Angle Between Vehicle 1 & Vehicle 2 (degrees)	N/A
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	400
Path Obstructions	None
Vehicle Obstructions	None
Road Class	Test Track
Traffic Conditions	N/A
Other Effects	None
Vehicle-Class of Cut-In Vehicle	N/A

Table 3. Test Scenario 1-3

Test Comments: In this test the RSU (GMC Envoy) sends messages (400 bytes) every 100 msec. The receiving vehicle (LeSabre) is traveling at 20 mph in a lane adjacent to the RSU. Both units are constantly in a clear line-of-sight. The communication link was very reliable since in all trials of this test, at the most, only 2 packets were lost per run.

Figure 49. Test Number 1-3 Results

Test Number	**1-3**	**Ambient Weather Conditions:**	**Sunny**
Trace File Name:	**[illegible]_1_3_1.trace***	**Sending Vehicle Model/Make:**	**GMC Envoy**
Date Collected:	**August 14, 2003**	**Receiving Vehicle Model/Make:**	**Buick LeSabre**
Files Resident With Whom:	**F. Ahmed-Zaid**	**Antenna Type Used:**	**Standard**
Operating System Used:	**Linux**	**VSC Obstacle Vehicle #1 Model/Make:**	**N/A**
Software Level Used:	**V2.3 (8-July-03)**	**VSC Obstacle Vehicle #2 Model/Make:**	**N/A**



4.1.4 Test Scenario 1-4

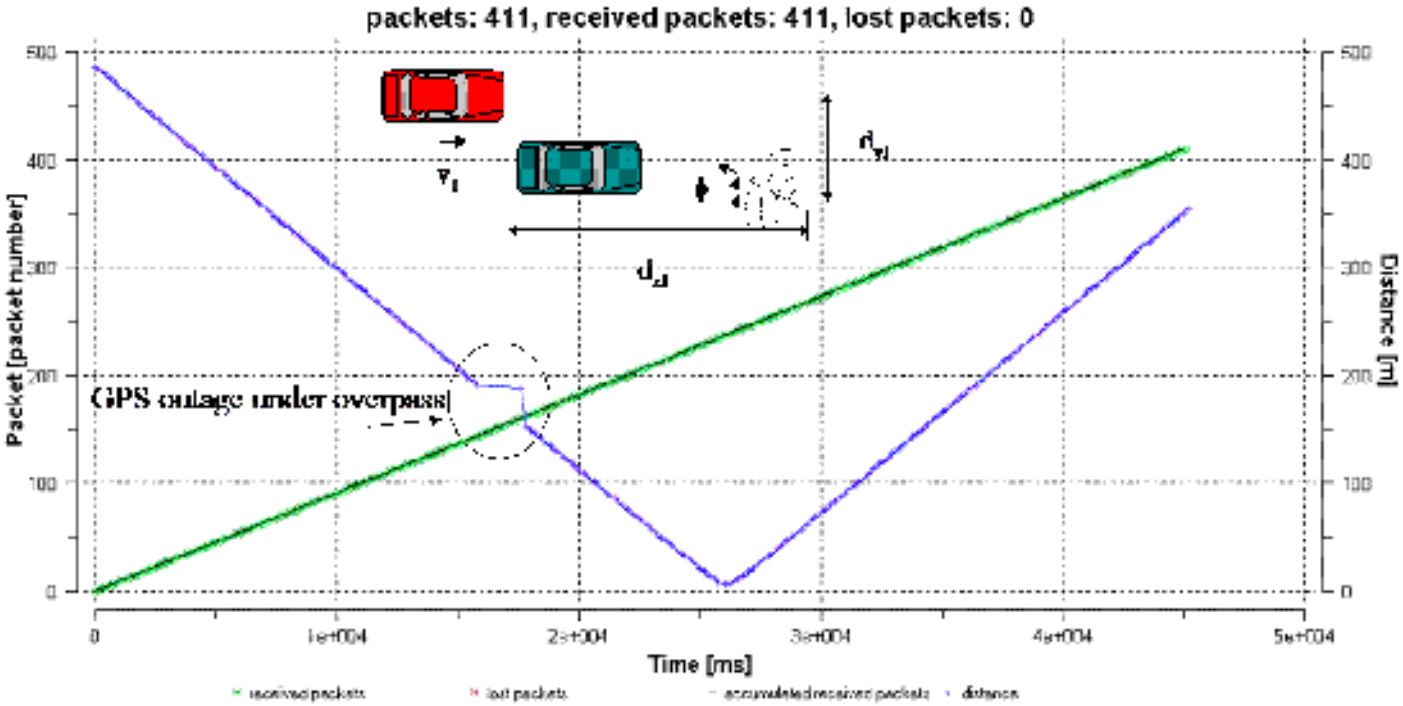
Test Scenario	**1-4**
Relevant Applications	Traffic Signal Violation Warning Curve Speed Warning / Rollover Warning Left-Turn Assistant
Velocity of Receiving Antenna (miles/hour)	40
Distance Between Antennas (meters)	< 300
Lateral Offset to Broadcast Antenna (meters)	8
Velocity of Sending Antenna (miles/hour)	0
Angle Between Vehicle 1 & Vehicle 2 (degrees)	N/A
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	200
Path Obstructions	None
Vehicle Obstructions	Sustained
Road Class	Test Track
Traffic Conditions	N/A
Other Effects	None
Vehicle-Class of Cut-In Vehicle	SUV

Table 4. Test Scenario 1-4

Test Comments: In this test, the RSU (GMC Envoy) sends messages (200 bytes) every 100 msec. The receiving vehicle (LeSabre) is traveling at 40 mph, two lanes over from the RSU. Both units are in a clear line-of-sight except when they are obstructed by a stopped SUV (GMC Envoy). The communication link was very reliable since no packets were dropped.

Figure 50. Test Number 1-4 Results

Test Number:	**1-4**	**Ambient Weather Conditions:**	**Sunny**
Trace File Name:	**000703_1_4_2.trace***	**Sending Vehicle Model/Make:**	**Buick LeSabre**
Date Collected:	**August 7, 2003**	**Receiving Vehicle Model/Make:**	**Buick LeSabre**
Files Resident With Whom:	**F. Ahmed-Zaid**	**Antenna Type Used:**	**Standard**
Operating System Used:	**Linux**	**VRC Outside Vehicle #1 Model/Make:**	**GMC Envoy**
Software Level Used:	**V2.3 (8-July-03)**	**VRC Outside Vehicle #2 Model/Make:**	**N/A**



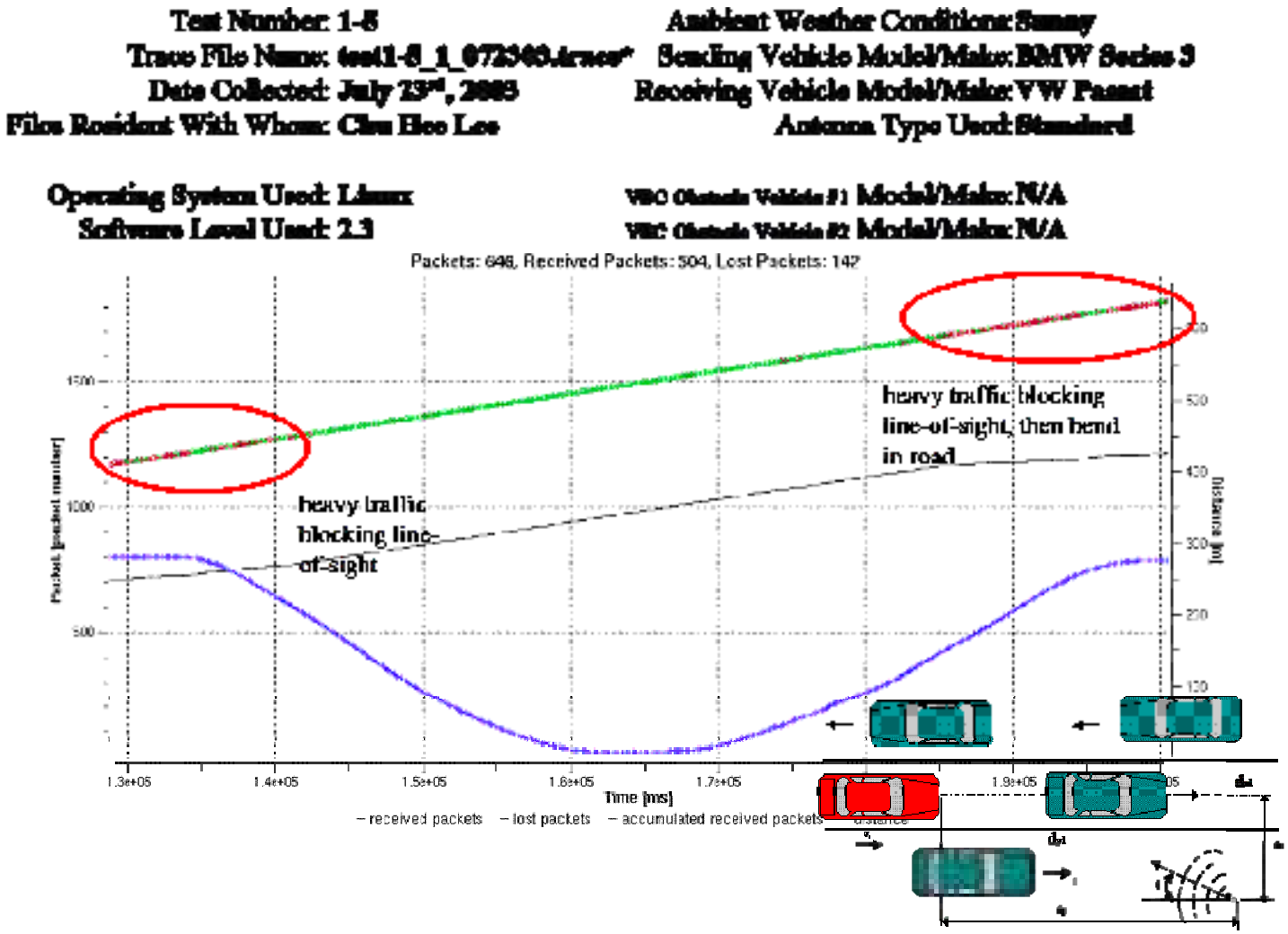
4.1.5 Test Scenario 1-5

Test Scenario	**1-5**
Relevant Applications	Traffic Signal Violation Warning Curve Speed Warning / Rollover Warning Left-Turn Assistant
Velocity of Receiving Antenna (miles/hour)	var
Distance Between Antennas (meters)	var
Lateral Offset to Broadcast Antenna (meters)	var
Velocity of Sending Antenna (miles/hour)	0
Angle Between Vehicle 1 & Vehicle 2 (degrees)	N/A
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	200
Path Obstructions	Yes
Vehicle Obstructions	Sustained
Road Class	Arterial
Traffic Conditions	High
Other Effects	None
Vehicle-Class of Cut-In Vehicle	N/A

Table 5. Test Scenario 1-5

Test Comments: The outages shown in the illustration are due to traffic, trees, and buildings that are in the way before and after the vehicle passes the other one on the side of the road. The road curves slightly after the vehicle passes, so that the maximum line-of-sight is shorter in that direction. The moving vehicle was in the lane closest to the curb.

Figure 51. Test Number 1-5 Results



4.1.6 Test Scenario 1-6

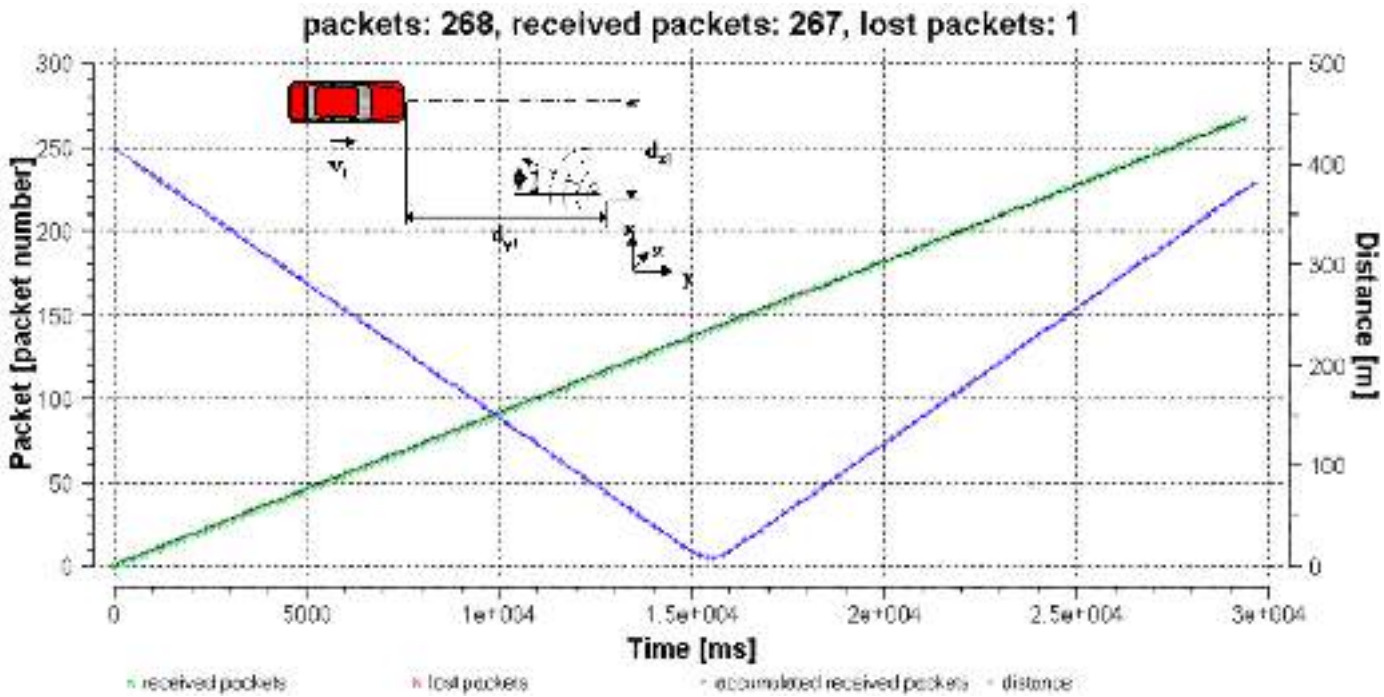
Test Scenario	**1-6**
Relevant Applications	Traffic Signal Violation Warning Curve Speed Warning / Rollover Warning Left-Turn Assistant
Velocity of Receiving Antenna (miles/hour)	60
Distance Between Antennas (meters)	< 300
Lateral Offset to Broadcast Antenna (meters)	8
Velocity of Sending Antenna (miles/hour)	0
Angle Between Vehicle 1 & Vehicle 2 (degrees)	N/A
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	400
Path Obstructions	None
Vehicle Obstructions	None
Road Class	Test Track
Traffic Conditions	N/A
Other Effects	None
Vehicle-Class of Cut-In Vehicle	N/A

Table 6. Test Scenario 1-6

Test Comments: In this test, the RSU (GMC Envoy) sends messages (400 bytes) every 100 msec. The receiving vehicle (LeSabre) is traveling at 60 mph, two lanes over from the RSU. Both units are constantly in a clear line-of-sight. The communication link was very reliable since in all trials of this test, at the most, only 4 packets were lost per run.

Figure 52. Test Number 1-6 Results

Test Number	**1-6**	**Ambient Weather Conditions:**	**Sunny**
Trace File Name:	**081403_1_6_Linux***	**Sending Vehicle Model/Make:**	**GMC Envoy**
Date Collected:	**August 14, 2003**	**Receiving Vehicle Model/Make:**	**Buick LeSabre**
Files Resident With Whom:	**F. Ahmed-Zaid**	**Antenna Type Used:**	**Standard**
Operating System Used:	**Linux**	**VSC Obstacle Vehicle #1 Model/Make:**	**N/A**
Software Level Used:	**V2.3 (8-July-03)**	**VSC Obstacle Vehicle #2 Model/Make:**	**N/A**



4.1.7 Test Scenario 1-9

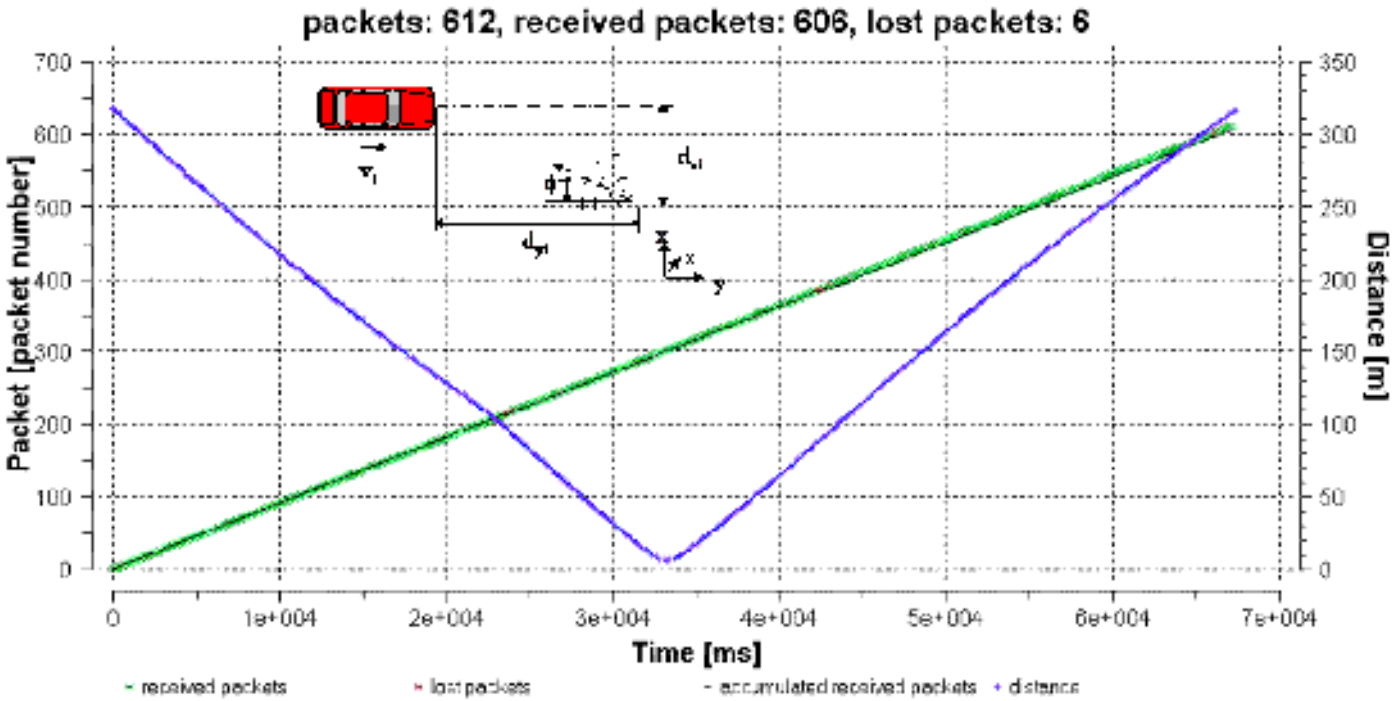
Test Scenario	**1-9**
Relevant Applications	Traffic Signal Violation Warning Curve Speed Warning / Rollover Warning Left-Turn Assistant
Velocity of Receiving Antenna (miles/hour)	20
Distance Between Antennas (meters)	< 300
Lateral Offset to Broadcast Antenna (meters)	8
Velocity of Sending Antenna (miles/hour)	0
Angle Between Vehicle 1 & Vehicle 2 (degrees)	N/A
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	400
Path Obstructions	None
Vehicle Obstructions	None
Road Class	Test Track
Traffic Conditions	N/A
Other Effects	None
Vehicle-Class of Cut-In Vehicle	N/A

Table 7. Test Scenario 1-9

Test Comments: In this test, the RSU (GMC Envoy) sends messages (400 bytes) every 100 msec. The receiving vehicle (LeSabre) is traveling at 20 mph, two lanes over from the RSU. Both units are constantly in a clear line-of-sight. The communication link was very reliable since in all trials of this test, at the most, only 10 packets were lost per run.

Figure 53. Test Number 1-9 Results

Test Number:	**1-9**	**Ambient Weather Conditions:**	**Sunny**
Trace File Name:	**[illegible]**	**Sending Vehicle Model/Maker:**	**GMC Envoy**
Date Collected:	**August 14, [illegible]**	**Receiving Vehicle Model/Maker:**	**Buick LeSabre**
Files Resident With Whom:	**F. Ahmed-Zaid**	**Antenna Type Used:**	**Standard**
Operating System Used:	**Linux**	**VSC Obstacle Vehicle #1 Model/Maker:**	**N/A**
Software Level Used:	**V1.3 (8-July-03)**	**VSC Obstacle Vehicle #2 Model/Maker:**	**N/A**



4.1.8 Test Scenario 1-10

Test Scenario	**1-10**
Relevant Applications	Traffic Signal Violation Warning Curve Speed Warning / Rollover Warning Left-Turn Assistant
Velocity of Receiving Antenna (miles/hour)	var
Distance Between Antennas (meters)	var
Lateral Offset to Broadcast Antenna (meters)	var
Velocity of Sending Antenna (miles/hour)	0
Angle Between Vehicle 1 & Vehicle 2 (degrees)	N/A
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	400
Path Obstructions	None
Vehicle Obstructions	Cut-in
Road Class	Highway
Traffic Conditions	N/A
Other Effects	None
Vehicle-Class of Cut-In Vehicle	SUV

Table 8. Test Scenario 1-10

Test Comments: The receiver started from a distance about 550 meters from the sender. The sender was at the traffic light. When the receiver approached the RSU, a big truck, in addition to the SUV used for the test, was in between the receiver and the RSU (sender) causing packet drops. As the receiver traveled out of the line-of-sight, the RSU started losing packets (packet number >700).

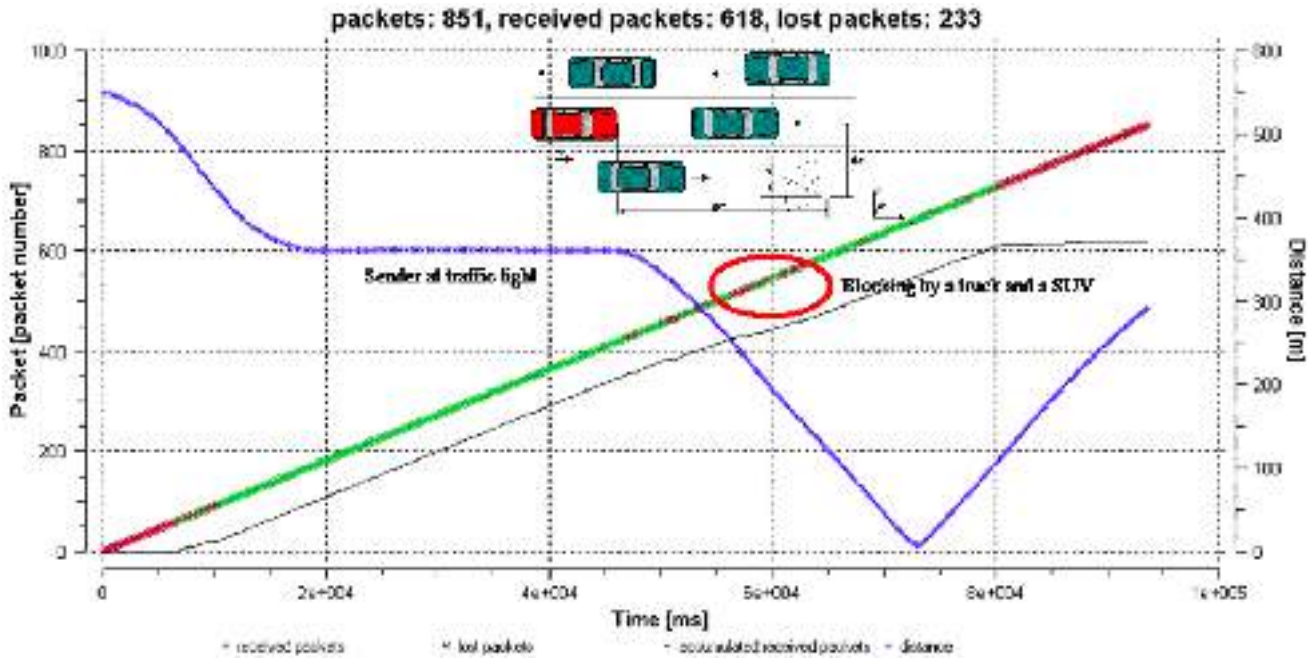
Figure 54. Test Number 1-10 Results

Test File: 1-10
Trace File Name: test1-10_1_[illegible].trace
Date Collected: August 6th, 2003
Files Resident With Whom: Chu-Hee Lee

Ambient Weather Conditions: Sunny
Sending Vehicle Model/Make: BMW 330
Receiving Vehicle Model/Make: VW Passat
Antenna Type Used: Standard

Operating System Used: Linux
Software Level Used: 2.3

VSC Obstacle Vehicle #1 Model/Make: BMW X5
VSC Obstacle Vehicle #2 Model/Make: N/A



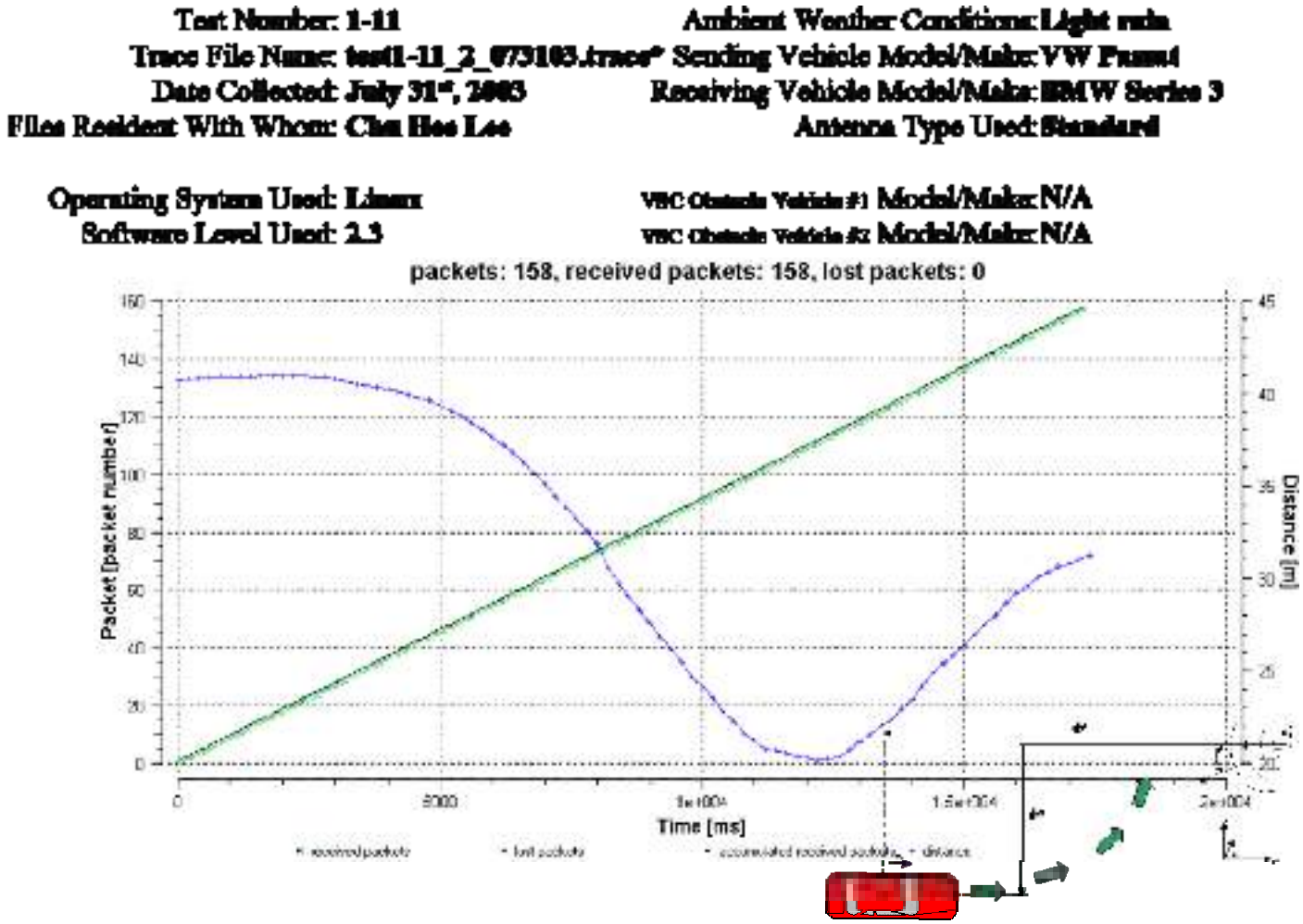
4.1.9 Test Scenario 1-11

Test Scenario	**1-11**
Relevant Applications	Left-Turn Assistant
Velocity of Receiving Antenna (miles/hour)	5
Distance Between Antennas (meters)	< 20
Lateral Offset to Broadcast Antenna (meters)	var
Velocity of Sending Antenna (miles/hour)	0
Angle Between Vehicle 1 & Vehicle 2 (degrees)	N/A
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	400
Path Obstructions	None
Vehicle Obstructions	None
Road Class	
Traffic Conditions	N/A
Other Effects	Left Turn
Vehicle-Class of Cut-In Vehicle	N/A

Table 9. Test Scenario 1-11

Test Comments: All packets were received during this test. The vehicles were within the line-of-sight for the entire test.

Figure 55. Test Number 1-11 Results



4.1.10 Test Scenario 1-12

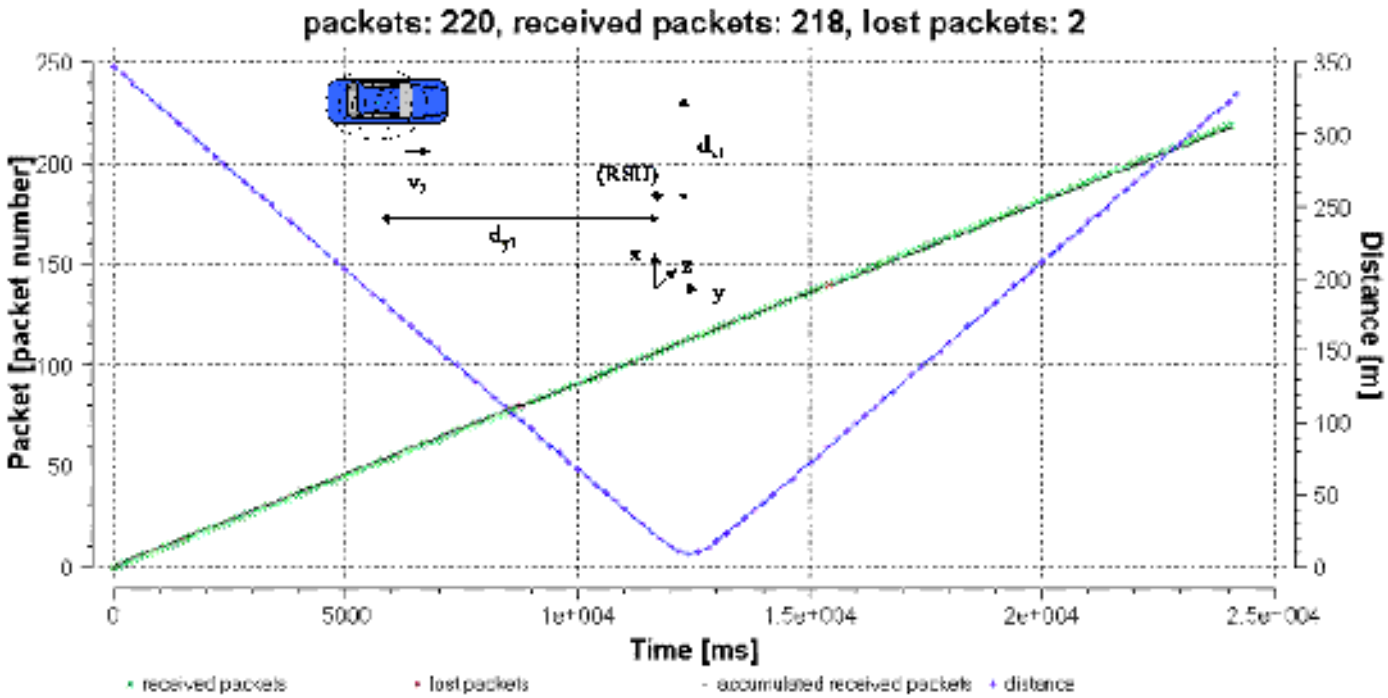
Test Scenario	**1-12**
Relevant Applications	Left-Turn Assistant Stop Sign Movement Assistant
Velocity of Receiving Antenna (miles/hour)	0
Distance Between Antennas (meters)	< 300
Lateral Offset to Broadcast Antenna (meters)	8
Velocity of Sending Antenna (miles/hour)	60
Angle Between Vehicle 1 & Vehicle 2 (degrees)	N/A
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	300
Path Obstructions	None
Vehicle Obstructions	None
Road Class	Test Track
Traffic Conditions	N/A
Other Effects	None
Vehicle-Class of Cut-In Vehicle	N/A

Table 10. Test Scenario 1-12

Test Comments: In this test, the OBU (LeSabre) sends messages (300 bytes) every 100 msec. The receiving vehicle (GMC Envoy) is traveling at 60 mph, two lanes over from the RSU. Both units are constantly in a clear line-of-sight. The communication link was very reliable since in all trials of this test, at the most, only 4 packets were lost per run.

Figure 56. Test Number 1-12 Results

Test Number:	1-12	Ambient Weather Conditions:	Sunny
Trace File Name:	081403_1_12_3.trace*	Sending Vehicle Model/Make:	Buick LeSabre
Date Collected:	August 14, 2003	Receiving Vehicle Model/Make:	GMC Envoy
Files Resident With Whom:	F. Ahmed-Zaid	Antenna Type Used:	Standard
Operating System Used:	Linux	VSC Obstacle Vehicle #1 Model/Make:	N/A
Software Level Used:	V1.3 (8-July-03)	VSC Obstacle Vehicle #2 Model/Make:	N/A



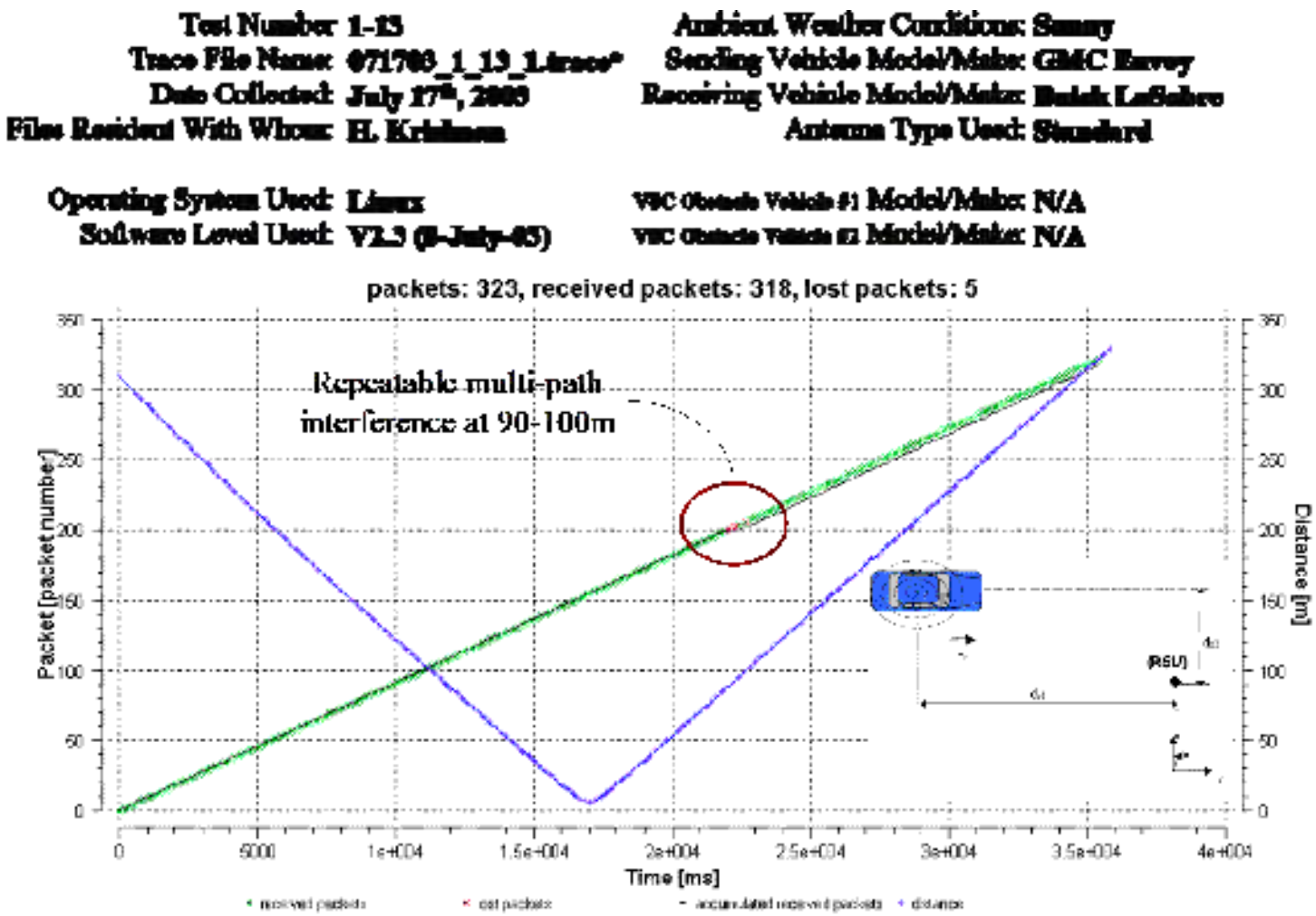
4.1.11 Test Scenario 1-13

Test Scenario	**1-13**
Relevant Applications	Left-Turn Assistant Stop Sign Movement Assistant
Velocity of Receiving Antenna (miles/hour)	0
Distance Between Antennas (meters)	< 300
Lateral Offset to Broadcast Antenna (meters)	8
Velocity of Sending Antenna (miles/hour)	40
Angle Between Vehicle 1 & Vehicle 2 (degrees)	N/A
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	300
Path Obstructions	None
Vehicle Obstructions	None
Road Class	Test Track
Traffic Conditions	N/A
Other Effects	None
Vehicle-Class of Cut-In Vehicle	N/A

Table 11. Test Scenario 1-13

Test Comments: There was a clear line-of-sight for the duration of this test between the sending vehicle and the stationary RSU. One reception outage was observed in the same location for all three trials (90-100 m away from the RSU), which was proven in Test 1-20 to be a multipath interference. Overall, 98 percent of the packets (1369 of 1391) sent during the four trials of the test were successfully received.

Figure 57. Test Number 1-13 Results



4.1.12 Test Scenario 1-14

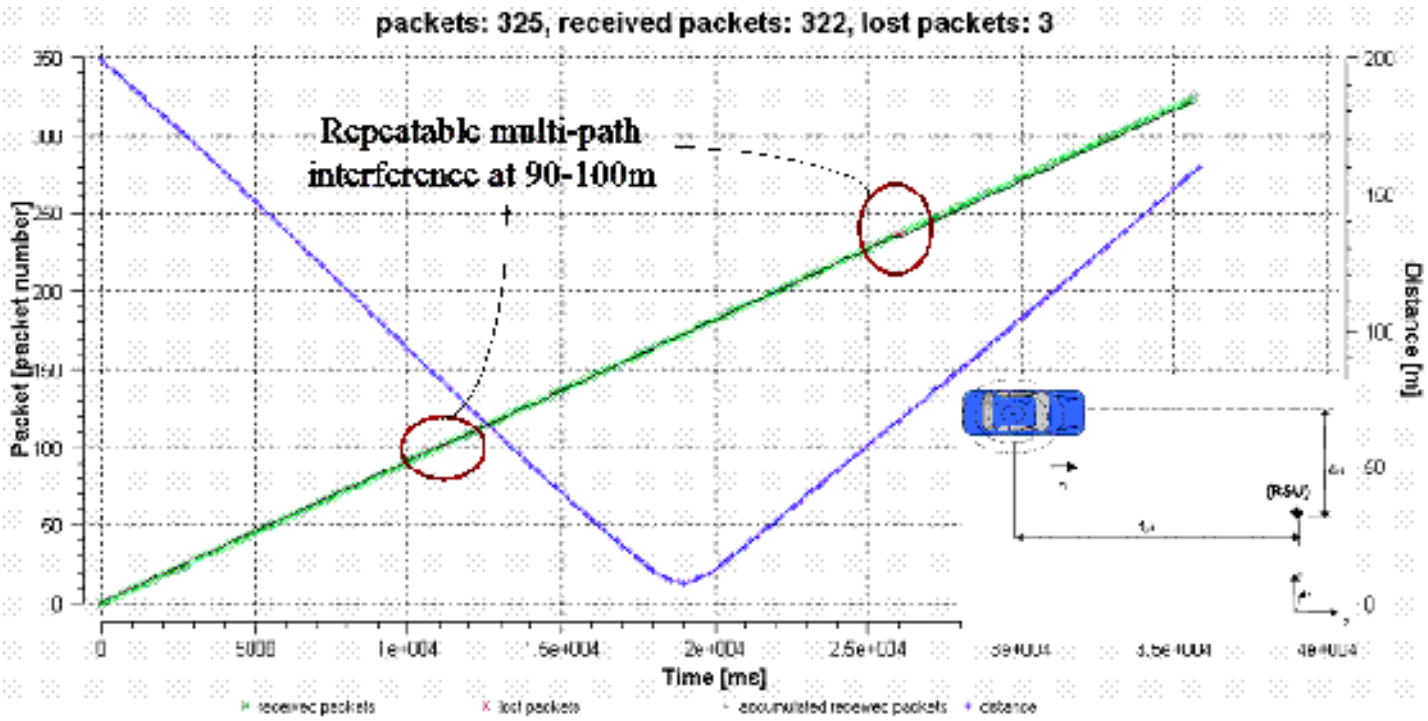
Test Scenario	**1-14**
Relevant Applications	Left-Turn Assistant Stop Sign Movement Assistant
Velocity of Receiving Antenna (miles/hour)	0
Distance Between Antennas (meters)	< 100
Lateral Offset to Broadcast Antenna (meters)	8
Velocity of Sending Antenna (miles/hour)	20
Angle Between Vehicle 1 & Vehicle 2 (degrees)	N/A
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	300
Path Obstructions	None
Vehicle Obstructions	None
Road Class	Test Track
Traffic Conditions	N/A
Other Effects	None
Vehicle-Class of Cut-In Vehicle	N/A

Table 12. Test Scenario 1-14

Test Comments: There was a clear line-of-sight for the duration of this test between the sending vehicle and the stationary RSU. Two reception outages (1 packet and 2 packets) were observed (70-80 m away from the RSU), which is explained in Test 1-20 as a NULL due to multipath interference.

Figure 58. Test Number 1-14 Results

Test Number:	**1-14**	**Ambient Weather Conditions:**	**Sunny**
Trace File Name:	**072403_1_14_3.trace***	**Sending Vehicle Model/Make:**	**Buick LeSabre**
Date Collected:	**July 24th, 2003**	**Receiving Vehicle Model/Make:**	**Buick LeSabre**
Files Resident With Whom:	**H. Krishnan**	**Antenna Type Used:**	**Standard**
Operating System Used:	**Linux**	**VSC Obstacle Vehicle #1 Model/Make:**	**N/A**
Software Level Used:	**V2.3 (8-July-03)**	**VSC Obstacle Vehicle #2 Model/Make:**	**N/A**



4.1.13 Test Scenario 1-15

Test Scenario	**1-15**
Relevant Applications	Left-Turn Assistant Stop Sign Movement Assistant
Velocity of Receiving Antenna (miles/hour)	0
Distance Between Antennas (meters)	< 100
Lateral Offset to Broadcast Antenna (meters)	8
Velocity of Sending Antenna (miles/hour)	20
Angle Between Vehicle 1 & Vehicle 2 (degrees)	N/A
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	300
Path Obstructions	None
Vehicle Obstructions	Sustained
Road Class	Test Track
Traffic Conditions	N/A
Other Effects	None
Vehicle-Class of Cut-In Vehicle	SUV

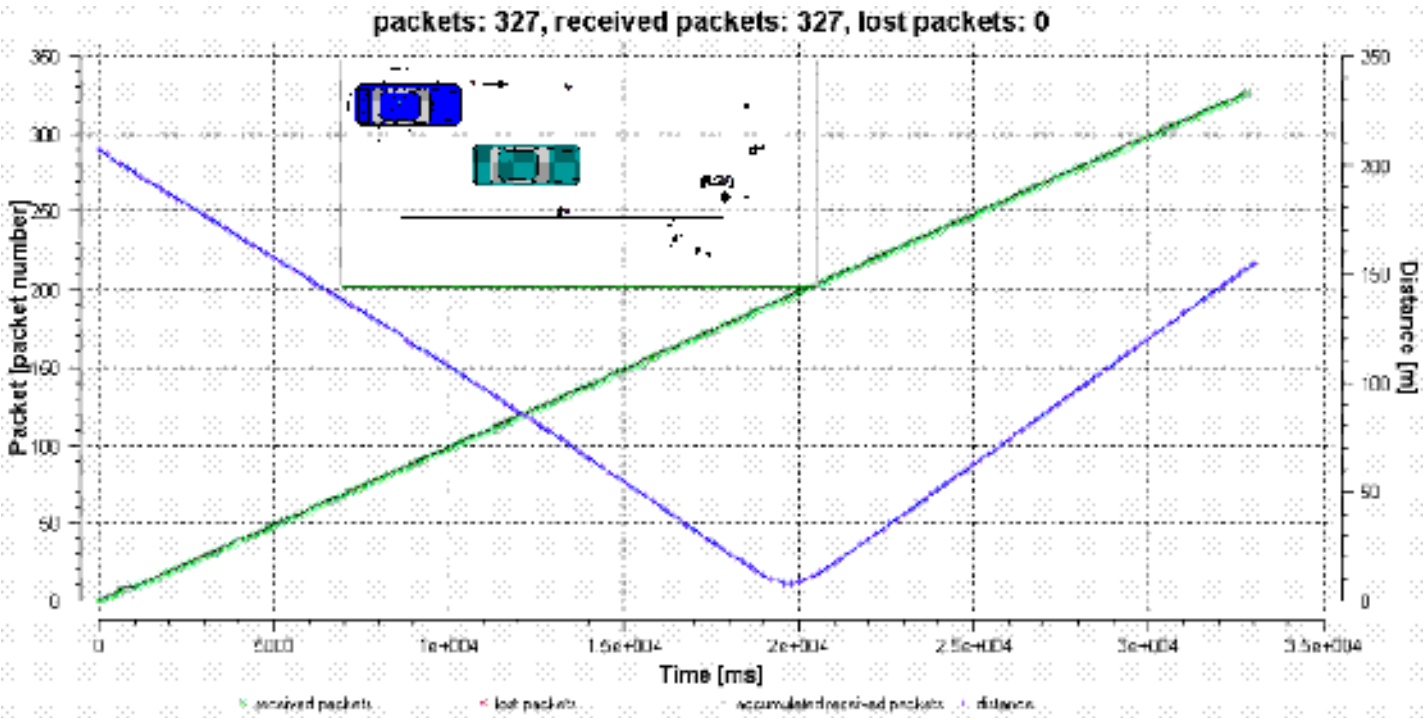
Table 13. Test Scenario 1-15

Test Comments: This test was done in MS Windows. The intercepting vehicle was a Chevy Suburban SUV. There was no loss of reception due to the SUV interception. No packets were lost in all trials of this test.

Figure 59. Test Number 1-15 Results

Test Number:	**1-15**	**Ambient Weather Conditions:**	**Mostly Sunny**
Trace File Name:	**040503_1_15_3.trace***	**Sending Vehicle Model/Make:**	**Buick Lesabre**
Date Collected:	**June 5th, 2003**	**Receiving Vehicle Model/Make:**	**Buick Lesabre**
Files Resident With Whom:	**H. Krishnan**	**Antenna Type Used:**	**Standard**

Operating System Used:	**Windows XP**	**VSC Obstacle Vehicle #1 Model/Make:**	**Chevy Suburban**
Software Level Used:	**2.4a beta (27-Feb-03)**	**VSC Obstacle Vehicle #2 Model/Make:**	**N/A**



4.1.14 Test Scenario 1-17

Test Scenario	**1-17**
Relevant Applications	Traffic Signal Violation Warning Curve Speed Warning / Rollover Warning Left-Turn Assistant
Velocity of Receiving Antenna (miles/hour)	60
Distance Between Antennas (meters)	< 300
Lateral Offset to Broadcast Antenna (meters)	4
Velocity of Sending Antenna (miles/hour)	0
Angle Between Vehicle 1 & Vehicle 2 (degrees)	N/A
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	300
Path Obstructions	None
Vehicle Obstructions	None
Road Class	Highway
Traffic Conditions	Light
Other Effects	None
Vehicle-Class of Cut-In Vehicle	N/A

Table 14. Test Scenario 1-17

Test Comments: Perfect line-of-sight for the middle section of the test, on the straight-away. Road makes sharp bends before and after the straight-away, and there is no reception beyond those bends.

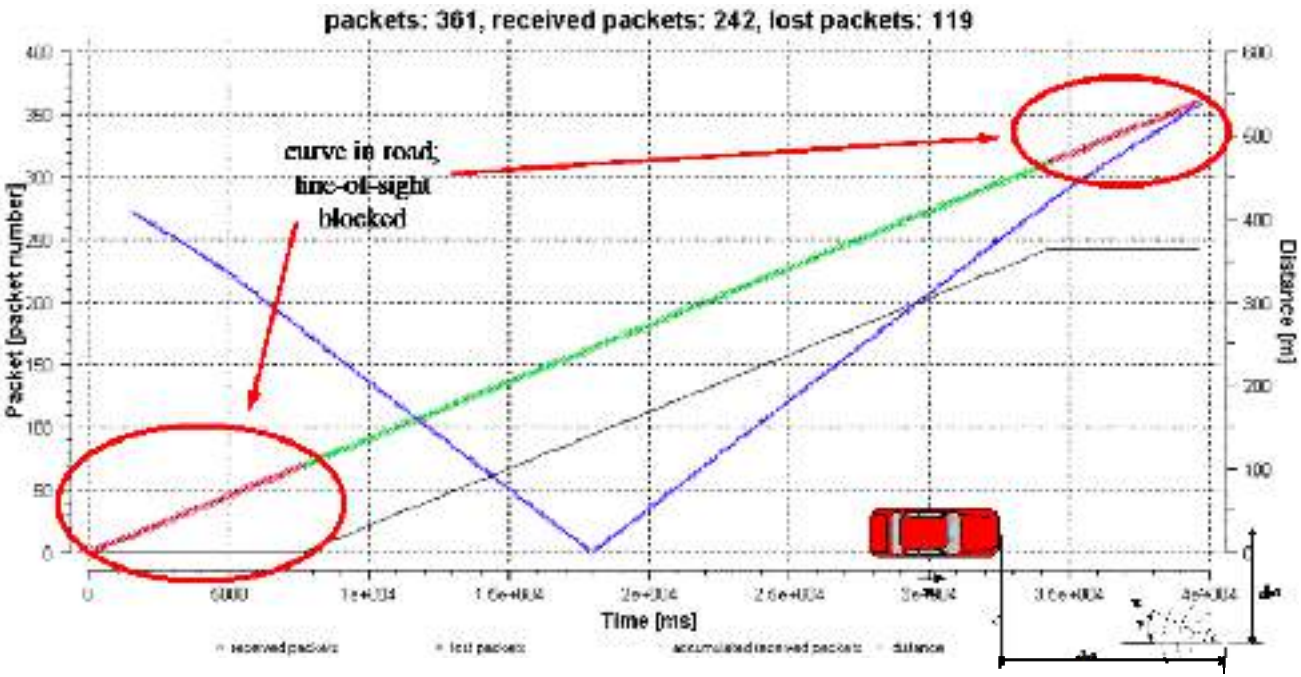
Figure 60. Test Number 1-17 Results

Test Number: 1-17
Trace File Name: test1-17_2_073005.trace*
Date Collected: July 30th, 2005
Files Resident With Whom: Chu Hee Lee

Ambient Weather Condition: Sunny
Sending Vehicle Model/Make: VW Passat
Receiving Vehicle Model/Make: BMW Series 3
Antenna Type Used: Standard

Operating System Used: Linux
Software Level Used: 2.3

VSC Obstacle Vehicle #1 Model/Make: N/A
VSC Obstacle Vehicle #2 Model/Make: N/A



4.1.15 Test Scenario 1-18

Test Scenario	**1-18**
Relevant Applications	Traffic Signal Violation Warning Curve Speed Warning / Rollover Warning Left-Turn Assistant
Velocity of Receiving Antenna (miles/hour)	80
Distance Between Antennas (meters)	< 300
Lateral Offset to Broadcast Antenna (meters)	4
Velocity of Sending Antenna (miles/hour)	0
Angle Between Vehicle 1 & Vehicle 2 (degrees)	N/A
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	300
Path Obstructions	None
Vehicle Obstructions	None
Road Class	Highway
Traffic Conditions	Light
Other Effects	None
Vehicle-Class of Cut-In Vehicle	N/A

Table 15. Test Scenario 1-18

Test Comments: This was a 80 mph drive-by test on a country road with no buildings, but with terrain blockage beyond the range limits of the scenario. Virtually no packet loss was experienced within the line-of-sight. However, there was essentially total packet loss when the receiver was blocked by the terrain.

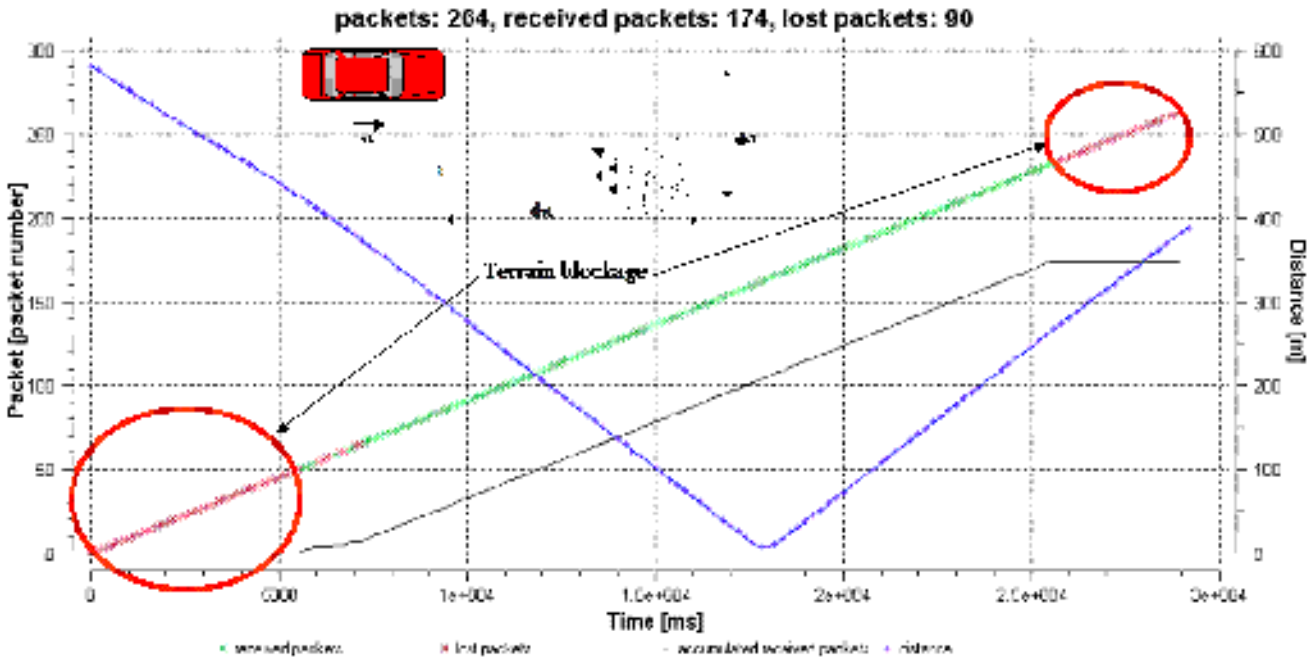
Figure 61. Test Number 1-18 Results

Test Number 1-18
Trace File Name: test1-18_1_073003.trace*
Date Collected: July 30th, 2003
Files Resident With Whom: Chu-Hao Lee

Ambient Weather Condition: Sunny
Sending Vehicle Model/Make: VW Passat
Receiving Vehicle Model/Make: BMW Series 3
Antenna Type Used: Standard

Operating System Used: Linux
Software Level Used: 2.3

VRC Obstacle Vehicle #1 Model/Make: N/A
VRC Obstacle Vehicle #2 Model/Make: N/A



4.1.16 Test Scenario 1-19

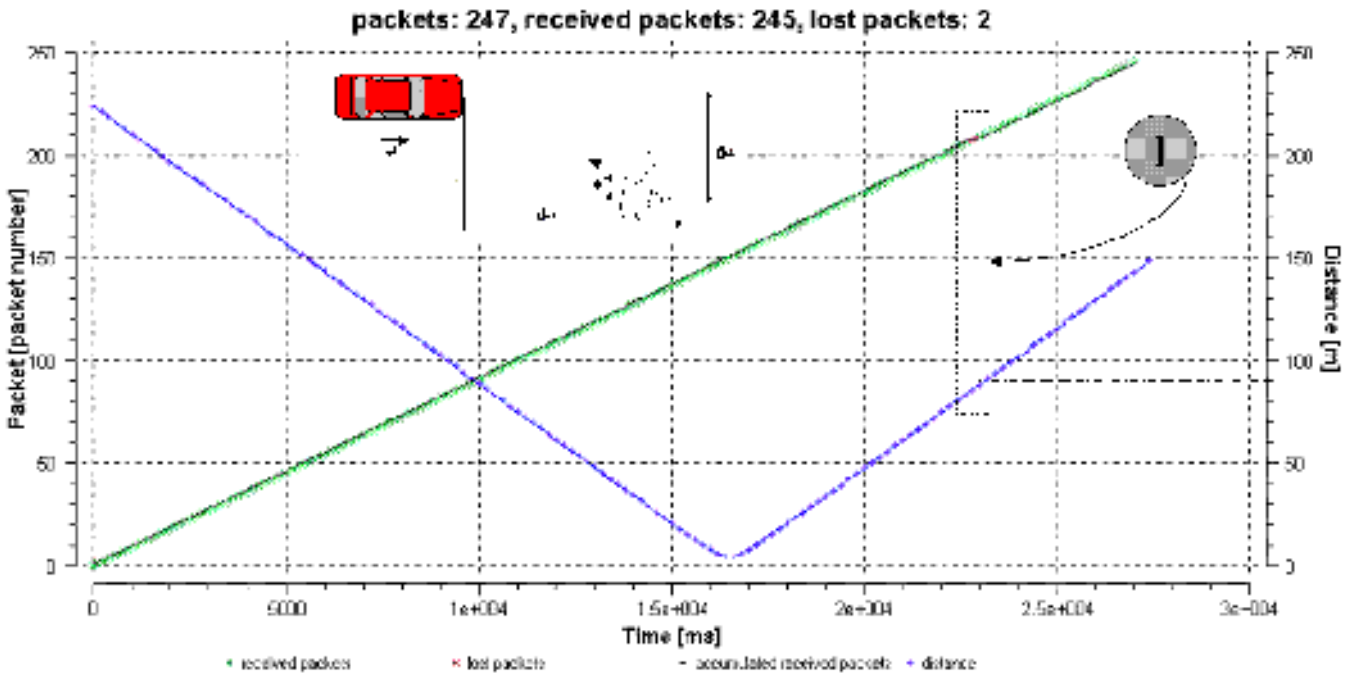
Test Scenario	**1-19**
Relevant Applications	Traffic Signal Violation Warning Curve Speed Warning / Rollover Warning Left-Turn Assistant
Velocity of Receiving Antenna (miles/hour)	30
Distance Between Antennas (meters)	< 100
Lateral Offset to Broadcast Antenna (meters)	4
Velocity of Sending Antenna (miles/hour)	0
Angle Between Vehicle 1 & Vehicle 2 (degrees)	N/A
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	300
Path Obstructions	None
Vehicle Obstructions	None
Road Class	Rural
Traffic Conditions	Light
Other Effects	None
Vehicle-Class of Cut-In Vehicle	N/A

Table 16. Test Scenario 1-19

Test Comments: This test considers a receiving vehicle that passes a stationary antenna at 30 mph. There was a clear line-of-sight throughout the duration of this test. Packets were lost in five of the six trials, and this loss always took place at the range of ~90m. The packet loss can be attributed to multipath cancellation that occurred consistently at that general range, as demonstrated in Test 1-20. Overall, 98.8 percent of the packets sent during the test were received (1,772 out of 1,794 packets).

Figure 62. Test Number 1-19 Results

Test Number	**1-19**	**Ambient Weather Conditions:**	**Sunny**
Trace File Name:	**071703_1_19_1.trace***	**Sending Vehicle Model/Make:**	**GMC Envoy**
Date Collected:	**July 17th, 2003**	**Receiving Vehicle Model/Make:**	**Buick LeSabre**
Files Resident With Whom:	**Jim Bauer**	**Antenna Type Used:**	**Standard**
Operating System Used:	**Linux**	**VBC Obstacle Vehicle #1 Model/Make:**	**N/A**
Software Level Used:	**Version 2.3**	**VBC Obstacle Vehicle #2 Model/Make:**	**N/A**



4.1.17 Test Scenario 1-20

Test Scenario	**1-20**
Relevant Applications	Traffic Signal Violation Warning Curve Speed Warning / Rollover Warning Emergency Electronic Brake Light Pre-Crash Sensing for Co-op Collision Mitigation Co-op Forward Collision Warning (FCW) Left-Turn Assistant Lane Change Warning Stop Sign Movement Assistant
Velocity of Receiving Antenna (miles/hour)	<5
Distance Between Antennas (meters)	vary
Lateral Offset to Broadcast Antenna (meters)	8
Velocity of Sending Antenna (miles/hour)	0
Angle Between Vehicle 1 & Vehicle 2 (degrees)	N/A
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	400
Path Obstructions	None
Vehicle Obstructions	None
Road Class	Test Track
Traffic Conditions	N/A
Other Effects	Multi-path
Vehicle-Class of Cut-In Vehicle	N/A

Table 17. Test Number 1-20

Test Comments: This test was conducted to investigate packet loss that took place at a range of ~90 m during several other tests. The test consisted of a stationary vehicle and a vehicle moving slowly over a distance of ~20 m. The loss of packets highlighted in (1) can be attributed to multipath that occurred consistently at that general range, as shown in the next slides. There was a clear line-of-sight for the duration of this test.

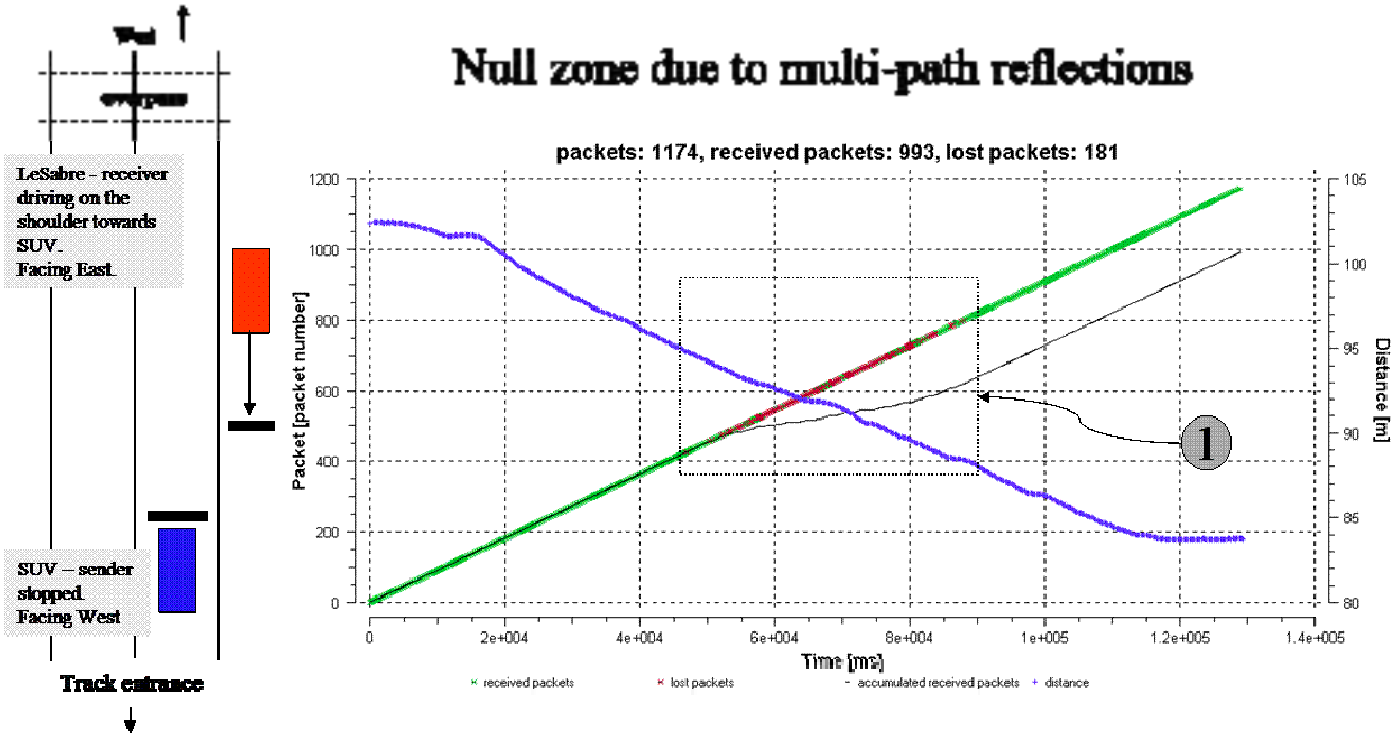
Figure 63. Test Number 1-20 Results

Test Number: 1-20
Trace File Name: 071703_1_20_1.trace*
Date Collected: July 17th, 2003
Files Resident With Whom: Jim Bauer

Ambient Weather Conditions: Sunny
Sending Vehicle Model/Make: GMC Envoy
Receiving Vehicle Model/Make: Buick LeSabre
Antenna Type Used: Standard

Operating System Used: Linux
Software Level Used: Version 2.3

VSC Obstacle Vehicle #1 Model/Make: N/A
VSC Obstacle Vehicle #2 Model/Make: N/A



4.1.18 Test Scenario 1-21

Test Scenario	**1-21**
Relevant Applications	Traffic Signal Violation Warning Curve Speed Warning / Rollover Warning Left-Turn Assistant
Velocity of Receiving Antenna (miles/hour)	60
Distance Between Antennas (meters)	< 300
Lateral Offset to Broadcast Antenna (meters)	4
Velocity of Sending Antenna (miles/hour)	0
Angle Between Vehicle 1 & Vehicle 2 (degrees)	N/A
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	300
Path Obstructions	Yes
Vehicle Obstructions	Sustained
Road Class	Highway
Traffic Conditions	Hvy
Other Effects	None
Vehicle-Class of Cut-In Vehicle	N/A

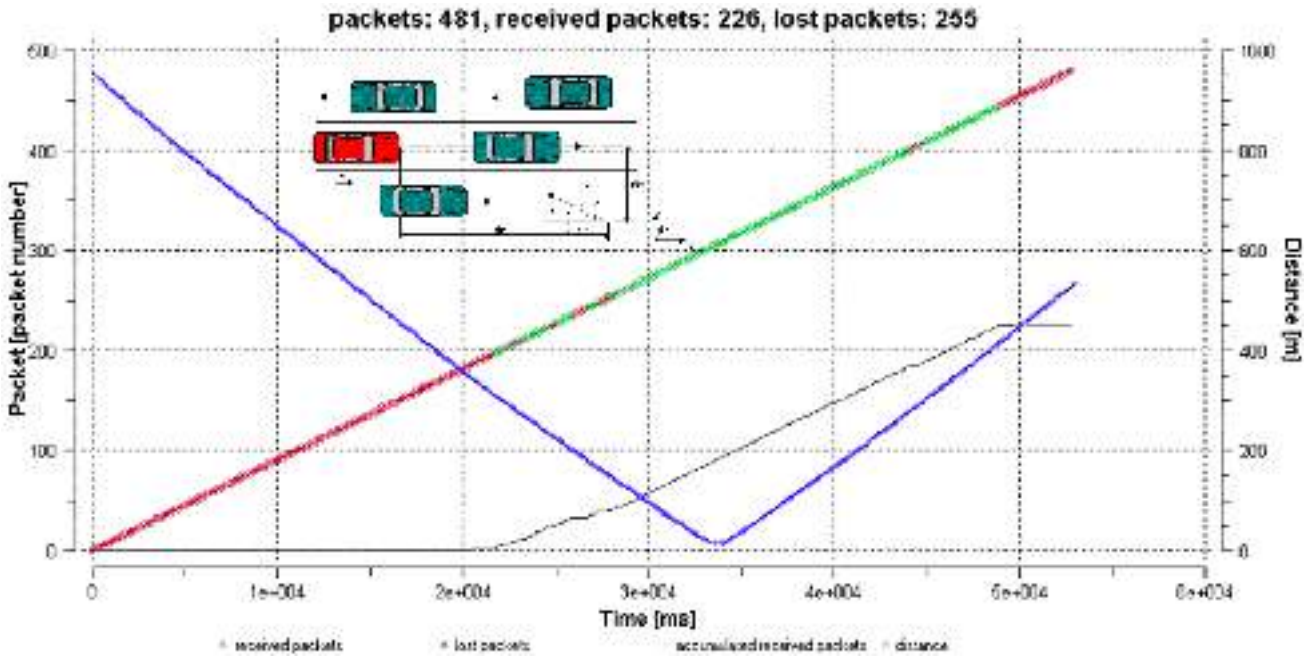
Table 18. Test Scenario 1-21

Test Comments: The sender was coming from a curve out of line-of-sight. This explains the packet drop at the beginning of the test. As the sender approached to the RSU (receiver), the RSU starts receiving (<375 m) packets until the sender goes out of line-of-sight again (>425 m).

Figure 64. Test Number 1-21 Results

Test Number: 1-21 | **Ambient Weather Condition: Sunny**
Trace File Name: test1-21_1_[illegible].trace* | **Sending Vehicle Model/Make: VW Passat**
Date Collected: August 8th, 2003 | **Receiving Vehicle Model/Make: BMW 330**
Files Resident With Whom: Chu-Hao Lee | **Antenna Type Used: Standard**

Operating System Used: Linux | **VSC Obstacle Vehicle #1 Model/Make: N/A**
Software Level Used: 2.3 | **VSC Obstacle Vehicle #2 Model/Make: N/A**



4.1.19 Test Scenario 1-22

Test Scenario	**1-22**
Relevant Applications	Traffic Signal Violation Warning Curve Speed Warning / Rollover Warning Left-Turn Assistant
Velocity of Receiving Antenna (miles/hour)	30
Distance Between Antennas (meters)	< 100
Lateral Offset to Broadcast Antenna (meters)	4
Velocity of Sending Antenna (miles/hour)	0
Angle Between Vehicle 1 & Vehicle 2 (degrees)	N/A
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	300
Path Obstructions	Yes
Vehicle Obstructions	Sustained
Road Class	Rural
Traffic Conditions	Hvy
Other Effects	None
Vehicle-Class of Cut-In Vehicle	N/A

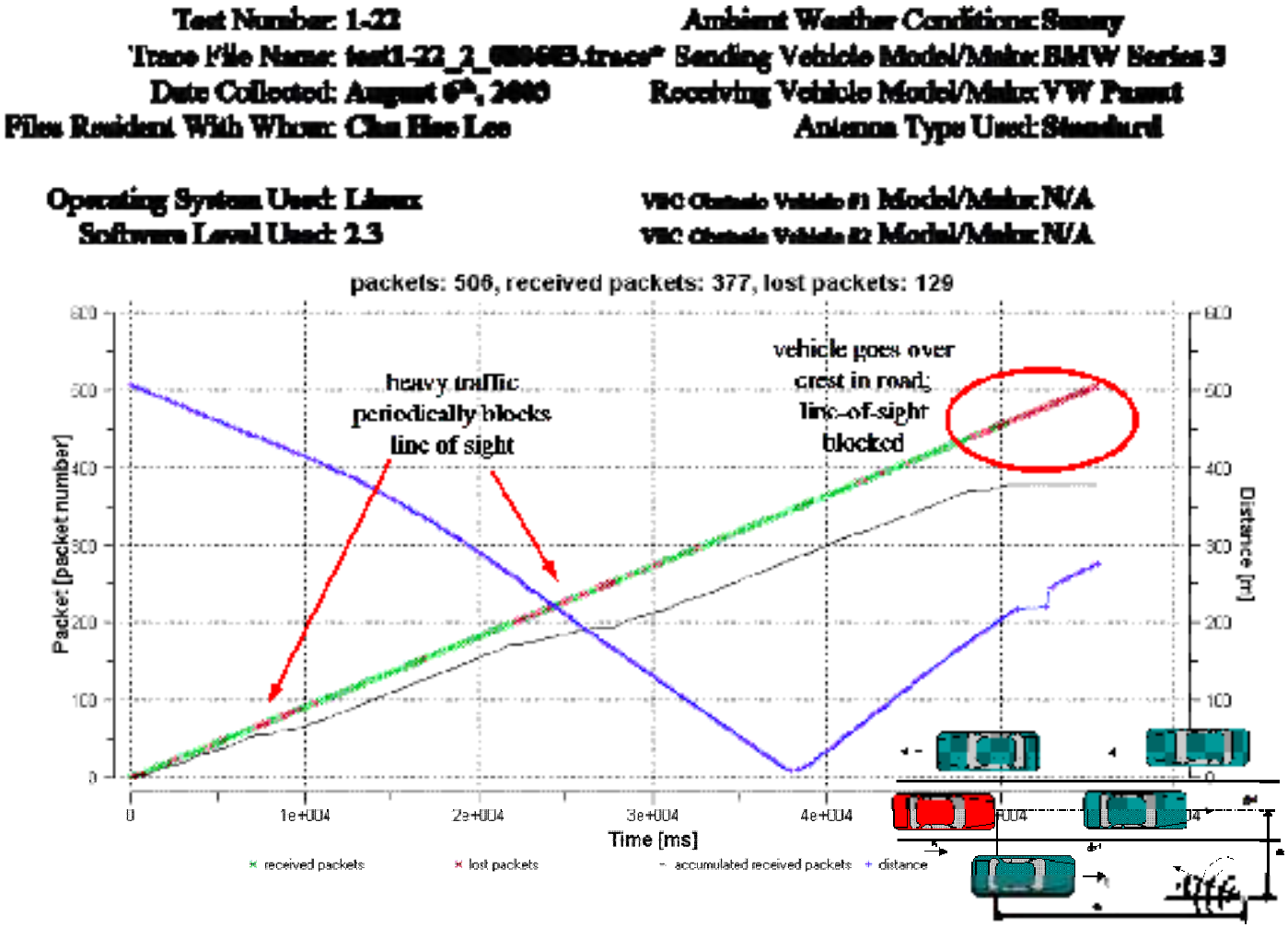
Table 19. Test Scenario 1-22

Test Comments: Heavy traffic periodically blocked the line-of-sight when the vehicle was approaching the RSU. After the vehicle passed the RSU, it went over a hill and out of line-of-sight.

Figure 65. Test Number 1-2 Results

NVP w.org (.5) (7am)

NVP w.org (.5) (7pm)NVP w.org (.5) (7am)
NVP w.org (.5) (7pm)



4.1.20 Test Scenario 1-23

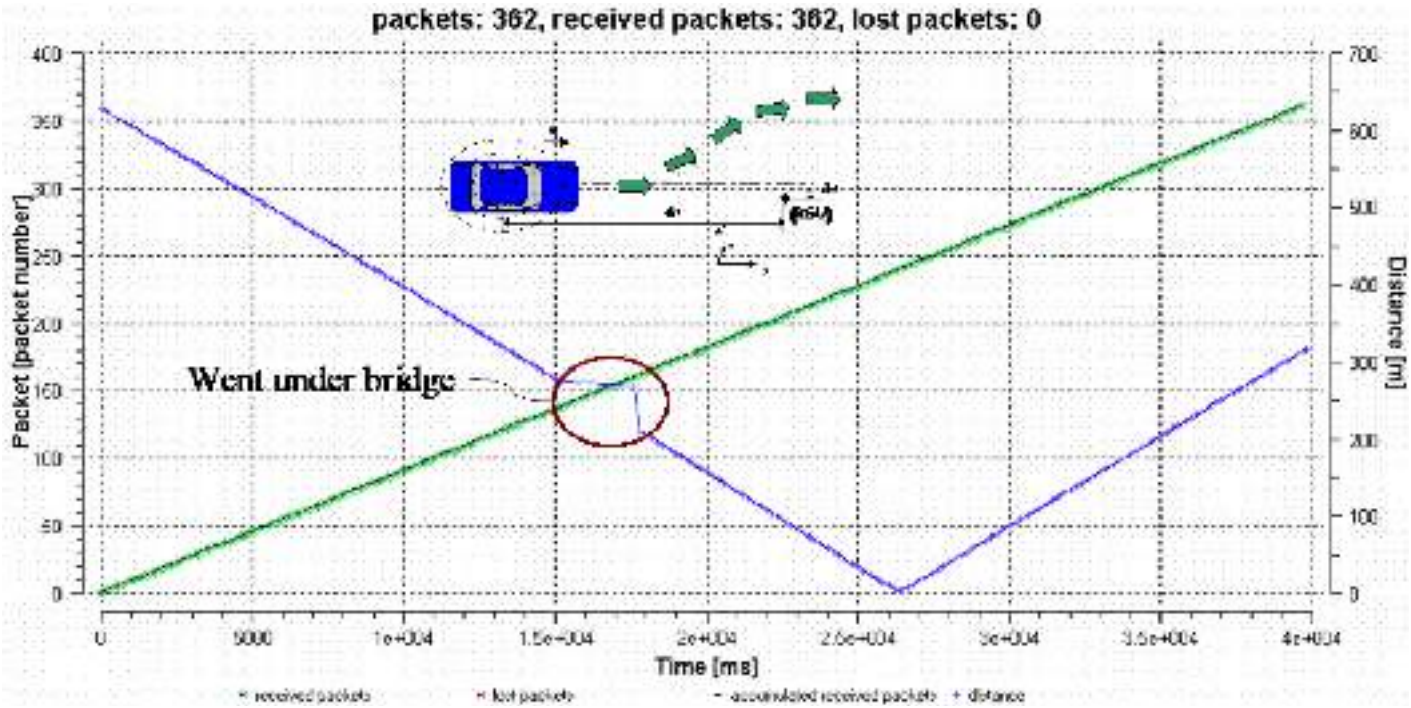
Test Scenario	**1-23**
Relevant Applications	Emergency Electronic Brake Light Pre-Crash Sensing for Co-op Collision Mitigation Co-op Forward Collision Warning (FCW) Lane Change Warning
Velocity of Receiving Antenna (miles/hour)	50
Distance Between Antennas (meters)	< 300
Lateral Offset to Broadcast Antenna (meters)	0
Velocity of Sending Antenna (miles/hour)	0
Angle Between Vehicle 1 & Vehicle 2 (degrees)	N/A
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	200
Path Obstructions	None
Vehicle Obstructions	None
Road Class	Test Track
Traffic Conditions	N/A
Other Effects	None
Vehicle-Class of Cut-In Vehicle	N/A

Table 20. Test Scenario 1-23

Test Comments: There was a clear line-of-sight for the duration of this test. One GPS outage was observed (while passing underneath a bridge), but no packets were lost. Overall, 100 percent of the packets sent during the test were received.

Figure 66. Test Number 1-23 Results

Test Number	**1-23**	**Ambient Weather Conditions:**	**Sunny**
Trace File Name:	**072403_1_23_4.trace***	**Sending Vehicle Model/Make:**	**Buick LeSabre**
Date Collected:	**July 24th, 2003**	**Receiving Vehicle Model/Make:**	**Buick LeSabre**
Files Resident With Whom:	**H. Krishnan**	**Antenna Type Used:**	**Standard**
Operating System Used:	**Linux**	**VSC Obstacle Vehicle #1 Model/Make:**	**N/A**
Software Level Used:	**V2.3 (8-July-03)**	**VSC Obstacle Vehicle #2 Model/Make:**	**N/A**



4.1.21 Test Scenario 1-24

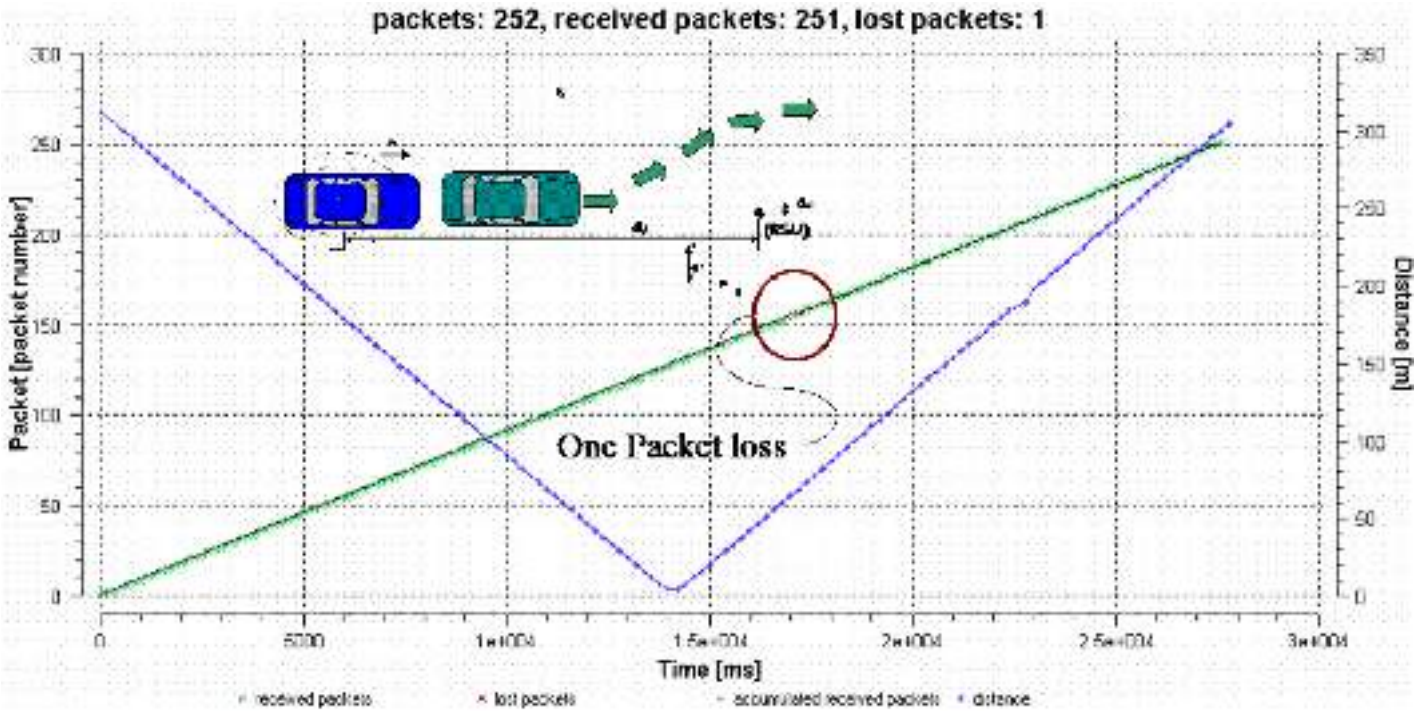
Test Scenario	**1-24**
Relevant Applications	Emergency Electronic Brake Light Pre-Crash Sensing for Co-op Collision Mitigation Co-op Forward Collision Warning (FCW) Lane Change Warning
Velocity of Receiving Antenna (miles/hour)	50
Distance Between Antennas (meters)	< 300
Lateral Offset to Broadcast Antenna (meters)	0
Velocity of Sending Antenna (miles/hour)	0
Angle Between Vehicle 1 & Vehicle 2 (degrees)	N/A
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	200
Path Obstructions	None
Vehicle Obstructions	Cut-out
Road Class	Test Track
Traffic Conditions	N/A
Other Effects	None
Vehicle-Class of Cut-In Vehicle	SUV

Table 21. Test Scenario 1-24

Test Comments: There was a clear line-of-sight for the duration of this test. One packet loss outage was observed (perhaps due to multipath), but no significant communication loss occurred due to the SUV obstruction. Overall, most of the packets sent during the test were received.

Figure 67. Test Number 1-24 Results

Test Number:	1-24	Ambient Weather Conditions:	Sunny
Trace File Name:	091203_1_24_8.trace*	Sending Vehicle Model/Make:	Buick LeSabre
Data Collected:	Sep 12th, 2003	Receiving Vehicle Model/Make:	Buick LeSabre
Files Resident With Whom:	H. Krishnan	Antenna Type Used:	Standard
Operating System Used:	Linux	VSC Obstacle Vehicle #1 Model/Make:	GMC Envoy
Software Level Used:	V2.3 (8-July-03)	VSC Obstacle Vehicle #2 Model/Make:	N/A



4.1.22 Test Scenario 1-25

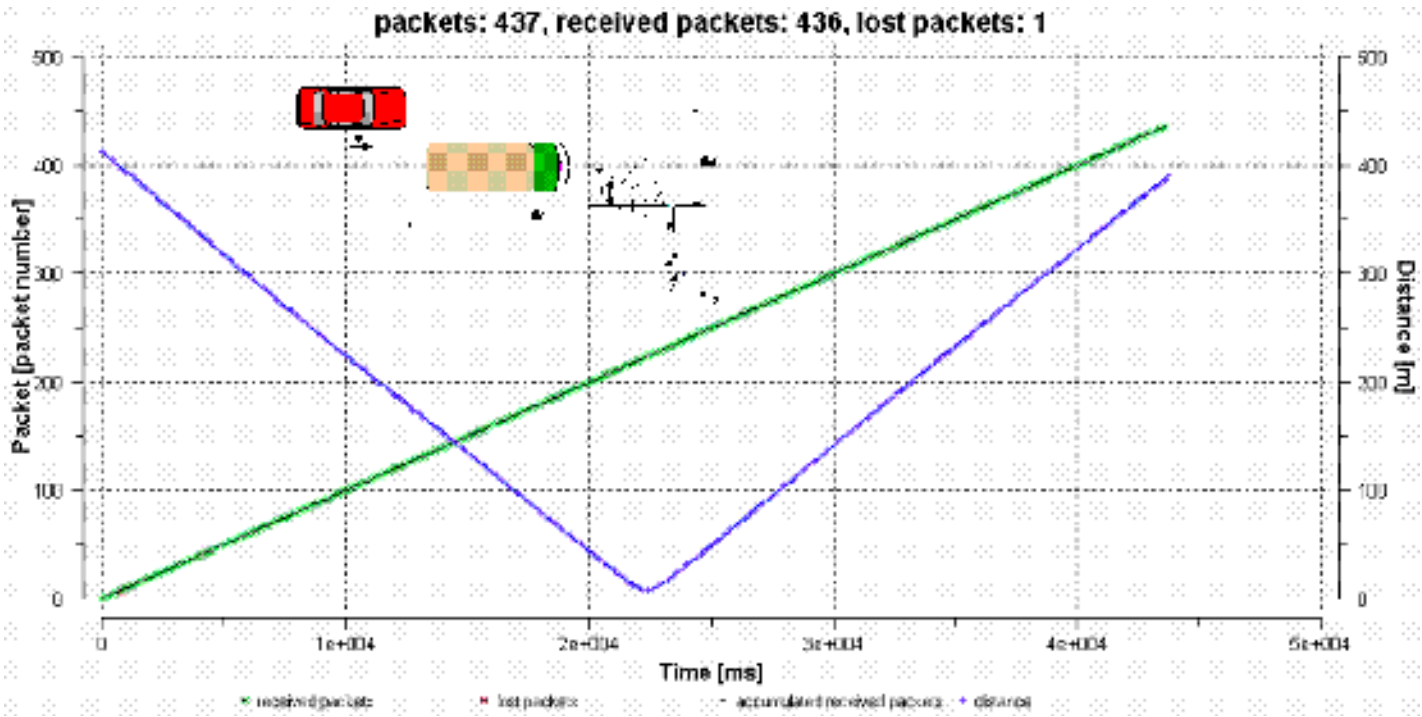
Test Scenario	**1-25**
Relevant Applications	Traffic Signal Violation Warning Curve Speed Warning / Rollover Warning Left-Turn Assistant
Velocity of Receiving Antenna (miles/hour)	40
Distance Between Antennas (meters)	< 300
Lateral Offset to Broadcast Antenna (meters)	8
Velocity of Sending Antenna (miles/hour)	0
Angle Between Vehicle 1 & Vehicle 2 (degrees)	N/A
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	200
Path Obstructions	None
Vehicle Obstructions	Sustained
Road Class	Test Track
Traffic Conditions	N/A
Other Effects	None
Vehicle-Class of Cut-In Vehicle	Truck

Table 22. Test Scenario 1-25

Test Comments: This test was done in MS Windows. The intercepting vehicle was a large truck. There was no significant loss of reception due to the large truck interception. Only one packet was lost in this trial and all trials of this test showed similar performance.

Figure 68. Test Number 1-25 Results

Test Number	**1-25**	**Ambient Weather Conditions:**	**Mostly Sunny**
Trace File Name:	**[illegible]_1_25_1.trace***	**Sending Vehicle Model/Make:**	**Buick LeSabre**
Date Collected:	**June[illegible], 2005**	**Receiving Vehicle Model/Make:**	**Buick LeSabre**
Files Resident With Whom:	**H. Krishnan**	**Antenna Type Used:**	**Standard**
Operating System Used:	**Windows XP**	**VRC Obstacle Vehicle #1 Model/Make:**	**Large Truck**
Software Level Used:	**2.4a beta (27-Feb-05)**	**VRC Obstacle Vehicle #2 Model/Make:**	**N/A**



4.1.23 Test Scenario 1-26

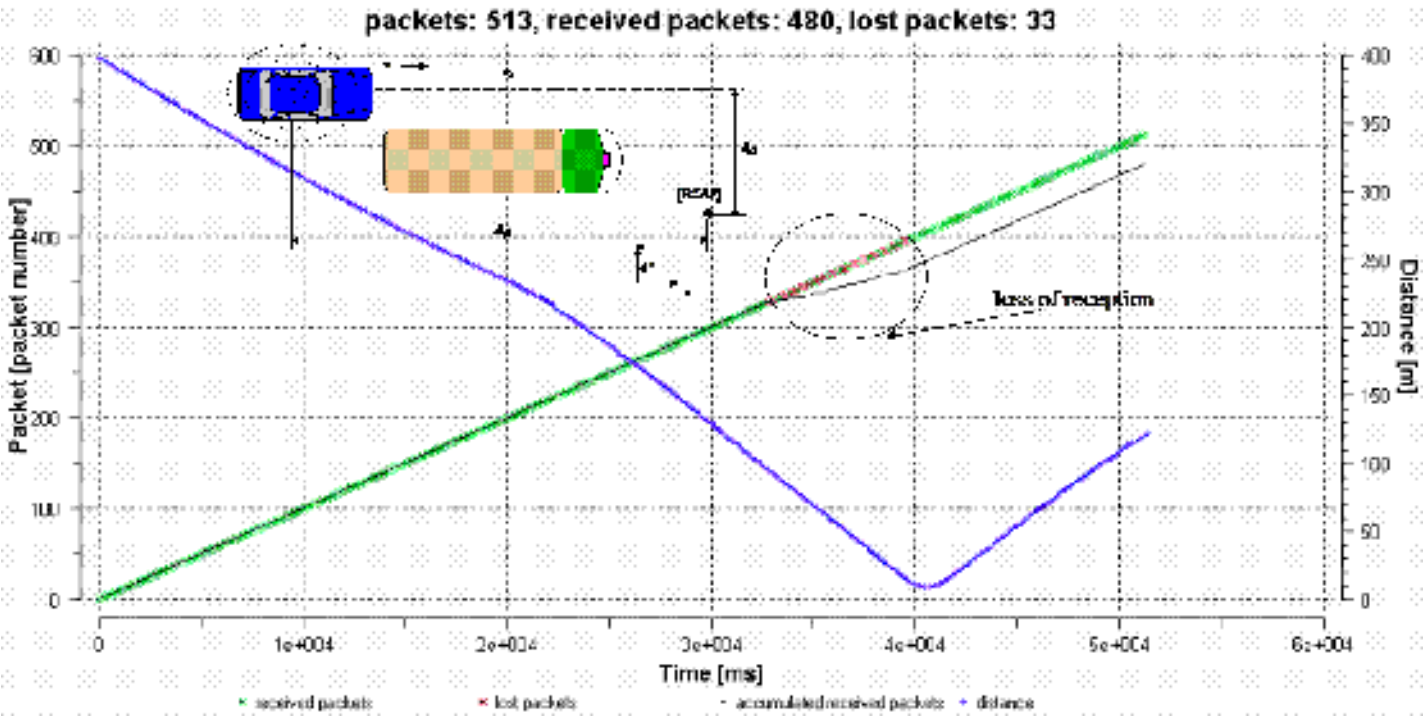
Test Scenario	**1-26**
Relevant Applications	Left-Turn Assistant Stop Sign Movement Assistant
Velocity of Receiving Antenna (miles/hour)	0
Distance Between Antennas (meters)	< 100
Lateral Offset to Broadcast Antenna (meters)	8
Velocity of Sending Antenna (miles/hour)	20
Angle Between Vehicle 1 & Vehicle 2 (degrees)	N/A
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	300
Path Obstructions	None
Vehicle Obstructions	Sustained
Road Class	Test Track
Traffic Conditions	N/A
Other Effects	None
Vehicle-Class of Cut-In Vehicle	Truck

Table 23. Test Scenario 1-26

Test Comments: This test was done in MS Windows. The intercepting vehicle was a large truck. There was significant loss of reception due to the large truck interception when the sender and receiver were obstructed by the truck.

Figure 69. Test Number 1-26 Results

Test Number	1-26	Ambient Weather Conditions:	Mostly Sunny
Trace File Name:	060503_1_26_3.trace*	Sending Vehicle Model/Make:	Buick LeSabre
Date Collected:	June 5th, 2003	Receiving Vehicle Model/Make:	Buick LeSabre
Files Resident With Whom:	H. Krishnan	Antenna Type Used:	Standard
Operating System Used:	Windows XP	VSC Obstacle Vehicle #1 Model/Make:	Large Truck
Software Level Used:	2.4a beta (27-Feb-03)	VSC Obstacle Vehicle #2 Model/Make:	N/A



4.1.24 Test Scenario 1-27

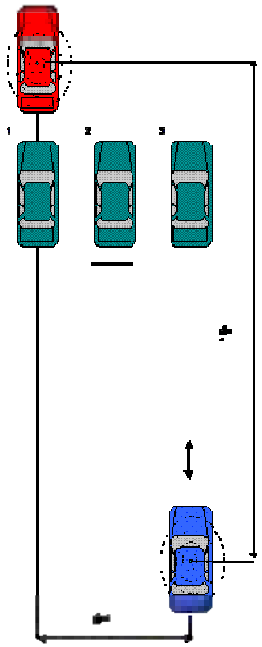
Test Scenario	**1-27**
Relevant Applications	Emergency Electronic Brake Light Pre-Crash Sensing for Co-op Collision Mitigation Co-op Forward Collision Warning (FCW) Lane Change Warning
Velocity of Receiving Antenna (miles/hour)	0
Distance Between Antennas (meters)	< 100
Lateral Offset to Broadcast Antenna (meters)	8
Velocity of Sending Antenna (miles/hour)	<5
Angle Between Vehicle 1 & Vehicle 2 (degrees)	0
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	400
Path Obstructions	None
Vehicle Obstructions	Sustained
Road Class	Test Track
Traffic Conditions	Light
Other Effects	None
Vehicle-Class of Cut-In Vehicle	SUV

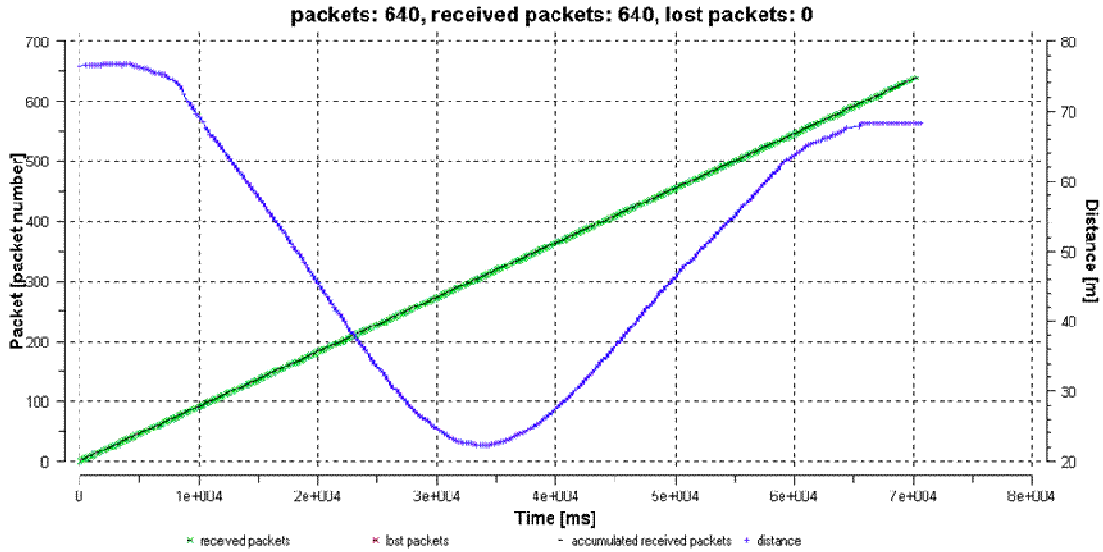
Table 24. Test Scenario 1-27

Test Comments: This test considers the effect of three side-by-side SUVs parked between a stationary receiving vehicle and a slowly moving sender vehicle. Obstacle Vehicle #2 blocked the line-of-sight during the test. Overall, 100 percent of the packets sent during the test were received.

Figure 70. Test Number 1-27-1 Results

Test Number:	1-27-1	Ambient Weather Conditions:	Mostly Sunny
Trace File Name:	082703_2_19_7_SUV.trace*	Sending Vehicle Model/Make:	Toyota Prius
Date Collected:	August 27th, 2003	Receiving Vehicle Model/Make:	Lexus GS300
Files Resident With:	Jim Bauer	Antenna Type Used:	Standard
		Obstacle Vehicle #1 Model/Make:	Toyota Sequoia
Operating System Used:	Linux	Obstacle Vehicle #2 Model/Make:	Toyota Sequoia
Software Level Used:	Version 2.3	Obstacle Vehicle #3 Model/Make:	Toyota Highlander





4.1.25 Test Scenario 1-28

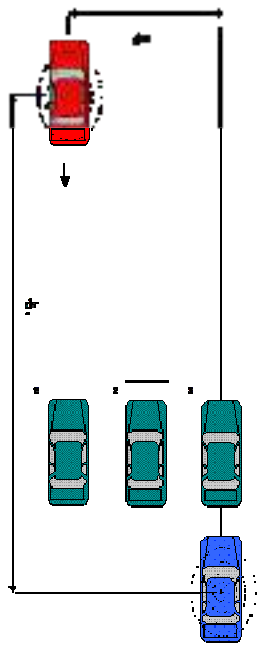
Test Scenario	**1-28**
Relevant Applications	Emergency Electronic Brake Light Pre-Crash Sensing for Co-op Collision Mitigation Co-op Forward Collision Warning (FCW) Lane Change Warning
Velocity of Receiving Antenna (miles/hour)	<5
Distance Between Antennas (meters)	< 100
Lateral Offset to Broadcast Antenna (meters)	8
Velocity of Sending Antenna (miles/hour)	0
Angle Between Vehicle 1 & Vehicle 2 (degrees)	0
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	400
Path Obstructions	None
Vehicle Obstructions	Sustained
Road Class	Test Track
Traffic Conditions	Light
Other Effects	None
Vehicle-Class of Cut-In Vehicle	SUV

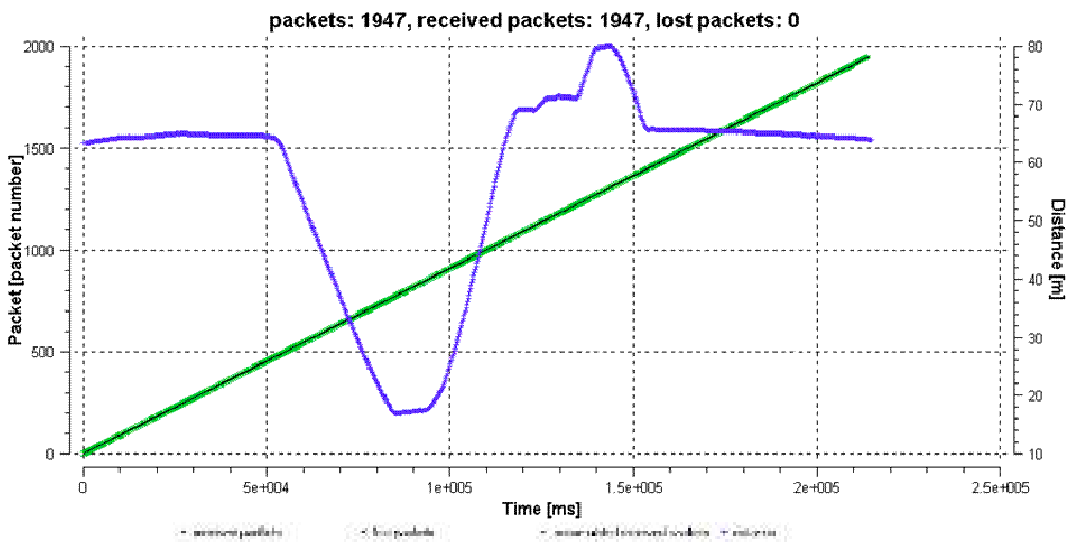
Table 25. Test Scenario 1-28

Test Comments: This test considers the effect of three side-by-side SUVs parked between a stationary sending vehicle and a slowly moving receiver vehicle. Obstacle Vehicle #2 blocked the line-of-sight during the test. Overall, 100 percent of the packets sent during the test were received.

Figure 71. Test Number 1-28-1 Results

Test Number:	1-28-1	Ambient Weather Conditions:	Mostly Sunny
Trace File Name:	082703_2_19_11_SUV.trace*	Sending Vehicle Model/Maker:	Toyota Prius
Date Collected:	August 27th, 2003	Receiving Vehicle Model/Maker:	Lexus GS300
Files Resident With:	Jim Bauer	Antenna Type Used:	Standard
		Obstacle Vehicle #1 Model/Maker:	Toyota Sequoia
Operating System Used:	Linux	Obstacle Vehicle #2 Model/Maker:	Toyota Sequoia
Software Level Used:	Version 2.3	Obstacle Vehicle #3 Model/Maker:	Toyota Highlander





5 Dynamic Vehicle-Vehicle Communication

5.1 Test Scenarios

5.1.1 Test Scenario 2-1

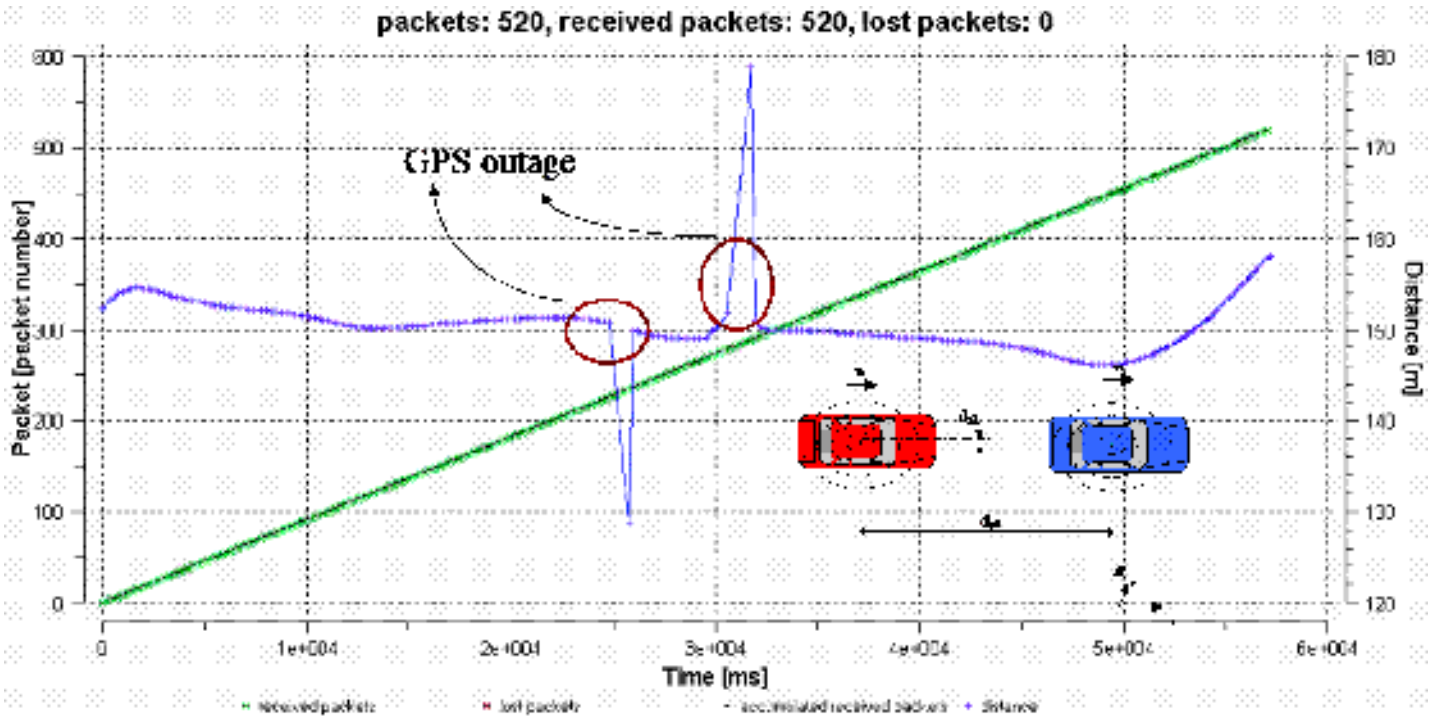
Test Scenario	**2-1**
Relevant Applications	Emergency Electronic Brake Light Pre-Crash Sensing for Co-op Collision Mitigation Co-op Forward Collision Warning (FCW) Lane Change Warning
Velocity of Receiving Antenna (miles/hour)	60
Distance Between Antennas (meters)	< 150
Lateral Offset to Broadcast Antenna (meters)	0
Velocity of Sending Antenna (miles/hour)	60
Angle Between Vehicle 1 & Vehicle 2 (degrees)	0
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	400
Path Obstructions	None
Vehicle Obstructions	None
Road Class	Test Track
Traffic Conditions	N/A
Other Effects	None
Vehicle-Class of Cut-In Vehicle	N/A

Table 26. Test Scenario 2-1

Test Comments: There was a clear line-of-sight for the duration of this test between the sending vehicle and the receiving vehicle. Two GPS outages were observed as the vehicles went under a bridge in the test track. There were no lost packets in all three trials of the test.

Figure 72. Test Number 2-1 Results

Test Number:	**2-1**	**Ambient Weather Conditions:**	**Sunny**
Trace File Name:	**072403_2_1_3.trace***	**Sending Vehicle Model/Make:**	**Buick LeSabre**
Date Collected:	**July 24th, 2003**	**Receiving Vehicle Model/Make:**	**Buick LeSabre**
Files Resident With Whom:	**H. Krishnan**	**Antenna Type Used:**	**Standard**
Operating System Used:	**Linux**	**VSC Chassis Vehicle #1 Model/Make:**	**N/A**
Software Level Used:	**V2.3 (8-July-03)**	**VSC Chassis Vehicle #2 Model/Make:**	**N/A**



5.1.2 Test Scenario 2-2

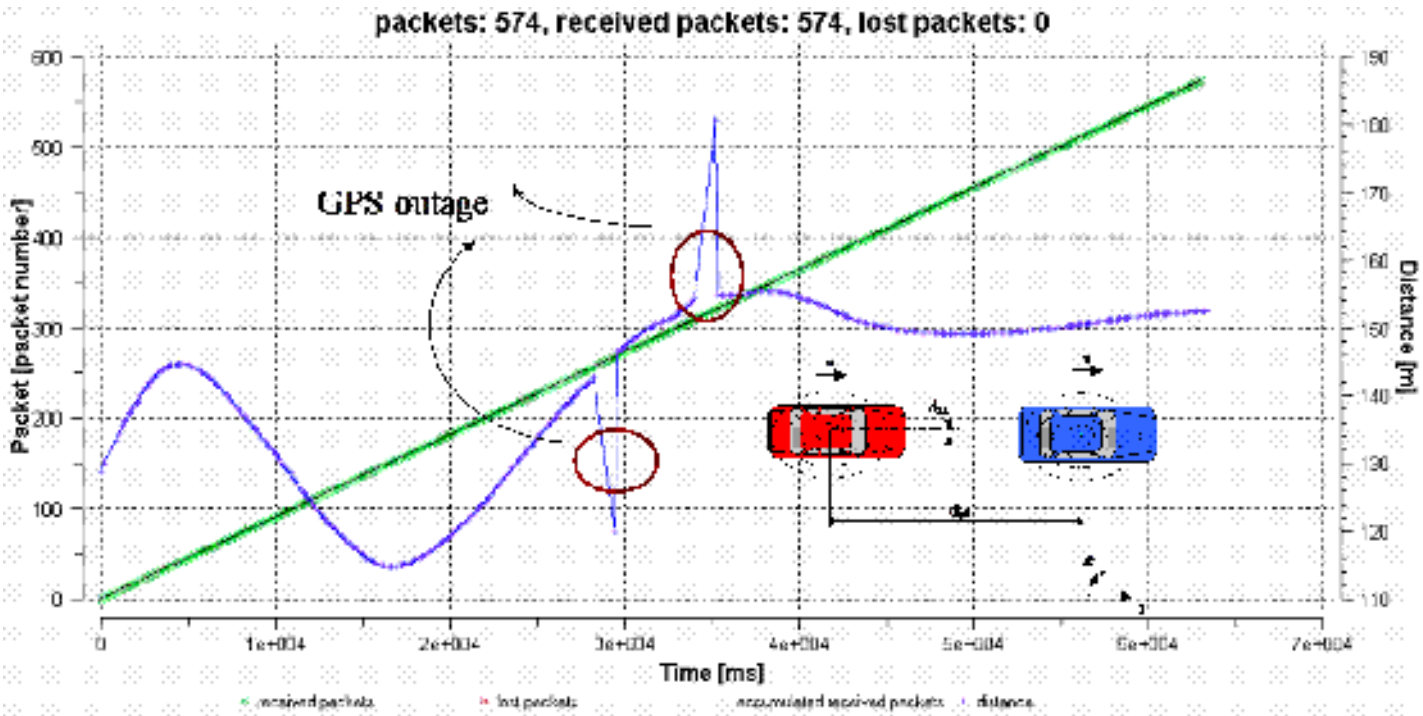
Test Scenario	**2-2**
Relevant Applications	Emergency Electronic Brake Light Pre-Crash Sensing for Co-op Collision Mitigation Co-op Forward Collision Warning (FCW) Lane Change Warning
Velocity of Receiving Antenna (miles/hour)	60
Distance Between Antennas (meters)	< 150
Lateral Offset to Broadcast Antenna (meters)	0
Velocity of Sending Antenna (miles/hour)	60
Angle Between Vehicle 1 & Vehicle 2 (degrees)	0
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	200
Path Obstructions	None
Vehicle Obstructions	None
Road Class	Test Track
Traffic Conditions	N/A
Other Effects	None
Vehicle-Class of Cut-In Vehicle	N/A

Table 27. Test Scenario 2-2

Test Comments: There was a clear line-of-sight for the duration of this test between the sending vehicle and the receiving vehicle. Two GPS outages were observed as the vehicles went under a bridge in the test track. There were no lost packets in all three trials of the test.

Figure 73. Test Number 2-2 Results

Test Number:	**2-2**	**Ambient Weather Condition:**	**Sunny**
Trace File Name:	**[illegible]_2_2_2.trace***	**Sending Vehicle Model/Maker:**	**Buick LeSabre**
Date Collected:	**July 24th, [illegible]**	**Receiving Vehicle Model/Maker:**	**Buick LeSabre**
Files Resident With Whom:	**H. Krishnan**	**Antenna Type Used:**	**Standard**
Operating System Used:	**Linux**	**VBC Obstacle Vehicle #1 Model/Maker:**	**N/A**
Software Level Used:	**V2.3 ([illegible]-July-[illegible])**	**VBC Obstacle Vehicle #2 Model/Maker:**	**N/A**



5.1.3 Test Scenario 2-3

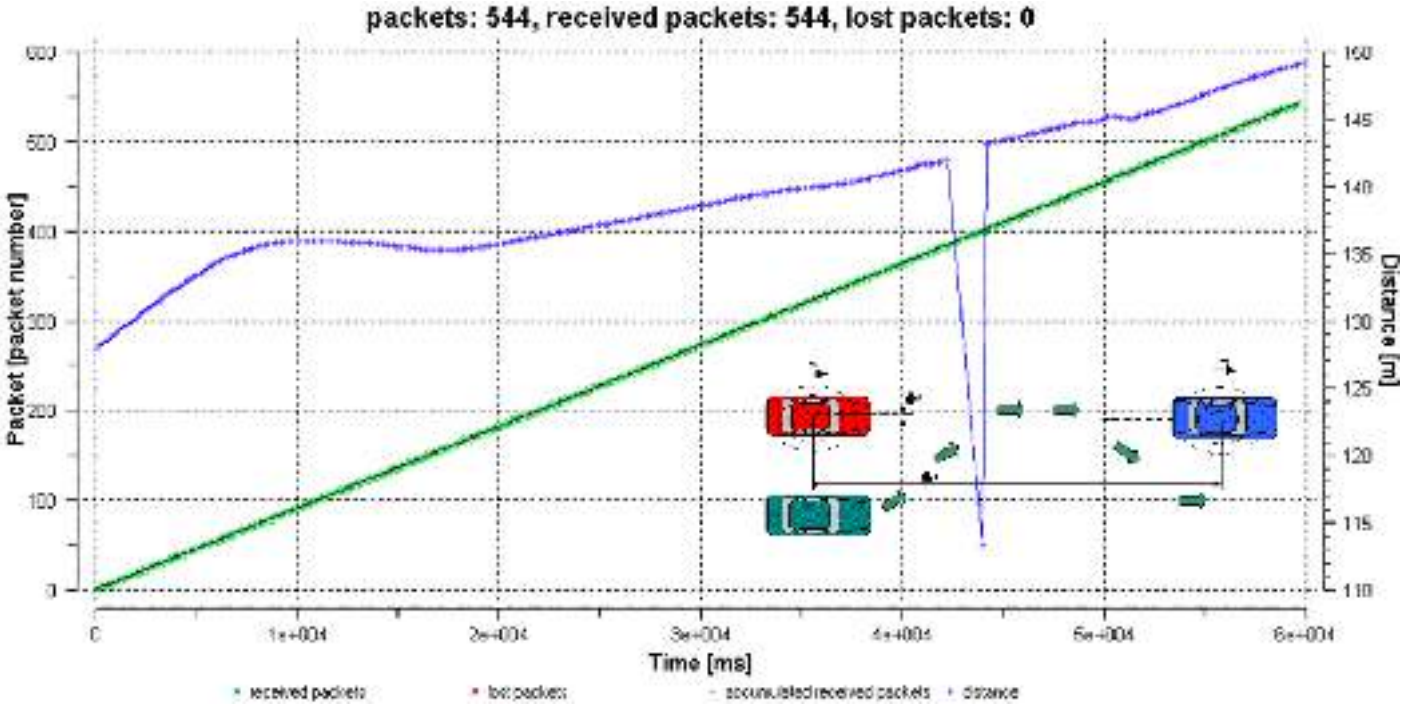
Test Scenario	**2-3**
Relevant Applications	Emergency Electronic Brake Light Pre-Crash Sensing for Co-op Collision Mitigation Co-op Forward Collision Warning (FCW) Lane Change Warning
Velocity of Receiving Antenna (miles/hour)	40
Distance Between Antennas (meters)	< 150
Lateral Offset to Broadcast Antenna (meters)	0
Velocity of Sending Antenna (miles/hour)	40
Angle Between Vehicle 1 & Vehicle 2 (degrees)	0
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	200
Path Obstructions	None
Vehicle Obstructions	Cut-in
Road Class	Test Track
Traffic Conditions	N/A
Other Effects	None
Vehicle-Class of Cut-In Vehicle	SUV

Table 28. Test Scenario 2-3

Test Comments: There was a clear line-of-sight for the duration of this test. One GPS outage was observed in the same location for all three trials (while passing underneath a bridge), but no packets were lost. Overall, 100 percent of the packets sent during the test were received.

Figure 74. Test Number 2-3 Results

Test Number:	**2-3**	**Ambient Weather Conditions:**	**Cloudy**
Trace File Name:	**091803_2_3_4.trace***	**Sending Vehicle Model/Make:**	**Buick LeSabre**
Date Collected:	**September 18th, 2003**	**Receiving Vehicle Model/Make:**	**Buick LeSabre**
Files Resident With Whom:	**S. Tengler**	**Antenna Type Used:**	**Standard**
Operating System Used:	**Linux**	**VRC Obstacle Vehicle #1 Model/Make:**	**GMC Envoy**
Software Level Used:	**V2.3 (8-July-03)**	**VRC Obstacle Vehicle #2 Model/Make:**	**N/A**



5.1.4 Test Scenario 2-4

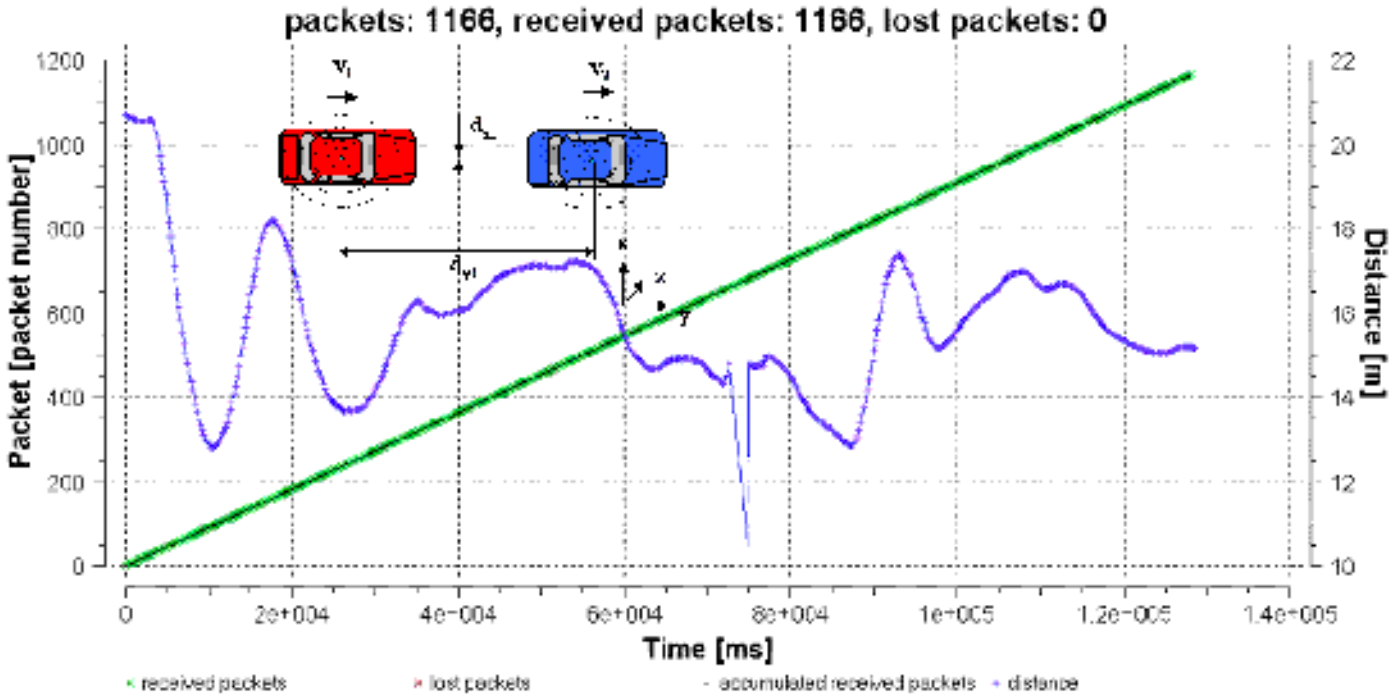
Test Scenario	**2-4**
Relevant Applications	Emergency Electronic Brake Light Pre-Crash Sensing for Co-op Collision Mitigation Co-op Forward Collision Warning (FCW) Lane Change Warning
Velocity of Receiving Antenna (miles/hour)	25
Distance Between Antennas (meters)	< 15
Lateral Offset to Broadcast Antenna (meters)	0
Velocity of Sending Antenna (miles/hour)	25
Angle Between Vehicle 1 & Vehicle 2 (degrees)	0
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	400
Path Obstructions	None
Vehicle Obstructions	None
Road Class	Residential
Traffic Conditions	Light
Other Effects	None
Vehicle-Class of Cut-In Vehicle	None

Table 29. Test Scenario 2-4

Test Comments: In this test, the RSU (GMC Envoy) sends messages (400 bytes) every 100 msec. Both vehicles are traveling at ~25 mph, unobstructed and < 20 m apart. Both units are constantly in a clear line-of-sight. The communication link was very reliable since in all trials of this test, no packets were dropped.

Figure 75. Test Number 2-4 Results

Test Number	2-4	Ambient Weather Conditions:	Sunny
Trace File Name:	081403_2_4_1.trace*	Sending Vehicle Model/Make:	GMC Envoy
Date Collected:	August 14, 2003	Receiving Vehicle Model/Make:	Buick LeSabre
Files Resident With Whom:	F. Ahmed-Zaid	Antenna Type Used:	Standard
Operating System Used:	Linux	VSC Obstacle Vehicle #1 Model/Make:	N/A
Software Level Used:	V2.3 (8-July-03)	VSC Obstacle Vehicle #2 Model/Make:	N/A



5.1.5 Test Scenario 2-5

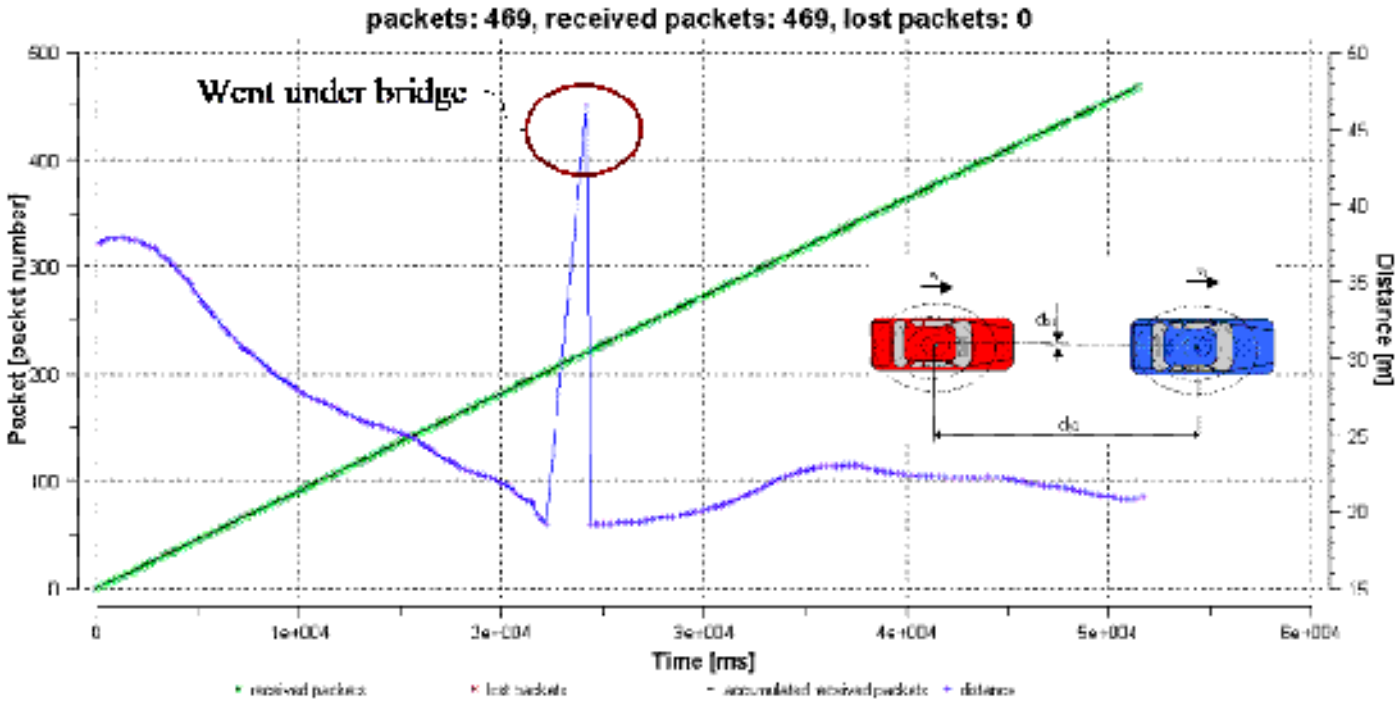
Test Scenario	**2-5**
Relevant Applications	Emergency Electronic Brake Light Pre-Crash Sensing for Co-op Collision Mitigation Co-op Forward Collision Warning (FCW) Lane Change Warning
Velocity of Receiving Antenna (miles/hour)	60
Distance Between Antennas (meters)	< 20
Lateral Offset to Broadcast Antenna (meters)	0
Velocity of Sending Antenna (miles/hour)	60
Angle Between Vehicle 1 & Vehicle 2 (degrees)	0
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	400
Path Obstructions	None
Vehicle Obstructions	None
Road Class	Test Track
Traffic Conditions	Light
Other Effects	None
Vehicle-Class of Cut-In Vehicle	None

Table 30. Test Scenario 2-5

Test Comments: There was a clear line-of-sight for the duration of this test. One GPS outage was observed in the same location for all three trials (while passing underneath a bridge), but no packets were lost. Overall, 100 percent of the packets sent during the test were received with both MS Windows and Linux.

Figure 76. Test Number 2-5 Results

Test Number	**2-5**	**Ambient Weather Conditions:**	**Sunny**
Trace File Name:	**071703_2_5_1.trace***	**Sending Vehicle Model/Maker:**	**GMC Envoy**
Date Collected:	**July 17th, 2003**	**Receiving Vehicle Model/Maker:**	**Buick LeSabre**
Files Resident With Whom:	**H. Krishnan**	**Antenna Type Used:**	**Standard**
Operating System Used:	**Linux**	**VBC Obstacle Vehicle #1 Model/Maker:**	**N/A**
Software Level Used:	**V2.3 (8-July-03)**	**VBC Obstacle Vehicle #2 Model/Maker:**	**N/A**



5.1.6 Test Scenario 2-6

Test Scenario	**2-6**
Relevant Applications	Emergency Electronic Brake Light Pre-Crash Sensing for Co-op Collision Mitigation Co-op Forward Collision Warning (FCW) Lane Change Warning
Velocity of Receiving Antenna (miles/hour)	60
Distance Between Antennas (meters)	< 100
Lateral Offset to Broadcast Antenna (meters)	0
Velocity of Sending Antenna (miles/hour)	60
Angle Between Vehicle 1 & Vehicle 2 (degrees)	0
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	400
Path Obstructions	None
Vehicle Obstructions	None
Road Class	Highway
Traffic Conditions	Light
Other Effects	None
Vehicle-Class of Cut-In Vehicle	None

Table 31. Test Scenario 2-6

Test Comments: Basic communication at ~100 m is working pretty well with less than 3 percent packet loss. The packet loss is most likely due to a truck moving in between the two cars and cutting the line-of-sight.

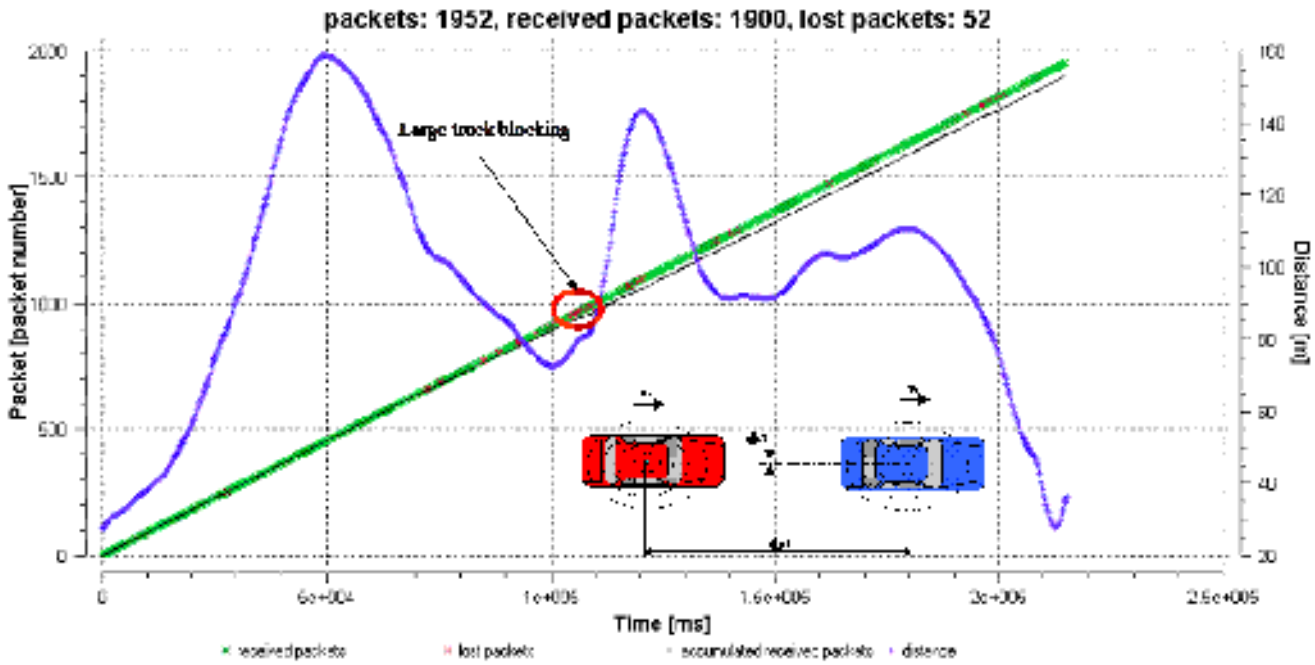
Figure 77. Test Number 2-6 Results

Test Number 2-6
Trace File Name: test2-6-1_070203.trace*
Date Collected: July 2nd, 2003
Files Resident With Whom: Chu-Hee Lee

Ambient Weather Conditions: Sunny
Sending Vehicle Model/Make: sedan
Receiving Vehicle Model/Make: sedan
Antenna Type Used: Standard

Operating System Used: Linux
Software Level Used: 2.1

VSC Obstacle Vehicle #1 Model/Make: N/A
VSC Obstacle Vehicle #2 Model/Make: N/A



5.1.7 Test Scenario 2-8

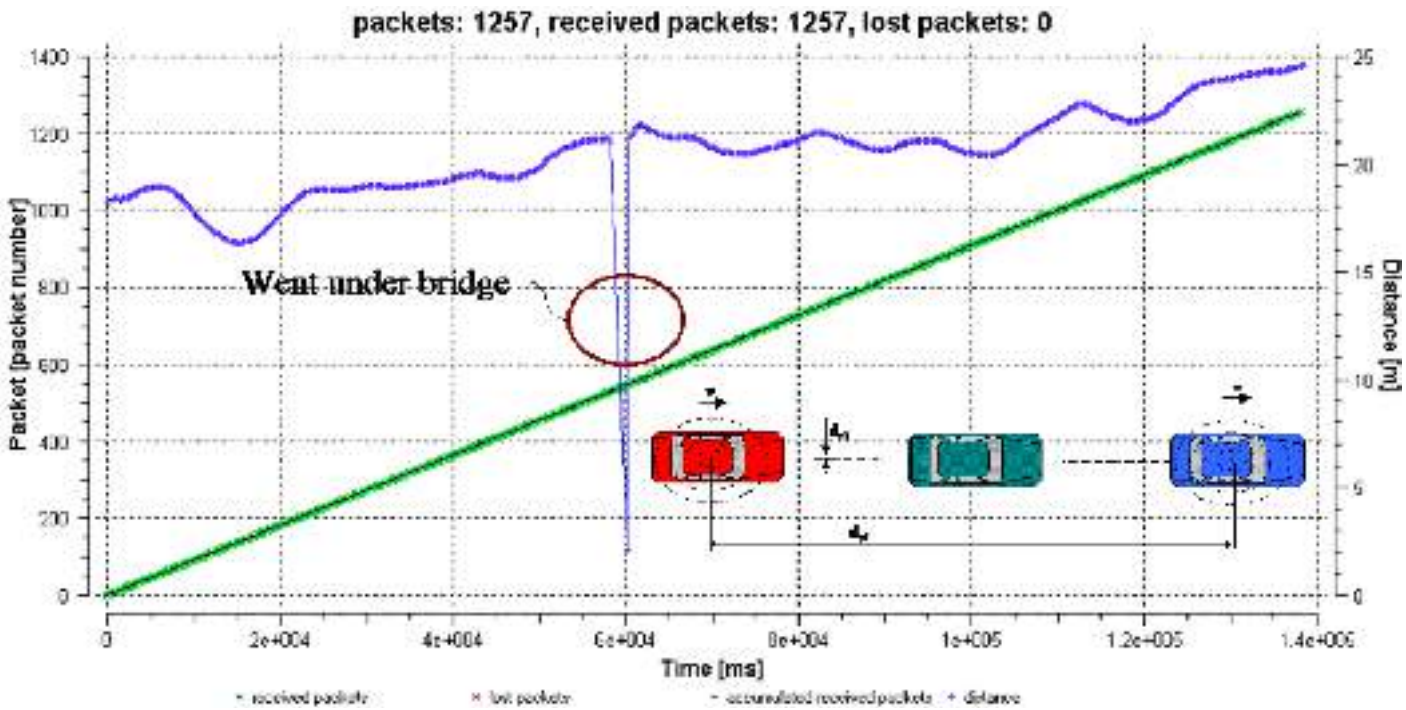
Test Scenario	**2-8**
Relevant Applications	Emergency Electronic Brake Light Pre-Crash Sensing for Co-op Collision Mitigation Co-op Forward Collision Warning (FCW) Lane Change Warning
Velocity of Receiving Antenna (miles/hour)	25
Distance Between Antennas (meters)	< 20
Lateral Offset to Broadcast Antenna (meters)	0
Velocity of Sending Antenna (miles/hour)	25
Angle Between Vehicle 1 & Vehicle 2 (degrees)	0
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	400
Path Obstructions	None
Vehicle Obstructions	Sustained
Road Class	Test Track
Traffic Conditions	Light
Other Effects	None
Vehicle-Class of Cut-In Vehicle	SUV

Table 32. Test Scenario 2-8

Test Comments: There was a clear line-of-sight for the duration of this test. One GPS outage was observed in the same location for all four trials (while passing underneath a bridge), but no packets were lost. Overall, 100 percent of the packets sent during the test were received.

Figure 78. Test Number 2-8 Results

Test Number	**2-8**	**Ambient Weather Conditions:**	**Cloudy**
Trace File Name:	**091203_2_8_1.trace***	**Sending Vehicle Model/Make:**	**Buick LeSabre**
Date Collected:	**September 15th, 2003**	**Receiving Vehicle Model/Make:**	**Buick LeSabre**
Files Resident With Whom:	**S. Tengler**	**Antenna Type Used:**	**Standard**
Operating System Used:	**Linux**	**VSC Obstacle Vehicle #1 Model/Make:**	**GMC Envoy**
Software Level Used:	**V2.3 (8-July-03)**	**VSC Obstacle Vehicle #2 Model/Make:**	**N/A**



5.1.8 Test Scenario 2-9

Test Scenario	**2-9**
Relevant Applications	Emergency Electronic Brake Light Pre-Crash Sensing for Co-op Collision Mitigation Co-op Forward Collision Warning (FCW) Lane Change Warning
Velocity of Receiving Antenna (miles/hour)	25
Distance Between Antennas (meters)	< 50
Lateral Offset to Broadcast Antenna (meters)	0
Velocity of Sending Antenna (miles/hour)	25
Angle Between Vehicle 1 & Vehicle 2 (degrees)	0
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	400
Path Obstructions	None
Vehicle Obstructions	Sustained
Road Class	Test Track
Traffic Conditions	Light
Other Effects	None
Vehicle-Class of Cut-In Vehicle	SUV

Table 33. Test Scenario 2-9

Test Comments: There was a clear line-of-sight for the duration of this test. One GPS outage was observed in the same location for all four trials (while passing underneath a bridge), but no packets were lost. Overall, 100 percent of the packets sent during the test were received.

Figure 79. Test Number 2-9 Results

Test Number	**2-9**	Ambient Weather Conditions:	**Cloudy**
Trace File Name:	**091803_2_9_1.trace***	Sending Vehicle Model/Make:	**Buick LaSabre**
Date Collected:	**September 18th, 2003**	Receiving Vehicle Model/Make:	**Buick LaSabre**
Files Resident With Whom:	**S. Tengler**	Antenna Type Used:	**Standard**
Operating System Used:	**Linux**	VSC Obstacle Vehicle #1 Model/Make:	**GMC Envoy**
Software Level Used:	**V2.3 (8-July-03)**	VSC Obstacle Vehicle #2 Model/Make:	**N/A**

(NO GRAPH AVAILABLE due to suspected corruption of the GPS files from the test)

5.1.9 Test Scenario 2-10

Test Scenario	**2-10**
Relevant Applications	Emergency Electronic Brake Light Pre-Crash Sensing for Co-op Collision Mitigation Co-op Forward Collision Warning (FCW) Lane Change Warning
Velocity of Receiving Antenna (miles/hour)	25
Distance Between Antennas (meters)	< 50
Lateral Offset to Broadcast Antenna (meters)	0
Velocity of Sending Antenna (miles/hour)	25
Angle Between Vehicle 1 & Vehicle 2 (degrees)	0
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	400
Path Obstructions	None
Vehicle Obstructions	Sustained
Road Class	Highway
Traffic Conditions	Light
Other Effects	None
Vehicle-Class of Cut-In Vehicle	SUV

Table 34.Test Scenario 2-10

Test Comments: Some periods of packet loss, but no continuous outages. Losses seemed to vary due to road curvature and the resulting position of the blocking vehicle relative to the test vehicles.

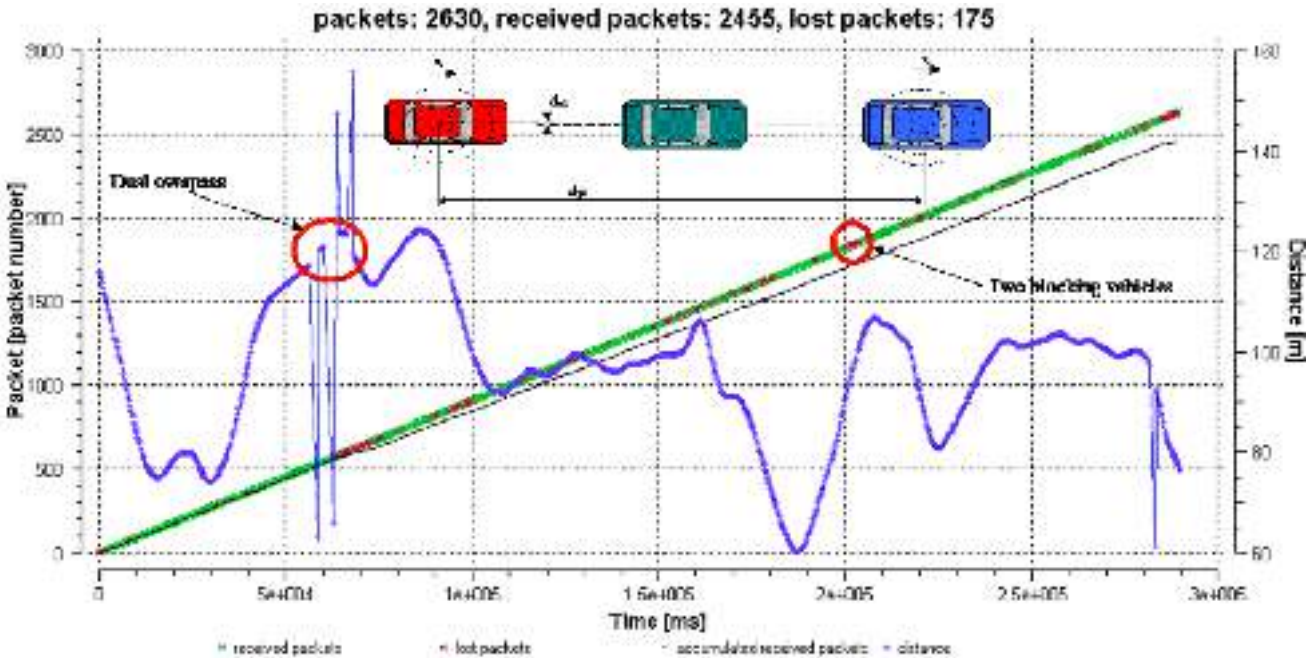
Figure 80. Test Number 2-10 Results

Test Number 2-10
Trace File Name: test2-10_1_073005.trace*
Date Collected: July 30th, 2005
Files Resident With Whom: Chu-Hao Lee

Ambient Weather Conditions: Sunny
Sending Vehicle Model/Make: VW Passat
Receiving Vehicle Model/Make: BMW Series 3
Antenna Type Used: Standard

Operating System Used: Linux
Software Level Used: 2.3

VSC Obstacle Vehicle #1 Model/Make: BMW X5
VSC Obstacle Vehicle #2 Model/Make: N/A



5.1.10 Test Scenario 2-11

Test Scenario	**2-11**
Relevant Applications	Emergency Electronic Brake Light Pre-Crash Sensing for Co-op Collision Mitigation Co-op Forward Collision Warning (FCW) Lane Change Warning
Velocity of Receiving Antenna (miles/hour)	60
Distance Between Antennas (meters)	< 100
Lateral Offset to Broadcast Antenna (meters)	0
Velocity of Sending Antenna (miles/hour)	60
Angle Between Vehicle 1 & Vehicle 2 (degrees)	0
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	400
Path Obstructions	None
Vehicle Obstructions	Sustained
Road Class	Highway
Traffic Conditions	Light
Other Effects	None
Vehicle-Class of Cut-In Vehicle	SUV

Table 35. Test Scenario 2-11

Test Comments: Two blocking SUVs caused significant, though not complete, packet loss, due primarily to relative positions and not overall separation distance. In fact, packet success seemed better at longer distances, possibly due to reduced field of view blockage compared to that of a tighter packed formation.

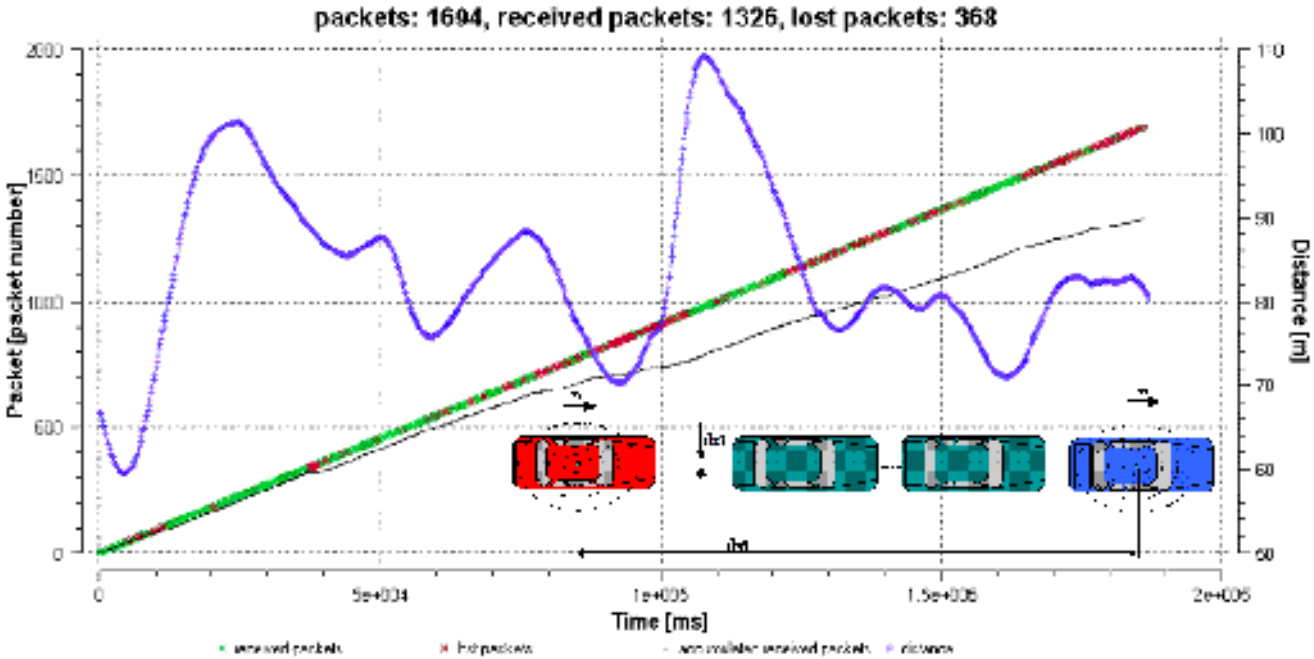
Figure 81. Test Number 2-11 Results

Test Number 2-11
Trace File Name: test2-11_3_[illegible].trace*
Date Collected: August 6th, 2003
Files Resident With Whom: Chu-Hao Lee

Ambient Weather Conditions: Sunny
Sending Vehicle Model/Make: BMW Series 3
Receiving Vehicle Model/Make: VW Passat
Antenna Type Used: Standard

Operating System Used: Linux
Software Level Used: 2.3

VSC Obstacle Vehicle #1 Model/Make: BMW X5
VSC Obstacle Vehicle #2 Model/Make: Mercedes M-class



5.1.11 Test Scenario 2-12

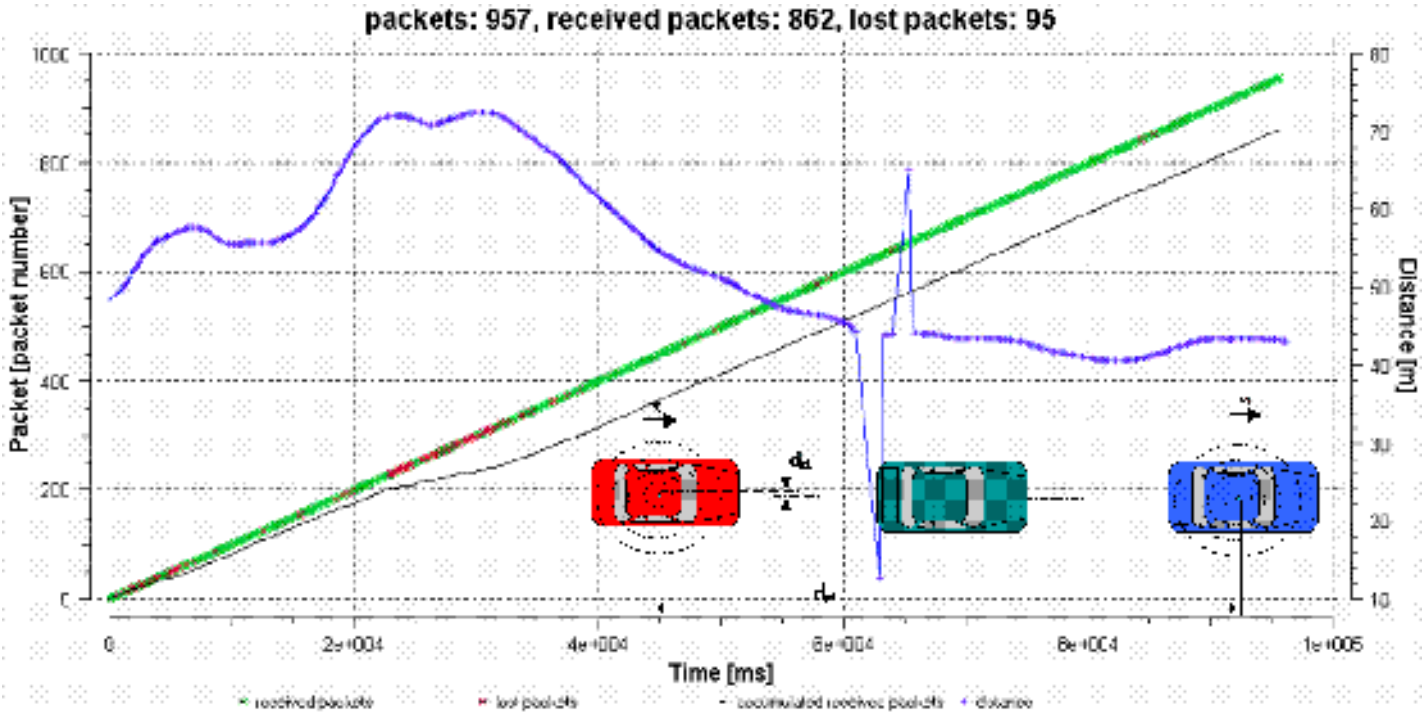
Test Scenario	**2-12**
Relevant Applications	Emergency Electronic Brake Light Pre-Crash Sensing for Co-op Collision Mitigation Co-op Forward Collision Warning (FCW) Lane Change Warning
Velocity of Receiving Antenna (miles/hour)	40
Distance Between Antennas (meters)	< 70
Lateral Offset to Broadcast Antenna (meters)	0
Velocity of Sending Antenna (miles/hour)	40
Angle Between Vehicle 1 & Vehicle 2 (degrees)	0
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	400
Path Obstructions	None
Vehicle Obstructions	Sustained
Road Class	Test Track
Traffic Conditions	Light
Other Effects	None
Vehicle-Class of Cut-In Vehicle	Truck

Table 36. Test Scenario 2-12

Test Comments: This test was done in MS Windows. The intercepting vehicle was a large truck. There were significant losses of reception due to the large truck interception and all trials of this test showed similar performance.

Figure 82. Test Number 2-12 Results

Test Number	**2-12**	**Ambient Weather Conditions:**	**Mostly Sunny**
Trace File Name:	**[illegible]_2_12_2.trace***	**Sending Vehicle Model/Make:**	**Buick LeSabre**
Date Collected:	**June 5th, 2003**	**Receiving Vehicle Model/Make:**	**Buick LeSabre**
Files Resident With Whom:	**H. Krishnan**	**Antenna Type Used:**	**Standard**
Operating System Used:	**Windows XP**	**VBC Obstacle Vehicle #1 Model/Make:**	**Large Truck**
Software Level Used:	**2.4a beta (27-Feb-03)**	**VBC Obstacle Vehicle #2 Model/Make:**	**N/A**



5.1.12 Test Scenario 2-13

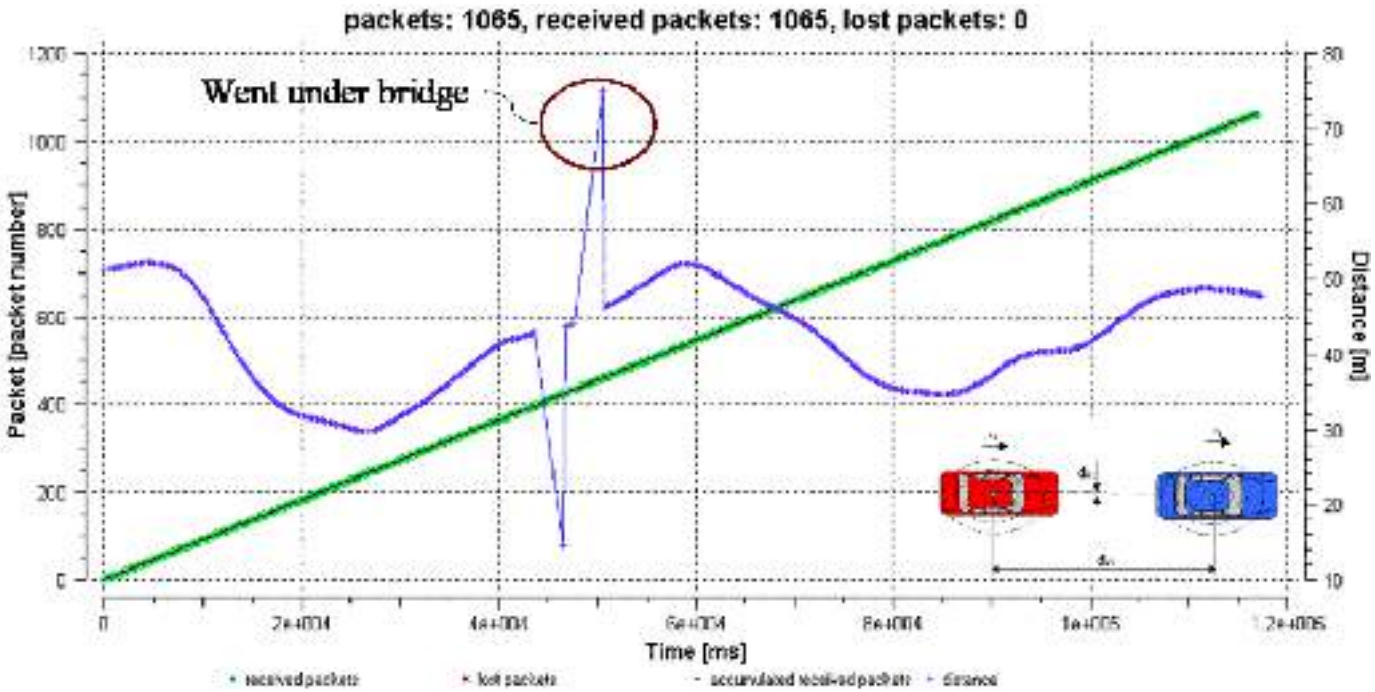
Test Scenario	**2-13**
Relevant Applications	Emergency Electronic Brake Light Pre-Crash Sensing for Co-op Collision Mitigation Co-op Forward Collision Warning (FCW) Lane Change Warning
Velocity of Receiving Antenna (miles/hour)	25
Distance Between Antennas (meters)	< 50
Lateral Offset to Broadcast Antenna (meters)	8
Velocity of Sending Antenna (miles/hour)	25
Angle Between Vehicle 1 & Vehicle 2 (degrees)	0
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	400
Path Obstructions	None
Vehicle Obstructions	None
Road Class	Test Track
Traffic Conditions	Light
Other Effects	None
Vehicle-Class of Cut-In Vehicle	None

Table 37. Test Scenario 2-13

Test Comments: There was a clear line-of-sight for the duration of this test. One GPS outage was observed in the same location for all three trials (while passing underneath a bridge), but no packets were lost. Overall, 100 percent of the packets sent during the test were received.

Figure 83. Test Number 2-13 Results

Test Number	**2-13**	**Ambient Weather Conditions:**	**Sunny**
Trace File Name:	**072403_2_13_1.trace***	**Sending Vehicle Model/Make:**	**Buick LeSabre**
Date Collected:	**July 17th, 2003**	**Receiving Vehicle Model/Make:**	**Buick LeSabre**
Files Resident With Whom:	**S. Tengler**	**Antenna Type Used:**	**Standard**
Operating System Used:	**Linux**	**VRC Obstacle Vehicle #1 Model/Make:**	**N/A**
Software Level Used:	**V2.3 (8-July-03)**	**VRC Obstacle Vehicle #2 Model/Make:**	**N/A**



5.1.13 Test Scenario 2-14

Test Scenario	**2-14**
Relevant Applications	Emergency Electronic Brake Light Pre-Crash Sensing for Co-op Collision Mitigation Co-op Forward Collision Warning (FCW) Lane Change Warning
Velocity of Receiving Antenna (miles/hour)	60
Distance Between Antennas (meters)	< 100
Lateral Offset to Broadcast Antenna (meters)	8
Velocity of Sending Antenna (miles/hour)	60
Angle Between Vehicle 1 & Vehicle 2 (degrees)	0
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	400
Path Obstructions	None
Vehicle Obstructions	None
Road Class	Highway
Traffic Conditions	Light
Other Effects	None
Vehicle-Class of Cut-In Vehicle	None

Table 38. Test Scenario 2-14

Test Comments: Brief GPS outage due to overpass. Noticeable, but not complete, packet loss due to loss of line-of-sight between test vehicles while on opposite sides of hill crest.

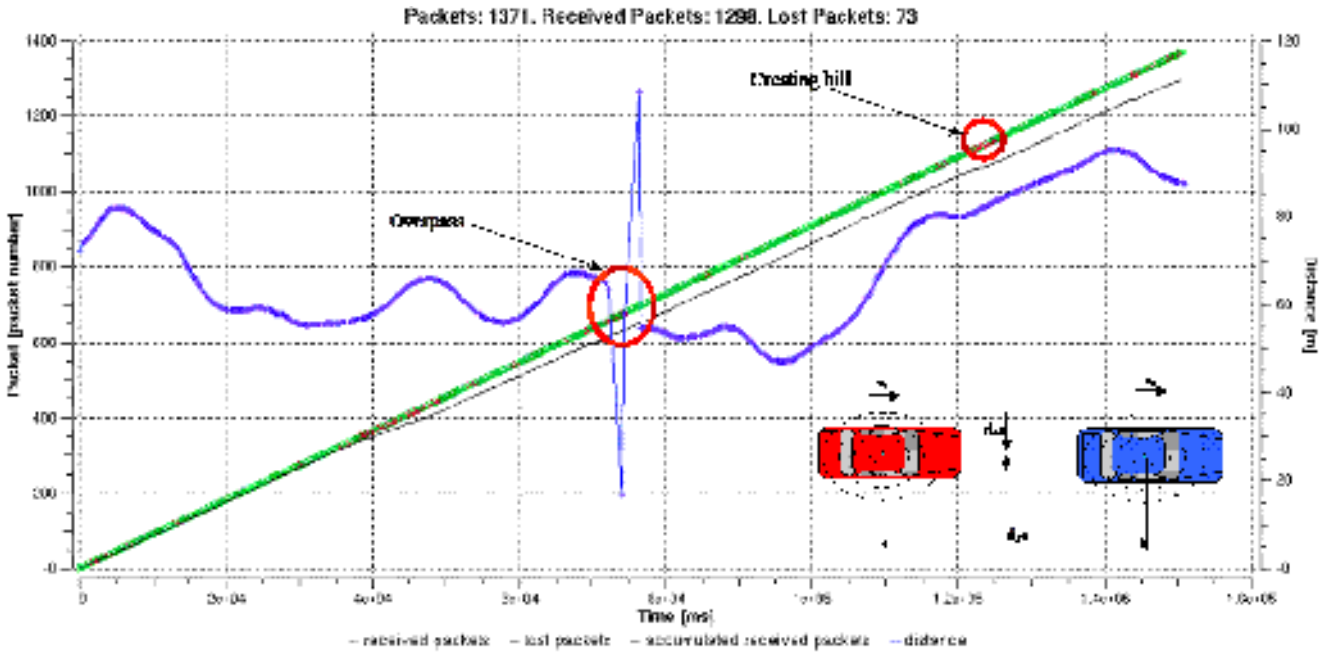
Figure 84. Test Number 2-14 Results

Test Number 2-14
Trace File Name: test2-14_3_072303.trace*
Date Collected: July 23rd, 2003
Files Resident With Whom: Chu-Hao Lee

Ambient Weather Conditions: Sunny
Sending Vehicle Model/Make: VW Passat
Receiving Vehicle Model/Make: BMW Series 3
Antenna Type Used: Standard

Operating System Used: Linux
Software Level Used: 2.3

VSC Obstacle Vehicle #1 Model/Make: N/A
VSC Obstacle Vehicle #2 Model/Make: N/A



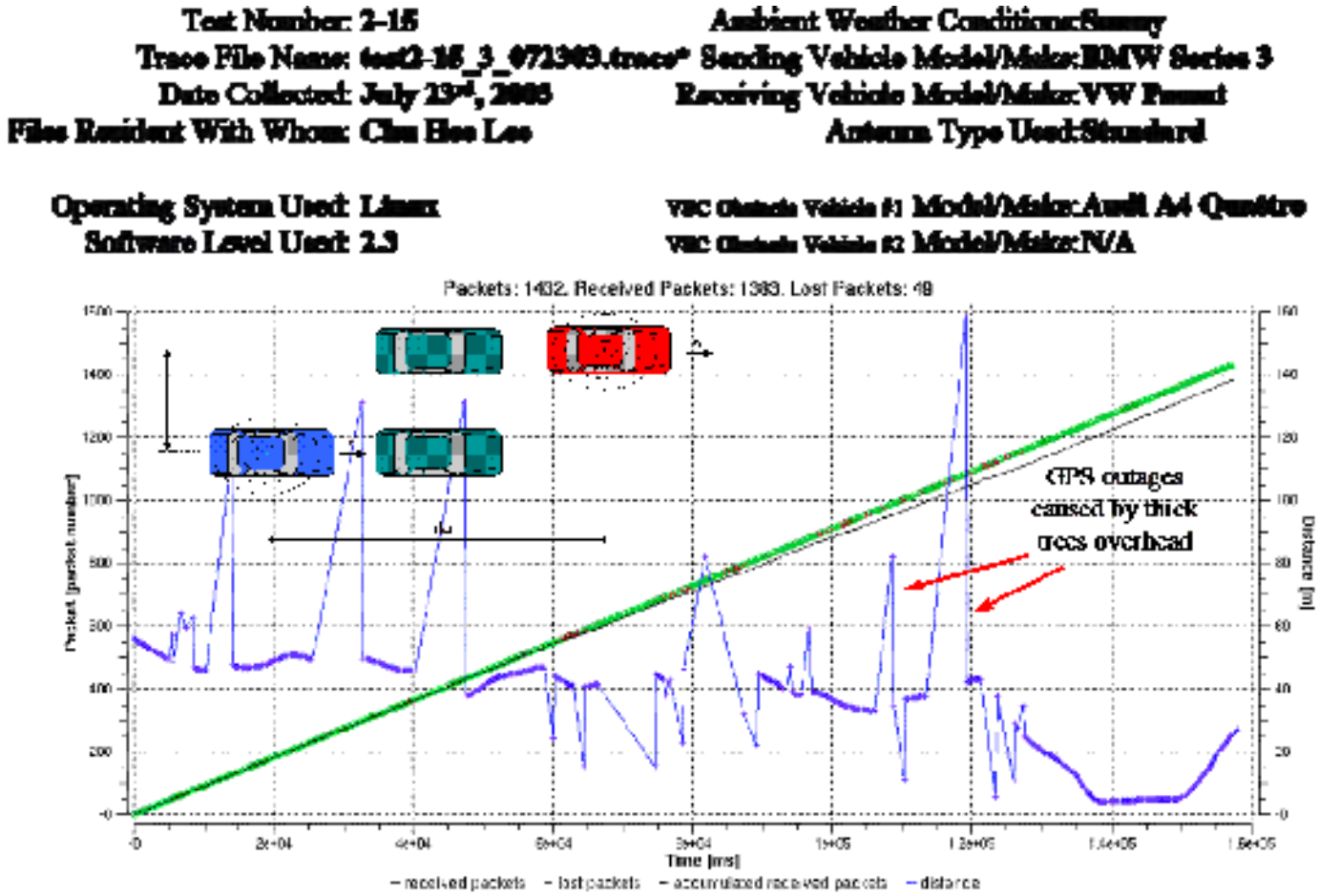
5.1.14 Test Scenario 2-15

Test Scenario	**2-15**
Relevant Applications	Emergency Electronic Brake Light Pre-Crash Sensing for Co-op Collision Mitigation Co-op Forward Collision Warning (FCW) Lane Change Warning
Velocity of Receiving Antenna (miles/hour)	40
Distance Between Antennas (meters)	< 20
Lateral Offset to Broadcast Antenna (meters)	4
Velocity of Sending Antenna (miles/hour)	40
Angle Between Vehicle 1 & Vehicle 2 (degrees)	0
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	400
Path Obstructions	None
Vehicle Obstructions	Sustained
Road Class	Arterial
Traffic Conditions	Light
Other Effects	None
Vehicle-Class of Cut-In Vehicle	Sedan

Table 39. Test Scenario 2-15

Test Comments: GPS outages likely due to many thick overhanging trees. Also went under an underpass at one point in the first third of the run. The few vehicle-to-vehicle outages that were observed were due to the blocking vehicle.

Figure 85. Test Number 2-15 Results



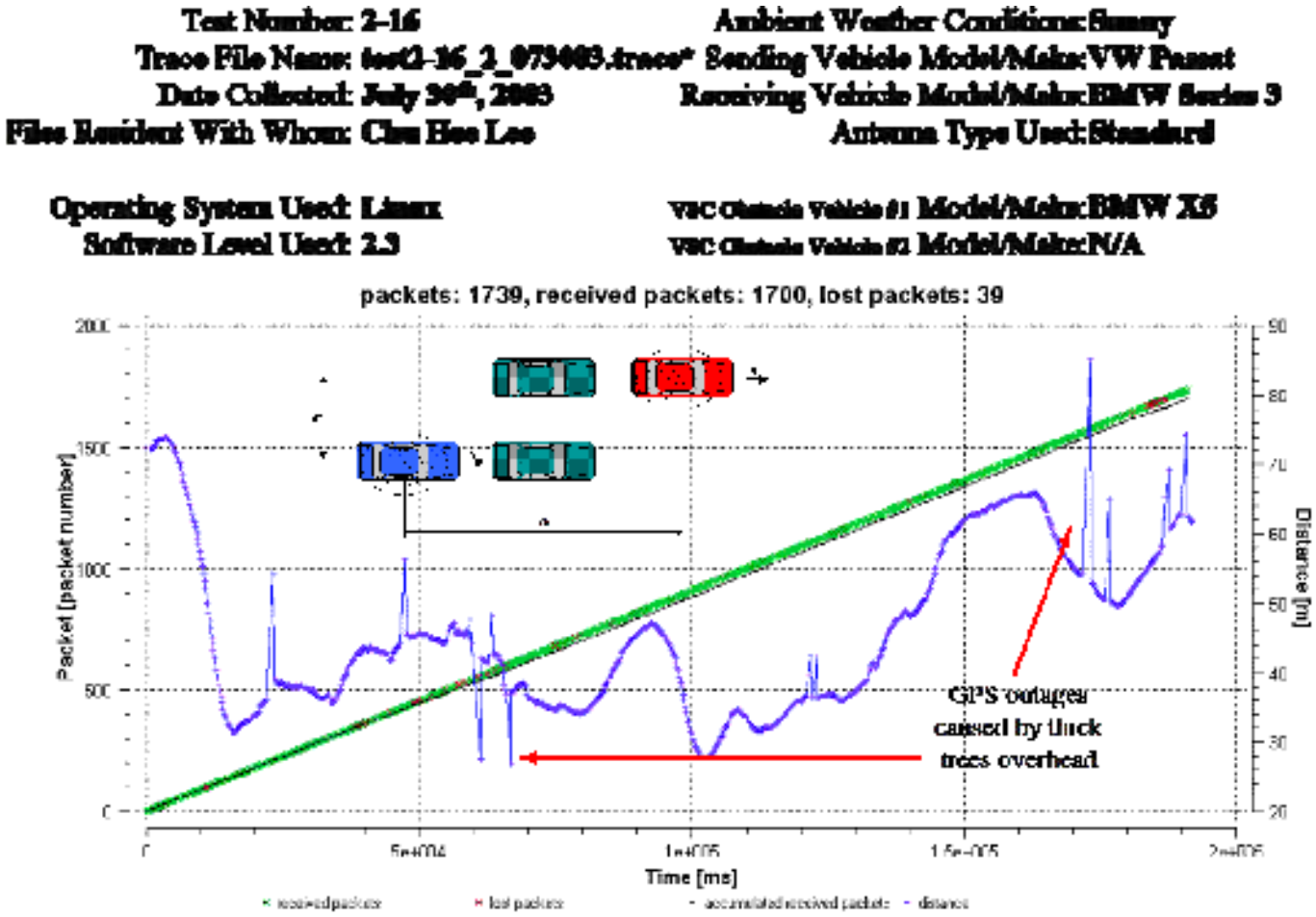
5.1.15 Test Scenario 2-16

Test Scenario	**2-16**
Relevant Applications	Emergency Electronic Brake Light Pre-Crash Sensing for Co-op Collision Mitigation Co-op Forward Collision Warning (FCW) Lane Change Warning
Velocity of Receiving Antenna (miles/hour)	40
Distance Between Antennas (meters)	< 20
Lateral Offset to Broadcast Antenna (meters)	4
Velocity of Sending Antenna (miles/hour)	40
Angle Between Vehicle 1 & Vehicle 2 (degrees)	0
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	400
Path Obstructions	None
Vehicle Obstructions	Sustained
Road Class	Arterial
Traffic Conditions	Light
Other Effects	None
Vehicle-Class of Cut-In Vehicle	SUV

Table 40. Test Scenario 2-16

Test Comments: GPS outages are likely due to many heavy trees overhanging the road. The few vehicle-to-vehicle outages that were observed were due to the blocking vehicle.

Figure 86. Test Number 2-16 Results



5.1.16 Test Scenario 2-17

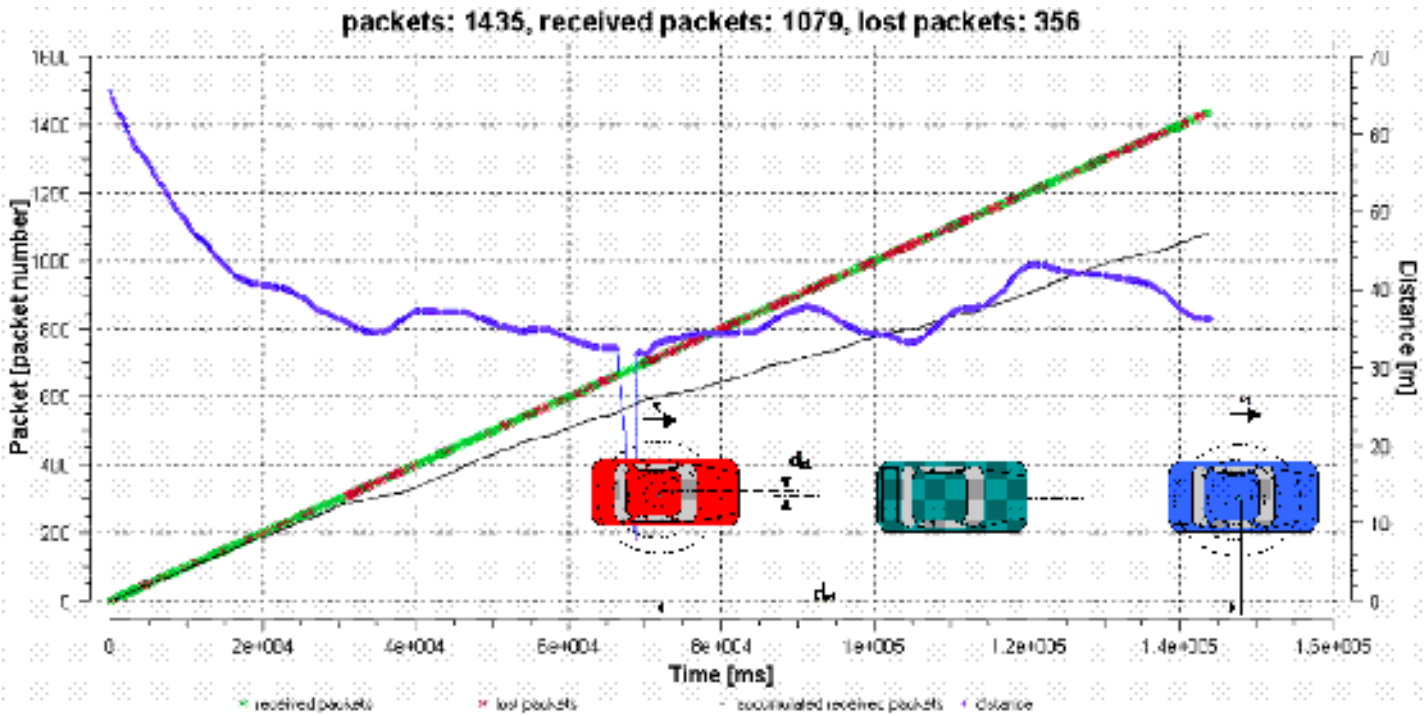
Test Scenario	**2-17**
Relevant Applications	Emergency Electronic Brake Light Pre-Crash Sensing for Co-op Collision Mitigation Co-op Forward Collision Warning (FCW) Lane Change Warning
Velocity of Receiving Antenna (miles/hour)	25
Distance Between Antennas (meters)	< 50
Lateral Offset to Broadcast Antenna (meters)	0
Velocity of Sending Antenna (miles/hour)	25
Angle Between Vehicle 1 & Vehicle 2 (degrees)	0
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	400
Path Obstructions	None
Vehicle Obstructions	Sustained
Road Class	Test Track
Traffic Conditions	Light
Other Effects	None
Vehicle-Class of Cut-In Vehicle	Truck

Table 41. Test Scenario 2-17

Test Comments: This test was done in MS Windows. The intercepting vehicle was a large truck. There were significant losses of reception due to the large truck interception and all trials of this test showed similar performance.

Figure 87. Test Number 2-17 Results

Test Number	2-17	Ambient Weather Conditions:	Mostly Sunny
Trace File Name:	040503_2_17_2.trace*	Sending Vehicle Model/Maker:	Buick LeSabre
Date Collected:	June 5th, 2003	Receiving Vehicle Model/Maker:	Buick LeSabre
Files Resident With Whom:	H. Krishnan	Antenna Type Used:	Standard
Operating System Used:	Windows XP	VSC Obstacle Vehicle #1 Model/Maker:	Large Truck
Software Level Used:	2.4a beta (27-Feb-03)	VSC Obstacle Vehicle #2 Model/Maker:	N/A



5.1.17 Test Scenario 2-18

Test Scenario	**2-18**
Relevant Applications	Emergency Electronic Brake Light Pre-Crash Sensing for Co-op Collision Mitigation Co-op Forward Collision Warning (FCW) Lane Change Warning
Velocity of Receiving Antenna (miles/hour)	60
Distance Between Antennas (meters)	< 100
Lateral Offset to Broadcast Antenna (meters)	4
Velocity of Sending Antenna (miles/hour)	60
Angle Between Vehicle 1 & Vehicle 2 (degrees)	0
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	400
Path Obstructions	None
Vehicle Obstructions	Sustained
Road Class	Highway
Traffic Conditions	Light
Other Effects	None
Vehicle-Class of Cut-In Vehicle	SUV

Table 42. Test Scenario 2-18

Test Comments: Significant, but not complete, blockage due to combination of curving terrain and blocking SUV.

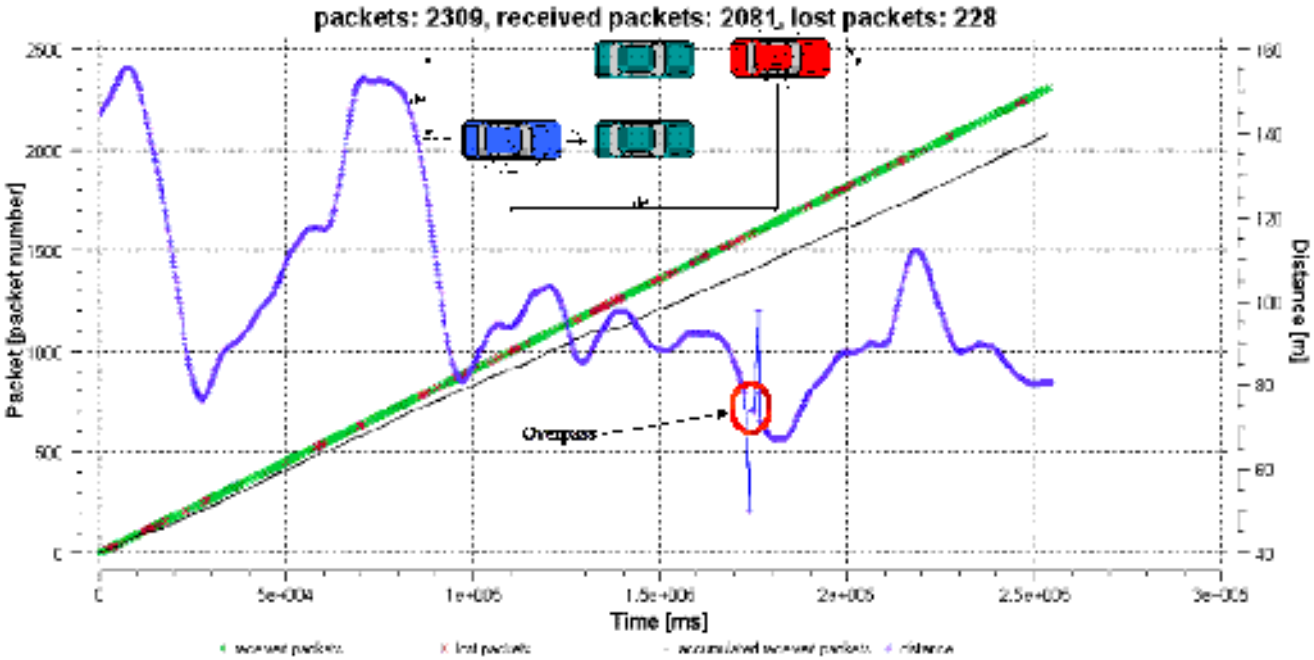
Figure 88. Test Number 2-18 Results

Test Number 2-18
Trace File Name: test2-18_2_073003.trace*
Date Collected: July 30th, 2003
Files Resident With Whom: Chu-Hee Lee

Ambient Weather Condition: Sunny
Sending Vehicle Model/Make: VW Passat
Receiving Vehicle Model/Make: BMW Series 3
Antenna Type Used: Standard

Operating System Used: Linux
Software Level Used: 2.5

VSC Obstacle Vehicle #1 Model/Make: BMW X5
VSC Obstacle Vehicle #2 Model/Make: N/A



5.1.18 Test Scenario 2-20

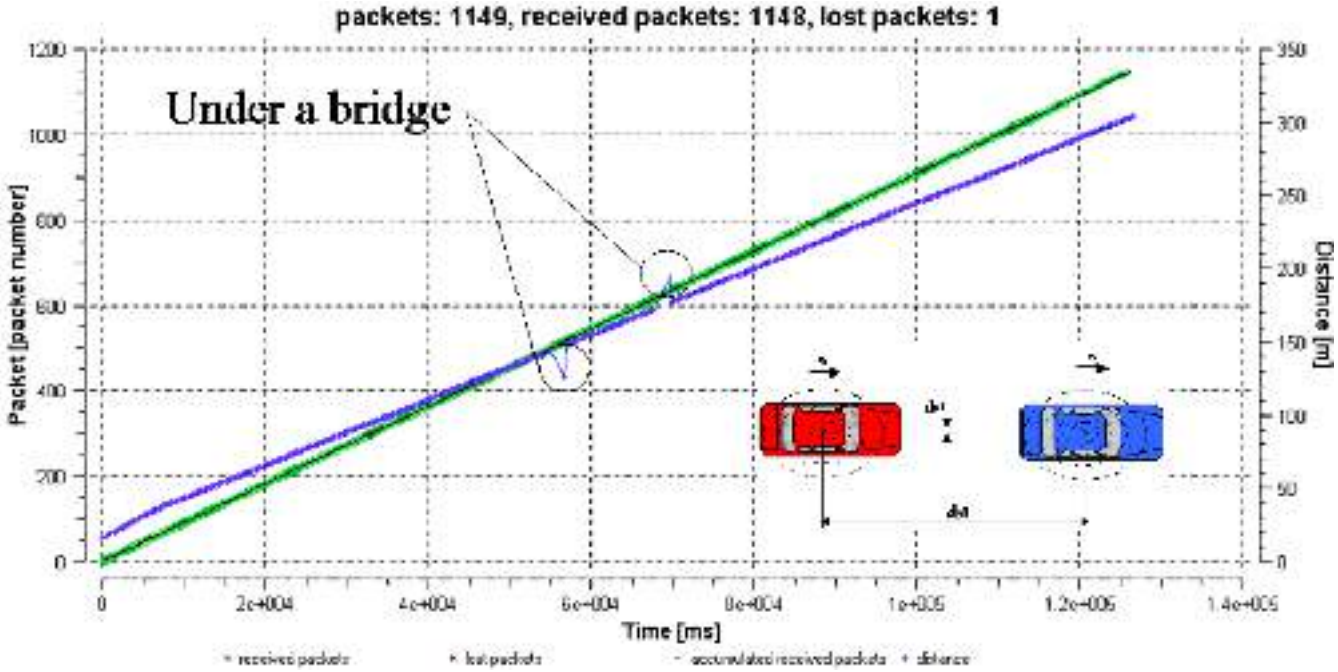
Test Scenario	**2-20**
Relevant Applications	Emergency Electronic Brake Light Pre-Crash Sensing for Co-op Collision Mitigation Co-op Forward Collision Warning (FCW) Lane Change Warning
Velocity of Receiving Antenna (miles/hour)	25
Distance Between Antennas (meters)	< 300
Lateral Offset to Broadcast Antenna (meters)	4
Velocity of Sending Antenna (miles/hour)	30
Angle Between Vehicle 1 & Vehicle 2 (degrees)	0
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	400
Path Obstructions	None
Vehicle Obstructions	None
Road Class	Test Track
Traffic Conditions	Light
Other Effects	None
Vehicle-Class of Cut-In Vehicle	None

Table 43. Test Scenario 2-20

Test Comments: This test considers a sending vehicle traveling at 30 mph that is slowly separating from a receiving vehicle moving at 25 mph. There was a clear line-of-sight for the duration of this test. A GPS outage was observed for all three trials while passing underneath a bridge, but no packets were lost. One packet was lost in Trial 3 at the range where multipath interference commonly occurs. Overall, 99.9 percent of the packets (3410 out of 3411) sent during the test were received.

Figure 89. Test Number 2-20-3 Results

Test Number:	**2-20-3**	**Ambient Weather Conditions:**	**Sunny**
Trace File Name:	**071703_2_20_3.trace***	**Sending Vehicle Model/Make:**	**GMC Envoy**
Date Collected:	**July 17th, 2003**	**Receiving Vehicle Model/Make:**	**Buick LeSabre**
Files Resident With Whom:	**Jim Bauer**	**Antenna Type Used:**	**Standard**
Operating System Used:	**Linux**	**VSC Obstacle Vehicle #1 Model/Make:**	**N/A**
Software Level Used:	**Version 2.3**	**VSC Obstacle Vehicle #2 Model/Make:**	**N/A**



5.1.19 Test Scenario 2-21

Test Scenario	**2-21**
Relevant Applications	Emergency Electronic Brake Light Pre-Crash Sensing for Co-op Collision Mitigation Co-op Forward Collision Warning (FCW) Lane Change Warning
Velocity of Receiving Antenna (miles/hour)	60
Distance Between Antennas (meters)	< 300
Lateral Offset to Broadcast Antenna (meters)	4
Velocity of Sending Antenna (miles/hour)	65
Angle Between Vehicle 1 & Vehicle 2 (degrees)	0
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	400
Path Obstructions	None
Vehicle Obstructions	None
Road Class	Highway
Traffic Conditions	Light
Other Effects	None
Vehicle-Class of Cut-In Vehicle	None

Table 44. Test Scenario 2-21

Test Comments: Overall, this test was successful, except for an extended outage (no clear cause) around the middle of the test period.

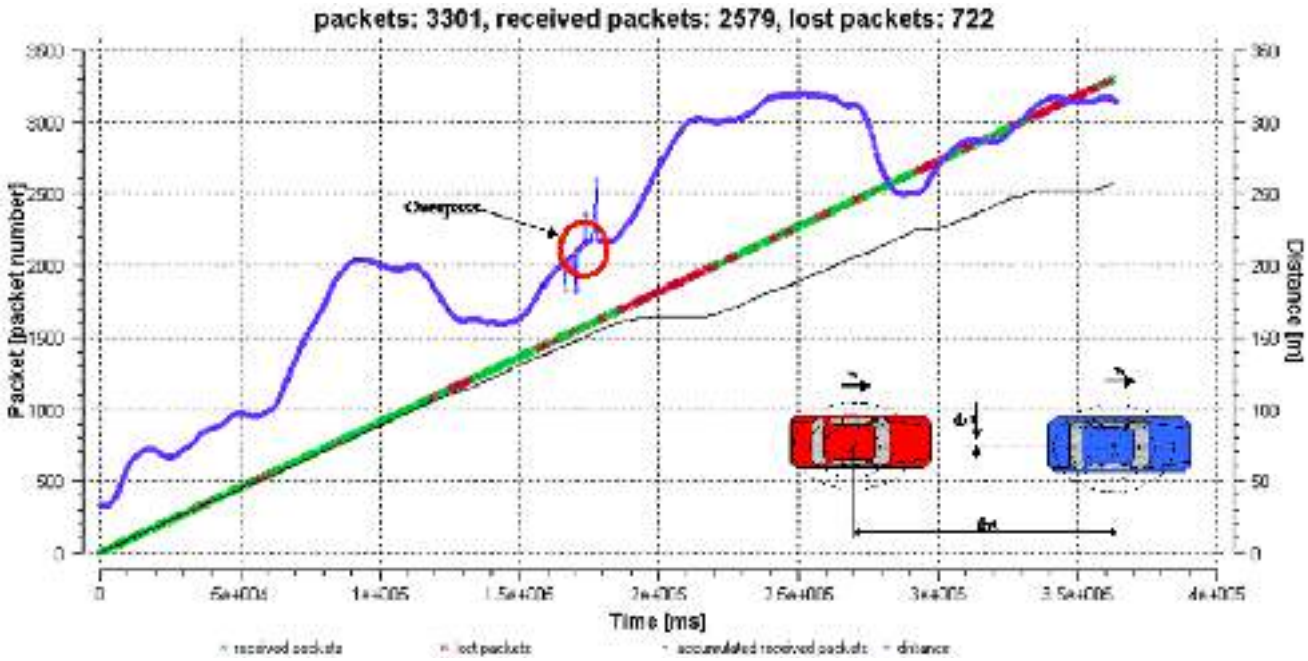
Figure 90. Test Number 2-21 Results

Test Number 2-21
Trace File Name: test2-21-3_070203.trace*
Date Collected: July 3rd, 2003
Files Resident With Whom: Chu-Hao Lee

Ambient Weather Conditions: Sunny
Sending Vehicle Model/Make: Sedan
Receiving Vehicle Model/Make: Sedan
Antenna Type Used: Standard

Operating System Used: Linux
Software Level Used: 2.1

VSC Obstacle Vehicle #1 Model/Make: N/A
VSC Obstacle Vehicle #2 Model/Make: N/A



5.1.20 Test Scenario 2-22

Test Scenario	**2-22**
Relevant Applications	Emergency Electronic Brake Light Pre-Crash Sensing for Co-op Collision Mitigation Co-op Forward Collision Warning (FCW) Lane Change Warning
Velocity of Receiving Antenna (miles/hour)	60
Distance Between Antennas (meters)	< 300
Lateral Offset to Broadcast Antenna (meters)	8
Velocity of Sending Antenna (miles/hour)	75
Angle Between Vehicle 1 & Vehicle 2 (degrees)	0
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	400
Path Obstructions	None
Vehicle Obstructions	None
Road Class	Highway
Traffic Conditions	Light
Other Effects	None
Vehicle-Class of Cut-In Vehicle	None

Table 45. Test Scenario 2-22

Test Comments: The chart shows only the pertinent portion of the test period. Although the overall packet loss for the whole test was over 50 percent, during the pertinent period shown, the packet loss rate was 1.7 percent.

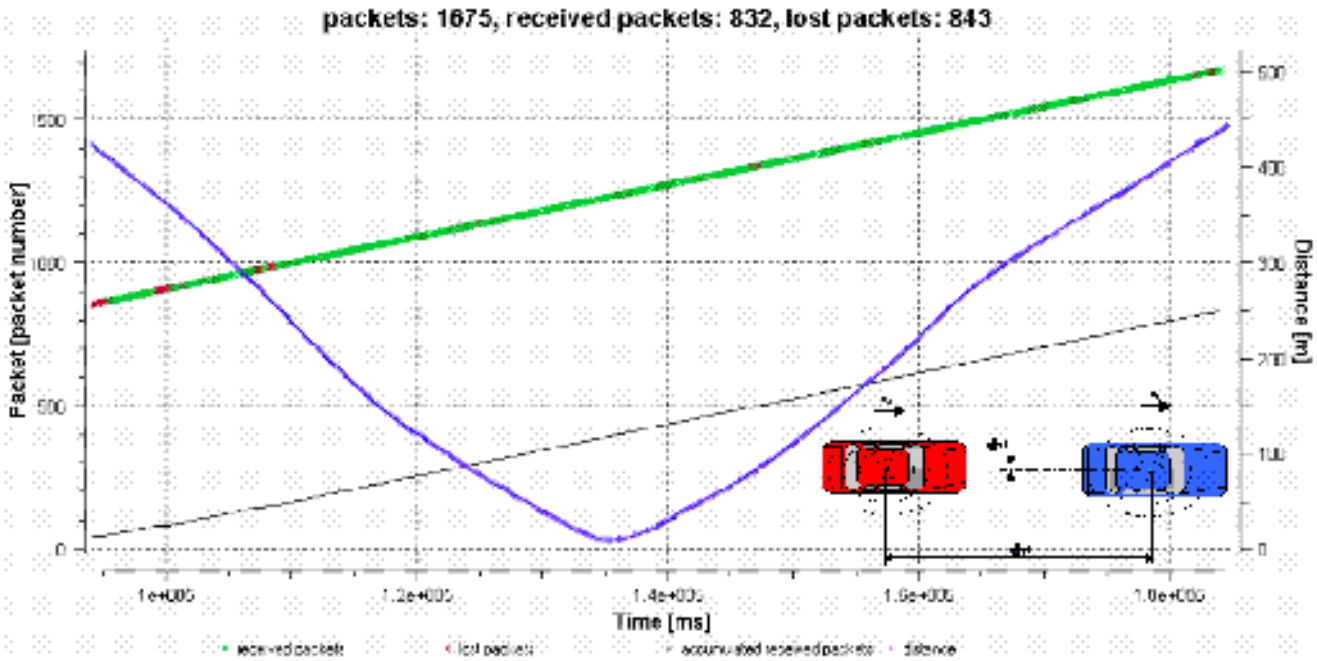
Figure 91. Test Number 2-22 Results

Test Number 2-22
Trace File Name: [illegible]2-22_4_071403.trace*
Date Collected: July 14th, 2003
Files Resident With Whom: Chu-Hee Lee

Ambient Weather Conditions: Sunny
Sending Vehicle Model/Make: BMW Series 3
Receiving Vehicle Model/Make: VW Passat
Antenna Type Used: Standard

Operating System Used: Linux
Software Level Used: 2.3

VSC Obstacle Vehicle #1 Model/Make: N/A
VSC Obstacle Vehicle #2 Model/Make: N/A



5.1.21 Test Scenario 2-23

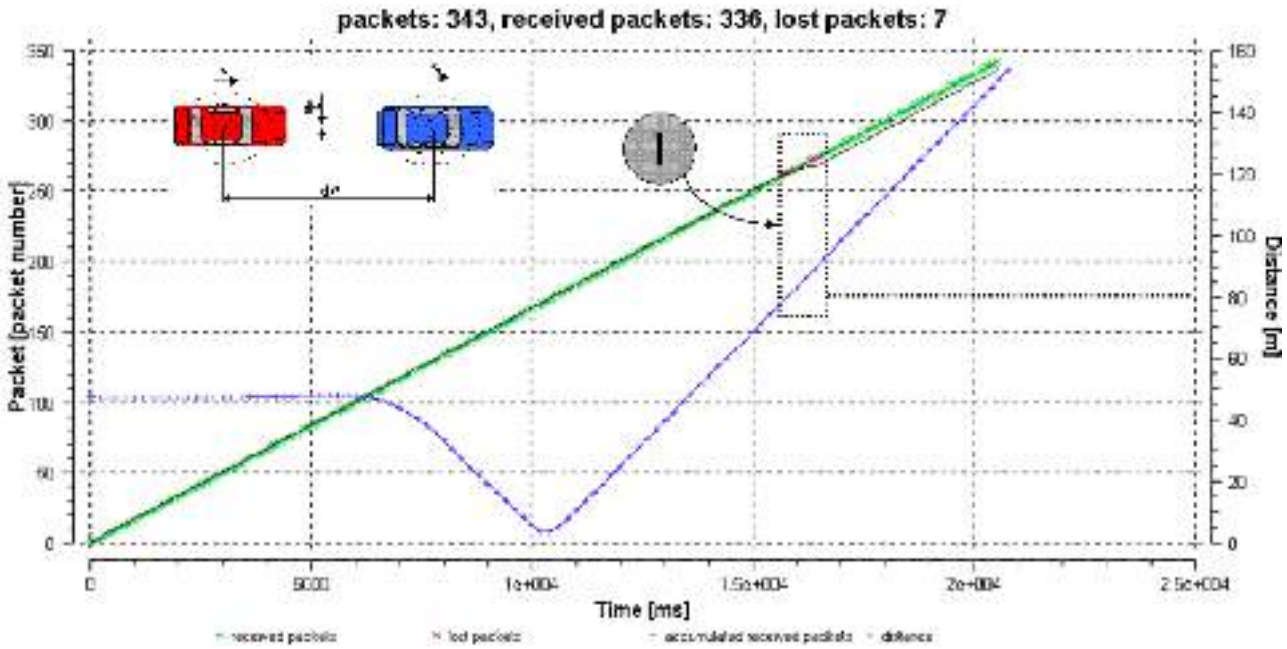
Test Scenario	**2-23**
Relevant Applications	Emergency Electronic Brake Light Pre-Crash Sensing for Co-op Collision Mitigation Co-op Forward Collision Warning (FCW) Lane Change Warning
Velocity of Receiving Antenna (miles/hour)	30
Distance Between Antennas (meters)	< 50
Lateral Offset to Broadcast Antenna (meters)	4
Velocity of Sending Antenna (miles/hour)	30 -> 0
Angle Between Vehicle 1 & Vehicle 2 (degrees)	0
Update Rate (milliseconds)	50
Transmitter Power Level (%)	100
Packet Size (bytes)	400
Path Obstructions	None
Vehicle Obstructions	None
Road Class	Test Track
Traffic Conditions	N/A
Other Effects	None
Vehicle-Class of Cut-In Vehicle	N/A

Table 46. Test Scenario 2-23

Test Comments: This test considers a receiving vehicle traveling at 30 mph that passes a sending vehicle braking from 30 to 0 mph. There was a clear line-of-sight for the duration of this test. All of the packets lost in eight of the nine trials occurred at the ~90m range, and this loss can be attributed to multipath that occurred consistently at that general range, as demonstrated in Test 1-20. There were no packets lost at ~90m in Trial 2-23-4 because the vehicles did not reach that separation distance during the course of data collection. Overall, 99 percent of the packets sent during the test were received (3837 out of 3876 packets).

Figure 92. Test Number 2-23 Results

Test Number	**2-23**	**Ambient Weather Conditions:**	**Sunny**
Trace File Name:	**071703_2_23_9.trace***	**Sending Vehicle Model/Make:**	**GMC Envoy**
Date Collected:	**July 17th, 2003**	**Receiving Vehicle Model/Make:**	**Buick LeSabre**
Files Resident With Whom:	**Jim Bauer**	**Antenna Type Used:**	**Standard**
Operating System Used:	**Linux**	**VSC Obstacle Vehicle #1 Model/Make:**	**N/A**
Software Level Used:	**Version 2.3**	**VSC Obstacle Vehicle #2 Model/Make:**	**N/A**



5.1.22 Test Scenario 2-24

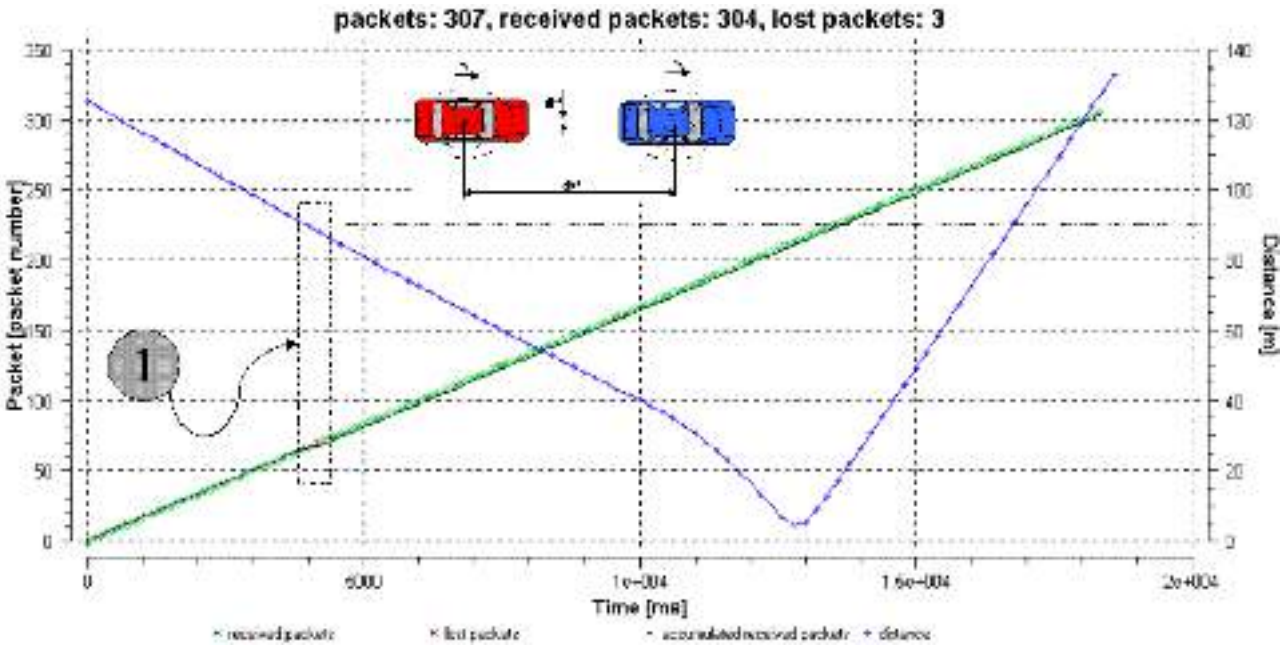
Test Scenario	**2-24**
Relevant Applications	Emergency Electronic Brake Light Pre-Crash Sensing for Co-op Collision Mitigation Co-op Forward Collision Warning (FCW) Lane Change Warning
Velocity of Receiving Antenna (miles/hour)	50
Distance Between Antennas (meters)	< 50
Lateral Offset to Broadcast Antenna (meters)	4
Velocity of Sending Antenna (miles/hour)	30 -> 0
Angle Between Vehicle 1 & Vehicle 2 (degrees)	0
Update Rate (milliseconds)	50
Transmitter Power Level (%)	100
Packet Size (bytes)	400
Path Obstructions	None
Vehicle Obstructions	None
Road Class	Test Track
Traffic Conditions	N/A
Other Effects	None
Vehicle-Class of Cut-In Vehicle	N/A

Table 47. Test Scenario 2-24

Test Comments: This test considers a receiving vehicle traveling at 50 mph that overtakes and passes a sending vehicle braking from 30 to 0 mph. There was a clear line-of-sight for the duration of this test. A loss of packets (1) took place at a range of ~90m in the 3 trials. This packet loss can be attributed to multipath that occurred consistently at that general range, as demonstrated in Test 1-20. Overall, 99 percent of the packets sent during this test were received (864 out of 873 packets).

Figure 93. Test Number 2-24-1 Results

Test Number	**2-24-1**	**Ambient Weather Conditions:**	**Sunny**
Trace File Name:	**072403_2_24_1.trace***	**Sending Vehicle Model/Make:**	**Buick LeSabre**
Date Collected:	**July 24th, 2003**	**Receiving Vehicle Model/Make:**	**Buick LeSabre**
Files Resident With Whom:	**Jim Bauer**	**Antenna Type Used:**	**Standard**
Operating System Used:	**Linux**	**VBC Obstacle Vehicle #1 Model/Make:**	**N/A**
Software Level Used:	**Version 2.3**	**VBC Obstacle Vehicle #2 Model/Make:**	**N/A**



5.1.23 Test Scenario 2-25

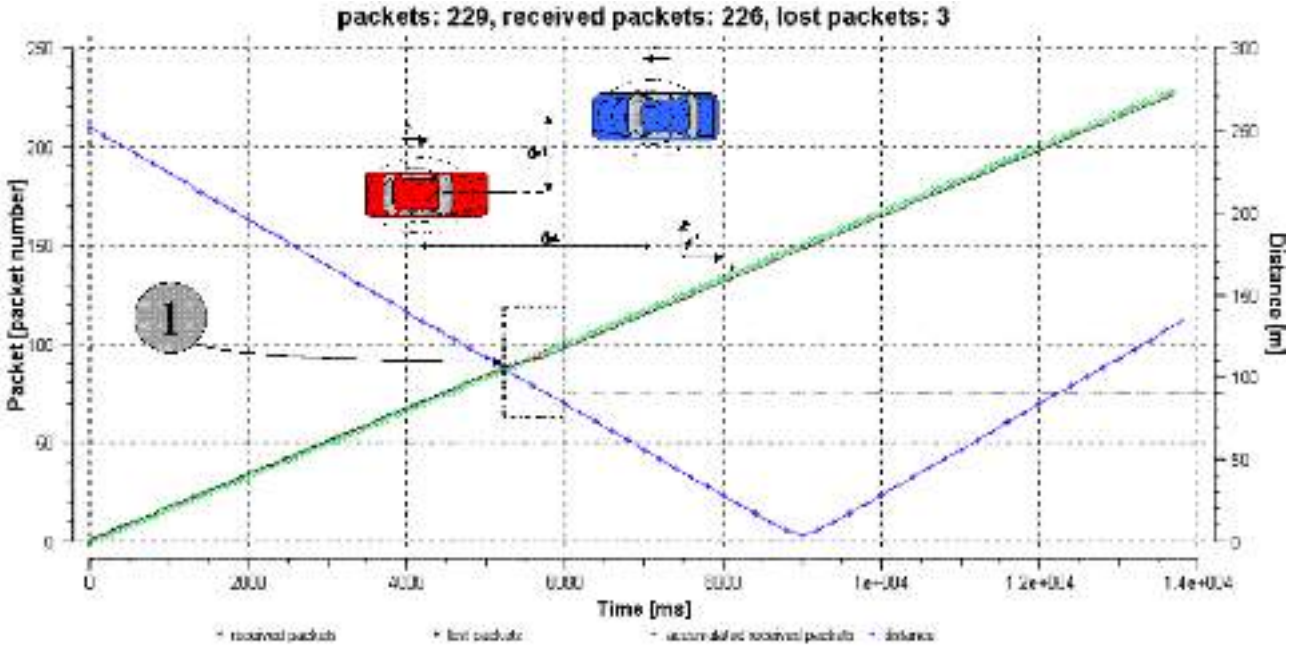
Test Scenario	**2-25**
Relevant Applications	Pre-Crash Sensing for Co-op Collision Mitigation
Velocity of Receiving Antenna (miles/hour)	30
Distance Between Antennas (meters)	< 50
Lateral Offset to Broadcast Antenna (meters)	4
Velocity of Sending Antenna (miles/hour)	30
Angle Between Vehicle 1 & Vehicle 2 (degrees)	180
Update Rate (milliseconds)	50
Transmitter Power Level (%)	100
Packet Size (bytes)	400
Path Obstructions	None
Vehicle Obstructions	None
Road Class	Test Track
Traffic Conditions	N/A
Other Effects	None
Vehicle-Class of Cut-In Vehicle	N/A

Table 48. Test Scenario 2-25

Test Comments: This test considers a sending vehicle traveling at 30 mph as it approaches and passes a receiving vehicle traveling at the same speed. There was a clear line-of-sight throughout the duration of this test. Of the four trials that were conducted, packets were lost only in Trial 1. The loss of packets (1) took place at the range of ~90m and can be attributed to multipath that commonly occurred at that general range, as demonstrated in Test 1-20. Overall, 99.6 percent of the packets sent during the test were received (793 out of 796 packets).

Figure 94. Test Number 2-25 Results

Test Number	**2-25**	**Ambient Weather Conditions:**	**Sunny**
Trace File Name:	**072403_2_25_1.trace***	**Sending Vehicle Model/Make:**	**Buick LeSabre**
Date Collected:	**July 24th, 2003**	**Receiving Vehicle Model/Make:**	**Buick LeSabre**
Files Resident With Whom:	**Jim Bauer**	**Antenna Type Used:**	**Standard**
Operating System Used:	**Linux**	**VSC Obstacle Vehicle #1 Model/Make:**	**N/A**
Software Level Used:	**Version 2.3**	**VSC Obstacle Vehicle #2 Model/Make:**	**N/A**



5.1.24 Test Scenario 2-26

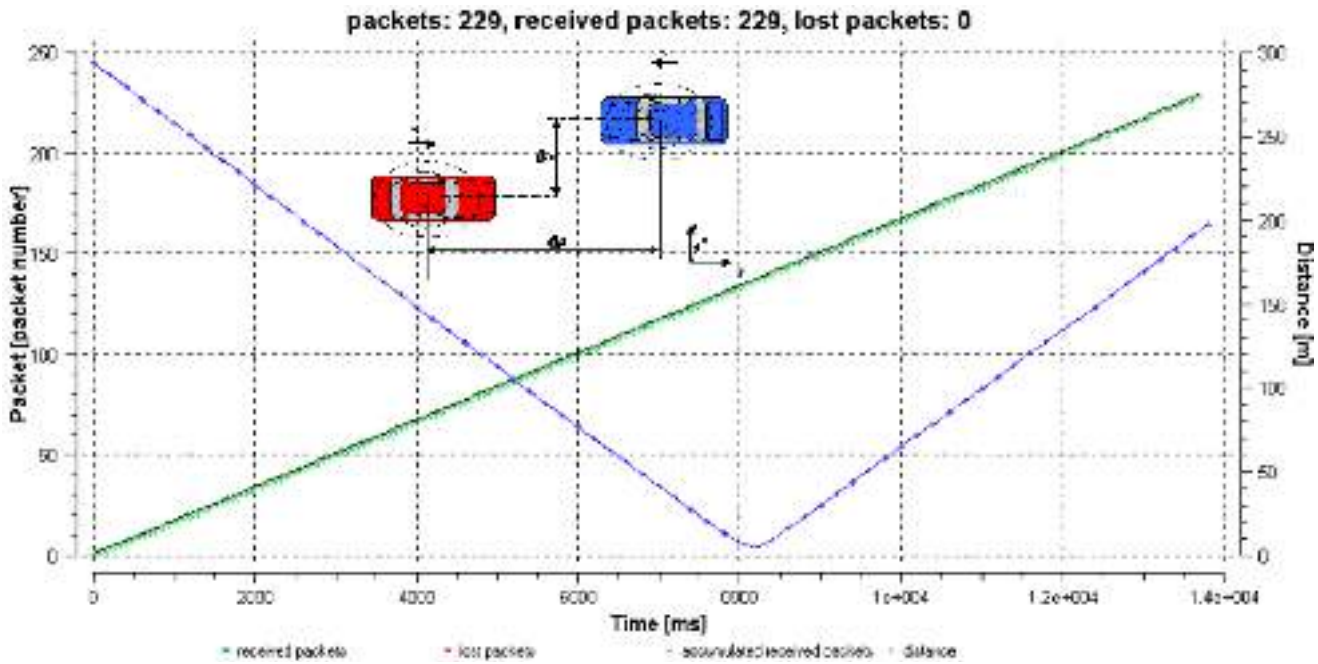
Test Scenario	**2-26**
Relevant Applications	Pre-Crash Sensing for Co-op Collision Mitigation
Velocity of Receiving Antenna (miles/hour)	50
Distance Between Antennas (meters)	< 50
Lateral Offset to Broadcast Antenna (meters)	4
Velocity of Sending Antenna (miles/hour)	30
Angle Between Vehicle 1 & Vehicle 2 (degrees)	180
Update Rate (milliseconds)	50
Transmitter Power Level (%)	100
Packet Size (bytes)	400
Path Obstructions	None
Vehicle Obstructions	None
Road Class	Test Track
Traffic Conditions	N/A
Other Effects	None
Vehicle-Class of Cut-In Vehicle	N/A

Table 49. Test Scenario 2-26

Test Comments: This test considers a receiving vehicle traveling at 50 mph that catches up to and passes a sending vehicle traveling at 30 mph. There was a clear line-of-sight for the duration of this test. There were no GPS outages in any of the 4 trials. Overall, 100 percent of the packets sent during the test were received.

Figure 95. Test Number 2-26 Results

Test Number:	2-26	Ambient Weather Conditions:	Sunny
Trace File Name:	072403_2_26_3.trace*	Sending Vehicle Model/Make:	Buick LeSabre
Date Collected:	July 24th, 2003	Receiving Vehicle Model/Make:	Buick LeSabre
Files Resident With Whom:	Jim Bauer	Antenna Type Used:	Standard
Operating System Used:	Linux	VSC Obstacle Vehicle #1 Model/Make:	N/A
Software Level Used:	Version 2.3	VSC Obstacle Vehicle #2 Model/Make:	N/A



5.1.25 Test Scenario 2-27

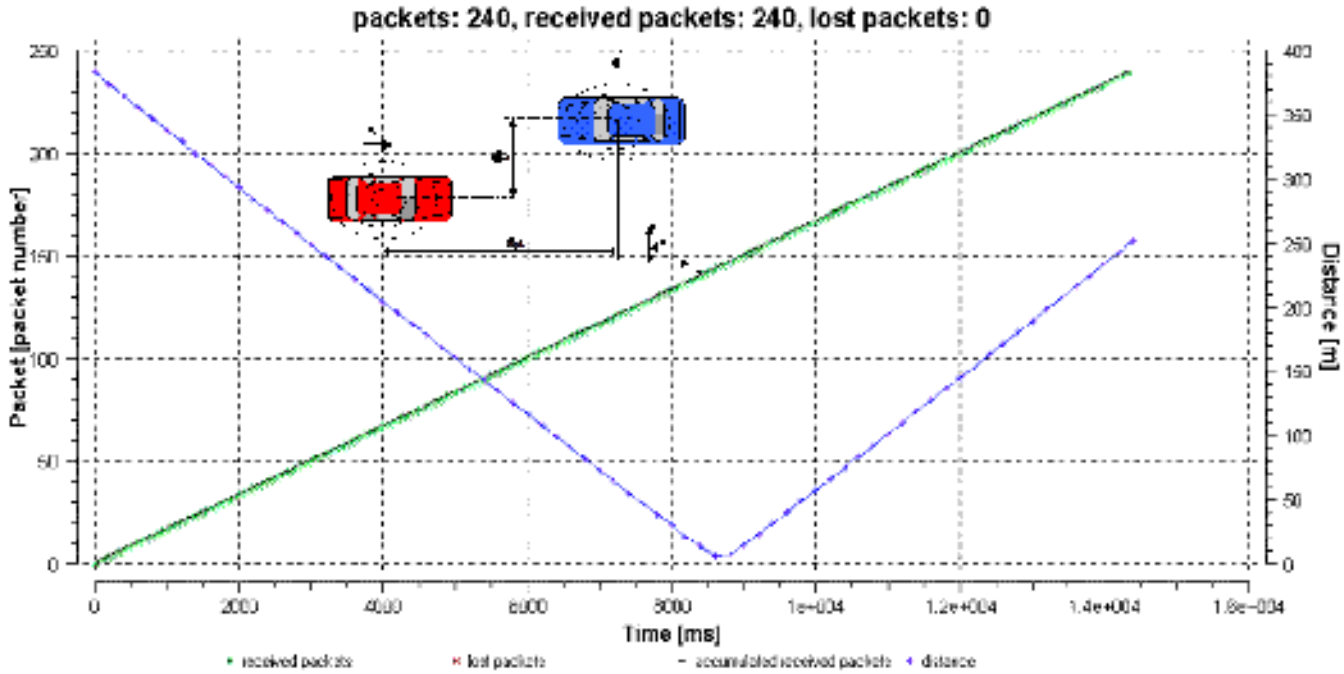
Test Scenario	**2-27**
Relevant Applications	Pre-Crash Sensing for Co-op Collision Mitigation
Velocity of Receiving Antenna (miles/hour)	50
Distance Between Antennas (meters)	< 50
Lateral Offset to Broadcast Antenna (meters)	4
Velocity of Sending Antenna (miles/hour)	50
Angle Between Vehicle 1 & Vehicle 2 (degrees)	180
Update Rate (milliseconds)	50
Transmitter Power Level (%)	100
Packet Size (bytes)	400
Path Obstructions	None
Vehicle Obstructions	None
Road Class	Test Track
Traffic Conditions	N/A
Other Effects	None
Vehicle-Class of Cut-In Vehicle	N/A

Table 50. Test Scenario 2-27

Test Comments: This test considers two vehicles that communicate while approaching and passing each other at 50 mph. There was a clear line-of-sight for the duration of this test. There were no GPS outages in any of the 4 trials. Overall, 100 percent of the packets sent during the test were received.

Figure 96. Test Number 2-27 Results

Test Number:	**2-27**	**Ambient Weather Conditions:**	**Sunny**
Trace File Name:	**072403_2_27_4.trace***	**Sending Vehicle Model/Make:**	**Buick LeSabre**
Date Collected:	**July 24th, 2003**	**Receiving Vehicle Model/Make:**	**Buick LeSabre**
Files Resident With Whom:	**Jim Bauer**	**Antenna Type Used:**	**Standard**
Operating System Used:	**Linux**	**VBC Obstacle Vehicle #1 Model/Make:**	**N/A**
Software Level Used:	**Version 2.3**	**VBC Obstacle Vehicle #2 Model/Make:**	**N/A**



5.1.26 Test Scenario 2-28

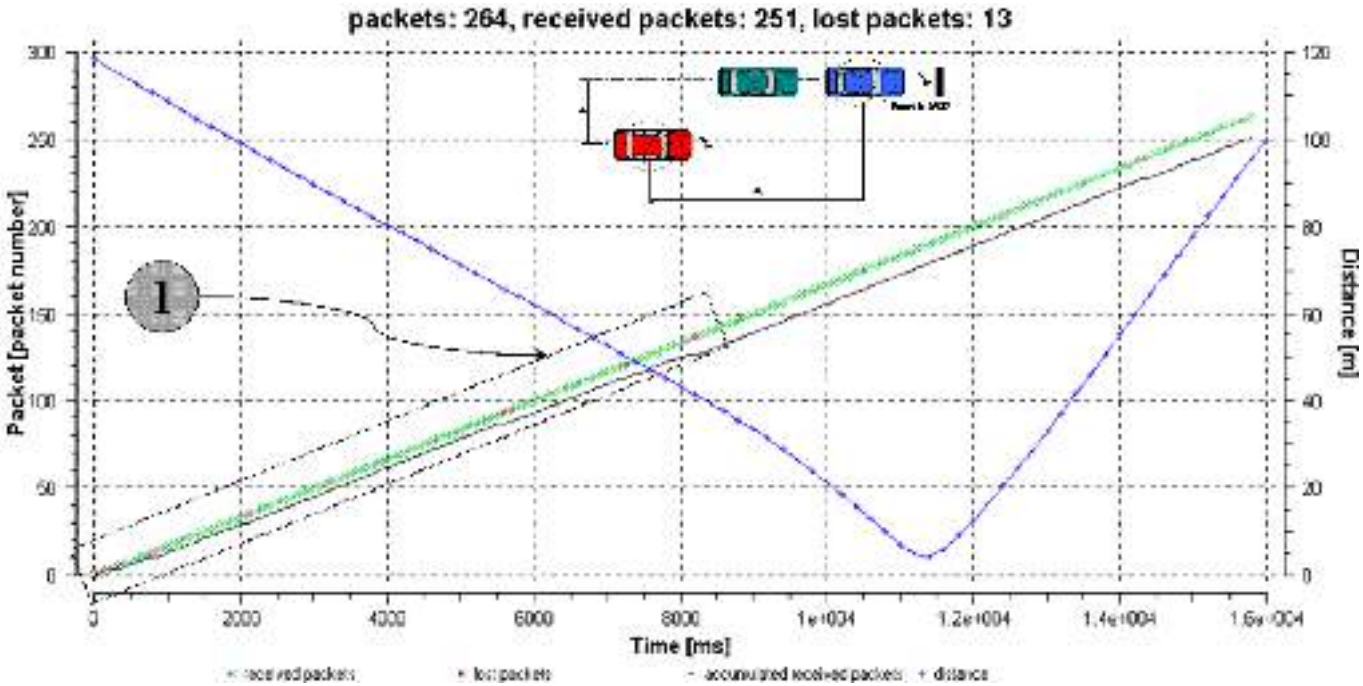
Test Scenario	**2-28**
Relevant Applications	Emergency Electronic Brake Light Pre-Crash Sensing for Co-op Collision Mitigation Co-op Forward Collision Warning (FCW)
Velocity of Receiving Antenna (miles/hour)	50
Distance Between Antennas (meters)	< 50
Lateral Offset to Broadcast Antenna (meters)	4
Velocity of Sending Antenna (miles/hour)	30 -> 0
Angle Between Vehicle 1 & Vehicle 2 (degrees)	0
Update Rate (milliseconds)	50
Transmitter Power Level (%)	100
Packet Size (bytes)	400
Path Obstructions	None
Vehicle Obstructions	Sustained
Road Class	Test Track
Traffic Conditions	N/A
Other Effects	None
Vehicle-Class of Cut-In Vehicle	SUV

Table 51. Test Scenario 2-28

Test Comments: This test considers a receiving vehicle traveling at 50 mph that overtakes and passes an SUV and a sending vehicle as they brake from 30 to 0 mph. The line-of-sight was obstructed by the SUV during the first part of this test, and cleared as the receiving vehicle passes the SUV. Packets were lost in each of the five trials. The packet loss (1) took place at various ranges early in the trials and are likely to be due to the obstructing SUV. Overall, 95 percent of the packets sent during the test were received.

Figure 97. Test Number 2-28-5 Results

Test Number	2-28-5	Ambient Weather Conditions:	Sunny
Trace File Name:	080703_2_28_5.trace*	Sending Vehicle Model/Make:	Buick LeSabre
Date Collected:	August 7th, 2003	Receiving Vehicle Model/Make:	Buick LeSabre
Files Resident With Whom:	Jim Bauer	Antenna Type Used:	Standard
Operating System Used:	Linux	VSC Obstacle Vehicle #1 Model/Make:	GMC Envoy
Software Level Used:	Version 2.3	VSC Obstacle Vehicle #2 Model/Make:	N/A



5.1.27 Test Scenario 2-29

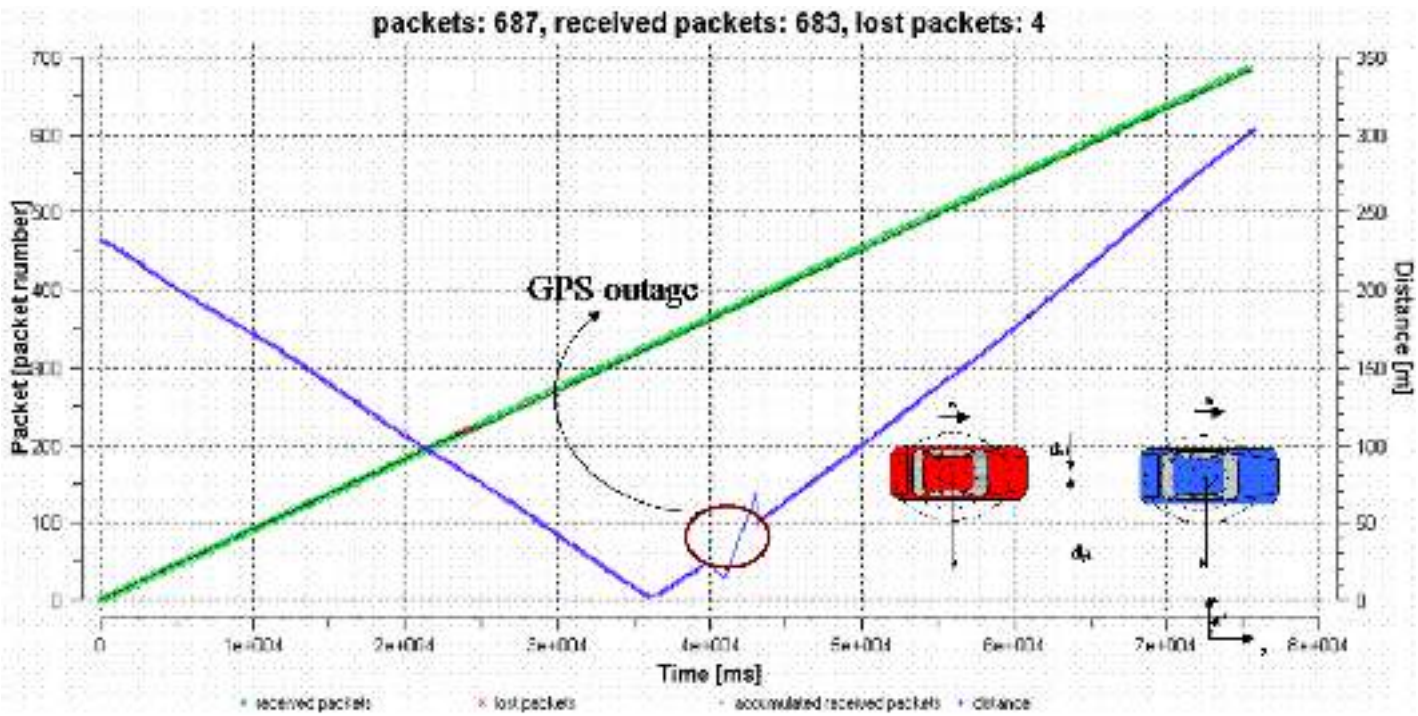
Test Scenario	**2-29**
Relevant Applications	Emergency Electronic Brake Light Pre-Crash Sensing for Co-op Collision Mitigation Co-op Forward Collision Warning (FCW) Lane Change Warning
Velocity of Receiving Antenna (miles/hour)	40
Distance Between Antennas (meters)	< 300
Lateral Offset to Broadcast Antenna (meters)	4
Velocity of Sending Antenna (miles/hour)	25
Angle Between Vehicle 1 & Vehicle 2 (degrees)	0
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	400
Path Obstructions	None
Vehicle Obstructions	None
Road Class	Test Track
Traffic Conditions	Light
Other Effects	None
Vehicle-Class of Cut-In Vehicle	None

Table 52. Test Scenario 2-29

Test Comments: There was a clear line-of-sight for the duration of this test between the sending vehicle and the receiving vehicle. Two GPS outages were observed as the vehicles went under a bridge in the test track. There were a few lost packets in all three trials of the test. The reception outage was observed in the same location for all three trials (80-90m) which was proven in Test 1-20 to be a multi-path interference.

Figure 98. Test Number 2-29 Results

Test Number	2-29	Ambient Weather Conditions:	Sunny
Trace File Name:	072403_2_29_1.trace*	Sending Vehicle Model/Make:	Buick LeSabre
Date Collected:	July 24th, 2003	Receiving Vehicle Model/Make:	Buick LeSabre
Files Resident With Whom:	H. Krishnan	Antenna Type Used:	Standard
Operating System Used:	Linux	VSC Obstacle Vehicle #1 Model/Make:	N/A
Software Level Used:	V2.3 (8-July-03)	VSC Obstacle Vehicle #2 Model/Make:	N/A



5.1.28 Test Scenario 2-30

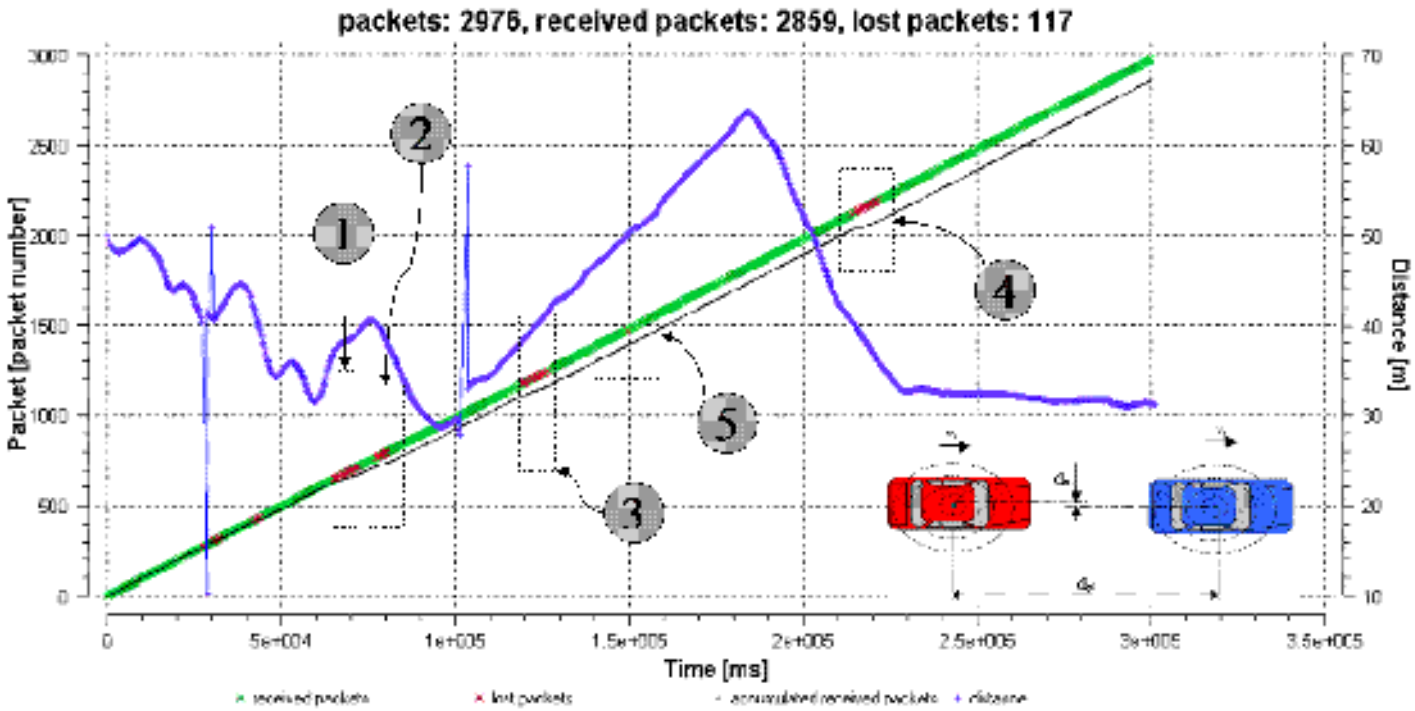
Test Scenario	**2-30**
Relevant Applications	Emergency Electronic Brake Light Pre-Crash Sensing for Co-op Collision Mitigation Co-op Forward Collision Warning (FCW) Lane Change Warning
Velocity of Receiving Antenna (miles/hour)	60
Distance Between Antennas (meters)	< 150
Lateral Offset to Broadcast Antenna (meters)	0
Velocity of Sending Antenna (miles/hour)	60
Angle Between Vehicle 1 & Vehicle 2 (degrees)	0
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	400
Path Obstructions	None
Vehicle Obstructions	None
Road Class	Highway
Traffic Conditions	N/A
Other Effects	None
Vehicle-Class of Cut-In Vehicle	N/A

Table 53. Test Scenario 2-30

Test Comments: There was a clear line-of-sight for the duration of this test. Several short partial outages were observed, and an explanation for the outages was not clear at the time of the test. Overall, 96 percent of the packets sent during the test were received.

Figure 99. Test Number 2-30 Results

Test Number:	**2-30**	**Ambient Weather Conditions:**	**Mostly Sunny**
Trace File Name:	**051303_01.trace***	**Sending Vehicle Model/Make:**	**Nissan Altima**
Date Collected:	**May 13th, 2005**	**Receiving Vehicle Model/Make:**	**Lexus GS300**
Files Resident With Whom:	**Jim Bauer**	**Antenna Type Used:**	**Standard**
Operating System Used:	**Windows XP**	**VSC Outside Vehicle #1 Model/Make:**	**N/A**
Software Level Used:	**2.4a beta (27-Feb-05)**	**VSC Outside Vehicle #2 Model/Make:**	**N/A**



5.1.29 Test Scenario 2-31

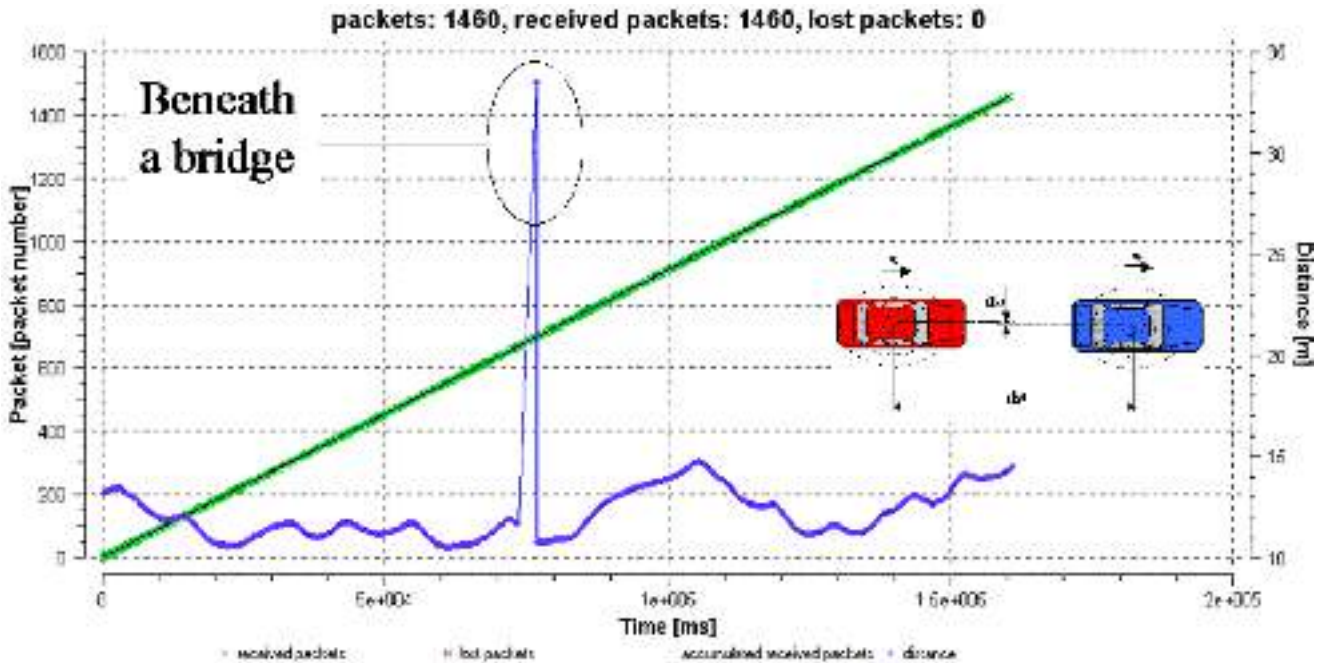
Test Scenario	**2-31**
Relevant Applications	Emergency Electronic Brake Light Pre-Crash Sensing for Co-op Collision Mitigation Co-op Forward Collision Warning (FCW) Lane Change Warning
Velocity of Receiving Antenna (miles/hour)	25
Distance Between Antennas (meters)	< 15
Lateral Offset to Broadcast Antenna (meters)	0
Velocity of Sending Antenna (miles/hour)	25
Angle Between Vehicle 1 & Vehicle 2 (degrees)	0
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	400
Path Obstructions	None
Vehicle Obstructions	None
Road Class	Test Track
Traffic Conditions	Light
Other Effects	None
Vehicle-Class of Cut-In Vehicle	None

Table 54. Test Scenario 2-31

Test Comments: This test considers two vehicles traveling at 25 mph in the same direction at close proximity. There was a clear line-of-sight throughout the duration of this test. A GPS outage was observed in the same location for all three trials (while passing underneath a bridge), but no packets were lost. Overall, 100 percent of the packets sent during the test were received.

Figure 100. Test Number 2-31 Results

Test Number:	**2-31**	**Ambient Weather Conditions:**	**Sunny**
Trace File Name:	**072403_2_31_1.trace***	**Sending Vehicle Model/Make:**	**Buick LeSabre**
Date Collected:	**July 24th, 2003**	**Receiving Vehicle Model/Make:**	**Buick LeSabre**
Files Resident With Whom:	**Jim Bauer**	**Antenna Type Used:**	**Standard**
Operating System Used:	**Linux**	**VSC Obstacle Vehicle #1 Model/Make:**	**N/A**
Software Level Used:	**Version 2.3**	**VSC Obstacle Vehicle #2 Model/Make:**	**N/A**



5.1.30 Test Scenario 2-32

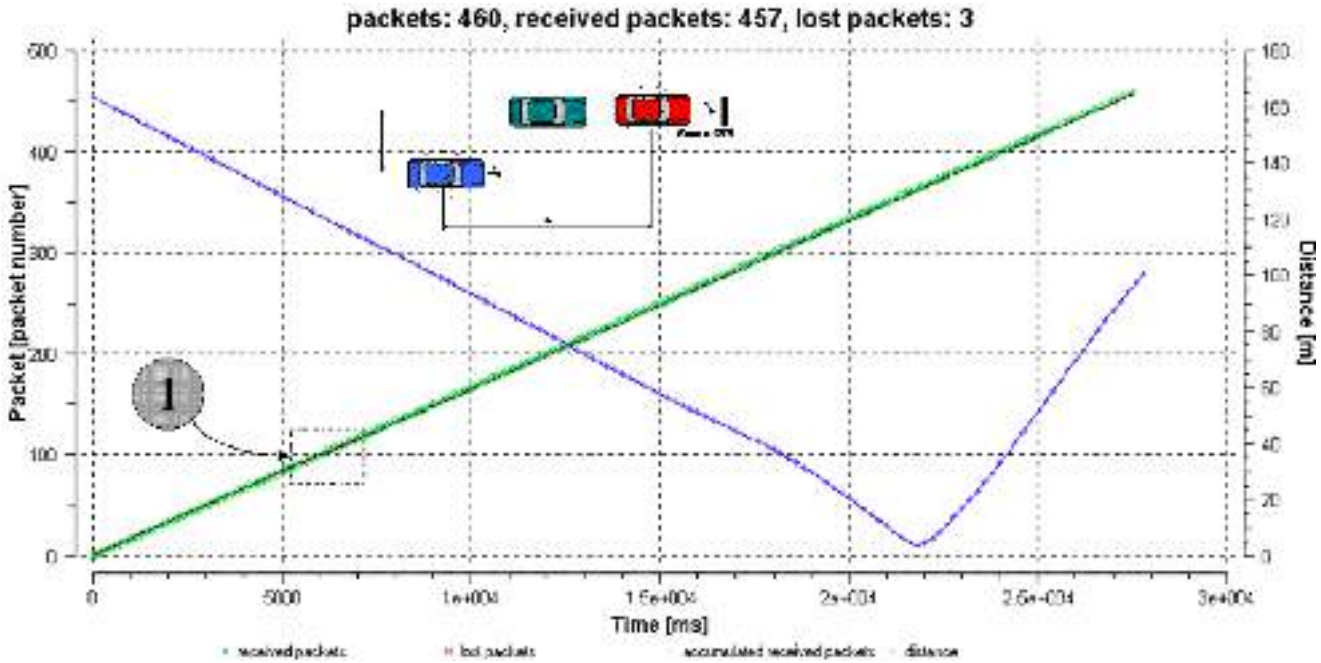
Test Scenario	**2-32**
Relevant Applications	Pre-Crash Sensing for Co-op Collision Mitigation Lane Change Warning
Velocity of Receiving Antenna (miles/hour)	30 -> 0
Distance Between Antennas (meters)	< 50
Lateral Offset to Broadcast Antenna (meters)	4
Velocity of Sending Antenna (miles/hour)	50
Angle Between Vehicle 1 & Vehicle 2 (degrees)	0
Update Rate (milliseconds)	50
Transmitter Power Level (%)	100
Packet Size (bytes)	400
Path Obstructions	None
Vehicle Obstructions	Sustained
Road Class	Test Track
Traffic Conditions	N/A
Other Effects	None
Vehicle-Class of Cut-In Vehicle	SUV

Table 55. Test Scenario 2-32

Test Comments: This test considers a sending vehicle traveling at 50 mph that overtakes and passes a receiving vehicle and an SUV that brake from 30 to 0 mph. The line-of-sight was obstructed by the SUV during the first part of this test, and clear after the receiving vehicle passes the sending vehicle. The 3 lost packets highlighted in (1) of Trial 2 took place at a range of ~40 and is probably due to the obstructing SUV, although the loss of packets at that range was not repeated in Trials 1 and 3. There was a lost packet in Trial 1 at a range of ~90m. The packet loss at this range happened in other tests and is likely due to multipath, as shown in Test 1-20. Overall, 99.7 percent of the packets sent during the test were received.

Figure 101. Test Number 2-32-2 Results

Test Number:	**2-32-2**	**Ambient Weather Conditions:**	**Sunny**
Trace File Name:	**080703_2_32_2.trace***	**Sending Vehicle Model/Make:**	**Buick LeSabre**
Date Collected:	**August 7th, 2003**	**Receiving Vehicle Model/Make:**	**Buick LeSabre**
Files Resident With Whom:	**Jim Bauer**	**Antenna Type Used:**	**Standard**
Operating System Used:	**Linux**	**VBC Obstacle Vehicle #1 Model/Make:**	**GMC Envoy**
Software Level Used:	**Version 2.3**	**VBC Obstacle Vehicle #2 Model/Make:**	**N/A**



5.1.31 Test Scenario 2-33

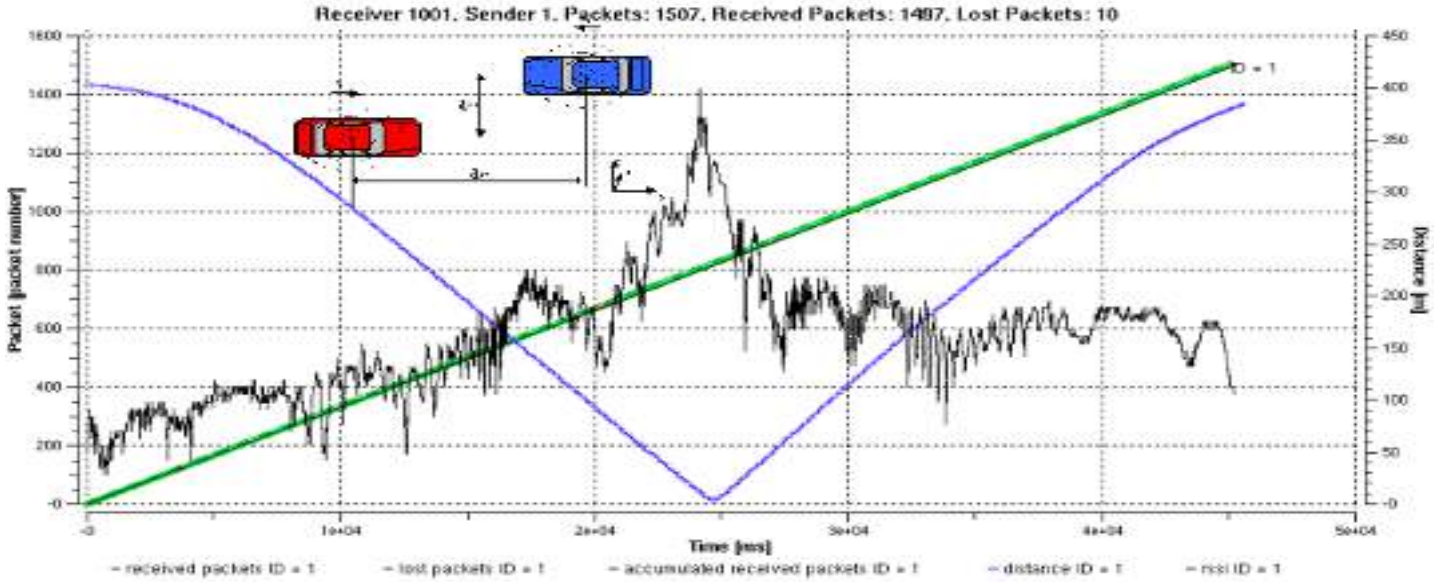
Test Scenario	**2-33**
Relevant Applications	Pre-Crash Sensing for Co-op Collision Mitigation
Velocity of Receiving Antenna (miles/hour)	25
Distance Between Antennas (meters)	< 50
Lateral Offset to Broadcast Antenna (meters)	4
Velocity of Sending Antenna (miles/hour)	25
Angle Between Vehicle 1 & Vehicle 2 (degrees)	180
Update Rate (milliseconds)	20
Transmitter Power Level (%)	100
Packet Size (bytes)	400
Path Obstructions	None
Vehicle Obstructions	None
Road Class	Test Track
Traffic Conditions	N/A
Other Effects	None
Vehicle-Class of Cut-In Vehicle	N/A

Table 56. Test Scenario 2-33

Test Comments: This test considers a receiving vehicle traveling at ~25 mph that approaches and passes a sending vehicle traveling at ~25 mph in the opposite direction. While this test was essentially conducted before (scenario 2-26), it was repeated in this context at an update rate of 20ms to be consistent with the safety requirements of Task 3. In this particular test, there was a reasonably clear line-of-sight, however there was a significant amount of clutter in the form of parked cars and trees along the side of the route. There were no more than a few packets lost in any of the runs, and they may have merely been due to the roadside clutter.

Figure 102. Test Number 3-33 Results

Test Number	**2-33**	Ambient Weather Conditions:	**Light Rain**
Trace File Name:	**Test_2_33_*.***	Sending Vehicle Model/Make:	**Camry**
Date Collected:	**March 30, 2004**	Receiving Vehicle Model/Make:	**Taurus**
Files Resident With Whom:	**Jim McBride**	Antenna Type Used:	**Standard**
Operating System Used:	**Linux**	VSC Obstacle Vehicle #1 Model/Make:	**N/A**
Software Level Used:	**V3.0 – B3**	VSC Obstacle Vehicle #2 Model/Make:	**N/A**



6 Stationary Vehicle Communications

6.1 Test Scenarios

6.1.1 Test Scenario 3-1

Test Scenario	**3-1**
Relevant Applications	Traffic Signal Violation Warning Left-Turn Assistant Stop Sign Movement Assistant
Velocity of Receiving Antenna (miles/hour)	0
Distance Between Antennas (meters)	10
Lateral Offset to Broadcast Antenna (meters)	0
Velocity of Sending Antenna (miles/hour)	0
Angle Between Vehicle 1 & Vehicle 2 (degrees)	N/A
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	200
Path Obstructions	None
Vehicle Obstructions	None
Road Class	Parking Lot
Traffic Conditions	Light
Other Effects	None
Vehicle-Class of Cut-In Vehicle	None

Table 57. Test Scenario 3-1

Test Comments: Two vehicles separated by ~20m. There was a clear line-of-sight and no packets were lost. Even though the vehicles were standing still, there was a distance variance of 0.5m (19.65m to 19.15m) in the GPS readings.

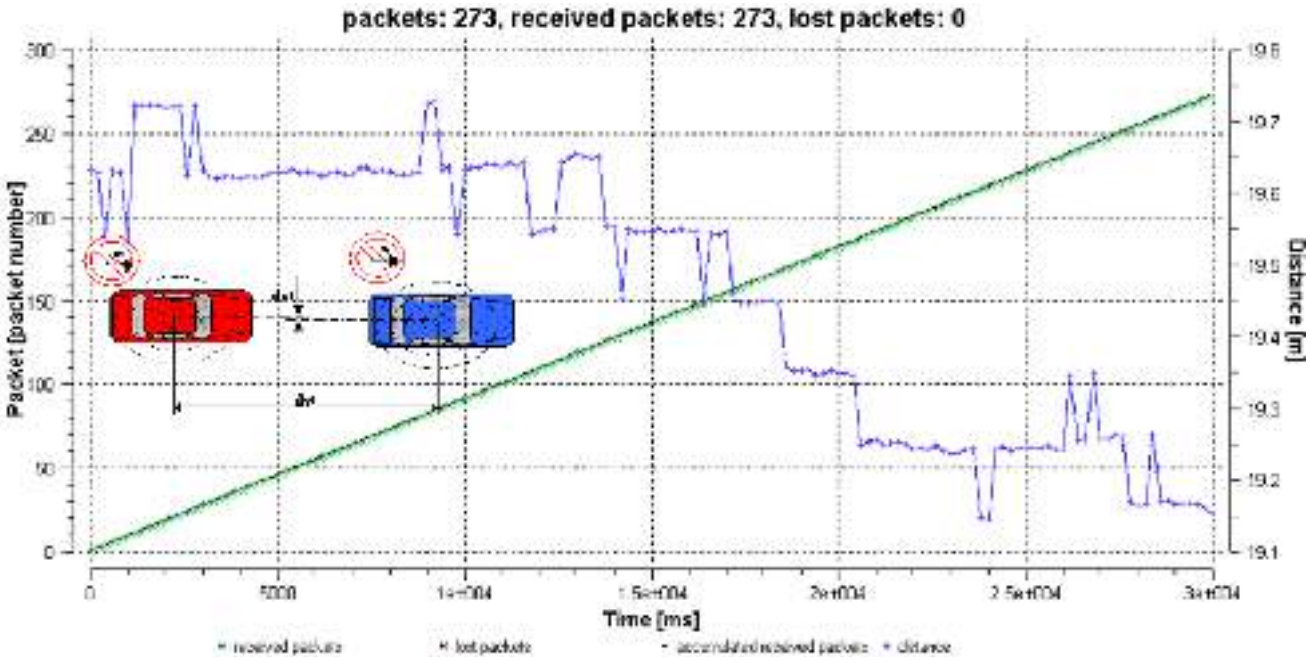
Figure 103. Test Number 3-1 Results

Test Number 3-1
Trace File Name: test3-1_1_072503.trace*
Date Collected: July 25th, 2003
Files Resident With Whom: Chu-Hao Lee

Ambient Weather Conditions: Sunny
Sending Vehicle Model/Make: VW Passat
Receiving Vehicle Model/Make: BMW 330
Antenna Type Used: Standard

Operating System Used: Linux
Software Level Used: 2.3

VRC Obstacle Vehicle #1 Model/Make: N/A
VRC Obstacle Vehicle #2 Model/Make: N/A



6.1.2 Test Scenario 3-2

Test Scenario	**3-2**
Relevant Applications	Traffic Signal Violation Warning Left-Turn Assistant Stop Sign Movement Assistant
Velocity of Receiving Antenna (miles/hour)	0
Distance Between Antennas (meters)	50
Lateral Offset to Broadcast Antenna (meters)	0
Velocity of Sending Antenna (miles/hour)	0
Angle Between Vehicle 1 & Vehicle 2 (degrees)	N/A
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	200
Path Obstructions	None
Vehicle Obstructions	None
Road Class	Parking Lot
Traffic Conditions	Light
Other Effects	None
Vehicle-Class of Cut-In Vehicle	None

Table 58. Test Scenario 3-2

Test Comments: Two vehicles separated by ~46m. There was a clear line-of-sight and no packets were lost. Even though the vehicles were standing still, there was a distance variance of 0.8m (46.5m to 45.7m) in the GPS readings.

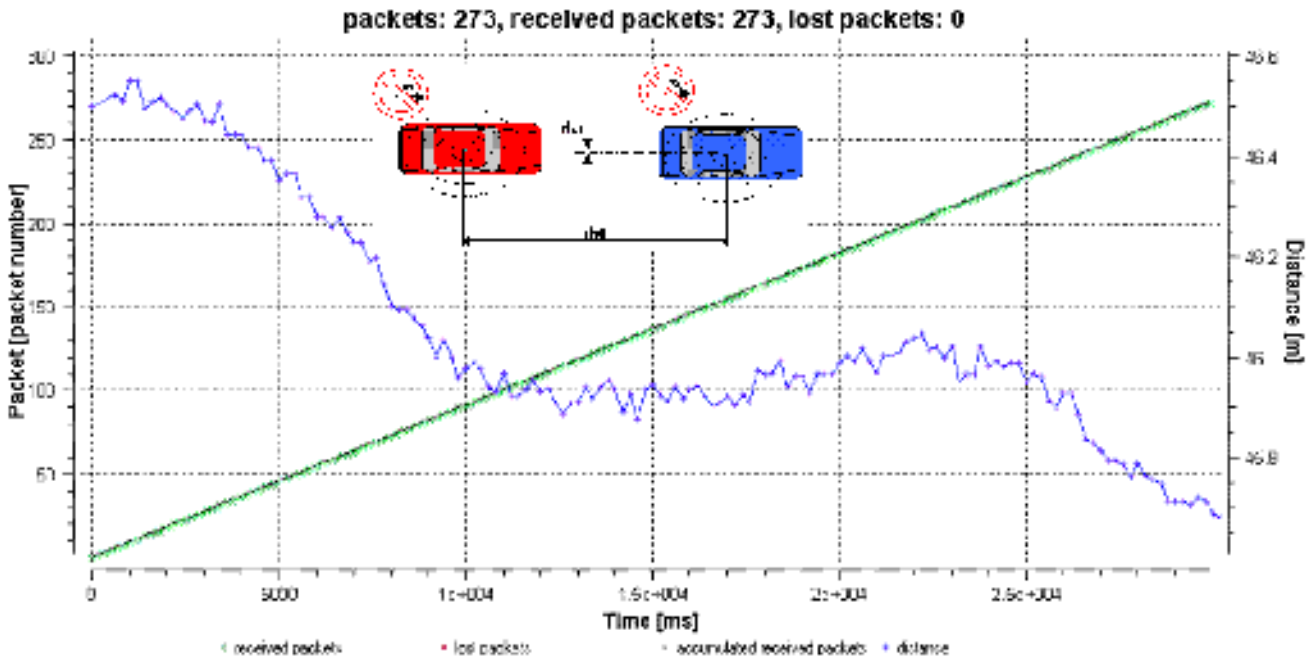
Figure 104. Test Number 3-2 Results

Test Number 3-2
Trace File Name: test3-2_2_072503.trace*
Date Collected: July 25th, 2003
Files Resident With Whom: Chu-Hao Lee

Ambient Weather Conditions: Sunny
Sending Vehicle Model/Make: VW Passat
Receiving Vehicle Model/Make: BMW 330
Antenna Type Used: Standard

Operating System Used: Linux
Software Level Used: 2.3

VSC Obstacle Vehicle #1 Model/Make: N/A
VSC Obstacle Vehicle #2 Model/Make: N/A



6.1.3 Test Scenario 3-3

Test Scenario	**3-3**
Relevant Applications	Traffic Signal Violation Warning Left-Turn Assistant Stop Sign Movement Assistant
Velocity of Receiving Antenna (miles/hour)	0
Distance Between Antennas (meters)	150
Lateral Offset to Broadcast Antenna (meters)	0
Velocity of Sending Antenna (miles/hour)	0
Angle Between Vehicle 1 & Vehicle 2 (degrees)	N/A
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	200
Path Obstructions	None
Vehicle Obstructions	None
Road Class	Parking Lot
Traffic Conditions	Light
Other Effects	None
Vehicle-Class of Cut-In Vehicle	None

Table 59. Test Scenario 3-3

Test Comments: Two vehicles separated by ~148m. There was a clear line-of-sight and no packets were lost. Even though the vehicles were standing still, there was a distance variance of 1.7m (147.1m to 148.8m) in the GPS readings.

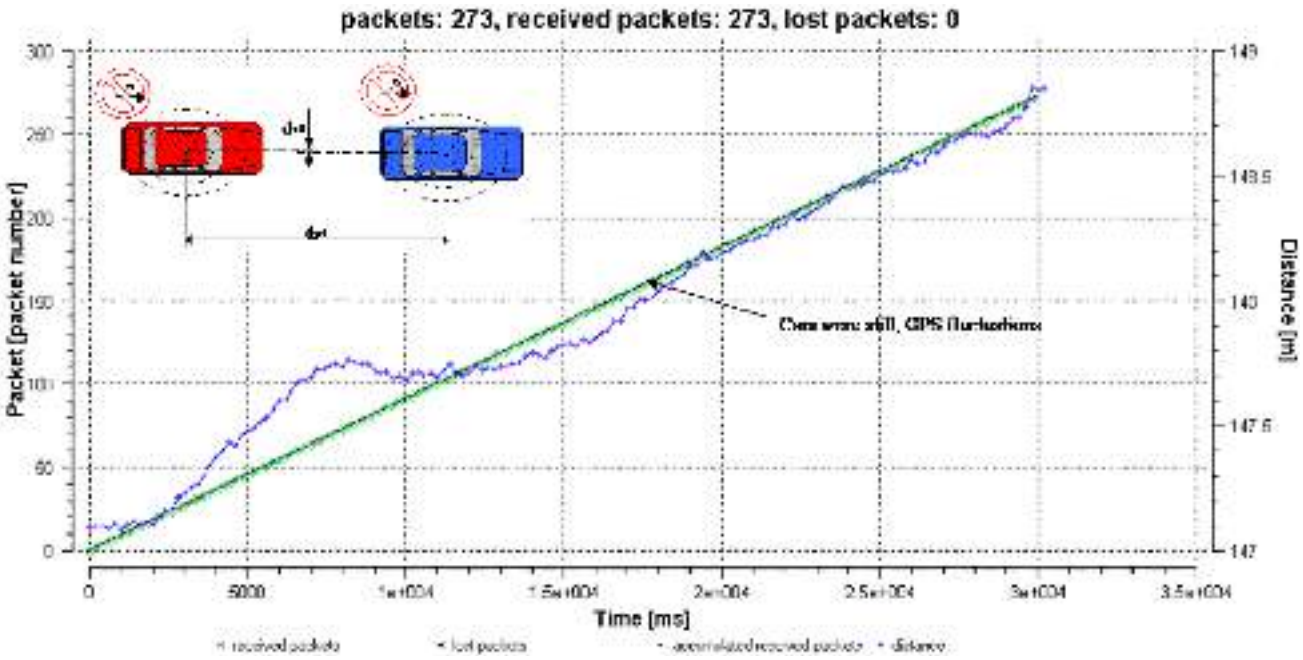
Figure 105. Test Number 3-3 Results

Test Number 3-3
Trace File Name: test3-3_2_072503.trace*
Date Collected: July 25th, 2003
Files Resident With Whom: Chu-Hao Lee

Ambient Weather Conditions: Sunny
Sending Vehicle Model/Make: VW Passat
Receiving Vehicle Model/Make: BMW 330
Antenna Type Used: Standard

Operating System Used: Linux
Software Level Used: 2.3

VSC Obstacle Vehicle #1 Model/Make: N/A
VSC Obstacle Vehicle #2 Model/Make: N/A



6.1.4 Test Scenario 3-4

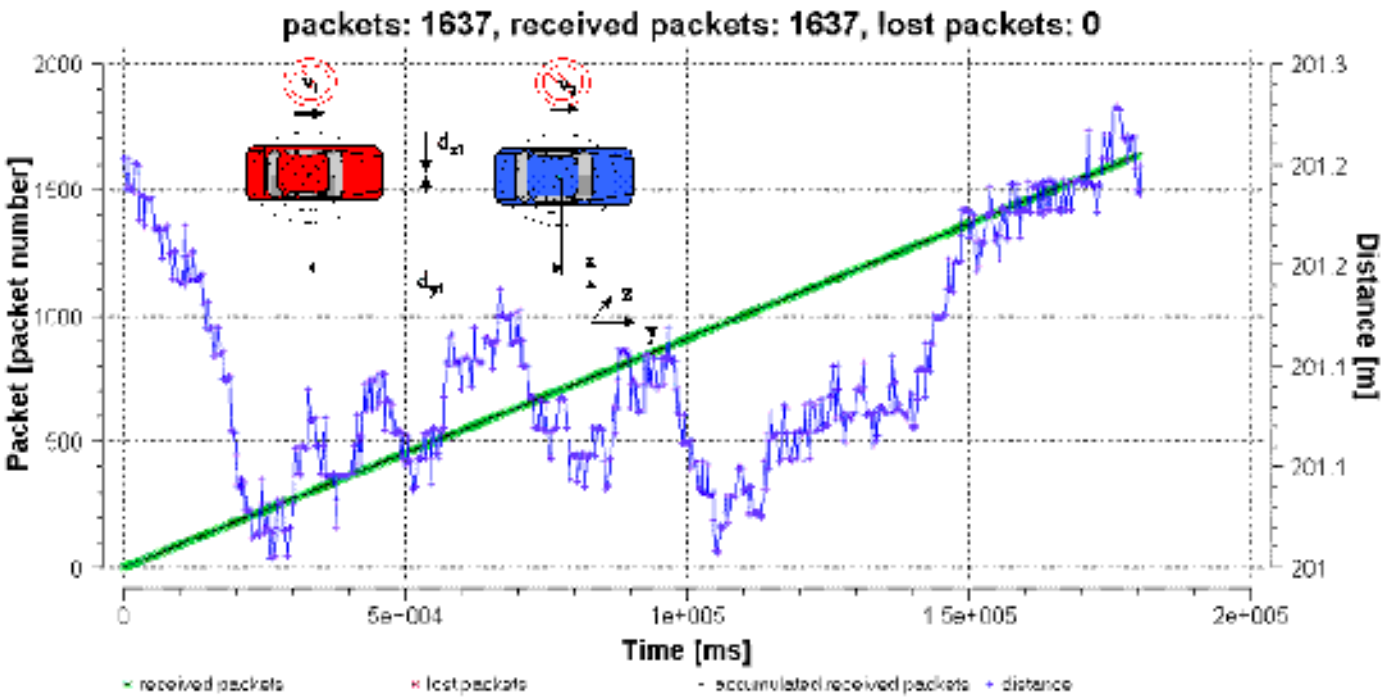
Test Scenario	**3-4**
Relevant Applications	Traffic Signal Violation Warning Left-Turn Assistant Stop Sign Movement Assistant
Velocity of Receiving Antenna (miles/hour)	0
Distance Between Antennas (meters)	200
Lateral Offset to Broadcast Antenna (meters)	0
Velocity of Sending Antenna (miles/hour)	0
Angle Between Vehicle 1 & Vehicle 2 (degrees)	N/A
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	200
Path Obstructions	None
Vehicle Obstructions	None
Road Class	Parking Lot
Traffic Conditions	Light
Other Effects	None
Vehicle-Class of Cut-In Vehicle	None

Table 60. Test Scenario 3-4

Test Comments: In this test, the RSU (GMC Envoy) sends messages (200 bytes) every 100 msec. Both vehicles are stationary and about 200 m apart. Both units are constantly in a clear line-of-sight. The communication link was very reliable since in all trials of this test, no packets were dropped.

Figure 106. Test Number 3-4 Results

Test Number:	**3-4**	**Ambient Weather Conditions:**	**Sunny**
Trace File Name:	**[illegible]_3_4_2.trace***	**Sending Vehicle Model/Make:**	**GMC Envoy**
Date Collected:	**August 14, 2003**	**Receiving Vehicle Model/Make:**	**Buick LeSabre**
Files Resident With Whom:	**F. Ahmed-Zaid**	**Antenna Type Used:**	**Standard**
Operating System Used:	**Linux**	**VSC Chassis Vehicle #1 Model/Make:**	**N/A**
Software Level Used:	**V2.3 (8-July-03)**	**VSC Chassis Vehicle #2 Model/Make:**	**N/A**



6.1.5 Test Scenario 3-5

Test Scenario	**3-5**
Relevant Applications	Traffic Signal Violation Warning Left-Turn Assistant Stop Sign Movement Assistant
Velocity of Receiving Antenna (miles/hour)	0
Distance Between Antennas (meters)	250
Lateral Offset to Broadcast Antenna (meters)	0
Velocity of Sending Antenna (miles/hour)	0
Angle Between Vehicle 1 & Vehicle 2 (degrees)	N/A
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	200
Path Obstructions	None
Vehicle Obstructions	None
Road Class	Parking Lot
Traffic Conditions	Light
Other Effects	None
Vehicle-Class of Cut-In Vehicle	None

Table 61. Test Scenario 3-5

Test Comments: Two vehicles separated by ~210m. There was a clear line-of-sight and no packets were lost. One of the vehicles moved twice during the test and it's shown in the plot.

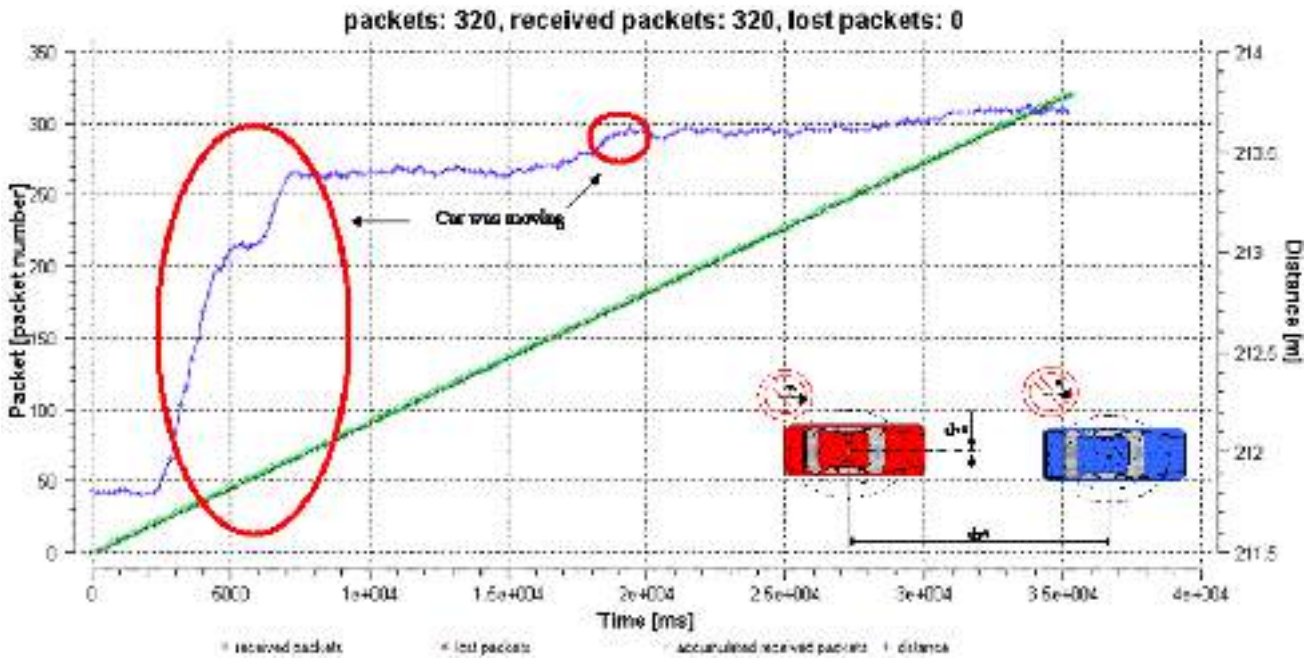
Figure 107. Test Number 3-5 Results

Test Number: 3-5
Trace File Name: test3-5_1_072803.trace*
Date Collected: July 28th, 2003
Files Resident With Whom: Chu-Hao Lee

Ambient Weather Conditions: Sunny
Sending Vehicle Model/Make: VW Passat
Receiving Vehicle Model/Make: BMW 330
Antenna Type Used: Standard

Operating System Used: Linux
Software Level Used: 2.3

VIC Obstacle Vehicle #1 Model/Make: N/A
VIC Obstacle Vehicle #2 Model/Make: N/A



6.1.6 Test Scenario 3-6

Test Scenario	**3-6**
Relevant Applications	Traffic Signal Violation Warning Left-Turn Assistant Stop Sign Movement Assistant
Velocity of Receiving Antenna (miles/hour)	0
Distance Between Antennas (meters)	300
Lateral Offset to Broadcast Antenna (meters)	0
Velocity of Sending Antenna (miles/hour)	0
Angle Between Vehicle 1 & Vehicle 2 (degrees)	N/A
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	200
Path Obstructions	None
Vehicle Obstructions	None
Road Class	Parking Lot
Traffic Conditions	Light
Other Effects	None
Vehicle-Class of Cut-In Vehicle	None

Table 62. Test Scenario 3-6

Test Comments: There wasn't a clear line-of-sight at the beginning (~350m) and it caused some packet loss. Once the vehicles were in line-of-sight (~300m) no packets were lost.

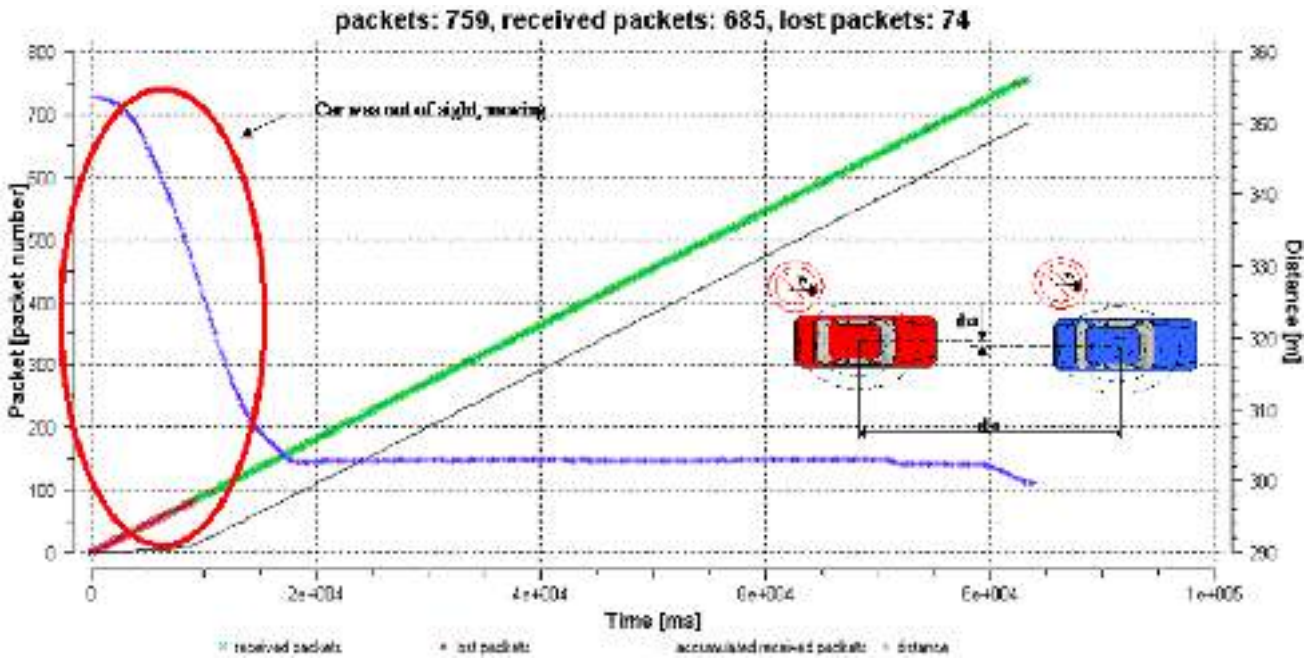
Figure 108. Test Number 3-6 Results

Test Number: 3-6
Trace File Name: test3-6_1_072803.trace*
Date Collected: July 28th, 2003
Files Resident With Whom: Chu-Hee Lee

Ambient Weather Conditions: Sunny
Sending Vehicle Model/Make: VW Passat
Receiving Vehicle Model/Make: BMW 330
Antenna Type Used: Standard

Operating System Used: Linux
Software Level Used: 2.3

VBC Obstacle Vehicle #1 Model/Make: N/A
VBC Obstacle Vehicle #2 Model/Make: N/A



6.1.7 Test Scenario 3-7

Test Scenario	3-7
Relevant Applications	Traffic Signal Violation Warning Left-Turn Assistant Stop Sign Movement Assistant
Velocity of Receiving Antenna (miles/hour)	0
Distance Between Antennas (meters)	10
Lateral Offset to Broadcast Antenna (meters)	0
Velocity of Sending Antenna (miles/hour)	0
Angle Between Vehicle 1 & Vehicle 2 (degrees)	N/A
Update Rate (milliseconds)	100
Transmitter Power Level (%)	50
Packet Size (bytes)	200
Path Obstructions	None
Vehicle Obstructions	None
Road Class	Parking Lot
Traffic Conditions	Light
Other Effects	None
Vehicle-Class of Cut-In Vehicle	None

Table 63. Test Scenario 3-7

Test Comments: Two vehicles separated by ~10m. There was a clear line-of-sight and no packets were lost. Even though the vehicles were standing still, there was a distance variance of ~2m. The sender used half power (50mW) and the average RSSI shown in the trace file but not in the graph was 34/60.

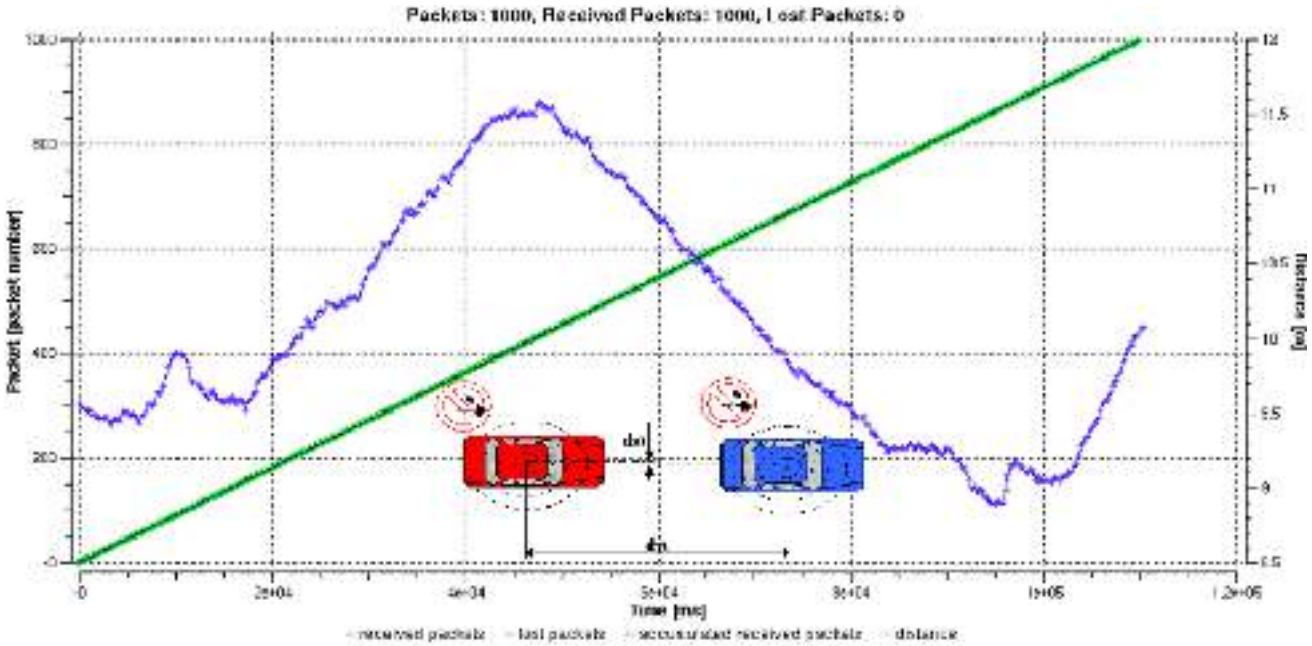
Figure 109. Test Number 3-7 Results

Test Number: 3-7
Trace File Name: test_3-7_1_2003-08-20.*
Date Collected: August 20th, 2003
Files Resident With Whom: Chu-Hee Lee

Ambient Weather Conditions: Sunny
Sending Vehicle Model/Make: VW Passat W8
Receiving Vehicle Model/Make: VW Passat
Antenna Type Used: Standard

Operating System Used: Linux
Software Level Used: 2.5

VSC Obstacle Vehicle #1 Model/Make: N/A
VSC Obstacle Vehicle #2 Model/Make: N/A



6.1.8 Test Scenario 3-8

Test Scenario	**3-8**
Relevant Applications	Traffic Signal Violation Warning Left-Turn Assistant Stop Sign Movement Assistant
Velocity of Receiving Antenna (miles/hour)	0
Distance Between Antennas (meters)	100
Lateral Offset to Broadcast Antenna (meters)	0
Velocity of Sending Antenna (miles/hour)	0
Angle Between Vehicle 1 & Vehicle 2 (degrees)	N/A
Update Rate (milliseconds)	100
Transmitter Power Level (%)	50
Packet Size (bytes)	200
Path Obstructions	None
Vehicle Obstructions	None
Road Class	Parking Lot
Traffic Conditions	Light
Other Effects	None
Vehicle-Class of Cut-In Vehicle	None

Table 64. Test Scenario 3-8

Test Comments: Two vehicles separated by ~100m. There was a clear line-of-sight and 11 packets got lost. Typically there is no packet loss in the setting with full transmission power (please refer to test 3-3 for comparison). Even though the vehicles were standing still, there was a distance variance of ~3m. The sender used half power (50mW) to transmit and the average RSSI shown in the trace file but not in the graph was 9/60.

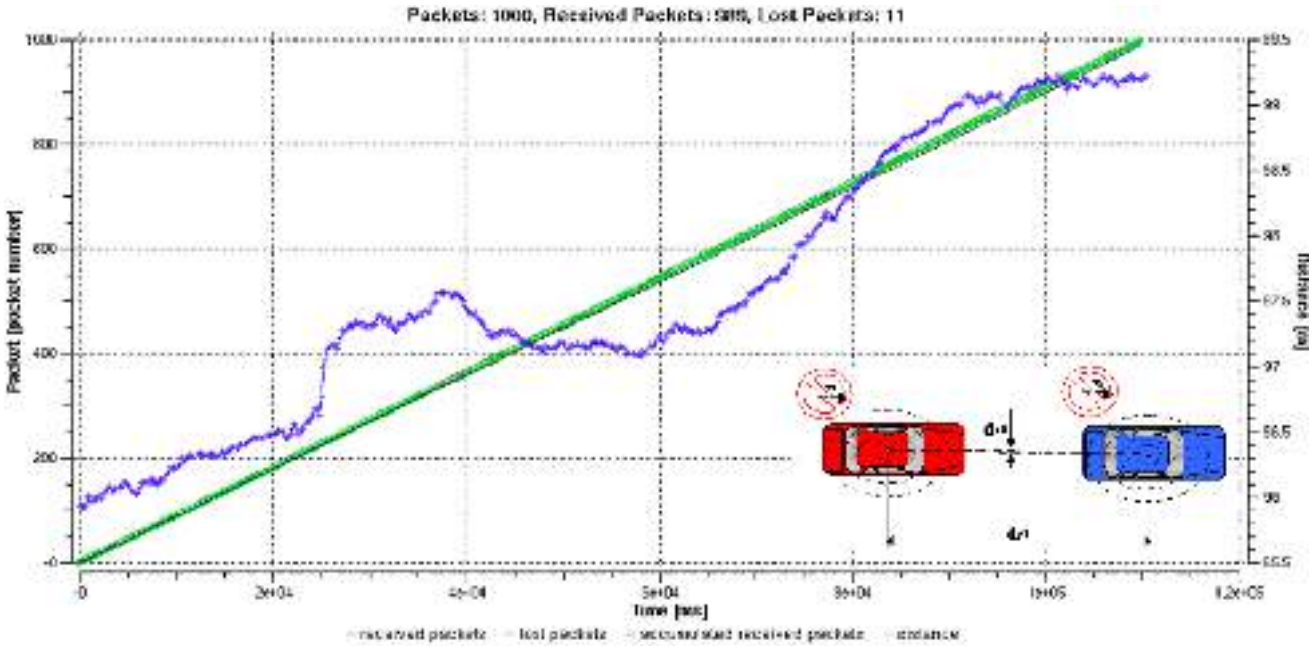
Figure 110. Test Number 3-8 Results

Test Number: 3-8
Trace File Name: test_3-8_1_2003-08-20.*
Date Collected: August 20th, 2003
Files Resident With Whom: Chu-Hee Lee

Ambient Weather Conditions: Sunny
Sending Vehicle Model/Make: VW Passat W8
Receiving Vehicle Model/Make: VW Passat
Antenna Type Used: Standard

Operating System Used: Linux
Software Level Used: 2.5

VSC Obstacle Vehicle #1 Model/Make: N/A
VSC Obstacle Vehicle #2 Model/Make: N/A



6.1.9 Test Scenario 3-9

Test Scenario	**3-9**
Relevant Applications	Traffic Signal Violation Warning Left-Turn Assistant Stop Sign Movement Assistant
Velocity of Receiving Antenna (miles/hour)	0
Distance Between Antennas (meters)	10
Lateral Offset to Broadcast Antenna (meters)	0
Velocity of Sending Antenna (miles/hour)	0
Angle Between Vehicle 1 & Vehicle 2 (degrees)	N/A
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	200
Path Obstructions	None
Vehicle Obstructions	Sustained
Road Class	Parking Lot
Traffic Conditions	Light
Other Effects	None
Vehicle-Class of Cut-In Vehicle	SUV

Table 65. Test Scenario 3-9

Test Comments: Sending and receiving vehicles were separated by ~10m. A blocking vehicle (an SUV) was in between but no packets were lost during the test. The distance based on GPS data fluctuated from ~9m to ~10m.

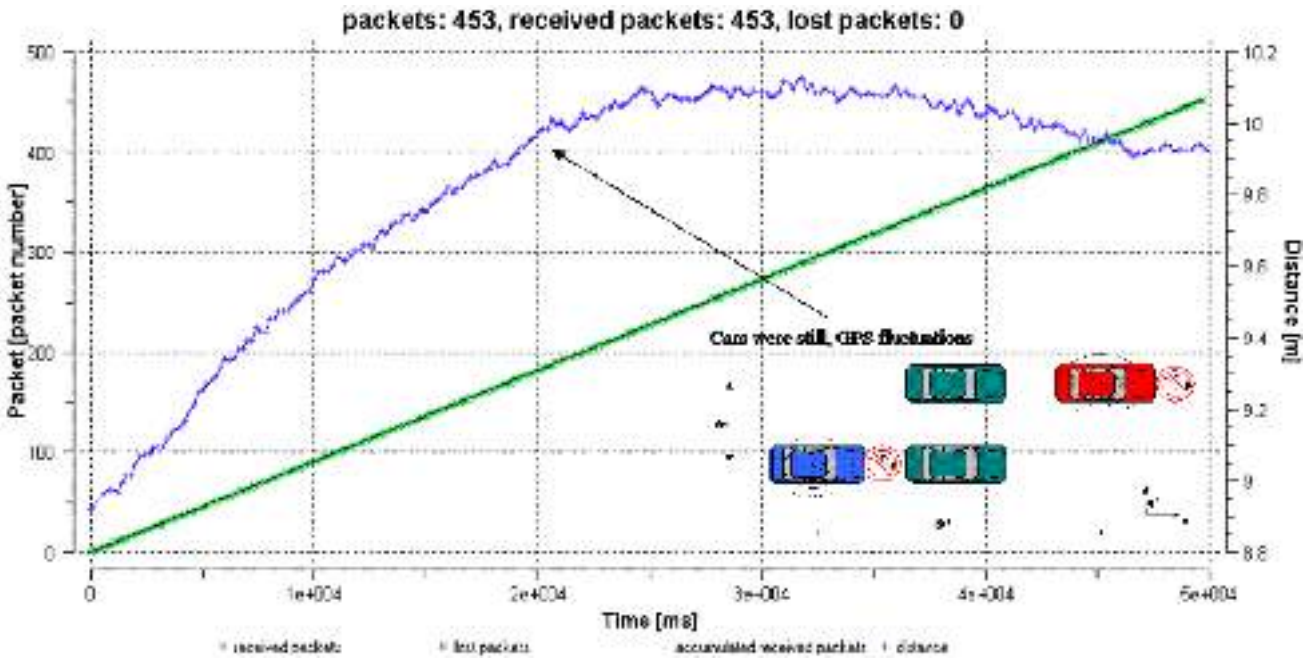
Figure 111. Test Number 3-9 Results

Test Number: 3-9
Trace File Name: test3-9_1_072803.trace*
Date Collected: July 28th, 2003
Files Resident With Whom: Chu-Hao Lee

Ambient Weather Conditions: Sunny
Sending Vehicle Model/Make: VW Passat
Receiving Vehicle Model/Make: BMW 330
Antenna Type Used: Standard

Operating System Used: Linux
Software Level Used: 2.3

VSC Obstacle Vehicle #1 Model/Make: Jeep SUV
VSC Obstacle Vehicle #2 Model/Make: N/A



6.1.10 Test Scenario 3-10

Test Scenario	**3-10**
Relevant Applications	Traffic Signal Violation Warning Left-Turn Assistant Stop Sign Movement Assistant
Velocity of Receiving Antenna (miles/hour)	0
Distance Between Antennas (meters)	100
Lateral Offset to Broadcast Antenna (meters)	0
Velocity of Sending Antenna (miles/hour)	0
Angle Between Vehicle 1 & Vehicle 2 (degrees)	N/A
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	200
Path Obstructions	None
Vehicle Obstructions	Sustained
Road Class	Parking Lot
Traffic Conditions	Light
Other Effects	None
Vehicle-Class of Cut-In Vehicle	SUV

Table 66. Test Scenario 3-10

Test Comments: Sending and receiving vehicles were separated by ~76m. A blocking vehicle (an SUV) was in between but no packets were lost during the test. The distance based on GPS data fluctuated from ~74m to ~77m.

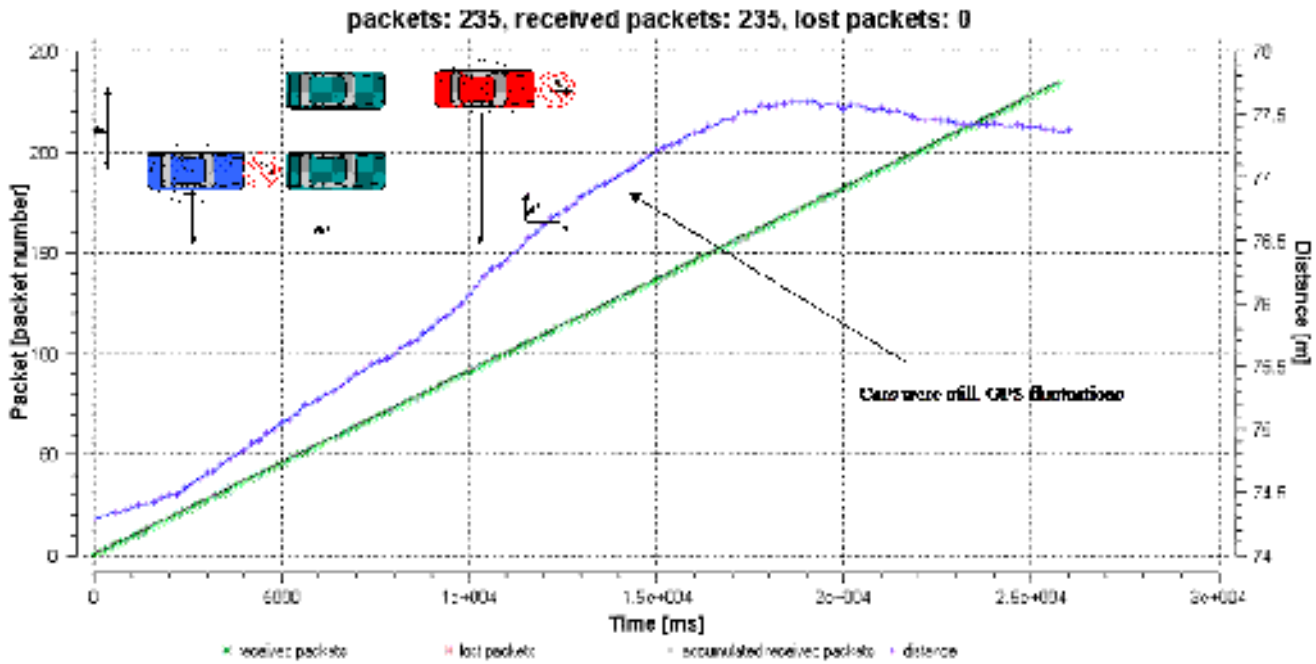
Figure 112. Test Number 3-10 Results

Test Number: 3-10
Trace File Name: test3-10_1_072803.trace*
Date Collected: July 28th, 2003
Files Resident With Whom: Chu-Hee Lee

Ambient Weather Conditions: Sunny
Sending Vehicle Model/Make: VW Passat
Receiving Vehicle Model/Make: BMW 330
Antenna Type Used: Standard

Operating System Used: Linux
Software Level Used: 2.3

VSC Obstacle Vehicle #1 Model/Make: Jeep SUV
VSC Obstacle Vehicle #2 Model/Make: N/A



6.1.11 Test Scenario 3-11

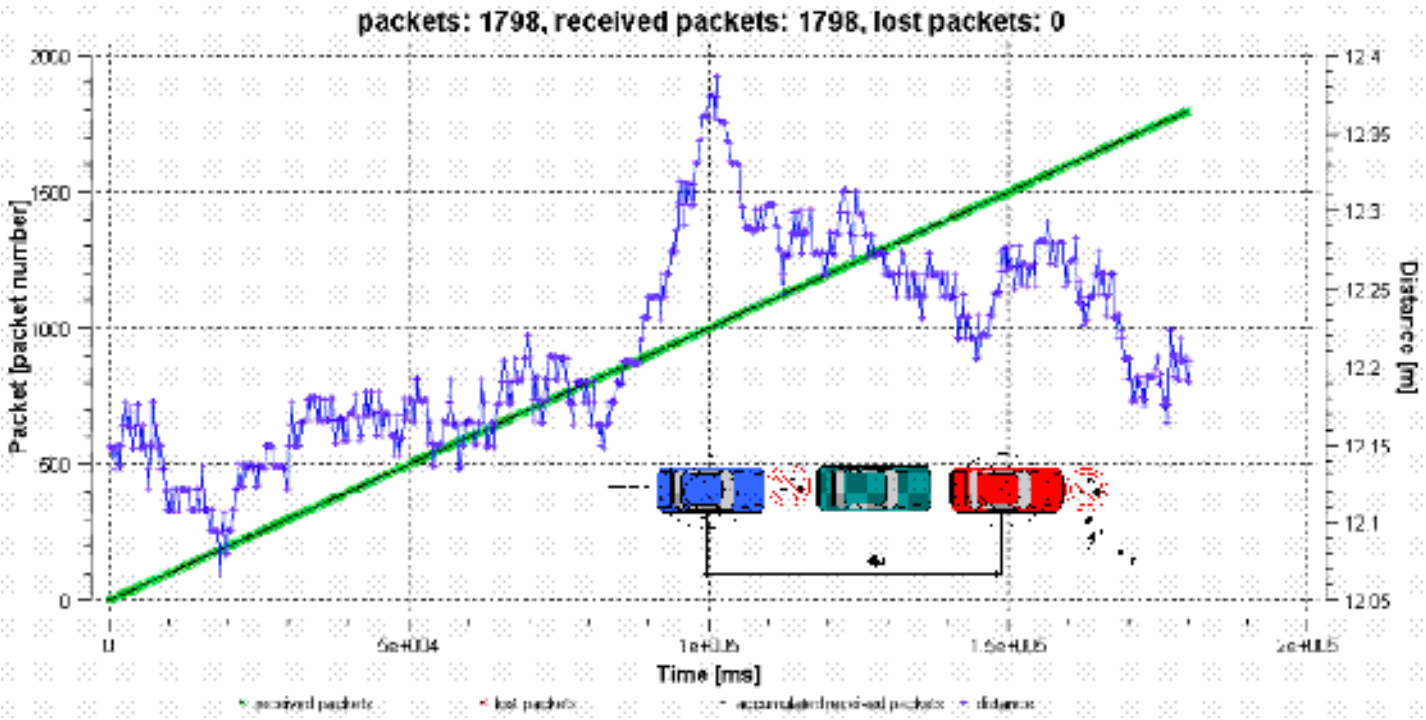
Test Scenario	**3-11**
Relevant Applications	Traffic Signal Violation Warning Left-Turn Assistant Stop Sign Movement Assistant
Velocity of Receiving Antenna (miles/hour)	0
Distance Between Antennas (meters)	10
Lateral Offset to Broadcast Antenna (meters)	0
Velocity of Sending Antenna (miles/hour)	0
Angle Between Vehicle 1 & Vehicle 2 (degrees)	N/A
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	200
Path Obstructions	None
Vehicle Obstructions	Sustained
Road Class	Test Track
Traffic Conditions	Light
Other Effects	None
Vehicle-Class of Cut-In Vehicle	SUV

Table 67. Test Scenario 3-11

Test Comments: This test was done in MS Windows. The intercepting vehicle was a Chevy Suburban SUV. There was no loss of reception due to the SUV interception. No packets were lost in all trials of this test.

Figure 113. Test Number 3-11 Results

Test Number	**3-11**	**Ambient Weather Conditions:**	**Mostly Sunny**
Trace File Name:	**060503_3_11_2.trace***	**Sending Vehicle Model/Make:**	**Buick LeSabre**
Date Collected:	**June 5th, 2003**	**Receiving Vehicle Model/Make:**	**Buick LeSabre**
Files Resident With Whom:	**H. Krishnan**	**Antenna Type Used:**	**Standard**
Operating System Used:	**Windows XP**	**VSC Obstacle Vehicle #1 Model/Make:**	**Chevy Suburban**
Software Level Used:	**2.4a beta (27-Feb-03)**	**VSC Obstacle Vehicle #2 Model/Make:**	**N/A**



6.1.12 Test Scenario 3-12

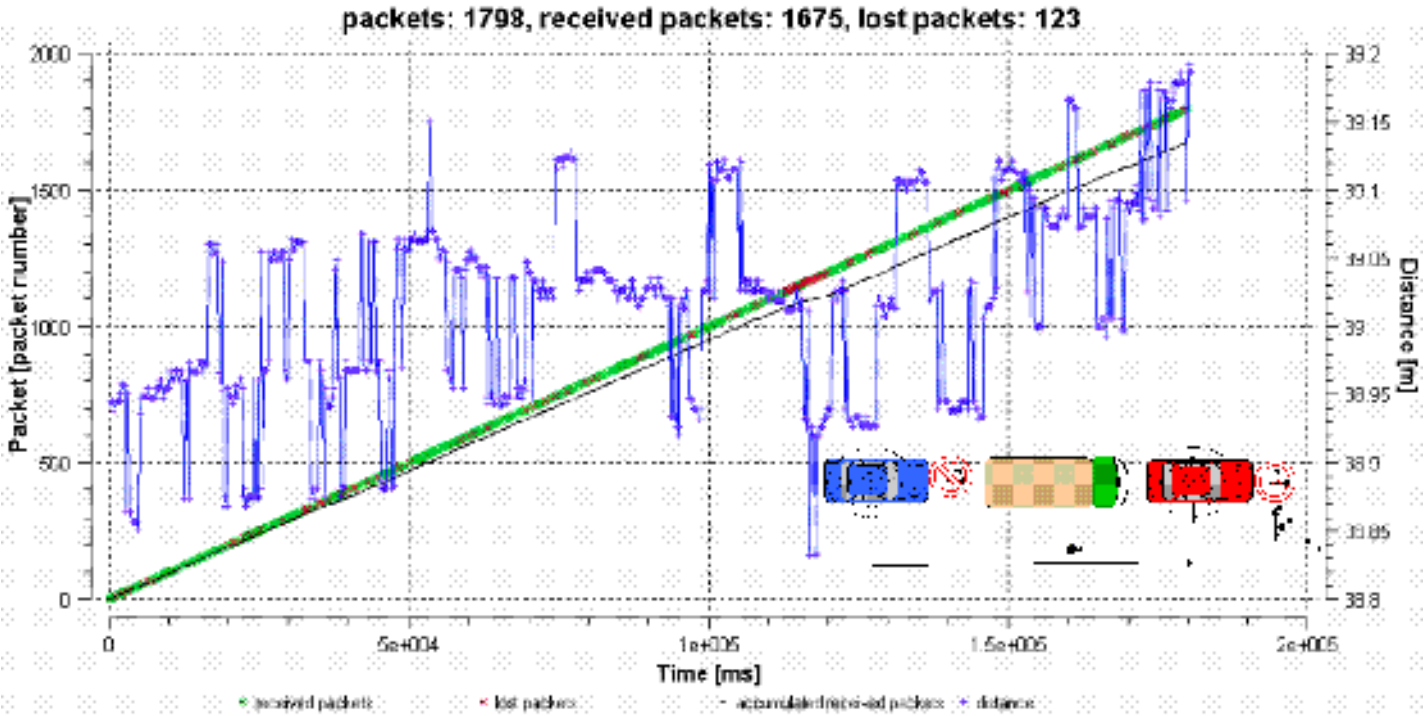
Test Scenario	**3-12**
Relevant Applications	Traffic Signal Violation Warning Left-Turn Assistant Stop Sign Movement Assistant
Velocity of Receiving Antenna (miles/hour)	0
Distance Between Antennas (meters)	40
Lateral Offset to Broadcast Antenna (meters)	0
Velocity of Sending Antenna (miles/hour)	0
Angle Between Vehicle 1 & Vehicle 2 (degrees)	N/A
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	200
Path Obstructions	None
Vehicle Obstructions	Sustained
Road Class	Test Track
Traffic Conditions	Light
Other Effects	None
Vehicle-Class of Cut-In Vehicle	Truck

Table 68. Test Scenario 3-12

Test Comments: This test was done in MS Windows. The intercepting vehicle was a Large Truck. There were frequent losses of reception due to the large truck interception. The packet loss of less than 10 percent was found in all trials of this test.

Figure 114. Test Number 3-12 Results

Test Number:	3-12	Ambient Weather Conditions:	Mostly Sunny
Trace File Name:	060503_3_12_4.trace*	Sending Vehicle Model/Make:	Buick LeSabre
Date Collected:	June 5th, 2003	Receiving Vehicle Model/Make:	Buick LeSabre
Files Resident With Whom:	H. Krishnan	Antenna Type Used:	Standard
Operating System Used:	Windows XP	VSC Obstacle Vehicle #1 Model/Make:	Large Truck
Software Level Used:	2.4a beta (27-Feb-03)	VSC Obstacle Vehicle #2 Model/Make:	N/A



6.1.13 Test Scenario 3-13

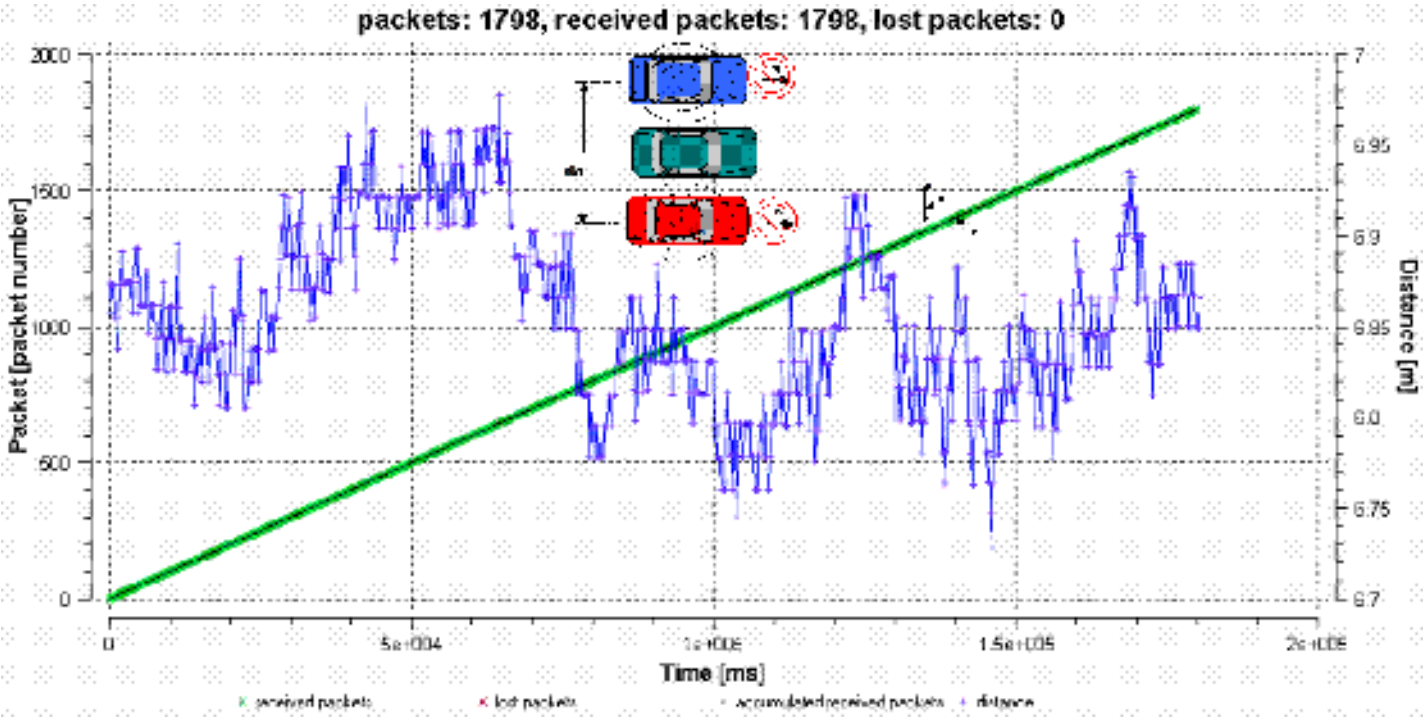
Test Scenario	**3-13**
Relevant Applications	Traffic Signal Violation Warning Left-Turn Assistant Stop Sign Movement Assistant
Velocity of Receiving Antenna (miles/hour)	0
Distance Between Antennas (meters)	0
Lateral Offset to Broadcast Antenna (meters)	8
Velocity of Sending Antenna (miles/hour)	0
Angle Between Vehicle 1 & Vehicle 2 (degrees)	N/A
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	200
Path Obstructions	None
Vehicle Obstructions	Sustained
Road Class	Test Track
Traffic Conditions	Light
Other Effects	None
Vehicle-Class of Cut-In Vehicle	SUV

Table 69. Test Scenario 3-13

Test Comments: This test was done in MS Windows. The intercepting vehicle was a Chevy Suburban SUV. There was no loss of reception due to the SUV interception. No packets were lost in all trials of this test.

Figure 115. Test Number 3-13 Results

Test Number	3-13	Ambient Weather Conditions:	Mostly Sunny
Trace File Name:	060503_3_13_1.4rscr*	Sending Vehicle Model/Make:	Buick LeSabre
Date Collected:	June 5th, 2003	Receiving Vehicle Model/Make:	Buick LeSabre
Files Resident With Whom:	H. Krishnan	Antenna Type Used:	Standard
Operating System Used:	Windows XP	VRC Obstacle Vehicle #1 Model/Make:	Chevy Suburban
Software Level Used:	2.4a beta (27-Feb-03)	VRC Obstacle Vehicle #2 Model/Make:	N/A



6.1.14 Test Scenario 3-14

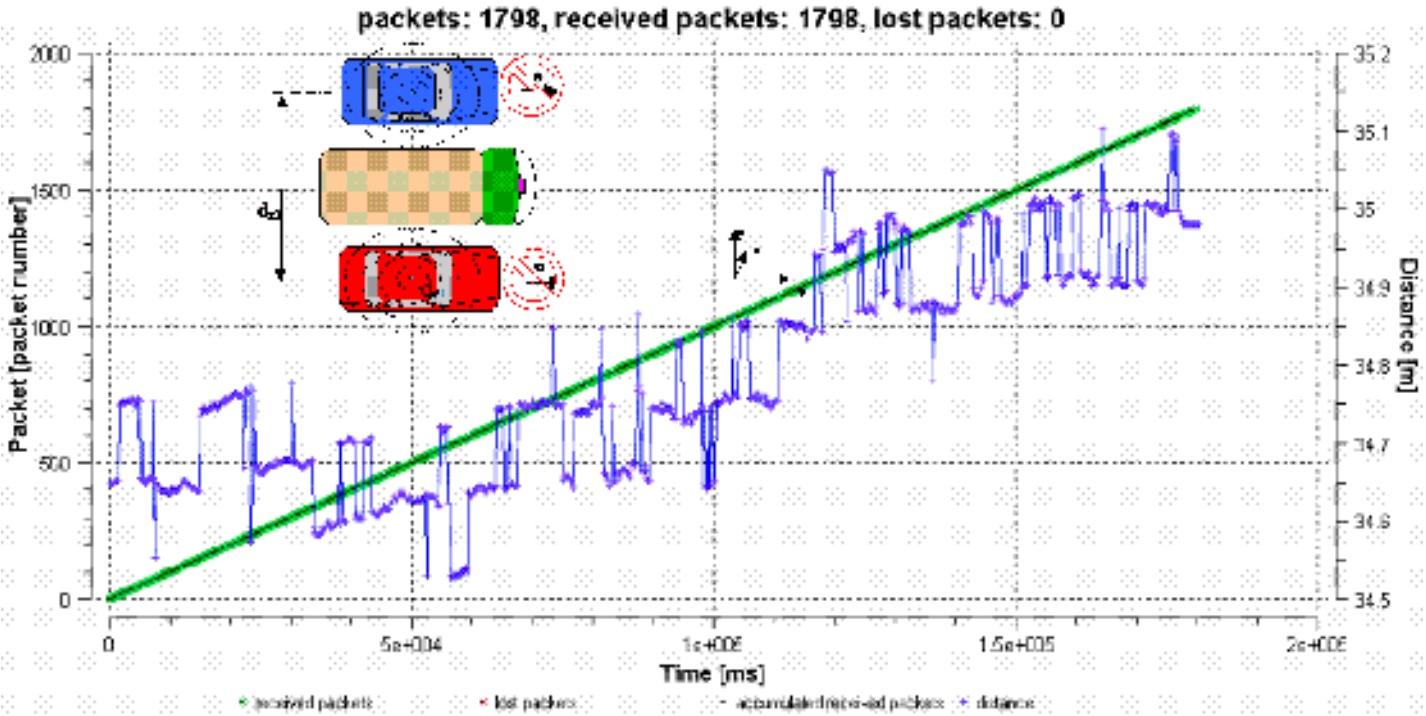
Test Scenario	**3-14**
Relevant Applications	Traffic Signal Violation Warning Left-Turn Assistant Stop Sign Movement Assistant
Velocity of Receiving Antenna (miles/hour)	0
Distance Between Antennas (meters)	0
Lateral Offset to Broadcast Antenna (meters)	8
Velocity of Sending Antenna (miles/hour)	0
Angle Between Vehicle 1 & Vehicle 2 (degrees)	N/A
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	200
Path Obstructions	None
Vehicle Obstructions	Sustained
Road Class	Test Track
Traffic Conditions	Light
Other Effects	None
Vehicle-Class of Cut-In Vehicle	Truck

Table 70. Test Scenario 3-14

Test Comments: This test was done in MS Windows. The intercepting vehicle was a Large Truck. There was no loss of reception due to the large truck interception. The phenomenon of no packet loss was found in several trials of this test.

Figure 116. Test Number 3-14 Results

Test Number:	3-14	Ambient Weather Conditions:	Mostly Sunny
Trace File Name:	060503_3_14_2.trace*	Sending Vehicle Model/Make:	Buick LeSabre
Date Collected:	June 5th, 2003	Receiving Vehicle Model/Make:	Buick LeSabre
Files Resident With Whom:	H. Krishnan	Antenna Type Used:	Standard
Operating System Used:	Windows XP	VSC Obstacle Vehicle #1 Model/Make:	Large Truck
Software Level Used:	2.4a beta (27-Feb-03)	VSC Obstacle Vehicle #2 Model/Make:	N/A



6.1.15 Test Scenario 3-15

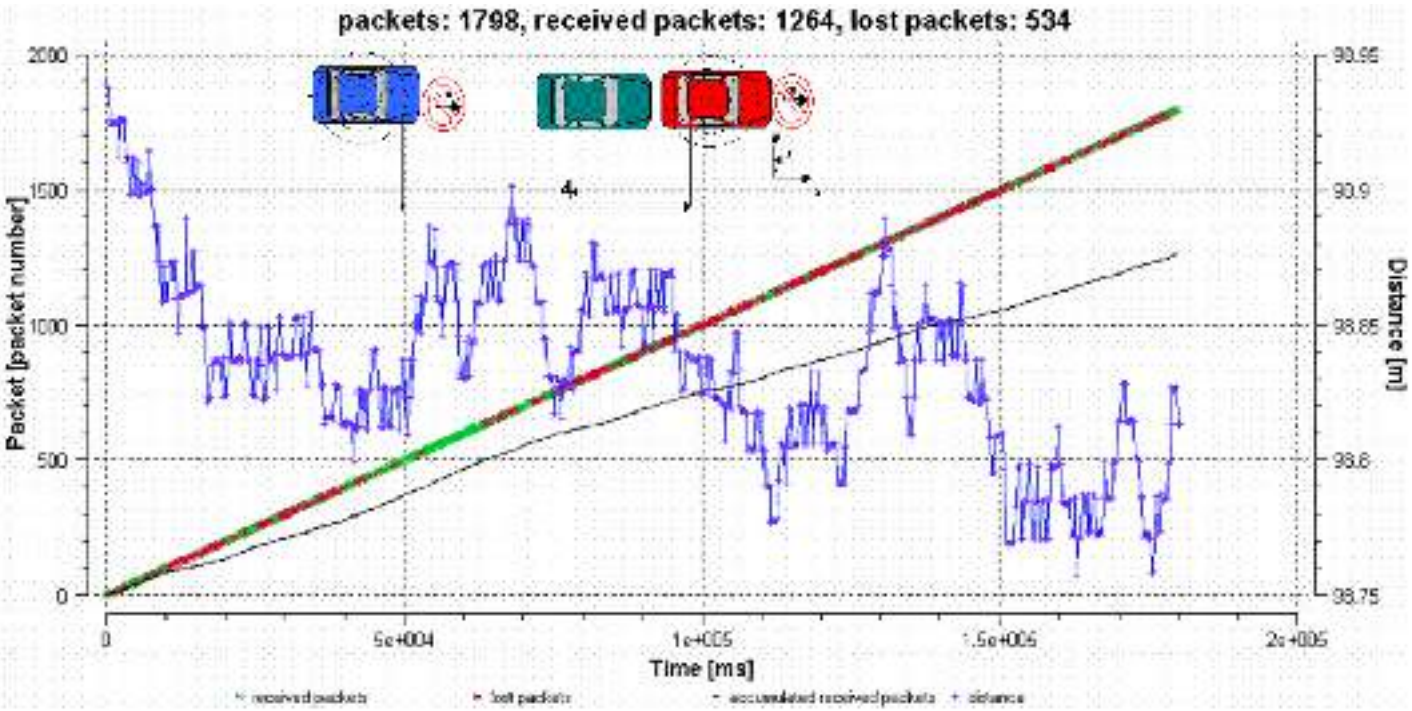
Test Scenario	**3-15**
Relevant Applications	Traffic Signal Violation Warning Left-Turn Assistant Stop Sign Movement Assistant
Velocity of Receiving Antenna (miles/hour)	0
Distance Between Antennas (meters)	100
Lateral Offset to Broadcast Antenna (meters)	0
Velocity of Sending Antenna (miles/hour)	0
Angle Between Vehicle 1 & Vehicle 2 (degrees)	N/A
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	200
Path Obstructions	None
Vehicle Obstructions	Sustained
Road Class	Test Track
Traffic Conditions	Light
Other Effects	None
Vehicle-Class of Cut-In Vehicle	SUV

Table 71. Test Scenario 3-15

Test Comments: This test was done in MS Windows. The intercepting vehicle was a Chevy Suburban SUV. There was significant loss of reception due to the SUV interception. The most significant packet loss was observed when the SUV was close to the front vehicle (receiver).

Figure 117. Test Number 3-15 Results

Test Number:	3-15	Ambient Weather Conditions:	Mostly Sunny
Trace File Name:	060503_3_15_1_trace*	Sending Vehicle Model/Make:	Buick LeSabre
Date Collected:	June 5th, 2003	Receiving Vehicle Model/Make:	Buick LeSabre
Files Resident With Whom:	H. Krishnan	Antenna Type Used:	Standard
Operating System Used:	Windows XP	VSC Obstacle Vehicle #1 Model/Make:	Chevy Suburban
Software Level Used:	2.4a beta (27-Feb-03)	VSC Obstacle Vehicle #2 Model/Make:	N/A



6.1.16 Test Scenario 3-16

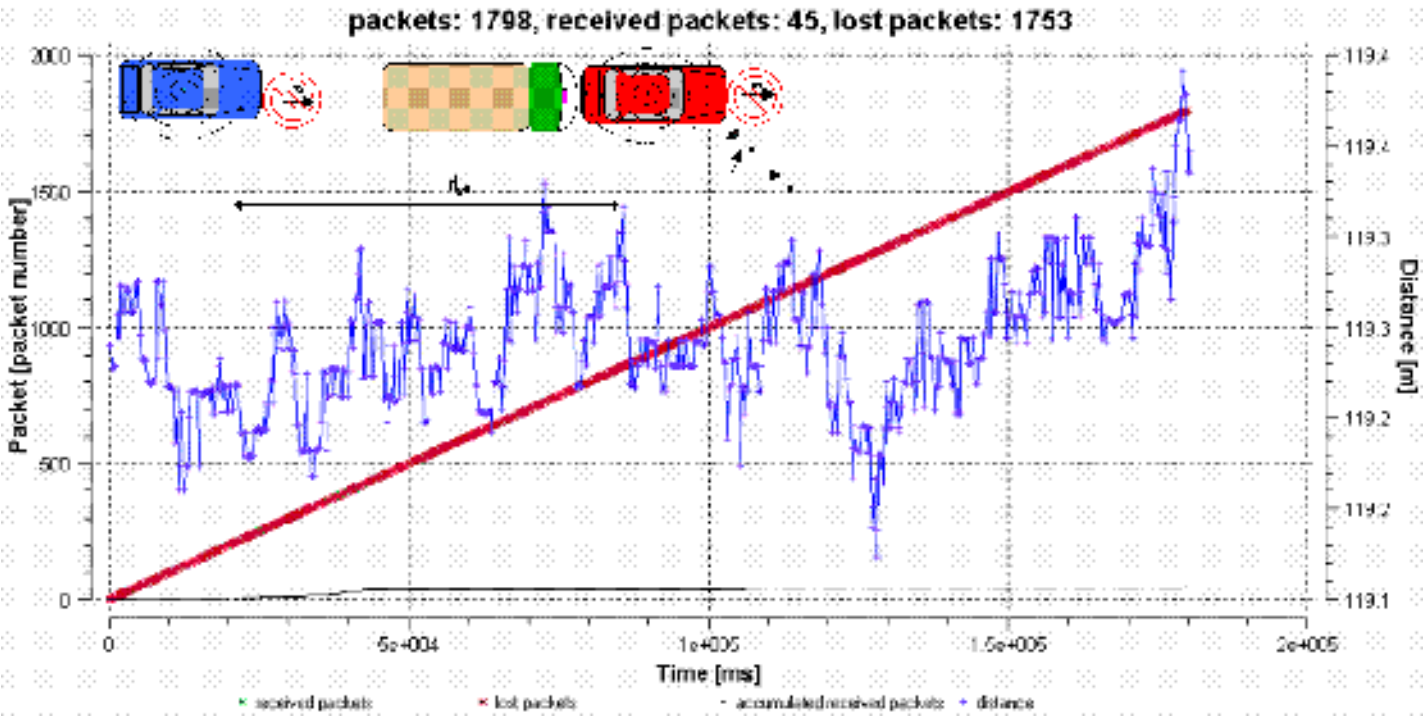
Test Scenario	**3-16**
Relevant Applications	Traffic Signal Violation Warning Left-Turn Assistant Stop Sign Movement Assistant
Velocity of Receiving Antenna (miles/hour)	0
Distance Between Antennas (meters)	100
Lateral Offset to Broadcast Antenna (meters)	0
Velocity of Sending Antenna (miles/hour)	0
Angle Between Vehicle 1 & Vehicle 2 (degrees)	N/A
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	200
Path Obstructions	None
Vehicle Obstructions	Sustained
Road Class	Test Track
Traffic Conditions	Light
Other Effects	None
Vehicle-Class of Cut-In Vehicle	Truck

Table 72. Test Scenario 3-16

Test Comments: This test was done in MS Windows. The intercepting vehicle was a Large Truck. There were very few packets that were received and the loss of reception due to the large truck interception was severe. The phenomenon of increased packet loss was found in all trials of this test and particularly when the truck was close to the front vehicle (receiver).

Figure 118. Test Number 3-16 Results

Test Number:	3-16	Ambient Weather Conditions:	Mostly Sunny
Trace File Name:	060503_3_16_1.trace*	Sending Vehicle Model/Make:	Buick LeSabre
Date Collected:	June 5th, 2003	Receiving Vehicle Model/Make:	Buick LeSabre
Files Resident With Whom:	H. Krishnan	Antenna Type Used:	Standard
Operating System Used:	Windows XP	VSC Obstacle Vehicle #1 Model/Make:	Large Truck
Software Level Used:	2.4a beta (27-Feb-03)	VSC Obstacle Vehicle #2 Model/Make:	N/A



6.1.17 Test Scenario 3-17

Test Scenario	**3-17**
Relevant Applications	Traffic Signal Violation Warning Left-Turn Assistant Stop Sign Movement Assistant
Velocity of Receiving Antenna (miles/hour)	0
Distance Between Antennas (meters)	< 100
Lateral Offset to Broadcast Antenna (meters)	8
Velocity of Sending Antenna (miles/hour)	0
Angle Between Vehicle 1 & Vehicle 2 (degrees)	0
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	400
Path Obstructions	None
Vehicle Obstructions	Sustained
Road Class	Test Track
Traffic Conditions	Light
Other Effects	None
Vehicle-Class of Cut-In Vehicle	SUV

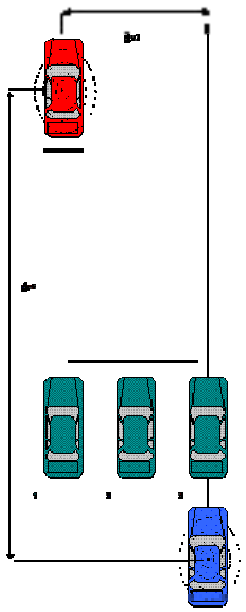
Table 73. Test Scenario 3-17

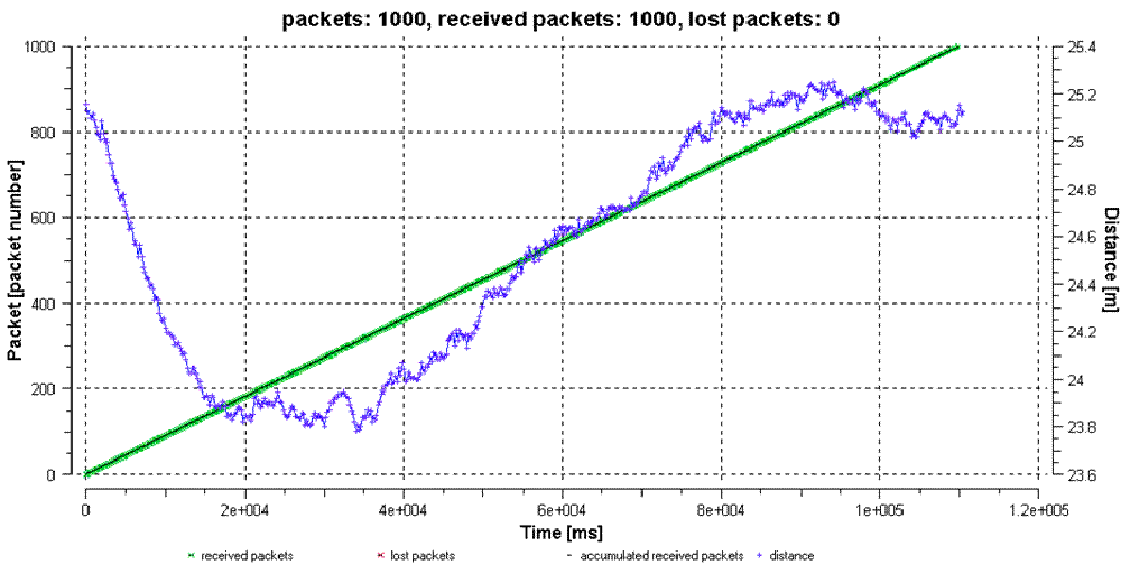
Test Comments: This test considers the effect of three side-by-side SUVs parked between a stationary sending and receiving vehicle. In Trial 1, the sender and receiver vehicles were positioned ~25m apart, and the obstacle vehicle was separated from the sender vehicle in the dy1 direction by ~5m. The line-of-sight was obstructed by Obstacle Vehicle #2. Overall, 100 percent of the packets sent during the test were received. Tests 1-27 and 1-28 were run to check this vehicle configuration under dynamic conditions.

Figure 73. Test Number 3-17-1 Results

Test Number:	3-17-1
Trace File Name:	082703_2_19_1_SUV.trace*
Date Collected:	August 27th, 2003
Files Resident With:	Jim Bauer
Operating System Used:	Linux
Software Level Used:	Version 2.3

Ambient Weather Conditions:	Mostly Sunny
Sending Vehicle Model/Make:	Toyota Prius
Receiving Vehicle Model/Make:	Lexus GS300
Antenna Type Used:	Standard
Obstacle Vehicle #1 Model/Make:	Toyota Sequoia
Obstacle Vehicle #2 Model/Make:	Toyota Sequoia
Obstacle Vehicle #3 Model/Make:	Toyota Highlander





6.2 Multiple Senders Communications

6.2.1 Test Scenario 4-1

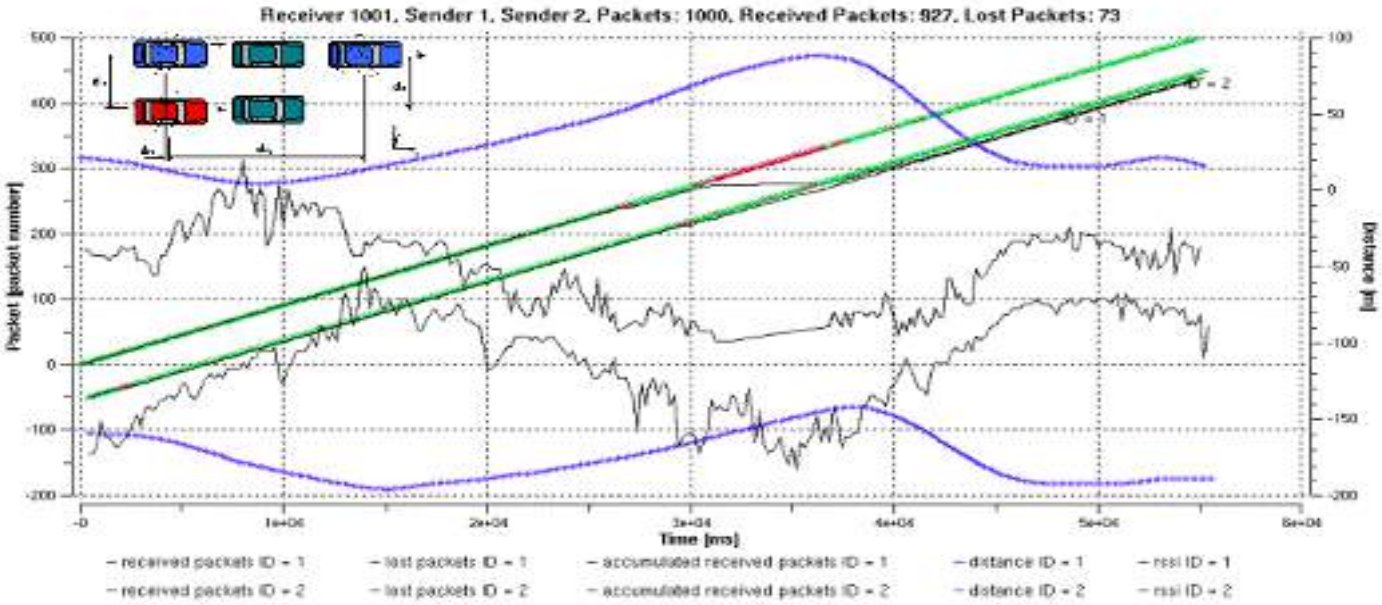
Test Scenario	**4-1**
Relevant Applications	Emergency Electronic Brake Light Pre-Crash Sensing for Co-op Collision Mitigation Co-op Forward Collision Warning (FCW) Lane Change Warning
Velocity of Receiving Antenna (miles/hour)	25
Distance Between Antennas (meters)	50
Lateral Offset to Broadcast Antenna (meters)	4
Velocity of Sending Antenna (miles/hour)	30
Angle Between Vehicle 1 & Vehicle 2 (degrees)	0
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	400
Path Obstructions	None
Vehicle Obstructions	None
Road Class	Arterial
Traffic Conditions	Light
Other Effects	None
Vehicle-Class of Cut-In Vehicle	N/A

Table 74. Test Scenario 4-1

Test Comments: Offset used for the graph is 20 (packets), 200 (distance), and 200 (RSSI). The test was done on arterial road with light traffic. The sending vehicles were moving approximately 40 mph and the receiver at 30 mph. The frequency used for this test was at 5.8GHz. There was no blocking vehicle between the 2 senders. However, there were some vehicles on the road blocking the receiver from the sender causing packet drops. The top number of packets, distance and RSSI correspond to sender 1.

Figure 119. Test Number 4-1 Results

Test Number	**4-1**	Ambient Weather Conditions:	**Cloudy**
Trace File Name:	**test_4_1_8_2_*.***	Sending Vehicle Model/Make:	**BMW 330, VW Passat**
Date Collected:	**March 26, 2004**	Receiving Vehicle Model/Make:	**Mercedes M class**
Files Resident With Whom:	**C. Lee**	Antenna Type Used:	**Standard**
Operating System Used:	**Linux**	VSC Obstacle Vehicle #1 Model/Make:	**N/A**
Software Level Used:	**v3.0.4**	VSC Obstacle Vehicle #2 Model/Make:	**N/A**



6.2.2 Test Scenario 4-2

Test Scenario	**4-2**
Relevant Applications	Emergency Electronic Brake Light Pre-Crash Sensing for Co-op Collision Mitigation Co-op Forward Collision Warning (FCW) Lane Change Warning
Velocity of Receiving Antenna (miles/hour)	60
Distance Between Antennas (meters)	100
Lateral Offset to Broadcast Antenna (meters)	4
Velocity of Sending Antenna (miles/hour)	65
Angle Between Vehicle 1 & Vehicle 2 (degrees)	0
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	400
Path Obstructions	None
Vehicle Obstructions	None
Road Class	Highway
Traffic Conditions	Light
Other Effects	None
Vehicle-Class of Cut-In Vehicle	N/A

Table 75. Test Scenario 4-2

Test Comments: Receiver constant speed of about 60mph, Senders slow pass at 65 mph, one-lane offset, up to and over 100m between the front sender (sender 1) and the receiver, 5.8 GHz, 100 percent power, nominal 600 packet duration. Occasionally, non-test vehicles entered the test pattern and blocked some packets. Offset values used for the plot: 0 (packets), 0 (distance), and 0 (RSSI).

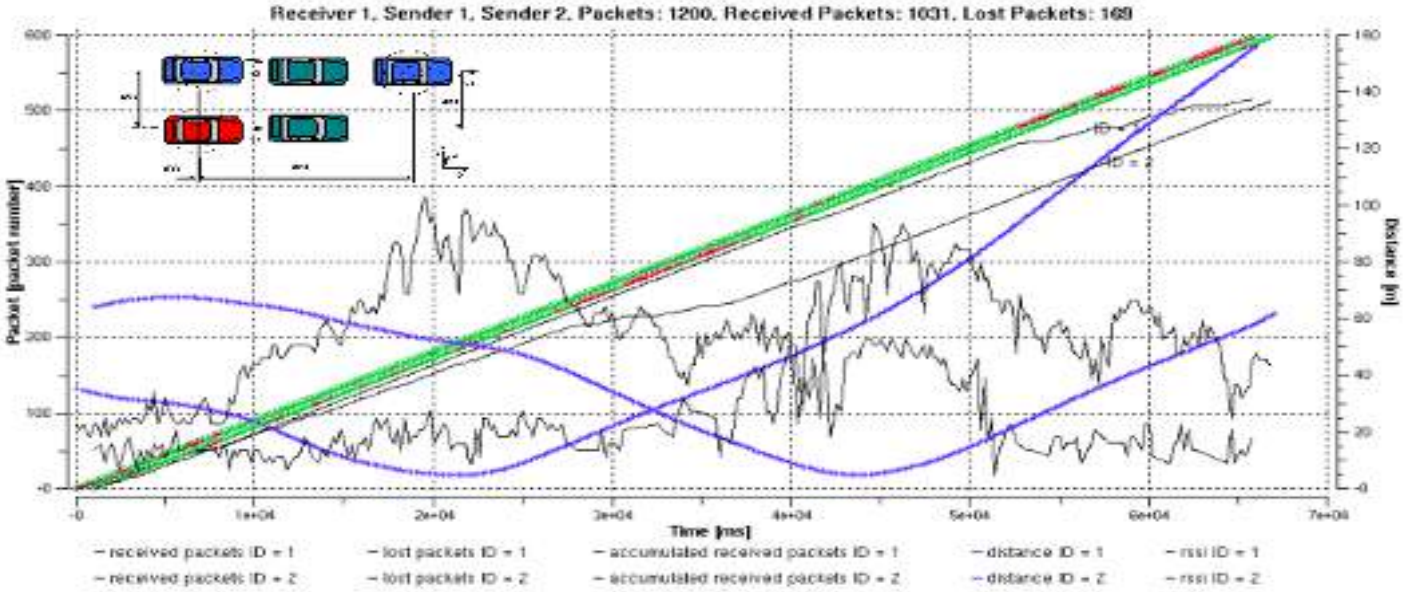
Figure 120. Test Number 4-2 Results

Test Number **4-2**
Trace File Name: **test_4-2_2_*.***
Date Collected: **March 22nd, 2004**
Files Resident With Whom: **Gordon Peredo**

Ambient Weather Conditions: **Sunny**
Sending Vehicle Model/Make: **BMW 330, VW Passat**
Receiving Vehicle Model/Make: **Chrysler Pacifica**
Antenna Type Used: **Standard**

Operating System Used: **Linux**
Software Level Used: **v3.0.4**

VSC Obstacle Vehicle #1 Model/Make: **N/A**
VSC Obstacle Vehicle #2 Model/Make: **N/A**



6.2.3 Test Scenario 4-3

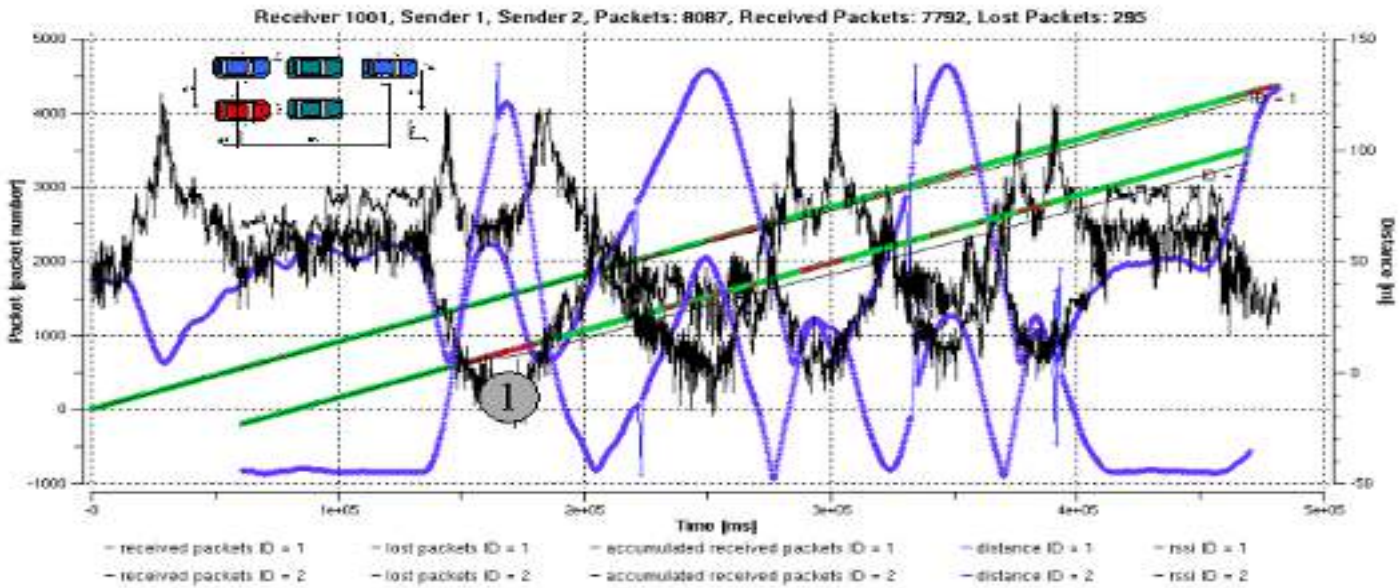
Test Scenario	**4-3**
Relevant Applications	Emergency Electronic Brake Light Pre-Crash Sensing for Co-op Collision Mitigation Co-op Forward Collision Warning (FCW) Lane Change Warning
Velocity of Receiving Antenna (miles/hour)	60
Distance Between Antennas (meters)	100
Lateral Offset to Broadcast Antenna (meters)	4
Velocity of Sending Antenna (miles/hour)	65
Angle Between Vehicle 1 & Vehicle 2 (degrees)	0
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	400
Path Obstructions	None
Vehicle Obstructions	None
Road Class	Highway
Traffic Conditions	Light
Other Effects	None
Vehicle-Class of Cut-In Vehicle	N/A

Table 76. Test Scenario 4-3

Test Comments: The test was conducted at highway speeds varying from the prescribed 60/65 mph to 75 mph with occasional obstacle vehicles outside the intended test vehicles. Overall, 96 percent of the packets sent during the test were received. The majority of the lost of packets (encircled by 1) was caused by an obstacle 18-wheeler in close proximity (under 25m). Offset values used for the plot was 200 (packets), 50 (distance), and 500 (RSSI). The sinusoidal nature of the distance curves during the middle of the test graph represents multiple repetitions of test 4-3 (the senders pass the receiver going approximately 5mph faster). This test was conducted at 5.32GHz.

Figure 121. Test Number 4-3 Results

Test Number	**4-3 and 4-5**	Ambient Weather Conditions:	**Mostly Sunny**
Trace File Name:	**test_4_3_2_*.***	Sending Vehicle Model/Make:	**M45 & Camry**
Date Collected:	**March 2nd, 2004**	Receiving Vehicle Model/Make:	**Lexus GS300**
Files Resident With Whom:	**Steve Tengler**	Antenna Type Used:	**Standard**
Operating System Used:	**Linux**	VSC Obstacle Vehicle #1 Model/Make:	**Infiniti Q45**
Software Level Used:	**v3.0-B2 (27-Feb-04)**	VSC Obstacle Vehicle #2 Model/Make:	**Ford Explorer**



6.2.4 Test Scenario 4-4

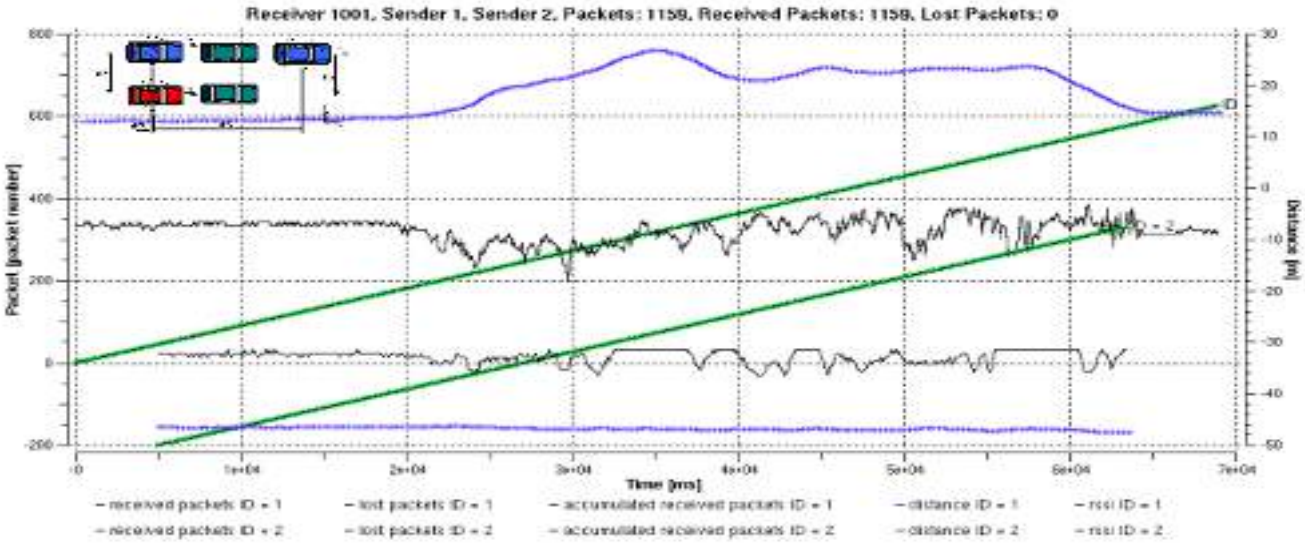
Test Scenario	**4-4**
Relevant Applications	Emergency Electronic Brake Light Pre-Crash Sensing for Co-op Collision Mitigation Co-op Forward Collision Warning (FCW) Lane Change Warning
Velocity of Receiving Antenna (miles/hour)	25
Distance Between Antennas (meters)	<20
Lateral Offset to Broadcast Antenna (meters)	4
Velocity of Sending Antenna (miles/hour)	25
Angle Between Vehicle 1 & Vehicle 2 (degrees)	0
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	400
Path Obstructions	None
Vehicle Obstructions	Sustained
Road Class	Arterial
Traffic Conditions	Light
Other Effects	None
Vehicle-Class of Cut-In Vehicle	SUV/sedan

Table 77. Test Scenario 4-4

Test Comments: The test was conducted at arterial speeds close to 25 mph. The tight formation maintained a distance less than 20 m between Sender1 and Receiver, and Sender2 was one lane to the left of the Receiver. Two obstructing vehicles were sustained during the test. Overall, over 99 percent of the packets sent during all three trials of the test were received. The obstructing vehicles did not cause any significant loss of reception from Sender1. The Sender 2 values are offset from the Sender 1 values by 200 packets, 50 meters, and 500 RSSI. This test was conducted at 5.32GHz.

Figure 122. Test Number 4-4 Results

Test Number	**4-4**	Ambient Weather Conditions:	**Mostly Sunny**
Trace File Name:	**test_4_4_2_*.***	Sending Vehicle Model/Make:	**M45 & Q45**
Date Collected:	**March 2nd, 2004**	Receiving Vehicle Model/Make:	**Buick LeSabre**
Files Resident With Whom:	**H. Krishnan**	Antenna Type Used:	**Standard**
Operating System Used:	**Linux**	VSC Obstacle Vehicle #1 Model/Make:	**Toyota Camry**
Software Level Used:	**v3.0-B3**	VSC Obstacle Vehicle #2 Model/Make:	**Ford Explorer**



6.2.5 Test Scenario 4-5

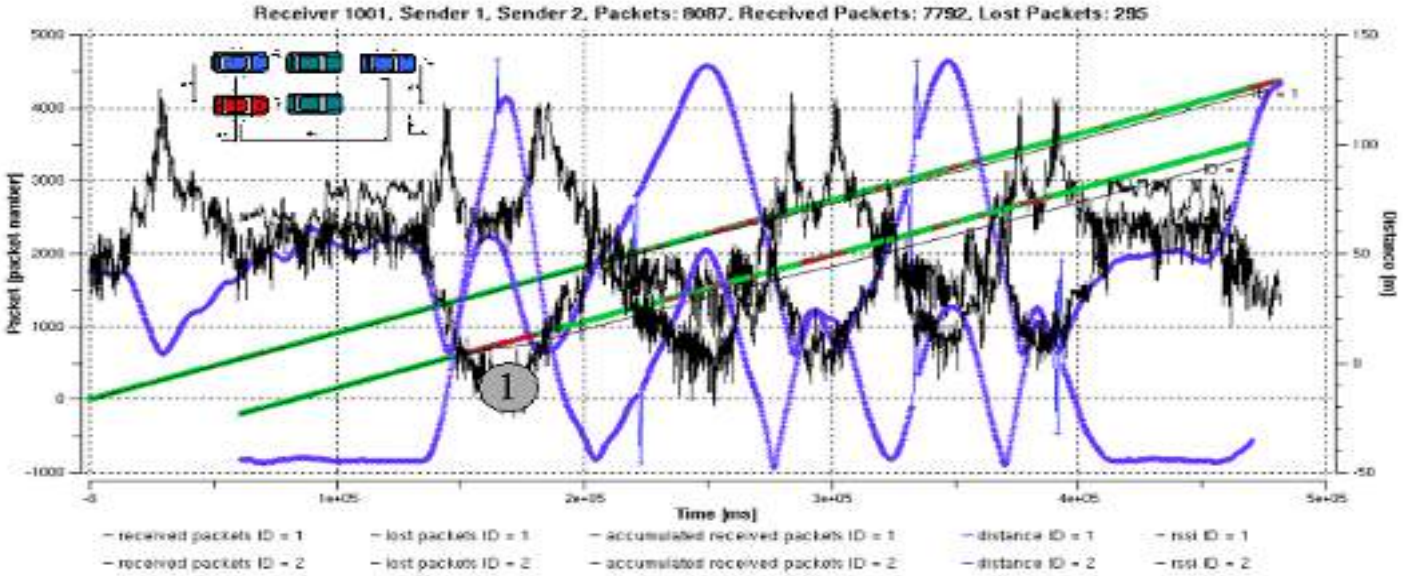
Test Scenario	**4-5**
Relevant Applications	Emergency Electronic Brake Light Pre-Crash Sensing for Co-op Collision Mitigation Co-op Forward Collision Warning (FCW) Lane Change Warning
Velocity of Receiving Antenna (miles/hour)	60
Distance Between Antennas (meters)	100
Lateral Offset to Broadcast Antenna (meters)	4
Velocity of Sending Antenna (miles/hour)	60
Angle Between Vehicle 1 & Vehicle 2 (degrees)	0
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	400
Path Obstructions	None
Vehicle Obstructions	Sustained
Road Class	Highway
Traffic Conditions	Light
Other Effects	None
Vehicle-Class of Cut-In Vehicle	SUV/Sedan

Table 78. Test Scenario 3-14

Test Comments: The test was conducted at highway speeds varying from the prescribed 60/65 mph to 75 mph with occasional obstacle vehicles outside the intended test vehicles. Overall, 96 percent of the packets sent during the test were received. The majority of the lost of packets (encircled by 1) was caused by an obstacle 18-wheeler in close proximity (under 25m). Offset values used for the plot was 200 (packets), 50 (distance), and 500 (RSSI). The ends of the graph demonstrate repetitions of test 4-5. This test was conducted at 5.32GHz.

Figure 123. Test number 4-5 Results

Test Number	**4-3 and 4-5**	Ambient Weather Conditions:	**Mostly Sunny**
Trace File Name:	**test_4_3_2_*.***	Sending Vehicle Model/Make:	**M45 & Camry**
Date Collected:	**March 2nd, 2004**	Receiving Vehicle Model/Make:	**Lexus GS300**
Files Resident With Whom:	**Steve Tengler**	Antenna Type Used:	**Standard**
Operating System Used:	**Linux**	VSC Obstacle Vehicle #1 Model/Make:	**Infiniti Q45**
Software Level Used:	**v3.0-B2 (27-Feb-04)**	VSC Obstacle Vehicle #2 Model/Make:	**Ford Explorer**



6.2.6 Test Scenario 4-6

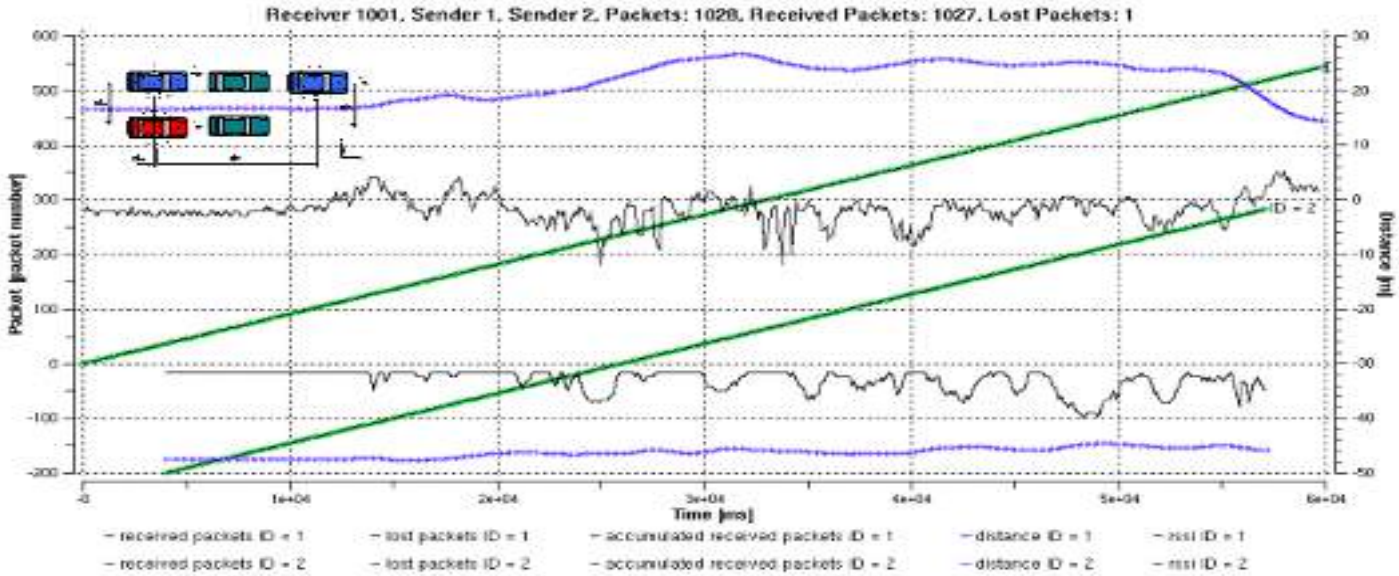
Test Scenario	**4-6**
Relevant Applications	Emergency Electronic Brake Light Pre-Crash Sensing for Co-op Collision Mitigation Co-op Forward Collision Warning (FCW) Lane Change Warning
Velocity of Receiving Antenna (miles/hour)	25
Distance Between Antennas (meters)	<20
Lateral Offset to Broadcast Antenna (meters)	4
Velocity of Sending Antenna (miles/hour)	25
Angle Between Vehicle 1 & Vehicle 2 (degrees)	0
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	400
Path Obstructions	None
Vehicle Obstructions	Sustained
Road Class	Arterial
Traffic Conditions	Light
Other Effects	None
Vehicle-Class of Cut-In Vehicle	SUV/Sedan

Table 79. Test Scenario 4-6

Test Comments: The test was conducted at arterial speeds close to 25 mph with occasional obstacle vehicles outside the intended test vehicles. The Sender 2 values are offset from the Sender 1 values by 200 packets, 50 meters, and 500 RSSI. Overall, over 99 percent of the packets sent during the test were received. No more than one packet was lost out of the thousand packets that were sent during each of the three trials. This test was conducted at 5.32GHz.

Figure 124. Test Number 4-6 Results

Test Number	**4-6**	Ambient Weather Conditions:	**Mostly Sunny**
Trace File Name:	**test_4_6_5_*.***	Sending Vehicle Model/Make:	**M45 & Q45**
Date Collected:	**March 2nd, 2004**	Receiving Vehicle Model/Make:	**Buick LeSabre**
Files Resident With Whom:	**Jim Bauer**	Antenna Type Used:	**Standard**
Operating System Used:	**Linux**	VSC Obstacle Vehicle #1 Model/Make:	**Ford Explorer**
Software Level Used:	**v3.0-B3**	VSC Obstacle Vehicle #2 Model/Make:	**Toyota Camry**



6.2.7 Test Scenario 4-7

Test Scenario	**4-7**
Relevant Applications	Emergency Electronic Brake Light Pre-Crash Sensing for Co-op Collision Mitigation Co-op Forward Collision Warning (FCW) Lane Change Warning
Velocity of Receiving Antenna (miles/hour)	60
Distance Between Antennas (meters)	100
Lateral Offset to Broadcast Antenna (meters)	4
Velocity of Sending Antenna (miles/hour)	60
Angle Between Vehicle 1 & Vehicle 2 (degrees)	0
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	400
Path Obstructions	None
Vehicle Obstructions	Sustained
Road Class	Highway
Traffic Conditions	Light
Other Effects	None
Vehicle-Class of Cut-In Vehicle	SUV

Table 80. Test Scenario 4-7

Test Comments: Test conditions: constant speed of about 60mph, one lane offset, approximately 100m between the front sender (sender 1) and the receiver, 5.8 GHz, 100 percent power, nominal 1000 packet duration. Traffic surrounding the vehicles was moderate. Almost all packets from sender 2 were received, but many packets from sender 1 were lost.

Offsets:

50 packets (on left y-axis); sender 1 packets on top in the diagram

200 meters (on right y-axis); sender 1 distance on top in the diagram

0 RSSI; 0 to 1000 packets corresponds to 0 to 60 RSSI; sender 2 RSSI on top in the diagram

Figure 125. Test Number 4-7 Results

Test Number	**4-7**	Ambient Weather Conditions:	**Sunny**
Trace File Name:	**test_4_7_3_*.***	Sending Vehicle Model/Make:	**BMW 330, VW Passat**
Date Collected:	**March 22, 2004**	Receiving Vehicle Model/Make:	**Chrysler Pacifica**
Files Resident With Whom:	**E. Clark**	Antenna Type Used:	**Standard**
Operating System Used:	**Linux**	VSC Obstacle Vehicle #1 Model/Make:	**VW Touareg**
Software Level Used:	**v3.0.4**	VSC Obstacle Vehicle #2 Model/Make:	**BMW X3**

6.2.8 Test Scenario 4-8

Test Scenario	**4-8**
Relevant Applications	Emergency Electronic Brake Light Pre-Crash Sensing for Co-op Collision Mitigation Co-op Forward Collision Warning (FCW) Lane Change Warning
Velocity of Receiving Antenna (miles/hour)	60
Distance Between Antennas (meters)	100
Lateral Offset to Broadcast Antenna (meters)	8
Velocity of Sending Antenna (miles/hour)	60
Angle Between Vehicle 1 & Vehicle 2 (degrees)	0
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	400
Path Obstructions	None
Vehicle Obstructions	Sustained
Road Class	Highway
Traffic Conditions	Light
Other Effects	None
Vehicle-Class of Cut-In Vehicle	SUV

Table 81. Test Scenario 4-8

Test Comments: Test conditions: constant speed of about 60mph, two-lane offset, approximately 100m between the front sender (sender 1) and the receiver, 5.8 GHz, 100 percent power, nominal 1000 packet duration. Virtually all packets from sender 2 were received, but many packets from sender 1 were lost. Additional (blocking) vehicles occasionally passed between the two lanes of test vehicles.

Offsets:

0 packets (on left y-axis); sender 2 on top in the diagram

0 meters (on right y-axis); sender 1 on top in the diagram

0 RSSI; 0 to 1000 packets corresponds to 0 to 60 RSSI; sender 2 RSSI on top in the diagram

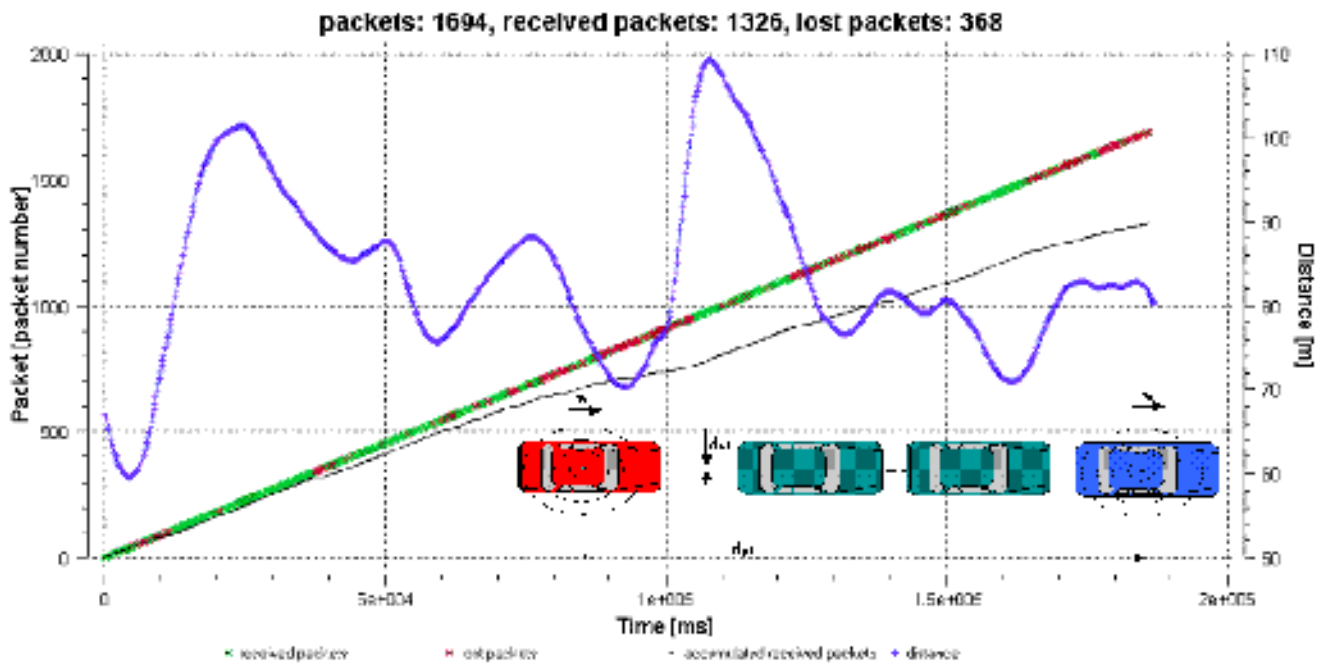
Figure 126. Test Number 4-8 Results

Test Number 2-11
Trace File Name: test2-11_3_[illegible].trace*
Date Collected: August 4th, 2003
Files Resident With Whom: Chu-Hao Lee

Ambient Weather Condition: Sunny
Sending Vehicle Model/Make: BMW Series 3
Receiving Vehicle Model/Make: VW Passat
Antenna Type Used: Standard

Operating System Used: Linux
Software Level Used: 2.3

VSC Obstacle Vehicle #1 Model/Make: BMW X5
VSC Obstacle Vehicle #3 Model/Make: Mercedes M-class



6.2.9 Test Scenario 4-9

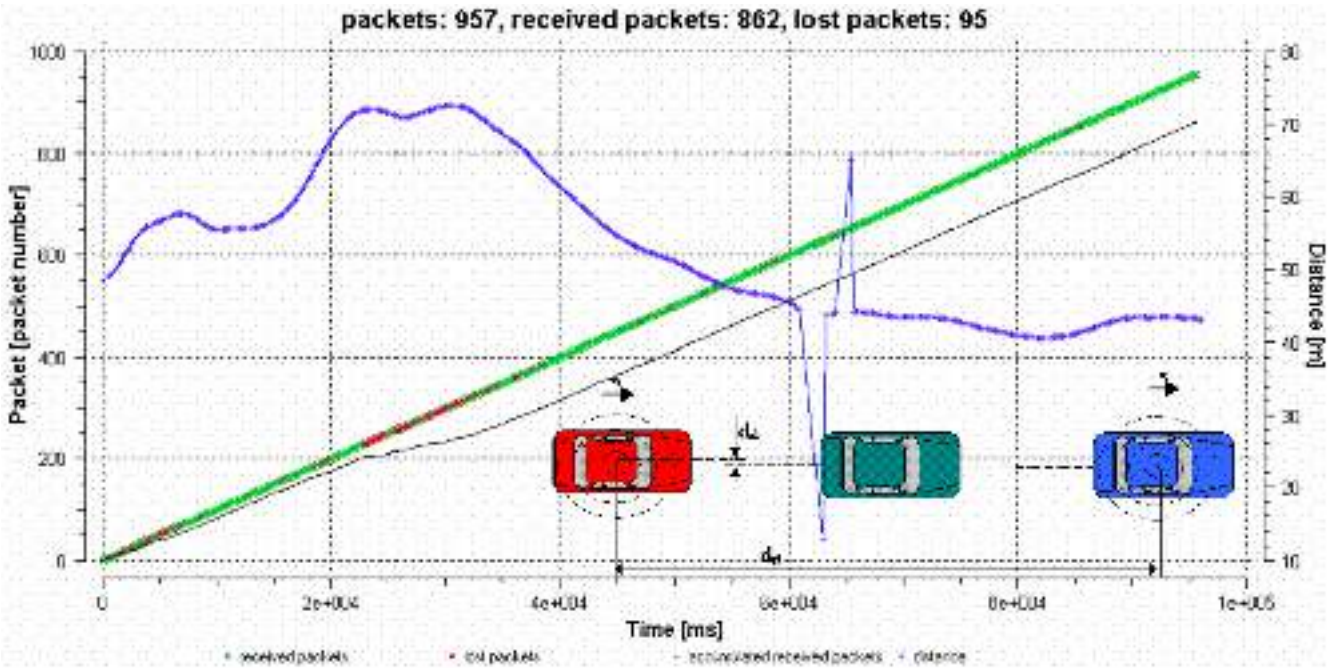
Test Scenario	**4-9**
Relevant Applications	Emergency Electronic Brake Light Pre-Crash Sensing for Co-op Collision Mitigation Co-op Forward Collision Warning (FCW) Lane Change Warning
Velocity of Receiving Antenna (miles/hour)	60
Distance Between Antennas (meters)	100
Lateral Offset to Broadcast Antenna (meters)	8
Velocity of Sending Antenna (miles/hour)	0
Angle Between Vehicle 1 & Vehicle 2 (degrees)	0
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	400
Path Obstructions	None
Vehicle Obstructions	Sustained
Road Class	Highway
Traffic Conditions	Light
Other Effects	None
Vehicle-Class of Cut-In Vehicle	SUV

Table 82. Test Scenario 4-9

Test Comments: Receiver constant speed of about 60mph, Senders slow pass at 65 mph, two-lane offset, up to and over 100m between the front sender (sender 1) and the receiver, 5.8 GHz, 100 percent power, nominal 600 packet duration. Severe packet loss due to large truck passing between test vehicles and blocking senders' line-of-sight to receiver. Occasional line-of-sight blockage by obstructing SUVs. Offset values used for the plot was 0 (packets), 0 (distance), and 0 (RSSI).

Figure 127. Test Number 4-9 Results

Test Number:	2-12	Ambient Weather Conditions:	Mostly Sunny
Trace File Name:	060503_2_12_2.trace*	Sending Vehicle Model/Make:	Buick LeSabre
Data Collected:	June 5th, 2003	Receiving Vehicle Model/Make:	Buick LeSabre
Files Resident With Whom:	H. Krishnan	Antenna Type Used:	Standard
Operating System Used:	Windows XP	VRC Obstacle Vehicle #1 Model/Make:	Large Truck
Software Level Used:	2.4a beta (27-Feb-03)	VRC Obstacle Vehicle #2 Model/Make:	N/A



6.2.10 Test Scenario 4-10

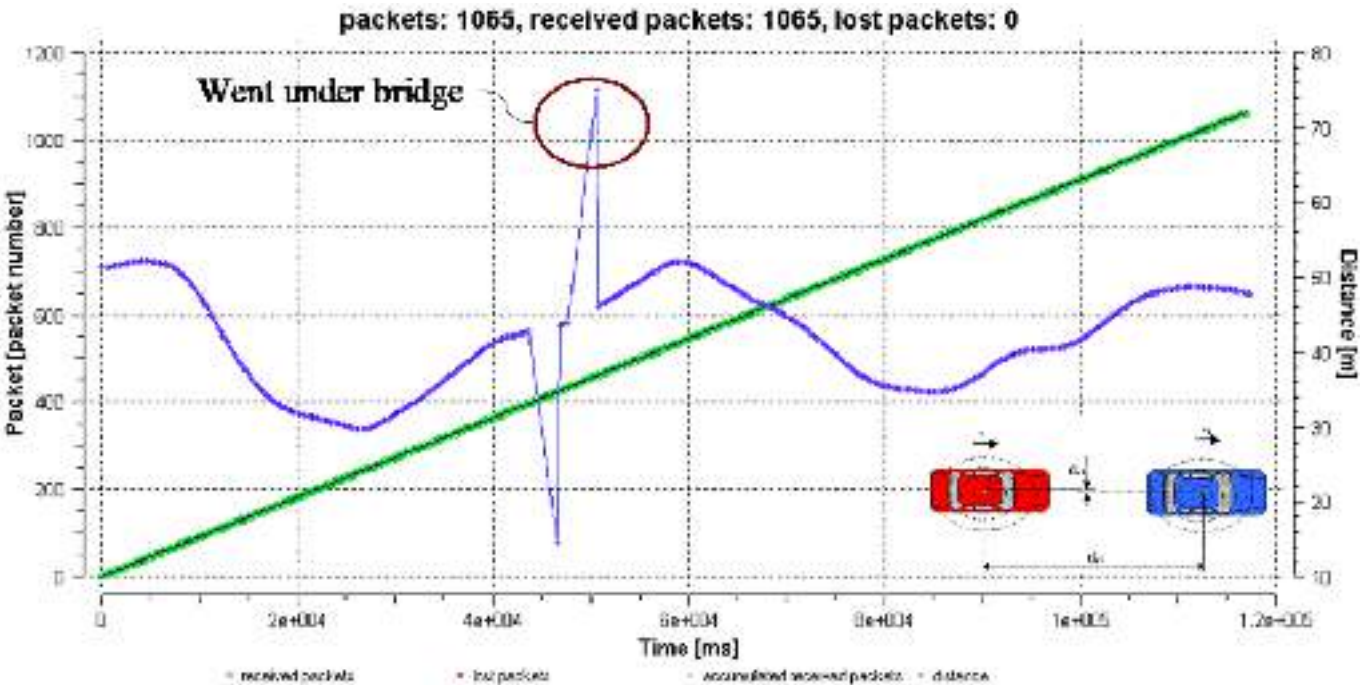
Test Scenario	**4-10**
Relevant Applications	Stop Sign Movement Assistant
Velocity of Receiving Antenna (miles/hour)	0
Distance Between Antennas (meters)	50
Lateral Offset to Broadcast Antenna (meters)	4
Velocity of Sending Antenna (miles/hour)	25
Angle Between Vehicle 1 & Vehicle 2 (degrees)	N/A
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	300
Path Obstructions	None
Vehicle Obstructions	None
Road Class	Arterial
Traffic Conditions	Light
Other Effects	None
Vehicle-Class of Cut-In Vehicle	N/A

Table 83. Test Scenario 4-10

Test Comments: This test was conducted at 5.32GHz. This test was conducted on an arterial road at speeds close to 25 mph. The distance between (stationary) Sender 1 and the Receiver was ~10m. The test demonstrates that having 2 senders in an intersection-type scenario has no adverse effect on packet reception. (Note that the data curves are offset for clarity, with a shift of 200 packets, 50 meters, and 500 RSSI units between each.) Sender 1 began transmission significantly prior to Sender 2 so that the receiver could verify packet reception. Only a few packets were lost during any of the multiple runs for this scenario; primarily near the endpoints where Sender 2 was often out of sight. A couple additional packets were lost during the actual drive-by portion, but it should be further noted that there was significant roadside clutter in the form of trees and parked cars, which may have partially contributed to this.

Figure 128. Test Number 4-10 Results

Test Number	**2-13**	**Ambient Weather Conditions:**	**Sunny**
Trace File Name:	**072403_2_13_1.trace***	**Sending Vehicle Model/Make:**	**Buick LeSabre**
Date Collected:	**July 17th, 2003**	**Receiving Vehicle Model/Make:**	**Buick LeSabre**
Files Resident With Whom:	**S. Tengler**	**Antenna Type Used:**	**Standard**
Operating System Used:	**Linux**	**VSC Obstacle Vehicle #1 Model/Make:**	**N/A**
Software Level Used:	**V2.3 (8-July-03)**	**VSC Obstacle Vehicle #2 Model/Make:**	**N/A**



6.2.11 Test Scenario 4-11

Test Scenario	**4-11**
Relevant Applications	Stop Sign Movement Assistant
Velocity of Receiving Antenna (miles/hour)	0
Distance Between Antennas (meters)	50
Lateral Offset to Broadcast Antenna (meters)	4
Velocity of Sending Antenna (miles/hour)	25
Angle Between Vehicle 1 & Vehicle 2 (degrees)	N/A
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	300
Path Obstructions	None
Vehicle Obstructions	None
Road Class	Arterial
Traffic Conditions	Light
Other Effects	None
Vehicle-Class of Cut-In Vehicle	N/A

Table 84. Test Scenario 4-11

Test Comments: The test was conducted at arterial speeds close to 25 mph. The distance between stationary Sender3 and Receiver was about 10m, and Sender1 and Sender2 were one lane apart. Overall, over 99 percent of the packets sent during all three trials of the test were received. The test shows that having 3 senders in an intersection type scenario has no effect on packet loss of reception. The Sender 2 values are offset from the Sender 1 values by 200 packets, 50 meters, and 500 RSSI. The Sender 3 values are offset from the Sender 2 values by 200 packets, 50 meters, and 500 RSSI. This test was conducted at 5.32GHz.

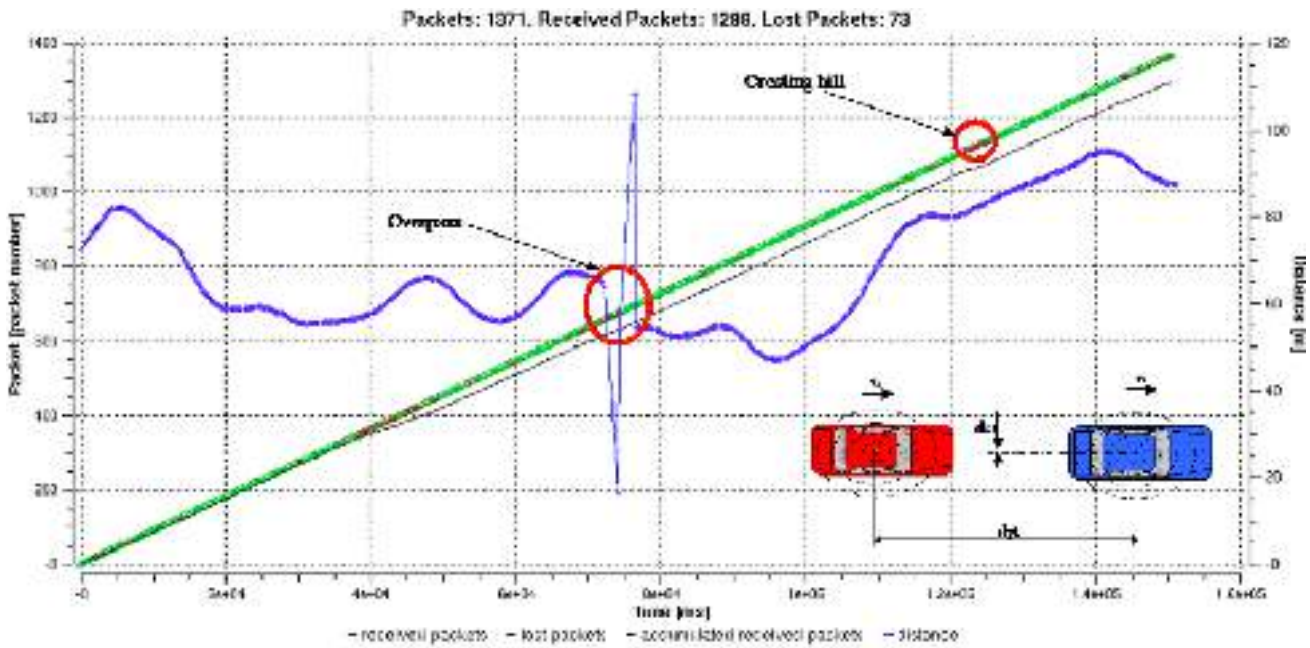
Figure 129. Test Number 4-11 Results

Test Number 2-14
Trace File Name: test2-14_3_072303.trace*
Date Collected: July 23rd, 2003
Files Resident With Whom: Chu-Hee Lee

Ambient Weather Conditions: Sunny
Sending Vehicle Model/Make: VW Passat
Receiving Vehicle Model/Make: BMW Series 3
Antenna Type Used: Standard

Operating System Used: Linux
Software Level Used: 2.3

VSC Obstacle Vehicle #1 Model/Make: N/A
VSC Obstacle Vehicle #2 Model/Make: N/A



6.2.12 Test Scenario 4-12

Test Scenario	**4-12**
Relevant Applications	Stop Sign Movement Assistant
Velocity of Receiving Antenna (miles/hour)	0
Distance Between Antennas (meters)	100
Lateral Offset to Broadcast Antenna (meters)	4
Velocity of Sending Antenna (miles/hour)	45
Angle Between Vehicle 1 & Vehicle 2 (degrees)	N/A
Update Rate (milliseconds)	100
Transmitter Power Level (%)	100
Packet Size (bytes)	200
Path Obstructions	None
Vehicle Obstructions	None
Road Class	Arterial
Traffic Conditions	Light
Other Effects	None
Vehicle-Class of Cut-In Vehicle	N/A

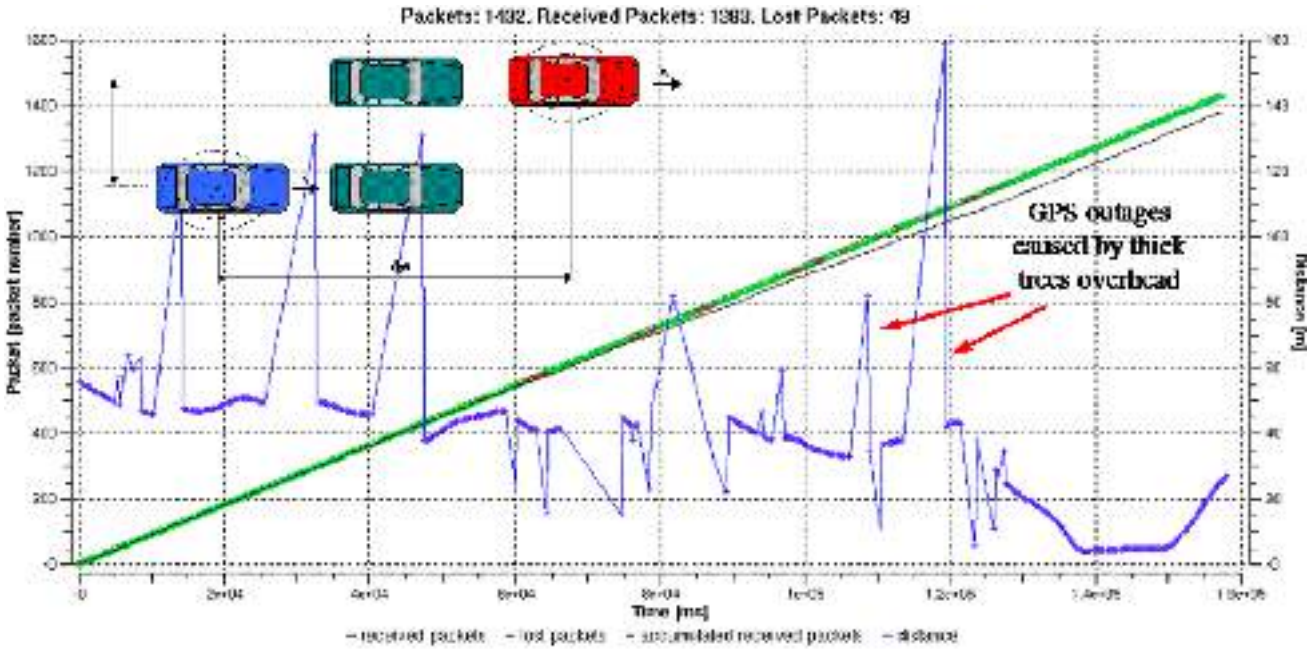
Table 85. Test Scenario 4-12

Test Comments: This test was conducted at highway speeds close to 50 mph. The distance between (stationary) Sender 3 and the Receiver was ~10m, and Sender 1 and Sender 2 were one lane apart. The test demonstrates that having 3 senders in an intersection-type scenario has no adverse effect on packet reception. (Note that the data curves are offset for clarity, with a shift of 200 packets, 50 meters, and 500 RSSI units between each.) Senders 1 and 2 were initially stationary for a significant period of time while waiting for unexpected traffic to clear from the test zone. Also, Sender 2 began well beyond the line-of-sight to the Receiver. Aside from this, very few packets were lost during the actual drive by. It should be further noted that there was significant roadside clutter in the form of trees and parked cars, which may have partially contributed to the few lost packets. This test was conducted at 5.32GHz.

Figure 130. Test Number 4-12 Results

Test Number: 2-15 | **Ambient Weather Conditions: Sunny**
Trace File Name: test2-15_3_072303.trace* | **Sending Vehicle Model/Make: BMW Series 3**
Date Collected: July 23rd, 2003 | **Receiving Vehicle Model/Make: VW Passat**
Files Resident With Whom: Chu Hee Lee | **Antenna Type Used: Standard**

Operating System Used: Linux | **VSC Obstacle Vehicle #1 Model/Make: Audi A4 Quattro**
Software Level Used: 2.3 | **VSC Obstacle Vehicle #2 Model/Make: N/A**



Appendix D:
Antennas

TABLE OF CONTENTS

1 Antenna Subproject Specification 1

1.1 Introduction 1

1.1.1 Acceptable Performance 1

1.1.2 Statement of Work 2

1.2 Definitions 2

1.3 Applicable Documents 3

1.3.1 Government Documents 3

1.3.2 CAMP – VSCC Documents 3

1.3.3 Industry Documents 3

1.4 Requirements 4

1.4.1 Component Definition 4

1.4.1.1 Antenna Assembly 4

1.4.1.2 System Operation 4

1.4.2 Environmental Requirements 4

1.4.2.1 Water Intrusion 4

1.4.2.2 Temperature 4

1.4.2.3 Vibration 4

1.4.3 Electrical Requirements 4

1.4.3.1 5.9GHz Antenna Performance Requirements 4

1.4.3.1.1 Operating Frequency Range 4

1.4.3.1.2 Impedance Match Requirement 5

1.4.3.1.3 Free-Space Gain 5

1.4.3.1.4 Vehicle Level Simulation 5

1.4.3.1.5 Pattern Coverage 5

1.4.3.1.6 Polarization 6

1.4.3.2 Electrical Interface Requirements 6

1.4.3.2.1 Coaxial Cable Electrical Properties 6

1.4.3.2.2 Connector 7

1.4.4 Physical Requirement 7

1.4.4.1 Antenna Appearance 7

1.4.4.1.1 Finish 7

1.4.4.1.2 Color 7

1.4.4.1.3 Shape 7

1.4.4.2 Mechanical 7
1.4.4.2.1 Mechanical Mounting 7
1.4.4.3 Label Requirements.....8
1.4.5 Antenna Correlation Matrix.....8
1.4.5.1 Antenna Correlation Matrix Terminology 8
1.4.5.2 Antenna Correlation Matrix 9
1.5 Selection of Antenna Polarization.....9
1.6 Thermax 0.070” Cable Test Data.....13
2 Antenna Subproject Simulation Results 14
2.1 Candidate Antenna Design Description.....14
2.2 Antenna Design Overview 16
2.3 Software Overview.....16
2.4 Design Specifications.....17
2.5 Side-View Mirror Simulation 17
2.5.1 Design Description.....17
2.5.2 Dimensioned Layout.....18
2.5.3 Model Assumptions 18
2.5.4 VSWR/Impedance 19
2.5.5 Free-Space Pattern/Gain Plots (Bottom Feed-Point) 21
2.5.6 On-Mirror Pattern/Gain Plots 26
2.5.7 Free Space Pattern/Gain Plots (Side Feed-Point) 32
2.6 Roof-Mount Simulation 37
2.6.1 Design Description.....37
2.6.2 Dimensioned Layout.....37
2.6.3 Model Assumptions 37
2.6.4 Infinite Ground Plan Pattern/Gain Plots 38
2.6.5 300mm Ground Plan Pattern/Gain Plots.....43
2.7 Free-Space Link Budget.....49
2.7.1 Free-Space Link Budget (Mirror-to-Mirror).....50
2.7.2 Free-Space Link Budget (Mirror-to-Roof) 50
2.7.3 Free-Space Link Budget (Roof-to-Roof) 51
2.8 Summary 51

3 Antenna Subproject Final Report 52
3.1 Antenna Design 52
3.1.1 Magnetic Roof Mount Antenna Drawings 52
3.1.2 Mirror Antenna Drawings 56
3.2 Anechoic Chamber and Bench Test Data 61
3.2.1 Chamber Characteristics 61
3.2.1.1 Gain – Mirror Mount Antenna 61
3.2.1.2 Gain – 5/8 Wave Roof Mount Antenna 62
3.2.1.3 Gain – 4-Element WLAN Roof Mount Antenna 64
3.2.2 Bench Test 66
3.2.2.1 VSWR – Side View Mirror 67
3.2.2.2 VSWR – Roof Mount 68
3.2.3 Summary 69
3.3 Vehicle Level Range Testing 69
3.3.1 J.E.F. Range Characteristics 69
3.3.2 Side-Mirror Antenna Tests 70
3.3.2.1 Driver Side-Mirror Pattern (unit 26) 5850 MHz 72
3.3.2.2 Passenger Side-Mirror Pattern (unit 26) 5850 MHz 73
3.3.2.3 Side Mirror Composite Diversity Pattern (Unit 26) 5850 MHz 74
3.3.3 Roof Mount Antenna Tests on Ground Plane 75
3.3.3.1 4 Element Array 5200MHz 76
3.3.3.2 5/8 Wave 5887.5MHz 77
3.3.4 Roof Mount Antenna Test on Vehicle With Sunroof 78
3.3.4.1 4 Element Array 5200MHz 78
3.3.4.2 5/8 Roof Mount 5850MHz 79
3.3.4.3 5/8 Roof Mount 5887.5MHz 80
3.3.4.4 5/8 Roof Mount 5925MHz 81
3.3.5 Roof Mount Antenna Tests on Vehicle Without Sunroof 82
3.3.5.1 4 Element Array 5200MHz 83
3.3.5.2 5-8 Wave 5850MHz 84
3.3.5.3 5-8 Wave 5887.5MHz 85
3.3.5.4 5-8 Wave 5925MHz 86
3.4 Summary 87
3.4.1 Side Mirror Antenna 87
3.4.2 Roof Mount 87

3.5 Test Kit Measurements 87
3.6 Drive Testing.....89
3.6.1 Receiving Vehicle Front 89
3.6.2 Receiving Vehicle Broadside.....90
3.6.3 Receiving Vehicle Rear 90
3.6.4 Clockwise Circular Passenger Side Antenna.....91
3.6.5 Counter-Clockwise Circular Passenger Side Antenna.....92
3.6.6 Test Results – Mirror Mount General Motors Proving Ground 92
3.6.6.1 GM 1 5890 Clockwise Circular Passenger Side Antenna.....93
3.6.6.2 GM 3 5890 Clockwise Circular Passenger Side Antenna.....94
3.6.6.3 GM 4 5200 Clockwise Circular Passenger Side Antenna.....95
3.6.6.4 GM 5 5890 Receiving Vehicle Front 96
3.6.6.5 GM 6 5200 Receiving Vehicle Front 97
3.6.6.6 GM 7 5200 Receiving Vehicle Broadside.....98
3.6.6.7 GM 8 5320 Receiving Vehicle Rear 99
3.6.6.8 GM 11 5890 Receiving Vehicle Rroadside.....100
3.6.6.9 GM 9 5200 Receiving Vehicle Rear 101
3.6.6.10 GM 10 5890 Receiving Vehicle Rear 102
3.6.6.11 GM 12 5890 Receiving Vehicle Passenger Side Broadside 103
3.6.6.12 GM 13 5890 Receiving Vehicle Passenger Side Broadside 104
3.6.6.13 GM 14 5200 Receiving Vehicle Passenger Side Broadside 105
3.6.6.14 GM 15 5200 Receiving Vehicle Passenger Side Broadside 106
3.6.6.15 GM 16 5200 Receiving Vehicle Passenger Side Broadside 107
3.6.6.16 GM 17 5890 Receiving Vehicle Passenger Side Broadside 108
3.6.6.17 Summary – GM Proving Ground.....109
3.6.7 Test Results – Troy 5/8 Wave Roof Mount Antenna 109
3.6.7.1 SS2 5890 Receiving Vehicle Front 110
3.6.7.2 SS3 5890 Receiving Vehicle Rear 111
3.6.7.3 Propagation Model 112
3.6.7.4 Summary – Side Street Drive Tests 115
3.6.8 Summary – Drive Tests 115
3.7 Summary 116
3.7.1 Test Results – Mirror Mount Ford Proving Ground 116
3.7.1.1 Ford 12 5890 Receiving Vehicle Front 116
3.7.1.2 Ford 13 5300 Receiving Vehicle Front 118
3.7.1.3 Ford 9 5300 Receiving Vehicle Broadside 119
3.7.1.4 Ford 10 5300 Receiving Vehicle Broadside 120

3.7.1.5 Ford 11 5890 Receiving Vehicle Broadside 121
3.7.1.6 Ford 14 5300 Receiving Vehicle Rear 122
3.7.1.7 Ford 15 5890 Receiving Vehicle Rear 123
3.7.1.8 Ford 16 5890 Clockwise Circular Passenger Side Antenna.....124
3.7.1.9 Ford 17 5300 Clockwise Circular Passenger Side Antenna.....125
3.7.1.10 Ford 18 5300 Counter-Clockwise Circular Passenger Side Antenna126
3.7.1.11 Ford 19 5890 Counter- Clockwise Circular Passenger Side Antenna127
3.7.1.12 Ford 20 5890 Clockwise Circular Driver Side Antenna 128
3.7.1.13 Ford 21 5300 Clockwise Circular Driver Side Antenna 129
3.7.1.14 Ford 22 5300 Counter- Clockwise Circular Passenger Side Antenna130
3.7.1.15 Ford 23 5890 Counter- Clockwise Circular Passenger Side Antenna131

TABLE OF FIGURES

Figure 1-A. Free Space – Conductor Interface 10
Figure 1-B. Test Setup for CP Antenna 11
Figure 1-C. CP Antenna Reception on a Ground Plane..... 11
Figure 1-D. Swept Gain of a 25 ft Long Sample From 3GHz to 6GHz. 13
Figure 2-A. Initial Antenna Element Design Over a Ground Plane 14
Figure 2-B. 2D View of Dipole Array 15
Figure 2-C. Isometric View of Dipole Array 15
Figure 2-D. Theoretical Cardiod Patterns for Each Dipole Array (Driver/Passenger Side) 16
Figure 2-E. VSWR – Free Space Dipole Array 19
Figure 2-F. VSWR – Dipole Array on Side View Mirror @ 5.850GHz 20
Figure 2-G. VSWR – Dipole Array on Side View Mirror @ 5.925GHz 20
Figure 2-H. Side and Top Views 21
Figure 2-I. Isometric View – Dipole Array in Free Space (Bottom Feed-Point) 22
Figure 2-J. Side View– Dipole Array in Free Space (Bottom Feed-Point) 23
Figure 2-K. Top View– Dipole Array in Free Space (Bottom Feed-Point)..... 24
Figure 2-L. Radiation Pattern – Dipole Array in Free Space 0° Elevation (Bottom Feed-Point) 25
Figure 2-M. Isometric View – Dipole Array on Side View Mirror..... 28
Figure 2-N. Top View – Dipole Array on Side View Mirror 29

Figure 2-O. Side View – Dipole Array on Side View Mirror 30
Figure 2-P. Radiation Pattern – Dipole Array on Side View Mirror 0° Elevation 31
Figure 2-Q. Dipole Array – Current Distribution 32
Figure 2-R. Side View– Dipole Array in Free Space (Side Feed-Point) 33
Figure 2-S. Top View– Dipole Array in Free Space (Side Feed-Point) 34
Figure 2-T. Radiation Pattern – Dipole Array in Free Space 0° Elevation (Side Feed-Point) 35
Figure 2-U. Smith Chart - Dipole Array in Free Space (Side Feed-Point) 36
Figure 2-V. Isometric View – 5/8 Wave on Infinite Ground Plane 39
Figure 2-W. Side view – 5/8 Wave on Infinite Ground Plane 40
Figure 2-X. Top view – 5/8 Wave on Infinite Ground Plane 41
Figure 2-Y. Radiation Pattern - 5/8 Wave on Infinite Ground Plane 0° Elevation 42
Figure 2-Z. Isometric View – 5/8 Wave on 300mm Ground Plane 44
Figure 2-AA. Side View – 5/8 Wave on 300mm Ground Plane 45
Figure 2-BB. Top View – 5/8 Wave on 300mm Ground Plane 46
Figure 2-CC. Radiation Pattern - 5/8 wave on 300mm Ground Plane Elevation Patterns at Phi 0 (XZ) and 90 (YZ) Degrees 47
Figure 2-DD. Radiation Pattern - 5/8 Wave on 300mm Ground Plane 70° Elevation 48
Figure 3-A. Azimuth Radiation Pattern of the Mirror Mount Antenna Including 2dB Cable Loss 61
Figure 3-B. Elevation Radiation Pattern of the Mirror Mount Antenna Including 2dB Cable Loss 62
Figure 3-C. Azimuth Radiation Pattern of the Roof Mount Antenna Including 2dB Cable Loss 63
Figure 3-D. Elevation Radiation Pattern of the Roof Mount Antenna Including 2dB Cable Loss 64
Figure 3-E. Azimuth Radiation Pattern of the Roof Mount Antenna Including 3dB Cable Loss 65
Figure 3-F. Azimuth Radiation Pattern of the Roof Mount Antenna Including 3dB Cable Loss 66
Figure 3-G. Time Domain Trace Showing Gate Window Showing Two-Way Propagation Time. 67
Figure 3-H. Measured VSWR 67
Figure 3-I. Time Domain Trace Showing Gate Window Showing Two-way propagation time. 68

Figure 3-J. Measured VSWR 68
Figure 3-K. Calibration Setup 70
Figure 3-L. Calibration Setup 70
Figure 3-M. Mirror Mount Antenna Including 2 ft Pigtail (2dB Loss) 72
Figure 3-N. Mirror Mount Antenna Including 2 ft Pigtail (2dB loss) 73
Figure 3-O. Composite Radiation Pattern 74
Figure 3-P. 4-Element WLAN Antenna Performance on Ground Plane Including 3dB Cable Loss 76
Figure 3-Q. 5/8 Wave Antenna Performance on Ground Plane Including 2dB Cable Loss 77
Figure 3-R. 4-Element Array With Sunroof Including 3dB Cable Loss 78
Figure 3-S. 5/8 Wave With Sunroof Including 2dB Cable Loss 79
Figure 3-T. 5/8 Wave With Sunroof Including 2B Cable Loss 80
Figure 3-U. 5/8 Wave With Sunroof Including 2dB Cable Loss 81
Figure 3-V. 4-Element Array Without Sunroof Including 3dB Cable Loss 83
Figure 3-W. 5/8 Wave Without Sunroof Including 2dB Cable Loss 84
Figure 3-X. 5/8 Wave Without Sunroof Including 2dB Cable Loss 85
Figure 3-Y. 5/8 Wave Without Sunroof Including 2dB Cable Loss 86
Figure 3-Z. Test Kit Evaluation Setup 88
Figure 3-AA. Comparison of Propagation Model and SS2 Data 112
Figure 3-BB. Comparison of Propagation Model and SS3 Data 113
Figure 3-CC. Approximate Range for Receiving Vehicle Front With Sunroof 114
Figure 3-DD. Approximate Range for Receiving Vehicle Rear With Sunroof 115

TABLE OF TABLES

Table 1. Test Kit Data Taken on January 30, 2004 88
Table 2. Test Kit Data Taken on February 9, 2004 89

1 Antenna Subproject Specification

1.1 Introduction

Early testing within the VSC project had involved a sizeable and wholly unrealistic antenna for automotive usage, and was originally selected for its wide availability (802.11a Access Point antenna) and DSRC-like frequency range. For roadside units (RSUs), the physical characteristics of these antennas would not likely be an issue since infrastructure mounting usually has few packaging or styling needs. The antennas, though, could not fully answer the question of communication range for on-board units (OBUs) since their protruding nature and frequency-optimization would not mirror likely automotive, production DSRC antennas. Therefore, CAMP-VSCC set about investigating alternative OBU antenna designs with the following goals:

- **Approximate Production Performance** – Although impossible to fully test production performance of final DSRC systems, moving the designs closer to likely designs would help better understand possible performance.
- **Realistic Protrusion** – Styling for experimental equipment is rarely a strong ingredient, yet it must be considered as a basic constraint for antenna designs.
- **Wide Flexibility** – At least one of two candidate designs must be usable on every make for every automotive manufacturer.
- **Easy Installation** – Although performance suffers with temporary mounting schemes, the prototype equipment must be used on multiple test vehicles for future testing and, therefore, must allow easy installation.
- **Involve Supply Base** – Engaging automotive suppliers early in development allows for wide understanding of technological hurdles and possibilities, and taps into vast engineering knowledge.
- **Answer Unknowns** – Several basic unknowns (e.g., desired polarization) needed answering to continue with standards development and future test kit designs.

1.1.1 Acceptable Performance

The term “acceptable performance” is unfortunately very application-specific and quite subjective; acceptable to one system or engineer might not be acceptable to another. Therefore, the Crash Avoidance Metrics Partnership Vehicle Safety Communications Consortium (CAMP-VSCC) brainstormed and investigated various safety systems and estimated the range of communications required for task effectiveness (see CAMP-VSCC Task 3 Report). For the OBU communications, the longest desired range was 1000m, but the system (“Approaching Emergency Vehicle Warning”) would likely be permitted greater power allowances and, therefore, greater range than the typical OBU. The next greatest range was 500m (“Wrong Way Driver Warning”), and almost every other safety-related system needed 400m or less in range. Therefore, 400m was deemed the minimum

acceptable system capability with 500m being a desired performance range given 100mW of power.

1.1.2 Statement of Work

The following document was written in conjunction with CAMP-VSCC by the identified contractor, M/A-COM, under a statement of work with the following activities:

- Activity 1: Define Target Antenna Performance
- Activity 2: Develop Candidate Antenna Designs
- Activity 3: Simulate Antenna Performance
- Activity 4: Prototype Reference DSRC Antennas
- Activity 5: Unit-Level Evaluation
- Activity 6: Vehicle-Level Evaluation
- Activity 7: Project Management
- Activity 8: Final Report

CAMP-VSCC chose a contractor to work on the program based upon antenna knowledge/experience, automotive knowledge/experience, quality of the facilities in regards to the Subproject's needs, proximity of facilities/personnel, cost, ability to meet the CAMP terms and conditions, and a subjective evaluation of the ease of program management.

As a result, the program succeeded in delivering all the identified deliverables and performance objectives with encouraging results regarding potential performance based upon a very conservative power budget. Two prototype antennas were simulated and built, and subsequently both designs were tested in the anechoic chamber, on the test range, and atop test vehicles. Field validation showed that the encouraging simulations and chamber results not only accurately predicted base performance, but also that true communication range exceeded expectations.

1.2 Definitions

The word "shall" will be used to state binding requirements of the component defined by this document. These requirements will be verified.

The word "must" will state requirements of other components or subsystems whose definitions are outside the scope of this document.

The word “will” is used to state either of the following:

a. Conditions that result from the immutable laws of physics.

b. Conditions that result from adherence to other stated binding requirements.

The word “withstand” will be defined as “Maintain design-intended functions and structural integrity while being subjected to the specified conditions.”

1.3 Applicable Documents

This section lists documents referenced as requirements for the component.

1.3.1 Government Documents

Suppliers are expected to be aware of and comply with worldwide component and vehicle standards and regulations where applicable. Requirements of national governments shall apply even if not explicitly stated below. Specific national requirements may be waived under specific purchase orders or engineering part drawings.

- FCC Report ET 98-7 Engineering & Technology Action – June 11, 1998
- FCC 02-302 NOTICE OF PROPOSED RULEMAKING AND ORDER Adopted: November 7, 2002 Released: November 15, 2002

1.3.2 CAMP – VSCC Documents

- Task 6 Antenna SOW - Vehicle Safety Communications Consortium: DSRC
- Antenna Basic Performance Understanding Statement of Work

1.3.3 Industry Documents

ASTM-E2213-02	Telecommunications and Information Exchange Between Roadside and Vehicle Systems — 5 GHz Band Dedicated Short Range Communications (DSRC) Medium Access Control (MAC) and Physical Layer (PHY) Specifications
IEEE 802.11a	Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications High-speed Physical Layer in the 5 GHz Band

1.4 Requirements

1.4.1 Component Definition

This section gives a high-level overview of the antenna assembly and defines its physical and electrical performance requirements.

1.4.1.1 Antenna Assembly

The antenna assembly will consist of the radiating element, a radome (housing), the mechanical mounting mechanism, a coaxial cable pigtail, and the SMA JACK connector.

1.4.1.2 System Operation

The antenna sub-system shall be capable of communicating with roadside units (RSUs) approximately 5m in height and other vehicles equipped with similar on-board units (OBUs). It is desired that the system will be capable of OBU-OBU and OBU-RSU communication at distances of up to 500m.

1.4.2 Environmental Requirements

1.4.2.1 Water Intrusion

The antenna shall be capable of withstanding typical outdoor exposure to rain, snow, and humidity without degradation of performance and/or mounting. The antenna, when properly installed to the vehicle, shall also provide a watertight seal to prevent leakage into the vehicle.

1.4.2.2 Temperature

The antenna shall be capable of withstanding typical vehicle interior and exterior temperatures. Specifically, the components in the antenna system shall meet the specifications when subjected to a temperature range of –40°C to +85°C (–40°F to +185°F).

1.4.2.3 Vibration

The antenna assembly shall be capable of withstanding typical vibrations as a result of normal shipping and handling and VSCC testing / demonstrations.

1.4.3 Electrical Requirements

Due to vehicle and mounting variations these requirements shall be met across the entire ITS-RS band (5.850-5.925GHz) as tested in an anechoic chamber.

1.4.3.1 5.9GHz Antenna Performance Requirements

1.4.3.1.1 <u>Operating Frequency Range</u>

The antenna shall meet all requirements across the entire ITS-RS band (5.850-5.925GHz) as defined by ASTM-E2213-02.

1.4.3.1.2 Impedance Match Requirement

The antenna shall have a VSWR equal to or better than 2:1 relative to 50 Ω measured at the antenna feed point. This specification is to be met across the entire ITS-RS band (5.850-5.925GHz) as defined by ASTM-E2213-02.

1.4.3.1.3 Free-Space Gain

The free-space gain of the antenna shall meet or exceed the following requirements measured at the antenna feed point. For antennas that require a ground plane, the free-space gain shall be measured with the antenna mounted at the center of a 1.0m rolled edge circular ground plane. If a diversity scheme is used the composite pattern of the individual antennas shall meet the same requirements.

Elevation Angle	Min Linear-Averaged Mean Gain	Polarization
0 (Horizon)	0dBil *	Vertical and RCP

* Assumes 100mW transmit power for OBU-OBU communications for distances up to 500m. This gain is necessary to support 3dB cable loss in the free-space link budget.

1.4.3.1.4 Vehicle Level Simulation

The expected antenna performance on a vehicle shall be simulated to demonstrate potential performance impacts due to vehicle structures. However, due to variation of vehicle/mirror types and software modeling limitations, no specific gain requirements will be identified. If actual vehicles cannot be modeled or does not provide additional benefit, the following guidelines should be met:

1. Models for roof-mounted antennas should assume that the antenna mounting location is free of roof racks, sunroofs, etc. relative to the signal wavelength. Based on this assumption, the vehicle roofs can be modeled as infinite ground-planes.
2. Sufficient side mirror material area should be included, in worst-case geometries, relative to the signal wavelength to ensure far field effects are captured.
3. If the mounting location is near other main body structures, relative to the signal wavelength, those structures should be included as necessary to ensure far field effects are captured.

1.4.3.1.5 Pattern Coverage

The antenna reception pattern shall provide sufficient coverage 360° in azimuth from 0° to 45° elevation. If sufficient coverage cannot be demonstrated with a single antenna strategy a diversity antenna strategy may be utilized. If a diversity scheme is used the composite pattern of the individual antennas shall meet the

same requirements. Negative elevation angles are considered out of scope since most OBU communication will take place at near-zero relative elevation.

1.4.3.1.6 Polarization

The antenna design shall be capable of receiving either RHCP or vertical polarization. In the development of the candidate designs it would be preferred to have one of each design to demonstrate satisfactory performance with either polarization. The contractor shall provide supporting documentation regarding their selection of antenna polarization.

1.4.3.2 Electrical Interface Requirements

1.4.3.2.1 Coaxial Cable Electrical Properties

For antenna cable routing that is not subjected to repeated flexing and/or tight bend radii, the coaxial cable shall be RG-316 U with the following properties:

a) Nominal impedance shall be 50Ω.

b) Nominal capacitance shall be 29.0 pF/ft.

c) Attenuation shall be 0.394 dB/m at 200 Mhz and 0.951 dB/m at 1000 MHz.

d) DC ground resistance shall be 0.0279 Ω/m typical.

e) Center conductor D.C. resistance shall be 0.2759 Ω/m typical.

f) Isolation resistance between the center pin (conductor) and the shield shall be greater than $1x10^6$ Ω.

For antenna cable routing that has the potential to be subjected to repeated flexing and/or tight bend radii, the coaxial cable shall be Thermax 0.070” cable with the following properties:

a) Nominal impedance shall be 50 Ω.

b) Nominal capacitance shall be 29.0 pF/ft.

c) Attenuation shall be 0.46 dB/ft at 1575 MHz and 0.96 dB/ft at 5.90 GHz.

d) DC ground resistance shall be 0.0279 Ω/m typical.

e) Center conductor D.C. resistance shall be 0.2759 Ω/m typical.

f) Isolation resistance between the center pin (conductor) and the shield shall be greater than $1x10^6$ Ω.

If the cable routing is such that a lower loss cable is required, an inline connector can be used to transition between Thermax 0.070” or RG316 U and LMR195. The LMR195 cable should have the following properties: (reference www.timesmicrowave.com)

a) Nominal impedance shall be 50 Ω.

b) Nominal capacitance shall be 24.3 pF/ft.

c) Attenuation shall be 28 dB/ft at 5.80 GHz.

d) DC ground resistance shall be 4.9 Ω/1000ft typical.

e) Center conductor D.C. resistance shall be 7.58 Ω/1000ft typical.

f) Isolation resistance between the center pin (conductor) and the shield shall be greater than $1x10^6$ Ω.

1.4.3.2.2 Connector

The antenna coaxial cable pigtail shall be terminated with a SMA JACK connector, to be mated with the PC test kit.

The connector should be Tyco-Amp P/N 1051855-1 (SMA Straight Cable Jack, Crimp) or equivalent and must mate to Tyco-Amp P/N 1082034-1 (SMA Straight Cable Plug, Crimp) or equivalent.

1.4.4 Physical Requirement

1.4.4.1 Antenna Appearance

The final antenna appearance will be determined by mounting location and electrical design. The units to be delivered in Activity 4 do not require formal styling but should follow the guidelines detailed below. Potential styling options should be presented to the TMT during the development process and approved/documented during the weekly program review meetings. The final styling shall be aesthetically acceptable (to the VSCC) for internal and public research activities, tests, and demonstrations.

1.4.4.1.1 Finish

The visible portions of the antenna, when mounted to the vehicle, should have a smooth finish free of burrs, flashing, sink marks, blemishes, etc.

1.4.4.1.2 Color

The visible portions of the antenna, when mounted to the vehicle, should be black in color.

1.4.4.1.3 Shape

The shape of the visible portions of the antenna, when mounted to the vehicle, should be styled in order to minimize its overall size, visibility, and expected wind noise.

1.4.4.2 Mechanical

1.4.4.2.1 Mechanical Mounting

Designs shall be optimized for easy installation & removal, ruggedness, and versatility when mounting across a wide variety of vehicle types, makes, and models.

Side-View Mirror Assembly

The side-view mirror antenna assembly shall be capable of mounting to most vehicle side mirror housings. The mounting mechanism should be designed to accommodate as wide a range of vehicle types as possible. The design should be a snap-fit or clamp-type attachment with the following design goals:

- Capable of withstanding wind forces due to vehicle travel at up to 100mph.
- Tool-free installation & assembly.
- No damage to mirror housing as a result of installation/removal.

Roof Mounted Assembly

The roof mounted antenna assembly shall be capable of mounting to all sheet metal vehicle roofs. The mounting mechanism should be designed to accommodate as wide a range of vehicle roof curvatures/profiles as possible and should not require a hole in the roof for cable routing. The design should be a magnetic base attachment with the following design goals:

- Capable of withstanding wind forces due to vehicle travel at up to 100mph.
- Tool-free installation and assembly.
- No damage to vehicle roof as a result of installation/removal.

1.4.4.3 Label Requirements

The visible portion of the antenna, when mounted to a vehicle, shall be free of any markings, logos, company names, etc. The antenna shall be clearly marked with a label attached to the pigtail that includes a part number and serial number (e.g. 001 through 040). If a diversity scheme is implemented that requires antenna pairs the label should include identification markings to signify front/back or left/right (e.g. 001R and 001L).

1.4.5 Antenna Correlation Matrix

The Antenna Correlation Matrix will trace all factors, developed/recognized constraints or enablers directly to originating requirements from the VSCC TMT and applicable documents identified in section 2. The matrix will also identify the level of testing required to show compliance with each requirement and when the results of such testing were approved.

1.4.5.1 Antenna Correlation Matrix Terminology

This paragraph defines the acronyms, abbreviations, and special terms used in this section.

Validation Method:	Level:
A = Analysis	V = Vehicle

D = Demonstration

C = Component (Anechoic Chamber)

I = Inspection

T = Test

1.4.5.2 Antenna Correlation Matrix

Requirement		**Source**			**Validation**	
Paragraph	Description	Document/Meeting	Paragraph	Date	Method	Test Report/Date
3.2.1	Water Intrusion	SOW	ACTIVITY 2	02JUL03	C/T	
3.2.2	Temperature	ASTM-E2213-02	8.8.6	10JUN02	C/T	
3.2.3	Vibration	SOW	ACTIVITY 2	02JUL03	C/T	
3.3.1.1	Operating Frequency Range	ASTM-E2213-02	8.8.3.1	10JUN02	C/T	
3.3.1.2	Impedance Match	N/A	N/A	30OCT03	C/T	
3.3.1.3	Free Space Gain	N/A	N/A	30OCT03	C/T	
3.3.1.4	Vehicle Level Simulation	TELECON	N/A	03NOV03	C/A	
3.3.1.5	Pattern Coverage	KICKOFF	N/A	26SEP03	C/T	
3.3.1.6	Polarization	SOW	ACTIVITY 2	02JUL03	C/T	
3.3.2.1	Coaxial Cable Electrical Properties	N/A	N/A	30OCT03	C/A	
3.3.2.2	Connector	KICKOFF	N/A	26SEP03	C/I	
3.4.1	Antenna Appearance	SOW	ACTIVITY 2	02JUL03	C/I	
3.4.2.1.1	Antenna Assembly Mounting Side-view Mirror Assembly	TELECON	N/A	27OCT03	C/I	
3.4.2.1.2	Antenna Assembly Mounting Roof Mounted Assembly	TELECON	N/A	27OCT03	C/I	
3.4.3	Label requirements	TELECON	N/A	06OCT03	C/I	

1.5 Selection of Antenna Polarization

The Task 6 Antenna SOW requires both vertical and circular polarization antenna design. M/A-COM strongly recommends the adoption of vertical polarization only for the following reasons:

1. Vehicle sheet metal will serve as the ground plane and will degrade reception of horizontally polarized waves at or near the horizon.

Figure 1 is a simple diagram of a free space – perfect conductor interface. By utilizing the Kirchoff's voltage law around the boundary *abcd* and the fact that E=0 everywhere inside the conductor you can determine one of the basic boundary conditions for electromagnetic fields, that the tangential component of the E field on a conductor surface is zero (E_t=0).

$$\text{As } \Delta h \to 0$$

$$\oint_{abcd} E \cdot dl = E_t \Delta w = 0$$

$$E_t = 0$$

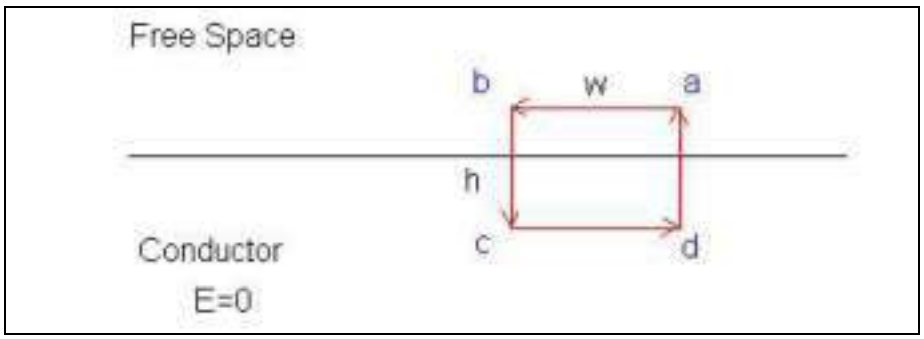


Figure 1-A. Free Space – Conductor Interface

To further illustrate this condition, M/A-COM has provided pattern data of a circular polarized antenna on a ground plane receiving rotating linear signals over different elevation angles (Figure 2). The source antenna is a vertically polarized antenna that is rotating to create right hand circular polarized waves. At boresight the ground plane does not impact the antenna reception and the pattern shows high circular polarization purity and low axial ratio. At the horizon, you can see the effects of the ground plane negating the horizontal component of the rotating linear transmission antenna. The lower elevations have a high axial ratio with the maximum coming from the vertical polarization and the deep nulls resulting from the horizontal polarization.

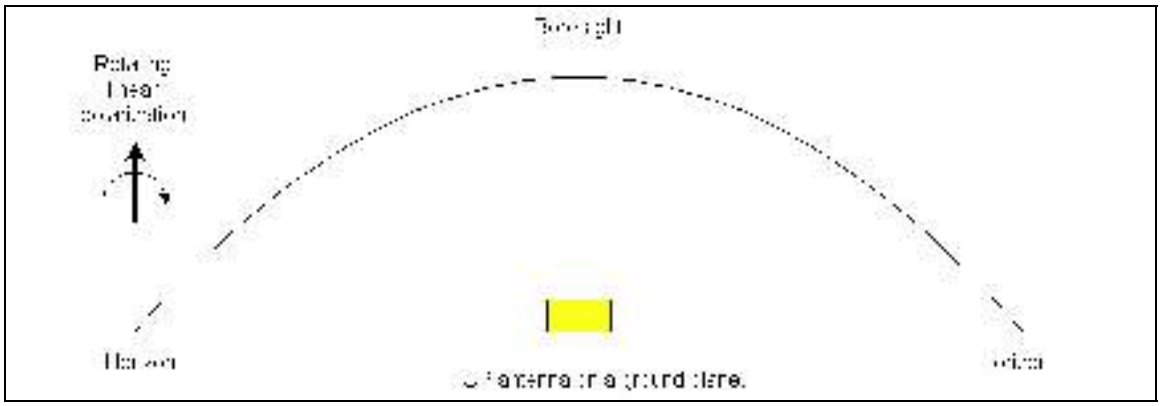


Figure 1-B. Test Setup for CP Antenna

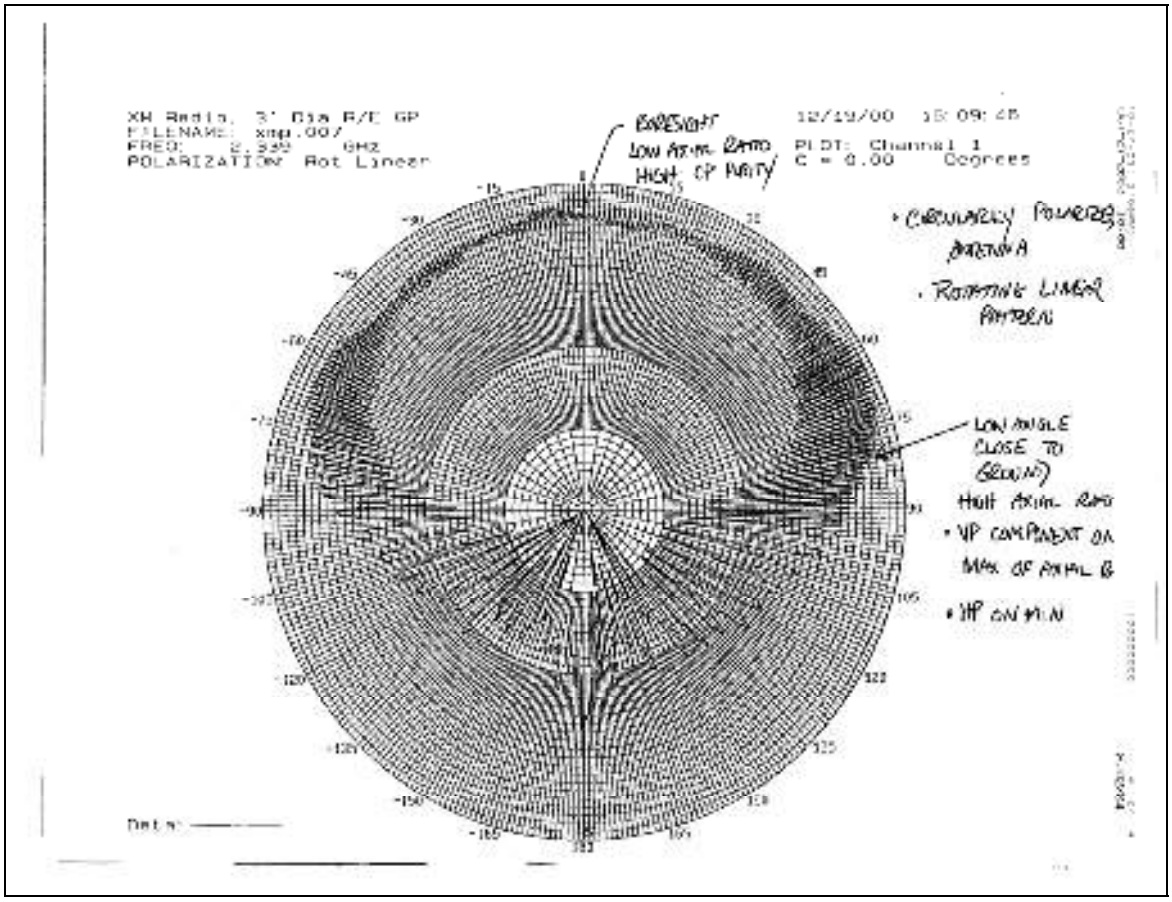


Figure 1-C. CP Antenna Reception on a Ground Plane

2. System complexity would be increased due to CP antenna limitations and pattern coverage requirements.

Initial analysis has shown that at least four antennas would be required to provide sufficient omni-directional coverage with acceptable axial ratio across the required elevation angles. The current receiver has diversity capability for two antennas. It is expected that the added cost of additional components and modification of the receiver to accommodate four antennas would significantly increase the overall subsystem cost. Additionally, this type of solution would not eliminate the issues described in item 1.

1.6 Thermax 0.070” Cable Test Data

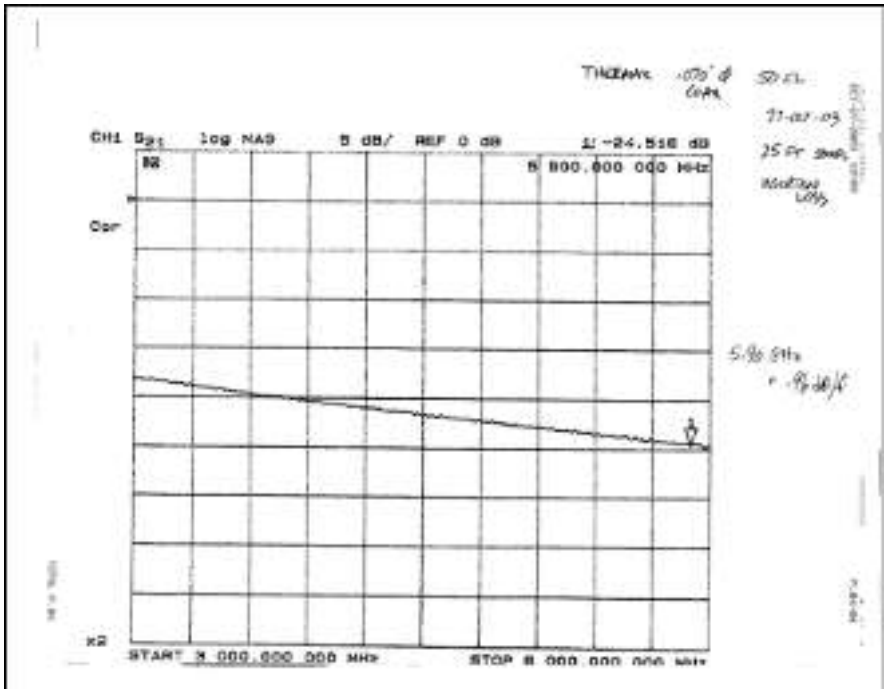


Figure 1-D. Swept Gain of a 25 ft Long Sample From 3GHz to 6GHz.

2 Antenna Subproject Simulation Results

2.1 Candidate Antenna Design Description

M/A-COM has developed two potential antenna designs, a magnetic mounted roof application and a diversity solution for a clamp-type side-view mirror application.

Roof mounted antenna design description:

- 5/8-wavelength monopole (internal element is approximately 1” tall).
- Requires approximately 2” radius of uninterrupted sheet metal surrounding the mounting location to serve as the ground plane.
- Overall omni-directional pattern at the required elevation angles.
- Geloy plastic radome (housing).
- Magnetic mounting mechanism with a coaxial pigtail parallel to the roof line.

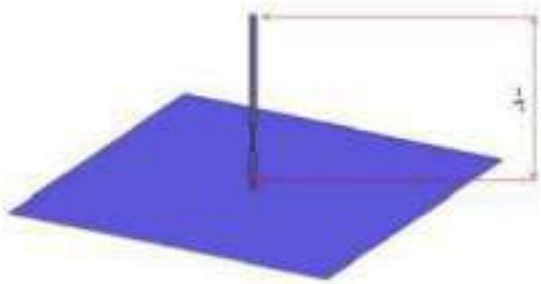


Figure 2-A. Initial Antenna Element Design Over a Ground Plane

Side mirror mounted antenna design description:

- Two-element dipole array.
- Ground plane independent
- Individual antennas will provide cardiod pattern coverage.
- Geloy plastic radome (housing).
- Clamp-type mounting mechanism with bottom exit coaxial pigtails.

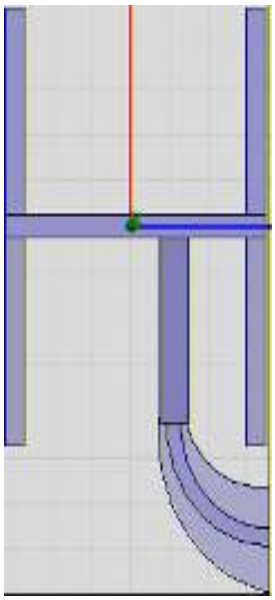


Figure 2-B. 2D View of Dipole Array

Figure 2-C. Isometric View of Dipole Array

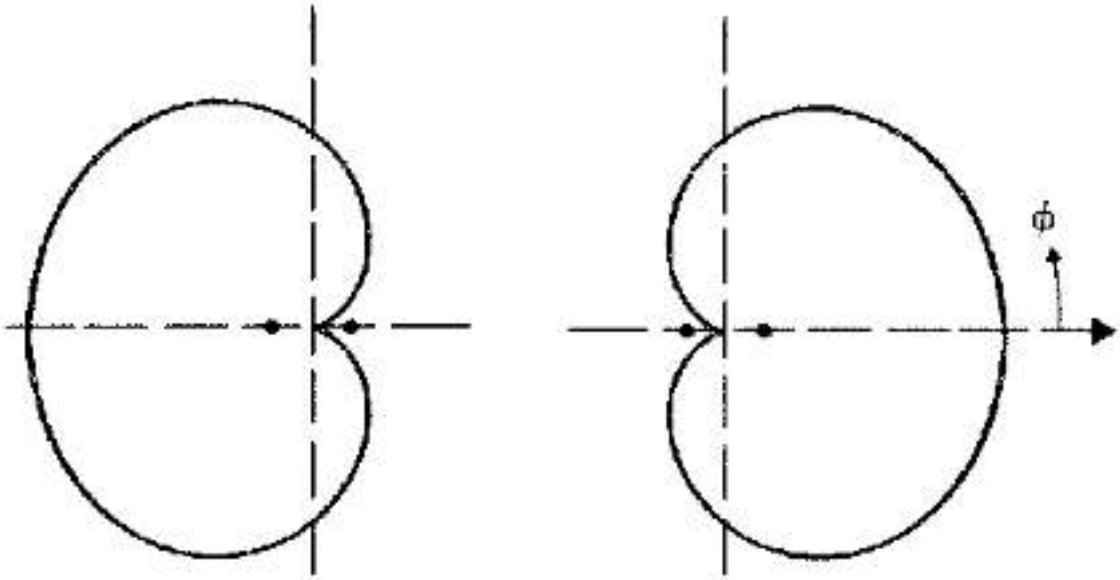


Figure 2-D. Theoretical Cardiod Patterns for Each Dipole Array (Driver/Passenger Side)

2.2 Antenna Design Overview

M/A-COM has developed two potential antenna designs to meet the Antenna Subproject Specification (Revision 1.1 11/5/03): a magnetic mounted roof application and a diversity solution for a clamp-type side-view mirror application. Due to the limitations and complexity of systems that incorporate circular polarized antennas both of these designs will be vertically polarized.

2.3 Software Overview

M/A-COM is currently using HFSS V9.0 and Designer V1.1 from Ansoft Corp to simulate antenna design performance. HFSS is capable of performing finite element method (FEM) through automatic adaptive mesh generation and refinement, tangential vector finite elements, and Adaptive Lanczos Pade Sweep (ALPS). HFSS automatically computes multiple adaptive solutions until a user-defined convergence criterion is met. Field solutions calculated from first principles accurately predict all high-frequency behavior such as dispersion, mode conversion, and losses due to materials and radiation. Some of the key product capabilities that we will be incorporating in this simulation are (reference www.ansoft.com):

Powerful Drawing Capabilities
Features of the 100% AutoCAD-compatible, fully integrated ACIS solid modeler include:

Advanced Materials
The comprehensive materials database contains permittivity, permeability, electric, and magnetic loss tangents for common substances.

Powerful Features for Antenna Design
Calculate antenna metrics such as gain, directivity, far-field pattern cuts, far-field 3D plots, and 3dB beamwidth. Plot polarization behavior including spherical field components, circular polarization field components, Ludwig's third definition field components, and axial ratio. Model half, quarter, or octet symmetry and automatically calculate far-field patterns.

Wideband Fast Frequency Sweep
A new fast frequency sweep technology called Adaptive Lanczos Pade Sweep (ALPS) has been implemented for efficient broad-band simulation. ALPS can produce a reduced order model for the structure that is valid over a broad frequency range by computing the system poles and zeros. ALPS includes port dispersion to determine input power level versus frequency and out-of-band rolloff accurately.

2.4 Design Specifications

In free space, the model simulation should meet the following requirements (Reference Antenna Subproject Specification Rev 1.1 11/5/03):

VSWR equal to or better than 2:1 relative to 50 Ω (at the antenna feed point)

Elevation Angle	Min Linear-Averaged Mean Gain	Polarization
0 (Horizon)	0dBil *	Vertical and RCP

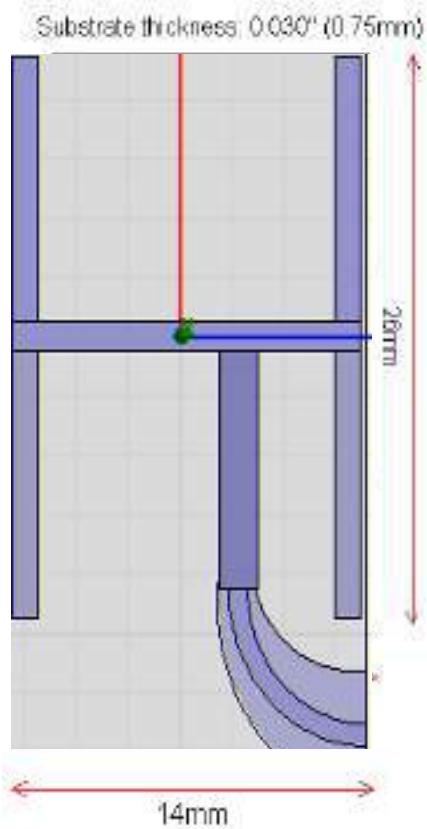
2.5 Side-View Mirror Simulation

2.5.1 Design Description

Side mirror mounted antenna design description:

- Two-element dipole array.
- Ground plane independent.
- Individual antennas will provide cardiod pattern coverage.
- Geloy plastic radome (housing).
- Clamp-type mounting mechanism with bottom exit coaxial pigtails.

2.5.2 Dimensioned Layout



2.5.3 Model Assumptions

The HFSS model assumed that the mirror housing and antenna radome would both be manufactured using the GE plastic Geloy. In order to determine the effects of the mirror and mirror housing both free-space and mirror-mounted models were simulated. The side-view mirror model assumed typical industry dimensions and materials. The results of these simulations have shown that very little energy would be transmitted in the direction of the vehicle. The combination of the distance to the A-pillar compared to the signal wavelength and the shape of the pattern support the assumption that the A-pillar would not have an affect on the pattern and therefore was not incorporated into the model.

2.5.4 VSWR/Impedance

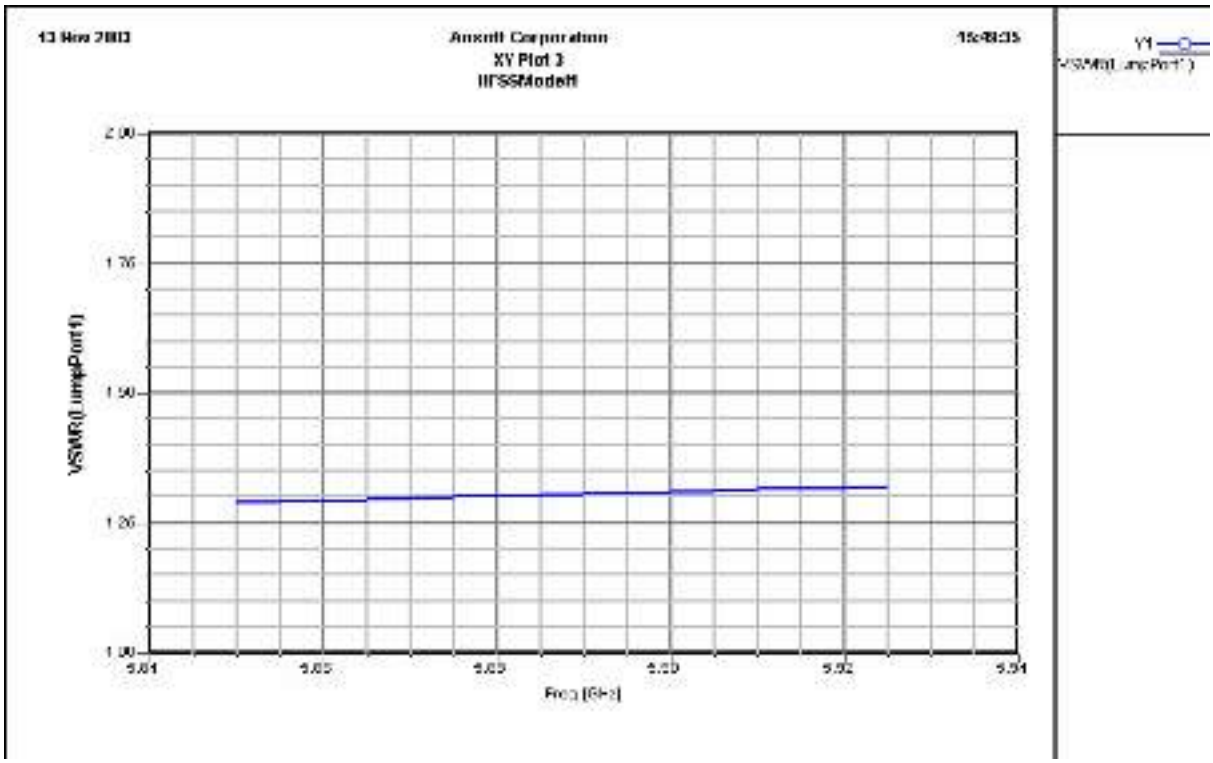


Figure 2-E. VSWR – Free-Space Dipole Array

The free-space swept VSWR models demonstrates that there is a sufficient margin to the 2:1 VSWR requirement. The VSWR is relative constant at ~1.3:1 across the entire frequency band 5.850GHz to 5.925GHz.*

** Note: Measuring VSWR at the antenna feed point is a conservative assumption. The added signal loss due to the coaxial cable pigtail will improve the VSWR as seen by the receiver.*

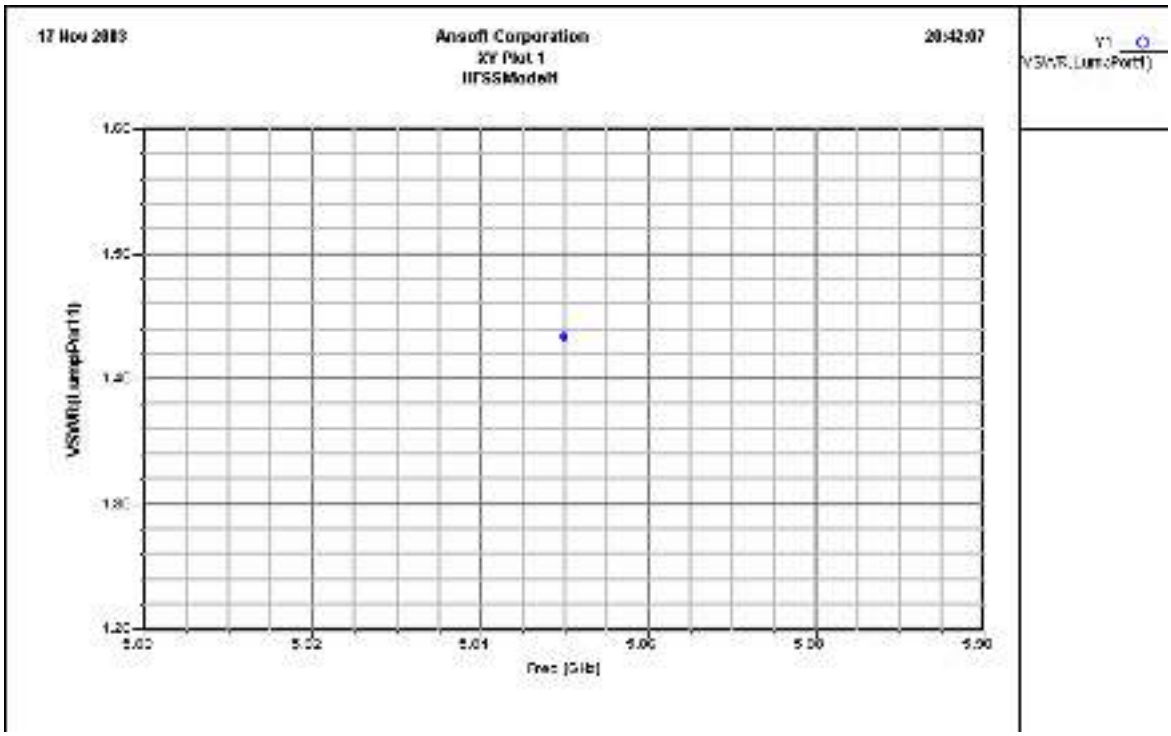


Figure 2-F. VSWR – Dipole Array on Side-View Mirror @ 5.850GHz

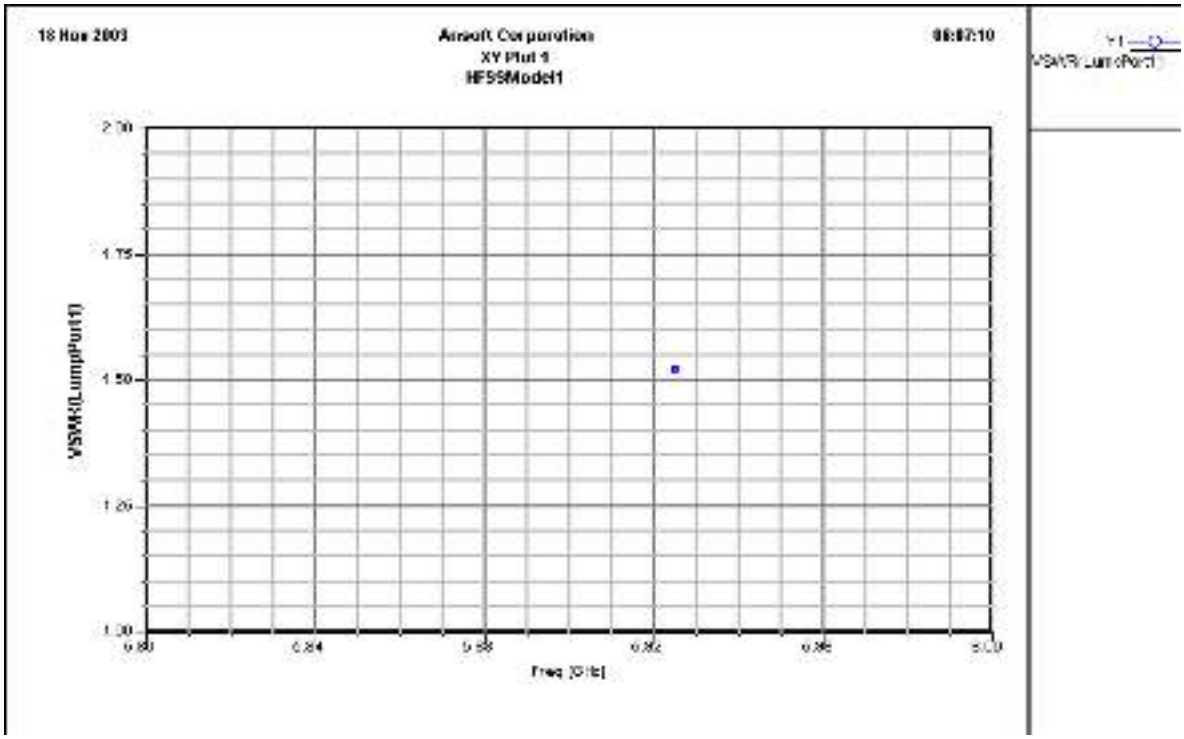


Figure 2-G. VSWR – Dipole Array on Side-View Mirror @ 5.925GHz

The VSWR model was also run with the typical side view mirror model. The side-view mirror structure did not have a significant impact on the input impedance of the antenna. Due to the size of the model and software limitations a mid-band VSWR measurement was taken: ~1.45:1 @ 5.9GHz.

2.5.5 Free-Space Pattern/Gain Plots (Bottom Feed-Point)

Gain plots and pattern measurements were simulated with the antenna element in free space encased in a generic cylindrical Geloy radome. The results show a 3-4dB margin to the 0dBi requirement from 0° (front) to 180° (rear) on one side of the vehicle. The peak gain of ~4.7dB is between 150° and 180°.

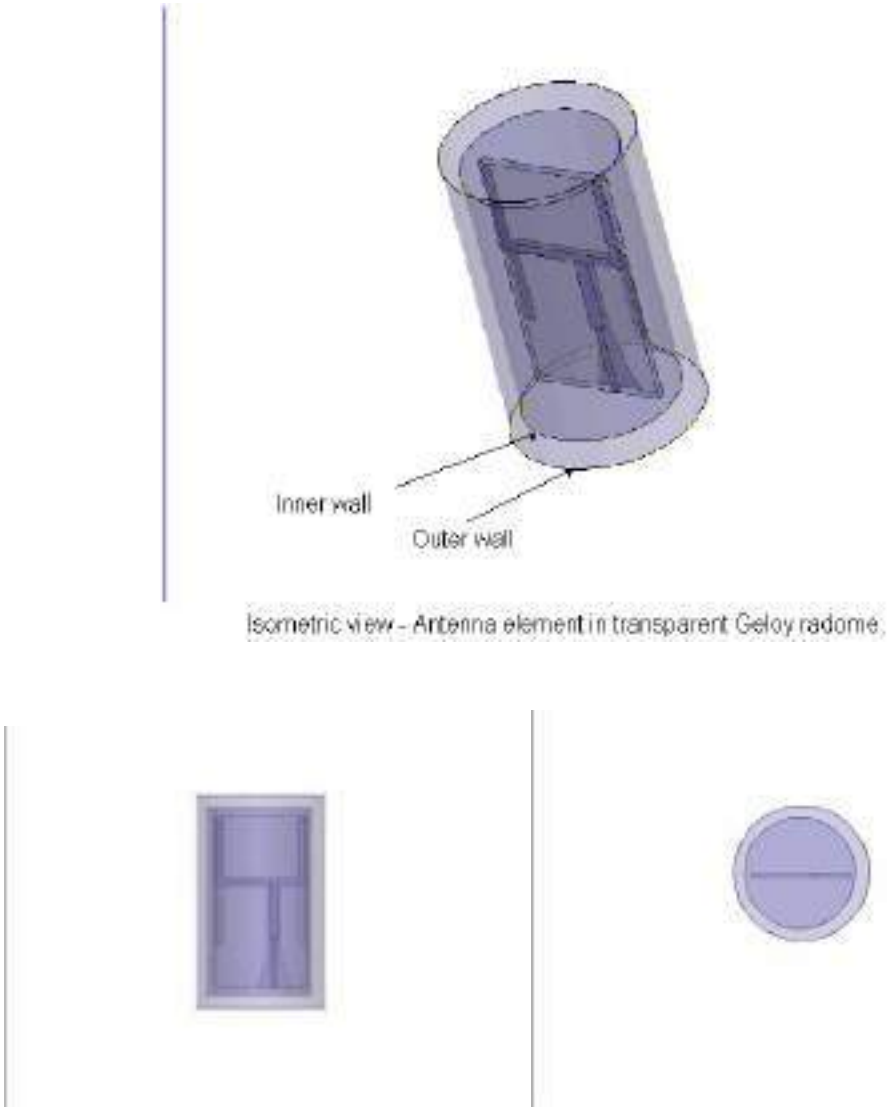


Figure 2-H. Side and Top Views

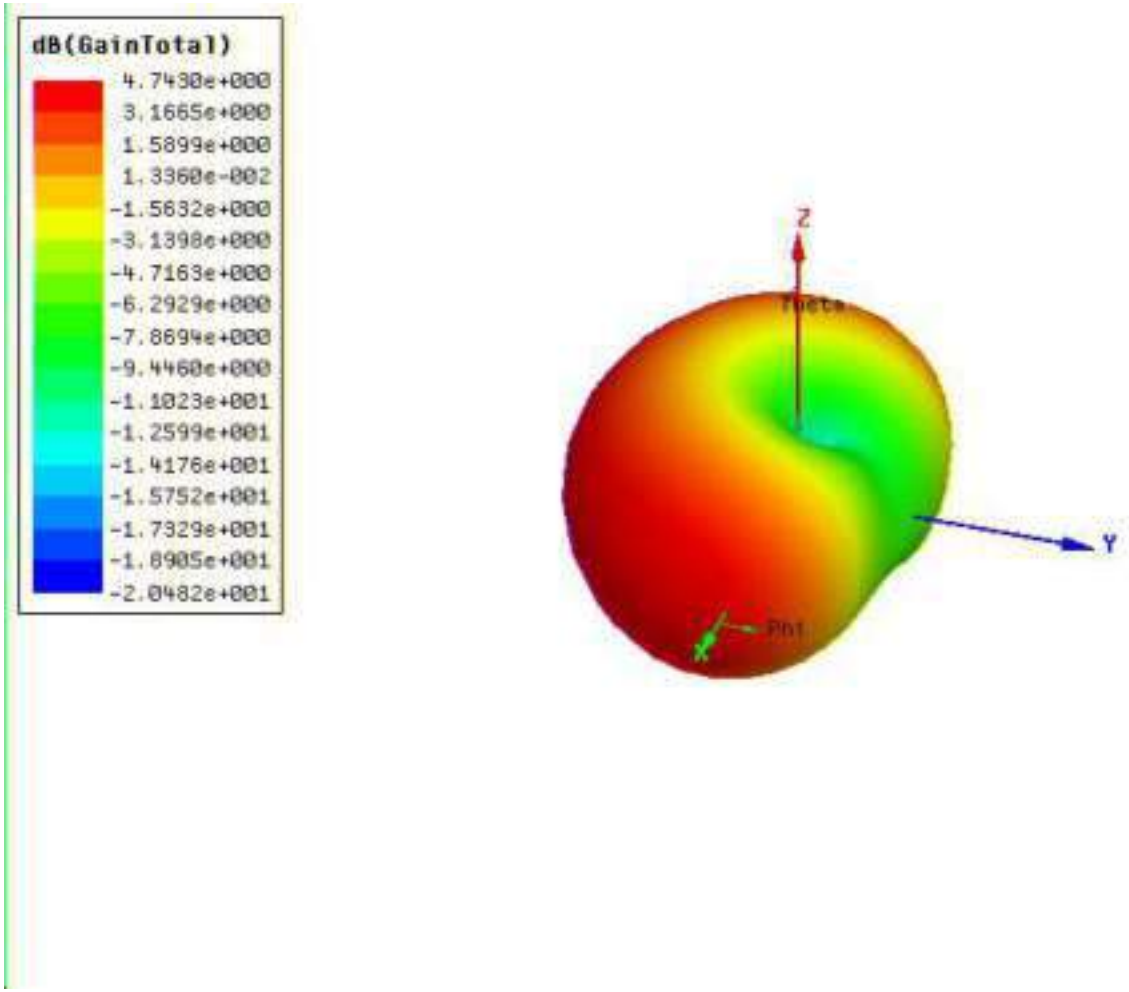


Figure 2-I. Isometric View – Dipole Array in Free Space (Bottom Feed-Point)

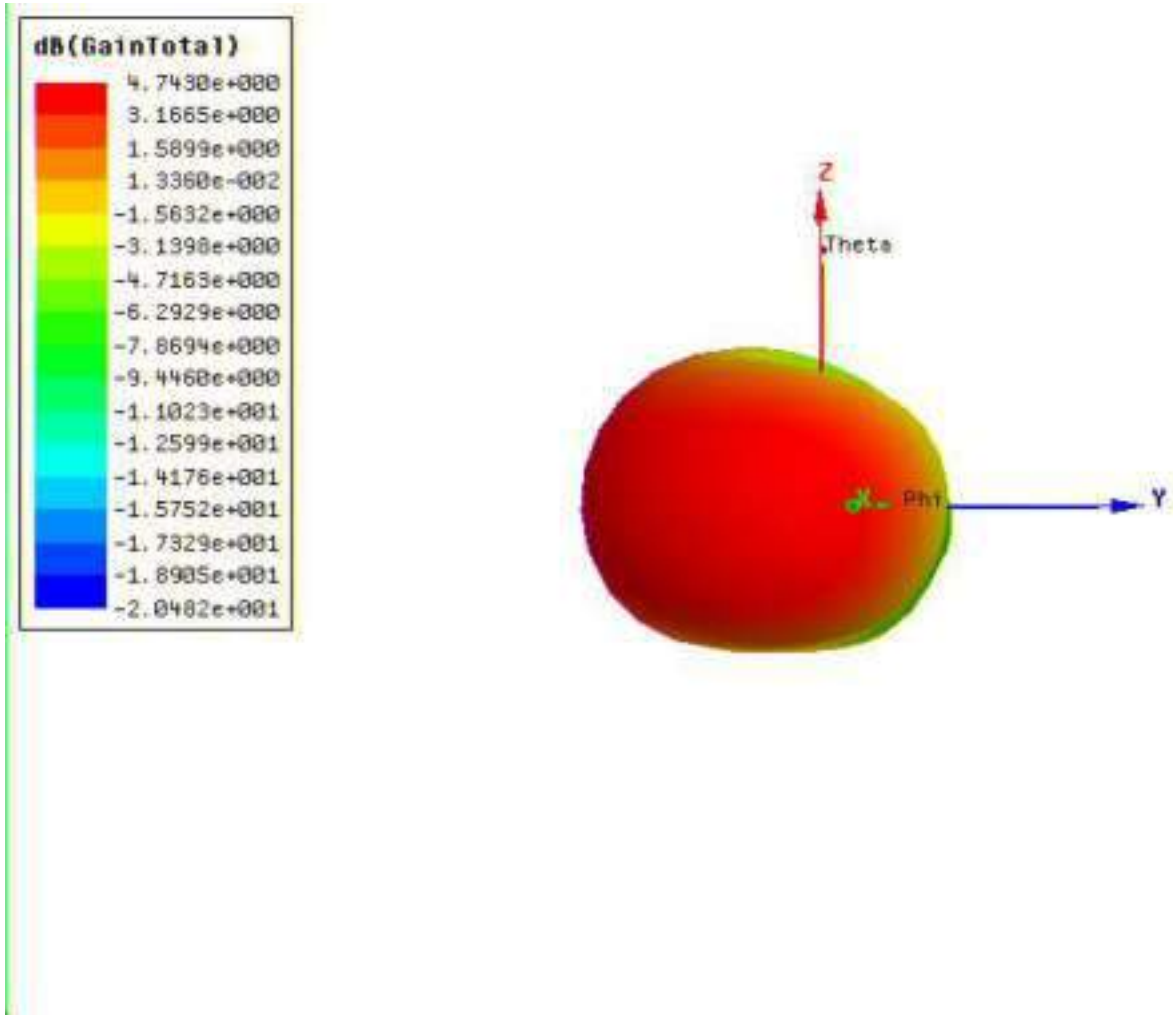


Figure 2-J. Side View– Dipole Array in Free Space (Bottom Feed-Point)

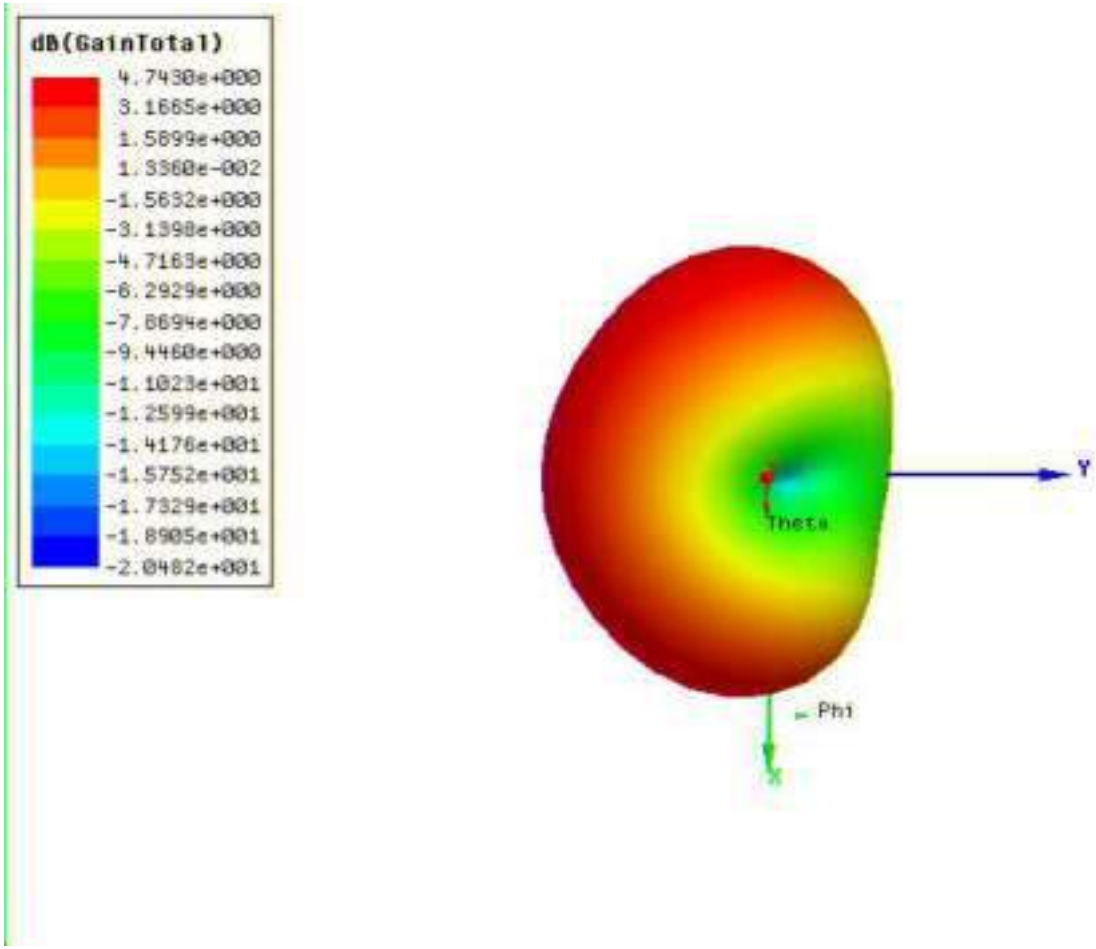


Figure 2-K. Top View– Dipole Array in Free Space (Bottom Feed-Point)

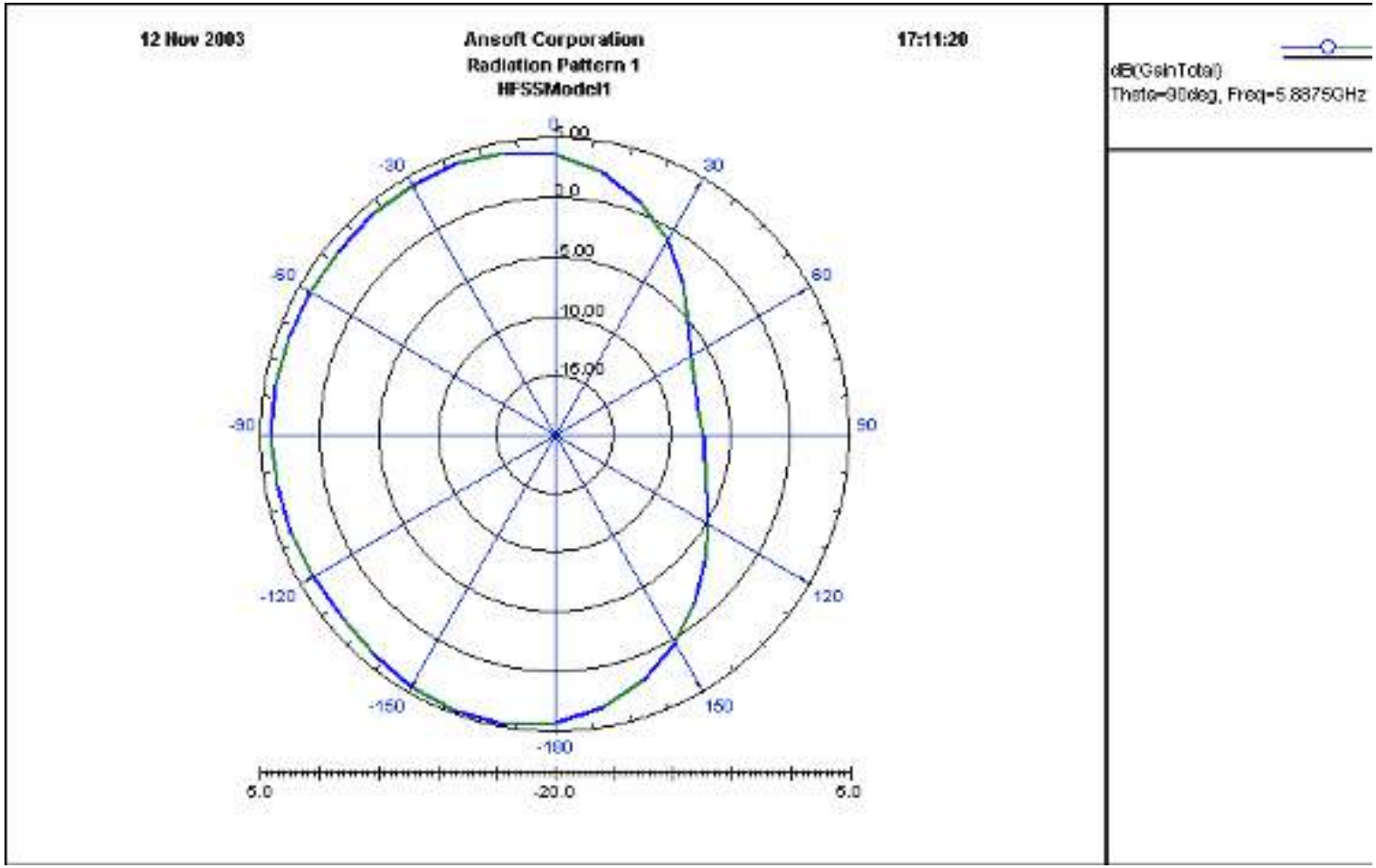
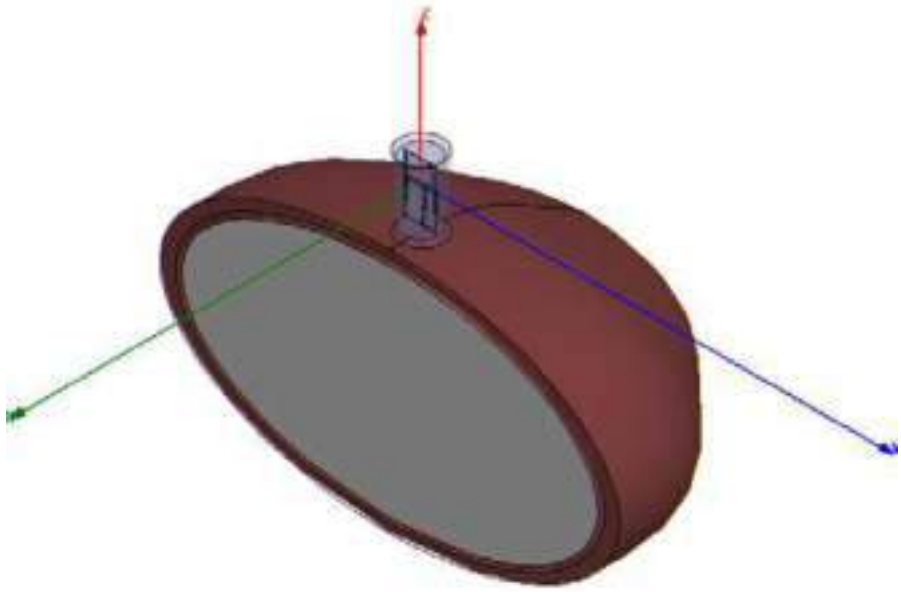
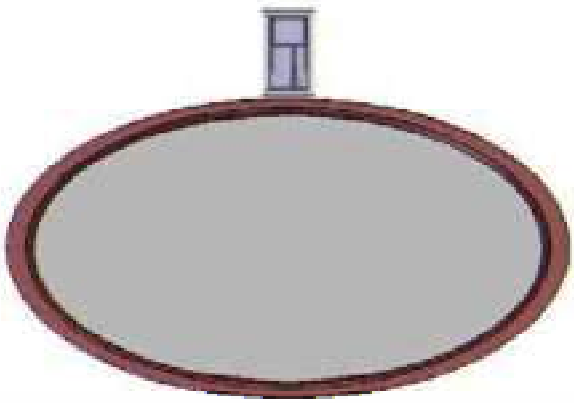


Figure 2-L. Radiation Pattern – Dipole Array in Free Space 0° Elevation (Bottom Feed-Point)

2.5.6 On-Mirror Pattern/Gain Plots

Gain plots and pattern measurements were then simulated with the antenna element in a generic cylindrical Geloy radome mounted on a typical side view mirror housing. The results show a perturbation of the pattern and a drop in gain towards the front and rear of the vehicle. The model still indicates satisfactory gain 0° (front) to 180° (rear) on one side of the vehicle. The peak gain of ~4.3dB is between 60° and 120°.





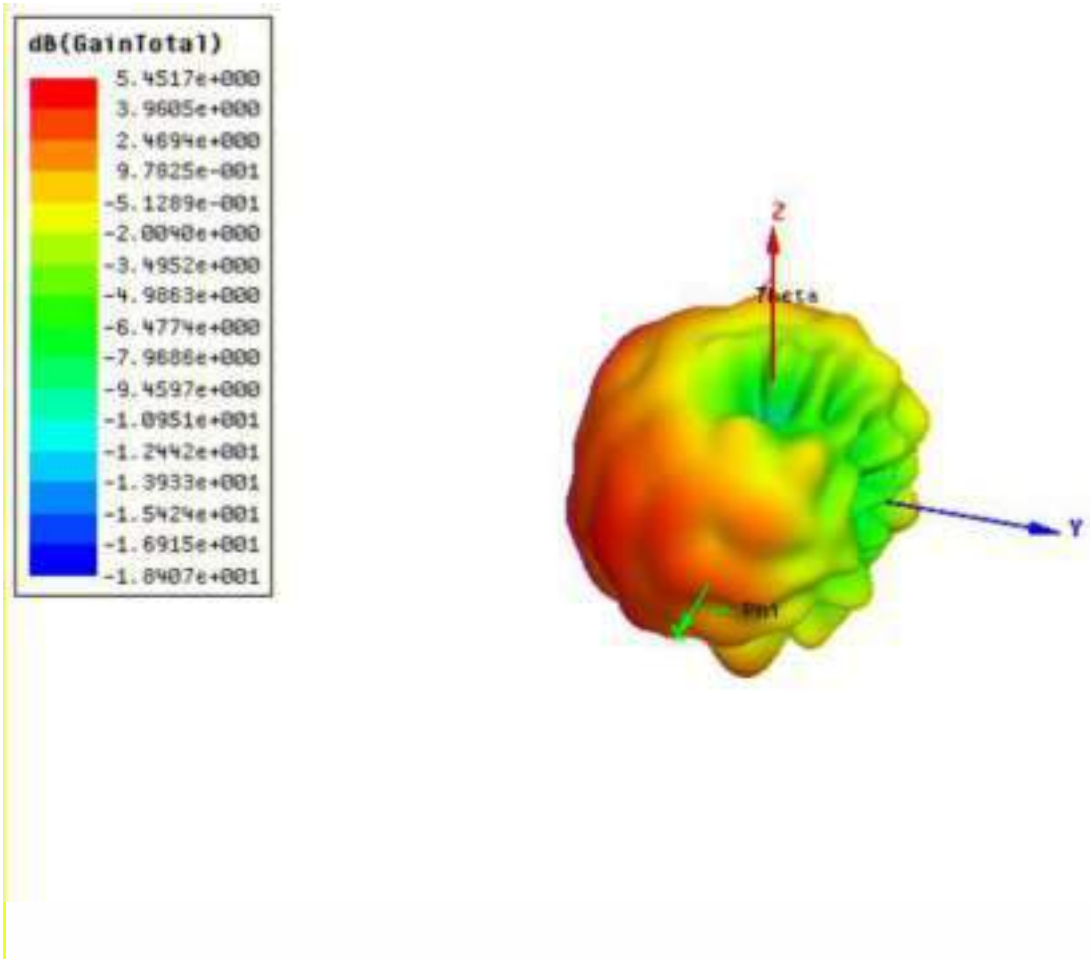


Figure 2-M. Isometric View – Dipole Array on Side-View Mirror

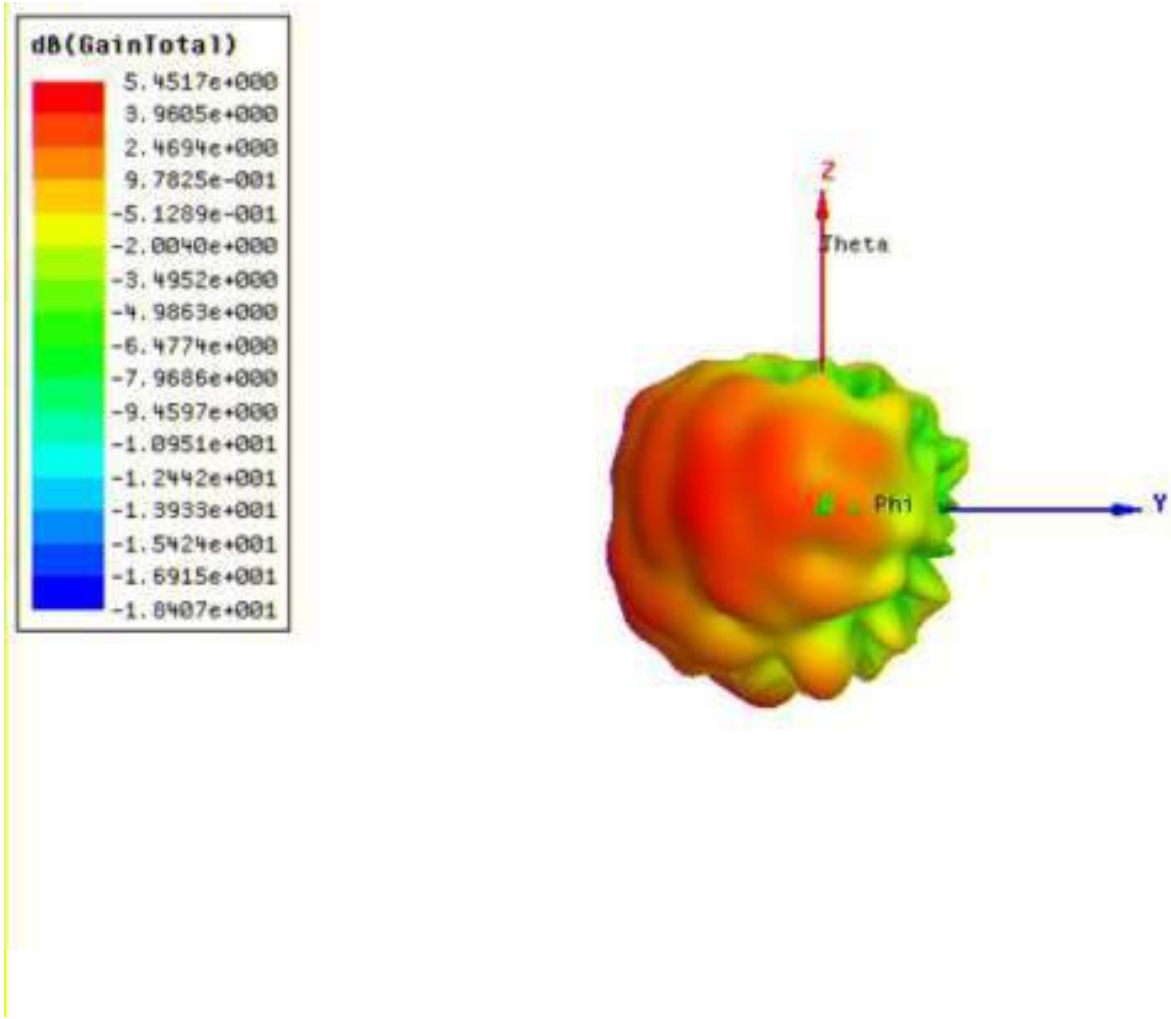


Figure 2-N. Top View – Dipole Array on Side-View Mirror

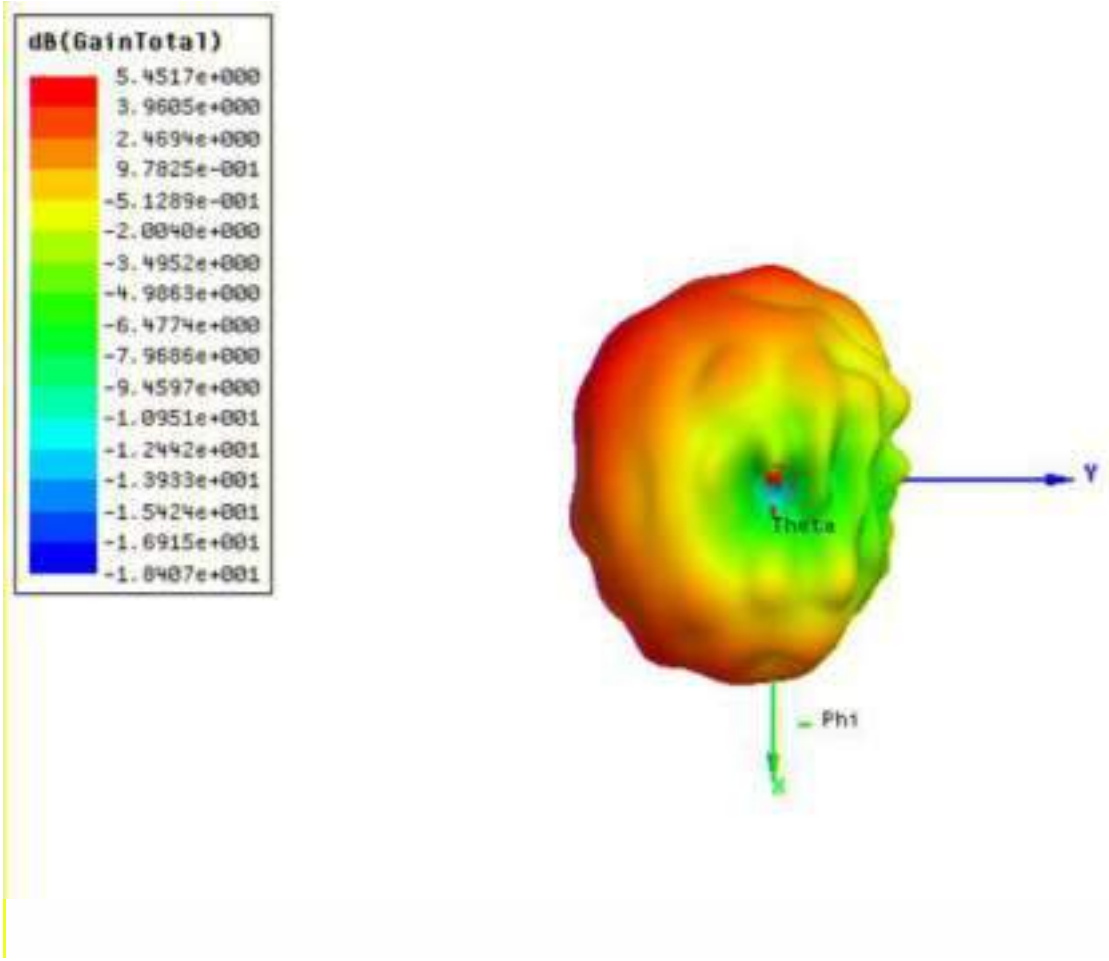


Figure 2-O. Side View – Dipole Array on Side-View Mirror

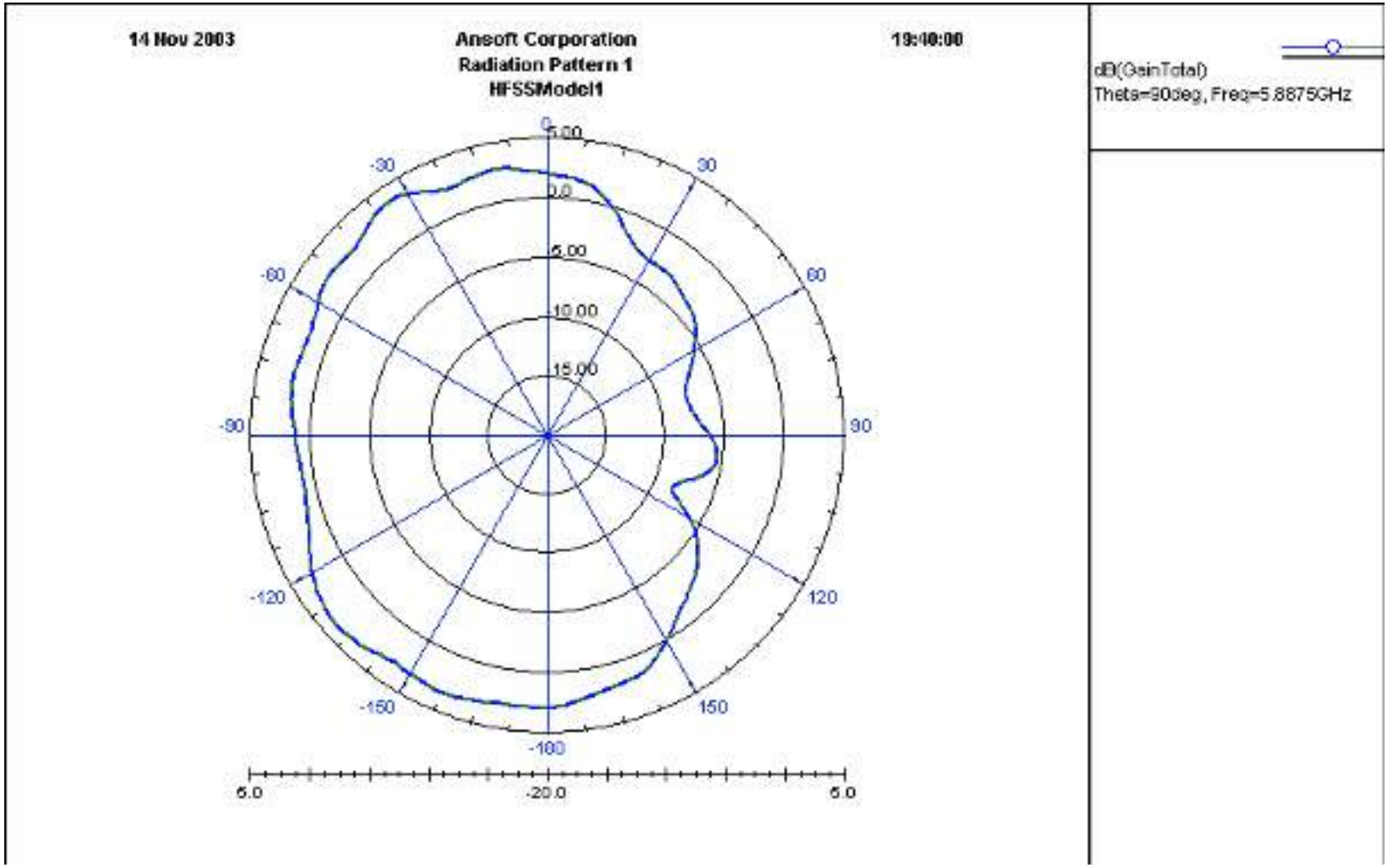
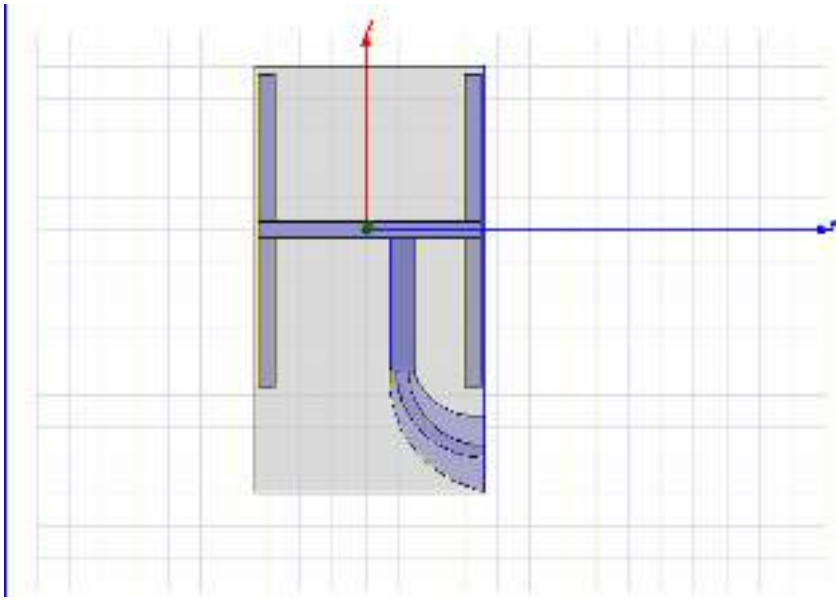


Figure 2-P. Radiation Pattern – Dipole Array on Side-View Mirror 0° Elevation

2.5.7 Free-Space Pattern/Gain Plots (Side Feed-Point)

To provide added flexibility for the mounting designs a second antenna element design was developed with a side feed-point. This simulation did not show any significant differences between the bottom and side feed-point designs.



Dipole Array -

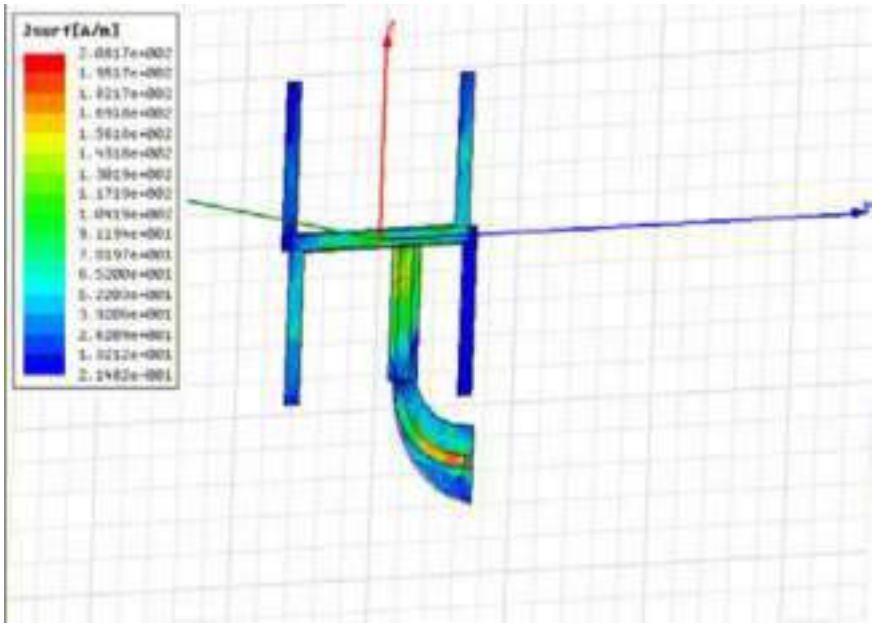


Figure 2-Q. Dipole Array – Current Distribution

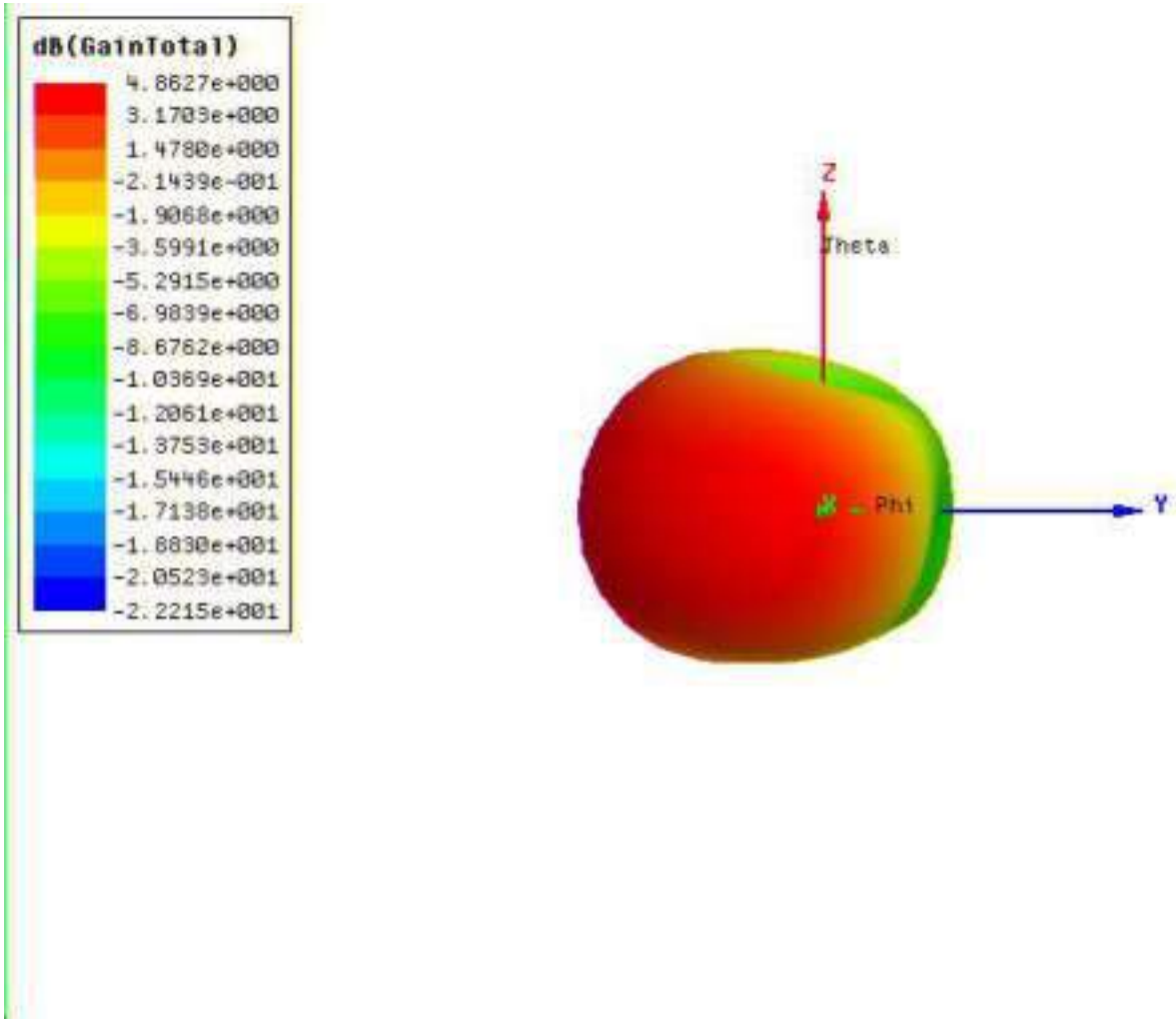


Figure 2-R. Side View– Dipole Array in Free Space (Side Feed-Point)

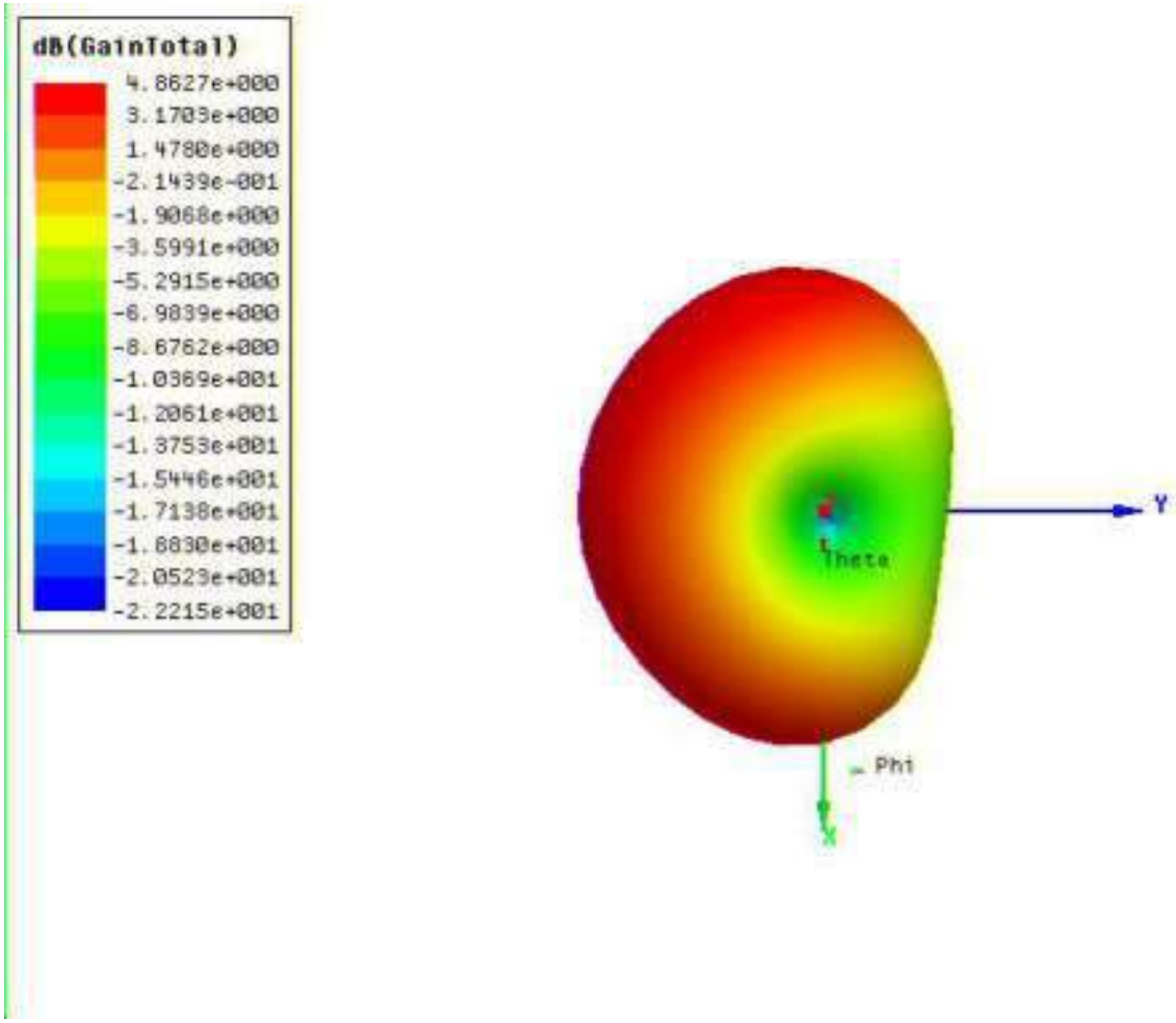


Figure 2-S. Top View– Dipole Array in Free Space (Side Feed-Point)

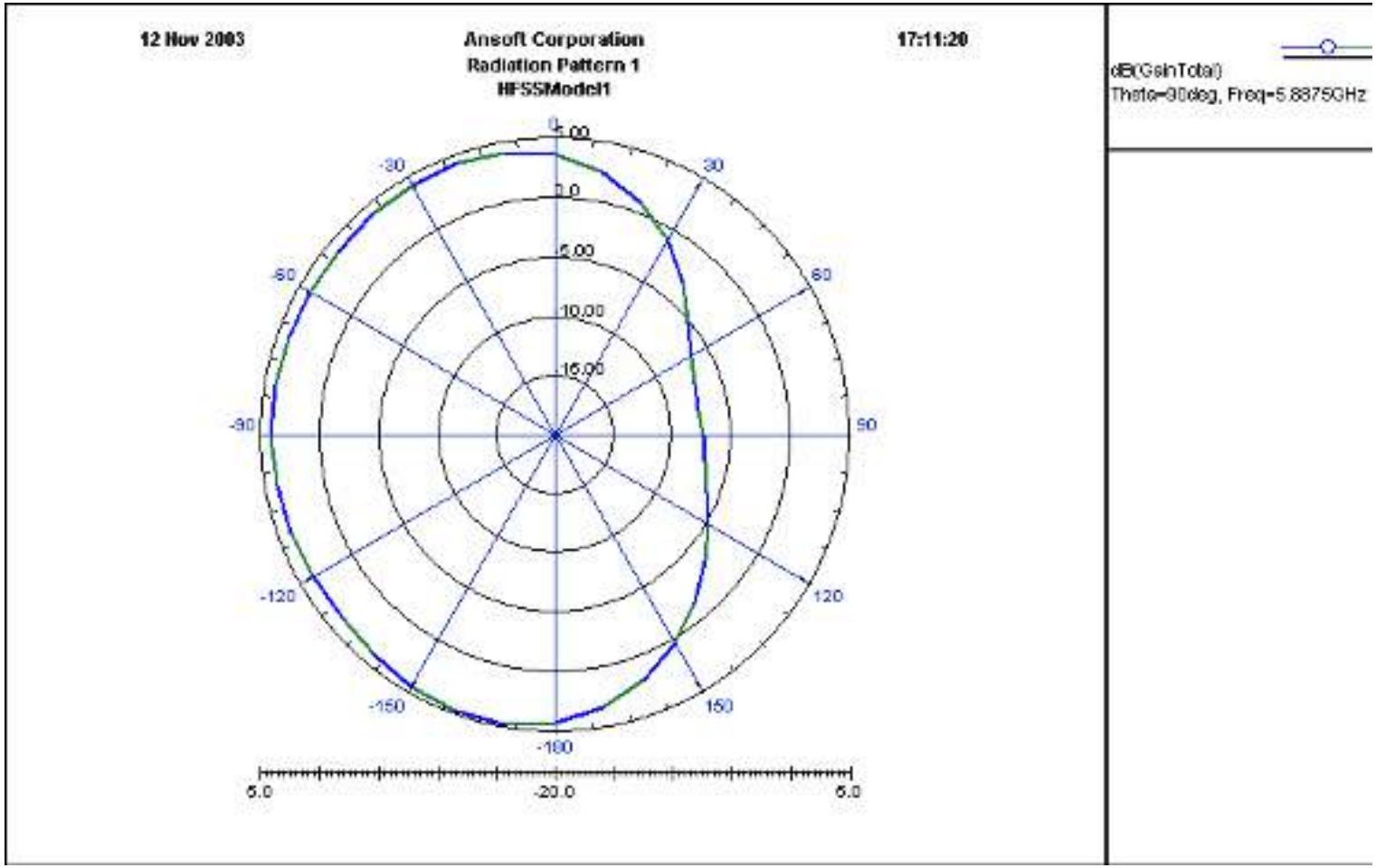


Figure 2-T. Radiation Pattern – Dipole Array in Free Space 0° Elevation (Side Feed-Point)

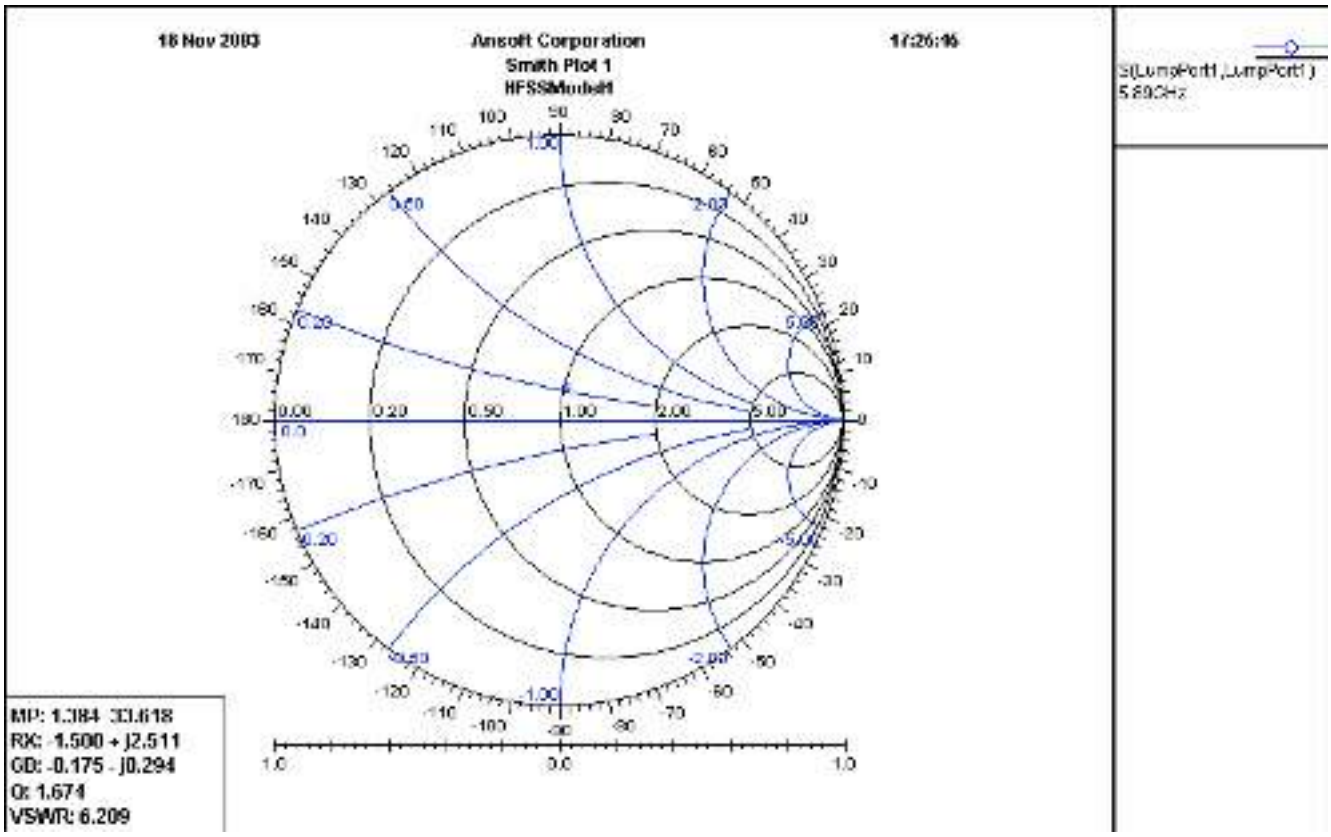


Figure 2-U. Smith Chart - Dipole Array in Free Space (Side Feed-Point)

The model simulation with the side feed-point did not impact the VSWR performance of the dipole array. The taper feed structure was tuned such that the input impedance was not affected.

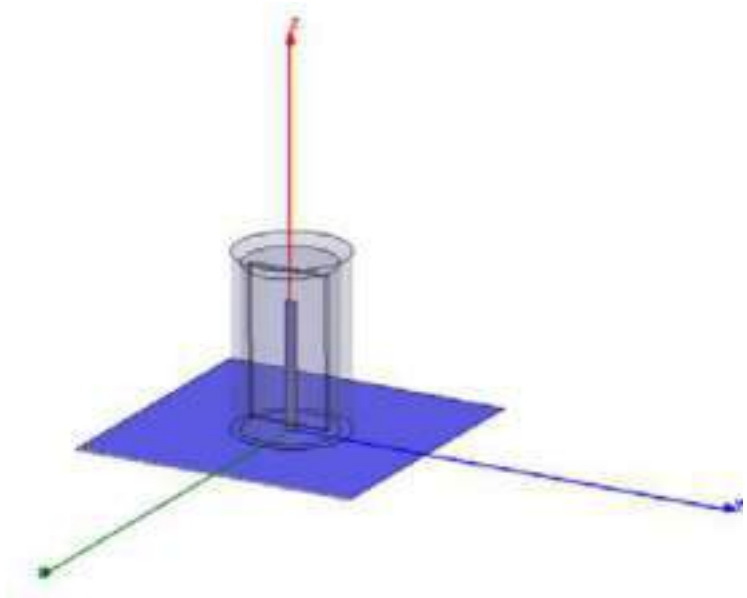
2.6 Roof-Mount Simulation

2.6.1 Design Description

Roof-mounted antenna design description:

- 5/8-wavelength element (internal element is approximately 1” tall).
- Requires approximately 2” radius of uninterrupted sheet metal surrounding the mounting location to serve as the ground plane.
- Overall omni-directional pattern at the required elevation angles.
- Geloy plastic radome (housing).
- Magnetic mounting mechanism with a coaxial pigtail parallel to the roof line.

2.6.2 Dimensioned Layout



The 5/8 wave element alone is approximately 26mm tall. It is modeled on a 14mm wide by 0.75mm thick substrate. The final shape and size of the antenna assembly will be determined by the mounting mechanism, appearance, and aerodynamics.

2.6.3 Model Assumptions

The HFSS model assumed that the antenna radome would be made of the GE plastic Geloy and mounted on a relatively flat conductive ground plane. In order to provide a more realistic model, both an infinite ground plane and a 300mm diameter ground plane simulation were run.

2.6.4 Infinite Ground Plan Pattern/Gain Plots

Gain plots and pattern measurements were simulated with the antenna element mounted on an infinite ground plane encased in a generic cylindrical Geloy radome. The results show a 5-8dB margin to the 0dBi requirement. The pattern is truncated below the horizon due to the theoretical assumption of the infinite ground plane. The presence of this ground plane also shifts the location of the peak gain closer towards the horizon.

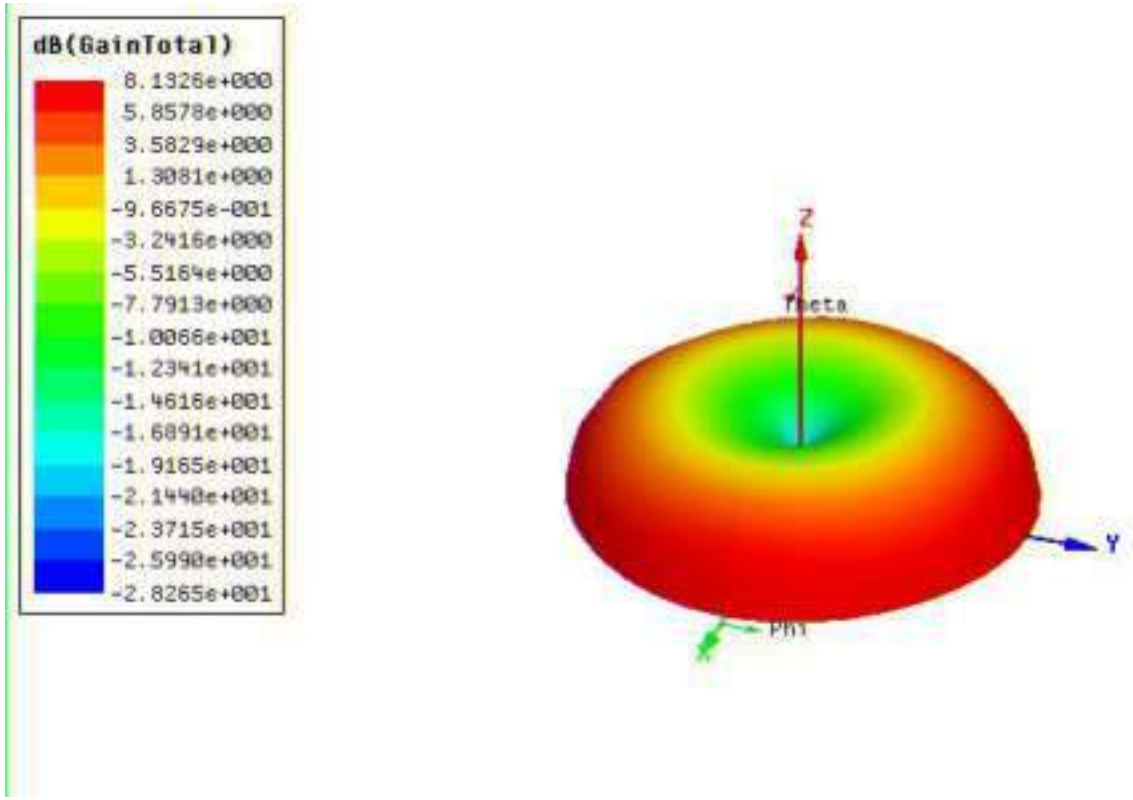


Figure 2-V. Isometric View – 5/8 Wave on Infinite Ground Plane

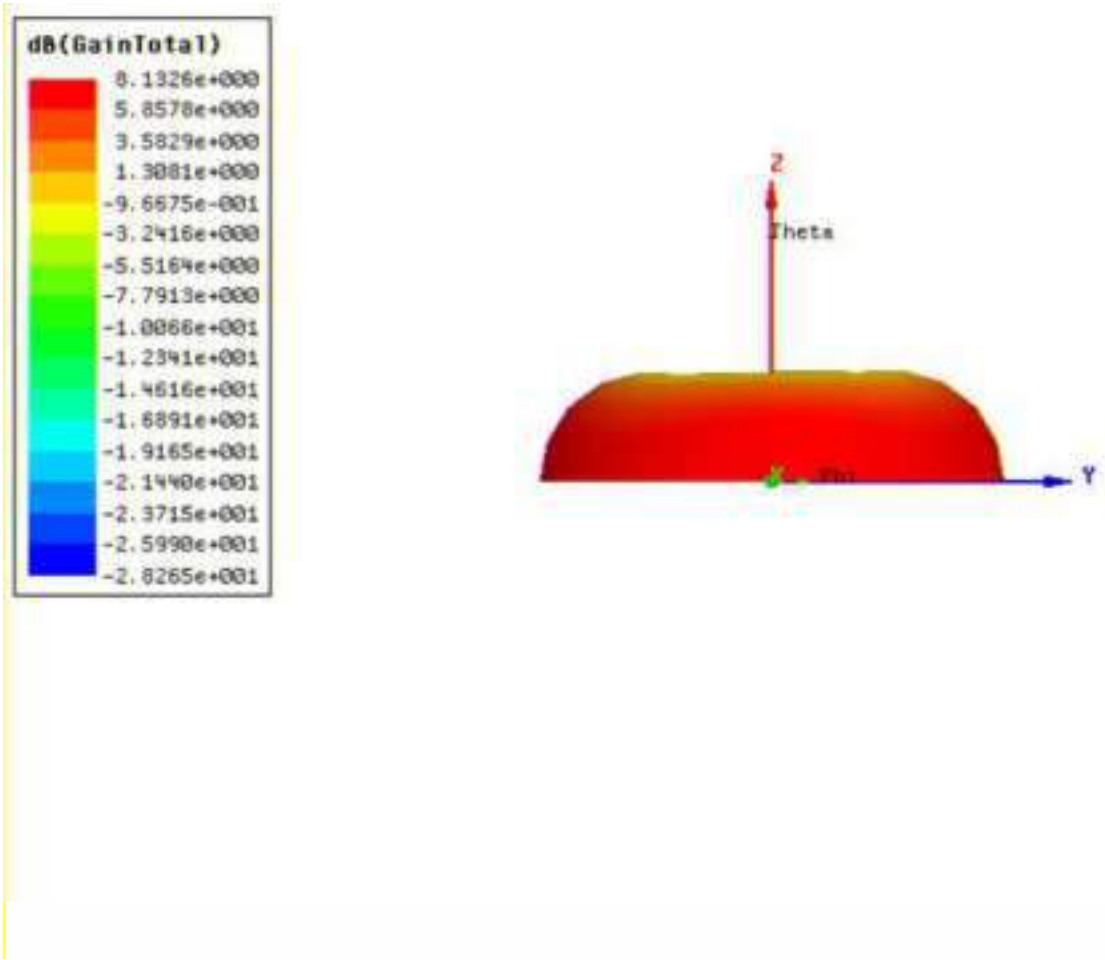


Figure 2-W. Side View – 5/8 Wave on Infinite Ground Plane

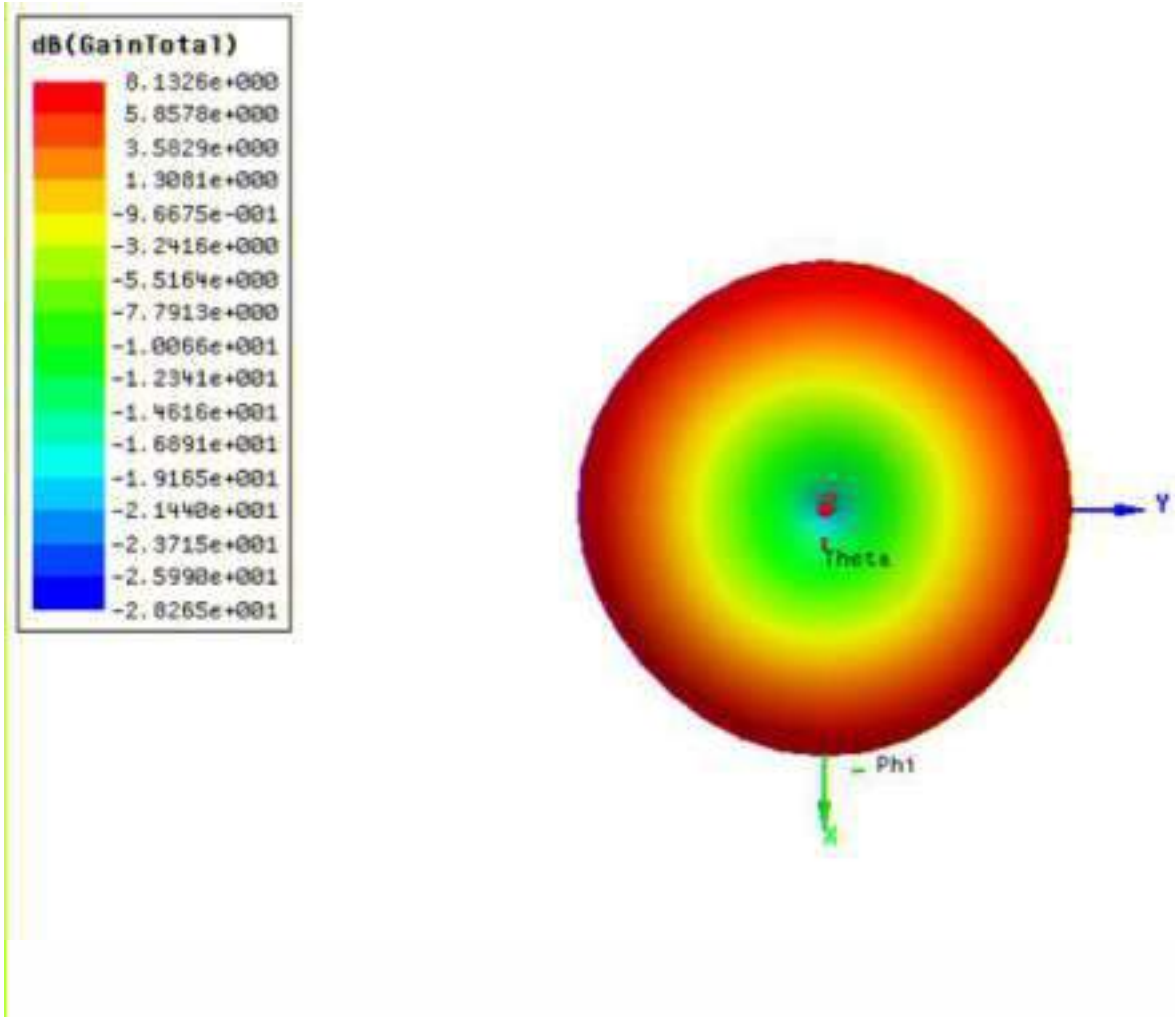


Figure 2-X. Top View – 5/8 Wave on Infinite Ground Plane

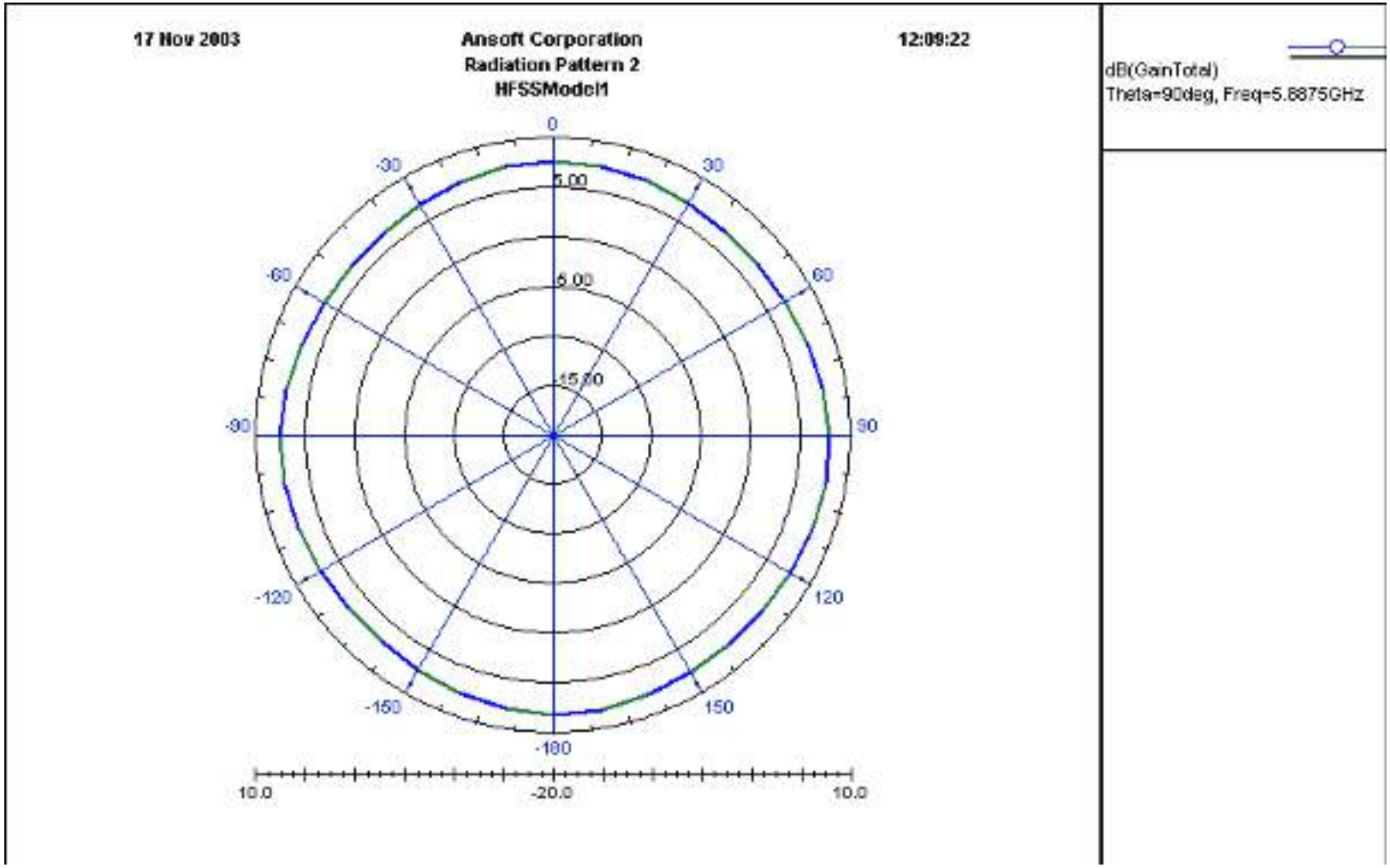
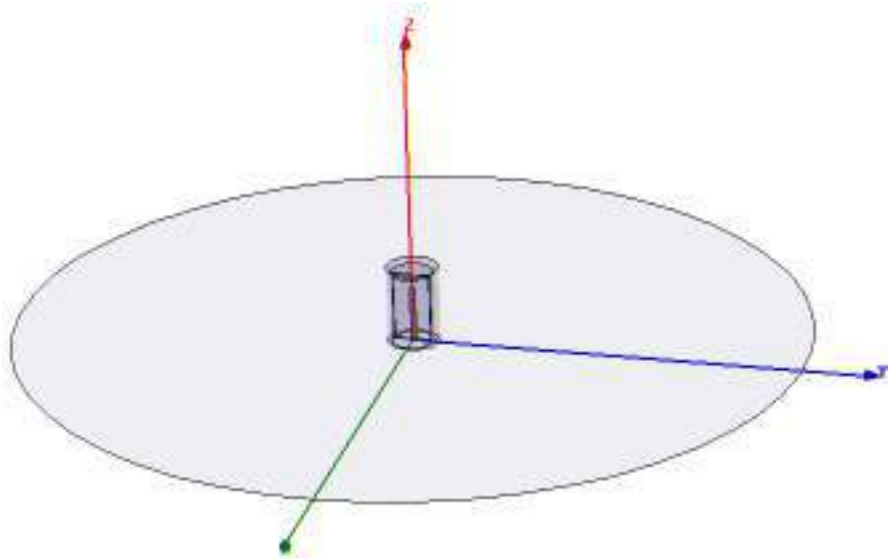


Figure 2-Y. Radiation Pattern - 5/8 Wave on Infinite Ground Plane 0° Elevation

2.6.5 300mm Ground Plan Pattern/Gain Plots

Gain plots and pattern measurements were also simulated with the antenna element encased in a generic cylindrical Geloy radome mounted in the center of a 300mm ground plane. The results show a minor reduction in overall gain, additional gain below the horizon and a shift in peak gain to approximately 30° above the horizon. The model still shows satisfactory gain with a ~2.5dB margin to the 0dBi requirement.



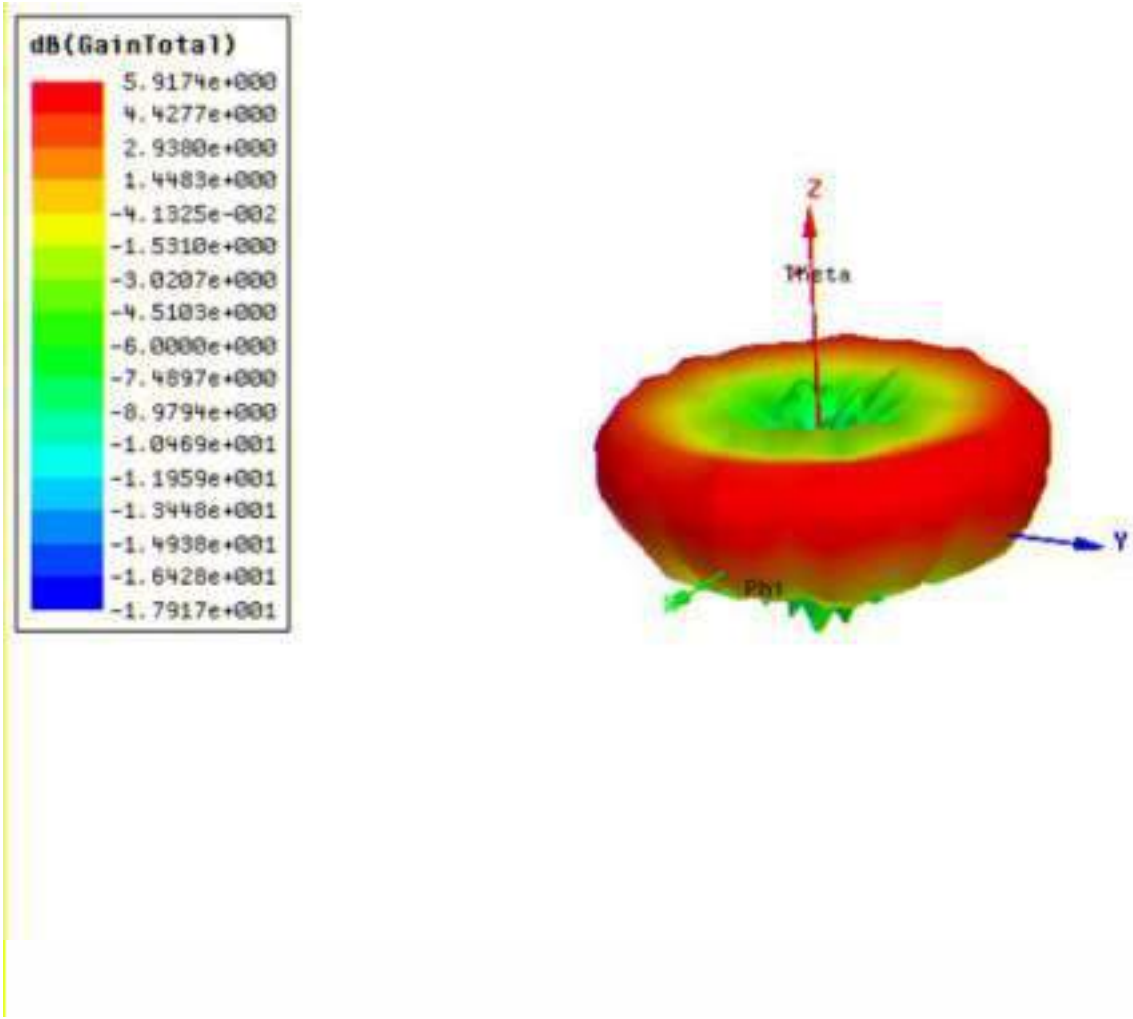


Figure 2-Z. Isometric View – 5/8 Wave on 300mm Ground Plane

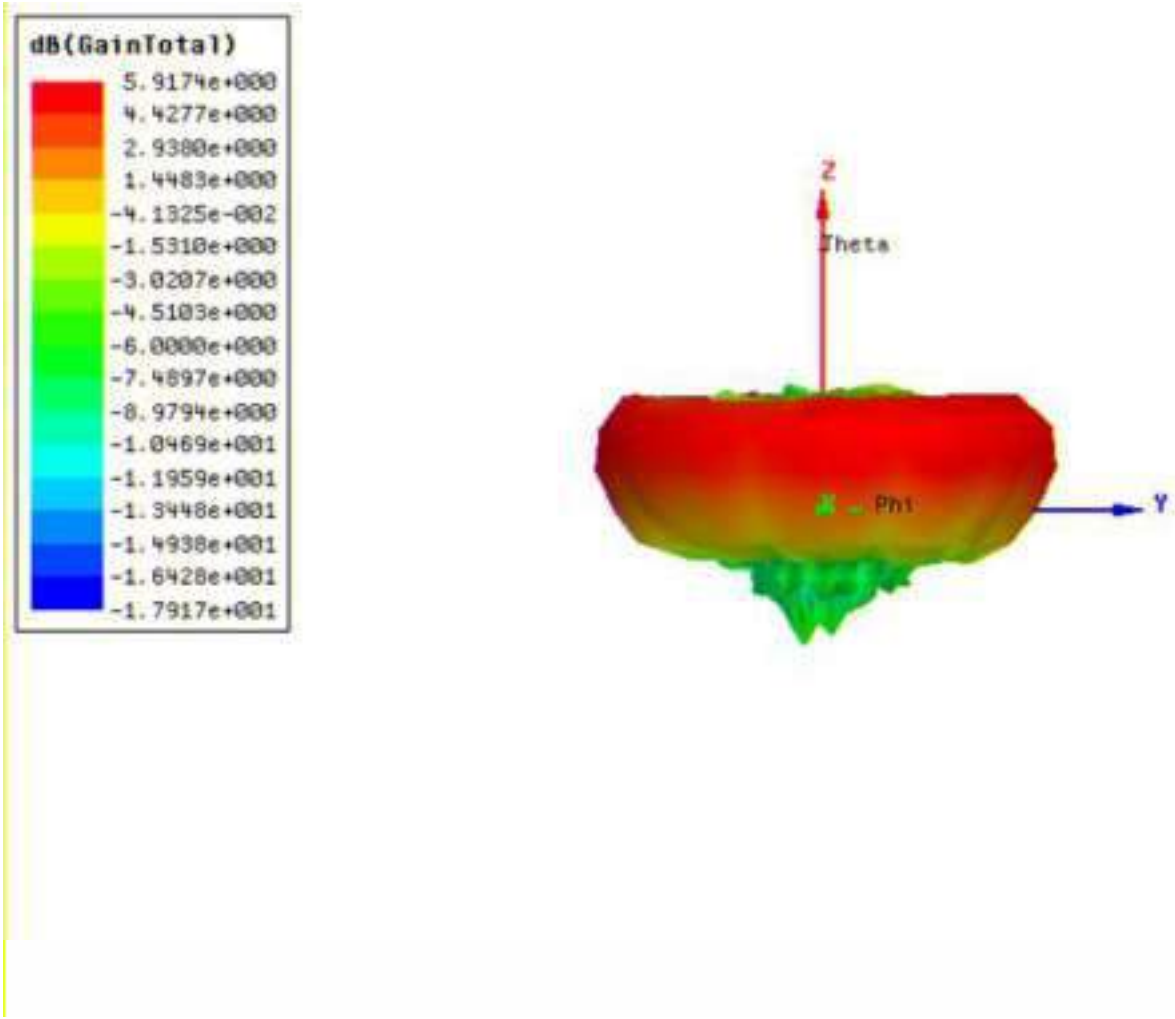


Figure 2-AA. Side View – 5/8 Wave on 300mm Ground Plane

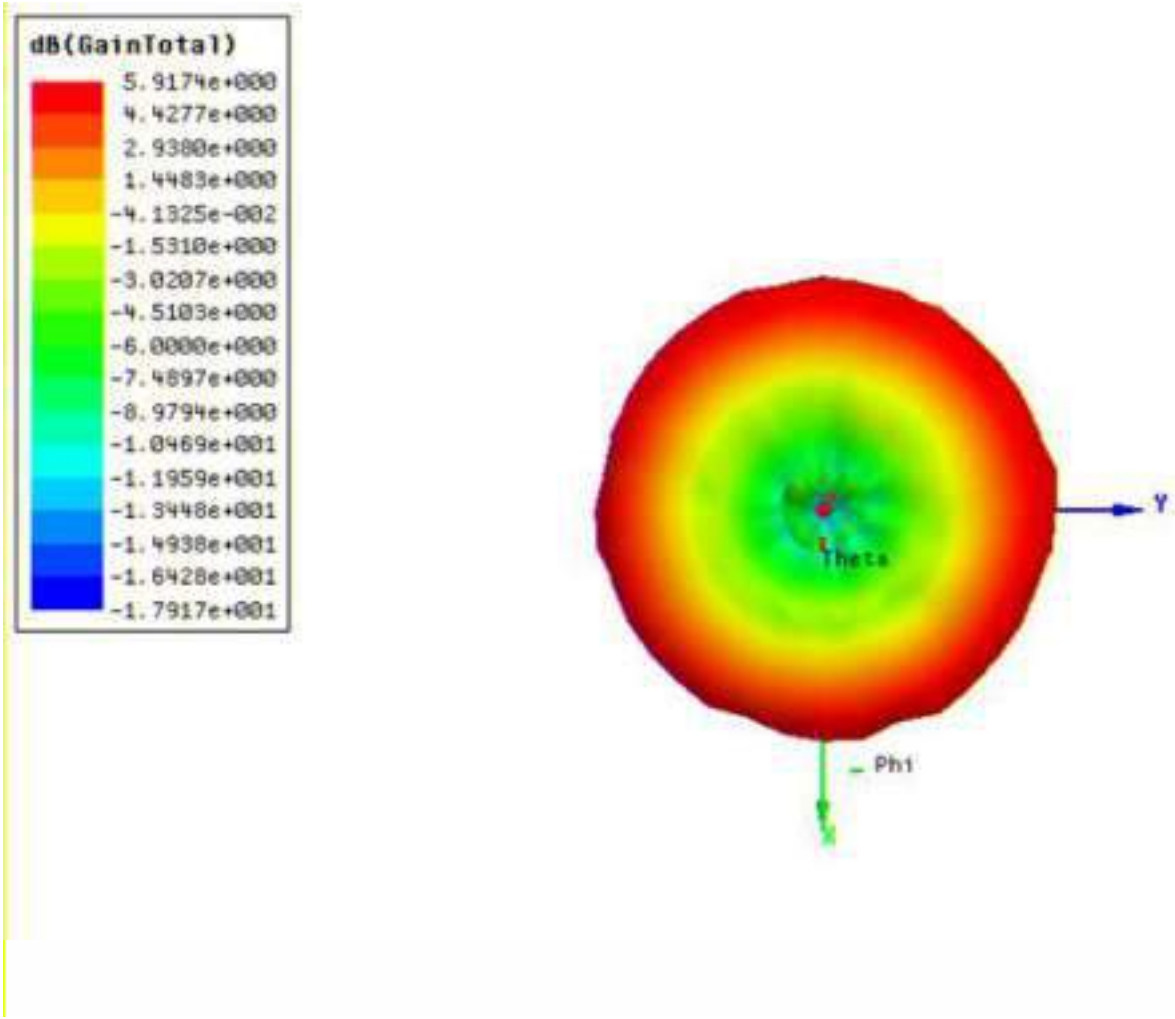


Figure 2-BB. Top View – 5/8 Wave on 300mm Ground Plane

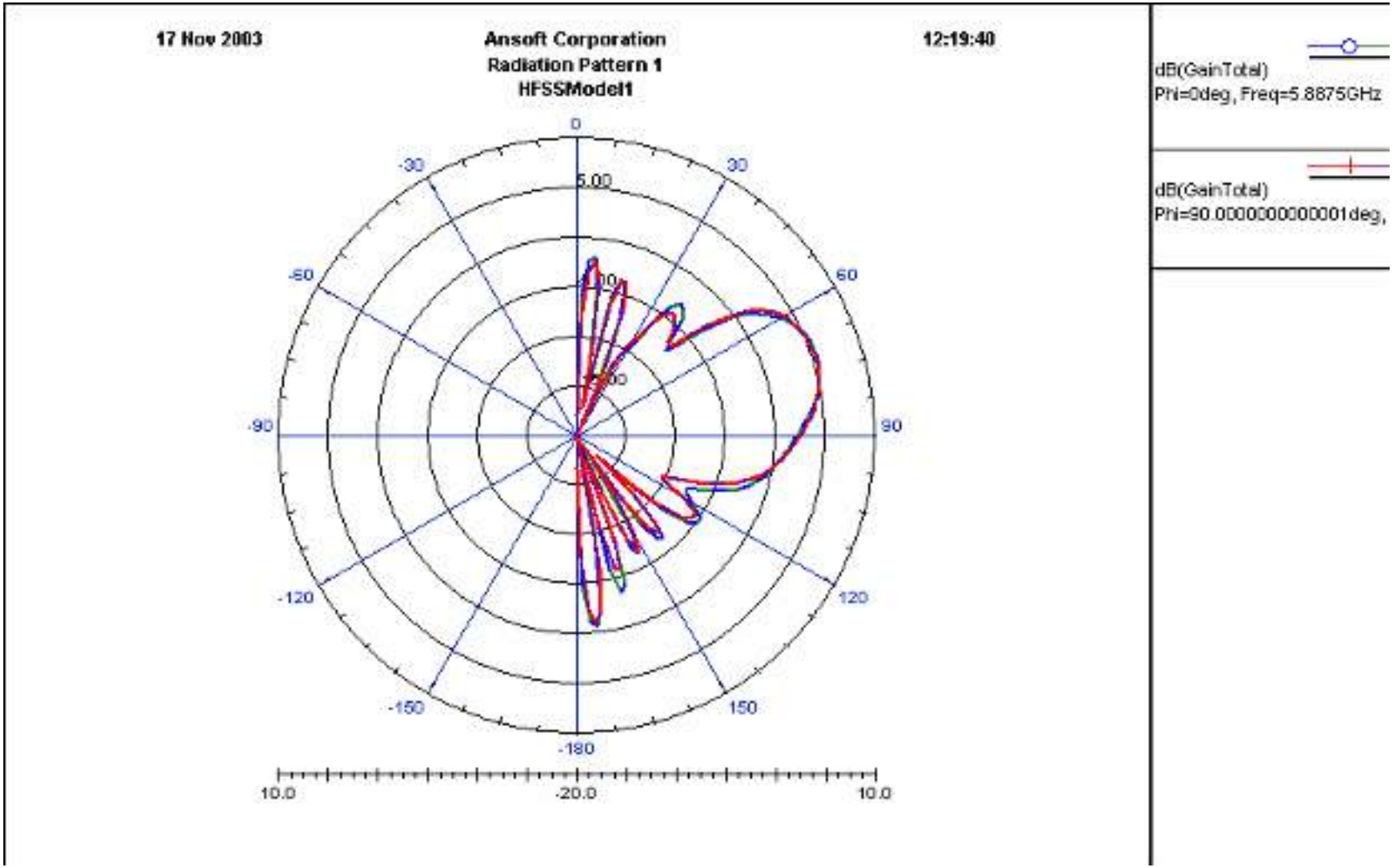


Figure 2-CC. Radiation Pattern - 5/8 Wave on 300mm Ground Plane Elevation Patterns at phi 0 (XZ) and 90 (YZ) Degrees

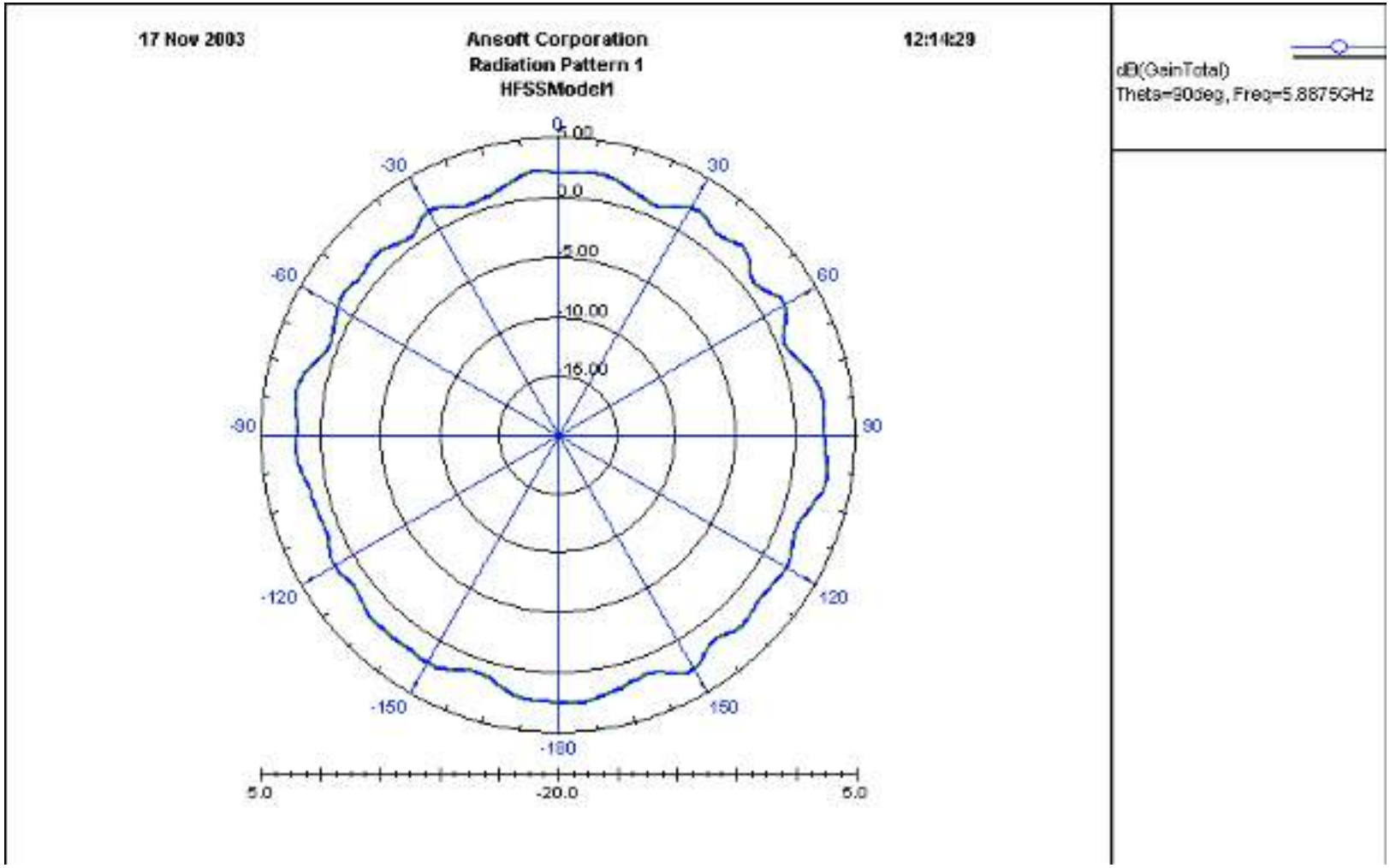


Figure 2-DD. Radiation Pattern - 5/8 Wave on 300mm Ground Plane 70° Elevation

2.7 Free-Space Link Budget

In order to demonstrate that the theoretical designs would be capable of system operation a free-space link budget calculator was developed. Three nominal cases were simulated: mirror-to-mirror, roof-to-roof, and mirror-to-roof. All calculations resulted in at least 3dB margin for the system.

Assumptions used in the model:

- 100mW transmit power
- 3.0dB cable loss for both transmit and receive systems
- 500m max range
- -86dBm receiver sensitivity (based on Atheros chip set)
- Mirror (dipole) gain 3.0dB
- Roof (5/8 wave) gain 2.5dB
- Multi-path nulls are not simulated

The specific cable routing is dependent on the individual vehicle structures and locations of the test equipment. The following calculations show a typical Thermax 0.070” antenna pigtail with a transition to LMR195 internal to the vehicle for additional length.

Cable loss calculations

Type	Loss / ft @5.8GHz	Length ft.	loss
0.070 cable	0.96	1.5	1.44 dB
LMR 195	0.28	5	1.4 dB
		Total loss	2.84 dB

Note: If a single cable type is used the maximum length of 0.070” cable is ~3 feet and maximum length of LMR195 is 10.5 feet.

2.7.1 Free-Space Link Budget (Mirror-to-Mirror)

	Inputs		
Frequency (GHz)	5.89		
Transmit power (mW)	100.00	20	(dBm)
cable loss, dB	3.00		
TX antenna gain (dBi)	3.00		
Range (M)	500.00	-101.82	(Path loss, dB)
RX antenna gain (dbi)	3.00		
cable loss, dB	3.00		
RX sensitivity (dBm)	-86.00		

Net RX power	-81.82	dBm	Link success
Link margin	4.18	DB	

2.7.2 Free-Space Link Budget (Mirror-to-Roof)

	Inputs		
Frequency (GHz)	5.89		
Transmit power (mW)	100.00	20	(dBm)
cable loss, dB	3.00		
TX antenna gain (dBi)	3.00		
Range (M)	500.00	-101.82	(Path loss, dB)
RX antenna gain (dbi)	2.50		
cable loss, dB	3.00		
RX sensitivity (dBm)	-86.00		

Net RX power	-82.32	dBm	Link success
Link margin	3.68	DB	

2.7.3 Free-Space Link Budget (Roof-to-Roof)

	Inputs		
Frequency (GHz)	5.89		
Transmit power (mW)	100.00	20	(dBm)
cable loss, dB	3.00		
TX antenna gain (dBi)	2.50		
Range (M)	500.00	-101.82	(Path loss, dB)
RX antenna gain (dbi)	2.50		
cable loss, dB	3.00		
RX sensitivity (dBm)	-86.00		

Net RX power	-82.82	dBm	Link success
Link margin	3.18	dB	

2.8 Summary

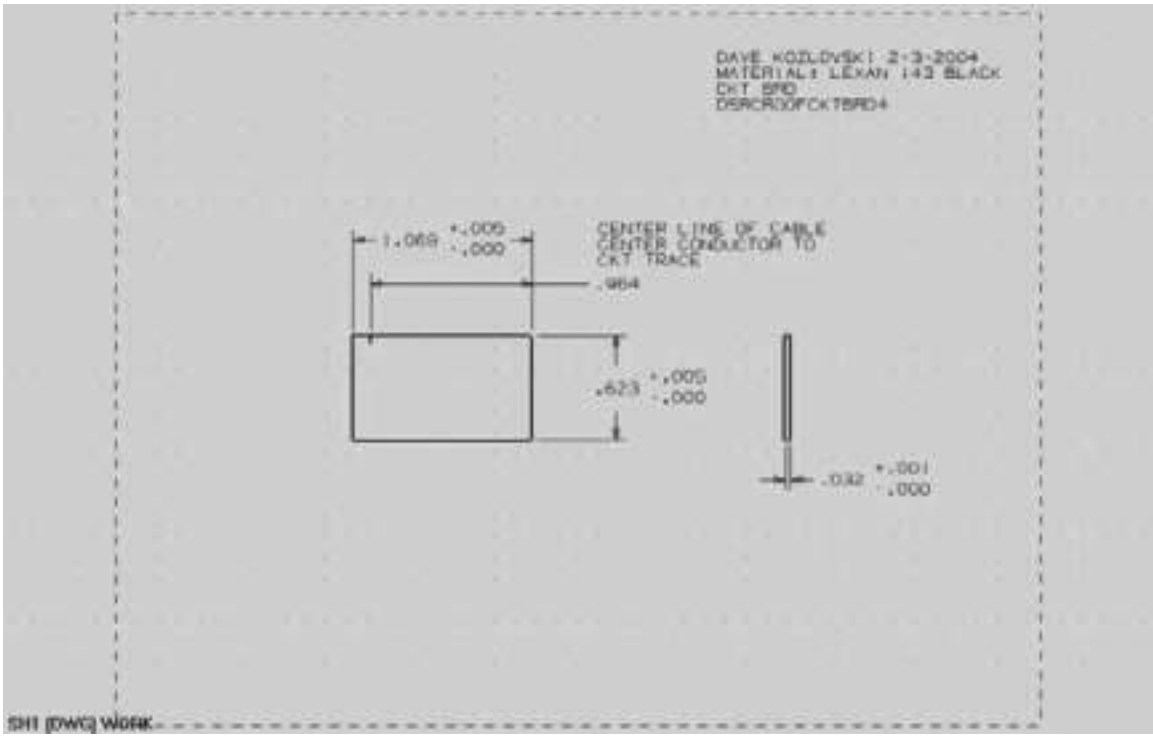
M/A-COM has achieved, on other projects, very comparable results between the theoretical modeling in HFSS and prototype component testing. These results are limited to the processing capability and the model assumptions used with the software. We do however feel confident that there is sufficient margin between the simulation and the design specification to ensure satisfactory actual antenna performance.

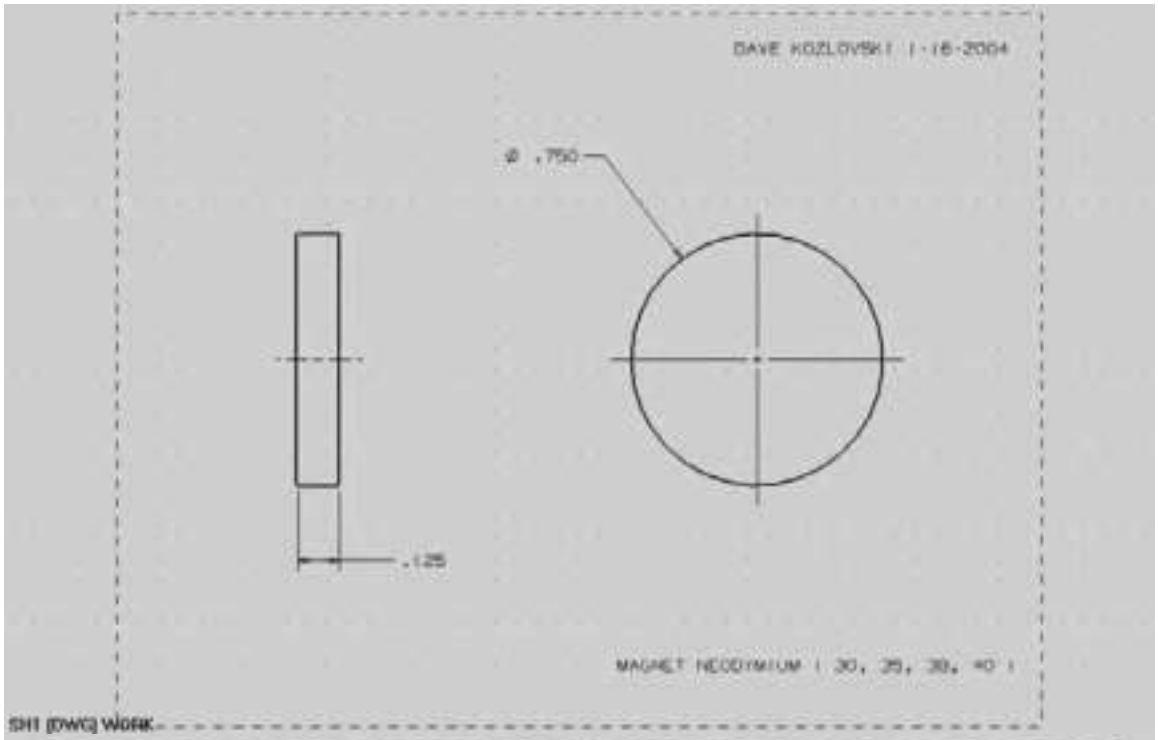
3 Antenna Subproject Final Report

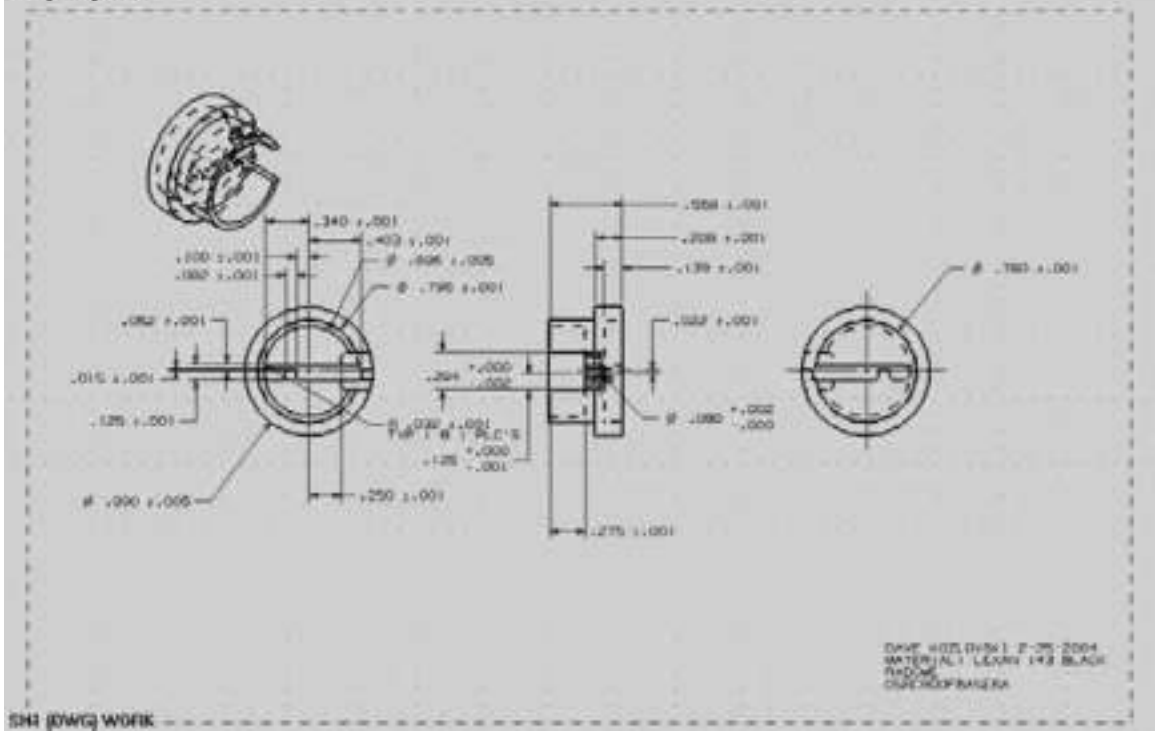
This final report describes measured test results of two antenna designs in support of Task 6C of the Collision Avoidance Metrics Program (CAMP) Vehicle Safety Communications (VSC) project. Antennas were designed for application to the vehicle side view mirror and roof locations for operation within the 5.85 to 5.925 GHz Intelligent Transportation System (ITS) Dedicated Short Range Communications (DSRC) band.

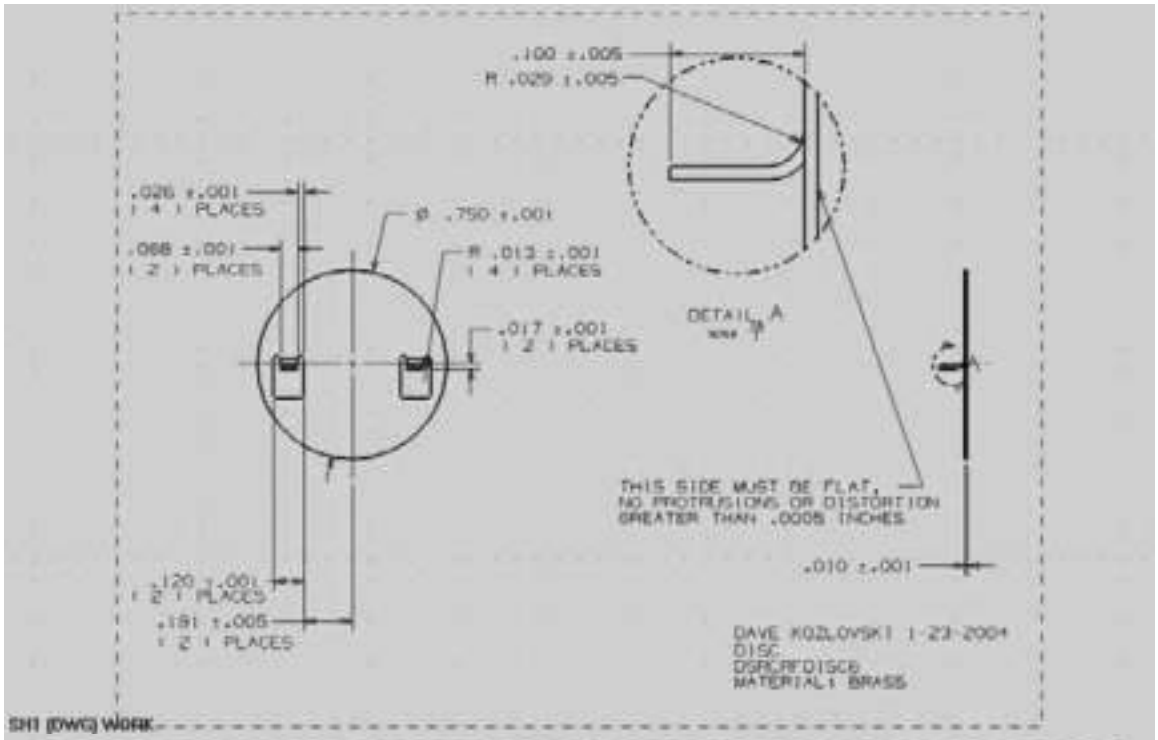
3.1 Antenna Design

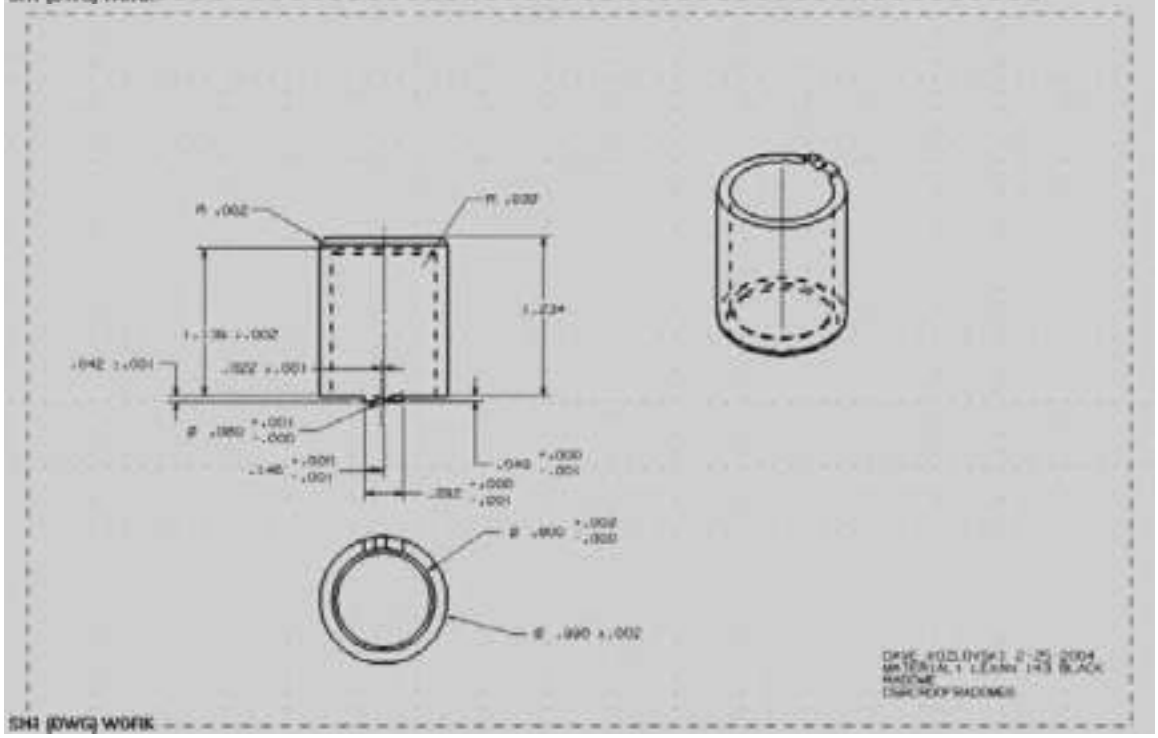
3.1.1 Magnetic Roof Mount Antenna Drawings

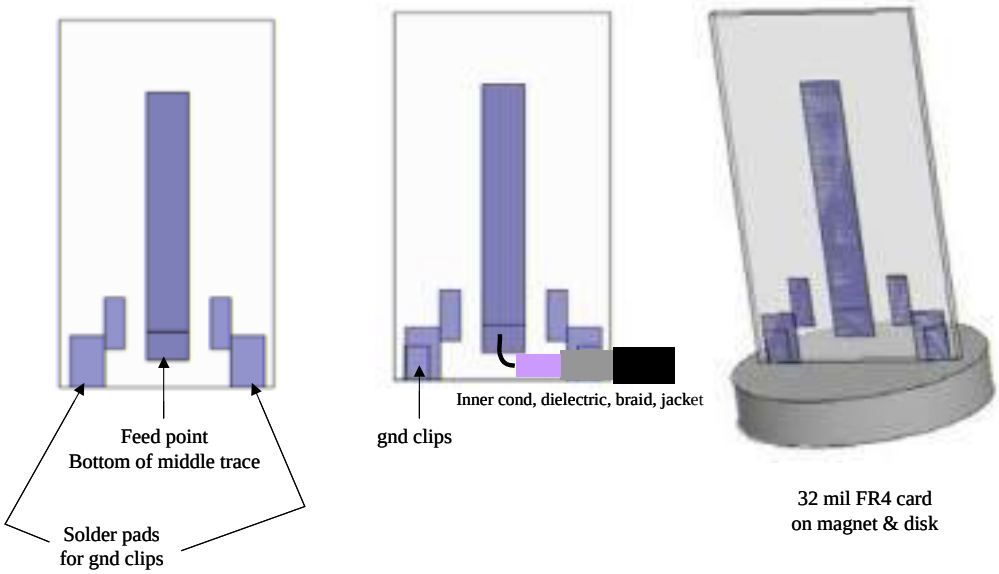


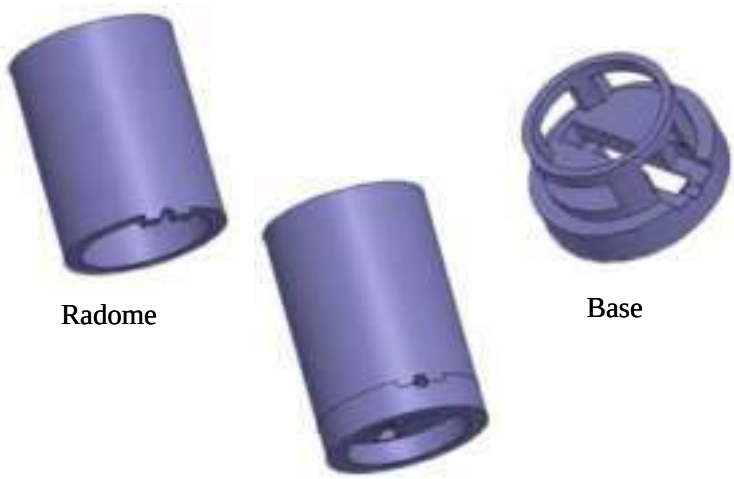

DAVE KOZLOVSKI 1-16-2004
Ø .750
.125
MAGNET NEODYMIUM (30, 35, 38, 40)
SH1 (DWG) WORK


.340 ±.001
.403 ±.001
.100 ±.001
.082 ±.001
Ø .796 ±.001
.082 ±.001
.015 ±.001
.125 ±.001
Ø .990 ±.005
.250 ±.001
.558 ±.001
.208 ±.001
.139 ±.001
.022 ±.001
Ø .780 ±.001
Ø .080
.275 ±.001
SH1 (DWG) WORK


.100 ±.005
R .029 ±.005
.026 ±.001
(4) PLACES
.068 ±.001
(2) PLACES
Ø .750 ±.001
R .013 ±.001
(4) PLACES
.017 ±.001
(2) PLACES
DETAIL A
THIS SIDE MUST BE FLAT,
NO PROTRUSIONS OR DISTORTION
GREATER THAN .0005 INCHES
.010 ±.001
.120 ±.001
(2) PLACES
.191 ±.005
(2) PLACES
DAVE KOZLOVSKI 1-23-2004
DISC
DSRCRFDISC6
MATERIAL: BRASS
SH1 (DWG) WORK


R .002
R .030
1.234
.042 ±.001
.022 ±.001
Ø .990 ±.002
SH1 (DWG) WORK

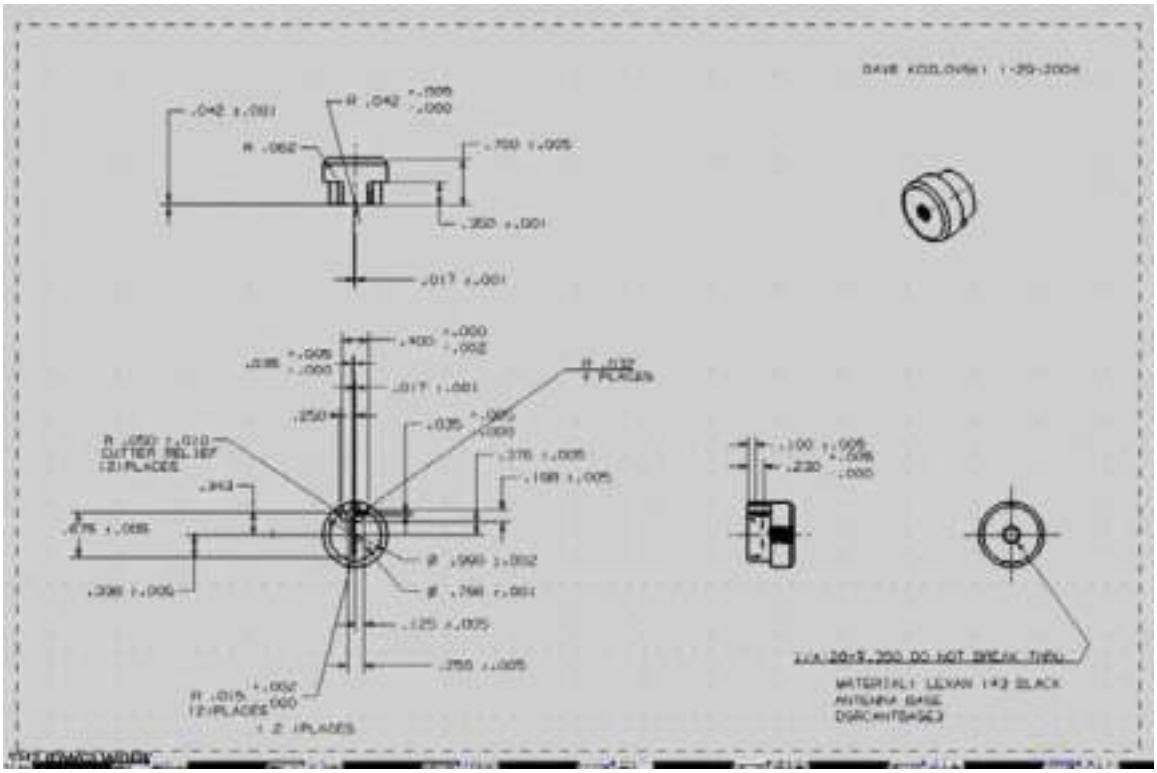


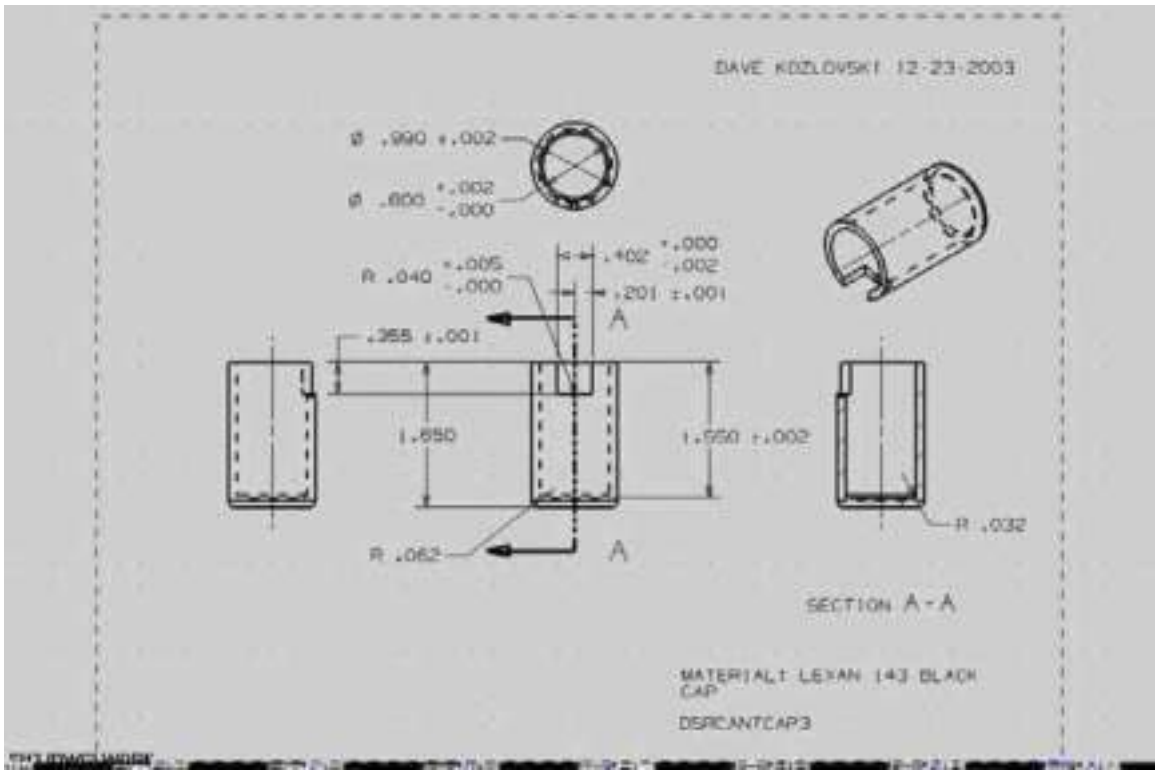


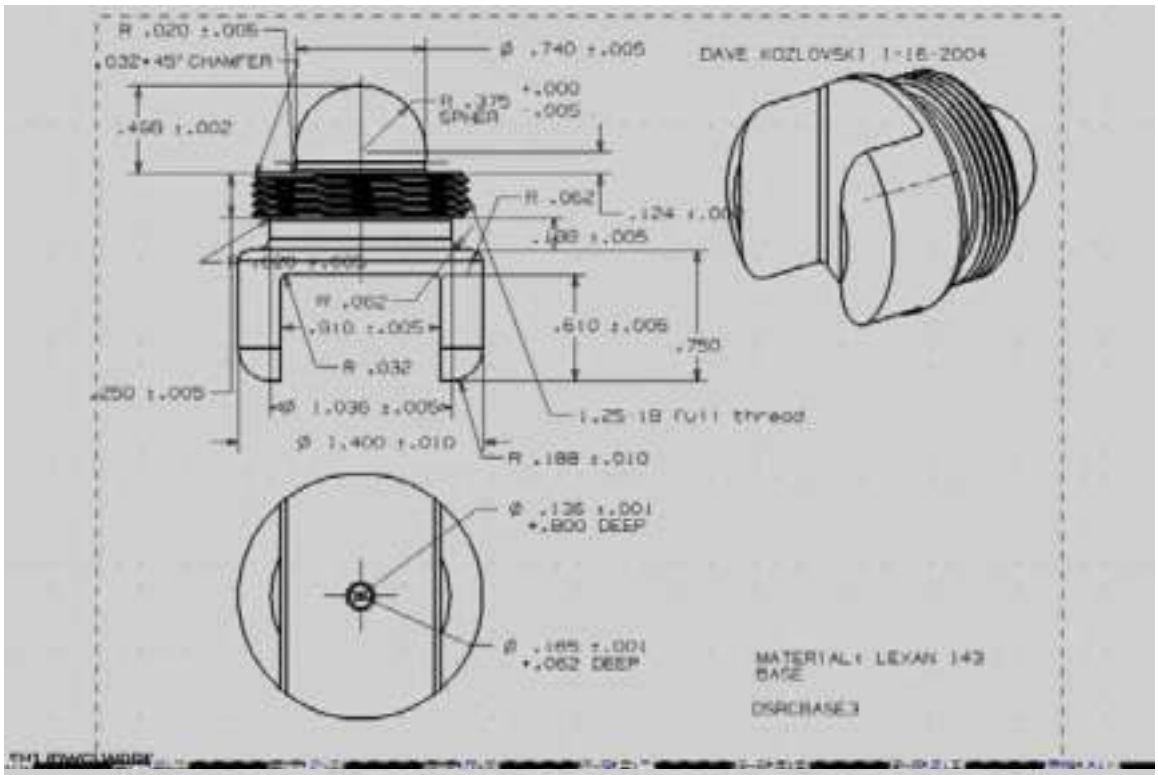
Assembly without magnet

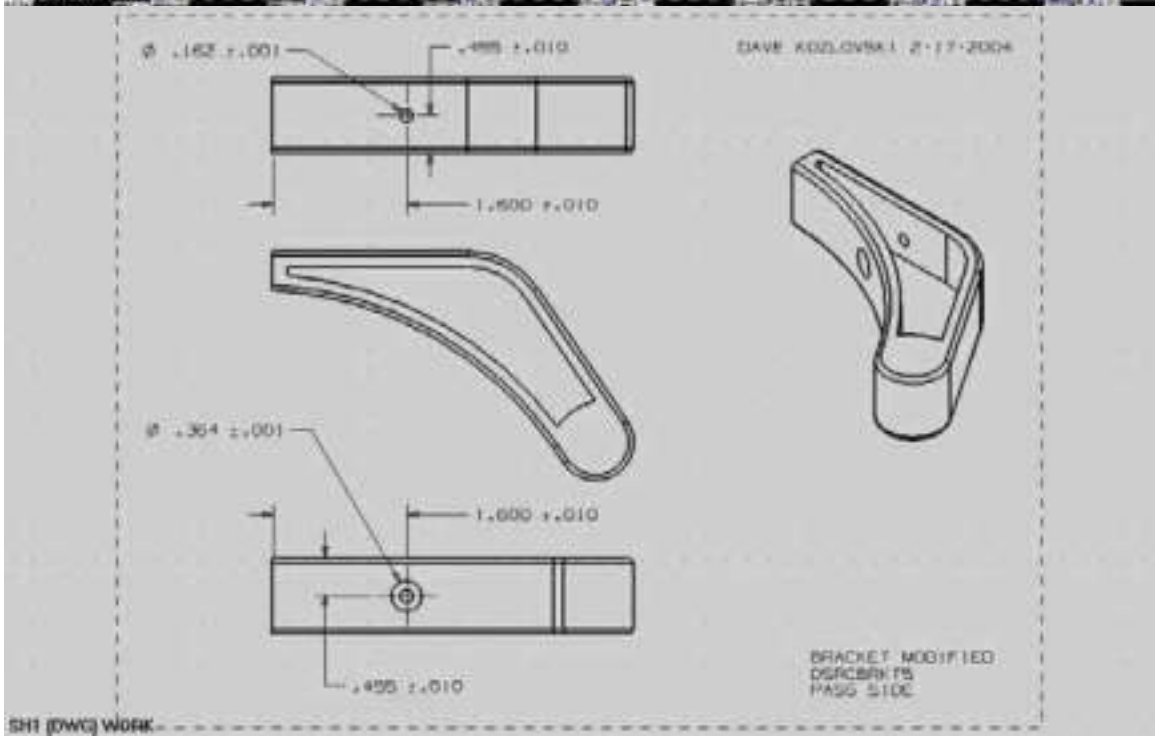
Complete assembly

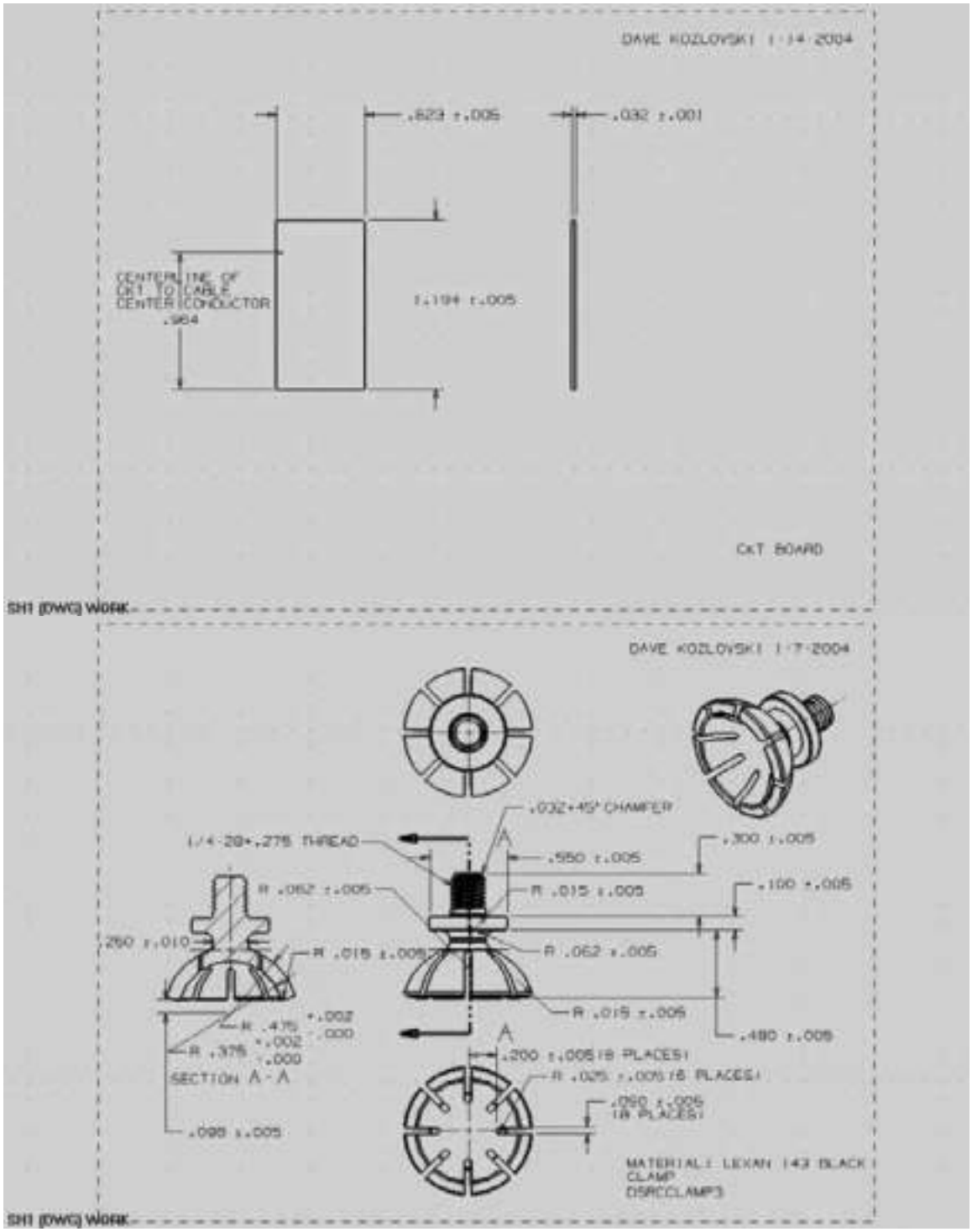
3.1.2 Mirror Antenna Drawings

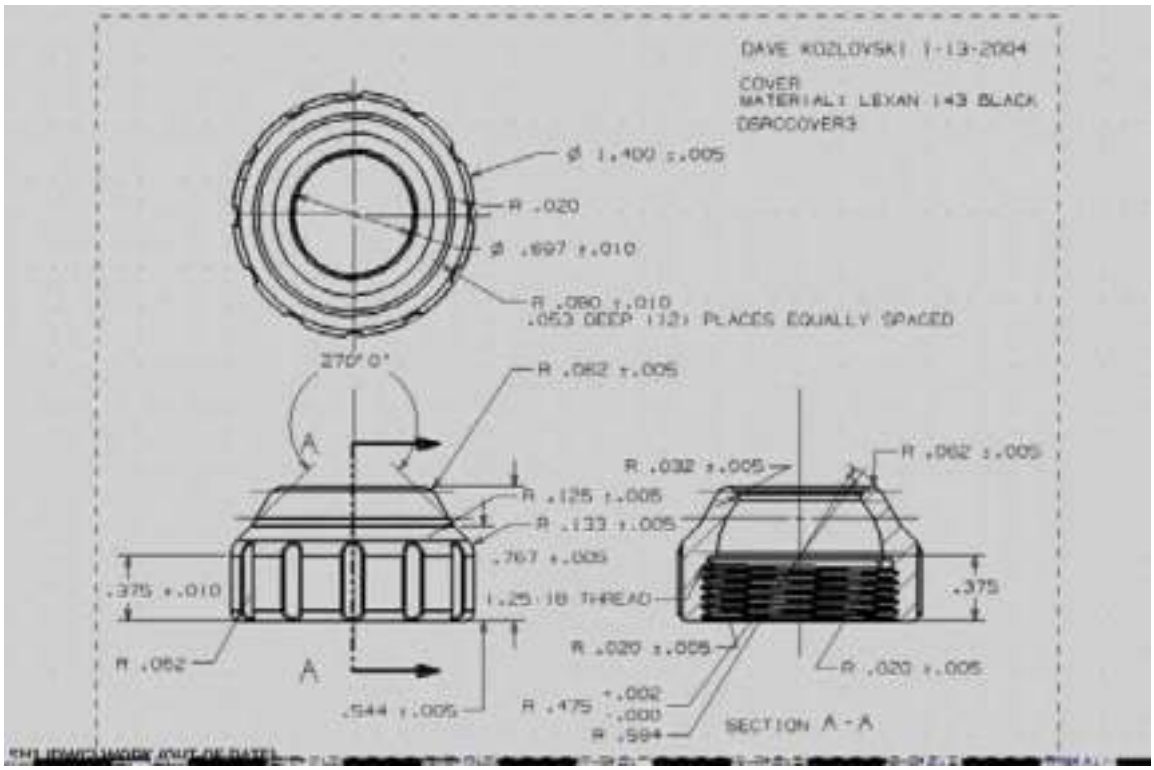


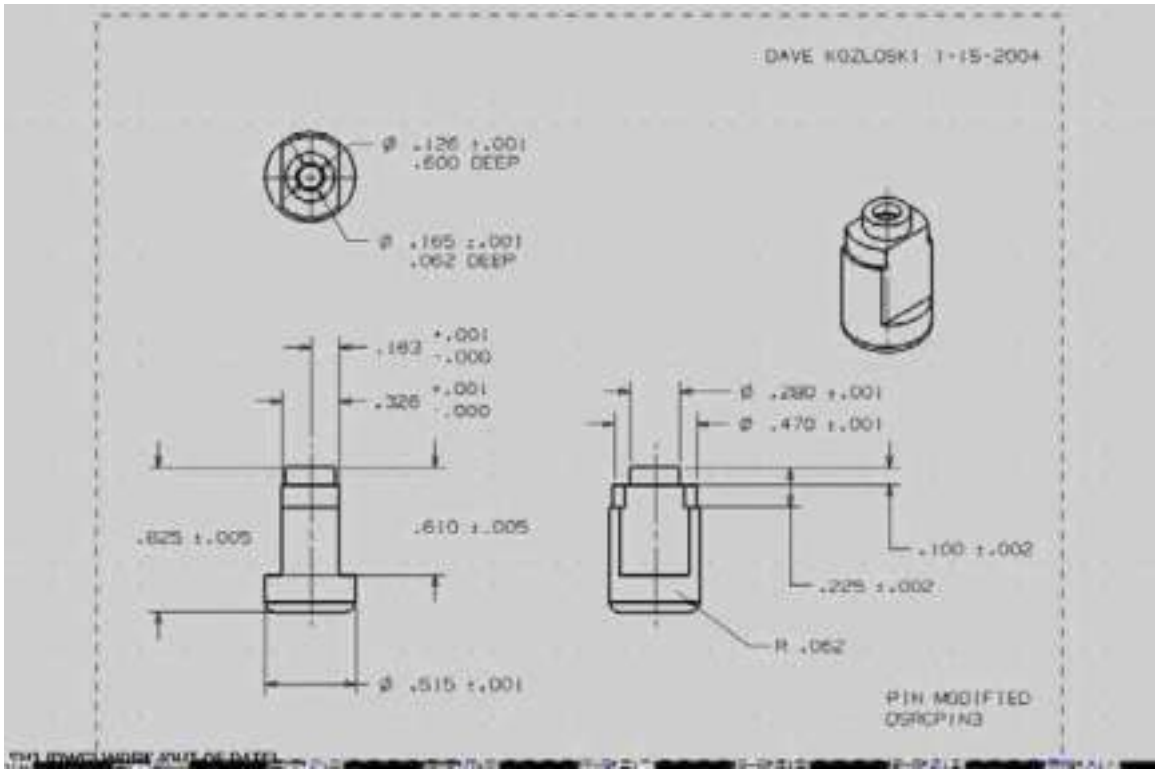

DAVE KOZLOVSKI 12-23-2003
Ø .990 ±.002
Ø .800 +.002 -.000
R .040 +.005 -.000
.402 +.000 -.002
.201 ±.001
A
.355 ±.001
1.650
1.550 ±.002
R .062
A
R .032
SECTION A-A
MATERIAL: LEXAN 143 BLACK
CAP
DSRCANTCAP3


R .020 ±.005
.032×45° CHAMFER
Ø .740 ±.005
DAVE KOZLOWSKI 1-16-2004
R .375 SPHER +.000 -.005
.498 ±.002
R .062
.124 ±.005
.188 ±.005
R .062
.910 ±.005
.610 ±.005
.750
R .032
.250 ±.005
Ø 1.036 ±.0004
1.25 18 full thread
Ø 1.400 ±.010
R .188 ±.010
Ø .136 ±.001
+.800 DEEP
Ø .165 ±.001
+.062 DEEP
MATERIAL: LEXAN 143
BASE
DSRCBASE3


Ø .162 ±.001
.455 ±.010
DAVE KOZLOWSKI 2-17-2004
1.600 ±.010
Ø .364 ±.001
1.600 ±.010
.455 ±.010
BRACKET MODIFIED
DSRCBRKTB
PASS SIDE


DAVE KOZLOVSKI 1-14-2004
.623 ±.005
.032 ±.001
CENTERLINE OF
CKT TO CABLE
CENTER CONDUCTOR
.964
1.194 ±.005
CKT BOARD
SH1 (DWG) WORK
DAVE KOZLOVSKI 1-7-2004
.032×45° CHAMFER
1/4-20×.275 THREAD
.550 ±.005
.300 ±.005
R .062 ±.005
R .015 ±.005
.100 ±.005
.260 ±.010
R .015 ±.005
R .062 ±.005
R .015 ±.005
.480 ±.005
R .475 +.002 -.000
R .375 +.002 -.000
SECTION A-A
.200 ±.005 (8 PLACES)
R .025 ±.005 (8 PLACES)
.060 ±.005 (8 PLACES)
.098 ±.005
MATERIAL: LEXAN 143 BLACK
CLAMP
DSRCCLAMP3
SH1 (DWG) WORK


DAVE KOZLOVSKI 1-13-2004
COVER
MATERIAL: LEXAN 143 BLACK
DSRCCOVER3
Ø 1.400 ±.005
R .020
Ø .697 ±.010
R .080 ±.010
.053 DEEP (12) PLACES EQUALLY SPACED
270° 0°
R .062 ±.005
A
R .032 ±.005
R .062 ±.005
R .125 ±.005
R .133 ±.005
.767 ±.005
.375 ±.010
1.25-18 THREAD
.375
R .062
A
R .020 ±.005
R .020 ±.005
.544 ±.005
R .475 +.002 -.000
R .594
SECTION A-A


DAVE KOZLOSKI 1-15-2004
Ø .126 ±.001
.600 DEEP
Ø .165 ±.001
.062 DEEP
.183 +.001 -.000
.326 +.001 -.000
Ø .280 ±.001
Ø .470 ±.001
.625 ±.005
.610 ±.005
.100 ±.002
.225 ±.002
R .062
Ø .515 ±.001
PIN MODIFIED
DSRCPIN3

3.2 Anechoic Chamber and Bench Test Data

3.2.1 Chamber Characteristics

Radiation pattern measurements were conducted in an anechoic chamber located at M/A-COM headquarters in Lowell, MA. The anechoic chamber used for these measurements is a 30 foot long tapered chamber including a 12 ft. x 12 ft. test box having a 4 ft quiet zone.

3.2.1.1 Gain – Mirror Mount Antenna

The mirror mount antenna including its radome and 2-foot long coaxial pigtail were placed in a free-space configuration in the anechoic chamber. The vertically polarized antenna gain was measured at a frequency of 5.9GHz. Because the 2-foot coaxial pigtail is an integral part of the antenna, the measured gain includes the 2dB loss of the coaxial pigtail. The azimuth gain pattern shown in Figure 35 was measured by rotating the antenna on its vertical axis. The elevation pattern shown in Figure 36 was measured by rotating the antenna along the horizontal.

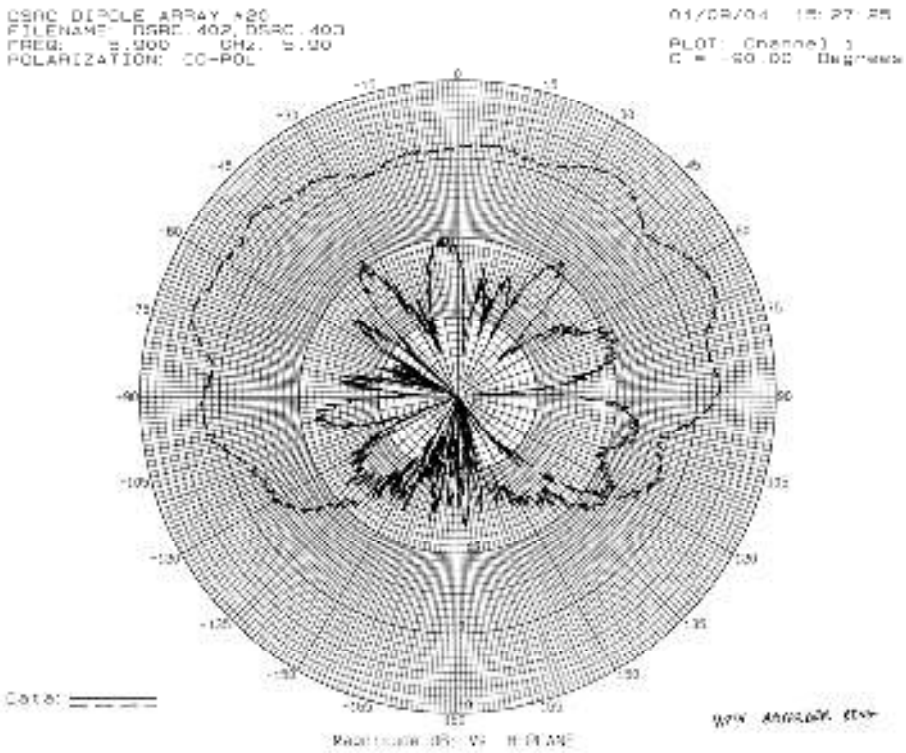


Figure 3-A. Azimuth Radiation Pattern of the Mirror Mount Antenna Including 2dB Cable Loss

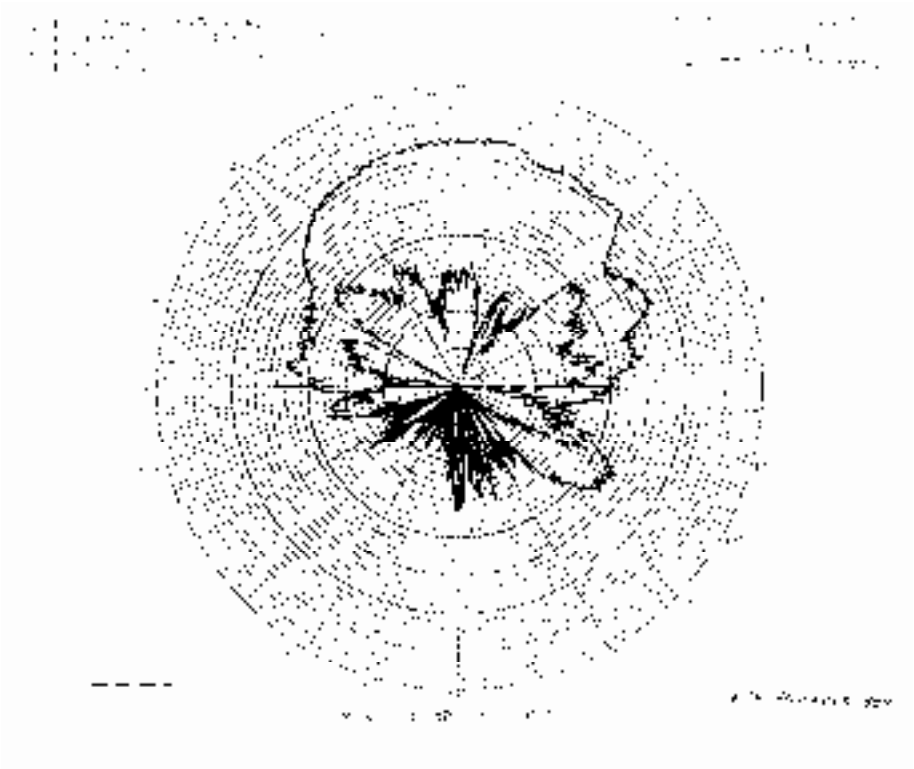


Figure 3-B. Elevation Radiation Pattern of the Mirror Mount Antenna Including 2dB Cable Loss

3.2.1.2 Gain – 5/8 Wave Roof Mount Antenna

The roof mount antenna including its radome and 2-foot long coaxial pigtail were placed on a 3-foot diameter rolled-edge ground plane in the anechoic chamber. The vertically polarized antenna gain was measured at a frequency of 5.888GHz. Because the 2-foot coaxial pigtail is an integral part of the antenna, the measured gain includes the 2dB loss of the coaxial pigtail. The azimuth gain pattern shown in Figure 37 was measured by rotating the antenna on its vertical axis. The elevation pattern shown in Figure 38 was measured by rotating the antenna along the horizontal.

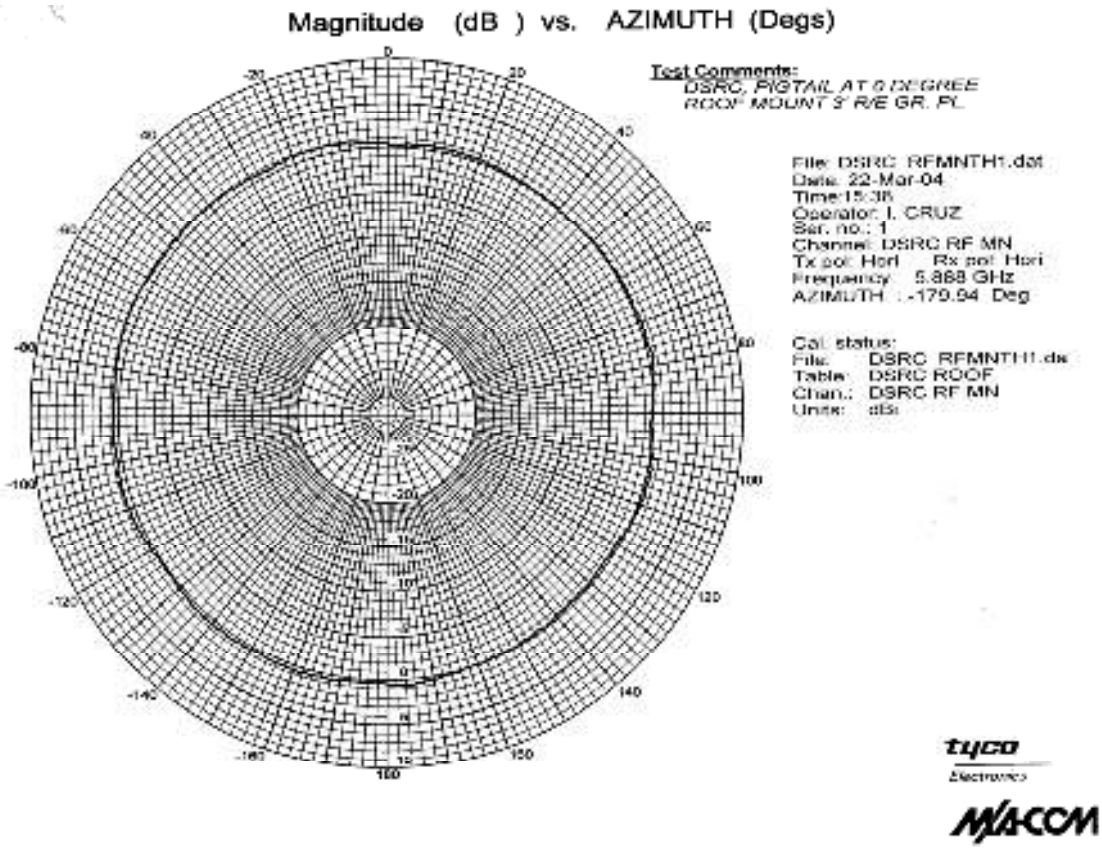


Figure 3-C. Azimuth Radiation Pattern of the Roof Mount Antenna Including 2dB Cable Loss

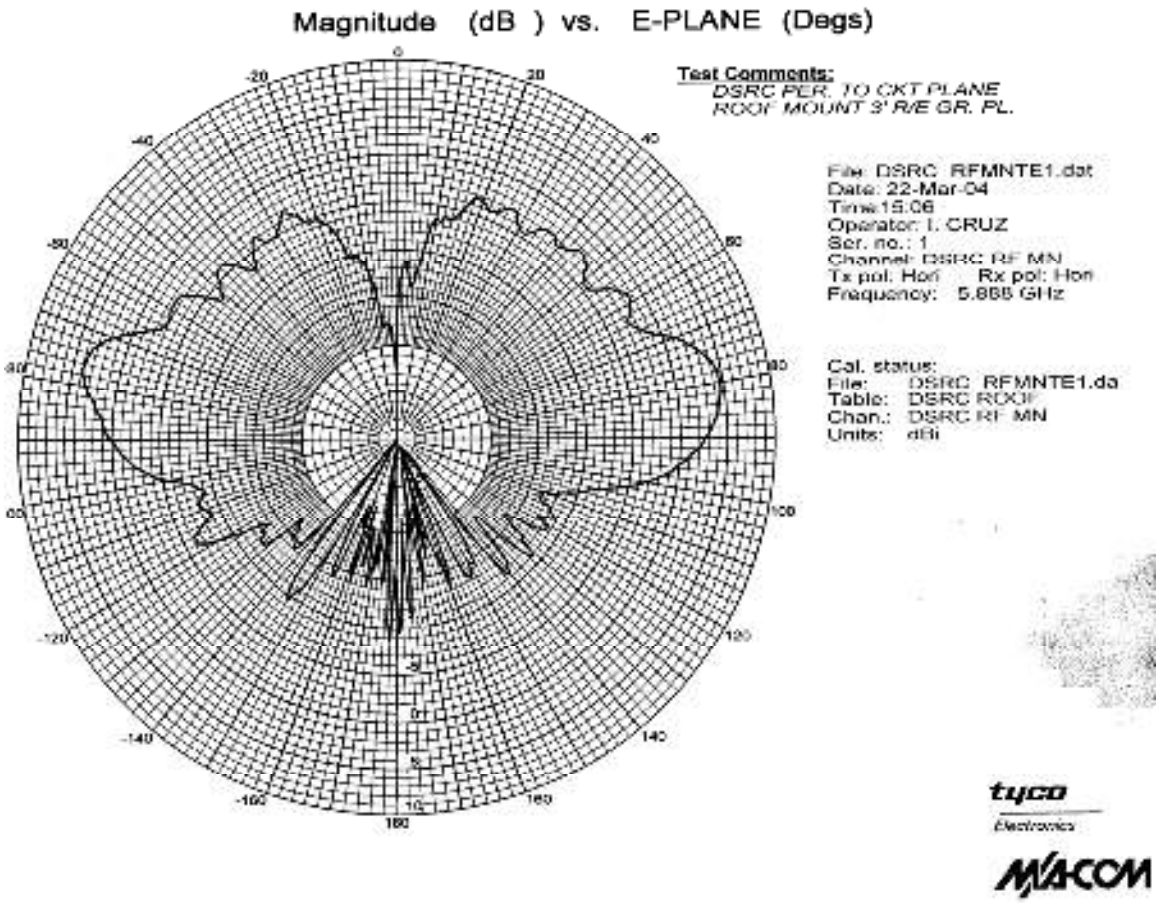


Figure 3-D. Elevation Radiation Pattern of the Roof Mount Antenna Including 2dB Cable Loss

3.2.1.3 Gain – 4-Element WLAN Roof Mount Antenna

Prior to the start of this subproject, CAMP-VSCC used a WLAN Access Point antenna with the VSC test kits to investigate approximate performance of DSRC systems. To understand how the antennas described above perform with respect to the WLAN antenna, base performance characteristic measurements needed to be taken in the same fashion.

The 4-element roof mount antenna including 3 meters of LMR-195 coaxial cable was placed on a 3-foot diameter rolled-edge ground plane in the anechoic chamber. The vertically polarized antenna gain was measured at a frequency of 5.2GHz. Because the 3-meter coaxial pigtail is an integral part of the antenna, the measured gain includes the 3dB loss of the coaxial pigtail. The azimuth gain pattern shown in Figure 39 was measured by rotating the antenna on its vertical axis. The elevation pattern shown in Figure 38 was measured by rotating the antenna along the horizontal.

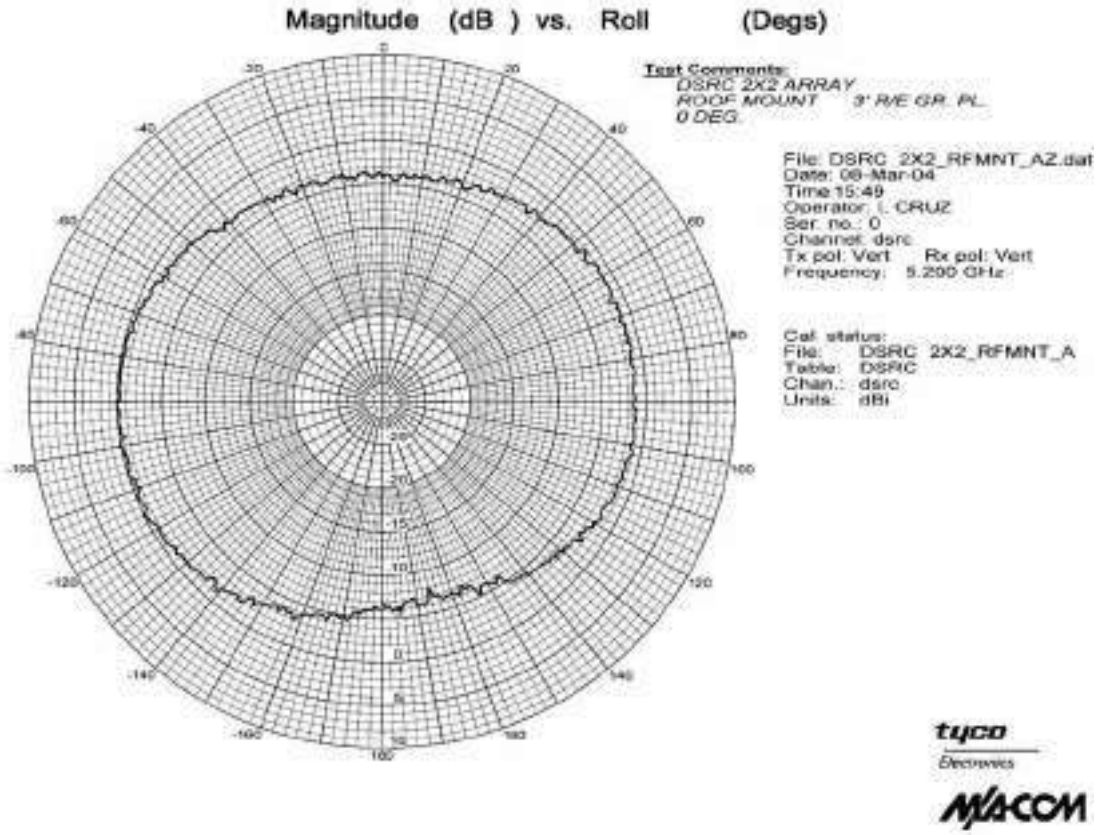


Figure 3-E. Azimuth Radiation Pattern of the Roof Mount Antenna Including 3dB Cable Loss

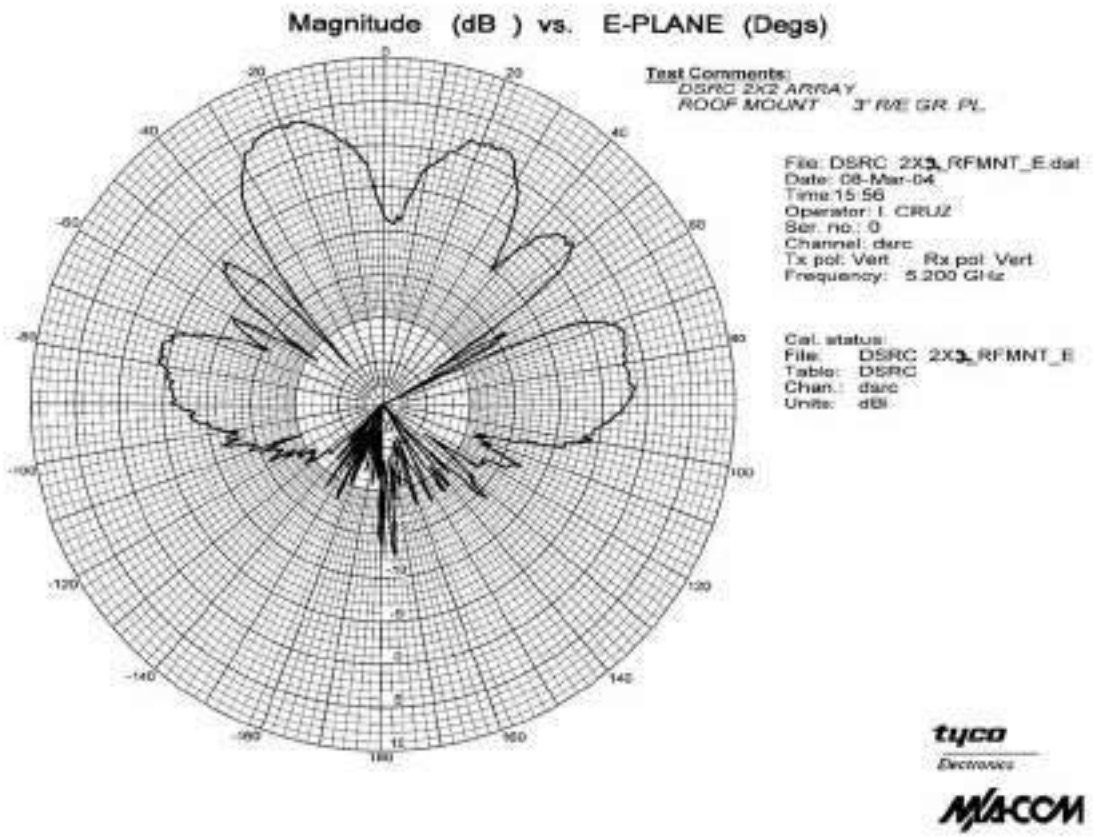


Figure 3-F. Azimuth Radiation Pattern of the Roof Mount Antenna Including 3dB Cable Loss

3.2.2 Bench Test

The Voltage Standing Wave Ratio (VSWR) measurements were conducted on each style antenna at JEF Consultant Inc. in Belleville, MI. using an HP 8753C vector network analyzer having time domain capabilities. The measurements were performed using time domain gating to eliminate the effects of the 2-foot coaxial pigtail.

3.2.2.1 VSWR – Side-View Mirror

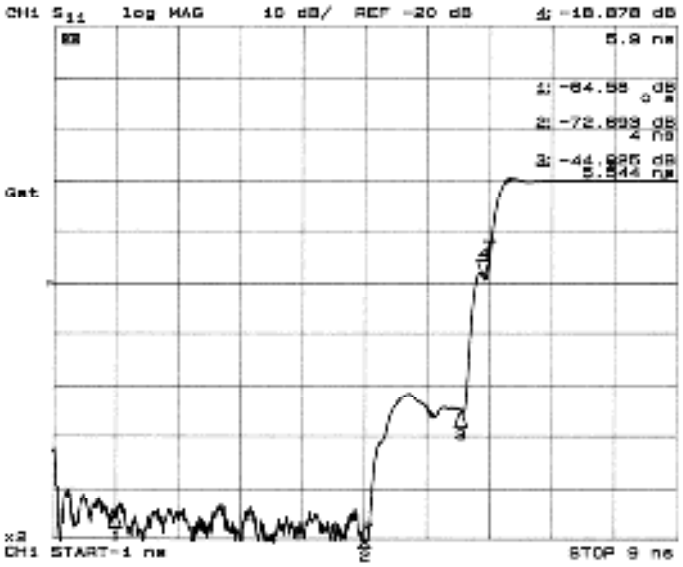


Figure 3-G. Time Domain Trace Showing Gate Window Showing Two-Way Propagation Time.

The gate was centered at 4ns with a width of 4ns

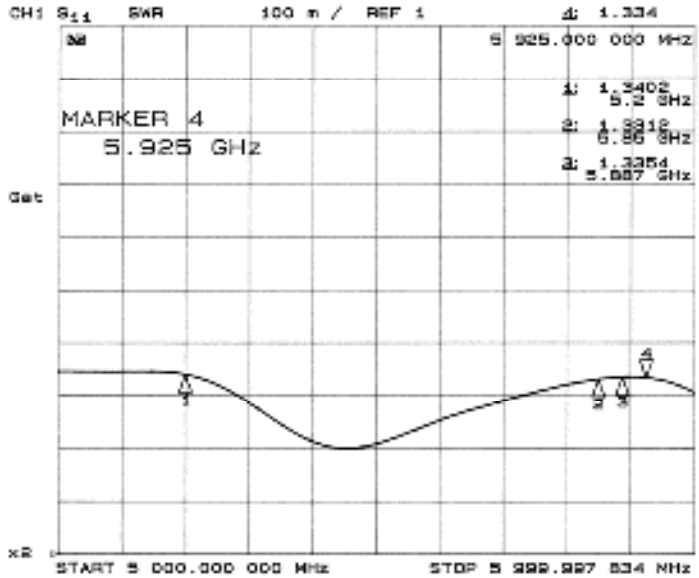


Figure 3-H. Measured VSWR

3.2.2.2 VSWR – Roof Mount

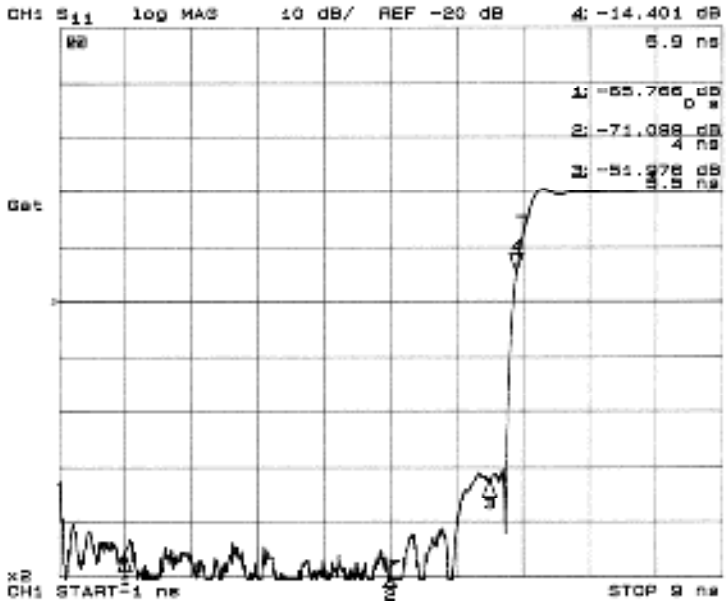


Figure 3-I. Time Domain Trace Showing Gate Window Showing Two-Way Propagation Time.

The gate was centered at 4ns with a width of 4ns.

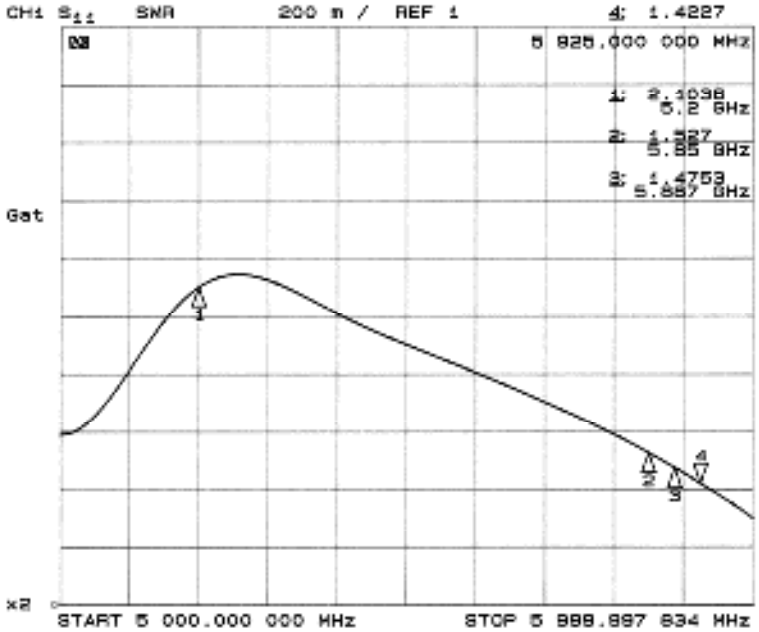


Figure 3-J. Measured VSWR

3.2.3 Summary

The measured gain of mirror mount antenna shows good agreement with the predicted performance as stated in the simulation report. The ripples in the azimuth radiation pattern in Figure 35 are due in part to the fixture suspending the antenna in free space and the housing. The antenna does provide good gain and nearly uniform coverage over ±90° azimuth. The elevation pattern shown in Figure 36 also shows good elevation coverage to ±30°.

The measured VSWR of the mirror mount antenna shown in Figure 42 is also in agreement with the simulation. The VSWR is nearly flat at approximately 1.3:1 over the entire frequency range of interest including the WLAN and ITS DSRC bands.

The roof mount antenna is not as broad banded as the mirror mount design as shown in Figure 44. The VSWR in the ITS DSRC band is approximately 1.4:1 and 2.1:1 in the WLAN band.

3.3 Vehicle Level Range testing

3.3.1 J.E.F. Range Characteristics

Vehicle level radiation pattern data was taken at the JEF antenna range. The antenna range utilizes a 40-foot turntable with a conductive surface. The large turntable allows a vehicle to be offset so as to align the rotation axis with the antenna under test. This greatly reduces rotation eccentricity thereby reducing or eliminating measured gain fluctuations due to both path loss variation and source beam width effects. The antenna range uses low loss Andrew ½” Helix coaxial cable and a rotary joint at the turntable.

The measurements were conducted using a Agilent E8742C synthesized signal generator, Hughes Instruments 8020H02 traveling wave tube amplifier, an HP 8593A spectrum analyzer, and two standard gain horns. With this equipment, a 70dB test dynamic range was achieved.

A standard gain horn was used as the source antenna and was located 7 meters (32 feet) from the turntable center. The height of the source standard was adjusted to the antenna under test (AUT) height prior to measurements.

Calibration Setup

Calibration was performed using two gain standard horns of known gains for the frequencies tested. Images of the calibration setup are shown in Figures 45 and 46. The horns are spaced at 23 feet at a height of 48”. Calibrations were performed at 5.2, 5.85, 5.8875, and 5.925GHz.

Figure 3-K. Calibration Setup

Figure 3-L. Calibration Setup

3.3.2 Side-Mirror Antenna Tests

Below are various images taken of the range configuration for testing the mirror mount antenna on both driver and passenger sides of the vehicle.

Antenna Height of 45”

Unavoidable Offset From Source

Antenna Aligned With Turntable Rotation Axis

Driver-Side Mirror Setup

Vehicle With Respect to Horn Source

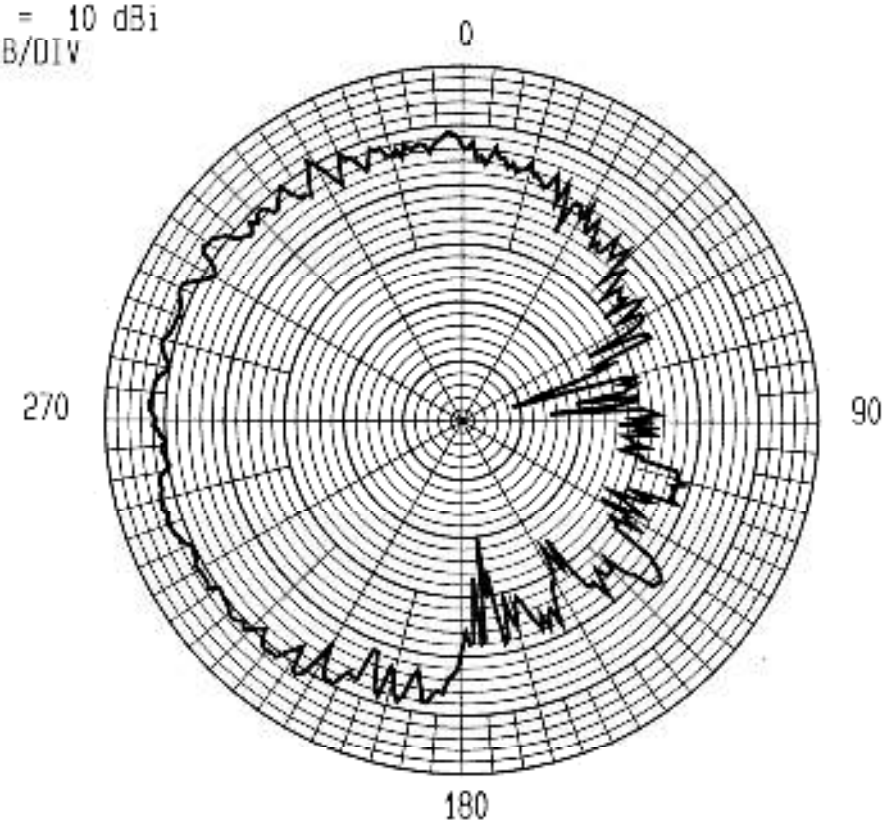
Passenger-Side Mirror Setup

3.3.2.1 Driver Side-Mirror Pattern (Unit 26) 5850 MHz

JEF CONSULTANT INC.

DATE.....02-25-2004 · TIME.....11:04:17 PATTERN.....004

REF = 10 dBi
2 dB/DIV



AVERAGE GAIN.....-2.9 dBi
MIN/MAX RATIO..... 43.8 dB

MAX GAIN..... 2.7 dBi
MIN GAIN.....-41.1 dBi

UNIT TESTED....2002 INFINITI
Mfg./Model.....Q45
Type.....MIRROR MOUNT ANTENNA
Comments.....UNIT 26

Frequency.....5.85 GHz
ID Number.....294515
Location.....DRIVER SIDE MIRROR

RF DETECTOR....SPECTRUM ANALYZER
Resolution BW..30 KHz

Mfg./Model.....HP 8593E
Detector Fn....Peak

RF SOURCE.....LAB SIGNAL
RF Level.....-10 dBm
Transmit Ant...NRL STD GAIN HORN
Height.....45 INCHES

Mfg./Model.....AGILENT E8247C
Modulation.....NONE
Polarization...VERTICAL
Range.....23 FT.

Software by JEF Consultant, Inc. (734) 482-5505

Figure 3-M. Mirror Mount Antenna Including 2 ft Pigtail (2dB Loss)

3.3.2.2 Passenger Side-Mirror Pattern (Unit 26) 5850 MHz

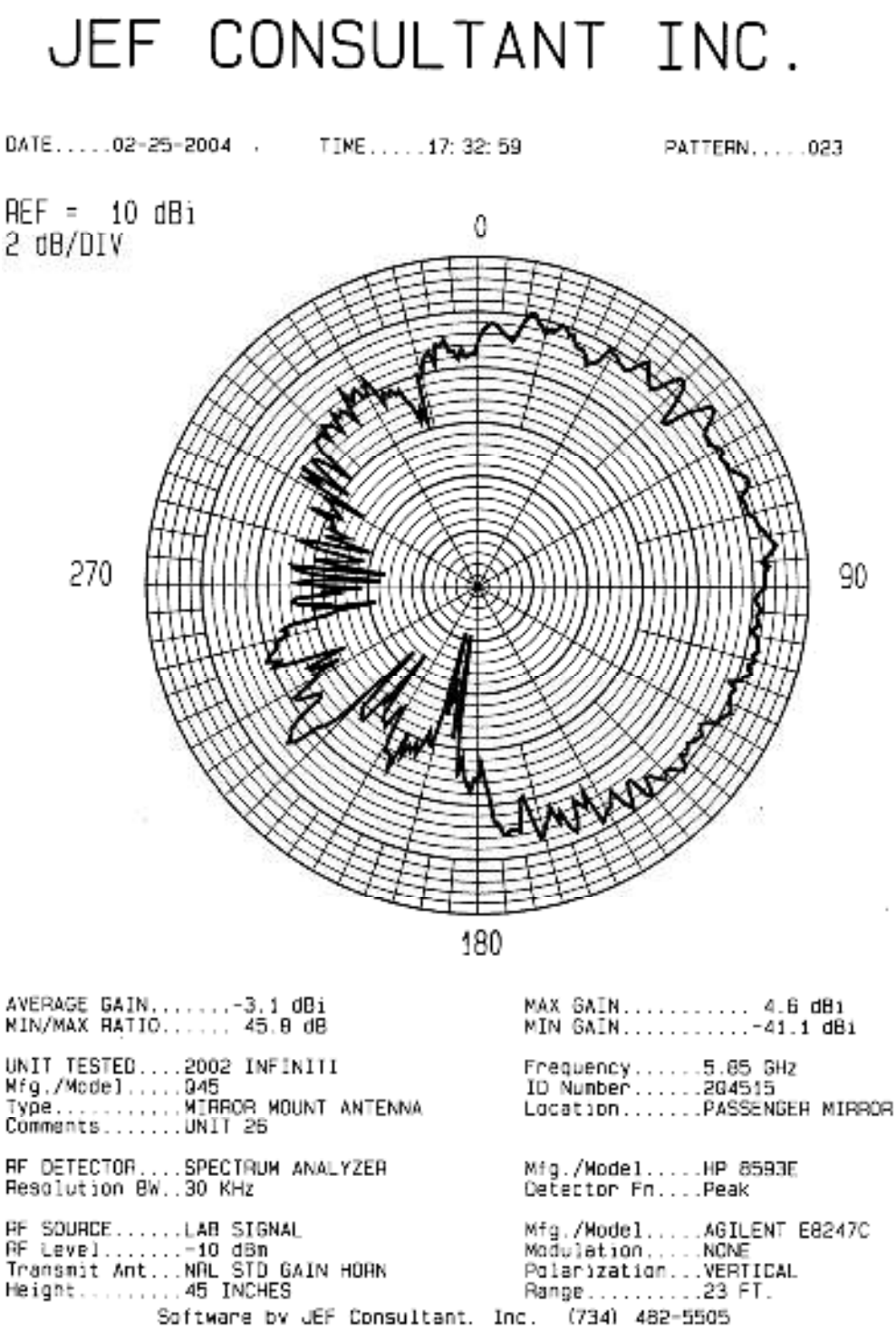
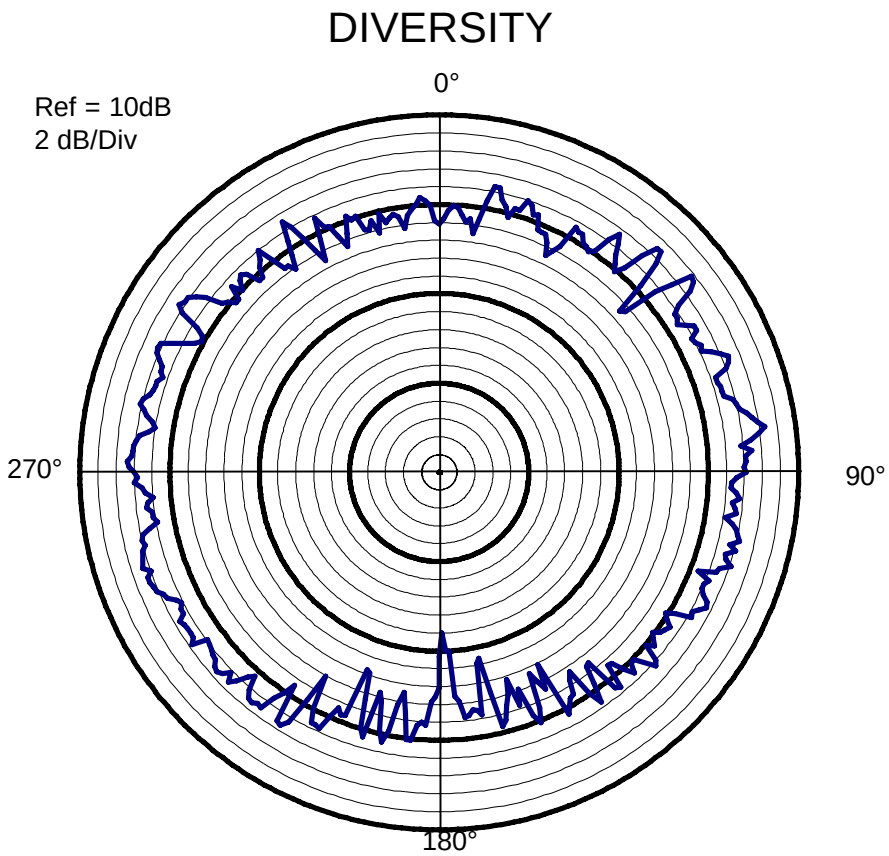


Figure 3-N. Mirror Mount Antenna Including 2 ft Pigtail (2dB Loss)

3.3.2.3 Side Mirror Composite Diversity Pattern (Unit 26) 5850 MHz

Combining the driver- and passenger-side mirror radiation patterns in Figures 47 and 48 respectively can create a simulated diversity pattern. Figure 49 was created by comparing point-by-point the driver and passenger side mirror antenna data and keeping the greater amplitude. There exists a null rear of the vehicle; otherwise the coverage is nearly uniform.



Statistics		**5.85 GHz**			
Average	1.73	dBil	Maximum	6.63	dBil
Std Dev	2.90	dBil	Minimum	-12.02	dBil
			Max-Min	18.65	dBil

Antenna 1	UNIT 26	DRIVER SIDE MIRROR
Antenna 2	UNIT 26	PASSENGER MIRROR

Figure 3-O. Composite Radiation Pattern

3.3.3 Roof Mount Antenna Tests on Ground Plane

The roof mount antennas were placed on a 36-inch diameter aluminum ground plane located 45 inches above the turntable.

4-Element WLAN Antenna on Ground Plane

5/8 Wave Antenna on Ground Plane

3.3.3.1 4-Element Array 5200MHz

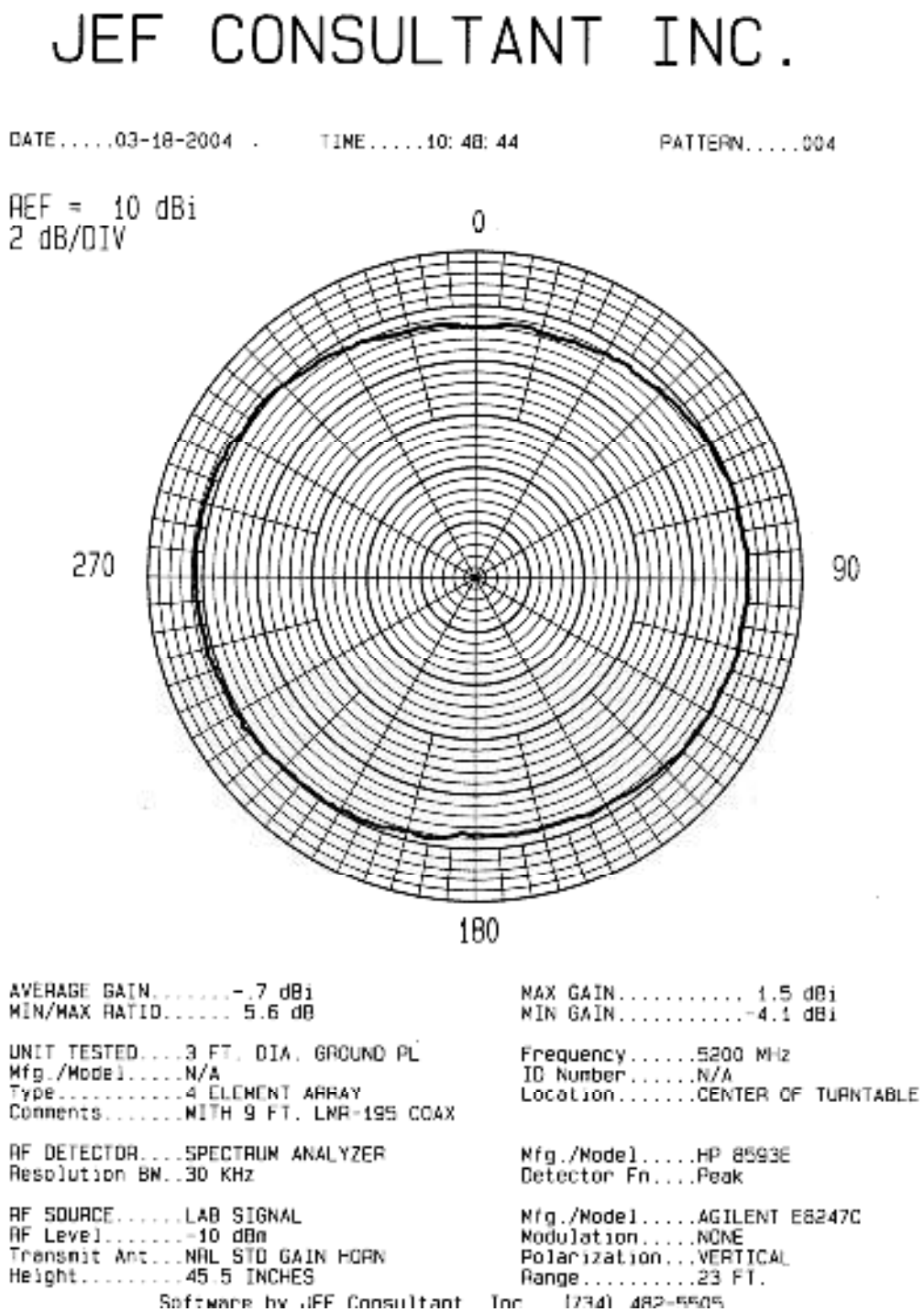


Figure 3-P. 4-Element WLAN Antenna Performance on Ground Plane Including 3dB Cable Loss

3.3.3.2 5/8 Wave 5887.5MHz

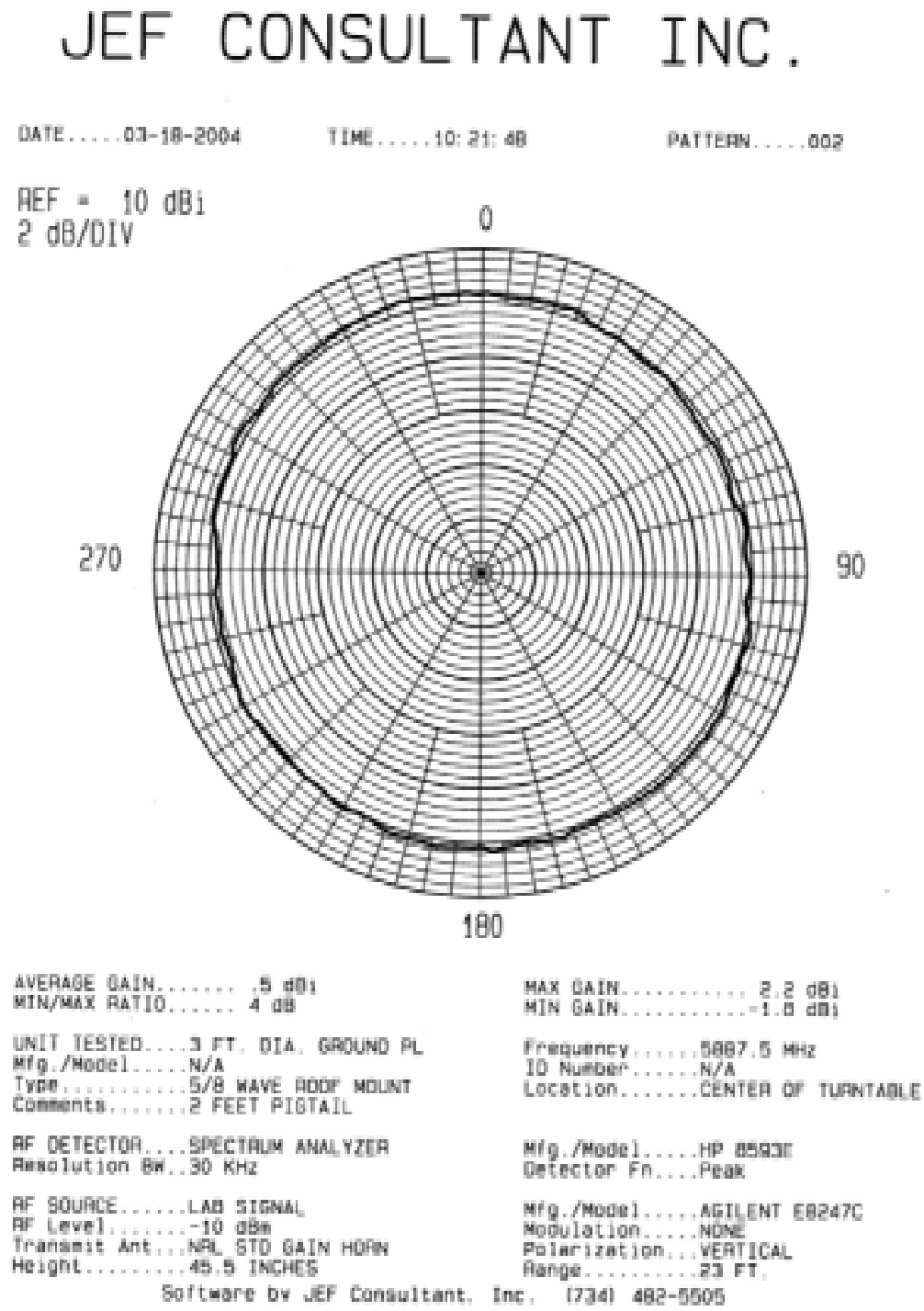


Figure 3-Q. 5/8 Wave Antenna Performance on Ground Plane Including 2dB Cable Loss

3.3.4 Roof Mount Antenna Test on Vehicle With Sunroof

The images below show the range configuration for testing the roof mount antennas on a vehicle with a sunroof. Both the 5/8 wave and 4-element WLAN antennas were located approximately 6 inches rearward of the sunroof.

Roof Mount Antenna

View From Source Antenna

Cable Route and Alignment

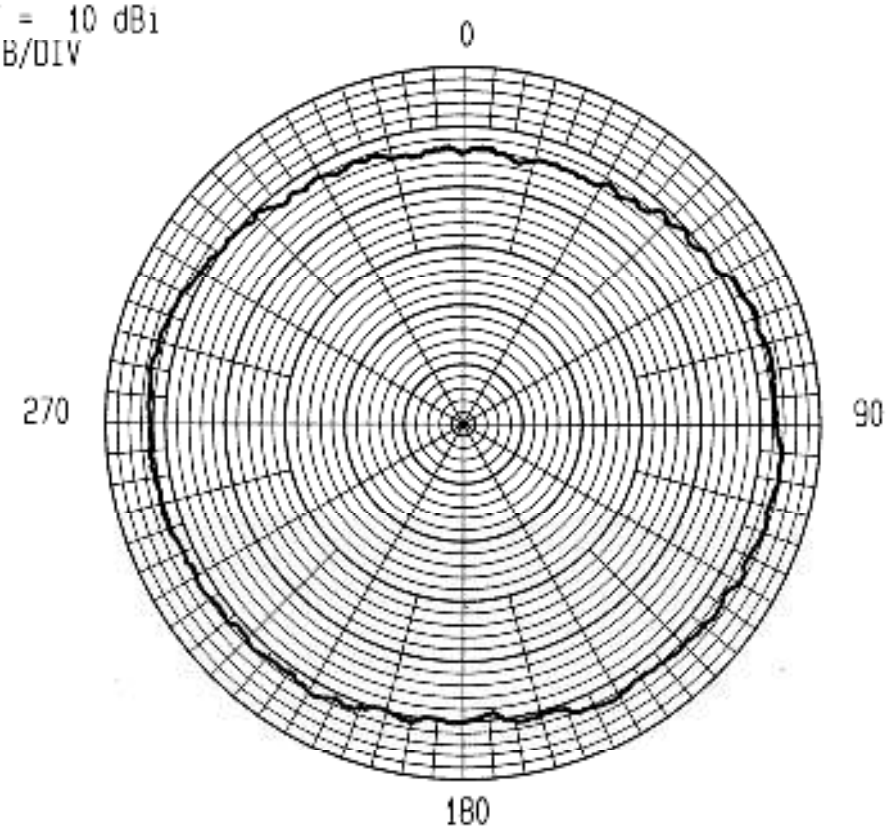
AUT Rotation on Turntable Axis

3.3.4.1 4-Element Array 5200MHz

JEF CONSULTANT INC.

DATE.....03-04-2004 . TIME.....11:13:53 PATTERN.....002

REF = 10 dBi
2 dB/DIV



AVERAGE GAIN..... 1.1 dBi
MIN/MAX RATIO..... 8.9 dB

MAX GAIN..... 3.8 dBi
MIN GAIN.....-5.1 dBi

UNIT TESTED....2002 INFINITI
Mfg./Model.....Q45
Type.....4-ELEMENT ARRAY
Comments.....WITH 9 FT. LMR-195 COAX

Frequency.....5200 MHz
ID Number.....204515
Location.....CENTER OF ROOF

RF DETECTOR....SPECTRUM ANALYZER
Resolution BW..30 KHz

Mfg./Model.....HP 8593E
Detector Fn....Peak

RF SOURCE.....LAB SIGNAL
RF Level.....-10 dBm
Transmit Ant...NRL STD GAIN HORN
Height.....58 INCHES

Mfg./Model.....AGILENT E8247C
Modulation.....NONE
Polarization...VERTICAL
Range.....23 FT.

Software by JEF Consultant, Inc. (734) 482-5605

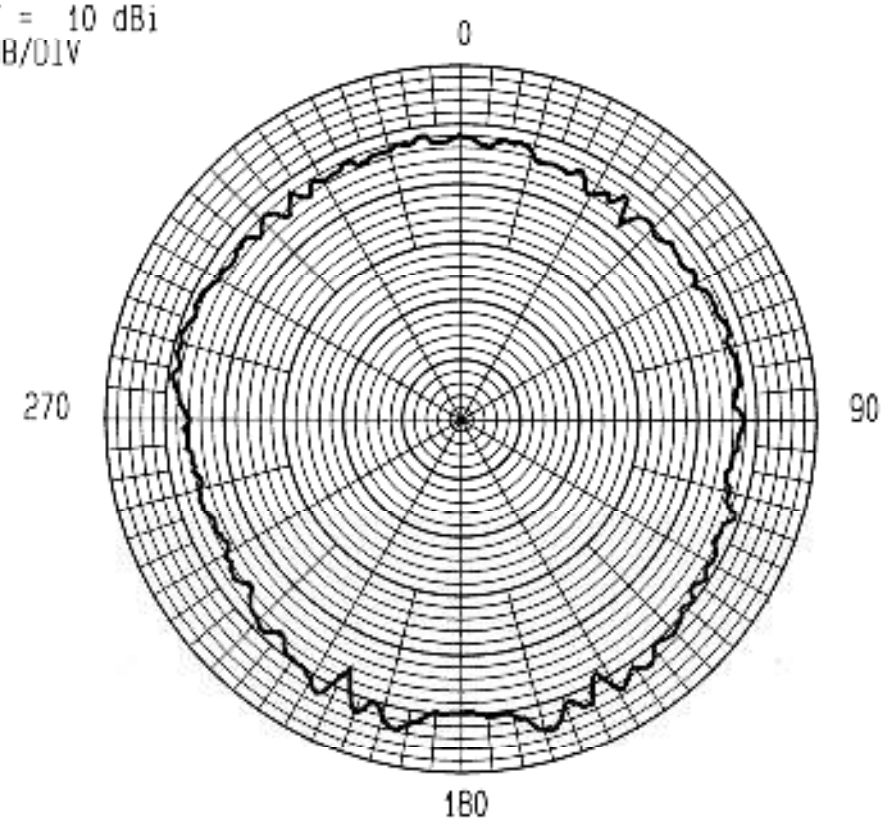
Figure 3-R. 4-Element Array With Sunroof Including 3dB Cable Loss

3.3.4.2 5/8 Roof Mount 5850MHz

JEF CONSULTANT INC.

DATE.....03-04-2004 . TIME.....11:24:05 PATTERN.....003

REF = 10 dBi
2 dB/DIV



AVERAGE GAIN.....-1.4 dBi
MIN/MAX RATIO..... 12.2 dB

MAX GAIN..... 4.8 dBi
MIN GAIN.....-7.4 dBi

UNIT TESTED....2002 INFINITI
Mfg./Model.....Q45
Type.....5/8 WAVE ROOF MOUNT
Comments.....2 FEET PIGTAIL

Frequency.....5850 MHz
ID Number.....294515
Location.....CENTER OF ROOF

RF DETECTOR....SPECTRUM ANALYZER
Resolution BW..30 KHz

Mfg./Model.....HP 8593E
Detector Fn....Peak

RF SOURCE.....LAB SIGNAL
RF Level.....-10 dBm
Transmit Ant...NRL STD GAIN HORN
Height.....58 INCHES

Mfg./Model.....AGILENT E8247C
Modulation.....NONE
Polarization...VERTICAL
Range.....23 FT.

Software by JEF Consultant, Inc. (734) 482-5505

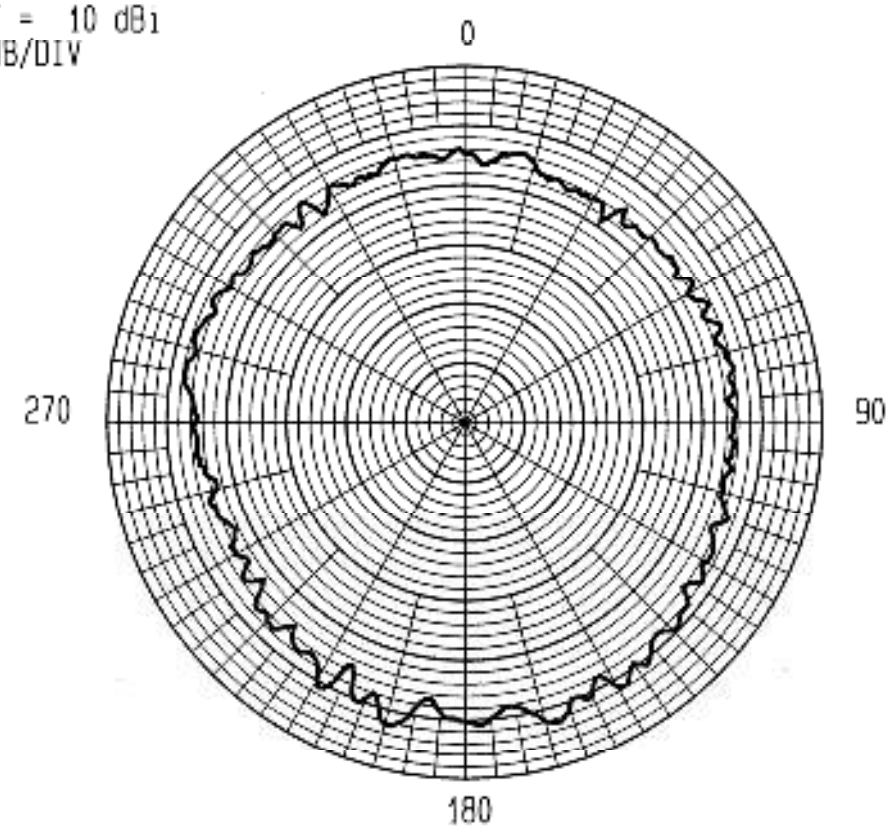
Figure 3-S. 5/8 Wave With Sunroof Including 2dB Cable Loss

3.3.4.3 5/8 Roof Mount 5887.5MHz

JEF CONSULTANT INC.

DATE.....03-04-2004 . TIME.....11:39:30 PATTERN.....004

REF = 10 dBi
2 dB/DIV



AVERAGE GAIN.....-3.2 dBi
MIN/MAX RATIO..... 11.7 dB

MAX GAIN..... 2.6 dBi
MIN GAIN.....-9 dBi

UNIT TESTED....2002 INFINITI
Mfg./Model.....Q45
Type.....5/8 WAVE ROOF MOUNT
Comments.....2 FEET PIGTAIL

Frequency.....5887.5 MHz
ID Number.....204515
Location.....CENTER OF ROOF

RF DETECTOR....SPECTRUM ANALYZER
Resolution BW..30 KHz

Mfg./Model.....HP 8593E
Detector Fn....Peak

RF SOURCE.....LAB SIGNAL
RF Level.....-10 dBm
Transmit Ant...NRL STD GAIN HORN
Height.....58 INCHES

Mfg./Model.....AGILENT E8247C
Modulation.....NONE
Polarization...VERTICAL
Range.....23 FT.

Software by JEF Consultant, Inc. (734) 482-5505

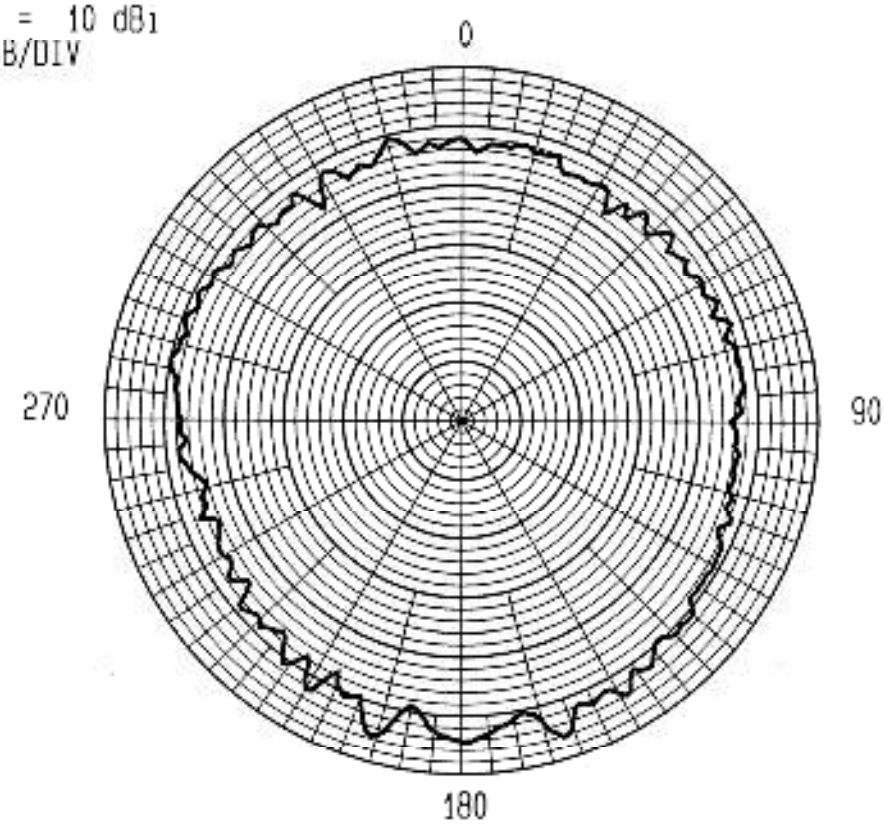
Figure 3-T. 5/8 Wave With Sunroof Including 2B Cable Loss

3.3.4.4 5/8 Roof Mount 5925MHz

JEF CONSULTANT INC.

DATE.....03-04-2004 . TIME.....11:48:25 PATTERN.....005

REF = 10 dBi
2 dB/DIV



AVERAGE GAIN.....-1 dBi
MIN/MAX RATIO..... 13.4 dB

MAX GAIN..... 6.1 dBi
MIN GAIN.....-7.3 dBi

UNIT TESTED....2002 INFINITI
Mfg./Model.....Q45
Type.....5/8 WAVE ROOF MOUNT
Comments.....2 FEET PIGTAIL

Frequency.....5925 MHz
ID Number.....204515
Location.....CENTER OF ROOF

RF DETECTOR....SPECTRUM ANALYZER
Resolution BW..30 KHz

Mfg./Model.....HP 8593E
Detector Fn....Peak

RF SOURCE.....LAB SIGNAL
RF Level.....-10 dBm
Transmit Ant...NRL STD GAIN HORN
Height.....58 INCHES

Mfg./Model.....AGILENT E8247C
Modulation.....NONE
Polarization...VERTICAL
Range.....23 FT.

Software by JEF Consultant. Inc. (734) 482-5505

Figure 3-U. 5/8 Wave With Sunroof Including 2dB Cable Loss

3.3.5 Roof Mount Antenna Tests on Vehicle Without Sunroof

Side View of WLAN Antenna on Vehicle

Side View of 5/8 Wave Antenna on Vehicle

Rear View of WLAN Antenna on Vehicle

Rear View of 5/8 Wave Antenna on Vehicle

3.3.5.1 4-Element Array 5200MHz

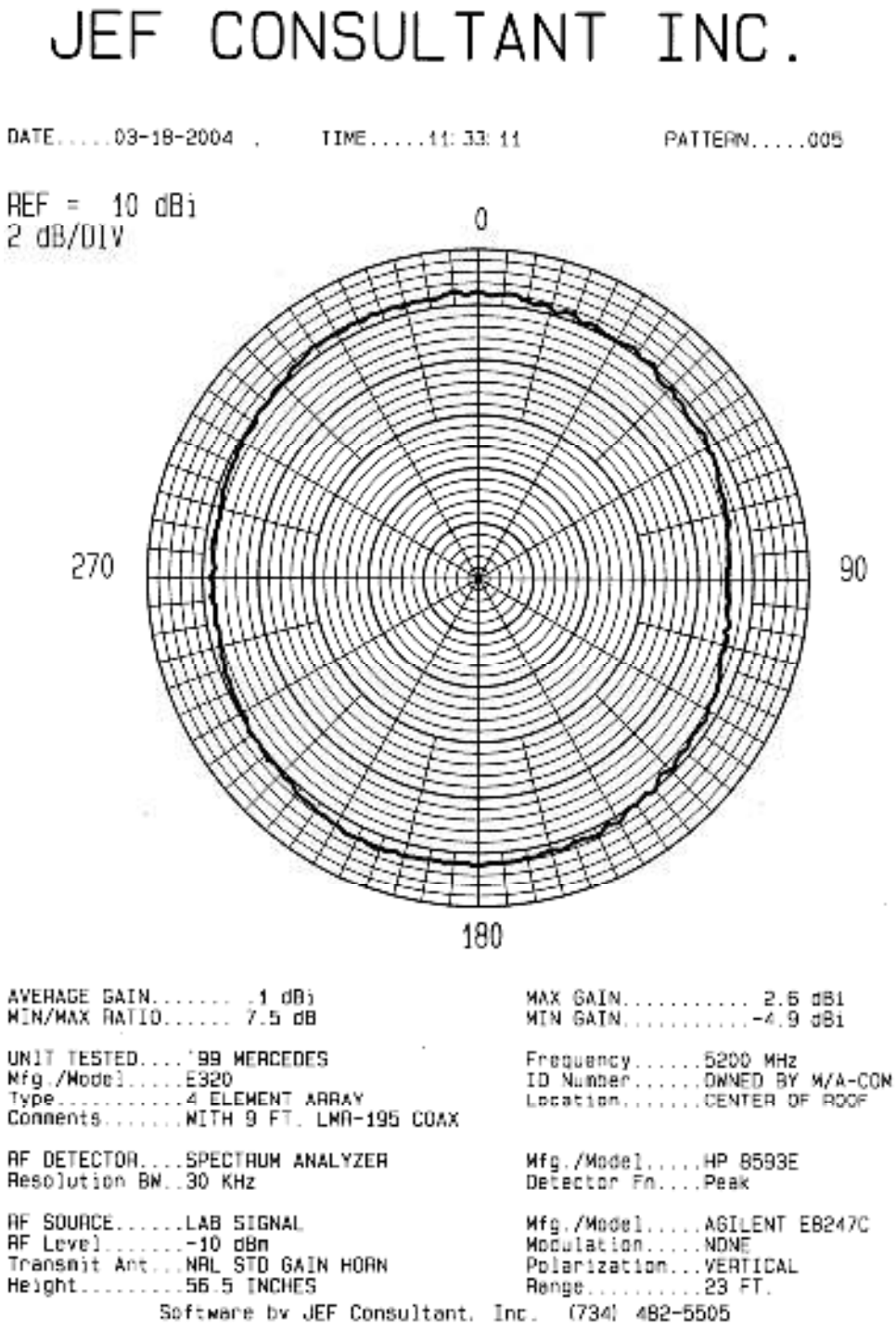


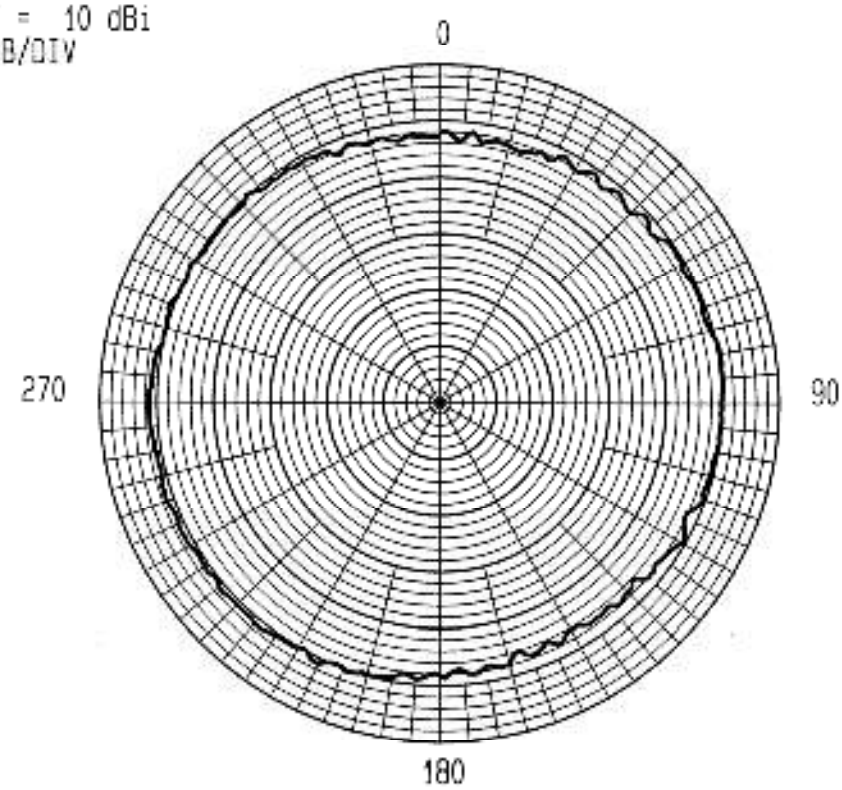
Figure 3-V. 4-Element Array Without Sunroof Including 3dB Cable Loss

3.3.5.2 5/8 Wave 5850MHz

JEF CONSULTANT INC.

DATE.....03-18-2004 . TIME.....12:55:47 PATTERN.....011

REF = 10 dBi
2 dB/DIV



AVERAGE GAIN.....-.7 dBi
MIN/MAX RATIO..... 5.2 dB

MAX GAIN..... 1.3 dBi
MIN GAIN.....-3.9 dBi

UNIT TESTED....'99 MERCEDES
Mfg./Model.....E320
Type.....5/8 WAVE ROOF MOUNT
Comments.....WITH 2 FT. PIG TAIL

Frequency.....5250 MHz
ID Number.....OWNED BY M/A-COM
Location.....CENTER OF ROOF

RF DETECTOR....SPECTRUM ANALYZER
Resolution BW..30 KHz

Mfg./Model.....HP 8593E
Detector Fn....Peak

RF SOURCE.....LAB SIGNAL
RF Level.....-10 dBm
Transmit Ant...NAL STD GAIN HORN
Height.....56.5 INCHES

Mfg./Model.....AGILENT E8247C
Modulation.....NONE
Polarization...VERTICAL
Range.....23 FT.

Software by JEF Consultant, Inc. (734) 482-5505

Figure 3-W. 5/8 Wave Without Sunroof Including 2dB Cable Loss

3.3.5.3 5/8 Wave 5887.5MHz

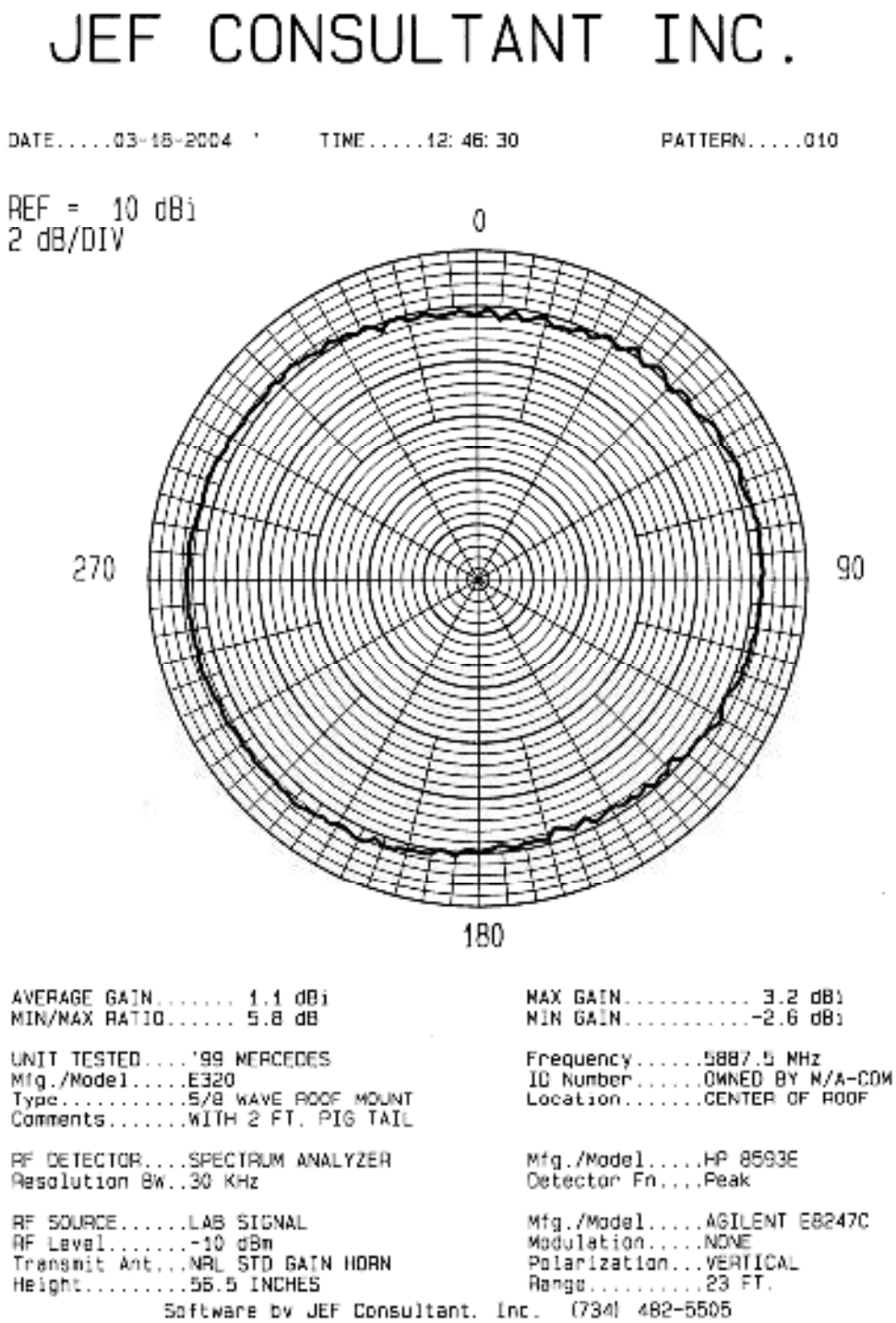


Figure 3-X. 5/8 Wave Without Sunroof Including 2dB Cable Loss

3.3.5.4 5/8 Wave 5925MHz

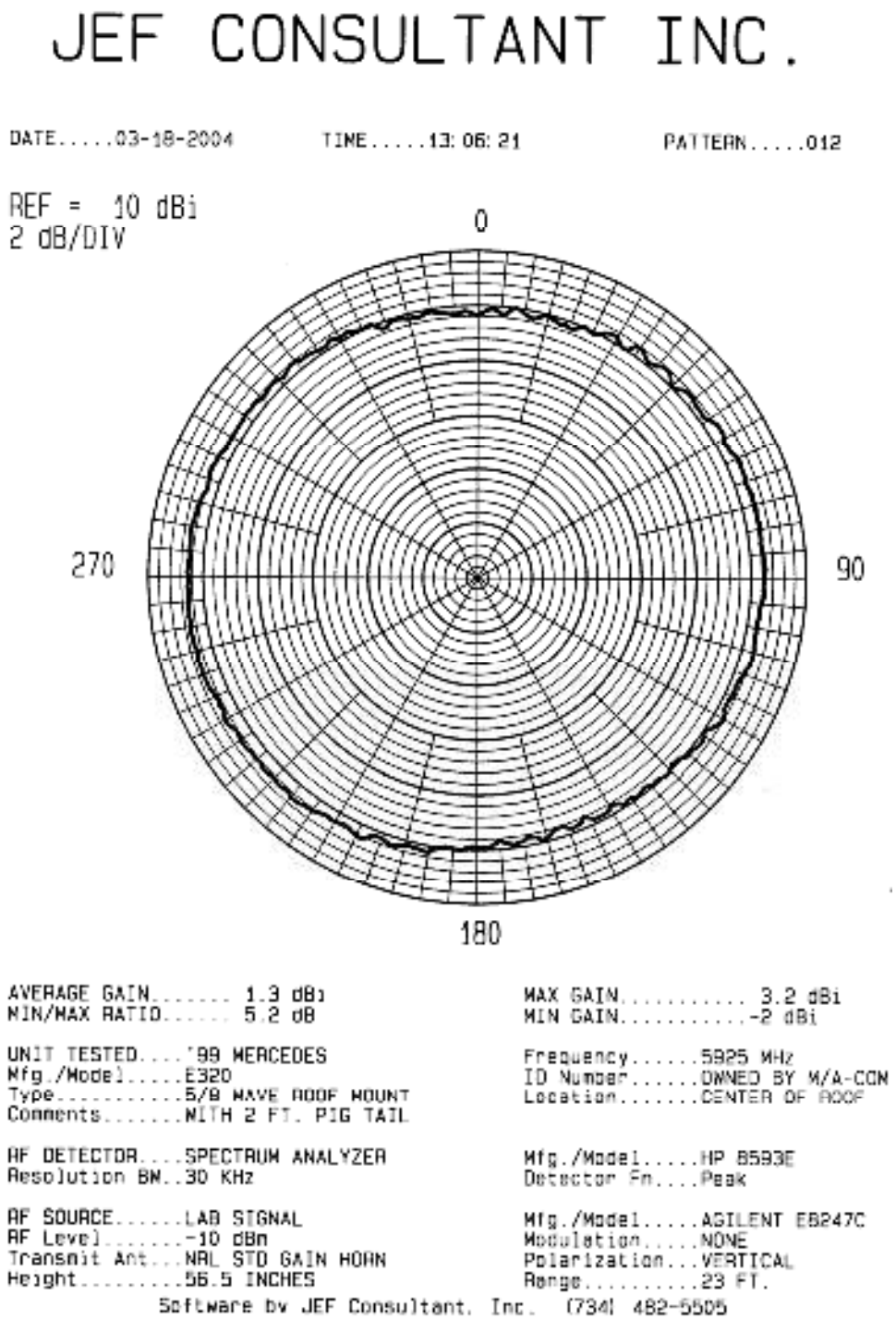


Figure 3-Y. 5/8 Wave Without Sunroof Including 2dB Cable Loss

3.4 Summary

3.4.1 Side Mirror Antenna

The measured vehicle level performance of the side mirror antenna shows no unexpected results having minimal vehicle influence. Each location provides good pattern coverage and gain for the respective driver and passenger sides of the vehicle. The simulated diversity combination of both patterns indicate nearly uniform azimuth coverage 360° around the vehicle and, in some cases, would provide better reception given diversity's ability to overcome physical obstacles realized by only one antenna.

3.4.2 Roof Mount

Both the 5/8 wave and a 4-element WLAN roof mount antennas were tested on a 36" diameter ground plane, a vehicle with a sunroof, and a vehicle without a sunroof. These measurements are intended to compare the vehicle and sunroof effects on antenna performance as compared to performance on a ground plane. The 4-element WLAN antenna serves as a reference antenna that was used in earlier drive testing conducted in the WLAN frequency band.

A comparison of the 5/8 wave and 4-element WLAN antennas operating at their center design frequency is shown below in Table 1.

	Avg gain, dBil, corrected for cable loss		
	36" GP	With sun roof	Without sun roof
4 element WLAN @ 5.2 GHz	2.3	4.1	3.1
5/8 wave @ 5.8875 GHz	2.5	-1.2	3.1

Table 1 Comparison of 5/8 Wave and WLAN Reference Antennas.

As shown Table 1, the antennas compare well on both the ground plane and vehicle without a sunroof however the 5/8 wave is more impacted by the presence of the sunroof. Both antennas exhibited gain bias to the vehicle rear and front to back gain variations of 4dB due to the sunroof as shown in Figures 52 and 54.

3.5 Test Kit Measurements

The test kits were evaluated for output frequency and transmit power at the JEF facility. This measurement was conducted using an HP 8593A spectrum analyzer as shown in Figure 60.

Figure 3-Z. Test Kit Evaluation Setup

The spectrum analyzer was set to a wide frequency span and max hold trace function. The test kit was configured to send 3000 packets of 4096 bytes per packet. The trace peak is then measured using a marker set to the desired frequency and the power level is read in dBm. The cable loss of 1.25dB is added back and the result is converted to mW.

The results of these tests are shown in Tables 1 and 2.

Logged in as root		**Power, mW**	
F (MHz)	**F measured**	**100%**	**25%**
5200	5200	47.3, 42.9	15.8
5800	5800	45.7, 45.9	
5900	5900	24.4	
5990	5990	16.8	

Logged in as DSRC		
F (MHz)	**F measured**	**100%**
5200	5320	57.8
5900	5320	62.7

Table 1. Test Kit Data Taken on January 30, 2004

	100%		50%	
	dBm	mW	dBm	mW
F (MHz)	raw	converted	raw	converted
5150	9.65	12.3	6.21	5.6
5350	10.05	13.5	6.9	6.5
5850	8.45	9.3	6.8	6.4
5890	9.56	12	7.48	7.5
5925	9.25	11.2	6.12	5.5

Table 2. Test Kit Data Taken on February 9, 2004

The inconsistency of the transmit power did not appear to be associated with the revision level of the software or output port selected.

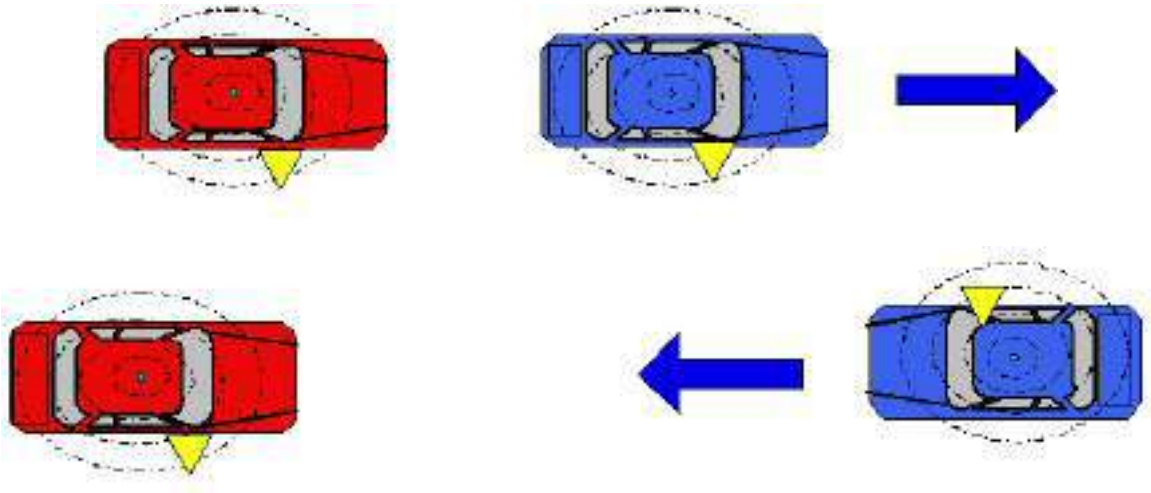
3.6 Drive Testing

Sections 3.6.1 through 3.6.5 define various drive test vehicle configurations. In all cases, the receiving vehicle is stationary and depicted in red. The transmitting vehicle is depicted in blue and the arrow indicates its direction of travel. The yellow triangle indicates the location of the side view mirror antenna; the roof mount is not indicated and is located in the center of the roof.

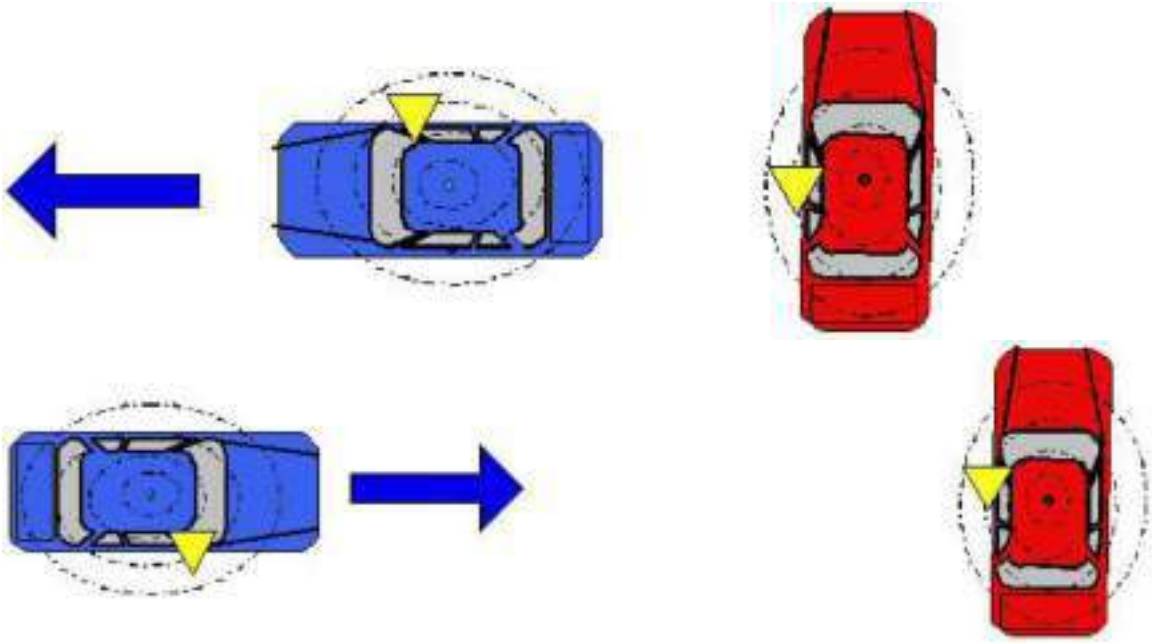
Drive tests were conducted at the Ford Motor Co. Dearborn Proving Ground, General Motors Milford Proving Ground (MPG), and a residential side street using test kits provided by CAMP. The collected data was processed through M/A-COM developed software to facilitate graphing and propagation modeling.

Drive tests conducted at the Ford Proving Ground are similar to those conducted at GM MPG, however the extension cables were not used at Ford due to connecter issues. Because the added cable losses are not in the system, the performance is 4dB better and so these results are listed at the end of Appendix D.

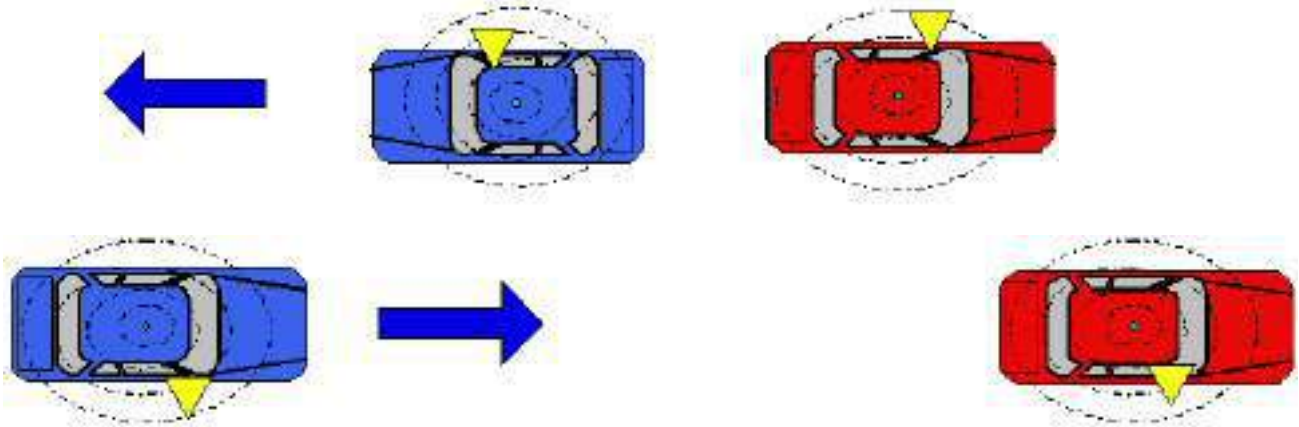
3.6.1 Receiving Vehicle Front



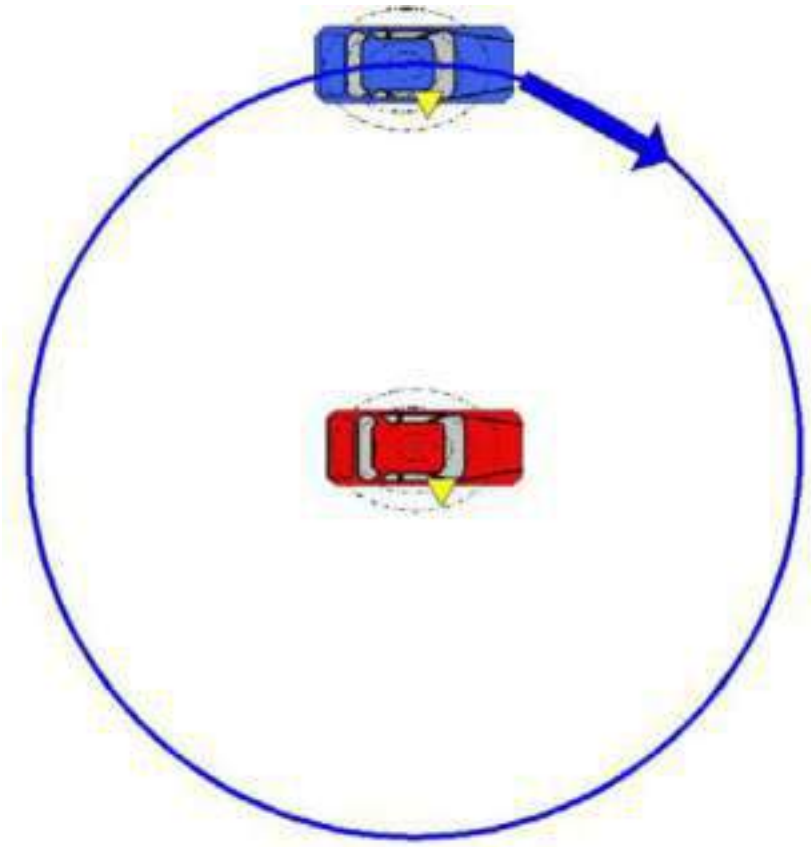
3.6.2 Receiving Vehicle Broadside



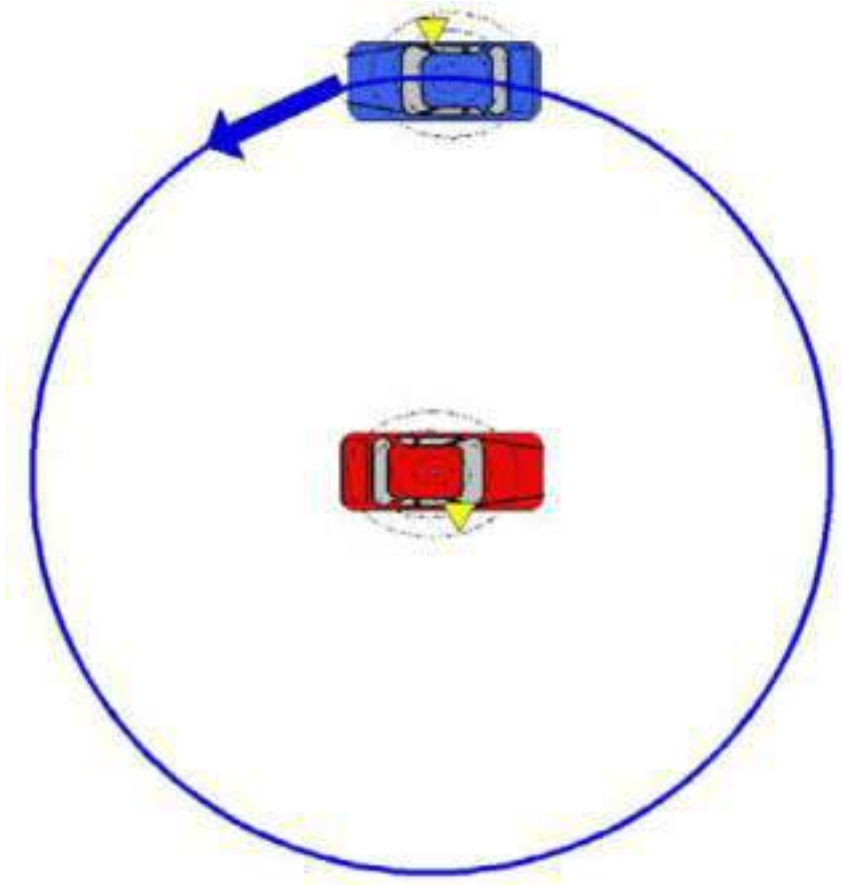
3.6.3 Receiving Vehicle Rear



3.6.4 Clockwise Circular Passenger-Side Antenna



3.6.5 Counter-Clockwise Circular Passenger-Side Antenna

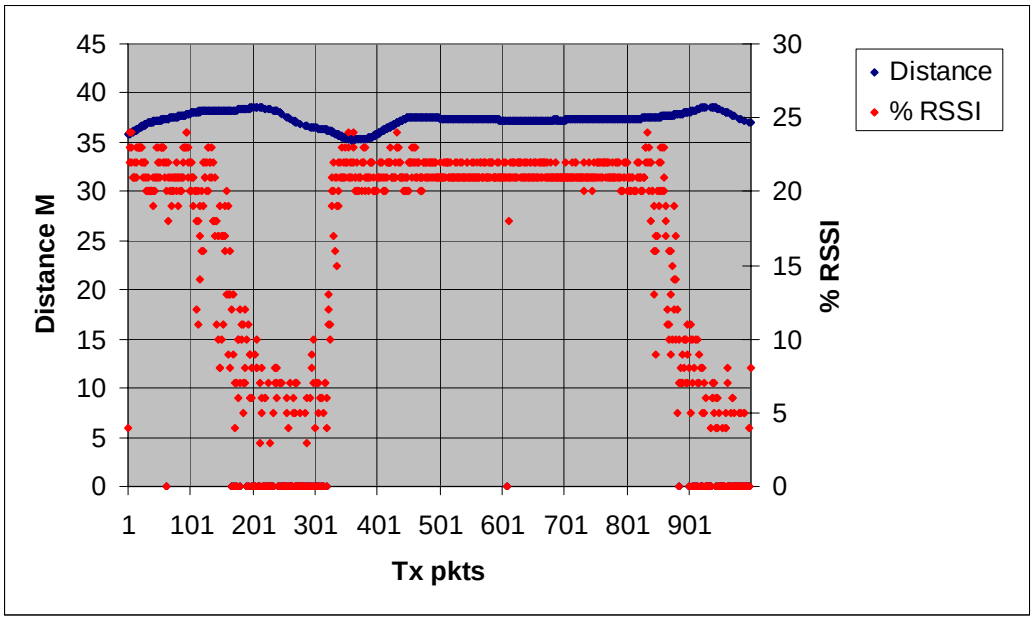


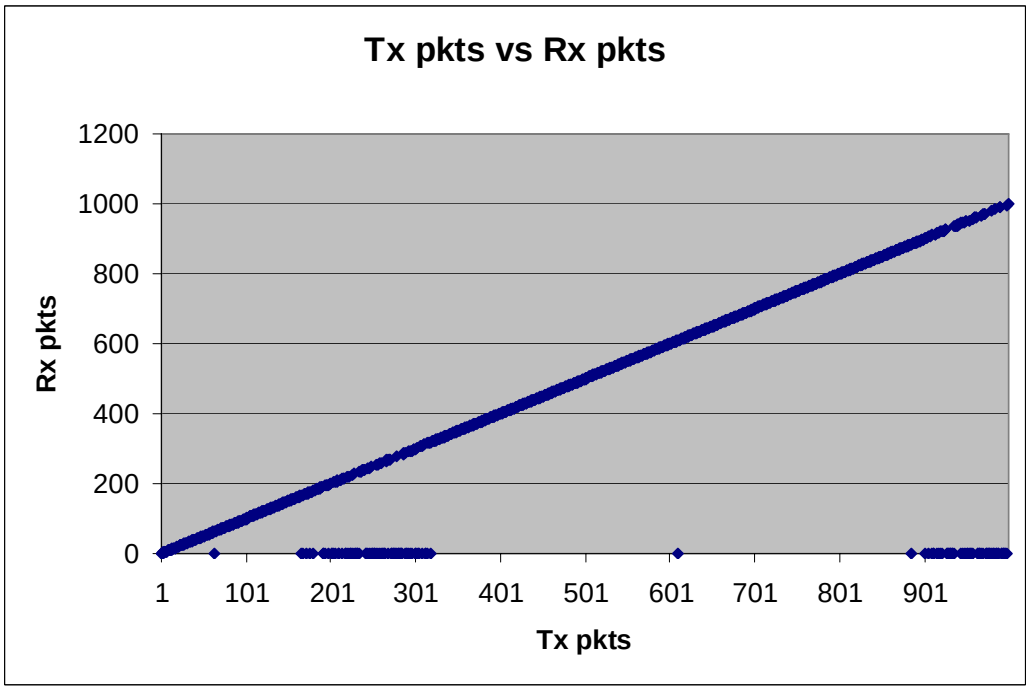
3.6.6 Test Results – Mirror Mount General Motors Proving Ground

Drive testing using both mirror mount antennas was conducted at the General Motors Milford Proving Ground. The intent for this testing was to measure the effective communication range of the mirror mount antennas under diversity conditions. The antenna pigtails are connected to the test kits using 6-foot long production intent extension coaxial cables made of LMR-195 having a measured 2dB of loss.

It was later discovered, during GM 12 test, that the auxiliary input port of the receiver test kit associated with the passenger side of the receiving vehicle was significantly less sensitive than the main port. As a result, the diversity measurements are not valid and explain why some packets were dropped during the initial grist mill track testing.

3.6.6.1 GM 1 5890 Clockwise Circular Passenger-Side Antenna

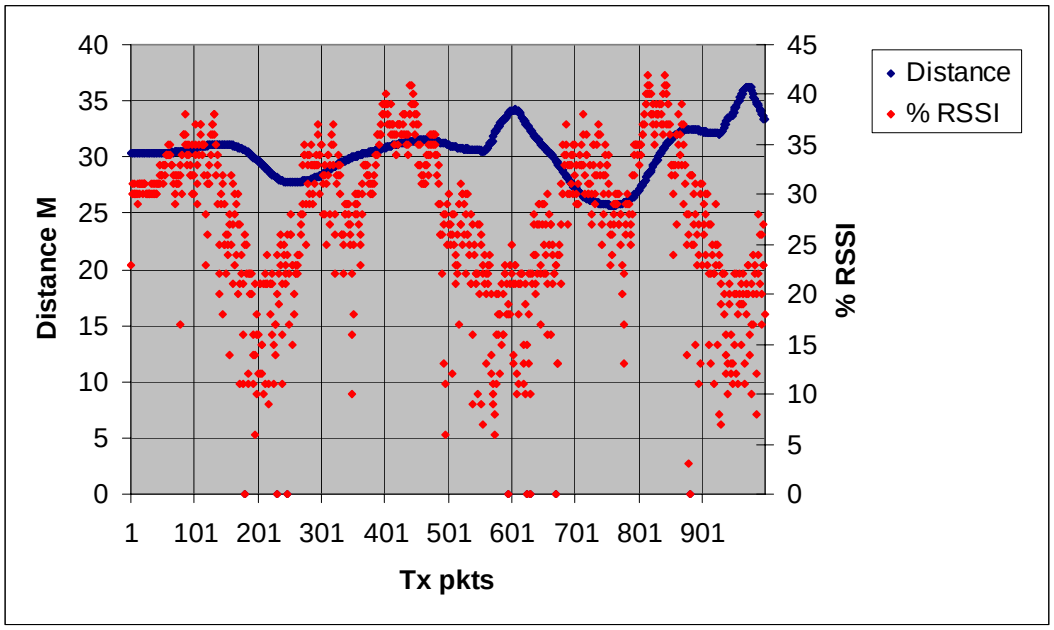


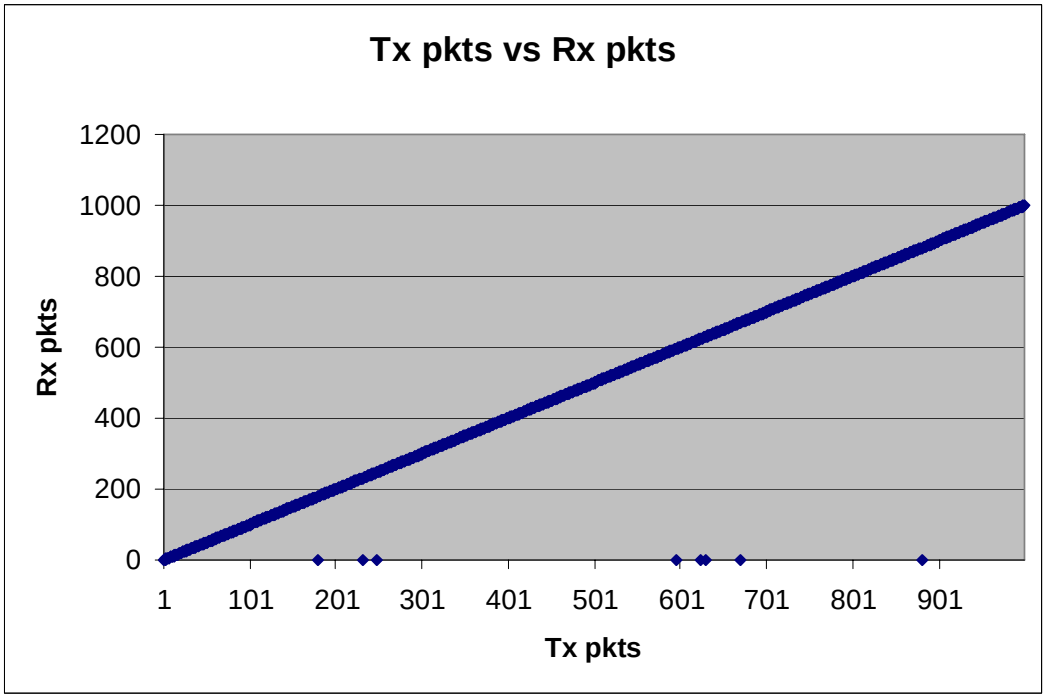


Total packets sent: 999

Total packets dropped: 134

3.6.6.2 GM 3 5890 Clockwise Circular Passenger-Side Antenna

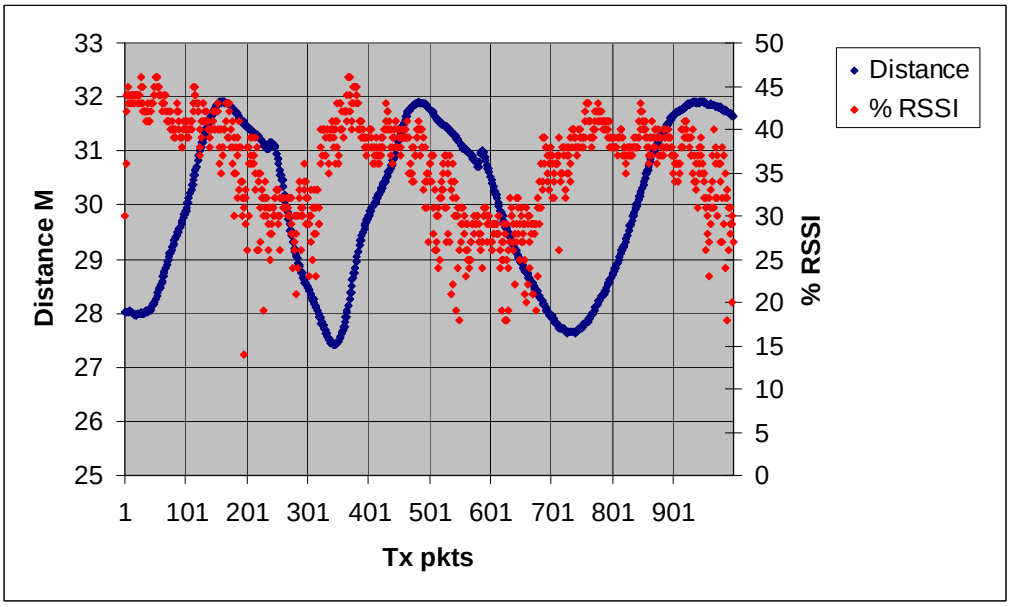


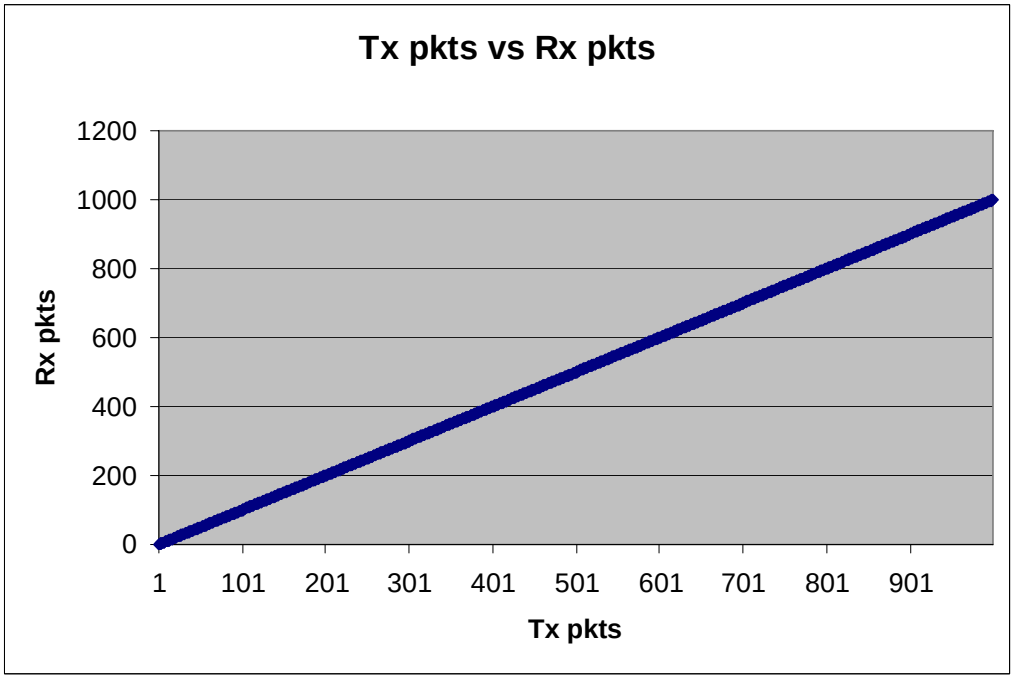


Total packets sent: 999

Total packets dropped: 8

3.6.6.3 GM 4 5200 Clockwise Circular Passenger-Side Antenna

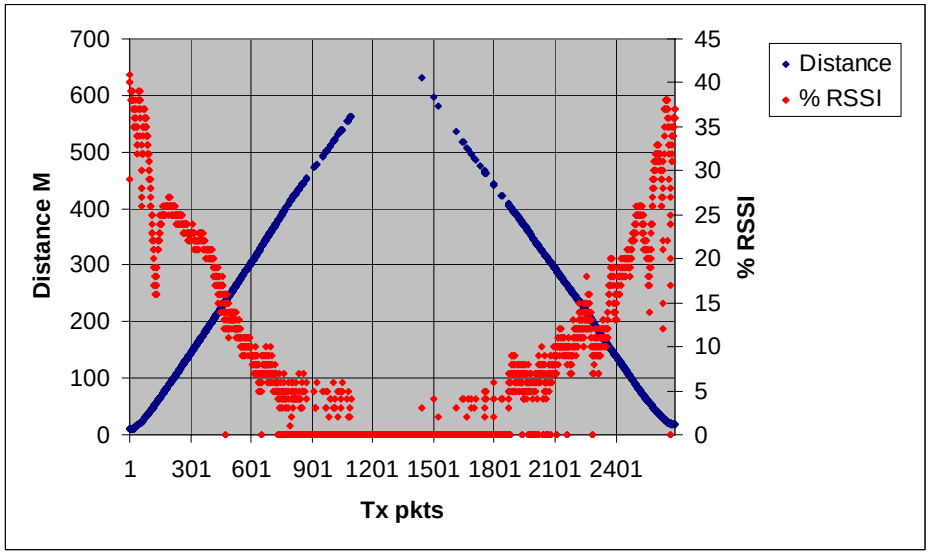


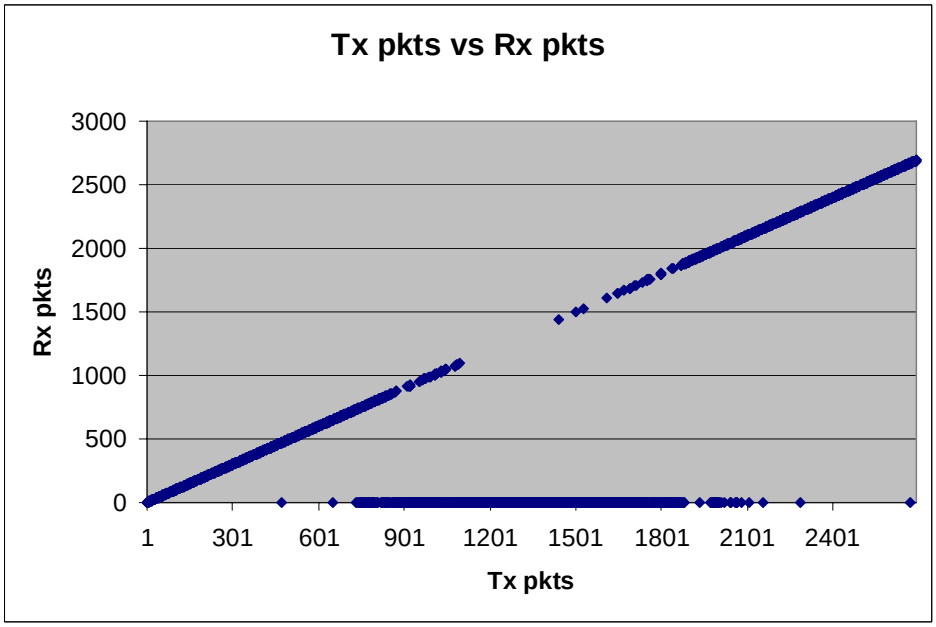


Total packets sent: 999

Total packets dropped: 0

3.6.6.4 GM 5 5890 Receiving Vehicle Front

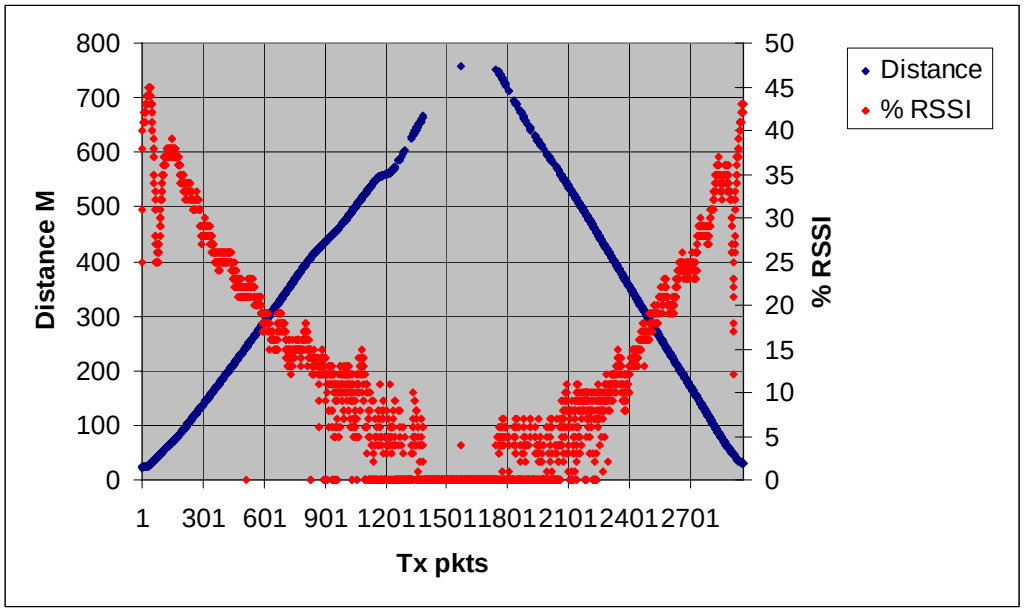


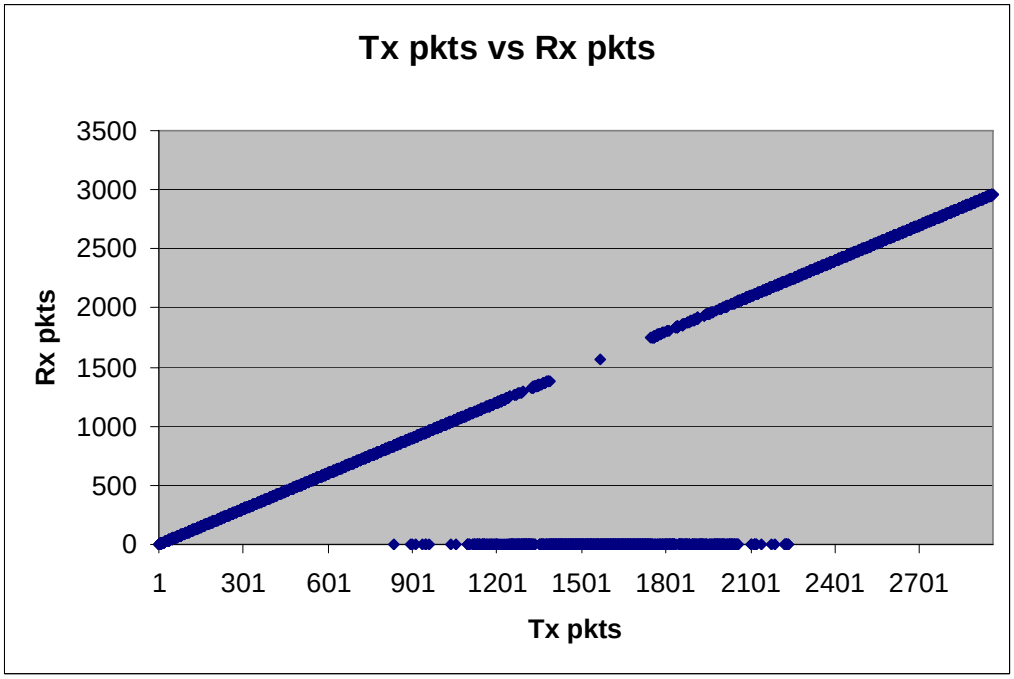


Total packets sent: 2691

Total packets dropped: 1036

3.6.6.5 GM 6 5200 Receiving Vehicle Front

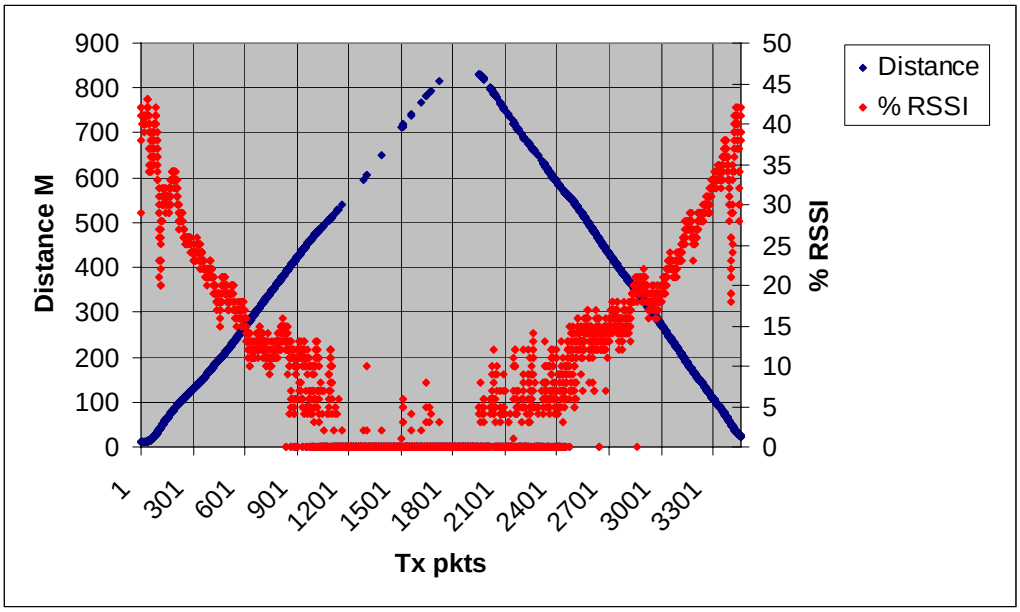


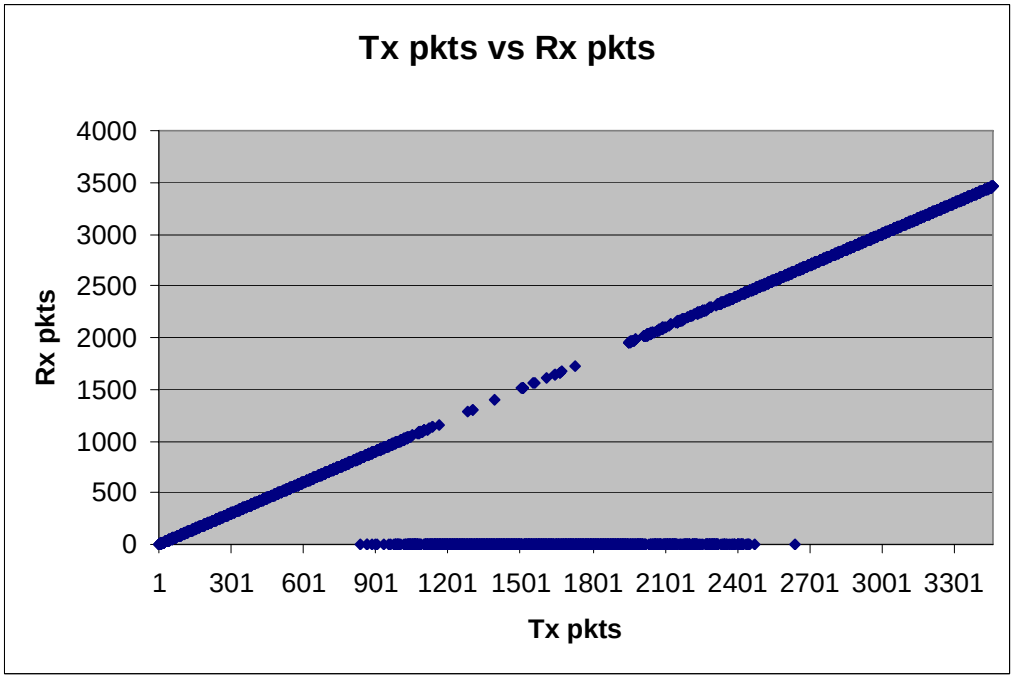


Total packets sent: 2960

Total packets dropped: 745

3.6.6.6 GM 7 5200 Receiving Vehicle Broadside

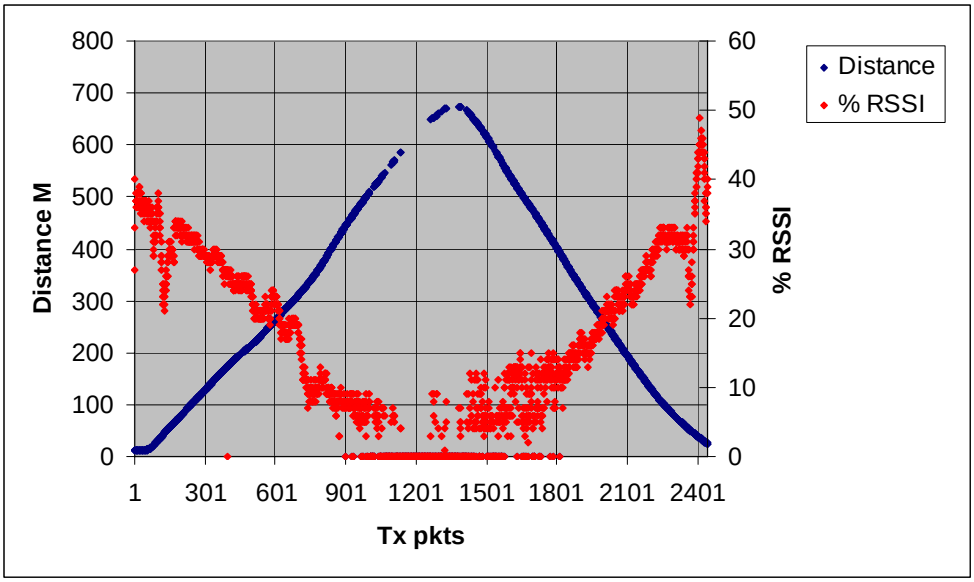


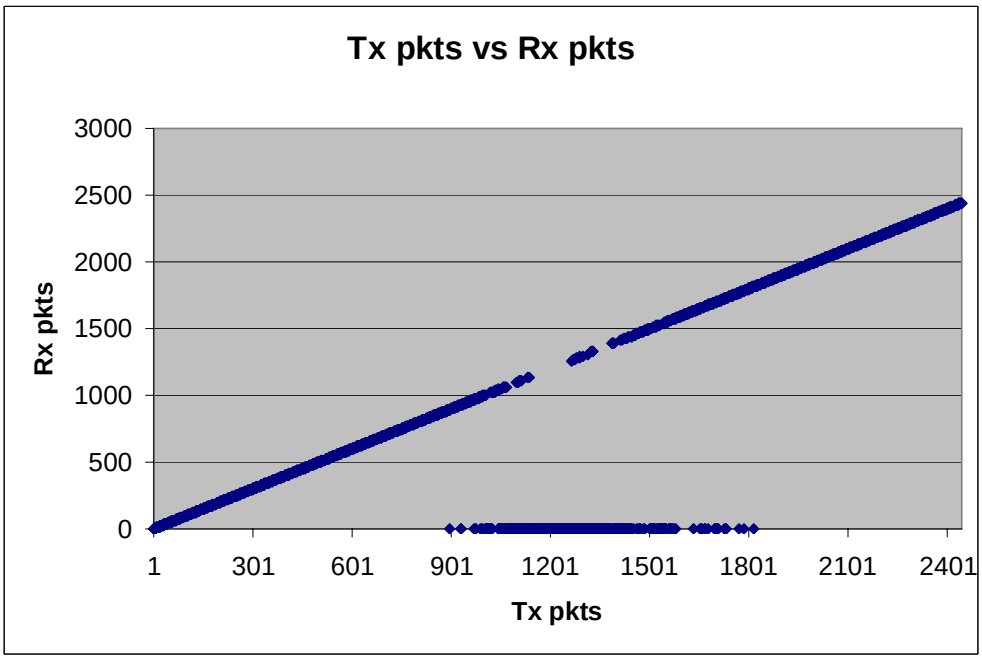


Total packets sent: 3460

Total packets dropped: 1161

3.6.6.7 GM 8 5320 Receiving Vehicle Rear

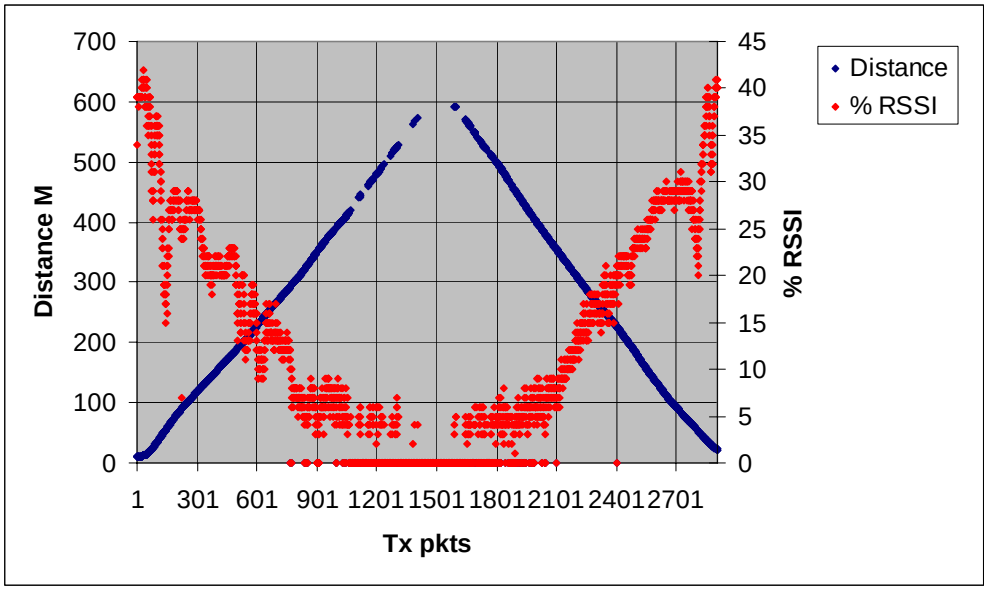


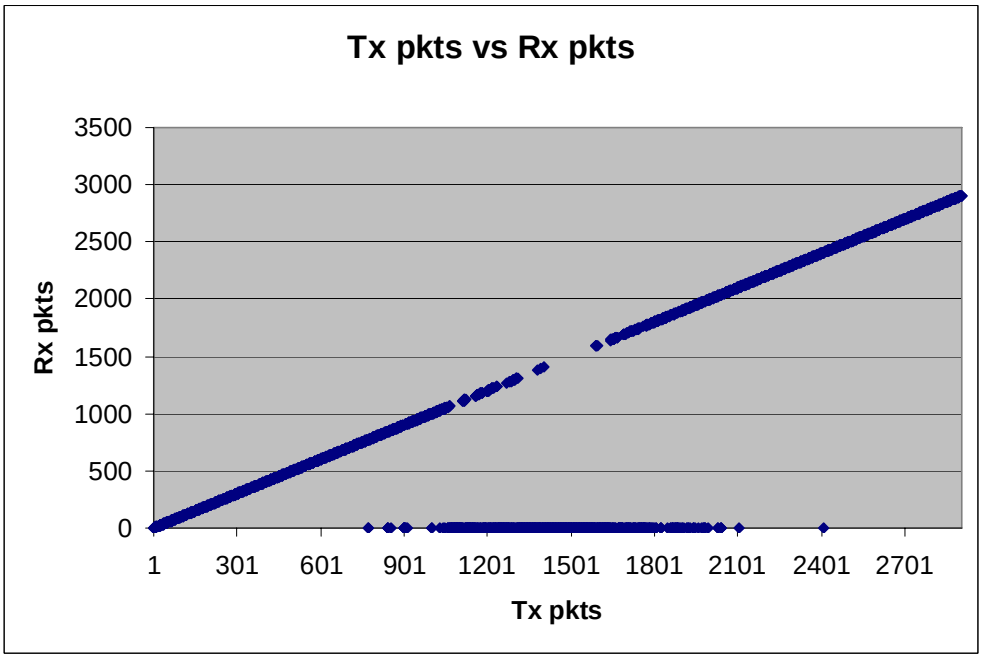


Total packets sent: 2442

Total packets dropped: 455

3.6.6.8 GM 11 5890 Receiving Vehicle Broadside

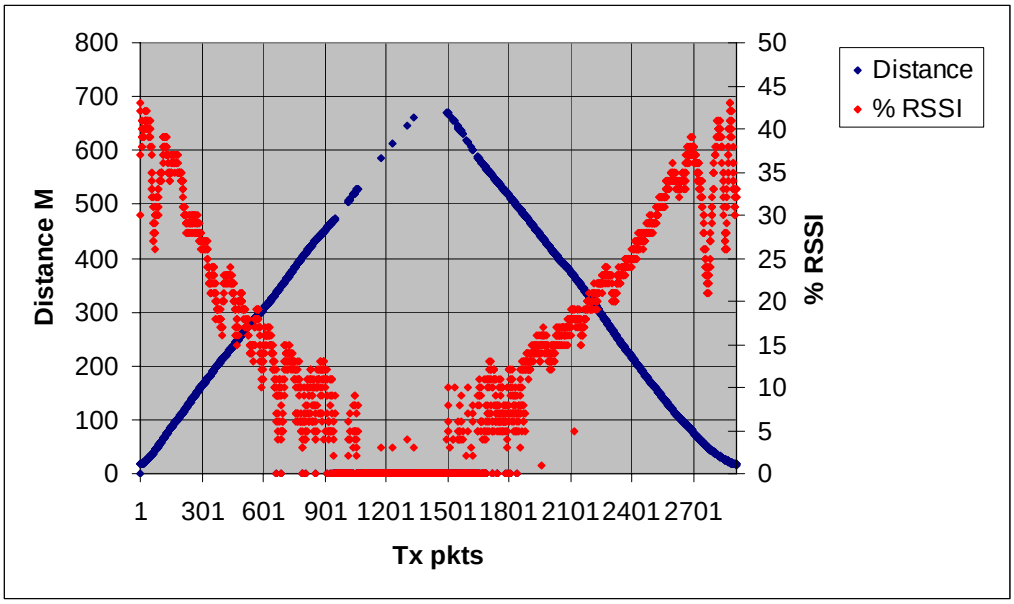


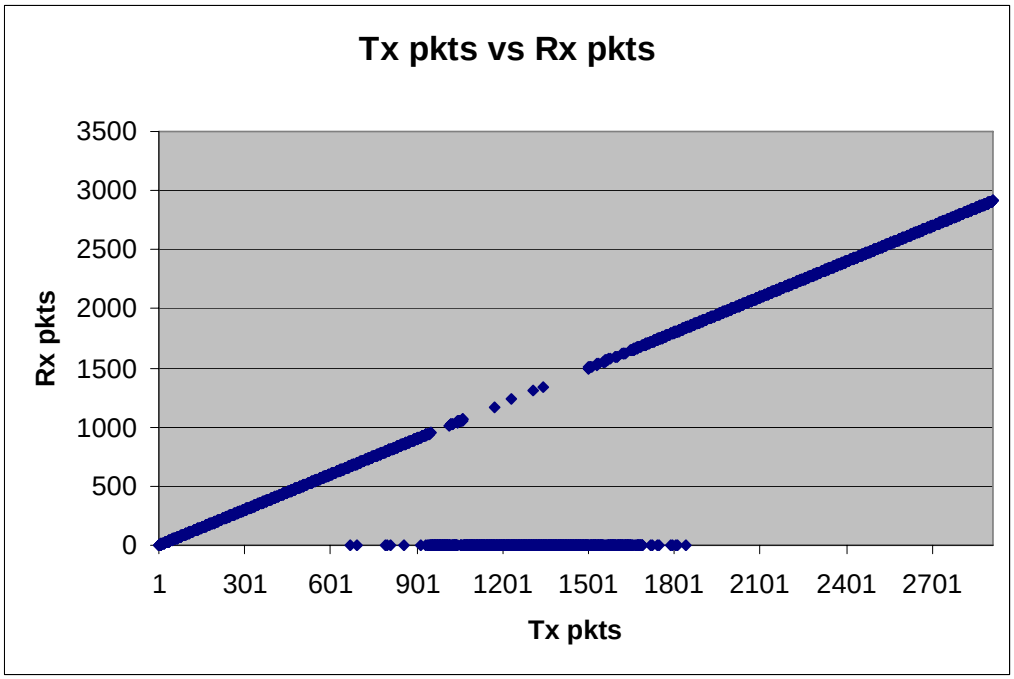


Total packets sent: 2905

Total packets dropped: 677

3.6.6.9 GM 9 5200 Receiving Vehicle Rear

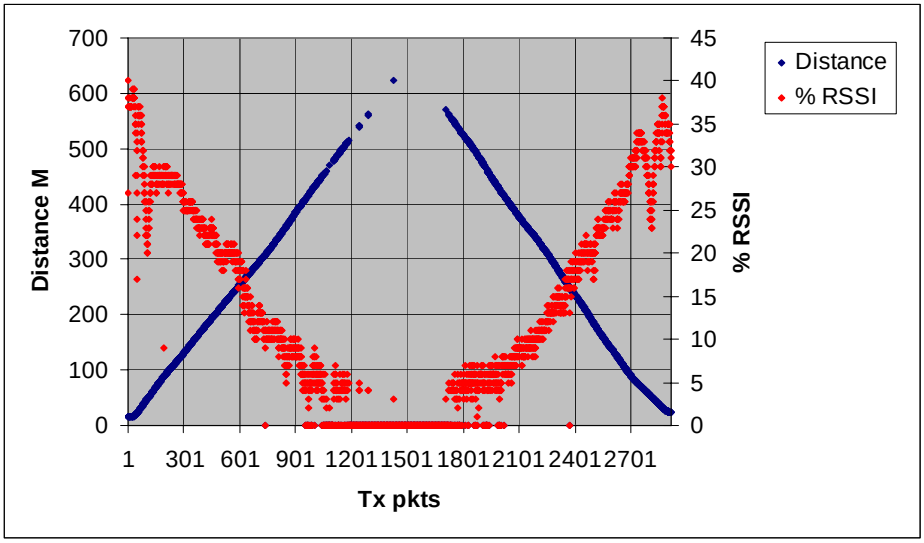


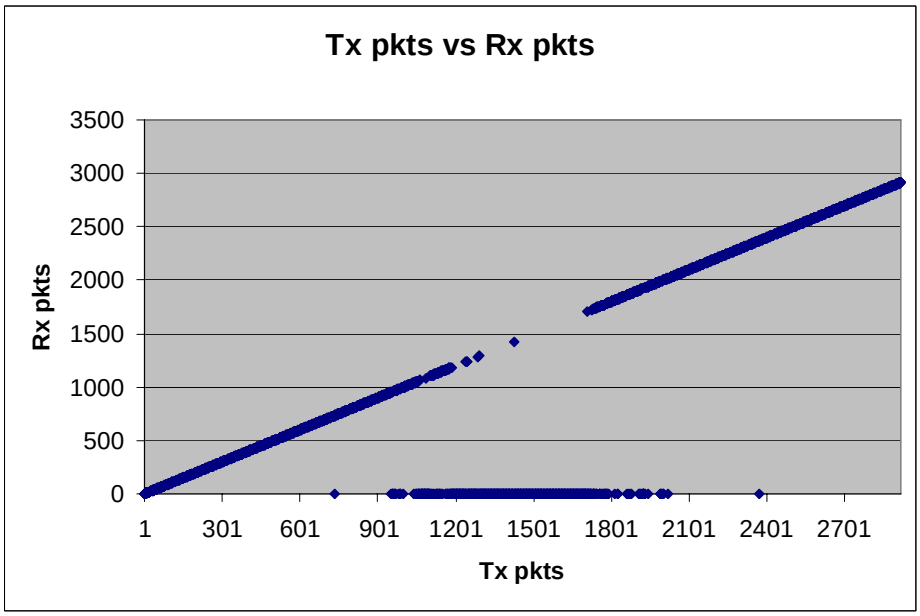


Total packets sent: 2912

Total packets dropped: 674

3.6.6.10 GM 10 5890 Receiving Vehicle Rear



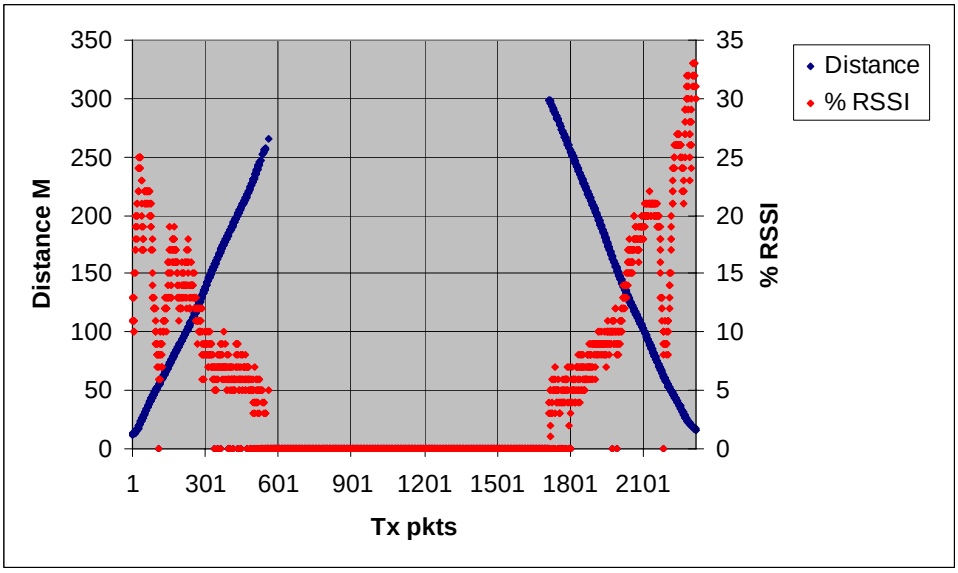


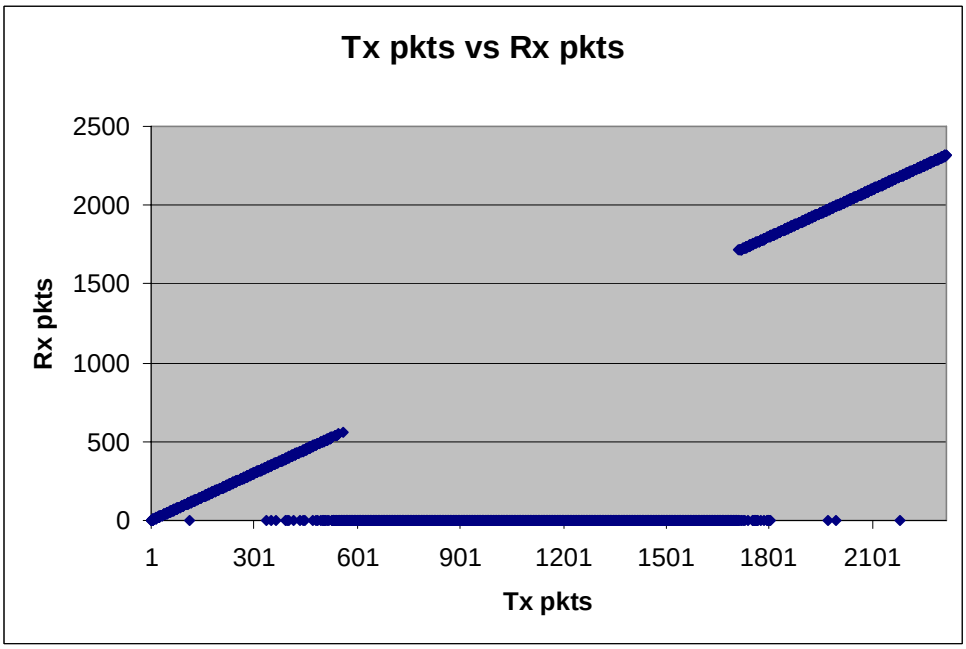
Total packets sent: 2915

Total packets dropped: 680

3.6.6.11 GM 12 5890 Receiving Vehicle Passenger-Side Broadside

Poor test kit auxiliary test port sensitivity first discovered.



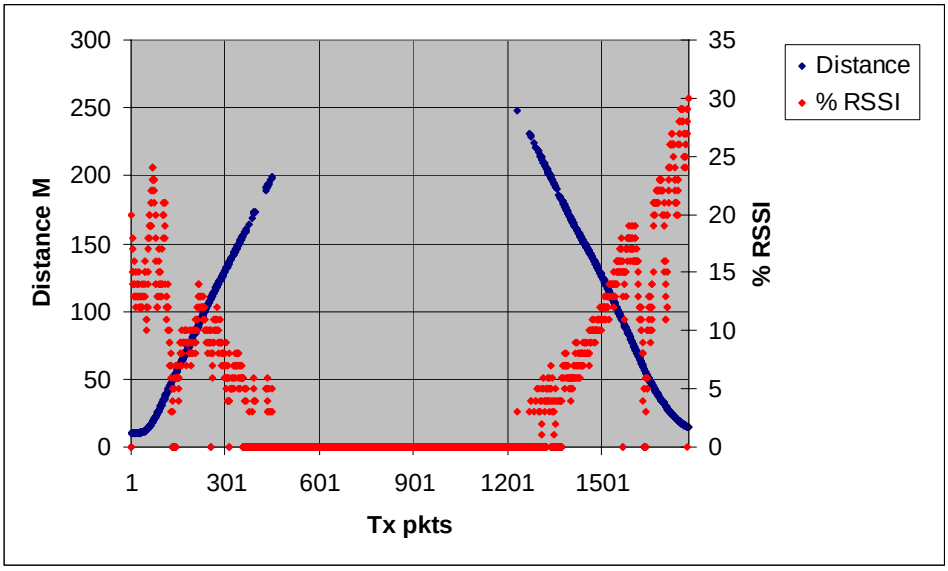


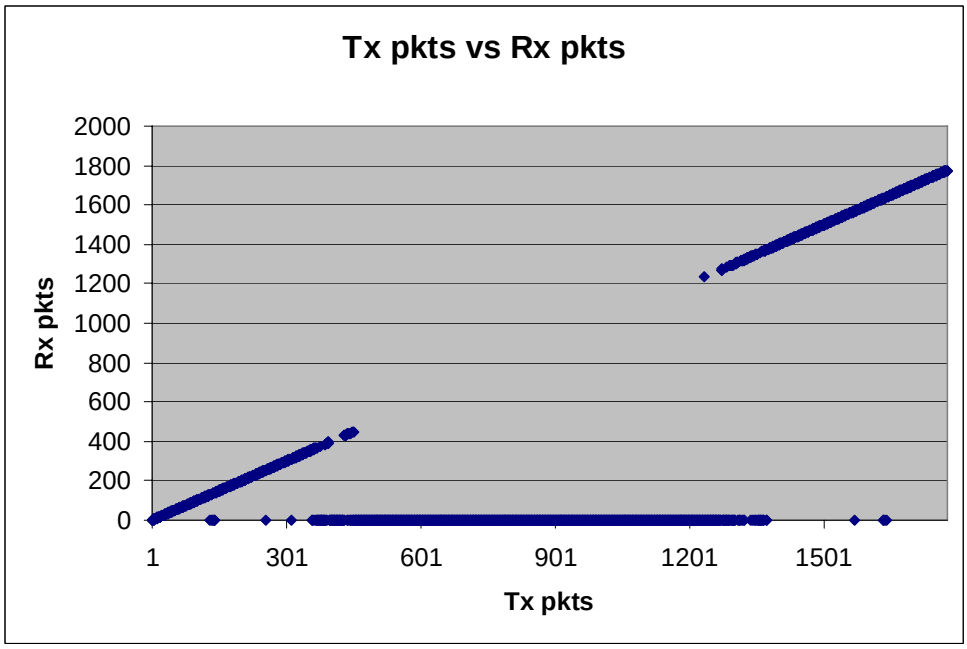
Total packets sent: 2316

Total packets dropped: 1223

3.6.6.12 GM 13 5890 Receiving Vehicle Passenger-Side Broadside

Passenger side antenna replaced with driver side antenna.



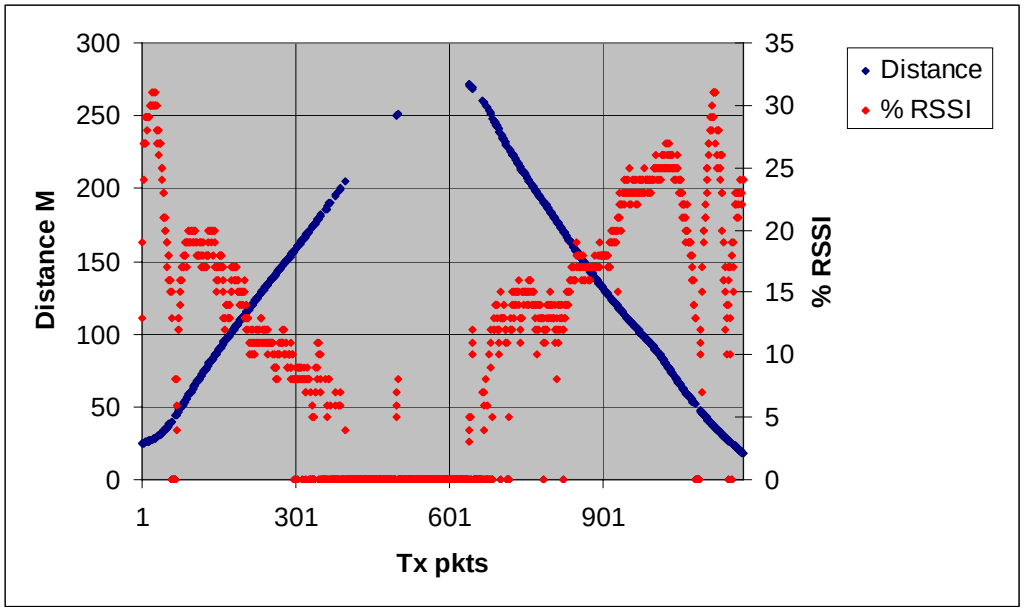


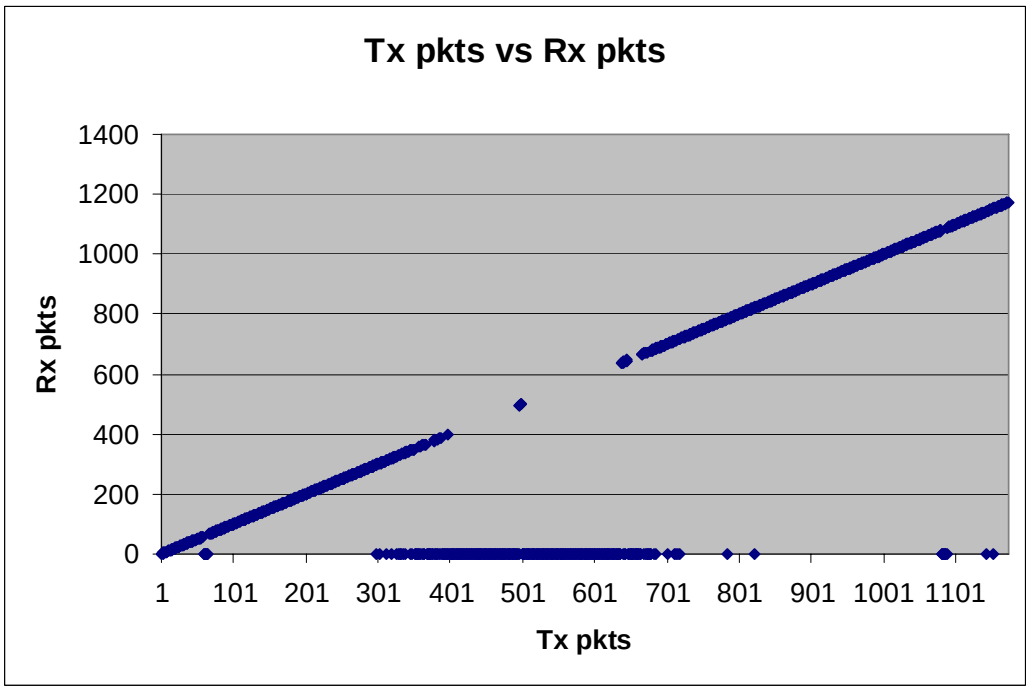
Total packets sent: 1776

Total packets dropped: 952

3.6.6.13 GM 14 5200 Receiving Vehicle Passenger-Side Broadside

Repeated GM 13 to investigate the possibility of frequency sensitivity.



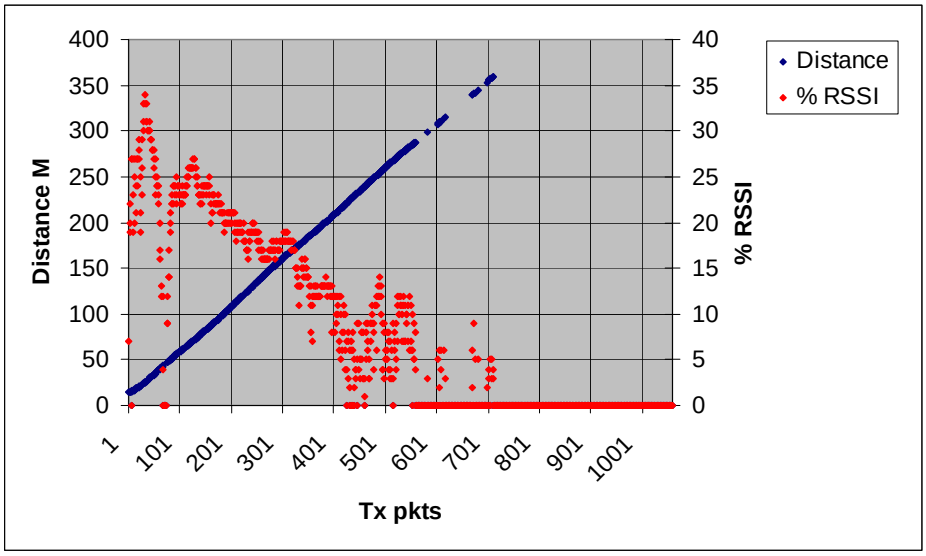


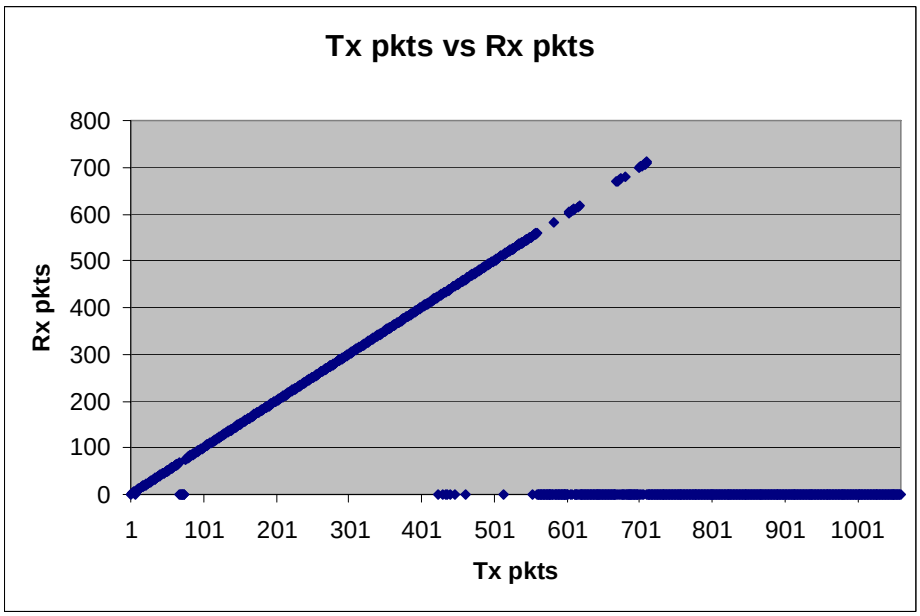
Total packets sent: 1173

Total packets dropped: 338

3.6.6.14 GM 15 5200 Receiving Vehicle Passenger-Side Broadside

All cables moved to swapped including test kit MMCX to SMA adapter using auxiliary input port.



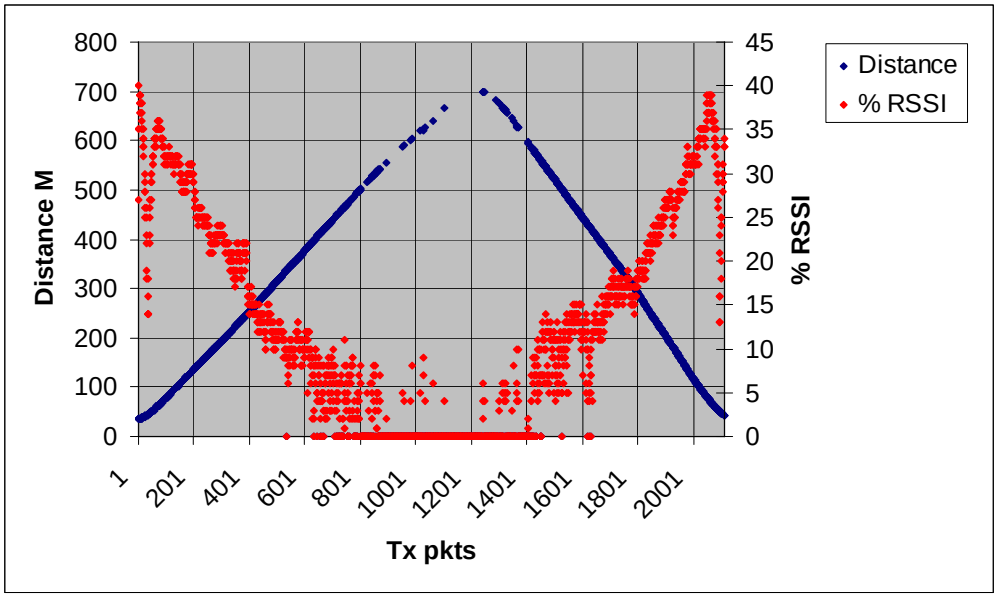


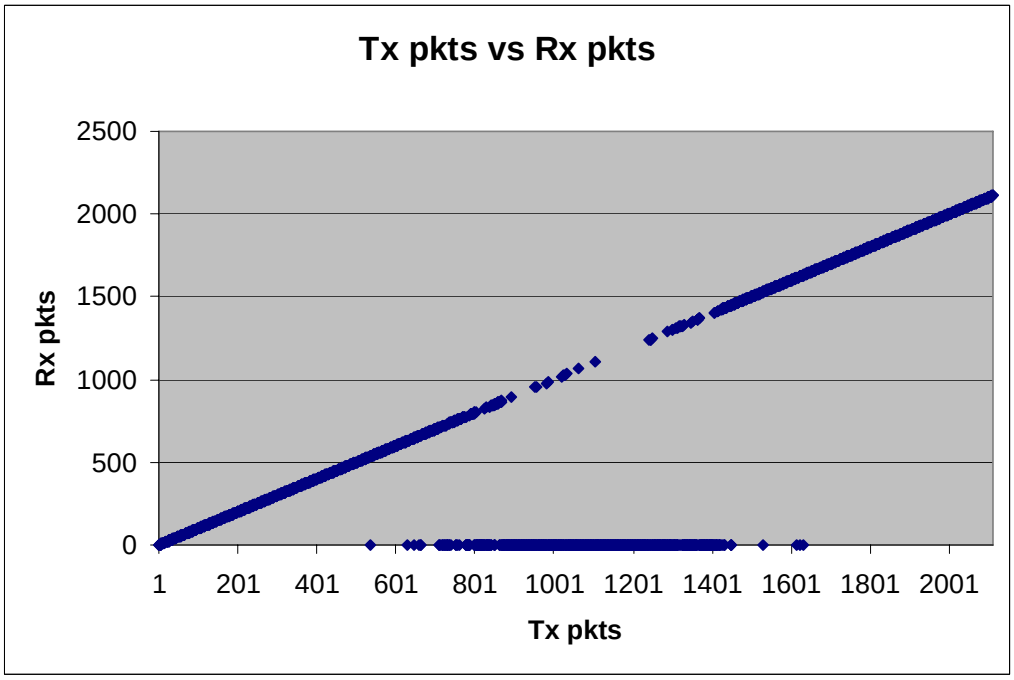
Total packets sent: 1059

Total packets dropped: 495

3.6.6.15 GM 16 5200 Receiving Vehicle Passenger-Side Broadside

Test kit cable MMCX end moved to main input port.

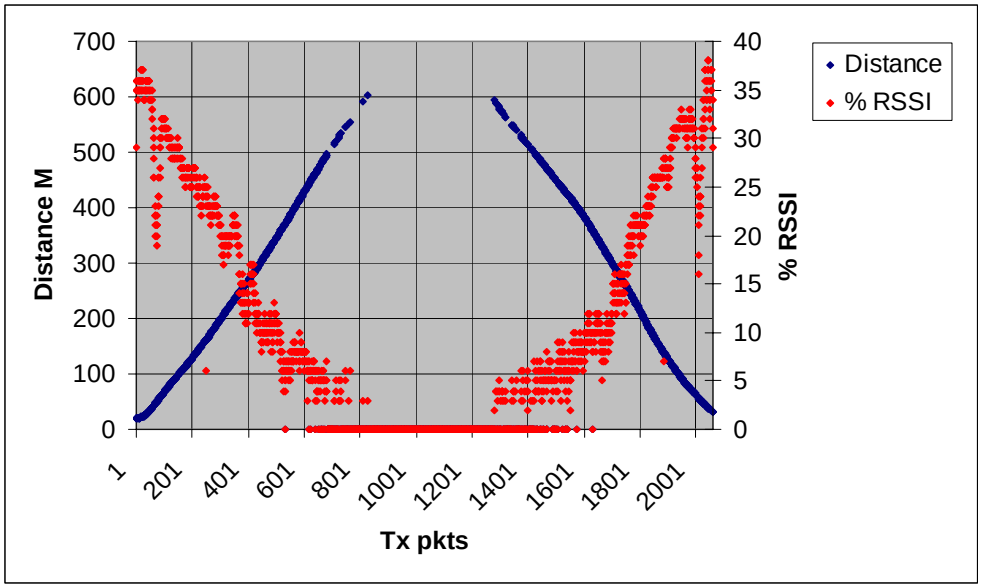


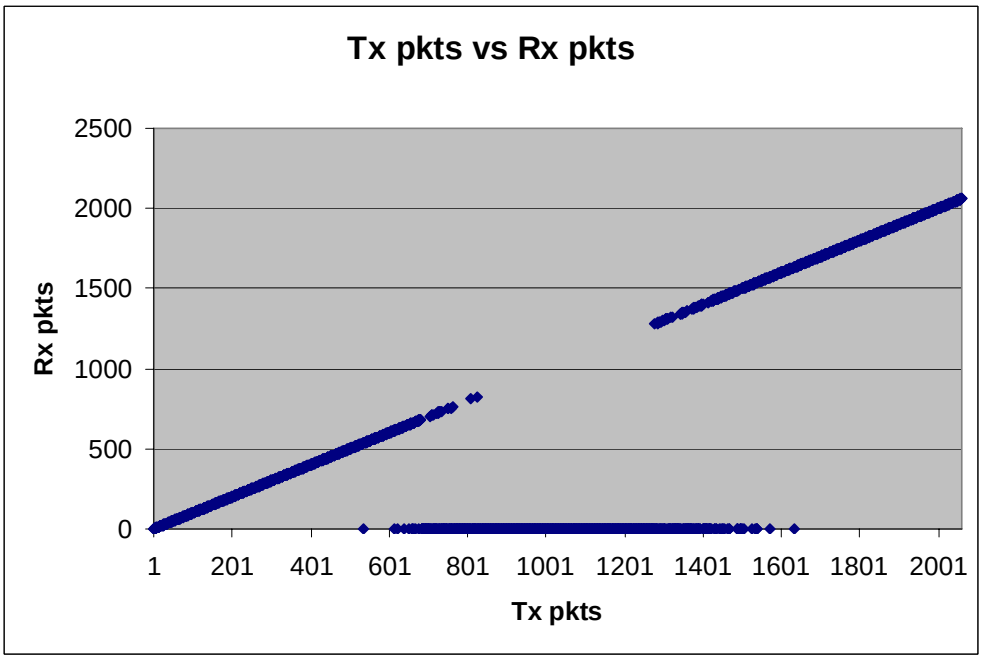


Total packets sent: 2111

Total packets dropped: 603

3.6.6.16 GM 17 5890 Receiving Vehicle Passenger-Side Broadside





Total packets sent: 2060

Total packets dropped: 720

3.6.6.17 Summary – GM Proving Ground

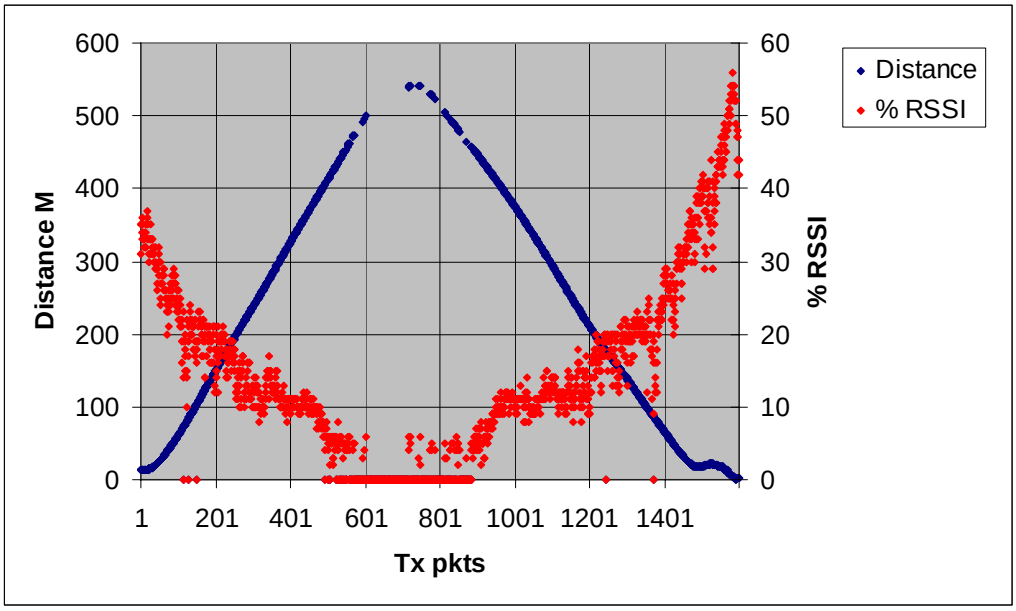
The mirror mount antenna configuration for these drive tests included only a single broadcasting antenna. Tests conducted at 5.2GHz indicate greater range than those taken at 5.89GHz. This is mainly due to the reduced transmit power of the test kits at the higher frequency as both frequencies are within the bandwidth of the antenna. Therefore, the expected performance will be similar to or better than tests conducted at 5.2GHz.

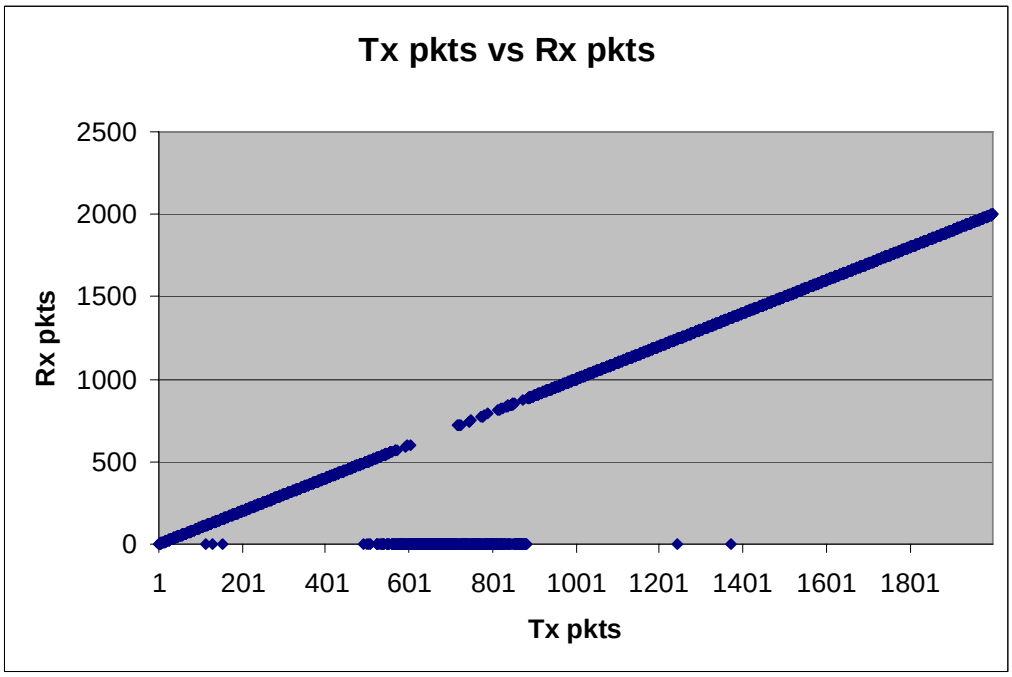
3.6.7 Test Results – Troy 5/8 Wave Roof Mount Antenna

Because the 5/8 wave roof mount antenna was not yet available for drive testing at the GM Proving Ground, these drive tests were subsequently conducted along a dead-end side street. This same street was used for preliminary testing with prototype mirror mount antennas and provides a clear unobstructed range of 550 meters. It should be noted that these particular drive tests occurred in the presence of rain.

Drive tests were conducted using a receiving vehicle with a sunroof and a transmit vehicle without a sunroof. The main antenna port of each test kit was connected to the 5/8 wave antenna pig tail with a 6-foot-long coaxial extension cable. The coaxial extension cable is made of LMR-195 coaxial cable and has a measured 2dB insertion loss at 5.888GHz. The 5/8 wave antenna was located on the receiving vehicle roof 7.5 inches rearward of the sunroof rear edge along the vehicle front-to-back center line. The transmit vehicle 5/8 wave antenna was located at the roof center.

3.6.7.1 SS2 5890 Receiving Vehicle Front

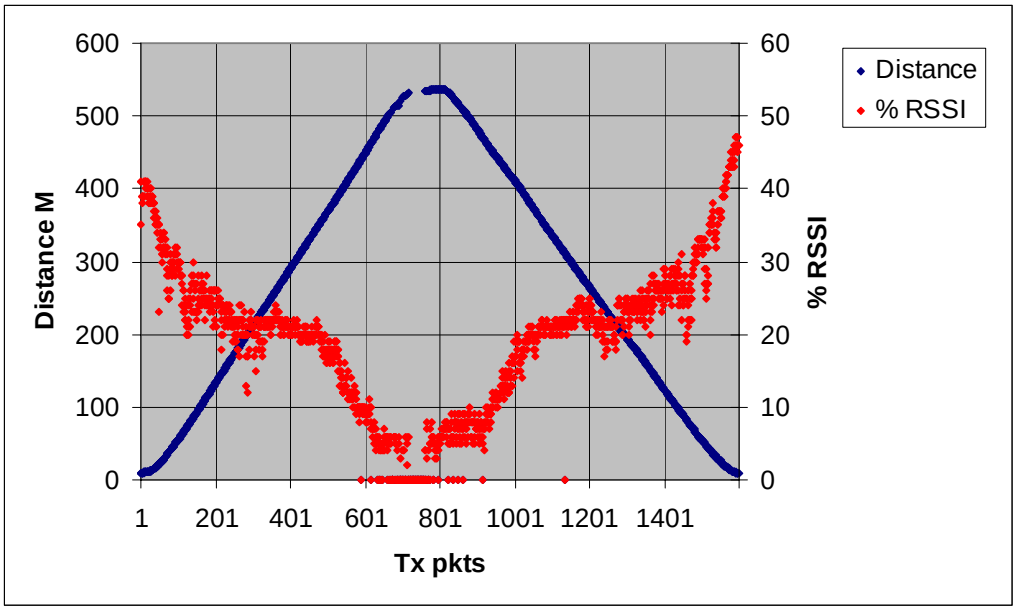


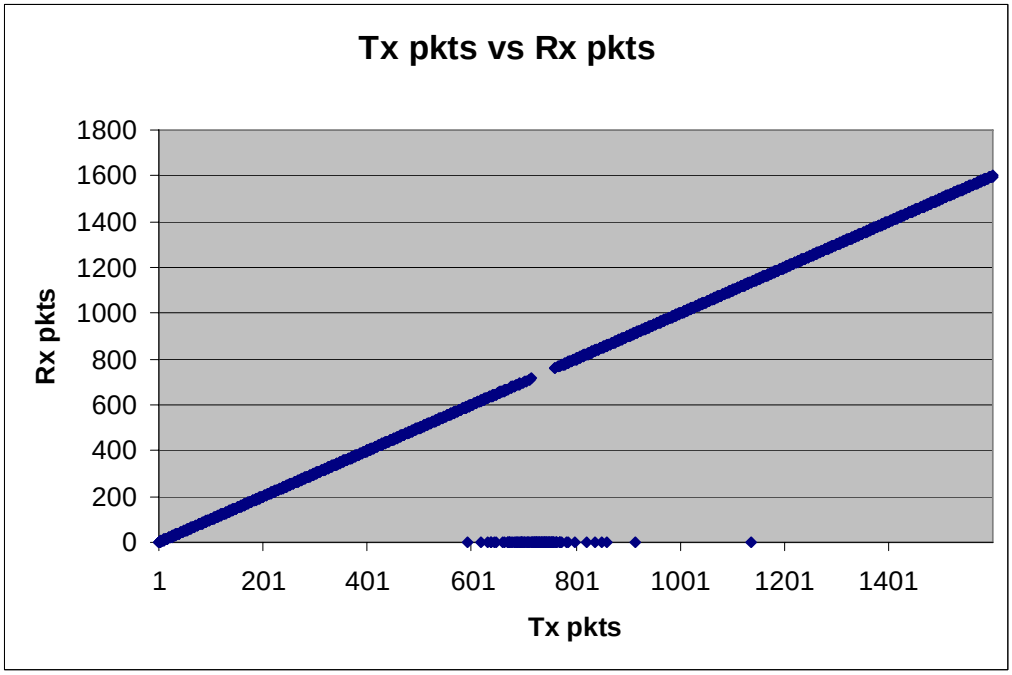


Total packets sent: 1999

Total packets dropped: 314

3.6.7.2 SS3 5890 Receiving Vehicle Rear





Total packets sent: 1599

Total packets dropped: 96

3.6.7.3 Propagation Model

Because the 5/8 wave antenna is not resonant in the WLAN band where the test kits have increased transmit power, the expected range cannot be directly measured. However the expected range can be modeled using the 5.8875GHz radiation pattern, Figure 54, 2dB extension cable loss, and height information of the vehicle with sunroof. The measured gain in Figure 54 at 0° is –4dBil corresponding to the receiving vehicle front configuration, and at 180° is 0dBil corresponding to the receiving vehicle rear configuration.

For the receiving vehicle front case, the propagation model results were computed at SS2 range points to facilitate an overlay comparison shown in Figure 61. Because the receiving and transmitting antenna gain and cable loss are known quantities, to correlate with the model, the transmit power at the time of these drive tests was approximately 50mW.

	tx	rx	
	Vehicle 1	Vehicle 2	
Ant gain	-4	1	dBil
El HPBW	10	10	°
tilt	0	0	° ± up/dn
height	1.4	1.4	M
Cable loss	2.00	2.00	dB
TX power	50.00		mW

Range	5	600	M
Frequency	5.89	GHz	
MDS	-86	dB	

Ground permittivity		
ε'	1	
ε"	-1.50E+01	
Brewster	45	deg
Range	2.8	M

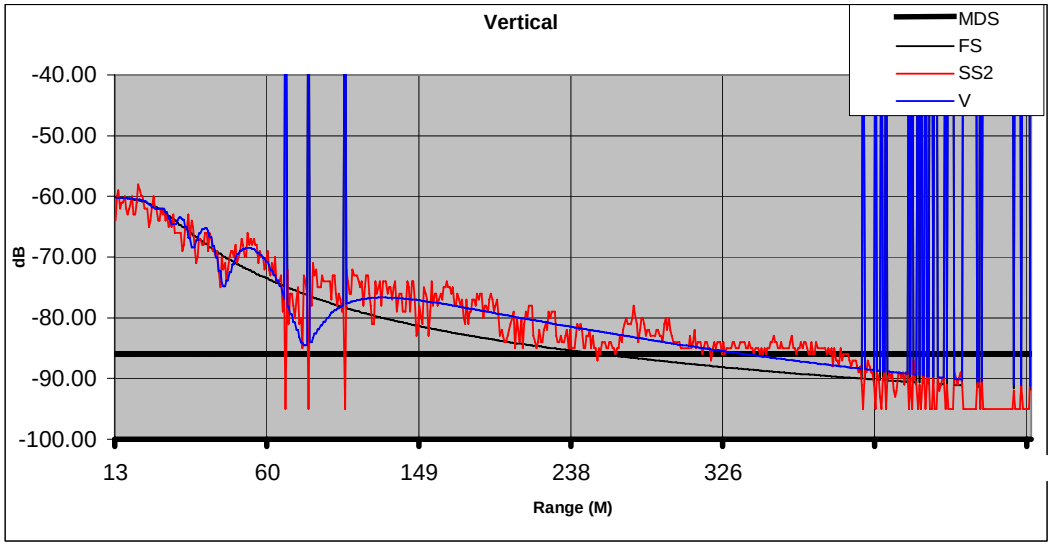


Figure 3-AA. Comparison of Propagation Model and SS2 Data

Similarly for the receiving vehicle rear configuration using 0dBil antenna gain, the model and measured, SS3 data, comparison is shown in Figure 62.

	tx	rx	
	Vehicle 1	Vehicle 2	
Ant gain	0	1	dBil
El HPBW	10	10	°
tilt	0	0	° ± up/dn
height	1.4	1.4	M
Cable loss	2.00	2.00	dB
TX power	50.00		mW

Range	5	600	M
Frequency	5.89	GHz	
MDS	-86	dB	

Ground permittivity		
ε'	1	
ε''	-1.50E+01	
Brewster	45	deg
Range	2.8	M

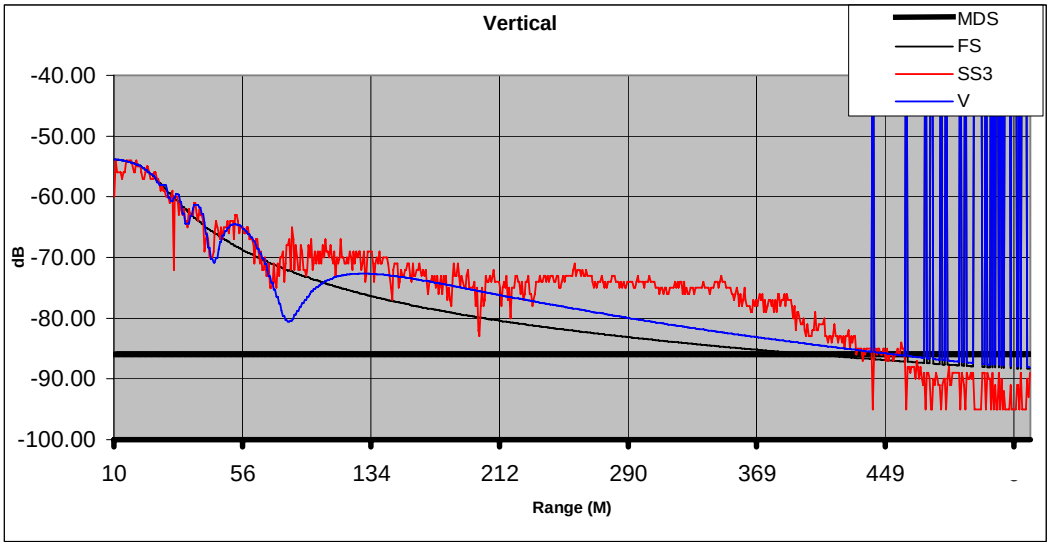


Figure 3-BB. Comparison of Propagation Model and SS3 Data

The modeled and measured data show good correlation with the 50mW transmit power approximation. Using this model and increasing the transmit power to 100mW for each case yields an approximate range of 424 meters for SS2 and 569 meters for SS3 shown in Figures 63 and 64 respectively. The modeled range predictions are considered conservative as the model assumes no packets can be received for signal levels below –86dBm at the receiver.

	tx	rx	
	Vehicle 1	Vehicle 2	
Ant gain	-4	1	dBil
El HPBW	10	10	°
tilt	0	0	° ± up/dn
height	1.4	1.4	M
Cable loss	2.00	2.00	dB
TX power	100.00		mW

Range	10	700	M
Frequency	5.89	GHz	
MDS	-86	dB	

424.69 M

Ground permittivity		
ε'	1	
ε"	-1.50E+01	
Brewster	45	deg
Range	2.8	M

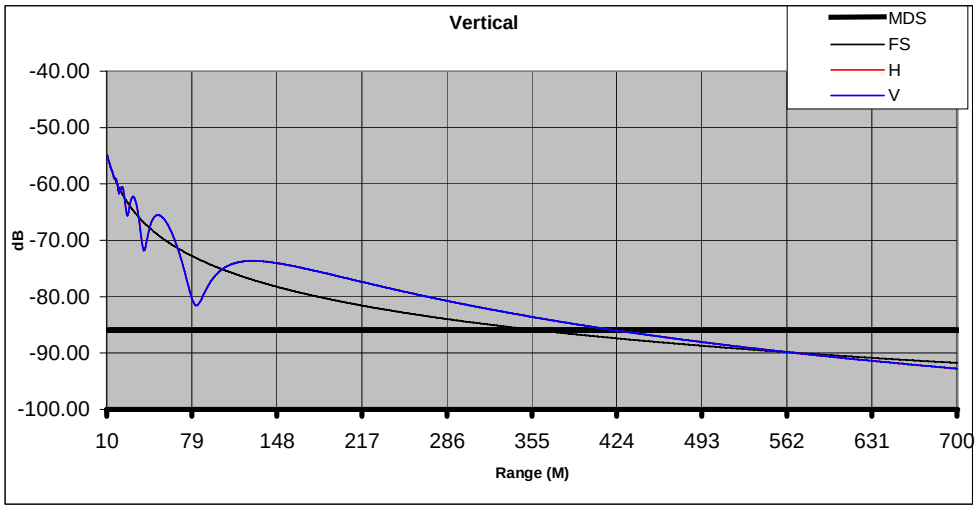


Figure 3-CC. Approximate Range for Receiving Vehicle Front With Sunroof

	tx	rx	
	Vehicle 1	Vehicle 2	
Ant gain	0	1	dBil
El HPBW	10	10	°
tilt	0	0	° ± up/dn
height	1.4	1.4	M
Cable loss	2.00	2.00	dB
TX power	100.00		mW

Range	10	700	M
Frequency	5.89	GHz	
MDS	-86	dB	

569.59 M

Ground permittivity		
ε'	1	
ε"	-1.50E+01	
Brewster	45	deg
Range	2.8	M

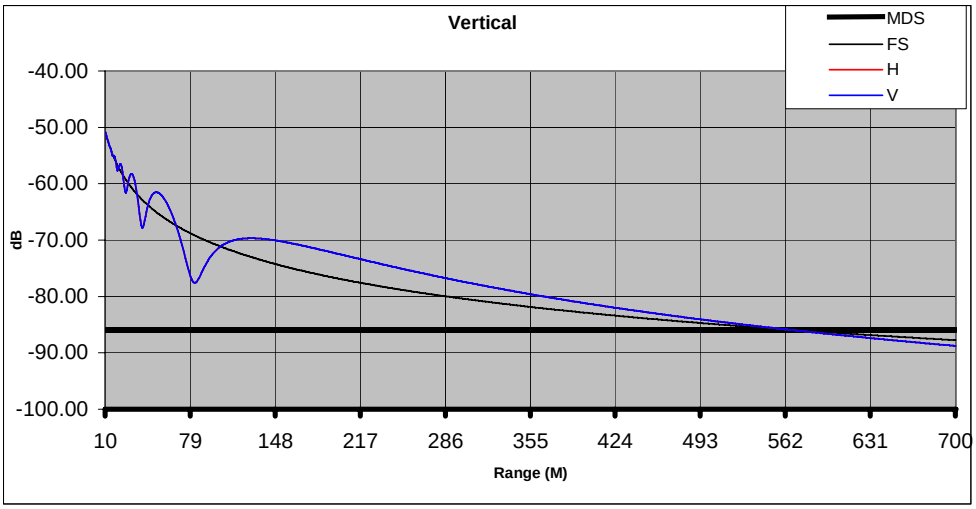


Figure 3-DD. Approximate Range for Receiving Vehicle Rear With Sunroof

3.6.7.4 Summary – Side Street Drive Tests

Both the vehicle radiation patterns measured at JEF and this drive testing show the effects of a sunroof on the effective communications range. While data packets were received at ranges beyond 500 meters with less than 100mW of transmit power, more packets were received in the rearward direction of the vehicle than in the forward direction as a consequence of the sunroof.

3.6.8 Summary – Drive Tests

Through extensive drive testing, the mirror mount antennas have shown to consistently provide good vehicle communications over both WLAN and ITS DSRC bands to at least 500 meters ±90° broadside of the vehicle.

The 5/8 roof mount antenna performance can be influenced by vehicle roof surface features such as a sunroof. However for recommended roof locations, the 5/8 wave antenna also meets design and performance goals.

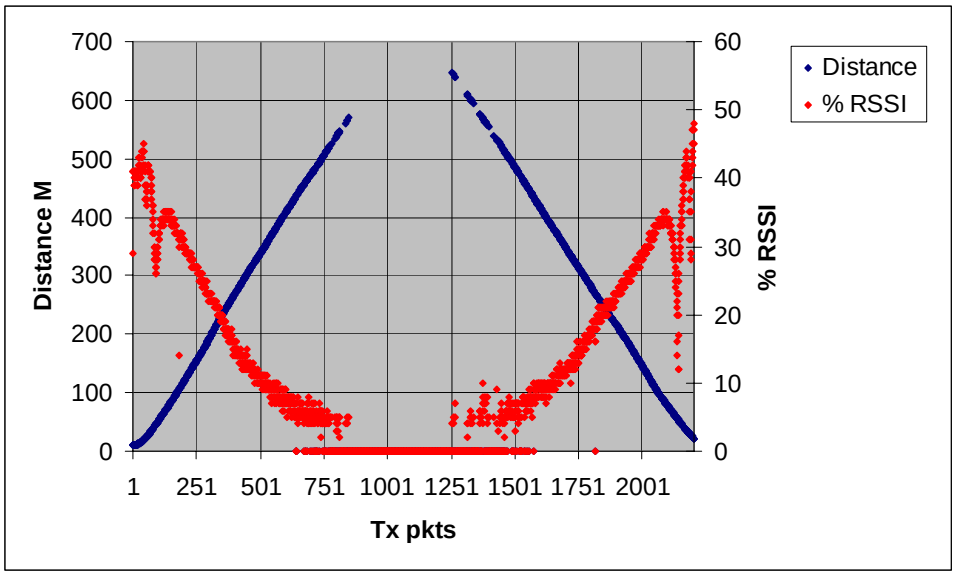
3.7 Summary

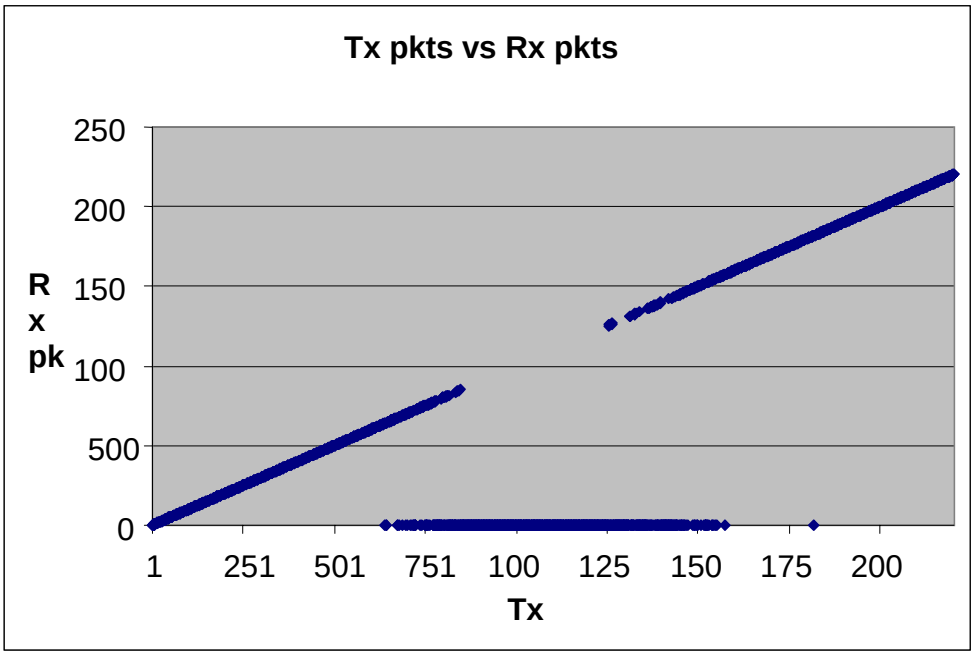
Two antennas have been designed, built, and tested both at component level and vehicle level. The results show that both antennas perform as designed and meet all goals of the design specification. Because the performance of each antenna can be influenced by vehicle type, the results reported here are typical for sedan type vehicles.

3.7.1 Test Results – Mirror Mount Ford Proving Ground

Drive testing of the mirror mount antenna was conducted at the Ford Proving Ground in Dearborn, MI. The initial tests resulted in poor range performance due to a problem with the coaxial extension cables which connect the test kit to the antenna pigtail. Subsequently, the test kits were connected directly to the antenna pigtail in each vehicle.

3.7.1.1 Ford 12 5890 Receiving Vehicle Front

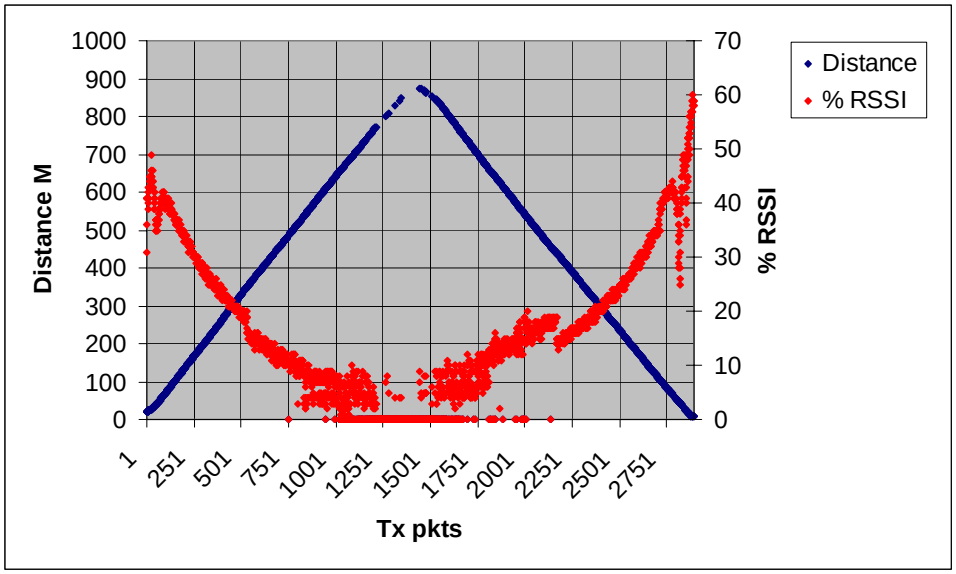


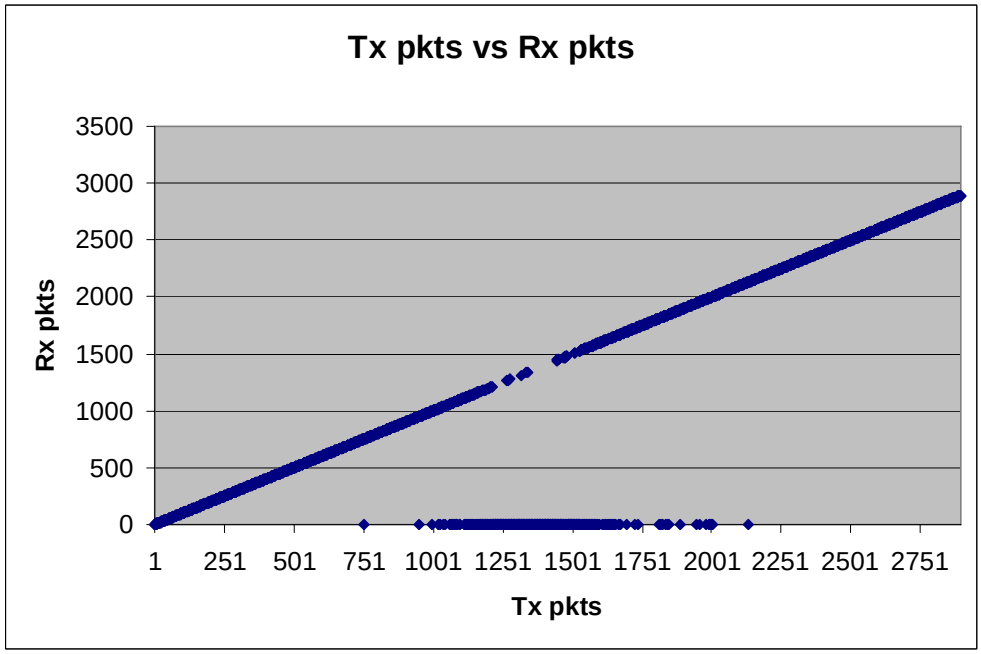


Total packets sent: 2203

Total packets dropped: 676

3.7.1.2 Ford 13 5300 Receiving Vehicle Front



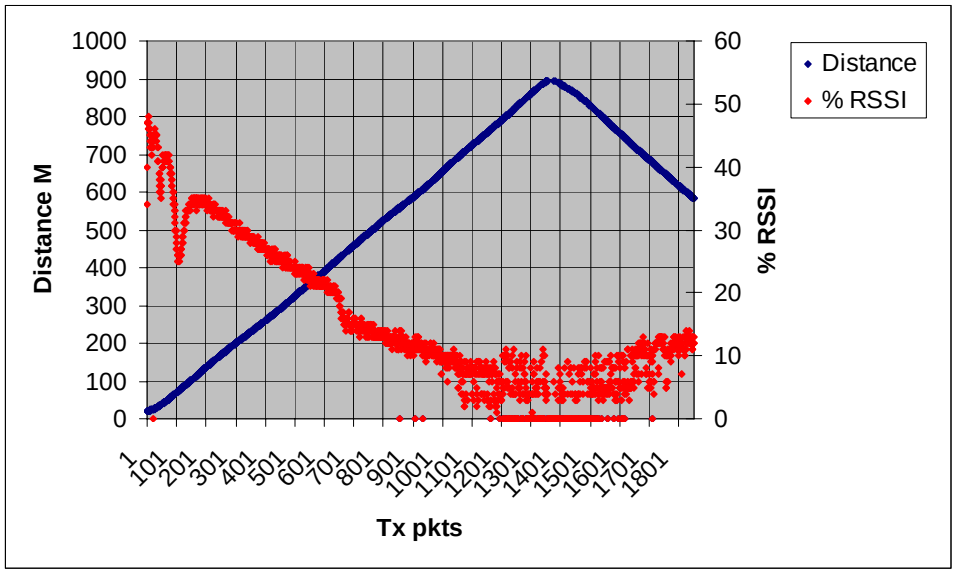


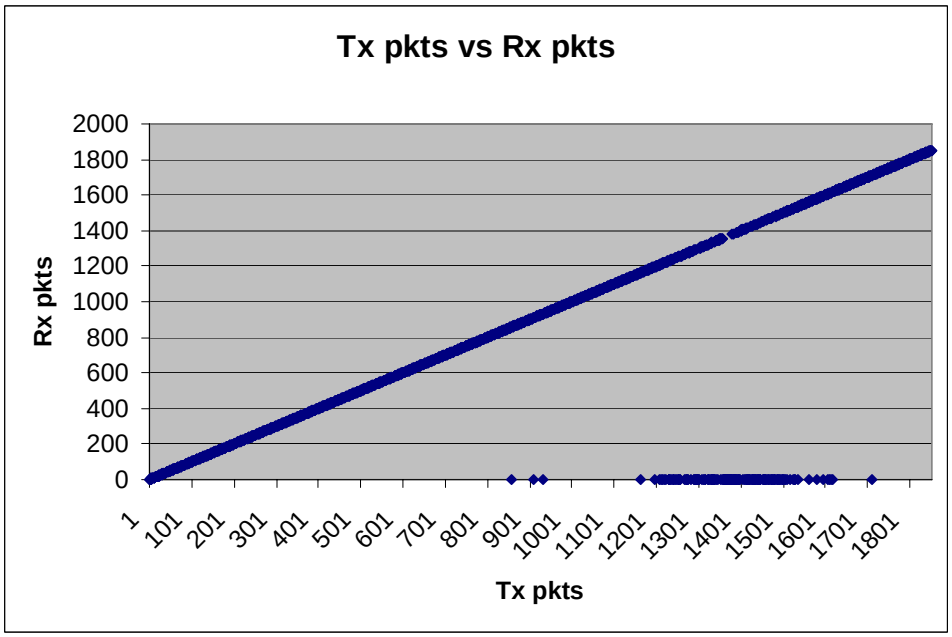
Total packets sent: 2894

Total packets dropped: 444

3.7.1.3 Ford 9 5300 Receiving Vehicle Broadside

This test is using the 4-element array antenna on loan from CAMP on both vehicles to ensure proper test kit operation.

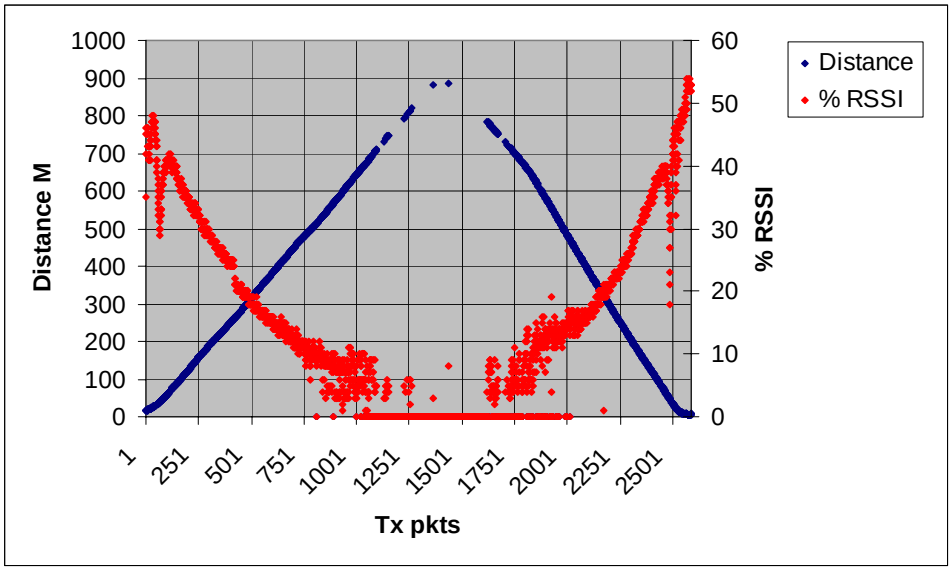


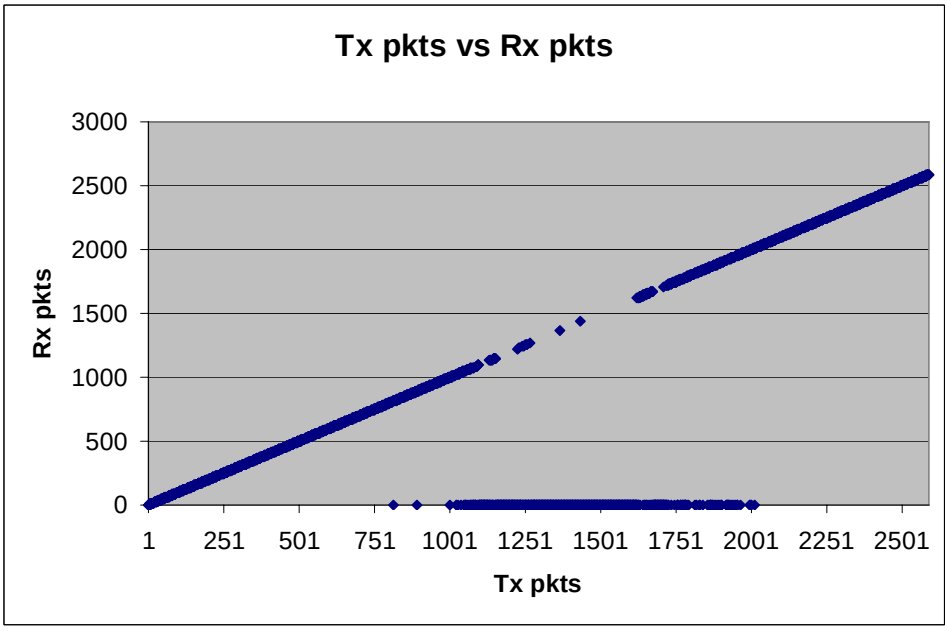


Total packets sent: 1852

Total packets dropped: 164

3.7.1.4 Ford 10 5300 Receiving Vehicle Broadside

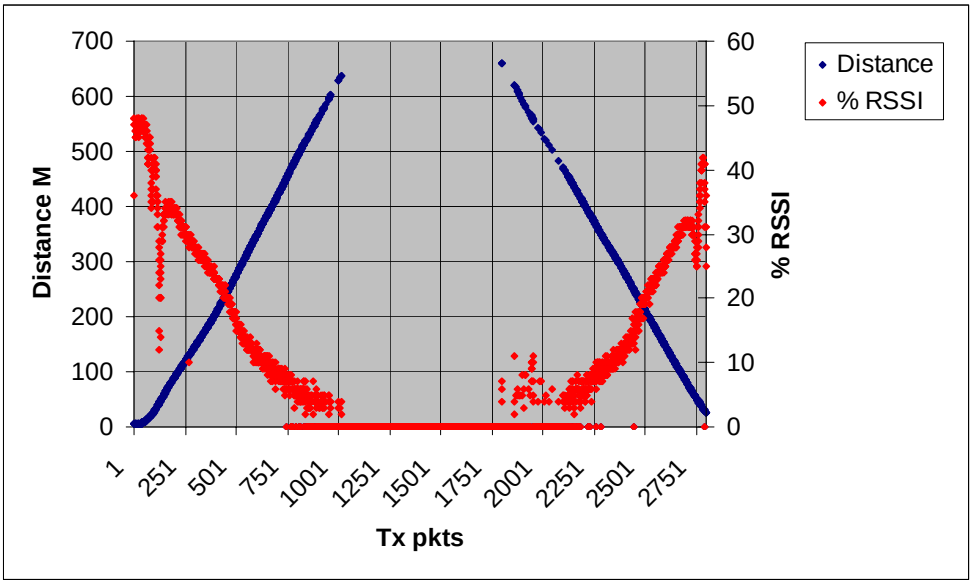


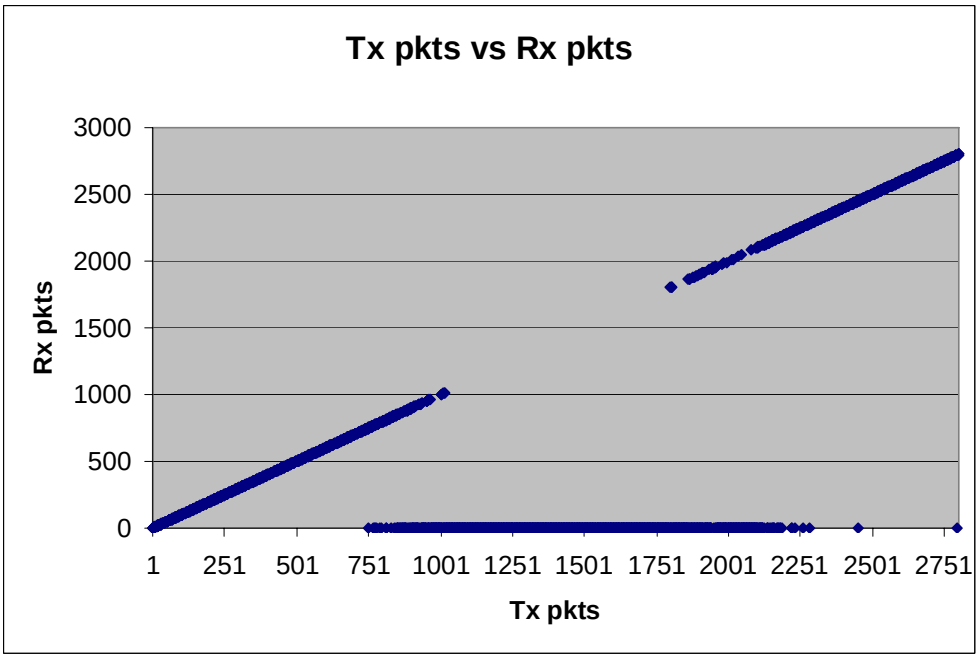


Total packets sent: 2588

Total packets dropped: 645

3.7.1.5 Ford 11 5890 Receiving Vehicle Broadside

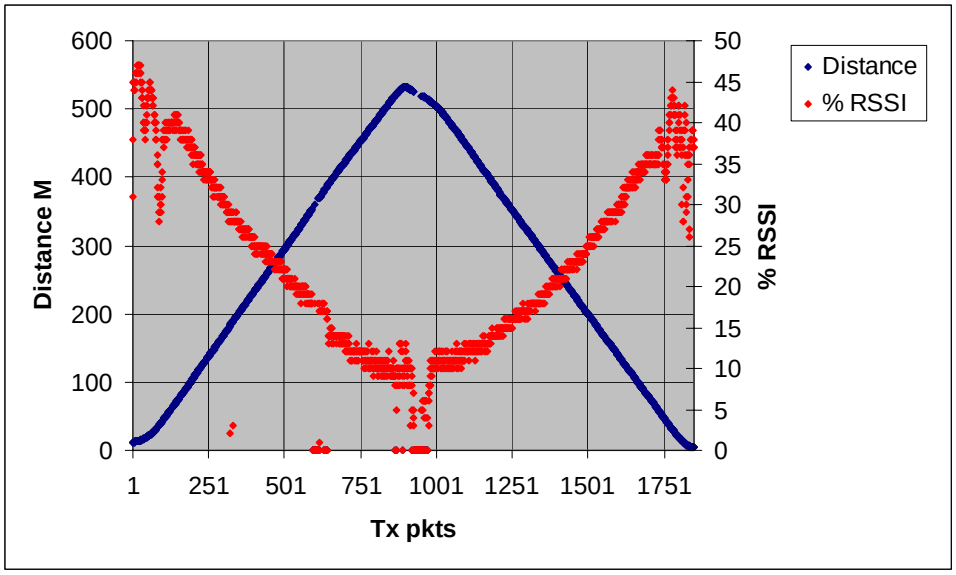


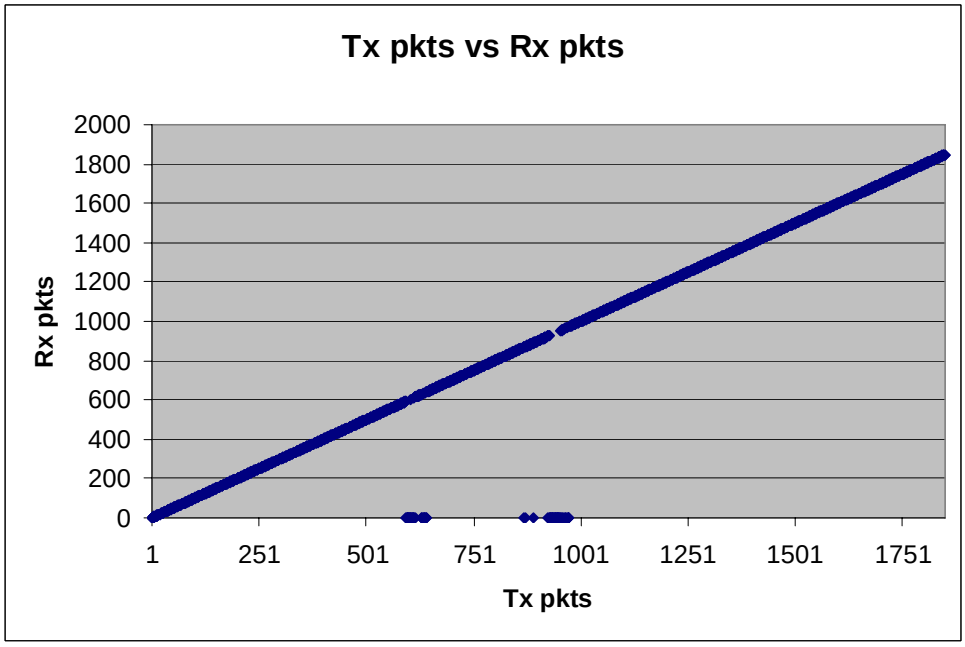


Total packets sent: 2800

Total packets dropped: 209

3.7.1.6 Ford 14 5300 Receiving Vehicle Rear

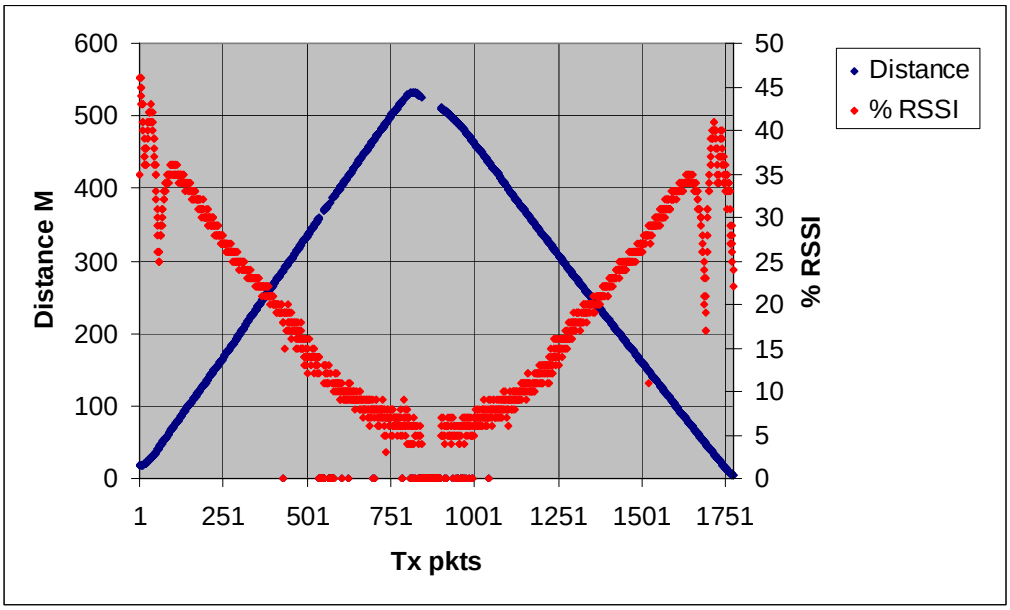


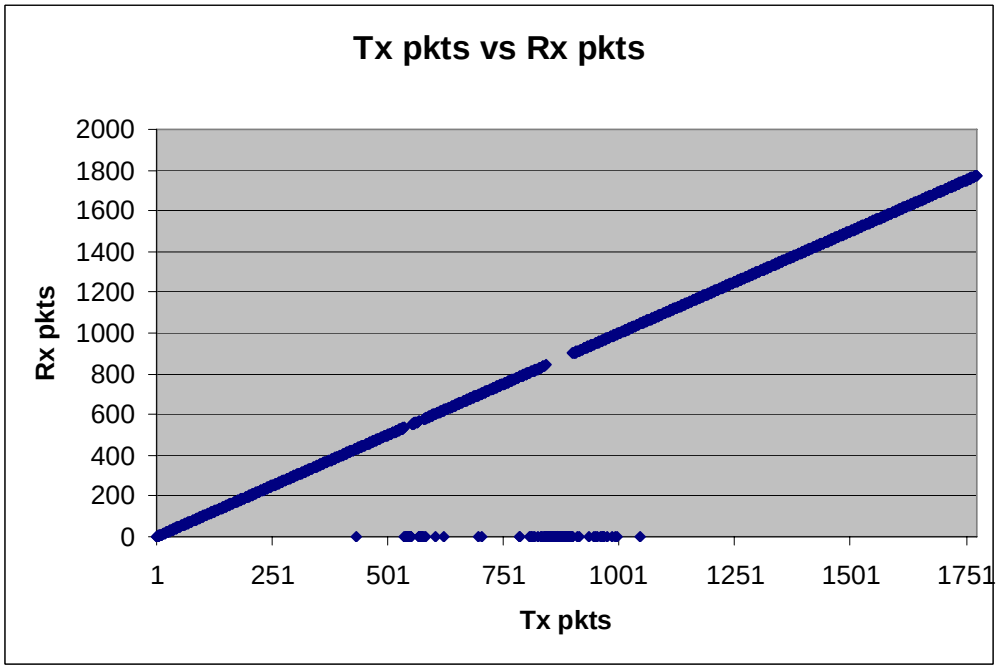


Total packets sent: 1849

Total packets dropped: 69

3.7.1.7 Ford 15 5890 Receiving Vehicle Rear

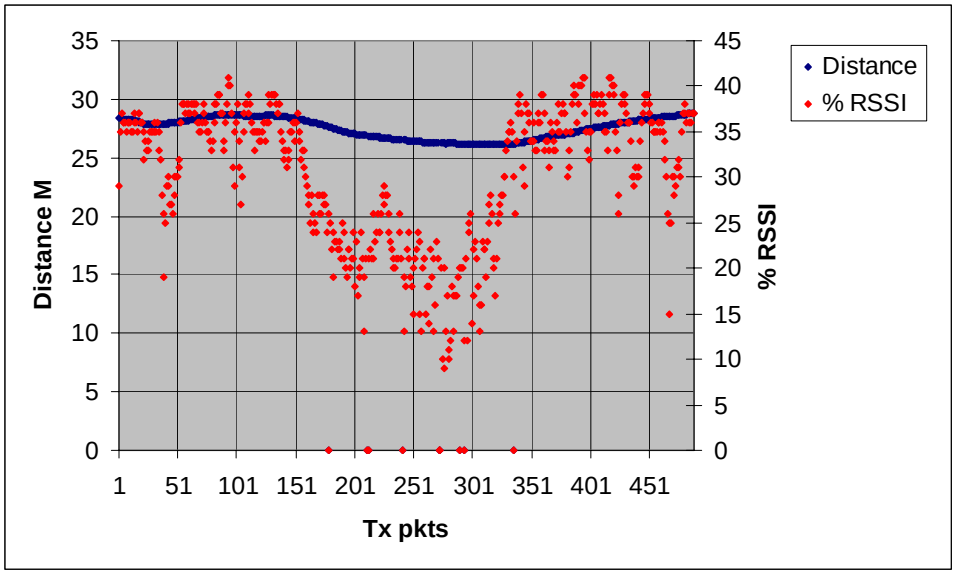


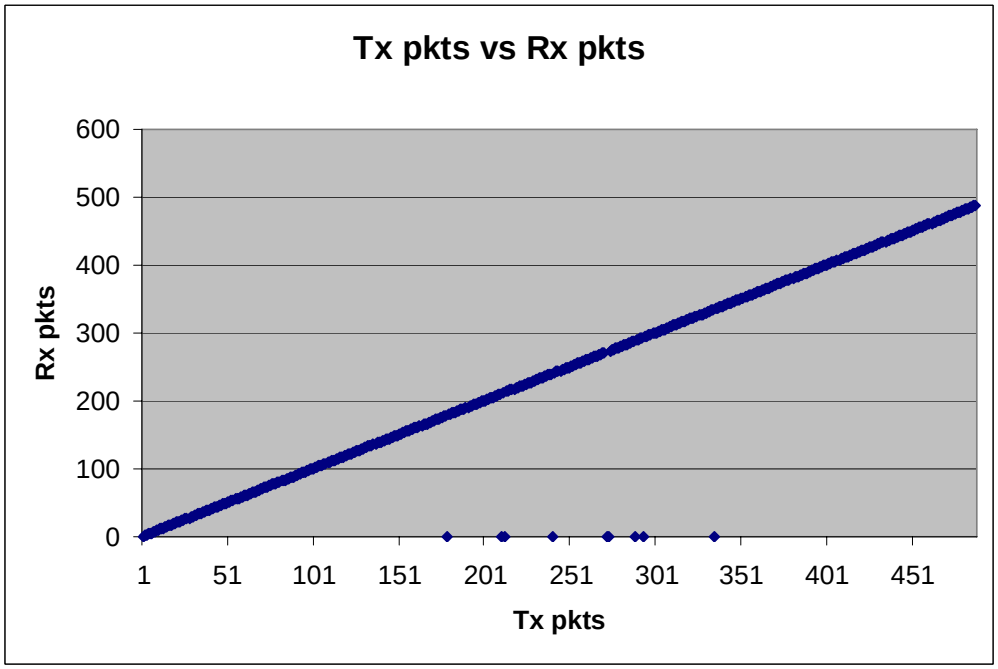


Total packets sent: 1773

Total packets dropped: 119

3.7.1.8 Ford 16 5890 Clockwise Circular Passenger-Side Antenna

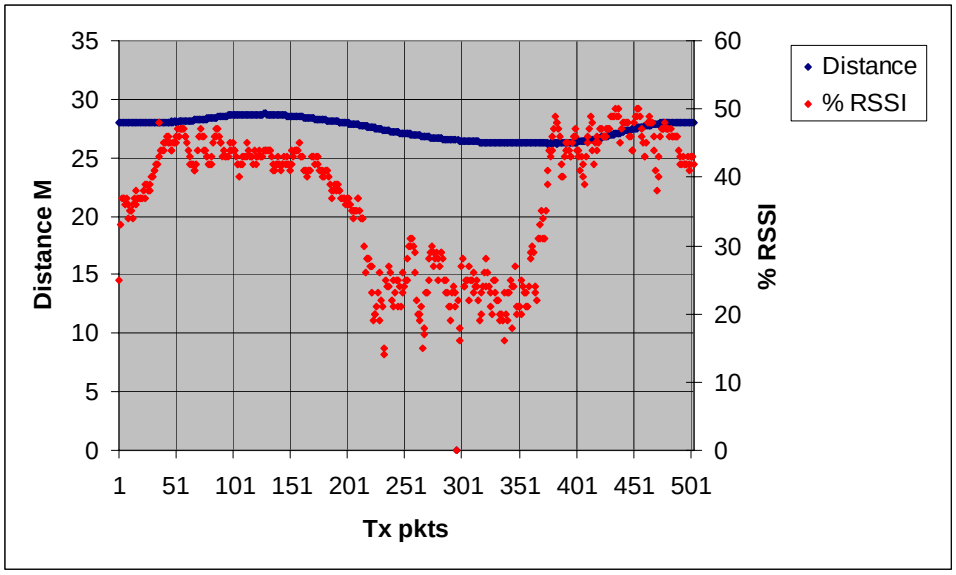


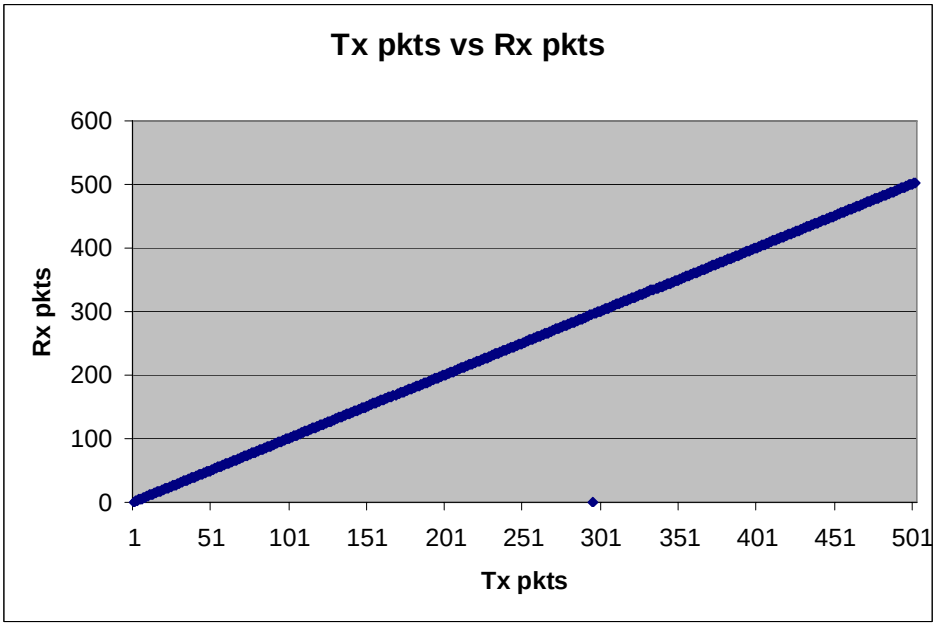


Total packets sent: 488

Total packets dropped: 9

3.7.1.9 Ford 17 5300 Clockwise Circular Passenger-Side Antenna

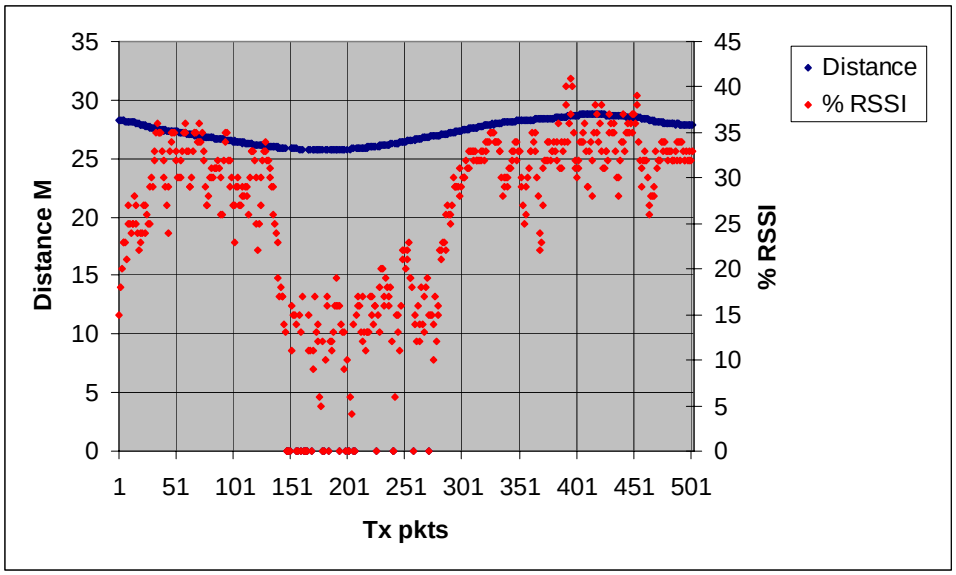


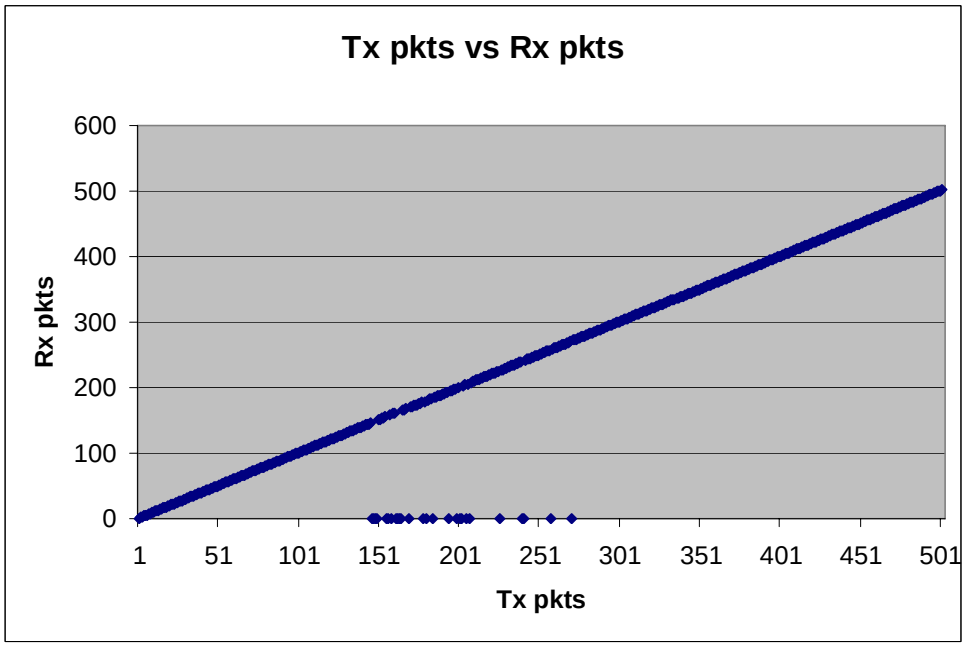


Total packets sent: 503

Total packets dropped: 1

3.7.1.10 Ford 18 5300 Counter-Clockwise Circular Passenger-Side Antenna

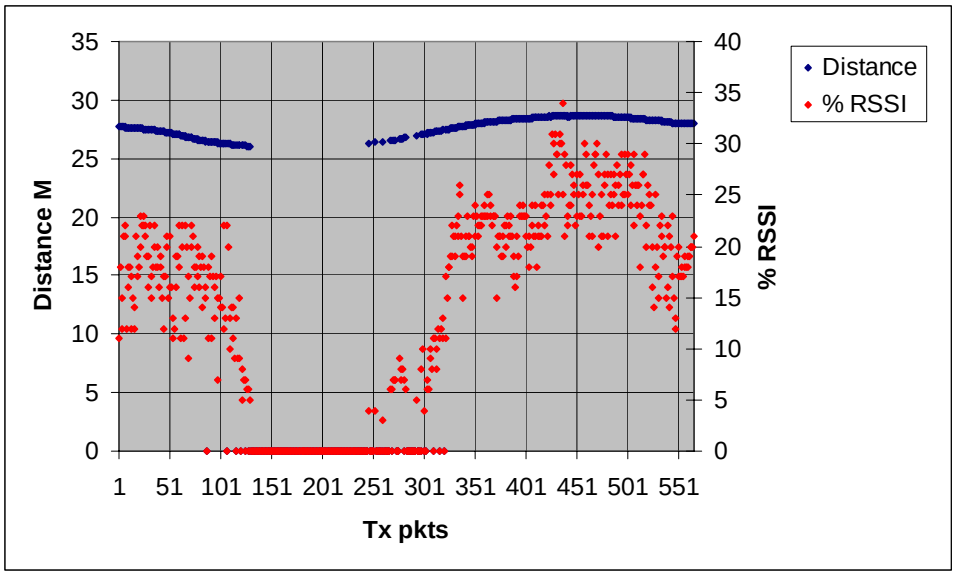


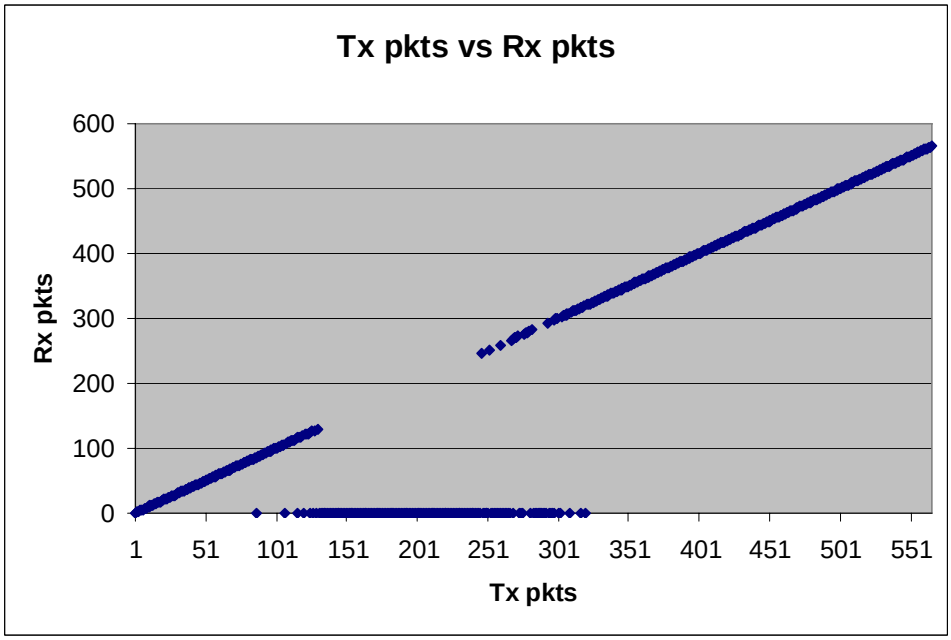


Total packets sent: 502

Total packets dropped: 26

3.7.1.11 Ford 19 5890 Counter-Clockwise Circular Passenger-Side Antenna

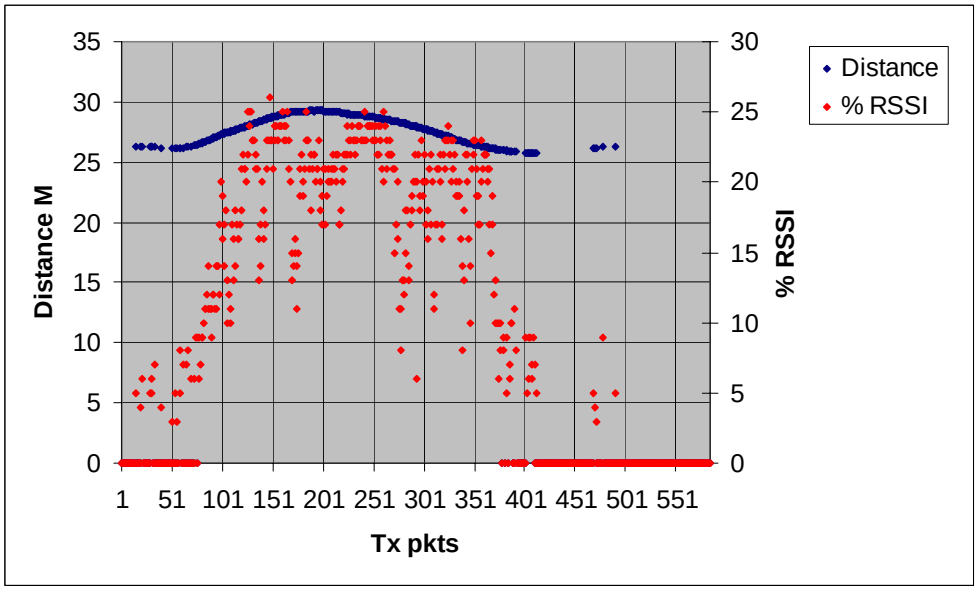


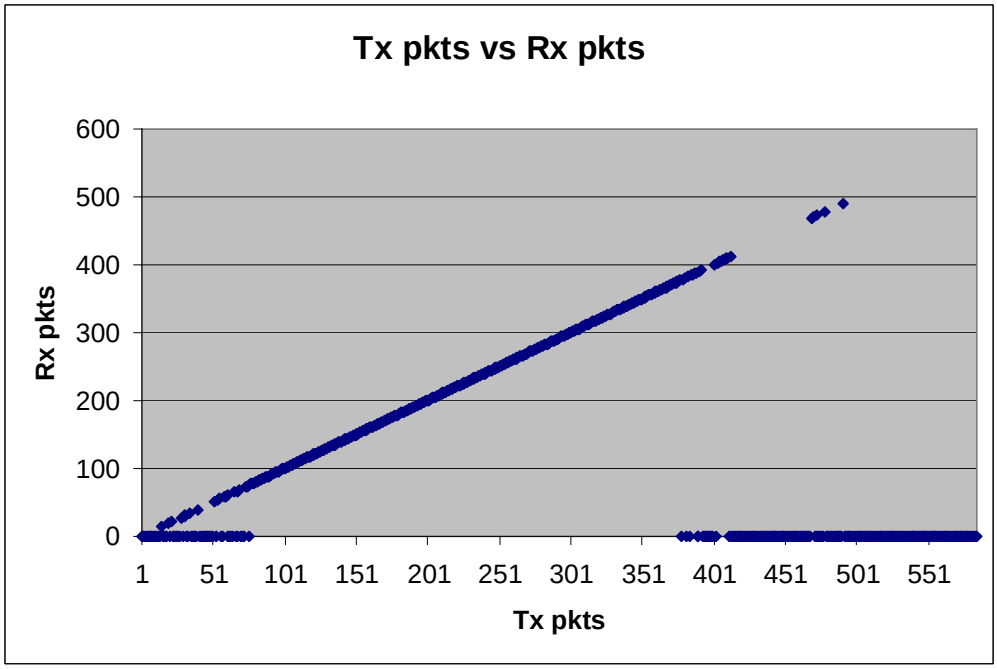


Total packets sent: 565

Total packets dropped: 164

3.7.1.12 Ford 20 5890 Clockwise Circular Driver-Side Antenna

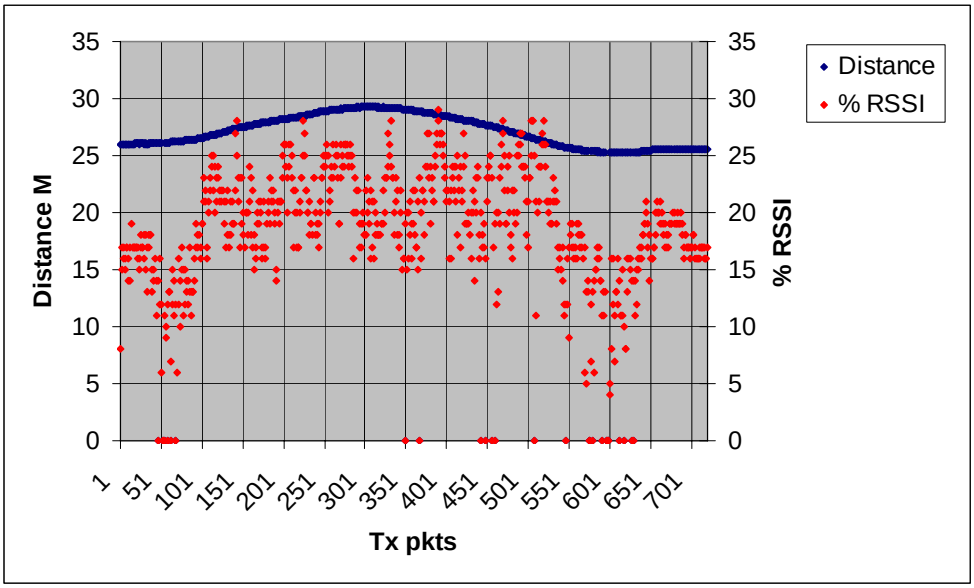


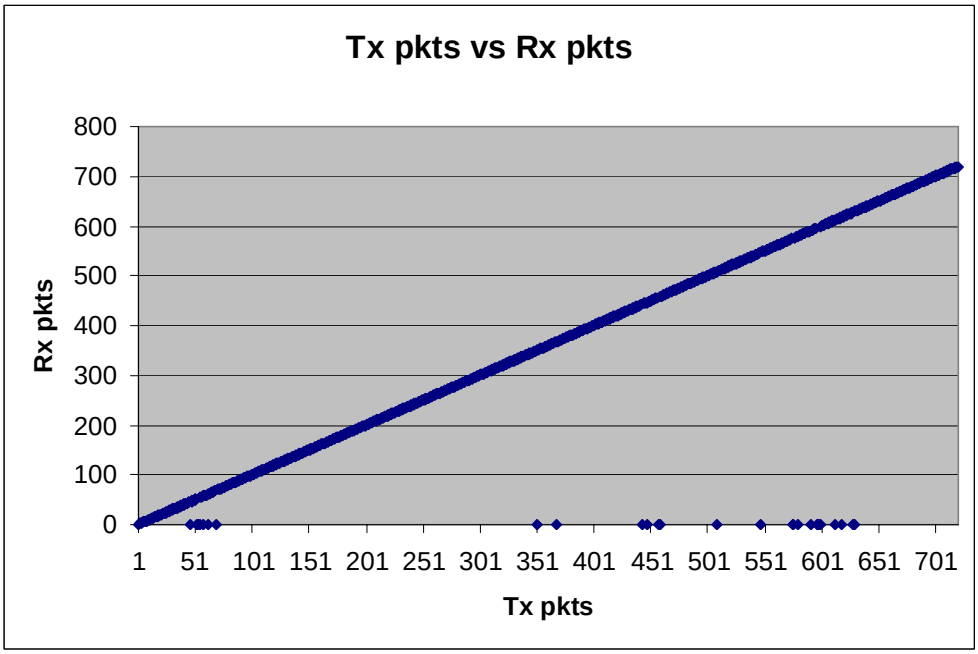


Total packets sent: 584

Total packets dropped: 238

3.7.1.13 Ford 21 5300 Clockwise Circular Driver-Side Antenna

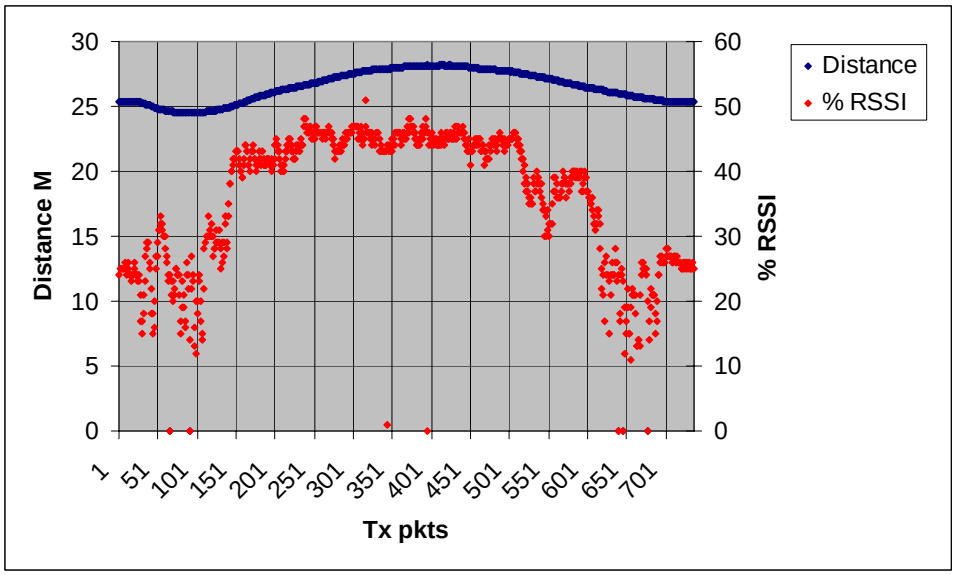


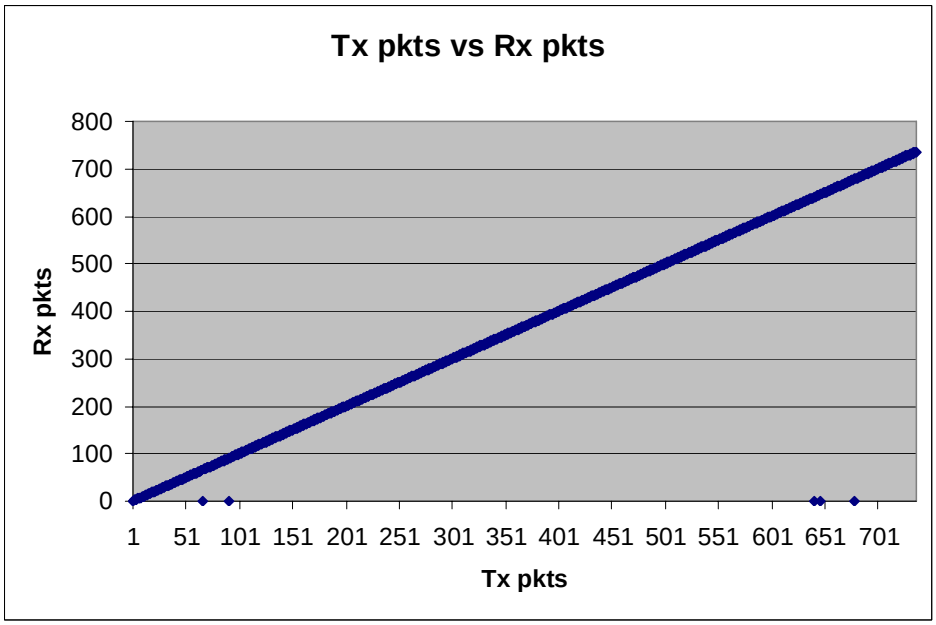


Total packets sent: 720

Total packets dropped: 27

3.7.1.14 Ford 22 5300 Counter-Clockwise Circular Passenger-Side Antenna

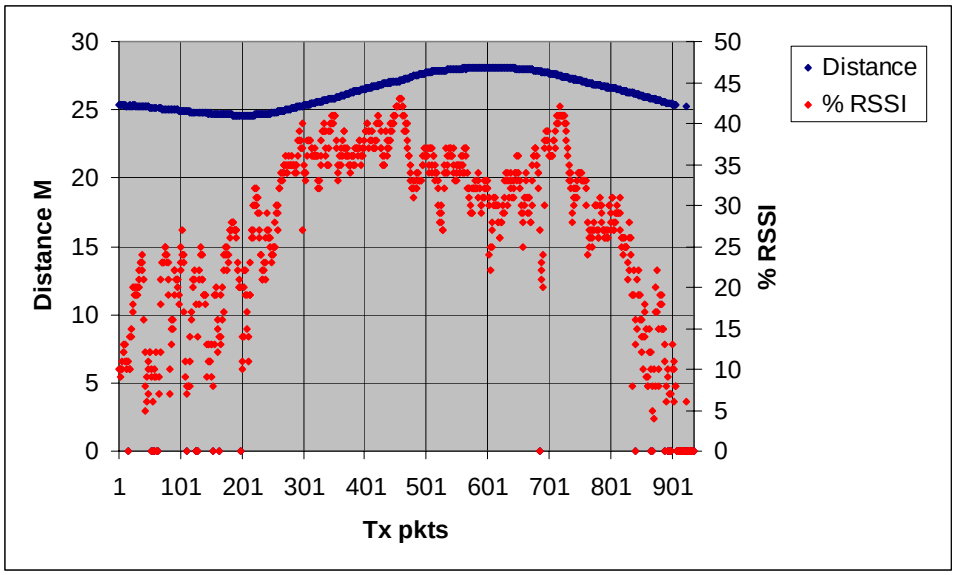


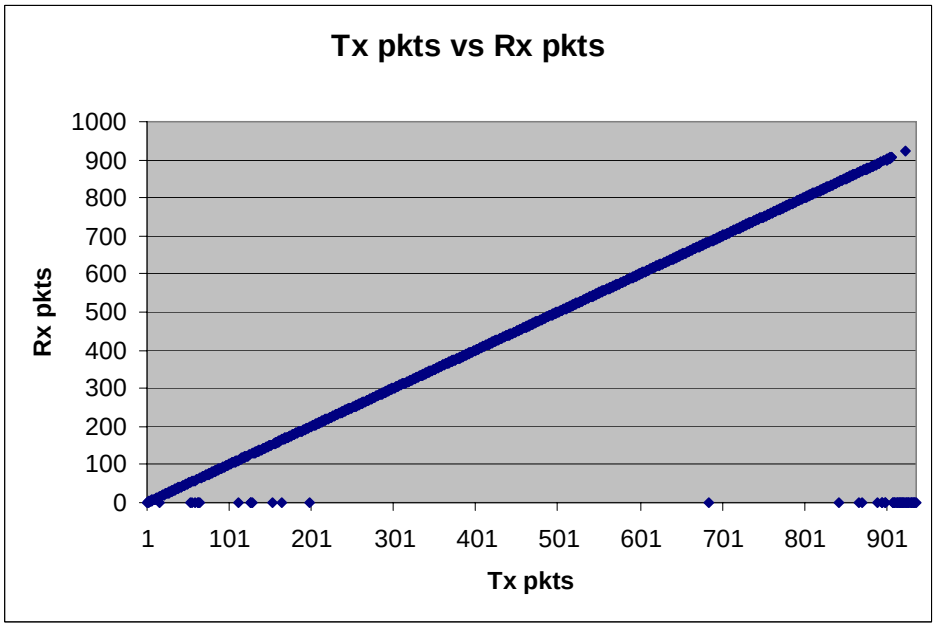


Total packets sent: 736

Total packets dropped: 5

3.7.1.15 Ford 23 5890 Counter-Clockwise Circular Passenger-Side Antenna





Total packets sent: 937

Total packets dropped: 52

Appendix E:
WAVE Radio Modules

TABLE OF CONTENTS

1 BACKGROUND 1
1.1 Goal 1
1.2 Preliminary Requirements for Second Generation WAVE Radio Module 1
2 DESIGN ISSUES AND DECISIONS 3
2.1 Basic Hardware Configuration 3
2.2 Basic Interface Configuration 3
2.3 Basic Lower Layer Functionality 3
3 FUNCTIONAL SPECIFICATION 4
3.1 Scope 4
3.2 WAVE Radio Module Interfaces 4
3.3 WAVE Radio Module Functional Requirements 5
3.4 WAVE Radio Module RF Performance Requirements 9
3.5 ASTM E2213-03 Exception Matrix 10
4 HARDWARE DESIGN SPECIFICATION 14
4.1 Scope 14
4.2 Rationale for Access Point Card Selection 14
4.3 WAVE Radio Module (WRM) Hardware Description 16
4.4 AP48 Interface Descriptions 20
4.5 AP48 Chipset Features 21
5 INTERFACE SPECIFICATION 24
5.1 Scope 24
5.2 WAVE Radio Module Attachment and Configuration 24
5.3 WAVE Radio Module Telnet Interface 25
5.4 WAVE Radio Module IP Interface 43

6 ACCEPTANCE TESTING 52
6.1 Scope 52
6.2 Test Configurations 52
6.3 WRM Interface Specification Tests 57
6.4 WRM Functional Specification Tests 141
6.5 WRM Network Tests 148
6.6 Requirement/Test Cross Reference Matrix 156
7 ACCEPTANCE TEST REPORT 158
7.1 Scope 158
7.2 Test Equipment 158
7.3 ATP Result Summary 158
7.4 Software Issues Discovered while Testing 161
A-1 TERMS, ACRONYMS, AND ABBREVIATIONS 163
A-2 REFERENCES 166

TABLE OF FIGURES

Figure 3-1. Wave Radio Module Interfaces 4
Figure 4-1. WRM Radio Module and Interfaces 16
Figure 4-2. WRM Front and Rear Views 17
Figure 4-3. AP48 Card with RF Cables, Internal Devices and Connectors 17
Figure 4-4. Example DC-DC Converter (left) and Wall Cube AC-DC Converter (right) 19
Figure 4-5. Key AP48 Atheros Chip Functions and Interfaces [5] 22
Figure 5-1. Host Device to Wave Radio Module Connection 24
Figure 5-2. Login Screen 26
Figure 5-3. Login Sequence 26
Figure 5-4. Invalid Command Response 28
Figure 5-5. Invalid Command Parameter Response 29
Figure 5-6. IPv4 Frame 43
Figure 5-7. WAVE Tx Option Format 44
Figure 5-8. WAVE RX Option Format 48
Figure 5-9. WRM Default Configuration Option Format 49
Figure 5-10. WRM Configuration Request Option Format 50
Figure 5-11. WRM Configuration Option Format 51
Figure 6-1. Single WRM Test Setup 53
Figure 6-2. WRMs with Power Meter and Attenuator Test Setup 53
Figure 6-3. WRM with Spectrum Analyzer Test Setup 53
Figure 6-4. WRM with Spectrum Analyzer and Vector Signal Analyzer Test Setup 53
Figure 6-5. WRM with Power Meter Test Setup 54
Figure 6-6. WRM with Vector Signal Analyzer Test Setup 54
Figure 6-7. WRMs with Cable Connection 54
Figure 6-8. Dual WRMs 54
Figure 6-9. WRMs with Step Attenuators and Vector Signal Analyzer Test Setup 55

TABLE OF TABLES

Table 3-1. WAVE Radio Module Functional Commands 6
Table 3-2. WAVE Radio Module Characteristics 9
Table 3-3. RF Transmit Performance Requirements 9
Table 3-4. RF Receive Performance Requirements 10
Table 3-5. RF Synthesizer Performance Requirements 10
Table 3-6. ASTM E2213-03 Exception Matrix 10
Table 4-1. WRM 802.11 Card Selection Criteria 14
Table 4-2. WRM Attributes 18
Table 4-3. DC-DC and AC-DC Converter Specs 19
Table 4-4. RF Cable Attributes [7] 20
Table 4-5. Summary of AP48 Chipset Features 22
Table 5-1. Telnet WAVE Command Summary 27
Table 5-2. Set/Get Command and Response Format 28
Table 5-3. Wireless Mode Command 29
Table 5-4. Default Parameter Values 29
Table 5-5. Service Mode Command 30
Table 5-6. Unit Mode Command 31
Table 5-7. Antenna Command 31
Table 5-8. Antenna 1 Compensation Factor Command 32
Table 5-9. Antenna 2 Compensation Factor Command 32
Table 5-10. Bandwidth Command 33
Table 5-11. Fast Channel Command 34
Table 5-12. WAVE Channels 34
Table 5-13. 802.11a Channels 35
Table 5-14. Fragmentation Threshold Command 36
Table 5-15. Transmit Power Command 36
Table 5-16. Maximum Transmit Power Limits 38
Table 5-17. Maximum Transmit Power Limits for Public Safety 38
Table 5-18. Maximum Transmit Power Limits for Private Usage 38
Table 5-19. Data Rate Command 39
Table 5-20. Data Rates 39
Table 5-21. RTS/CTS Threshold Command 39
Table 5-22. WAVE Default Parameters Command 40

Table 5-23. Configuration Parameters Command 40
Table 5-24. Configuration Parameters Response 40
Table 5-25. Hardware Version Command 41
Table 5-26. RSSI Command 42
Table 5-27. Copy (C) Flag Field Definition 44
Table 5-28. Class Field Definition 44
Table 5-29. Option Field Definition 44
Table 5-30 Length Field Definition 44
Table 5-31. WAVE Channel Field Definition 45
Table 5-32. 802.11a Channel Field Definition 45
Table 5-33. Tx Power Field Definition 46
Table 5-34. Data Rate Field Definition 46
Table 5-35. Fragmentation Threshold Field Definition 46
Table 5-36. RTS/CTS Threshold Field Definition 46
Table 5-37. Destination MAC Address Field Definition 47
Table 5-38. Service Mode (SM) Field Definition 47
Table 5-39. Unit Mode (UM) Field Definition 47
Table 5-40. Antenna (ANT) Field Definition 47
Table 5-41. Bandwidth (BW) Field Definition 47
Table 5-42. Reserved (RSV) Field Definition 47
Table 5-43. Option Field Definition 48
Table 5-44. Length Field Description 48
Table 5-45. RSSI Field Definition 48
Table 5-46. Received MAC Header Field Definition 49
Table 5-47. Antenna (ANT) Field Definition 49
Table 5-48. Option Field Definition 49
Table 5-49. Length Field Definition 49
Table 5-50. Option Field Definition 50
Table 5-51. Length Field Definition 50
Table 5-52. Option Field Definition 51
Table 5-53. Length Field Definition 51
Table 5-54. Antenna 1 Compensation Factor Field 51
Table 5-55. Antenna 2 Compensation Factor Field 51
Table 5-56. Local MAC Address Field Definition Field 51
Table 6-1. Telnet Initialization Procedure 55

Table 6-2. IP Initialization Procedure 56
Table 6-3. WAVE Default Parameters 56
Table 6-4. WRM and API Tester Software Versions 57
Table 6-5. IP API Function Calls 58
Table 6-6. Telnet API Function Calls 59
Table 6-7. WAVEdefault Telnet Test 60
Table 6-8. WAVEdefault Telnet Test Results – Modified Parameters 61
Table 6-9. WAVEdefault Telnet Test Results – Default Parameters 62
Table 6-10. WAVEdefault IP Configuration Test 62
Table 6-11. WAVEdefault IP Configuration Test Results – Initial Values 63
Table 6-12. WAVEdefault IP Configuration Test Results - Modified Parameters 63
Table 6-13. WAVEdefault IP Configuration Test Results - Default Parameters 64
Table 6-14. Wireless Mode Telnet Test 65
Table 6-15. Service Mode Telnet Test 66
Table 6-16. Service Mode IP Configuration Test 67
Table 6-17. Service Mode IP Packet-by-Packet Test 68
Table 6-18. Unit Mode Telnet Test 69
Table 6-19. Unit Mode IP Configuration Test 70
Table 6-20. Unit Mode IP Packet-by-Packet Test 71
Table 6-21. Antenna Configuration Telnet Test 72
Table 6-22. Antenna Configuration *"best"* Telnet Test Result 75
Table 6-23. Antenna Configuration IP Configuration Test 75
Table 6-24. Antenna Configuration IP Packet-by-Packet Test 77
Table 6-25. Antenna 1 Configuration IP Packet-by-Packet Tx Test Results 78
Table 6-26. Antenna 1 Configuration IP Packet-by-Packet Rx Test Results 79
Table 6-27. Antenna 2 Configuration IP Packet-by-Packet Tx Test Results 79
Table 6-28. Antenna 2 Configuration IP Packet-by-Packet Rx Test Results 79
Table 6-29. Antenna Best Configuration IP Packet-by-Packet Tx Results 80
Table 6-30. Antenna Best Configuration IP Packet-by-Packet Rx Results 80
Table 6-31. Antenna 1 Compensation Factor Telnet Test 80
Table 6-32. Antenna 1 Compensation Factor Telnet Test Results 81
Table 6-33. Antenna 1 Compensation Factor IP Configuration Test 81
Table 6-34. Antenna 1 Compensation Factor IP Configuration Test Results 82
Table 6-35. Antenna 2 Compensation Factor Telnet Test Results 82
Table 6-36. Antenna 2 Compensation Factor IP Configuration Test Results 83

Table 6-37. Bandwidth Telnet Test 84
Table 6-38. Bandwidth IP Configuration Test..... 86
Table 6-39. Bandwidth IP Packet-by-Packet Test 87
Table 6-40. Fastchannel Telnet Test..... 89
Table 6-41. WAVE Channel Frequency and BW Telnet Test Results 90
Table 6-42. 802.11a Channel Frequency and BW Telnet Test Results 91
Table 6-43. WAVE Channel Data Rate Telnet Test Results 91
Table 6-44. 802.11a Channel Data Rate Telnet Test Results 92
Table 6-45. Fastchannel IP Configuration Test 92
Table 6-46. WAVE Channel Frequency and BW IP ConfigurationTest Results 93
Table 6-47. 802.11a Channel Frequency and BW IP Configuration Test Results 94
Table 6-48. Fastchannel IP Packet-by-Packet Test 94
Table 6-49. WAVE Channel Frequency and BW IP Packet-by-Packet Test Results..... 95
Table 6-50. 802.11a Channel Frequency and BW IP Packet-by-Packet Test Results 96
Table 6-51. Fragment Threshold Telnet Test 96
Table 6-52. Fragment Threshold IP Configuration Test..... 97
Table 6-53. Fragment Threshold IP Packet-by-Packet Test 98
Table 6-54. Power Level Telnet Test 100
Table 6-55. Antenna 1 Output Power Level Telnet Test Results 101
Table 6-56. Antenna 2 Output Power Level Telnet Test Results 102
Table 6-57. Power Level IP Configuration Test..... 103
Table 6-58. Antenna 1 Output Power Level IP Configuration Test Results..... 104
Table 6-59. Antenna 2 Output Power Level IP Configuration Test Results..... 105
Table 6-60. Power Level IP Packet-by-Packet Test 106
Table 6-61. Antenna 1 Output Power Level IP Packet-by-Packet Test Results 107
Table 6-62. Antenna 2 Output Power Level IP Packet-by-Packet Test Results 108
Table 6-63. RSU Power Limiting Telnet Test..... 109
Table 6-64. RSU Power Limiting at Antenna 1 Telnet Test Results..... 110
Table 6-65. RSU Power Limiting at Antenna 2 Telnet Test Results..... 112
Table 6-66. RSU Power Limiting IP Configuration Test 113
Table 6-67. RSU Power Limiting at Antenna 1 IP Configuration Test Results 114
Table 6-68. RSU Power Limiting at Antenna 2 IP Configuration Test Results 114
Table 6-69. RSU Power Limiting Packet-by-Packet IP Test..... 116
Table 6-70. RSU Power Limiting at Antenna 1 Packet-by-Packet IP Test Results..... 117
Table 6-71. RSU Power Limiting at Antenna 2 Packet-by-Packet IP Test Results..... 118

Table 6-72. OBU Power Limiting Telnet Test 119
Table 6-73. OBU Power Limiting at Antenna 1 Telnet Test Results 120
Table 6-74. OBU Power Limiting at Antenna 2 Telnet Test Results 121
Table 6-75. OBU Power Limiting IP Configuration Test..... 122
Table 6-76. OBU Power Limiting at Antenna 1 IP Configuration Test Results..... 124
Table 6-77. OBU Power Limiting at Antenna 2 IP Configuration Test Results..... 125
Table 6-78. Data Rate Telnet Test..... 126
Table 6-79. 10MHz Channel Data Rate Telnet Test Results..... 127
Table 6-80. 20MHz Channel Data Rate Telnet Test Results..... 127
Table 6-81. Data Rate IP Configuration Test 128
Table 6-82. 10 MHz Channel Data Rate IP Configuration Test Results 129
Table 6-83. 20 MHz Channel Data Rate IP Configuration Test Results 129
Table 6-84. Data Rate IP Packet-by-Packet Test..... 130
Table 6-85. 10MHz Channel Data Rate IP Packet-by-Packet Test Results..... 131
Table 6-86. 20MHz Channel Data Rate IP Packet-by-Packet Test Results..... 131
Table 6-87. RTS Threshold Telnet Test 132
Table 6-88. RTS Threshold IP Configuration Test..... 134
Table 6-89. RTS Threshold IP Packet-by-Packet Test 136
Table 6-90. Hardware Version Telnet Test 138
Table 6-91. RSSI Telnet Test 139
Table 6-92. RSSI Telnet Test Results 139
Table 6-93. RSSI IP Packet-by-Packet Test 140
Table 6-94. RSSI IP Packet-by-Packet Tests and Results 140
Table 6-95. Software Version Telnet Test..... 141
Table 6-96. Power-Up Initialization Test 142
Table 6-97. MAC Address Test..... 143
Table 6-98. 802.11 Management Frames Test 144
Table 6-99. Data Tx/Rx Test 145
Table 6-100. WRM Reconfiguration Time Test..... 146
Table 6-101. Broadcast Addressing Single Channel Operation Test..... 148
Table 6-102. Broadcast Addressing Multi-Channel Operation Test..... 149
Table 6-103. Directed Addressing Single Channel Operation Test..... 151
Table 6-104. Directed Addressing Multi-Channel Operation Test..... 152
Table 6-105. Multiple Transmitters with Multiple Receivers Test..... 154

1 BACKGROUND

The purpose of this project was to develop a WAVE Radio Module, in accordance with the preliminary requirements (see Section 1.2), to support and enable future VSCC activities in communication protocol implementation and testing, safety application prototyping, and/or field trials. This radio module was intended to have a defined interface accessible by a variety of different computer arrangements. The radio module implements ASTM 2213-03: "Standard Specification for Telecommunications and Information Exchange between Roadside and Vehicle Systems — 5 GHz Band Dedicated Short Range Communications (DSRC) Medium Access Control (MAC) and Physical Layer (PHY) Specifications" [1] within the technical capabilities achievable with currently available hardware. ASTM 2213-03 is the lower layer standard that has been mandated by the FCC for use in the 5.9 GHz DSRC spectrum.

The materials contained in Chapters 3-7 of this report were written by the identified contractor, Denso LA Laboratories, in conjunction with the VSCC. The materials prepared by Denso comprised a number of separate specifications and reports. These were integrated into this report with minor editorial and formatting revisions.

This project was completed successfully within the planned time. Twenty second-generation WAVE radio module units were built and delivered according to the functional, hardware design and interface specifications described in this report. In addition, all radio interface Application Programming Interfaces (APIs) were provided, as well as automated software to verify API operations.

1.1 Goal

The overall goals of this project were to deliver WAVE radio modules that:

1) Provide higher layer prototyping compatibility, with APIs for application control of the radio;
2) Are robust, and usable with various computing platforms; and,
3) Offer design considerations that are likely to be cost-effective for potential medium- to large-scale field trials in the future

1.2 Preliminary Requirements for Second-Generation WAVE Radio Module

While the second-generation WAVE radio modules are not expected to be fully compliant with production automotive requirements, they must operate in the vehicle environment, as well as in various roadside locations (such as traffic signal control cabinets).

1.2.1 Functional Requirements

The major functional requirements for this project, identified on a preliminary basis, included:

1) Implement ASTM 2213-03: "Standard Specification for Telecommunications and Information Exchange between Roadside and Vehicle Systems — 5 GHz Band Dedicated Short Range Communications (DSRC) Medium Access Control (MAC) and Physical Layer (PHY) Specifications" [1] to the extent technically possible with an appropriate, currently available IEEE 802.11a chip set. The known differences from ASTM 2213-03 include:
   - Maximum transmission power in the 20 dbm range
   - Channel switching capability in less than 5 ms

2) Support the "WAVE" *ad hoc* mode:
   - Remove usage of all management frames and their associated management functions
   - In particular, no more associations

3) Support operations using 10 MHz channels in the 5.8 and 5.9 GHz bands

4) Design and implement an Application Programming Interface (API) for software control in real-time, including:
   - Channel of operation
   - Service Set Identifier (SSID)
   - Antenna switch operation mode (selection of single, dedicated antenna or two diversity antennas)
   - Power of transmission
   - Feedback from radio on Received Signal Strength Indicator (RSSI) of each received frame

1.2.2 Interface Requirements

Preliminary identification of interface requirements included:

1) Antenna connector(s)
2) Physical interface suitable for interconnection with embedded systems
3) Power, preferably automotive compatible (i.e. 12.6 volt DC)

2 DESIGN ISSUES AND DECISIONS

The initial stages of this project included several basic design decisions of major significance to the planned VSC project field testing. In most cases, the project schedule was one of the main determining factors in these decisions.

2.1 Basic Hardware Configuration

There were many different concepts discussed regarding the hardware configuration of the WAVE Radio Module. Since the use of these radio modules was to be primarily for testing purposes, size and unit cost became less consequential decision parameters. Within the compressed 18-week schedule to design and build the radio modules, it became imperative to select current, off-the-shelf hardware that would require as little modification as possible and still support the field testing requirements of the VSC project.

The decision to use a reference design Access Point (AP) card was based upon the schedule considerations, as well as the identification of the Atheros AP48 AP card that would support the necessary customization to meet the channel width, power, and frequency requirements.

2.2 Basic Interface Configuration

During the design phase of this project, the interface configuration was the focus of substantial discussion. Eventually, the embedded nature of the operating system and the limited capabilities of the processor on the AP determined that applications would more effectively need to be run on processors external to the radio module.

The decision to use an Ethernet interface to connect the radio module to the external processor (Host Device or HD), was reached by considerations of interoperability and the wide availability of Ethernet devices and drivers.

2.3 Basic Lower Layer Functionality

The decision to make the radio modules as compliant as possible with the version of the ASTM lower layer standard that had already been mandated by the Federal Communications Commission (FCC) was reached only after careful consideration of the proposals to modify the lower layer standards. The final decision was based upon the understanding that the proposed modifications to the lower layer standards were unlikely to be formally agreed in time to be incorporated into the radio modules. Even if the main concepts of the modifications were known prior to the design decision, various iterations would be expected to preclude a specific reference standard to which the radio modules could be built.

3 FUNCTIONAL SPECIFICATION

This chapter provides the Functional Specification for the WAVE Radio Module delivered in accordance with the VSC Project: Requirements for Second Generation WAVE Radio Module [Section 1.2].

3.1 Scope

This WAVE Radio Module (WRM) Functional Specification describes the WRM interface, functional, and RF performance requirements. It also provides a matrix identifying the areas of non-compliance with the ASTM E2213-03 [1] specification. The requirements in this document were derived from the VSC Project: Preliminary Requirements for Second Generation WAVE Radio Module [Section 1.2] and the ASTM E2213-03 specification.

3.2 WAVE Radio Module Interfaces

This section specifies the WRM physical interface requirements. Figure 3-1 illustrates the configuration. The WRM supports interfaces for two antennas, an Ethernet connection, and power. The WRM rear panel incorporates four connectors to support these interfaces. The subparagraphs below specify the requirements for each interface.

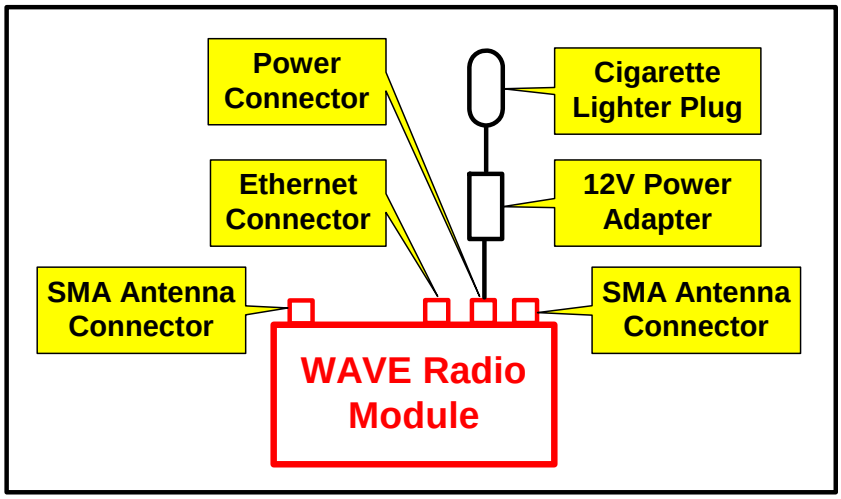


Figure 3-1. Wave Radio Module Interfaces

3.2.1 Antenna Interface

The WRM shall provide two 50-ohm chassis-mounted SMA jack (female) connectors for connecting external antennas. The antennas provide single antenna or receive diversity operation. Antennas will not be supplied with the WRM.

3.2.2 Ethernet Interface

The WRM shall provide a RJ45 jack into which a standard or crossover Ethernet cable with a RJ45 connector can be plugged. The interface shall support data rates of 10 Mbps or 100 Mbps and is used for communication between a Host Device (HD) and the WRM.

3.2.3 Power Interface

The WRM shall include a vehicle DC/DC power converter with a cable that plugs into a standard 12.6V cigarette lighter and to the WRM (5V). The WRM draws up to 2A of current at 5V.

3.3 WAVE Radio Module Functional Requirements

This section specifies the requirements for WAVE mode operation.

3.3.1 Host Device Interface

The WRM shall communicate with a HD over the Ethernet interface (see Section 3.2.2). The WRM shall support the commands and responses described in the WRM Interface Specification (Chapter 5). These commands support setting and retrieving the WRM mode, the RF configuration, and WAVE protocol parameters, as well as retrieving status. Table 3-1 lists the settable parameters that affect the functional operation of the WRM along with the specification paragraph where the effect is described. The WRM Interface Specification provides the default values for each of these parameters. Upon receiving a command to change to a new wireless mode followed by a reboot command, the WRM shall begin operation in the new mode within 10 seconds after receiving the reboot command. Upon receiving a command to change any other parameter, the WRM shall reconfigure to the new setting within 5 ms.

Table 3-1. WAVE Radio Module Functional Commands

Parameter Type	Parameter	Options	Specification Paragraph(s)
WRM Mode	Wireless Mode	WAVE or 802.11a protocol	3.3.3
	Unit Mode	Road Side Unit (RSU) or On Board Unit (OBU)	3.3.2.3, 3.3.3.2
RF Configuration	Antenna	1, 2, or Best	3.3.2.1
	Bandwidth	10 MHz or 20 MHz	3.3.2.2
	Channel	802.11a channel (in mid or upper UNII band) or WAVE channel	3.3.2.2
	Data Rate	Valid 802.11a or WAVE data rate.	3.3.2.2
	Tx Power	0 to 20 dBm or full power	3.3.2.3
WAVE Protocol	RTS/CTS threshold	Threshold in bytes	3.3.3.6

3.3.2 RF Configuration

3.3.2.1 Antenna Configuration

The WRM shall support two antennas. The WRM shall support transmit and receive on a single antenna (antenna 1 or 2), and shall also support an antenna "best" mode. In "best" mode, antenna 1 is used for transmit and receive diversity is enabled. The WRM monitors received signal strength on both antennas, and selects the receive antenna based on the strongest received signal. The antenna configuration is settable by the HD.

3.3.2.2 Channel Configuration

The WRM shall be able to tune to any WAVE channel as specified by ASTM E2213-03, and any US 802.11a channel as specified by IEEE 802.11a (except the lower UNII band channels (36-48), due to a restriction from the FCC when issuing grant). U.S. Government permission is required to transmit in the WAVE band. For WAVE channels, the WRM shall support operation at the bandwidth (10 or 20 MHz) specified by ASTM E2213-03. For 802.11a channels, the WRM radio shall support operation with either a 10 or 20 MHz bandwidth. The WRM shall support all data rates specified by

ASTM E2213-03 for channels operating with a 10 MHz bandwidth. The WRM shall support all data rates specified by IEEE 802.11a for channels operating with a 20 MHz bandwidth. The channel, channel bandwidth, and data rate are settable by the HD. Refer to the WRM Interface Specification for a complete listing of the channels, channel bandwidths, and data rates.

3.3.2.3 Transmit Power

The WRM shall support transmitting at an HD-settable power level up to nominally 20 dBm or higher if available. Due to variation in test equipment measurement, transmitter temperature changes, and 802.11 duty cycle changes, the tolerance on AP48 power output measurements is +/-1 dB or greater. For WAVE channels, the WRM shall limit the transmit power at the SMA connector so the maximum allowable level at the antenna input, as specified by ASTM E2213-03, will not be exceeded. The tolerance on the maximum limit is +/-2 dB. The maximum allowable antenna input power is a function of channel and unit mode. Refer to the WRM Interface Specification for a complete listing of the maximum allowable levels.

3.3.3 WAVE Protocol

3.3.3.1 Power-Up Initialization

Upon power-up, the WRM shall initialize to the last stored configuration.

3.3.3.2 MAC Address

When the WRM is operating in RSU mode, it shall use the last stored MAC address. When the WRM is operating in OBU mode, it shall generate a random MAC address when it powers up. The WRM will use standard C library functions to generate the random address.

3.3.3.3 MAC Frame Construction

The WRM shall construct MAC frames in accordance with IEEE 802.11 [3]. The MAC frames contain address fields which shall be set as follows:

1. To DS and From DS bits (Frame Control Field) – these bits shall both be set to 0.
2. Address 1 (Destination Address) – broadcast or unicast MAC address.
3. Address 2 (Source Address) – this field shall be set to the WRM MAC address (see Section 3.3.3.2).

4. Address 3 (Basic Service Set Identification (BSSID)) – this field shall be set to all 0s.
5. Address 4 – unused

The WRM shall always set the Power Management, More Data, and Wired Equivalent Privacy (WEP) fields to 0.

3.3.3.4 802.11 Management Frames

The WRM shall not transmit any IEEE 802.11 management frames. Upon receiving a management frame, the WRM shall acknowledge the frame but not take action based on its contents. As a result, the following 802.11 functions are not supported:

- Association/reassociation/disassociation
- Probes
- Time synchronization (beacons are disabled). This precludes the use of power save mode.
- Authentication/deauthentication
- WEP

3.3.3.5 802.11 Control Frames

The WRM shall not transmit any RTS/CTS control frames on the control channel (channel 178). On non-control channels, the WRM shall support the use of 802.11 RTS, CTS, and ACK control frames. The WRM shall not transmit any other type of control frame. As a result, operation with an 802.11 point control function (PCF) is not supported.

When transmitting on a non-control channel, the WRM shall send an RTS frame only if the MAC frame length exceeds the RTS/CTS threshold (which can be set by the HD).

3.3.3.6 802.11 Data Frames

The WRM shall support the use of 802.11 data frames with the subtype data. The WRM shall not transmit any other type of data frame.

3.3.3.7 DSRC Management Frames

The WRM will not support the DSRC management frames specified in Section 9 of ASTM E2213-03.

3.4 WAVE Radio Module RF Performance Requirements

The subsections below list the RF requirements from the VSCC preliminary requirements and ASTM E2213-03. Section 3.5 lists the WRM exceptions to these requirements.

3.4.1 General Characteristics

Table 3-2 lists the WRM characteristics.

Table 3-2. WAVE Radio Module Characteristics

Characteristic	Class	ASTM E2213-03 Reference
Regulatory Requirements	N/A	Sections 8.8.2, 8.8.3.1, and 8.9.3
Temperature	Type 1 (0 to 40°C)	Section 8.8.6
DSRC Device	Class C (Maximum Output Power of 20 dBm)	Section 8.9.2.2
Receiver Channel Rejection	Type 1	Section 8.10.2, 8.10.3

3.4.2 Transmit Requirements

Table 3-3 lists the RF transmit performance requirements.

Table 3-3. RF Transmit Performance Requirements

Parameter	Requirement
Transmit Power	The WRM shall output nominally 20 dBm or higher if available (measured at the SMA antenna connector).
Transmit Spectrum Mask	ASTM E2213-03, Section 8.9.2.
Spurious Transmissions	ASTM E2213-03, Table 7 (FCC CFR47, Part 90, I & M) **Error! Reference source not found.**.
Transmit Center Frequency Tolerance	ASTM E2213-03, Section 8.9.4.
Symbol Clock Frequency Tolerance	ASTM E2213-03, Section 8.9.5.
Transmit Modulation Accuracy	ASTM E2213-03, Section 8.9.6.

3.4.3 Receive Requirements

Table 3-4 lists the RF receive performance requirements.

Table 3-4. RF Receive Performance Requirements

Parameter	Requirement
Receiver Sensitivity	ASTM E2213-03, Section 8.10.1.
Adjacent Channel Rejection	ASTM E2213-03, Section 8.10.2.
Nonadjacent Channel Rejection	ASTM E2213-03, Section 8.10.3.
CCA Sensitivity	ASTM E2213-03, Section 8.10.4.
Multipath Delay Spread	ASTM E2213-03, Section 8.10.5.
Doppler Spread	ASTM E2213-03, Section 8.10.6.
Amplitude Variation	ASTM E2213-03, Section 8.10.7.
Rician Channel Variation	ASTM E2213-03, Section 8.10.8.

3.4.4 Synthesizer Requirements

Table 3-5 lists the synthesizer requirements.

Table 3-5. RF Synthesizer Performance Requirements

Parameter	Requirement
Channel Switching Time	< 5 ms (from VSCC Preliminary Requirements) < 2 ms (from ASTM E2213-03, Section 8.12)

3.5 ASTM E2213-03 Exception Matrix

Table 3-6 identifies the WRM exceptions to the ASTM E2213-03 requirements and the requirements where Denso performed testing to verify compliance. The compliance column identifies: compliance (C); non-compliance (N); or untested (U). If compliance is U, Denso does not have the equipment to perform the tests.

Table 3-6. ASTM E2213-03 Exception Matrix

E2213-03 Section	Requirement Summary	Com-pliance	Exceptions/Clarifications
4.1.1.2 (3)	*RSUs* RSUs may function as stations or access points (APs).	N	The WRM will operate in WAVE Ad Hoc mode. No access point management frames will be transmitted or processed in compliance with Section 4.1.1.2 (6).

E2213-03 Section	Requirement Summary	Com-pliance	Exceptions/Clarifications
4.1.1.2 (7)	*RF Measurements* RF power, sensitivity, and antenna pattern are referenced to a standard location on the vehicle.	N	The TX power output and the Rx sensitivity will be measured at the SMA antenna connector.
4.9.4, A.2.1	*Initialization* Device shall initialize to Annex A2 settings.	N	The WRM will initialize to the last stored configuration.
5.4.1	*Packet Fragmentation* *The [Frag-ACK-] frame sequence shall be supported.*	N	The WRM will not support MAC packet fragmentation. No packets will be fragmented by the transmitting WRM while in WAVE Ad Hoc mode.
6.4.2.1	*Duplicate Address Detection* If the OBU receives a frame with its own address, it selects a new MAC address. Duplicate address detection is done during association.	N	The WRM will not perform duplicate address detection. Association is not performed in WAVE Ad Hoc mode.
6.4.2.2, 7.1.5.1	*Random Number Generator* FIPS or ANSI random generators shall be used.	N	The WRM will use standard C library functions to generate the random MAC address.
7.1.1-7.1.3	*High Resolution RSSI* The device shall support high resolution RSSI mode.	N	The WRM will not support high resolution RSSI mode due to limitations of the Atheros hardware (See 8.3.1).
8.3.1, A3.1-A3.3	*RXVECTOR RSSI* RSSI resolution 0.2dB, accuracy of +/-1dB.	N	The Atheros cards report RSSI in dB with integer level resolution. High-resolution RSSI (~0.2dB) is not available. The RSSI reported by the WRM does not meet the +/- 1 DB accuracy requirement.
8.8.2, 8.8.3.1, 8.9.3	*Regulatory Requirements* US FCC requirements for operation in ITS-RS and UNII bands, including spurious emissions.	U, C	Denso does not currently have the equipment to perform the WAVE certification tests in the ITS-RS band. This requirement was not formally tested. In informal conducted emissions tests, the WRM complied with Part 90 requirements in the ITS-RS band and Part 15 requirements in the 802.11a bands.

E2213-03 Section	Requirement Summary	Com-pliance	Exceptions/Clarifications
8.8.2	*Transmit and Receive Operating Temperature* The device shall operate over the temperature range specified for its type.	U	The SOW does not require operation over any specific temperature range.
8.9.2	*Transmit Spectrum Mask* Maximum spectral density, 10MHz channels; Out-of-band max EIRP emissions.	C, N	The WRM complies with the ASTM mask for 10 MHz channels. The WRM did not comply with the 802.11a mask for 20 MHz channels on channels 175 and 181.
8.9.4	*TX Center Frequency Tolerance* Maximum tolerance of +/- 10 ppm for RSUs and OBUs.	C	The WRM complies with this requirement.
8.9.5	*Symbol Clock Frequency Tolerance* Maximum tolerance of +/- 10 ppm.	C	The WRM complies with this requirement.
8.9.6, 8.9.6.3, 8.9.7	*Transmit Modulation Accuracy* Relative constellation RMS error – also known as error vector magnitude (EVM).	N	The WRM marginally fails the EVM spec at the highest rate WAVE 64 QAM OFDM signal (27Mbps), and sometimes marginally fails at lower rates (16 and 64 QAM).
8.10.1	*Receiver Minimum Sensitivity* Lowest RSS for which reception of 1000-byte packets is greater than 90% of best-case throughput.	C	The WRM complies with this requirement.
8.10.2	*Adjacent Channel Rejection* Minimum rejection levels given for all WAVE rates.	N	The WRM adjacent channel rejection does not comply with the ASTM specs, based on type 1 requirements. The WRM passes ASTM specs at some of the higher burst rates.
8.10.3	*Nonadjacent Channel Rejection* Minimum rejection levels given for all WAVE rates.	N	The WRM non-adjacent channel rejection does not comply with the ASTM specs, based on type 1 requirements. The WRM passes ASTM specs at some of the higher burst rates.

E2213-03 Section	Requirement Summary	Com-pliance	Exceptions/Clarifications
8.10.5	*Multipath Delay Spread* <10% PER for two signals with 400 ns RMS delay spread, at 3, 6, and 12 Mbps rates averaged over 5 seconds.	U	Denso does not currently have the equipment to perform the test. This requirement will not be tested.
8.10.6	*Doppler Spread* <10% PER for a signal with max Doppler shift of +/- 2100 Hz, at 3, 6, and 12Mbps rates averaged over 5 seconds.	U	Denso does not currently have the equipment to perform the test. This requirement will not be tested.
8.10.7	*Amplitude Variation* <10% PER for a signal with 10 dB amplitude variation at 100 Hz rate, at 3, 6, and 12 Mbps rates averaged over 5 seconds.	U	Denso does not currently have the equipment to perform the test. This requirement will not be tested.
8.10.8	*Rician Channel Variation* <10% PER for signals with simulated Rician channel fading, at 3, 6, and 12 Mbps rates averaged over 5 seconds.	U	Denso does not currently have the equipment to perform the test. This requirement will not be tested.
8.11 (Table 14)	*Tx Power Levels* 64 power levels	N	The WRM will support setting power from 0 to 20 dBm in 1 dB increments. The WRM Tx output variability from the setting may be up to +/- 2 dB.
8.12	*Channel Switching Time* Channel switching time less than 2 ms.	N	The WRM supports channel switching time in under 4 ms. This is non-compliant with the ASTM spec, but meets the SOW requirement.
9	*DSRC Management Actions* Action Frame Support	N	The ASTM E2213-03 specification does not describe these requirements in sufficient detail to support implementation.
A.3.4, A.3.4.1 – A.3.4.3	*Antenna Position Calibration* Provide calibration parameters to the RSU	N	The WRM will not support transmission of antenna calibration parameters to the RSU.

4 HARDWARE DESIGN SPECIFICATION

This chapter provides the Hardware Design Specification for the WAVE Radio Module delivered in accordance with the VSC Project: Preliminary Requirements for Second Generation WAVE Radio Module [Section 1.2].

4.1 Scope

This WAVE Radio Module (WRM) Hardware Design Specification gives the rationale for selecting the 802.11a access point (AP), describes the WRM hardware and power supplies, describes WRM interfaces, and gives chipset features.

4.2 Rationale for Access Point Card Selection

Denso selected the Atheros AP48 AP card because it gave the best combination of features from the WRM 802.11 Card Selection Criteria in Table 4-1 below. The Atheros AP48 card is the latest available AP card from Atheros, and operates reliably with Atheros reference code and test tools. It provides nominally 20dBm or higher if available of maximum output power, including 1.4dB of test cable loss. The card offers a built-in Ethernet interface, and includes a MIPS processor to host the software. Denso will modify the Atheros software (SW) to operate in WAVE half-rate mode and in the WAVE frequency band. The Ethernet interface was preferred over more expensive mini-PCI and Cardbus interfaces offered by laptop-style 802.11 card designs.

Table 4-1. WRM 802.11 Card Selection Criteria

Selection Criteria	Associated Implementation Rules	AP48 Comments
Card is modifiable to operate in WAVE mode and WAVE band	Atheros is the only known source for 802.11 cards with software modifiable to operate in half-rate mode and tune to WAVE frequencies.	AP48 card is modifiable to run in WAVE mode and band.
Supports SOW schedule	Use existing 802.11 cards. Avoid design and layout of a new 802.11 card.	AP48 card is latest available card and it supports the schedule.
SW availability and documentation	Licensed Atheros code and Test SW works with their reference cards. Avoid use of commercial AP hardware and software due SW porting and OS uncertainties.	AP48 card runs with latest available Atheros code, and is modifiable.

Selection Criteria	Associated Implementation Rules	AP48 Comments
On-board processor	Implement stand-alone radio module. Avoid WLAN card drivers on host device.	AP48 includes an onboard (MIPS) processor.
Small form factor	Use a single board design; Avoid additional cards for power supply, a MIPS processor, and Ethernet driver.	AP48 card is a single board design.
Low-cost data interface to host	Use Ethernet interface; Avoid Cardbus and miniPCI interfaces.	AP48 includes an Ethernet interface.
Provide at least 20 dBm of RF output power	Most AP cards have higher RF output than Cardbus or miniPCI cards. Avoid these lower power cards.	AP48 has nominally 20dBm or higher RF output in WAVE band.
Provide two diversity antenna connections	AP cards provide two diversity antenna RF connections. Some Cardbus cards do not.	AP48 card has two diversity antenna connections.

4.2.1 Use of Commercial Access Points for the WRM

Denso investigated less expensive commercial APs for use in the WRM. The cheapest APs ($75-$200) did not use the Atheros AP chipset, but used third-party MIPS processors and Cardbus cards that typically have lower RF power output. Most of the more expensive APs ($600-$800) used the Atheros AP chipset. However, for all commercial APs, it was considered a risk to the 18-week schedule to establish vendor NDAs, procure the commercial vendor SW that runs in their third-party RTOS processors, determine the extent of vendor changes made to the Atheros code, and modify their build to develop WAVE capabilities. The key risks with commercial AP usage are uncertainties in porting the existing Denso code and a mismatch between VxWorks OS and the OS in the commercial AP.

4.2.2 Meeting Higher WAVE RF Output Power Limits

ASTM E2213-03 [1] allows for a maximum 28.8dBm output power (after cable losses). Commercial and Atheros 802.11a access points do not provide such high output power. The highest power commercial APs deliver only about 24dBm (for 802.11a, not WAVE). The WRM transmitter output power is nominally 20dBm or slightly higher in the WAVE band. Meeting these higher power ASTM limits was not a requirement of the SOW. However, Denso investigated approaches to obtain higher output power performance.

In order to use the WRM to evaluate higher output power performance called out in ASTM E2213-03, an external bi-directional amplifier (BDA) would need to be developed. It would need to operate in the WAVE band without distorting the WAVE orthogonal frequency division multiplexing (OFDM) waveforms. Currently, no vendor provides a WAVE band BDA. Denso is investigating the possibility of procuring and evaluating a modified 802.11a BDA that could work in part or all of the WAVE band.

4.3 WAVE Radio Module (WRM) Hardware Description

Figure 4-1 shows the WRM hardware elements. The WRM consists of the AP48 access point card, two RF cable assemblies and a housing (not shown), a car power supply, an office/lab power supply, and external WAVE antennas (not supplied). Front-panel LEDs identify system status, and internal connectors allow for debug and software development using RS-232 and EJTAG interfaces.

Denso will supply the radio module and the car power supply to VSCC. Although an office/lab power supply is not included in the SOW, Denso will also supply VSCC with the office/lab power supply that came with the AP48 access point. The module and power supplies are discussed in sections 4.3.1 and 4.3.2 below.

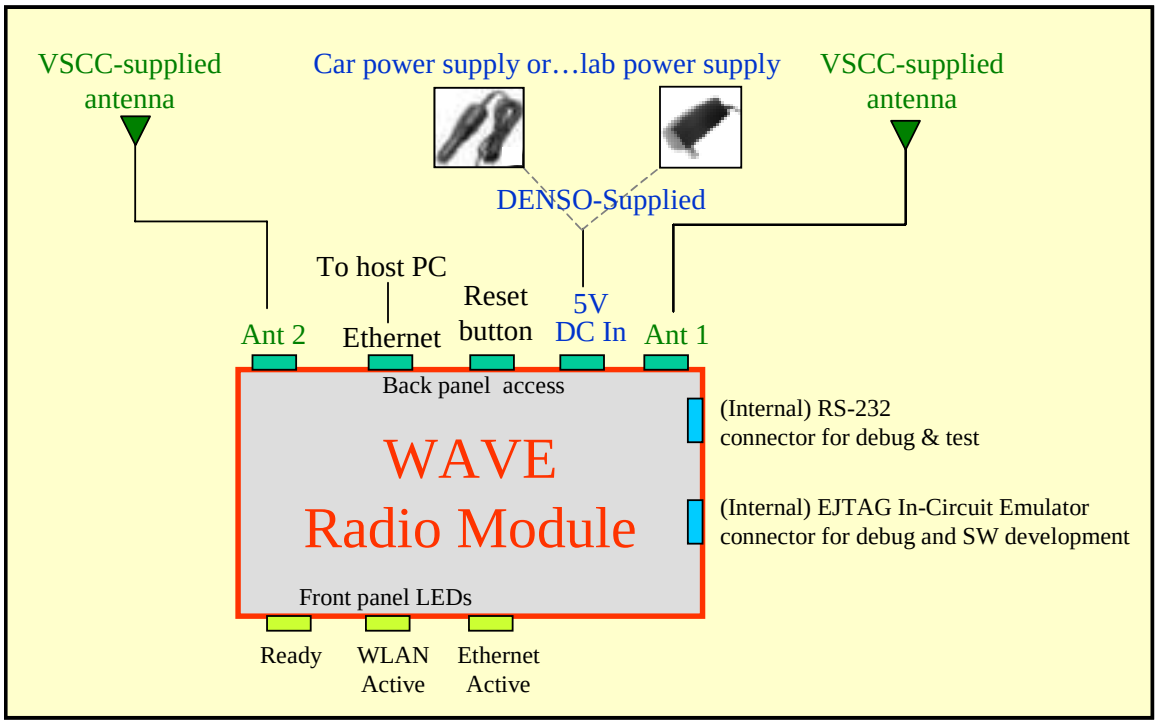


Figure 4-1. WRM Radio Module and Interfaces

4.3.1 Radio Module

Figure 4-2 shows the WRM front and rear views. The WRM supports external interfaces for two antennas, an Ethernet connection, reset button, and 5V direct-current (DC) power. The WRM rear panel incorporates the connectors to support these interfaces. The 5V DC input connector interfaces to either a car or lab supply. A dust cover for the back housing and various WRM labels are not shown.

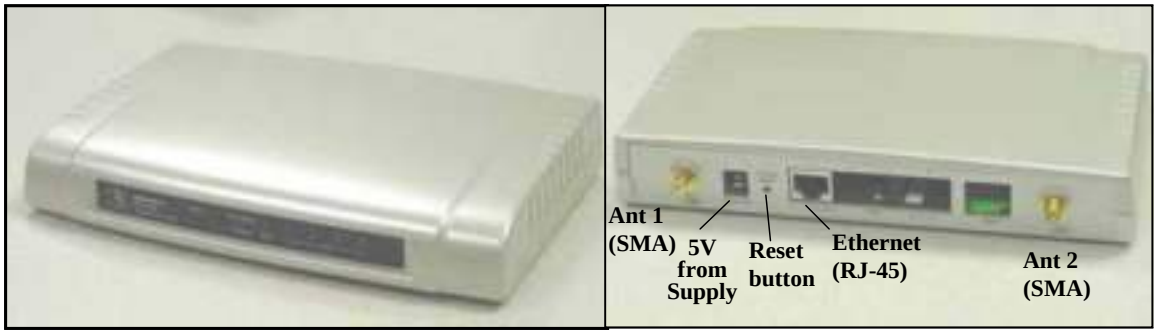


Figure 4-2. WRM Front and Rear Views

Figure 4-3 shows the AP48 card inside the WRM with two internal RF cables. One RF cable is not attached to a connector at back left. Figure 4-3 shows the location of RF connectors, RF circuit area, and Atheros MIPS/MAC processor on the card. Last, Figure 4-3 shows internal connectors for an RS-232 data interface for debug purposes (using dongle, not supplied) and an EJTAG interface, for in-circuit emulation. EJTAG is a standard developed by MIPS Technologies.

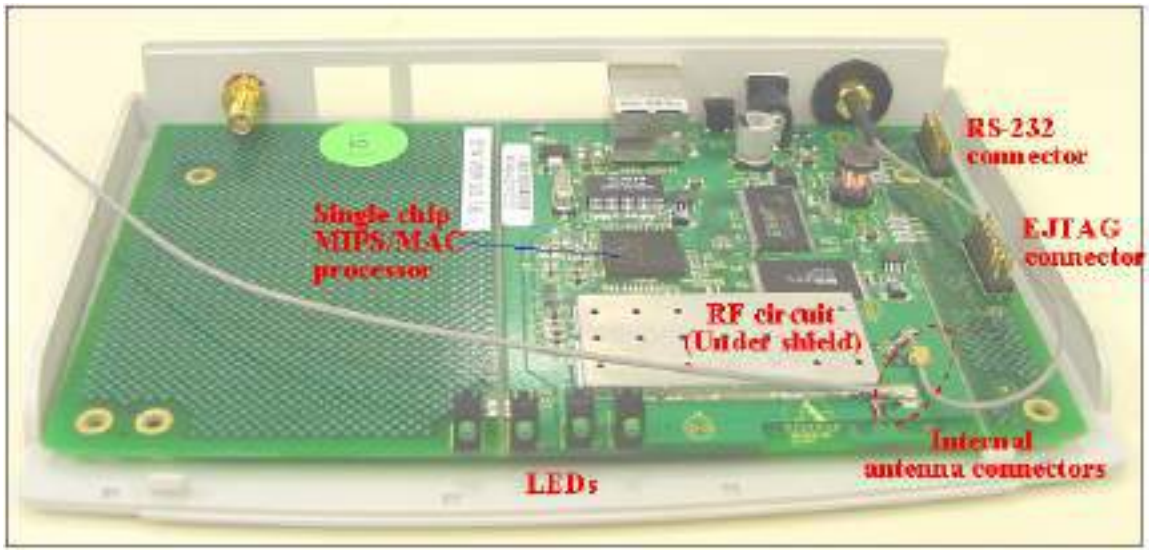


Figure 4-3. AP48 Card with RF Cables, Internal Devices and Connectors

Table 4-2 below gives the attributes of the WRM.

Table 4-2. WRM Attributes

WRM Attribute	Value or Range
FCC Certification	Certified to Part 15 for 802.11a operation. Tested at Denso for Part 90 for WAVE-band operation.
802.11-compliant modes	802.11a, WAVE
Operating frequencies	5.725-5.825GHz; 5.85-5.925GHz (WAVE)
Operating ambient temperature	0° to 40° C (typical commercial APs using Atheros chips)
RF output power (w/ cable)	16 to 20dBm* (rate-dependent), measured at SMA connector
RF TX power steps	1dB steps from 0 to 20dBm, and full power
Size with housing	7.5”W x 4.7”L x 1.25”H
Total weight (w/o DC convert)	0.6 lb
Power consumption, TX active	1.1A typical
Power consumption, RX active	0.9A typical
DC power interface	5V DC, via 5.5mm barrel connector
Ethernet interface	RJ-45 connector
Antenna interface	SMA female bulkhead connector
AP48 card size	5.2”W x 4.11”L
AP48 card type [12]	Single-sided 4 layer FR4 printed circuit board (PCB)

* The AP48 provides an output power of nominally 20dBm or higher if available. Because of variation in test equipment measurement, transmitter temperature changes, and 802.11 duty cycle changes, the tolerance on AP48 power output measurements is +/- 1dB or greater.

4.3.2 Power Supplies

Figure 4-4 shows two power supplies (converters), one of which is needed to provide 5V DC input to the WRM. The first unit is a 12V/5V DC-DC converter that includes a cigarette lighter adapter (CLA) that allows for WRM testing in a vehicle. The second unit is a 120V/5V AC-DC converter (wall cube) that allows for WRM testing in an office or lab.

Figure 4-4. Example DC-DC Converter (left) and wall cube AC-DC converter (right)

Table 4-3 gives the specs for the 12/5V DC-DC converter and the AC/DC power converter.

Table 4-3. DC-DC and AC-DC Converter Specs

Power Supply Specs	**12V/5V DC-DC Converter Target Value or Range**	**120V AC-5V DC Converter Value or Range**
Part Number	Lind DN0525-1220A	CUI Inc. DSA-0151A-05A
Input voltage	10.5V to 18V	90-132V AC
Input current	3 to 4A	0.40A (RMS) for 115V AC
Output voltage	5V DC nominal	+5V DC nominal
Output current	0 to 2.5A	0 to 2.4A typical
Voltage regulation	5% maximum	5% maximum
Line regulation	2% maximum	2% maximum
Fusing	Yes, 5A	Yes
Protection	Over current, over voltage, short circuit, under voltage	Over current, over voltage, short circuit
Operating ambient temperature	0° to 45° C typical	0° to 40° C
Size and weight	3”L x 5”W x 2”H, 0.6 lbs.	3.2”L x 2.1”W x 1.4”H, 0.4 lbs.

4.4 AP48 Interface Descriptions

The AP48 card has an internal interface for RF cable assemblies, and external interfaces for Ethernet, DC power, RS-232, antennas, and an in-circuit emulator. These interfaces are discussed beginning in section 4.4.1.

4.4.1 RF Cable Assemblies (Internal Interface)

Because the AP48 card uses micro-miniature RF coaxial connectors (see Figure 4-3) and operates up to 6GHz, Denso procured two cable assemblies to connect the two card connectors to standard SMA RF connectors on the housing. Hirose makes the card connector and cable. Denso provides and installs the cable assemblies. Table 4-4 gives the RF cable attributes.

Table 4-4. RF Cable Attributes [7]

RF Cable Attribute	Value or Range
Type	Hirose U.FL-LP-066 1.13mm diameter coaxial cable
Vendor cable part no.	RFW10531-8 (from Talley Communications)
Impedance	50 ohms nominal
Length	8 inch
Cable loss	1.2dB at 5.9GHz (typical)
Connectors	Hirose U.FL-LP-066 female plug and SMA jack bulkhead

4.4.2 Ethernet Interface

The WRM provides a RJ-45 jack for use with a standard or crossover Ethernet cable. The interface supports data rates of 10 Mbps or 100 Mbps and is used for communication between a Host Device (HD) and the WRM.

4.4.3 DC Power Interface

The WRM includes a vehicle DC/DC power converter with a cable that plugs into a standard cigarette lighter (CLA) and to the WRM. It also includes an AC/DC converter that mates to the same WRM power receptacle.

4.4.4 RS-232 Interface

The AP48 card includes an onboard connector that allows for software development and debug through a standard RS-232 serial data interface. An RS232 dongle mates to the onboard connector. The dongle can be procured directly from Atheros.

4.4.5 Antennas Interface

The WRM provides two standard 50-ohm RF SMA (SubMiniature version A) jack (female) connectors for connecting external antennas. The antennas provide single antenna or receive diversity operation. Denso does not provide antennas with the WRM.

4.4.6 In-Circuit Emulator Interface

An EJTAG interface is available for connecting an in-circuit emulator (ICE) for debug and software development purposes. The EJTAG interface directly interfaces to Wind River System's VisionICE, but also operates with other industry standard emulators and debuggers [11].

4.5 AP48 Chipset Features

Figure 4-5 shows the functions and interfaces of two primary Atheros chips in the AP48: the AR5112 dual-band RF chip and the AR2312 baseband processor chip. The AP48 card has a newer AR2313 chip to replace the AR2312. The AR2313 has the same performance as the AR2312.

4.5.1 AR5112 RF Chip Features

The design of the AR5112 RF chip allows for WAVE operation. According to the Atheros AR5112 datasheet, the AR5112 transmitter, receiver, and frequency synthesizer operate and tune to all WAVE frequencies. Software changes are needed to implement WAVE mode. The AR5112 operates in the 2.4GHz (802.11b/g) band, the 5GHz (802.11a) band, and the 5.9GHz WAVE band (with SW mods). However, software support will be disabled for 2.4GHz operation, 5.15 to 5.25 GHz operation, and for turbo mode because FCC certification of the WRM will not include these bands and mode. Figure 4-5 is a simplified view of the RF section. The AR5112 requires additional transmitter and receiver amplifiers (not shown) to achieve nominally 20dBm or higher output power [12]. In addition, Figure 4-5 does not show the antenna diversity supported by the chips.

4.5.2 AR2313 Baseband Chip Features

The AR2313 includes a built-in 32-bit MIPS R4000-class processor and wireless MAC and PHY functions. The functions for Ethernet MAC and fast UART (for RS-232) are also integrated.

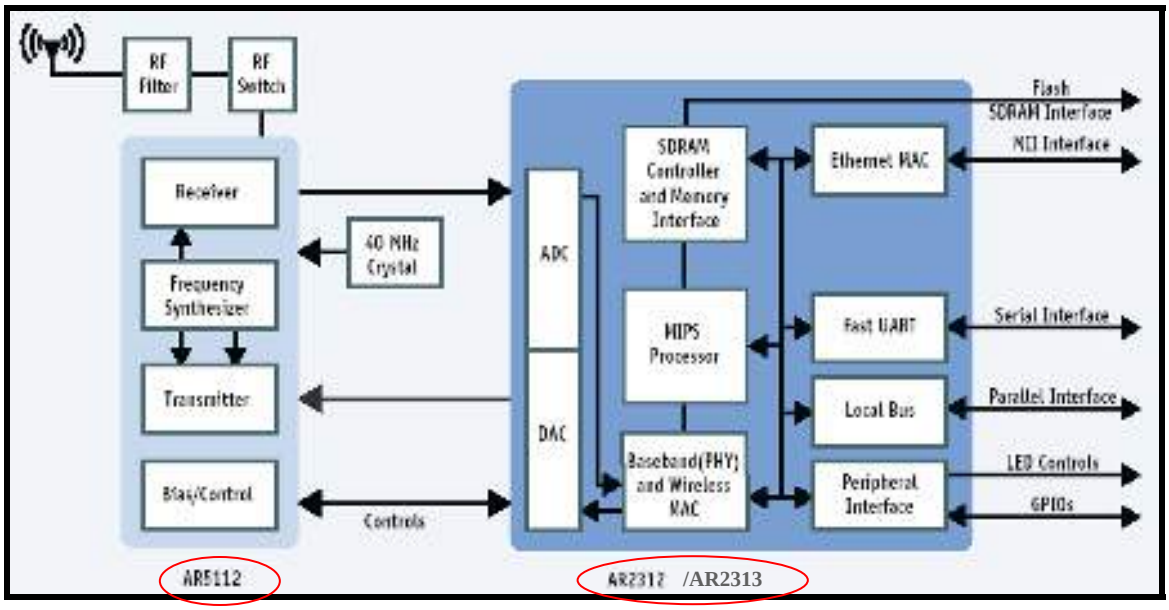
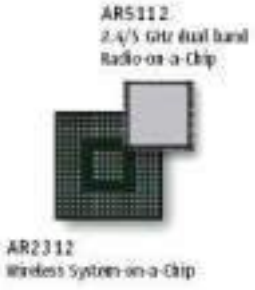


Figure 4-5. Key AP48 Atheros Chip Functions and Interfaces [5]

Table 4-5 summarizes the design features available with the Atheros AP48 chipset.

Table 4-5. Summary of AP48 Chipset Features

AP48 Chipset Features	Value or Range
Frequency Bands	US: 5.25-5.35GHz, 5.725-5.850GHz [2] **US DSRC: 5.85-5.925GHz [1]**
IEEE Data Rates: 802.11a, **WAVE mode**	1 - 54 Mbps (802.11a) [2] **3-27Mbps (WAVE 10MHz channels) [13], [14]** **6-54Mbps (WAVE 20MHz channels)**
802.11-compliant modes	802.11a, **WAVE**
Modulation Technology	OFDM with BPSK, QPSK, 16 QAM, 64 QAM;
FEC Coding Rate	1/2, 1/3, 3/4
Hardware Encryption	AES, TKIP, WEP
Quality of Service	802.11e draft
Media Access Technique	CSMA/CA
Communication Interface	MII, High Speed UART, local bus
Peripheral Interface	GPIOs, LEDs

AP48 Chipset Features	Value or Range
Memory Interface	FLASH, SDRAM
Operating temperature	**0° to 85° C (chip operating temperature range) [13], [14]**
Storage temperature range	**-60°C to 150°C [13], [14]**
Chip part numbers	**AR5112, AR2312/3**
Chip View	

5 INTERFACE SPECIFICATION

This chapter provides the Interface Specification for the WAVE Radio Module delivered in accordance with the VSC Project: Preliminary Requirements for Second Generation WAVE Radio Module [Section 1.2].

5.1 Scope

This WAVE Radio Module (WRM) Interface Specification describes the WRM setup, Telnet command interface and the Internet Protocol (IP) interface. The interface requirements in this document were derived from the VSC Project: Preliminary Requirements for Second Generation WAVE Radio Module [Section 1.2], the ASTM E2213-03 specification [1], and the Atheros AR5002 Access Point (AP) User's Guide [11].

5.2 WAVE Radio Module Attachment and Configuration

This chapter describes the procedure for connecting a Host Device (HD) to the WRM and configuring the HD IP address.

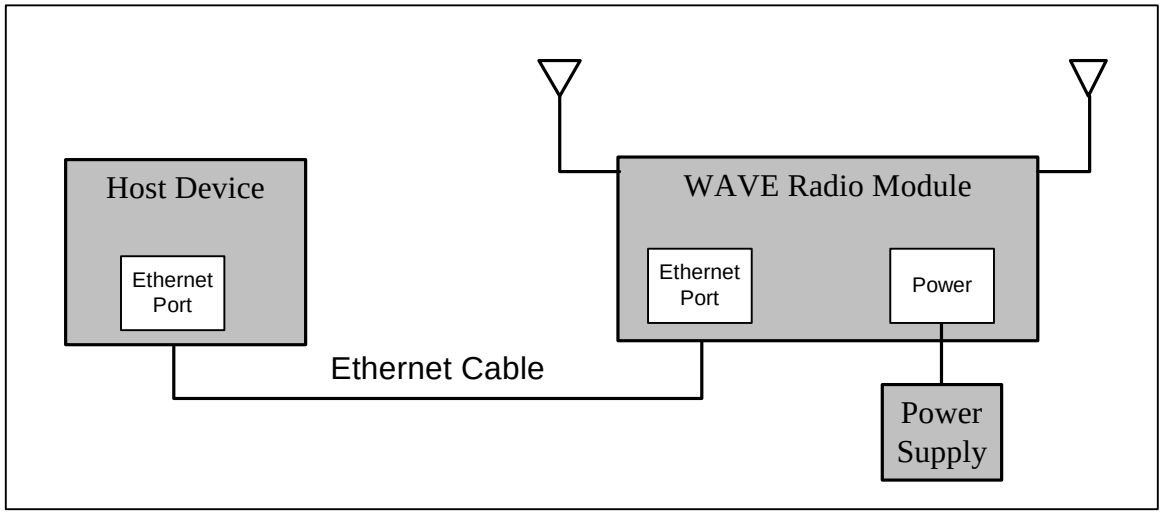


Figure 5-1. Host Device to Wave Radio Module Connection

5.2.1 WAVE Radio Module Network Connection

Connect the HD to the WRM using one of the following methods:

- Use an Ethernet crossover cable to connect the HD Ethernet port directly to the WRM Ethernet port.
- Use standard Ethernet cables to connect the HD and WRM through a hub or Ethernet switch.

Configure the HD IP address to an address of the format 192.168.001.xxx with Subnet Mask of 255.255.255.000. For communication to succeed, the HD IP address must be different from the WRM IP address (each WRM is delivered with a unique IP address of 192.168.1.0nn, where nn is the Denso assigned unit number).

5.2.2 Windows IP Configuration Example

If the HD is a PC running the Windows operating system, use the following procedure to configure the HD IP address.

- From the Host PC's Start menu, choose Settings and open the Network and Dialup Connections dialog box.
- Right click on the Local Area Connection icon that belongs to the Ethernet controller connected to the WRM and select Properties.
- Within the Local Area Connection Properties dialog box, choose Internet Protocol (TCP/IP) and click Properties.
- Configure the Host IP address to (192.168.001.xxx) for the Ethernet connection in the Internet Protocol (TCP/IP) Properties dialog box.
- Accept the settings and close the Internet Protocol Properties dialog box.
- The HD is now configured to communicate with the WRM.

5.3 WAVE Radio Module Telnet Interface

A HD configures the WRM using a Telnet Client Command Line Interface (CLI). Refer to the Telnet specification [9] for detailed requirements. The WRM supports Telnet login plus commands to get and set configuration parameters.

5.3.1 Telnet Login

To access the WRM, use the Telnet Client to log into the WRM using its IP address (e.g., Telnet 192.168.1.20). The CLI prompts for a login user name and password. After successfully entering this data, the CLI displays a version banner and prompt. The WRM is now ready to accept CLI commands as seen in Figure 5-2. Figure 5-3 illustrates the login sequence.

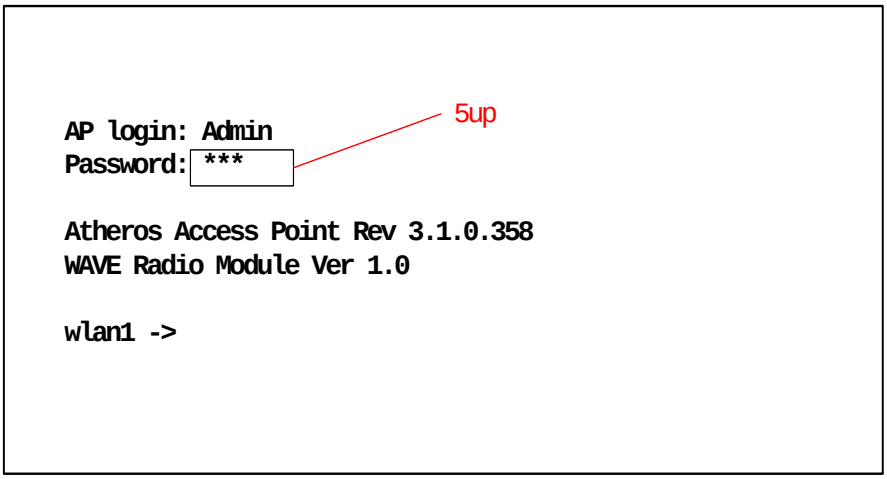


Figure 5-2. Login Screen

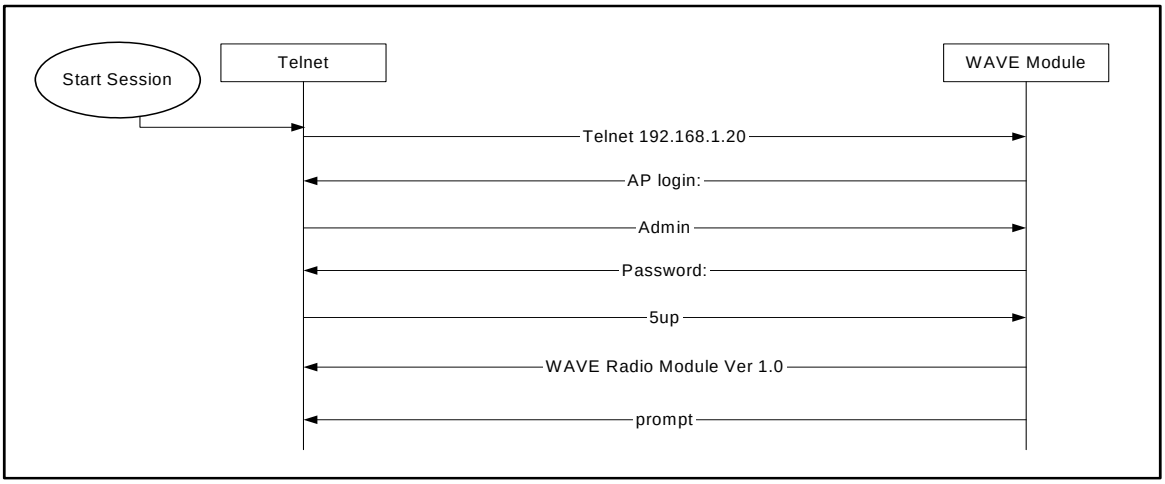


Figure 5-3. Login Sequence

5.3.2 Telnet Command Summary

Table 5-1 summarizes the Telnet WAVE commands. If the table indicates the set command requires a reboot, the HD must first send the set command and then a reboot command for the new parameter value to take effect. All commands are case insensitive.

Table 5-1. Telnet WAVE Command Summary

Command Category	Get Commands	Set Commands	Set Command Requires Reboot
Mode	get wirelessmode	set wirelessmode	Yes
	get servicemode	set servicemode	No
	get unitmode	set unitmode	No
Parameter	get antenna	set antenna	No
	get antenna1comp	set antenna1comp	No
	get antenna2comp	set antenna2comp	No
	get bandwidth	set bandwidth	No
	get fastchannel	set fastchannel	No
	get fragmentthreshold	set fragmentthreshold	No
	get power	set power	No
	get rate	set rate	No
	get rtsthreshold	set rtsthreshold	No
		set WAVEdefault	Yes
Status	get config		No
	get hardware		No
	get rssi		No
	version		No
Reboot		reboot	No

The WRM sends a response to every command.

Table 5-2 summarizes the format of the get/set commands and the response to valid commands.

Table 5-2. Set/Get Command and Response Format

Commands	**Description/Parameters**
get parameter	get “parameter” is used to retrieve the value of the designated “parameter”
set parameter newvalue	set “parameter” is used to set the value of the designated “parameter”
Response	**Description/Parameters**
parameter: value	The response for both the get and set commands provides the current parameter value.

If the WRM receives an invalid command or a command with an invalid or out of range parameter, it sends an error response. Figure 5-4 shows the response to an invalid command.

Figure 5-5. Invalid Command Parameter Response

Shows the response to an invalid parameter. A HD application may parse the response and check for the text “Unknown” or “Invalid” to determine if the command was rejected.

Figure 5-4. Invalid Command Response

```
wlan1 ->
wlan1 -> set wirelessmode 11z
Invalid parameter: 11z
List of valid parameter(s):
 wave                                   -- E2213-03
 11a                                    -- 802.11a
wlan1 ->
```

Figure 5-5. Invalid Command Parameter Response

5.3.3 Mode Commands

5.3.3.1 Get / Set Wireless Mode

This command gets or sets the WRM wireless mode (WAVE or 802.11a).

Table 5-3. Wireless Mode Command

Commands	**Description/Parameters**
get wirelessmode	Retrieve the current wireless mode
set wirelessmode wave	Begin operation in WAVE mode
set wirelessmode 11a	Begin operation in 802.11a mode
Response	**Description/Parameters**
Wireless LAN Mode: current mode	Current mode = WAVE, 11a

The following table lists the default parameter values in WAVE mode. These parameters are valid at first power up and can be modified using the CLI. The WRM saves its current configuration approximately every minute or upon a reboot command if any parameters have changed via the Telnet interface. At subsequent power ups, it will default to the last saved configuration.

Table 5-4. Default Parameter Values

Parameter	**Default Value**
Wireless Mode	WAVE
Unit Mode	OBU
Service Mode	Public Safety
Antenna	Best

Parameter	Default Value
Antenna1 Compensation	0 dB
Antenna2 Compensation	0 dB
Bandwidth (802.11a channels)	20 MHz
Channel	5890 MHz (IEEE 178) [Note: Channel 178 bandwidth is 10 MHz]
Data Rate	6 Mbps
Fragmentation Threshold	2346 bytes
Request to Send/Clear to Send (RTS/CTS) Threshold	2346 bytes
Transmit Power	20 dBm (at SMA antenna connector)

The Get/Set commands and responses described in the following sections are valid for WAVE mode. For the 802.11a mode, refer to the AR5002 AP User's Guide [5].

5.3.3.2 Get / Set Service Mode

This command gets or sets the WRM service mode (public safety or private service). This setting does not affect the current WRM functionality, but is implemented for future use.

Table 5-5. Service Mode Command

Commands	Description/Parameters
get servicemode	Retrieve current service mode
set servicemode public	Set WRM mode to public safety operation
set servicemode private	Set WRM mode to private service operation
Response	**Description/Parameters**
Service Mode: current mode	Current mode = public or private

5.3.3.3 Get / Set Unit Mode

This command gets or sets the WRM unit mode (OBU or RSU). The maximum allowable antenna input power is a function of channel and unit mode. Refer to Section 5.3.4.6 for details.

Table 5-6. Unit Mode Command

Commands	Description/Parameters
get unitmode	Retrieve current unit mode
set unitmode OBU	Set WRM to OBU mode
set unitmode RSU	Set WRM to RSU mode
Response	**Description/Parameters**
Unit Mode: current mode	Current mode = OBU or RSU

5.3.4 Parameter Commands

5.3.4.1 Get/Set Antenna

This command gets or sets the antenna configuration (best, 1, or 2). If antenna is set to best, antenna 1 is used for transmit and receive diversity is enabled. If the antenna is set to 1 or 2, the specified antenna is used for both transmit and receive.

Table 5-7. Antenna Command

Commands	Description/Parameters
get antenna	Retrieve current selected antenna
set antenna best	Transmit on antenna 1, enable receive diversity
set antenna 1	Transmit and receive on antenna 1
set antenna 2	Transmit and receive on antenna 2
Response	**Description/Parameters**
Antenna: current mode	Current mode = best, 1, or 2

5.3.4.2 Get/Set Antenna 1 Compensation

This command gets or sets the antenna 1 power compensation factor. This factor is the net gain or loss in dB between the WRM SMA connector and the antenna input due to cable losses and/or external amplifier gains. A positive value represents a gain and a negative value represents a loss. Section 5.3.4.6 describes how the WRM uses the power compensation factor to limit output power.

Table 5-8. Antenna 1 Compensation Factor Command

Commands	Description/Parameters
get antenna1comp	Retrieve the current antenna 1 power compensation factor
set antenna1comp xxx	Set antenna 1 power compensation factor to xxx dB (range = -10 thru +19)
Response	**Description/Parameters**
Antenna 1 comp: xxx dB	Current antenna 1 compensation factor in dB

5.3.4.3 Get/Set Antenna 2 Compensation

This command gets or sets the antenna 2 power compensation factor. See Section 5.3.4.3 for details.

Table 5-9. Antenna 2 Compensation Factor Command

Commands	Description/Parameters
get antenna2comp	Retrieve the current antenna 2 power compensation factor
set antenna2comp xxx	Set antenna 2 power compensation factor to xxx dB (range = -10 thru +19)
Response	**Description/Parameters**
Antenna 2 comp xxx dB	Current antenna 2 compensation factor in dB

5.3.4.4 Get/Set Bandwidth

This command gets or sets the channel bandwidth in MHz. This command is only valid for 802.11a channels (see

Table 5-13 for the list of 802.11a channels), which have a default bandwidth of 20 MHz. This command enables these channels to be used for either 10 or 20 MHz operation. Switching from 10 MHz to 20 MHz causes the WRM data rate to be doubled, while switching from 20 MHz to 10 MHz causes the data rate to be cut in half.

Table 5-10. Bandwidth Command

Commands	Description/Parameters
get bandwidth	Retrieve the current 802.11a channel bandwidth
set bandwidth 10	Set 802.11a channel bandwidth to 10 MHz
set bandwidth 20	Set 802.11a channel bandwidth to 20 MHz
Response	**Description/Parameters**
Channel Bandwidth: xx MHz	xx is the current bandwidth (10 or 20)

Get/Set Fast Channel

This command gets or sets the channel. Upon switching to a WAVE channel, the WRM will set the channel bandwidth to the value shown in Table 5-12. Upon switching to an 802.11a channel, the WRM will set the channel bandwidth based on the 802.11a bandwidth setting (refer to section 3.4.4 Get/Set Bandwidth). When switching from a 20 MHz to a 10 MHz channel, the WRM will halve the previous data rate. When switching from a 10 MHz to a 20 MHz channel, the WRM will double the previous data rate. The maximum allowable transmit power is a function of channel and unit mode. Refer to Section 5.3.4.6 for details. If the current transmit power setting exceeds the maximum allowed, the WRM will set the power to the maximum allowed.

Table 5-11. Fast Channel Command

Commands	**Description/Parameters**
get fastchannel	Retrieve the current channel
set fastchannel xxx	Set radio channel where xxx is one of the channel numbers specified in Table 5-12 or Table 5-13
Response	**Description/Parameters**
Radio Frequency: yyyy MHz (IEEE xxx)	yyyy is the frequency and xxx is the channel number specified in Table 5-12 or Table 5-13

Table 5-12. WAVE Channels

Channel Number	**Channel Frequency (MHz)**	**Bandwidth (MHz)**
172	5860	10
174	5870	10
175	5875	20
176	5880	10
178	5890	10
180	5900	10
181	5905	20

Channel Number	Channel Frequency (MHz)	Bandwidth (MHz)
182	5910	10
184	5920	10

Table 5-13. 802.11a Channels

Channel Number	Frequency (MHz)	Default Bandwidth (MHz)
52	5260	20
56	5280	20
60	5300	20
64	5320	20
149	5745	20
153	5765	20
157	5785	20
161	5805	20

5.3.4.5 Get / Set Fragment Threshold

This command gets or sets the MAC packet fragmentation length threshold. If the MAC frame length exceeds the threshold, the WRM will perform fragmentation. The valid range of values is 256 to 2346 bytes. This setting does not affect the current WRM functionality (no fragmentation is performed), but is implemented for future use.

Table 5-14. Fragmentation Threshold Command

Commands	Description/Parameters
get fragmentthreshold	Retrieve fragmentation threshold
set fragmentthreshold: xxxx	Set new fragmentation threshold where xxxx is the length in bytes
Response	**Description/Parameters**
Fragmentation Threshold: xxxx	xxxx is the length in bytes

5.3.4.6 Get/Set Power

This command gets or sets the transmit power in dBm (at the SMA antenna connector). The valid range is 0 to 20 dBm in 1 dB increments or full for maximum power. Full power may or may not be higher than 20 dBm.

Table 5-15. Transmit Power Command

Commands	Description/Parameters
get power	Retrieve current transmit power in dBm
set power xx	Set the transmit power to xx dBm (range = 0-20)
set power full	Set the transmit power to the maximum level
Response	**Description/Parameters**
Transmit Power: xx dBm Current Transmit Output Power yy dBm	xx is set the transmit power in dBm or full yy is the reduced transmit power, after any limiting has been applied

For 802.11a channel 64 (5320 MHz), the WRM limits the transmit output power at the SMA connector to 16 dBm, per the requirements of the FCC grant.

For WAVE channels, the ASTM E2213-03 specification [1] limits the maximum power. Table 5-16 lists the maximum antenna input power and Equivalent Isotropically Radiated Power (EIRP) where the same limit applies for all channel, unit mode, and service mode combinations. Table 5-17 lists the limits for public safety operation for channels not in Table 5-16. Table 5-18 lists the power limits for private service operation for channels not in Table 5-16.

The WRM calculates the maximum allowed output power at the SMA antenna connector based on the antenna input limits shown in the tables below and the Tx antenna compensation factor (see Sections 5.3.4.2 and 5.3.4.3). Specifically, the maximum output at the SMA connector is the antenna input limit minus the compensation factor. [Note: The EIRP values are listed for reference only. The WRM does not vary the maximum allowed output power based on service mode (i.e., public safety/private usage). As a result, Table 5-17 and 5-18 are treated identically within the WRM.]

As an example, suppose the antenna input limit for the current channel/unit mode combination is 10 dBm, antenna 1 is being used for Tx, and the antenna 1 compensation factor is +3 dB (net external gain of 3 dB). The maximum allowed output power at the SMA connector is 7 dBm. As a second example, suppose the antenna 1 compensation factor is –1 dB (net loss of 1 dB). The maximum allowed output power at the SMA connector would be 11 dBm.

If the WRM receives a set command for higher than the allowed output value at the SMA antenna connector, it will set the power to the highest allowed value. If the WRM receives a set command for lower than the allowed value, it will set the power to the specified value.

The WRM supports antenna compensation factors in the range –10 through +19 dB.

Table 5-16. Maximum Transmit Power Limits

WAVE Channel	Freq-uency (GHz)	Band-width (MHz)	RSU		OBU	
			Antenna Input (dBm)	EIRP (dBm)	Antenna Input (dBm)	EIRP (dBm)
172	5.860	10	28.8	33.0	28.8	33.0
174	5.870	10	28.8	33.0	28.8	33.0
175	5.875	20	10.0	23.0	10.0	23.0
176	5.880	10	28.8	33.0	28.8	33.0
180	5.900	10	10.0	23.0	20.0	23.0
181	5.905	20	10.0	23.0	20.0	23.0
182	5.910	10	10.0	23.0	20.0	23.0

Table 5-17. Maximum Transmit Power Limits for Public Safety

WAVE Channel	Freq-agency (GHz)	Band-width (MHz)	RSU		OBU	
			Antenna Input (dBm)	EIRP (dBm)	Antenna Input (dBm)	EIRP (dBm)
178	5.890	10	28.8	44.8	28.8	44.8
184	5.920	10	28.8	40.0	28.8	40.0

Table 5-18. Maximum Transmit Power Limits for Private Usage

WAVE Channel	Freq-uency (GHz)	Band-width (MHz)	RSU		OBU	
			Antenna Input (dBm)	EIRP (dBm)	Antenna Input (dBm)	EIRP (dBm)
178	5.890	10	28.8	33.0	28.8	33.0
184	5.920	10	28.8	33.0	28.8	33.0

5.3.4.7 Get / Set Rate

This command gets or sets the transmit data rate. For a set command, the data rate must be valid for the current channel bandwidth (10 or 20 MHz – see Section 5.3.4.4).

Table 5-19. Data Rate Command

Commands	Description/Parameters
get rate	Retrieve the current data rate
set rate xx	Set the current data rate to one of the rates specified in Table 5-20
Response	**Description/Parameters**
Data Rate: xx	xx is the data rate

Table 5-20. Data Rates

20 MHz Channel Data Rates (Mbps)	10 MHz Channel Data Rates (Mbps)
6	3
9	4.5
12	6
18	9
24	12
36	18
48	24
54	27

5.3.4.8 Get / Set RTS/CTS Threshold

This command gets or sets the RTS/CTS threshold in bytes. If the MAC frame length exceeds the threshold, the WRM will use RTS/CTS. The valid range of values is 256 to 2346 bytes. Per the ASTM E2213-03 specification [1], RTS/CTS is disabled on the WAVE control channel (channel 178).

Table 5-21. RTS/CTS Threshold Command

Commands	Description/Parameters
get rtsthreshold	Retrieve RTS/CTS threshold
set rtsthreshold: xxxx	Set the RTS/CTS threshold where xxxx is the length in bytes
Response	**Description/Parameters**
RTS/CTS Threshold: xxxx	xxxx is the length in bytes

5.3.4.9 Set WAVE Default Parameters

This command sets the WAVE parameters to the default values as specified in Table 5-4.

Table 5-22. WAVE Default Parameters Command

Commands	**Description/Parameters**
set WAVEdefault	Set the WRM to the WAVE default parameters specified in Table 5-4.
Response	**Description/Parameters**
<none>	

5.3.5 Status Commands

5.3.5.1 Get Configuration Parameters

This command gets the WRM configuration parameters.

Table 5-23. Configuration Parameters Command

Command	**Parameters**
get config	Retrieve WRM configuration parameters

The following is the list of WAVE-related parameters retrieved by the configuration command:

Table 5-24. Configuration Parameters Response

Response Parameters
Wireless Mode
Operational Mode
Wlan State
Antenna
Antenna1 Compensation Factor
Antenna2 Compensation Factor
Bandwidth
Channel/Frequency

Response Parameters
Data Rate
Fragment Threshold
RTS/CTS Threshold
Transmit Power
IP Address
Host IP address
HW Transmit Retry Limit
Service Mode
Unit Mode

5.3.5.2 Get Hardware Version

This command gets the WRM hardware version.

Table 5-25. Hardware Version Command

Command	Description/Parameters
get hardware	Retrieve hardware version
Response	**Description/Parameters**
wlan1 revisions: mac x.x phy y.y analog z.z PCI Vendor ID: aaaa, Device ID: bbbb Sub Vendor ID: cccc, Sub Device ID: dddd Chip is AR2312	x.x, y.y, z.z, aaaa. bbbb. cccc. dddd are the hardware versions for the different components

Get RSSI

This command gets the RSSI in dBm.

Table 5-26. RSSI Command

Command	**Parameters**
get rssi	Retrieve RSSI in dBm
Response	**Description/Parameters**
RSSI: xxx dBm	xxx is the current RSSI in dBm

5.3.5.3 Get Software Version

This command gets the WRM software version.

Table 5-27. Software Version Command

Command	**Description/Parameters**
Version	Retrieve the software version
Response	**Description/Parameters**
AP software: x.x.x.x WRM software: y.y <Time/Date of build>	x.x.x.x is the Atheros software version upon which the WRM software is based y.y is the Denso software version

5.3.6 Reboot Command

This command causes the WRM to reboot. The WRM will save the current configuration (if any changes were made via Telnet) and restore the configuration after the reset.

Table 5-28. Reboot Command

Command	**Description/Parameters**
Reboot	Reboot the WRM

5.4 WAVE Radio Module IP Interface

The WRM supports an IP packet interface to the HD. Refer to the IP specification [10] for detailed requirements. The HD and WRM use the IP interface to transfer data sent or received over the air. If the WRM is operating in WAVE mode, the WRM supports a modified version of the IP Options field in the IP header. WAVE Option types are used to support packet-by-packet control and status, and to set and get the radio configuration parameters.

5.4.1 IP Frame Format

Figure 5-6 illustrates the IPv4 frame format. All fields with the exception of the Protocol and IP Options fields must be set according to the IP specification. The Protocol field should be set to 0xff. The IP Options field optionally includes one of the WAVE options specified in section 5.4.2.

<table>
<tr><th>00</th><th>01</th><th>02</th><th>03</th><th>04</th><th>05</th><th>06</th><th>07</th><th>08</th><th>09</th><th>10</th><th>11</th><th>12</th><th>13</th><th>14</th><th>15</th><th>16</th><th>17</th><th>18</th><th>19</th><th>20</th><th>21</th><th>22</th><th>23</th><th>24</th><th>25</th><th>26</th><th>27</th><th>28</th><th>29</th><th>30</th><th>31</th></tr>
<tr><td colspan="4">Version</td><td colspan="4">IHL</td><td colspan="8">Type of Service</td><td colspan="16">Total Length</td></tr>
<tr><td colspan="16">Identification</td><td colspan="3">Flags</td><td colspan="13">Fragment Offset</td></tr>
<tr><td colspan="8">Time-To-Live</td><td colspan="8">Protocol</td><td colspan="16">Header Checksum</td></tr>
<tr><td colspan="32">Source IP</td></tr>
<tr><td colspan="32">Destination IP</td></tr>
<tr><td colspan="32">IP Options</td></tr>
<tr><td colspan="32">Payload</td></tr>
</table>

Figure 5-6. IPv4 Frame

5.4.2 WAVE Options

5.4.2.1 WAVE Tx Option

The WAVE Tx Option enables the HD to specify the radio configuration to be used for transmitting the packet, and to set the destination MAC address. This radio configuration will remain valid until a new configuration command is received or until the WRM is rebooted (this command does not save the configuration into non-volatile memory). Figure 5-7 illustrates the format of the WAVE Tx Option. Table 5-27 through Table 5-42 provide detailed field definitions.

<table>
<tr><th>00</th><th>01</th><th>02</th><th>03</th><th>04</th><th>05</th><th>06</th><th>07</th><th>08</th><th>09</th><th>10</th><th>11</th><th>12</th><th>13</th><th>14</th><th>15</th><th>16</th><th>17</th><th>18</th><th>19</th><th>20</th><th>21</th><th>22</th><th>23</th><th>24</th><th>25</th><th>26</th><th>27</th><th>28</th><th>29</th><th>30</th><th>31</th></tr>
<tr><td>C</td><td colspan="2">Class</td><td colspan="4">Option</td><td colspan="8">Length</td><td colspan="8">Channel</td><td colspan="8">Tx Power</td><td colspan="8">Data Rate</td></tr>
<tr><td colspan="16">Fragmentation Threshold</td><td colspan="16">RTS/CTS Threshold</td></tr>
<tr><td colspan="32">Destination MAC Address</td></tr>
<tr><td colspan="16">Destination MAC Address</td><td>SM</td><td>UM</td><td>ANT</td><td>BW</td><td colspan="12">RSV</td></tr>
</table>

Figure 5-7. WAVE Tx Option Format

Table 5-27. Copy (C) Flag Field Definition

Bits (00)	Description
0	Indicates option field is not to be copied into all IP Packet fragments.
1	Indicates option is to be copied into all IP Packet fragments.

Table 5-28. Class Field Definition

Bits (01-02)	Description
00-01	RESERVED.
10	Set this field to debugging and measurement.
11	RESERVED.

Table 5-29. Option Field Definition

Bits (03-07)	Description
11001	Set this field to 25.

Table 5-30 Length Field Definition

Bits (08-15)	Description
00010000	Set this field to 16 (option length in octets).

Table 5-31. WAVE Channel Field Definition

Bits (16-21)	Channel Number	Channel Frequency (MHz)
000000	172	5860
000001	174	5870
000010	175	5875
000011	176	5880
000100	178	5890
000101	180	5900
000110	181	5905
000111	182	5910
001000	184	5920

Table 5-32. 802.11a Channel Field Definition

Bits (16-21)	Channel Number	Channel Frequency (MHz)
001001	RESERVED	
001010	RESERVED	
001011	RESERVED	
001100	RESERVED	
001101	52	5260
001110	56	5280
001111	60	5300
010000	64	5320
010001	149	5745
010010	153	5765
010011	157	5785
010100	161	5805
010101-111111	RESERVED	

Table 5-33. Tx Power Field Definition

Bits (22-27)	Description
111111	Set the transmit power to the maximum level
xxxxxx	Set the transmit power to xxxxxx dBm.

Table 5-34. Data Rate Field Definition

Bits (28-31)	20 MHz Channel Data Rates (Mbps)	10 MHz Channel Data Rates (Mbps)
0000	RESERVED	
0001	6	3
0010	9	4.5
0011	12	6
0100	18	9
0101	24	12
0110	36	18
0111	48	24
1000	54	27
1001-1111	RESERVED	

Table 5-35. Fragmentation Threshold Field Definition

Bits (0-15)	Description
xxxxxx	Set fragmentation threshold where xxxxxx is the length in bytes. This setting does not affect the current WRM functionality, but is implemented for future use.

Table 5-36. RTS/CTS Threshold Field Definition

Bits (16-31)	Description
xxxxxx	Set the RTS/CTS threshold where xxxxxx is the length in bytes.

Table 5-37. Destination MAC Address Field Definition

Bits (00-31, 00-15)	Description
LSB to MSB 00-31, 00-15	Set destination MAC address.

Table 5-38. Service Mode (SM) Field Definition

Bits (16-17)	Description
00	Set WRM mode to public safety operation.
01	Set WRM mode to private service operation.
10-11	RESERVED

Table 5-39. Unit Mode (UM) Field Definition

Bits (18-19)	Description
00	Set WRM to OBU mode.
01	Set WRM to RSU mode.
10-11	RESERVED

Table 5-40. Antenna (ANT) Field Definition

Bits (20-21)	Description
00	Transmit and receive on antenna 1.
01	Transmit and receive on antenna 2.
10	Transmit on antenna 1, enable receive diversity.
11	RESERVED

Table 5-41. Bandwidth (BW) Field Definition

Bits (22-23)	Description
00	Set 802.11a channel bandwidth to 10 MHz.
01	Set 802.11a channel bandwidth to 20 MHz.
10-11	RESERVED

Table 5-42. Reserved (RSV) Field Definition

Bits (24-31)	Description
00	RESERVED

5.4.2.2 WAVE Rx Option

The WAVE Rx Option enables the WRM to send the RSSI, receive antenna, and the received MAC header to the HD. Figure 5-8 illustrates the format of the WAVE Rx Option. The Copy and Class fields must be set as described for the WAVE Tx Option. Table 5-43 through Table 5-47 provide detailed field definitions for the remaining fields.

<table>
<tr><th>00</th><th>01</th><th>02</th><th>03</th><th>04</th><th>05</th><th>06</th><th>07</th><th>08</th><th>09</th><th>10</th><th>11</th><th>12</th><th>13</th><th>14</th><th>15</th><th>16</th><th>17</th><th>18</th><th>19</th><th>20</th><th>21</th><th>22</th><th>23</th><th>24</th><th>25</th><th>26</th><th>27</th><th>28</th><th>29</th><th>30</th><th>31</th></tr>
<tr><td>C</td><td>Class</td><td colspan="6">Option</td><td colspan="8">Length</td><td colspan="16">RSSI</td></tr>
<tr><td colspan="32">Begin Received MAC Header</td></tr>
<tr><td colspan="32">:</td></tr>
<tr><td colspan="32">:</td></tr>
<tr><td colspan="32">:</td></tr>
<tr><td colspan="32">:</td></tr>
<tr><td colspan="32">:</td></tr>
<tr><td colspan="32">:</td></tr>
<tr><td colspan="16">End Received MAC Header</td><td>ANT</td><td colspan="15">RSV</td></tr>
</table>

Figure 5-8. WAVE RX Option Format

Table 5-43. Option Field Definition

Bits (03-07)	Description
11010	Set this field to 26.

Table 5-44. Length Field Description

Bits (08-15)	Description
00100100	Set this field to 36 (option length in octets).

Table 5-45. RSSI Field Definition

Bits (16-31)	Description
xxxxxxx	xxxxxxxx is the received packet RSSI in dBm (negative number in 2's complement representation).

Table 5-46. Received MAC Header Field Definition

Bits (00-31, 00-15)	Description
LSB to MSB 00-31, 00-15	Set to Received MAC Header (30 octets). Refer to Section 7 in IEEE 802.11 [3].

Table 5-47. Antenna (ANT) Field Definition

Bits (16-17)	Description
00	Frame was received on Antenna 1.
01	Frame was received on Antenna 2.
10-11	RESERVED

5.4.2.3 WRM Default Configuration Option

The WAVE Default Configuration Option enables the HD to set the radio configuration to the default values specified in Table 5-4. This command causes the WRM to save the default settings into non-volatile memory. Figure 5-9 illustrates the format of the WRM Default Configuration Option. The Copy and Class must be set as described for the WAVE Tx Option. Table 5-48 through Table 5-49 provide detailed field definitions of the Option and Length fields.

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
C	Class		Option					Length								RSV															

Figure 5-9. WRM Default Configuration Option Format

Table 5-48. Option Field Definition

Bits (03-07)	Description
11011	Set this field to 27.

Table 5-49. Length Field Definition

Bits (08-15)	Description
00000100	Set this field to 4 (option length in octets).

5.4.2.4 WRM Configuration Request Option

The WRM Configuration Request Option enables the HD to retrieve the WRM current radio configuration. Upon receiving the Configuration Request Option, the WRM returns the current WAVE configuration to the HD by sending a WRM Configuration Option in an IP frame (see Section 5.4.2.5). Figure 5-10 illustrates the format of the WRM Configuration Request Option. The Copy and Class must be set as described for the WAVE Tx Option. Table 5-50 through Table 5-51 provide detailed field definitions of the Option and Length fields.

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
C	Class		Option					Length								RSV															

Figure 5-10. WRM Configuration Request Option Format

Table 5-50. Option Field Definition

Bits (03-07)	Description
11100	Set this field to 28.

Table 5-51. Length Field Definition

Bits (08-15)	Description
00000100	Set this field to 4 (option length in octets).

5.4.2.5 WRM Configuration Option

The WRM Configuration Option is sent from the HD to the WRM to configure the radio with specified parameters and also sent from the WRM to the HD in response to a WRM Configuration Request. The radio configuration will remain valid until a new configuration command is received or until the WRM is rebooted (this command does not save the configuration into non-volatile memory). Figure 5-11 illustrates the format of the WRM Configuration Option. The Copy and Class must be set as described for the WAVE Tx Option. Table 5-31 through Table 5-41 provides detailed field definitions for the fields common with the Tx Option [Please note that the bit position of the parameters is different from the WAVE Tx Option but the field definitions remain the same]. Table 5-52 through Table 5-56 provide detailed field definitions for the fields unique to this message.

<table>
<tr><th colspan="8">00 01 02 03 04 05 06 07</th><th colspan="8">08 09 10 11 12 13 14 15</th><th colspan="8">16 17 18 19 20 21 22 23</th><th colspan="8">24 25 26 27 28 29 30 31</th></tr>
<tr><td>C</td><td colspan="2">Class</td><td colspan="4">Option</td><td colspan="8">Length</td><td colspan="8">Channel</td><td colspan="8">Tx Power</td><td colspan="8">Data Rate</td></tr>
<tr><td colspan="16">Fragmentation Threshold</td><td colspan="16">RTS/CTS Threshold</td></tr>
<tr><td colspan="2">SM</td><td colspan="2">UM</td><td colspan="2">ANT</td><td colspan="2">BW</td><td colspan="8">ANT1 COMP</td><td colspan="8">ANT2 COMP</td><td colspan="8">RSV</td></tr>
<tr><td colspan="32">Local MAC Address</td></tr>
<tr><td colspan="16">Local MAC Address</td><td colspan="16">RSV</td></tr>
</table>

Figure 5-11. WRM Configuration Option Format

Table 5-52. Option Field Definition

Bits (03-07)	Description
11101	Set this field to 29.

Table 5-53. Length Field Definition

Bits (08-15)	Description
00010100	Set this field to 20 (option length in octets).

Table 5-54. Antenna 1 Compensation Factor Field

Bits (08-15)	Description
xxxxxxxx	xxxxxxxx is the antenna 1 compensation factor in dB (positive/negative numbers are in 2's complement representation).

Table 5-55. Antenna 2 Compensation Factor Field

Bits (16-23)	Description
xxxxxxxx	xxxxxxxx is the antenna 2 compensation factor in dB (positive/negative numbers are in 2's complement representation).

Table 5-56. Local MAC Address Field Definition Field

Bits (00-31, 00-15)	Description
LSB to MSB 00-31, 00-15	Contains the local WRM's MAC address. This field is only valid when sent from the WRM to the HD. It is unused when sent from the HD to WRM.

6 ACCEPTANCE TESTING

This chapter provides the Acceptance Test Plan (ATP) and test results for the WAVE Radio Module delivered in accordance with the VSC Project: Preliminary Requirements for Second Generation WAVE Radio Module [Section 1.2].

6.1 Scope

This WAVE Radio Module (WRM) ATP defines the tests Denso conducted to verify WRM compliance with the WAVE Radio Module Interface Specification (Chapter 5) and the software requirements of the WAVE Radio Module Functional Specification (Chapter 3). This test plan is intended to globally verify the software build which is delivered with each WRM, not to verify operation of each delivered unit. A separate set of tests was executed to verify selected functions of each delivered WRM.

As a separate task, Denso conducted tests on a limited number of units to verify whether the WRM hardware (purchased from Atheros) meets the RF performance requirements of the Functional Specification (which references ASTM E2213-03 [1]). Denso documented any areas of non-compliance in the Functional Specification.

6.2 Test Configurations

This section describes how to connect a host device to a WRM. It also describes the test setups and initialization procedures required by the tests specified in subsequent chapters.

6.2.1 WAVE Radio Module Network Connection

Set up each Host Device (HD) and WRM as shown in Figure 6-1. Each HD and WRM must have a unique IP address. Configure the HD Internet Protocol (IP) address to 192.168.001.1xx, where xx is the unit number assigned by Denso. Configure each HD with a Subnet Mask of 255.255.255.000.

6.2.2 Test Setups

For all test setups, each HD is connected to its corresponding WRM using an Ethernet crossover cable. Each HD has the API Tester and Ethereal software installed. Ethereal is a software network analyzer that may be downloaded at no charge from www.ethereal.com. The test procedures use Ethereal to verify the contents of the IP packets exchanged between the HD and the WRM. The WRM is powered using a wall power supply. See Figure 6-1. For figures illustrating subsequent test setups, the crossover cable is not labeled and the API Tester, Ethereal, and the power supply are not shown for simplicity. Unless otherwise specified, 5 dBi dipole antennas are used for both antenna 1 and antenna 2.

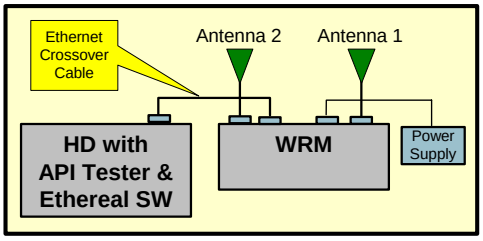


Figure 6-1. Single WRM Test Setup

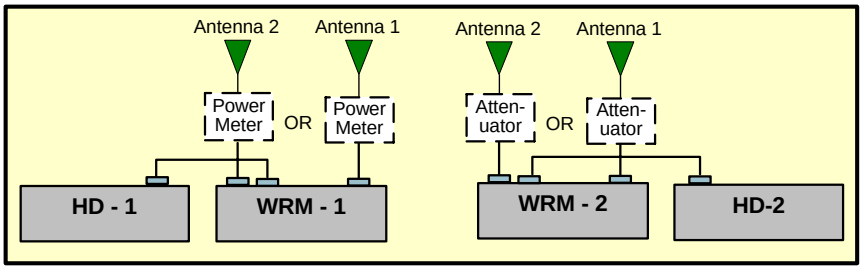


Figure 6-2. WRMs with Power Meter and Attenuator Test Setup

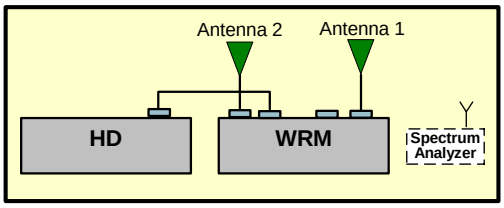


Figure 6-3. WRM with Spectrum Analyzer Test Setup

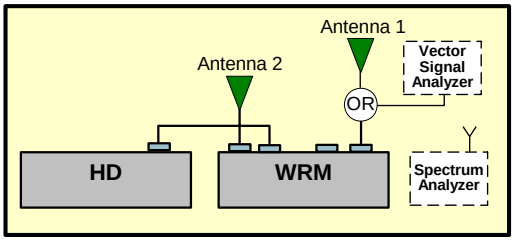


Figure 6-4. WRM with Spectrum Analyzer and Vector Signal Analyzer Test Setup

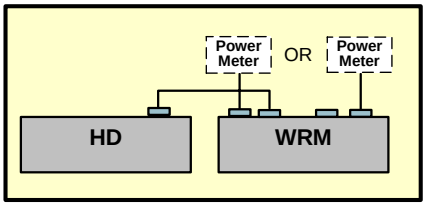


Figure 6-5. WRM with Power Meter Test Setup

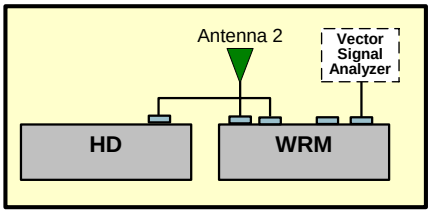


Figure 6-6. WRM with Vector Signal Analyzer Test Setup

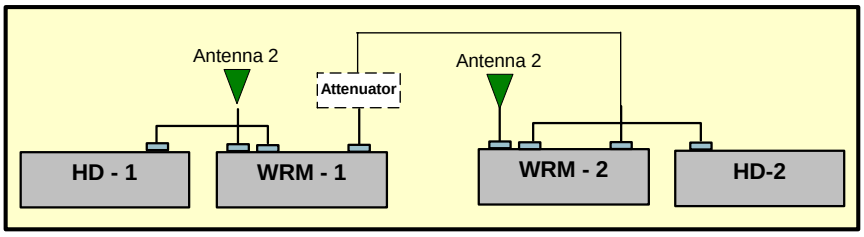


Figure 6-7. WRMs with Cable Connection

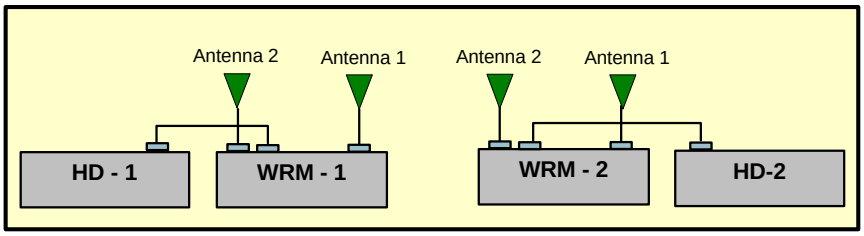


Figure 6-8. Dual WRMs

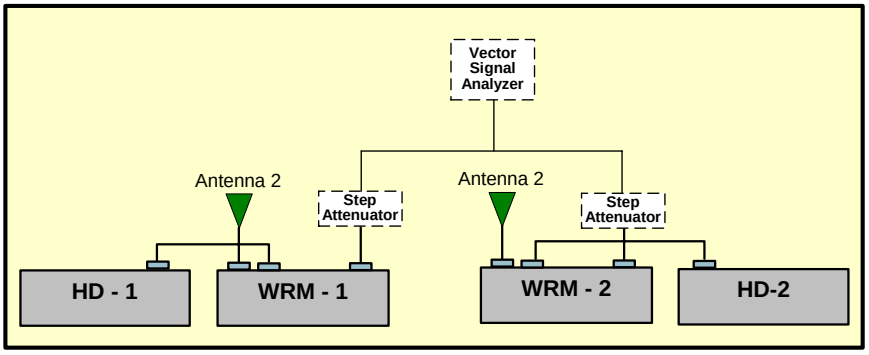


Figure 6-9. WRMs with Step Attenuators and Vector Signal Analyzer Test Setup

6.2.3 Initialization Procedures

This section defines the procedures that are used to configure the hardware and software to a known state prior to starting a test. The tests in subsequent chapters refer to these procedures when required.

6.2.3.1 Telnet Initialization Procedure

Table 6-1. Telnet Initialization Procedure

#	Description	Test Steps	Expected Results
1.	Initialize HD.	1. If it is not already running, launch the API Tester application. 2. Select the API Tester Telnet display. 3. If it is not already running, launch the Ethereal application.	The HD displays the API Tester GUI for Telnet commands/responses and the Ethereal GUI.
2.	Initialize WRM.	1. Use the API Tester to send the *set WAVEdefault* Telnet command.	API Tester displays response: *WAVEdefault.* The WRM reboots after receiving the command.

6.2.3.2 IP Initialization Procedure

Table 6-2. IP Initialization Procedure

#	Description	Test Steps	Expected Results
1.	Initialize HD.	1. If it is not already running, launch the API Tester application. 2. Select the API Tester IP display. 3. If it is not already running, launch the Ethereal application.	The HD displays the API Tester GUI for IP commands/responses and the Ethereal GUI.
2.	Initialize WRM.	1. If the WRM is not in WAVE mode, select the API Tester Telnet display and send the *set wirelessmode WAVE* Telnet command. Return to the API Tester IP display.	If the command is sent, API Tester displays WRM response: *Wireless Mode: WAVE*. The WRM reboots after receiving the command.
		2. Use the API Tester to configure the WRM to the WAVE default configuration.	The WRM reboots after receiving the command.
		3. Use the API Tester to get the current WRM configuration.	API Tester displays the current WRM configuration. The parameter values match Table 6-3.

Table 6-3. WAVE Default Parameters

Parameter	Default Value
Wireless Mode	WAVE
Unit Mode	OBU
Service Mode	Public Safety
Antenna	Best
Antenna1 Compensation	0 dB
Antenna2 Compensation	0 dB
Bandwidth *[used for 802.11a channels only]*	20 MHz
Channel	5890 MHz (IEEE 178) *[Note: Channel 178 bandwidth is 10MHz.]*
Data Rate	6 Mbps
Fragmentation Threshold	2346 bytes
Request to Send/Clear to Send (RTS/CTS) Threshold	2346 bytes
Transmit Power	20 dBm (at SMA antenna connector)

6.2.4 Software Builds

Record the WRM software version and the API Tester software version.

Table 6-4. WRM and API Tester Software Versions

WRM Software Version	API Tester Software Version	WRM Unit Number	Tests
VSCC_WRM_V0.1	VSCC API TESTER V0.1	11	6.3.3.5 (Fastchannel)
VSCC_WRM_V0.2	VSCC API TESTER V0.1	13 (WRM 1), 11 (WRM 2), 4 (WRM 3), 8 (WRM , 4 (WRM 3), 8 (WRM 4), 5 (WRM 5), 9 (WRM 6)	All other tests
VSCC_WRM_V0.2	VSCC API TESTER V0.2	13	6.3.3.4 (Bandwidth)
VSCC_WRM_V0.2	VSCC API TESTER V0.2	4	6.4.2 (MAC Address)

6.3 WRM Interface Specification Tests

This section specifies the tests to verify the WRM Interface Specification requirements. The tests get and set WRM parameters using Telnet commands and IP frames with WAVE options. The tests also verify the WRM supports transmitting and receiving IP frames with and without packet-by-packet (PBP) control and status. Refer to Section 3 of the WRM Interface Specification (Chapter 5) for the Telnet requirements and Section 4 for the IP requirements.

The subsections below define the following types of tests:

1. Telnet Tests: The Telnet tests use the API Tester to send “get” and “set” commands and display the WRM response. For set commands, the tests also verify the WRM modifies its configuration to the specified parameter values. The API Tester sends packets (i.e., IP frames with a data payload) without PBP control to the WRM for transmission, and test equipment measurements verify the configuration.
2. IP Configuration Tests: The IP Configuration Tests use the API tester to send IP frames with the WRM Configuration Option (WCO) to set the WRM configuration. The API tester gets the WRM configuration by sending an IP frame with the WRM Configuration Request Option (WCRO). The WRM responds with an IP frame with the WCO and the API tester displays the contents. The tests use Ethereal to verify the WCO and WCRO fields.

   The tests also verify the WRM modifies its configuration to the specified parameter values. The API Tester sends packets without PBP control to the

WRM for transmission, and test equipment measurements verify the configuration.

3. IP Packet-by-Packet Tests: The IP PBP Tests verify both PBP control and PBP status. For PBP control verification, the tests use the API tester to send IP frames with the WAVE Tx Option (WTXO) and a data payload to the WRM for transmission. The tests use Ethereal to verify the WTXO fields. Test equipment measurements verify the WRM configuration complies with the values specified by the WTXO.

   For PBP status verification, the test setup consists of two WRMs and their associated HDs. One WRM transmits packets with PBP control. When the second WRM receives a packet with a WTXO, it modifies the IP header by deleting the WTXO and adding the WAVE Rx Option (WRXO) before sending the packet to the HD. The tests use Ethereal to verify the WRXO fields, and also confirm the field values on the API tester display. Test equipment measurements verify the WRXO values are consistent with the receive environment.

For all of the WAVE options, the first test using the option verifies the fields with fixed values (e.g., option number, option length). Subsequent tests do not repeat this verification.

The API Tester uses all of the IP API function calls and Telnet API function calls to support the ATP. Table 6-65 and Table 6-6 describe when the calls are executed.

Table 6-5. IP API Function Calls

IP API Function Calls	When Executed
`init_WAVE_comm ()`	Executed during API Tester initialization.
`term_WAVE_comm ()`	Executed during API Tester exit.
`set_WRM_WAVEdefault ()`	Executed during 6.3.1.2 WAVEdefault IP Configuration Test.
`set_WRM_configuration ()`	Executed during all IP Configuration Tests where the WCO option is sent by the HD to the WRM.
`get_WRM_configuration ()`	Executed during all IP Configuration Tests where the WCO option is sent by the WRM to the HD.
`send_WAVE_tx_pkt ()`	Executed during all IP Configuration Tests and IP PBP Tests where packets are broadcast with PBP control.
`send_WAVE_tx_pkt_wo_config ()`	Executed during all Telnet, IP Configuration, and IP PBP Tests where packets are broadcast without PBP control.
`check_WAVE_rx_pkt ()`	Executed during all tests where packets are received by the API Tester.
`receive_WAVE_rx_pkt ()`	Executed during all tests where packets are received by the API Tester.

Table 6-6. Telnet API Function Calls

Telnet API Function Calls	When Executed
`init_telnet_comm ()`	Executed during API Tester initialization
`term_telnet_comm ()`	Executed during API Tester exit
`set_telnet_cmd ()`	Executed once each time the API Tester executes a *set* Telnet command, where the *set* command requires a parameter.
`send_telnet_cmd ()`	Executed once each time the API Tester executes a *set* Telnet command, where the *set* command does not require a parameter.
`get_telnet_cmd ()`	Executed each time the API Tester sends a *get* Telnet command to the WRM.
`get_telnet_rsp ()`	Executed after each *get* Telnet command to retrieve the parameter requested by the API Tester.
`check_telnet_rsp ()`	Executed after each *get* Telnet command to check if the WRM has responded to the request posted by the API Tester.

6.3.1 WAVE Default Command

Verify the WRM sets the WAVE parameters to the default values. This command is used to initialize the WRM to a known state at the beginning of all other tests. This command is not available with PBP control.

6.3.1.1 WAVEdefault Telnet Test

Table 6-7. WAVEdefault Telnet Test

#	Description	Test Steps	Expected Results	Actual Results
	Initialization	1. Use the test setup shown in Figure 6-1. Single WRM Test Setup. 2. Execute Telnet initialization procedure in Section 6.2.3.1.	WRM reboots.	WRM reboots.
1.	Verify default parameters	1. Use API Tester to send *get config* command and verify WRM response.	API Tester displays configuration data including default parameter values listed in Table 6-3.	Results match table 2-3.
	Verify WRM operation for key default parameters (other parameters will be tested in subsequent tests).	2. Use the test setup shown in Figure 6-4. WRM with Spectrum Analyzer and Vector Signal Analyzer Test Setup. 3. Use the API Tester to continuously broadcast packets w/o PBP control.	N/A	N/A
		4. Use the spectrum analyzer to verify channel frequency and bandwidth.	Spectrum analyzer shows center frequency of 5890 MHz and 10 MHz BW.	Center frequency = 5890 MHz. BW = 10 MHz
		5. Use the VSA to verify data rate.	VSA shows data rate of 6 Mbps.	6 Mbps
		6. Use the API tester to stop packet broadcast.	N/A	N/A
		7. Use the test setup shown in Figure 6-5. WRM with Power Meter Test Setup, with the power meter connected to the antenna 1 SMA connector. 8. Use the API Tester to continuously broadcast packets w/o PBP control. 9. Use the power meter to measure output power. 10. Use the API Tester to stop packet broadcast.	Power meter shows output power of 20dBm +\- 1 dB.	20.0 dBm

#	Description	Test Steps	Expected Results	Actual Results
	Modify configuration.	11. Use API Tester to send the following commands and display WRM response: • *set unitmode RSU* • *set servicemode private* • *set antenna 1* • *set antenna1comp 2* • *set antenna2comp –4* • *set fastchannel 52* • *set bandwidth 10 MHz* • *set rate 12 Mbps* • *set fragmentthreshold 300* • *set rtsthreshold 400* • *set power 10*	API Tester displays WRM responses echoing new settings after each *set* command.	All Telnet set and get commands correctly set and report the parameter changes.
	Verify modified configuration	12. Use the API Tester to send the *get config* command and verify the WRM response.	API Tester displays configuration data including parameter values as set in step 10.	All parameters match the values indicated in step 10.
	Verify WRM operation for key parameters.	13. Repeat test steps 2-10.	Test equipment measurements confirm values set in step 10.	Record the results in Table 6-8
	Verify WRM response to *set WAVEdefault* command.	14. Use the API Tester to send the *set WAVEdefault* Telnet command and verify the WRM response.	API Tester displays *WAVEdefault* and WRM reboots.	WRM reboots.
	Get configuration and verify default parameters.	15. Use API Tester to send *get config* command and verify WRM response.	API Tester displays configuration data including default parameter values listed in Table 6-3.	Results match default values listed in Table.
	Verify WRM operation for key parameters.	16. Repeat test steps 2-10.	Test equipment measurements confirm values in Table 6-3.	Record the results in **Error! Reference source not found.**.

Table 6-8. WAVEdefault Telnet Test Results – Modified Parameters

Settings	Expected Results	Actual Results
Frequency (MHz)	5260	5260 MHz
Bandwidth (MHz)	10	10 MHz
Data Rate	12	12 Mbps
Antenna 1 Tx Power (dBm)	10	10.4 dBm

Table 6-9. WAVEdefault Telnet Test Results – Default Parameters

Settings	Expected Results	Actual Results
Frequency (MHz)	5890	5890 MHz
Bandwidth (MHz)	10	10 MHz
Data Rate	6	6 Mbps
Antenna 1 Tx Power (dBm)	20	20.0 dBm

6.3.1.2 WAVEdefault IP Configuration Test

Table 6-10. WAVEdefault IP Configuration Test

#	Description	Test Steps	Expected Results	Actual Results
	Initialization	1. Use the test setup shown in Figure 6-1. Single WRM Test Setup. 2. Execute IP initialization procedure in Section 0.	WRM reboots.	WRM reboots.
1.	Verify default configuration.	1. Use API Tester to get WRM configuration and verify WRM response.	API Tester displays configuration data including default parameter values listed in Table 6-3.	Results match default values listed in Table.
	Verify WRM operation for key parameters.	2. Execute Table 6-7, Test Case # 1, test steps 2-10.	Test equipment measurements confirm values in Table 6-3.	Record results in Table 6-11
	Modify configuration.	3. Use API Tester to configure the WRM with the following parameter settings: • *unitmode RSU* • *servicemode private* • *antenna 1* • *antenna1comp 2* • *antenna2comp –4* • *fastchannel 52* • *bandwidth 10* • *rate 12* • *fragmentthreshold 300* • *rtsthreshold 400* • *power 10*	N/A	N/A
	Verify modified configuration	4. Use the API Tester to get the current WRM configuration.	API Tester displays configuration data including parameter values as set in step 3.	Record results in Table 6-12

#	Description	Test Steps	Expected Results	Actual Results
	Set WRM to default settings.	5. Use the API Tester to configure the WRM to the default settings. 6. Use Ethereal to verify the fixed value WDCO fields.	API Tester sends WAVE Default Configuration Option (WDCO) with the C field (Word 1, bit 00) set to copy (1), Class field (Word 1, bits 01-02) set to debugging and measurement (10), Option field (Word 1, bits 03-07) set to 27, Length field (Word 1, bits 08-15) set to 4, and RSV field (Word 1, bits 16-31 set to 0.	DB 04 00 00 **1101 1011** **0000 0100** **0000 0000** **0000 0000**
	Get configuration and verify default parameters.	7. Use API Tester to get the WRM configuration.	API Tester displays configuration data including default parameter values listed in Table 6-3.	Results match default values listed in Table.
	Verify default configuration.	8. Execute Table 6-7, Test Case # 1, test steps 2-10.	Test equipment measurements confirm values in Table 6-3.	Record results in Table 6-13

Table 6-11. WAVEdefault IP Configuration Test Results – Initial Values

Settings	Expected Results	Actual Results
Frequency (MHz)	5890	5890 MHz
Bandwidth (MHz)	10	10 MHz
Data Rate	6	6 Mbps
Antenna 1 Tx Power (dBm)	20	19.9 dBm

Table 6-12. WAVEdefault IP Configuration Test Results - Modified Parameters

Settings	Expected Results	Actual Results
Unitmode	RSU	RSU
Servicemode	Private	Private
Antenna	1	1
Antenna 1 Compensation	2	2
Antenna 2 Compensation	-4	-4
Bandwidth	10	10
Channel	52	52 (5260 MHz)

Settings	Expected Results	Actual Results
Data Rate	12	12
Fragmentation Threshold	300	300
RTS/CTS Threshold	400	400
Tx Power	10	10

Table 6-13. WAVEdefault IP Configuration Test Results - Default Parameters

Settings	Expected Results	Actual Results
Frequency (MHz)	5890	5890 MHz
Bandwidth (MHz)	10	10 MHz
Data Rate	6	6 Mbps
Antenna 1 Tx Power (dBm)	20	20.1 dBm

6.3.2 Mode Commands

6.3.2.1 Wireless Mode

Verify the WRM response to commands to get and set the wireless mode to 802.11a [2] or WAVE. After receiving a set wireless mode command, verify the WRM begins operation in the new mode within 10 seconds after receiving a reboot command. Verification of 802.11a functionality is not within the scope of this ATP. The scope of this ATP is limited to verifying the response to the mode change requests. The complete set of tests specified in this test plan verifies WAVE functionality. This command is only available through the Telnet interface.

Test Cases:

1. Wireless Mode 802.11a
2. Wireless Mode WAVE

Table 6-14. Wireless Mode Telnet Test

#	Description	Test Steps	Expected Results	Actual Results
	Initialization.	1. Use the test setup shown in Figure 6-1. Single WRM Test Setup. 2. Execute Telnet initialization procedure in Section 6.2.3.1.	N/A	N/A
1.	Verify WRM response to *set wirelessmode 11a* command.	1. Use the API Tester to send the *set wirelessmode 11a* Telnet command and verify theWRM reboots.	API Tester sets Wireless Mode to 11a and reboots.	WRM rebooted.
	Verify WRM response to *get wirelessmode* command.	2. Use the API Tester to send the *get wirelessmode* Telnet command and verify the response. Send the command 10 seconds after the reboot command.	API Tester displays response: *Wireless Mode: 11a*.	Wireless LAN Mode: 802.11a
2.	Verify WRM response to *set wirelessmode WAVE* command.	1. Use the API Tester to send the *set wirelessmode WAVE* Telnet command and verify the WRM reboots.	API Tester sets Wireless Modeto WAVE and reboots.	WRM reboots.
	Verify WRM response to *get wirelessmode* command.	2. Use the API Tester to send the *get wirelessmode* Telnet command and verify the response. Send the command 10 seconds after the reboot command.	API Tester displays response: *Wireless Mode: WAVE*.	Wireless LAN Mode: WAVE

6.3.2.2 Service Mode

Verify the WRM response to commands to get and set the service mode to public safety or private service. This setting does not affect the current WRM functionality, but is implemented for future use.

Test Cases:

1. Service Mode Private
2. Service Mode Public Safety

Service Mode Telnet Test

Table 6-15. Service Mode Telnet Test

#	Description	Test Steps	Expected Results	Actual Results
	Initialization.	1. Use the test setup shown in Figure 6-1. Single WRM Test Setup. 2. Execute Telnet initialization procedure in Section 6.2.3.1.	N/A	N/A
1.	Verify WRM response to *set servicemode private* command.	1. Use the API Tester to send the *set servicemode private* Telnet command and verify the response.	API Tester displays response: *Service Mode: private*.	Service Mode: private
	Verify WRM response to *get servicemode* command.	2. Use the API Tester to send the *get servicemode* Telnet command and verify the response.	API Tester displays response: *Service Mode: private*.	Service Mode: private
2.	Verify WRM response to *set servicemode public* command.	1. Use the API Tester to send the *set servicemode public* Telnet command and verify the response.	API Tester displays response: *Service Mode: public*.	Service Mode: public
	Verify WRM response to *get servicemode* command.	2. Use the API Tester to send the *get servicemode* Telnet command and verify the response.	API Tester displays response: *Service Mode: public*.	Service Mode: public

Service Mode IP Configuration Test

Table 6-16. Service Mode IP Configuration Test

#	Description	Test Steps	Expected Results	Actual Results
	Initialization.	1. Use the test setup shown in Figure 6-1. Single WRM Test Setup. 2. Execute IP initialization procedure in Section 6.2.3.2.	N/A	N/A
1.	Set WRM *service mode* to *private*	1. Use the API Tester to set the WRM configuration with the *service mode* field set to *private*. 2. Use Ethereal to verify the fixed value fields in the WCO sent from the API Tester to the WRM.	API Tester sends WCO with the C field (Word 1, bit 00) set to copy (1), Class field (Word 1, bits 01-02) set to debugging and measurement (10), Option field (Word 1, bits 03-07) set to 29, Length field (Word 1, bits 08-15) set to 20, and RSV fields (Word 3, bits 24-31 and Word 5, bits 16-31) set to 0.	(W1) DD 14 11 43 1101 1101 0001 0100 0001 0001 0100 0011 (W2) 09 2A 09 2A (W3) 49 00 00 00 (W4) 00 00 00 00 (W5) 00 00 00 00
		3. Use Ethereal to verify the WCO service mode field.	API Tester sends WCO with service mode field (Word 3, bits 00-01) set to private (01).	(W3) 49 00 00 00 0100 1001
	Verify WRM response to *service mode private* command.	4. Use the API Tester to get the WRM configuration and verify the response.	API Tester displays service mode as private.	Private
		5. Use Ethereal to verify the WCRO fixed value fields.	API Tester sends WCRO with the C field (Word 1, bit 00) set to copy (1), Class field (Word 1, bits 01-02) set to debugging and measurement (10), Option field (Word 1, bits 03-07) set to 28, Length field (Word 1, bits 08-15) set to 4, and RSV field (Word 1, bits 16-31) set to 0.	DC 04 00 00 1101 1100 0000 0100 0000 0000 0000 0000
		6. Use Ethereal to verify the fixed value fields in the WCO sent from the WRM to the API Tester.	WRM sends WCO with the values set as described for test steps 1-2.	(W1) DD 14 11 43 (W2) 09 2A 09 2A (W3) 49 00 00 00 (W4) DA 21 3F CF (W5) 9D 5D 00 00

#	Description	Test Steps	Expected Results	Actual Results
		7. Use Ethereal to verify the WCO service mode field.	WRM sends WCO with service mode field (Word 3, bits 00-01) set to private (01).	(W3) 49 00 00 00 0100 1001 0000 0000
2.	Set WRM *service mode* to *public*	1. Use the API Tester to set the WRM configuration with the *service mode* field set to *public*. 2. Use Ethereal to verify the WCO service mode field.	API Tester sends WCO with service mode field (Word 3, bits 00-01) set to public (00).	(W3) 09 00 00 00 0000 1001 0000 0000
	Verify WRM response to *service mode public* command.	3. Use the API Tester to get the WRM configuration and verify the response.	API Tester displays service mode as public.	Public
		4. Use Ethereal to verify the WCO service mode field.	WRM sends WCO with the service mode field (Word 3, bits 00-01) set to public (00).	(W3) 09 00 00 00 0000 1001 0000 0000

Service Mode IP Packet-by-Packet Test

Table 6-17. Service Mode IP Packet-by-Packet Test

#	Description	Test Steps	Expected Results	Actual Results
	Initialization.	1. Use the test setup shown in Figure 6-1. Single WRM Test Setup. 2. Execute IP initialization procedure in Section 6.2.3.2.	N/A	N/A
1.	Send packet with *service mode* set to *private*	1. Use the API Tester to set the *service mode* to *private* and transmit one packet with PBP control. 2. Use Ethereal to verify the fixed value fields in the WTXO.	API Tester sends WTXO with the C field (Word 1, bit 00) set to copy (1), Class field (Word 1, bits 01-02) set to debugging and measurement (10), Option field (Word 1, bits 03-07) set to 25, Length field (Word 1, bits 08-15) set to 16, and RSV field (Word 4, bits 24-31) set to 0.	(W1) D9 10 11 43 1101 1001 0001 0000 0001 0001 0100 0011 (W2) 09 2A 09 2A (W3) FF FF FF FF (W4) FF FF 49 00 1111 1111 1111 1111 0100 1001 0000 0000
		3. Use Ethereal to verify the WTXO service mode field.	API Tester sends WTXO with service mode field (Word 4, bits 16-17) set to private (01).	(W4) FF FF 49 00 1111 1111 1111 1111 0100 1001 0000 0000
	Verify WRM configuration.	4. Use the API Tester to get the WRM configuration and verify the response.	API Tester displays service mode as private.	Private

#	Description	Test Steps	Expected Results	Actual Results
2.	Send packet with *service mode* set to *public*	1. Use the API Tester to set the *service mode* to *public* and transmit one packet with PBP control. 2. Use Ethereal to verify the WTXO service mode field.	API Tester sends WTXO with service mode field (Word 4, bits 16-17) set to public (00).	(W4) 00 00 00 00
	Verify WRM configuration.	3. Use the API Tester to get the WRM configuration and verify the response.	API Tester displays service mode as public.	Public

6.3.2.3 Unit Mode

Verify the WRM response to commands to get and set the unit mode to OBU or RSU. The Unit Mode setting affects the maximum output power, which is verified in Section 6.2.3.2 and the random MAC address generation, which is verified in Section 6.4.2.

Test Cases:

1. Unit Mode RSU
2. Unit Mode OBU

Unit Mode Telnet Test

Table 6-18. Unit Mode Telnet Test

#	Description	Test Steps	Expected Results	Actual Results
	Initialization.	1. Use the test setup shown in Figure 6-1. Single WRM Test Setup. 2. Execute Telnet initialization procedure in Section 6.2.3.1.	N/A	N/A
1.	Verify WRM response to *set unitmode RSU* command.	1. Use the API Tester to send the *set unitmode RSU* Telnet command and verify the response.	API Tester displays response: *Unit Mode: RSU*.	Unit Mode: RSU
	Verify WRM response to *get unitmode* command.	2. Use the API Tester to send the *get unitmode* Telnet command and verify the response.	API Tester displays response: *Unit Mode: RSU*.	Unit Mode: RSU
2.	Verify WRM response to *set unitmode OBU* command.	1. Use the API Tester to send the *set unitmode OBU* Telnet command and verify the response..	API Tester displays response: *Unit Mode: OBU*.	Unit Mode: OBU

#	Description	Test Steps	Expected Results	Actual Results
	Verify WRM response to *get unitmode* command.	2. Use the API Tester to send the *get unitmode* Telnet command and verify the response.	API Tester displays response: *Unit Mode: OBU*.	Unit Mode: OBU

Unit Mode IP Configuration Test

Table 6-19. Unit Mode IP Configuration Test

#	Description	Test Steps	Expected Results	Actual Results
	Initialization.	1. Use the test setup shown in Figure 6-1. Single WRM Test Setup. 2. Execute IP initialization procedure in Section 6.2.3.2.	N/A	N/A
1.	Set WRM *unit mode* to *RSU*	1. Use the API Tester to set the WRM configuration with the *unit mode* field set to *RSU*. 2. Use Ethereal to verify the unit mode field.	API Tester sends WCO with unit mode field (Word 3, bits 02-03) set to RSU (01).	(W3) 19 00 00 00 0001 1001 0000 0000
	Verify WRM response to *unit mode RSU* command.	3. Use the API Tester to get the WRM configuration and verify the response.	API Tester displays unit mode as RSU.	RSU
		4. Use Ethereal to verify the WCO unit mode field.	WRM sends WCO with the unit mode field (Word 3, bits 02-03) set to RSU (01).	(W3) 19 00 00 00 0001 1001 0000 0000
2.	Set WRM *unit mode* to *OBU*	1. Use the API Tester to set the WRM configuration with the *unit mode* field set to *OBU*. 2. Use Ethereal to verify the WCO unit mode field.	API Tester sends WCO with unit mode field (Word 3, bits 02-03) set to OBU (00).	(W3) 09 00 00 00 0000 1001 0000 0000
	Verify WRM response to *unit mode OBU* command.	3. Use the API Tester to get the WRM configuration and verify the response.	API Tester displays unit mode as OBU.	OBU
		4. Use Ethereal to verify the WCO unit mode field.	WRM sends WCO with the unit mode field (Word 3, bits 02-03) set to OBU (00).	(W3) 09 00 00 00 0000 1001 0000 0000

6.3.2.4 Unit Mode IP Packet-by-Packet Test

Table 6-20. Unit Mode IP Packet-by-Packet Test

#	Description	Test Steps	Expected Results	Actual Results
	Initialization.	1. Use the test setup shown in Figure 6-1. Single WRM Test Setup. 2. Execute IP initialization procedure in Section 6.2.3.2.	N/A	N/A
1.	Send packet with *unit mode* set to *RSU*.	1. Use the API Tester to set the *unit mode* to *RSU* and transmit one packet with PBP control. 2. Use Ethereal to verify the WTXO unit mode field.	API Tester sends WTXO with unit mode field (Word 4, bits 18-19) set to RSU (01).	(W4) FF FF 19 00 1111 1111 1111 1111 0001 1001 0000 0000
	Verify WRM configuration.	3. Use the API Tester to get the WRM configuration and verify the response.	API Tester displays unit mode as RSU.	RSU
2.	Send packet with *unit mode* set to *OBU*.	1. Use the API Tester to set the *unit mode* to *OBU* and transmit one packet with PBP control. 2. Use Ethereal to verify the WTXO unit mode field.	API Tester sends WTXO with unit mode field (Word 4, bits 18-19) set to OBU (00).	(W4) FF FF 09 00 1111 1111 1111 1111 0000 1001 0000 0000
	Verify WRM configuration.	3. Use the API Tester to get the WRM configuration and verify the response.	API Tester displays unit mode as OBU.	OBU

6.3.3 Parameter Commands

6.3.3.1 Antenna Configuration

Verify the WRM response to commands to get and set the antenna configuration. The WRM supports transmit and receive on a single antenna (antenna 1 or 2), and also an antenna "best" mode. In "best" mode, antenna 1 is used for transmit and receive diversity is enabled.

Test Cases:

1. Antenna 1
2. Antenna 2
3. Antenna Best

Antenna Configuration Telnet Test

Table 6-21. Antenna Configuration Telnet Test

#	Description	Test Steps	Expected Results	Actual Results
	Initialization.	1. Use the test setup shown in Figure 6-2. WRMs with Power Meter and Attenuator Test Setup, with the initial condition of no power meter or attenuator attached. 2. Execute Telnet initialization procedure in Section 6.2.3.1 on both HD/WRM setups.	N/A	N/A
1.	Verify WRM-1 and WRM-2 responses to *set antenna 1* command.	1. Use HD-1 and HD-2 API Testers to send the *set antenna 1* Telnet command and verify the responses.	API Testers display response *Antenna: 1*.	Antenna: 1 Displayed by HD-1 and HD-2.
	Verify WRM-1 and WRM-2 responses to *get antenna* command.	2. Use HD-1 and HD-2 API Testers to send the *get antenna* Telnet command and verify the response.	API Testers display response A*ntenna: 1*.	Antenna: 1 Displayed by HD-1 and HD-2
	Verify WRM–1 transmits on Antenna 1.	3. Disconnect the WRM-1 antennas and attach the power meter to the antenna 1 SMA connector. 4. Use HD-1 API Tester to continuously broadcast packets w/o PBP control. 5. Measure power at the WRM-1 antenna 1 SMA connector using the power meter.	Antenna 1 power measurement = 20 dBm +/- 1 dB.	20.1 dBm
		6. Measure power at the WRM-1 antenna 2 SMA connector using the power meter	Antenna 2 power measurement <= 0.	-6 dBm
		7. Use HD-1 API Tester to stop packet broadcast. 8. Reconnect the WRM-1 antennas.	N/A	N/A

#	Description	Test Steps	Expected Results	Actual Results
	Verify WRM-2 receives on Antenna 1.	9. Attach 50 dB attenuator between WRM-2 antenna 1 and the SMA connector to reduce the received signal strength (verifies WRM will use selected antenna even though RSSI is lower). 10. Use HD-1 API Tester to continuously broadcast packets with PBP control. 11. Use HD-2 Ethereal to verify the WRXO fixed value fields.	WRM-2 sends WRXOs with the C field (Word 1, bit 00) set to copy (1), Class field (Word 1, bits 01-02) set to debugging and measurement (10), Option field (Word 1, bits 03-07) set to 26, Length field (Word 1, bits 08-15) set to 36, and RSV field (Word 9, bits 18-31) set to 0.	(W1) DA 24 FF C3 1101 1010 0010 0100 1111 1111 1100 0011 (W9) 00 00 00 00
		12. Use HD-2 Ethereal to verify the WRXO antenna field.	WRM-2 sends WRXOs with the antenna field (Word 9, bits 16-17) set to antenna 1 (00).	(W9) 00 00 00 00
		13. Use HD-2 API Tester to verify the antenna used to receive the packets.	API tester displays the packets are being received on antenna 1.	Most packets are received on antenna 1, however a few are reported received on antenna 2.
		14. Use HD-1 API Tester to stop packet broadcast. 15. Remove the attenuator on WRM-2 antenna 1.	N/A	N/A
2.	Verify WRM-1 and WRM-2 responses to *set antenna 2* command.	1. Use HD-1 and HD-2 API Testers to send the *set antenna 2* Telnet command and verify the responses.	API Testers display response *Antenna: 2*.	Antenna: 2 Displayed by HD-1 and HD-2
	Verify WRM-1 and WRM-2 responses to *get antenna* command.	2. Use HD-1 and HD-2 API Testers to send the *get antenna* Telnet command and verify the response.	API Testers display response A*ntenna: 2*.	Antenna: 2 Displayed by HD-1 and HD-2
	Verify WRM–1 transmits on Antenna 2.	3. Disconnect the WRM-1 antennas and attach the power meter to antenna 2. 4. Use HD-1 API Tester to continuously broadcast packets w/o PBP control. 5. Measure power at the WRM-1 antenna 2 SMA connector using the power meter.	Antenna 2 power measurement = 20 dBm +/- 1 dB.	19.7 dBm
		6. Measure power at the WRM-1 antenna 1 SMA connector using the power meter.	Antenna 1 power measurement <= 0 dBm.	-8 dBm

#	Description	Test Steps	Expected Results	Actual Results
		7. Use HD-1 API Tester to stop packet broadcast. 8. Reconnect the WRM-1 antennas.	N/A	N/A.
	Verify WRM-2 receives on Antenna 2.	9. Attach 50 dB attenuator between WRM-2 antenna 2 and the SMA connector. 10. Use HD-1 API Tester to continuously broadcast packets with PBP control. 11. Use HD-2 Ethereal to verify the WRXO antenna field.	WRM-2 sends WRXOs with the antenna field (Word 9, bits 16-17) set to antenna 2 (01).	(W9) 00 00 40 00 0000 0000 0000 0000 0100 0000 0000 0000
		12. Use HD-2 API Tester to verify the antenna used to receive the packets.	API Tester displays the packets are being received on antenna 2.	Most packets are received on antenna 2, however a few are reported received on antenna 1.
		13. Use HD-1 API Tester to stop packet broadcast. 14. Remove the attenuator on antenna 2.	N/A	N/A
3.	Verify WRM-1 and WRM-2 responses to *set antenna best* command.	1. Use HD-1 and HD-2 API Testers to send the *set antenna best* Telnet command and verify the responses.	API Testers display response *Antenna: best*.	Antenna: best Displayed by HD-1 and HD-2.
	Verify WRM-1 and WRM-2 responses to *get antenna* command.	2. Use HD-1 and HD-2 API Testers to send the *get antenna* Telnet command and verify the response.	API Testers display response A*ntenna: best*.	Antenna: best Displayed by HD-1 and HD-2
	Verify WRM-1 transmits on antenna 1.	3. Repeat Test Case # 1, steps 3-8.	[Same as for Test Case # 1]	Record results in Table 6-22
	Verify WRM-2 receives on “best” antenna.	4. Attach 50 db attenuator between WRM-2 antenna 1 and its SMA connector. 5. Use HD-1 API Tester to continuously broadcast packets with PBP control. 6. Use HD-2 API Tester to verify packets are received on antenna 2. 7. Use HD-1 API Tester to stop packet broadcast.	API Tester displays packets are received on antenna 2.	All packets received on antenna 2.

#	Description	Test Steps	Expected Results	Actual Results
		8. Remove attenuator from antenna 1 and attach to WRM-2 antenna 2. 9. Use HD-1 API Tester to continuously broadcast packets with PBP control. 10. Use HD-2 API Tester to verify packets are received on antenna 1. 11. Use HD-1 API Tester to stop packet broadcast.	API Tester displays packets are received on antenna 1.	All packets received on antenna 1.

Table 6-22. Antenna Configuration *"Best"* Telnet Test Result

Antenna Configuration	Expected Results		Actual Results	
	Power Measurement		Power Measurement	
	Antenna 1	Antenna 2	Antenna 1	Antenna 2
Best	20 dBm	<= 0 dBm	20.1 dBm	-5 dBm

Antenna Configuration IP Configuration Test

Table 6-23. Antenna Configuration IP Configuration Test

#	Description	Test Steps	Expected Results	Actual Results
	Initialization	1. Use the test setup shown in Figure 6-2. WRMs with Power Meter and Attenuator Test Setup, with the initial condition of no power meter or attenuator attached. 2. Execute IP initialization procedure in Section 6.2.3.2 on both HD/WRM setups.	N/A	N/A
1.	Set WRM-1 and WRM-2 *antenna* to *1*.	1. Use the HD-1 and HD-2 API Testers to set the WRM configuration with the *Antenna* field set to *1*. 2. Use Ethereal to verify the WCO antenna field.	API Testers send WCO with antenna field (Word 3, bits 04-05) set to Antenna 1 (00).	(W3) 01 00 00 00 0000 0001 0000 0000 0000 0000 0000 0000
	Verify WRM-1 and WRM-2 response to *antenna 1* command.	3. Use the HD-1 and HD-2 API Tester to get the WRM configuration and verify the response.	API Testers display antenna configuration as Antenna 1.	Antenna 1 displayed by HD-1 and HD-2.
		4. Use Ethereal to verify the WCO antenna field.	WRMs send WCO with the antenna field (Word 3, bits 04-05) set to Antenna 1 (00).	(W3) 01 00 00 00 0000 0001 0000 0000 0000 0000 0000 0000

#	Description	Test Steps	Expected Results	Actual Results
	Verify WRM-1 transmits on Antenna 1.	5. Execute Table 6-21. Antenna Configuration Telnet Test, Test Case # 1, steps 3 through 8.	[See Telnet Test]	Ant 1 = 20.0 dBm Ant 2 = -5 dBm
	Verify WRM-2 receives on Antenna 1.	6. Execute Table 6-21. Antenna Configuration Telnet Test, Test Case # 1, steps 9 through 15.	[See Telnet Test]	(W1) DA 24 FF B3 1101 1010 0010 0100 1111 1111 1011 0011 (W9) 00 00 00 00 Most packets are received on antenna 1, however a few are reported received on antenna 2.
2.	Set WRM-1 and WRM-2 *antenna* to *2*	1. Use the HD-1 and HD-2 API Testers to set the WRM configuration with the *Antenna* field set to *2*. 2. Use Ethereal to verify the WCO antenna field.	API Testers send WCO with antenna field (Word 3, bits 04-05) set to Antenna 2 (01).	(W3) 05 00 00 00 0000 0101 0000 0000 0000 0000 0000 0000
	Verify WRM-1 and WRM-2 response to *antenna 2* command.	3. Use the HD-1 and HD-2 API Testers to get the WRM configuration and verify the response.	API Testers display antenna configuration as Antenna 2.	
		4. Use Ethereal to verify the WCO antenna field.	WRMs send WCO with the antenna field (Word 3, bits 04-05) set to Antenna 2 (01).	(W3) 05 00 00 00
	Verify WRM-1 transmits on Antenna 2.	5. Execute Table 6-21. Antenna Configuration Telnet Test, Test Case # 2, steps 3 through 8.	[See Telnet Test]	Ant 2 = 19.7 dBm Ant 1 = -7 dBm
	Verify WRM-2 receives on Antenna 2.	6. Execute Table 6-21. Antenna Configuration Telnet Test, Test Case # 2, steps 9 through 14.	[See Telnet Test]	(W9) 00 00 40 00 Most packets are received on antenna 2, however a few are reported received on antenna 1.
3.	Set WRM-1 and WRM-2 *antenna* to *best*	1. Use the HD-1 and HD-2 API Testers to set the WRM configuration with the *Antenna* field set to *best*. 2. Use Ethereal to verify the WCO antenna field.	API Testers send WCO with antenna field (Word 3, bits 04-05) set to Antenna best (10).	(W3) 09 00 00 00 0000 1001 0000 0000

#	Description	Test Steps	Expected Results	Actual Results
	Verify WRM-1 and WRM-2 response to *antenna best* command.	3. Use the HD-1 and HD-2 API Testers to get the WRM configuration and verify the response.	API Testers display antenna configuration as Antenna best.	Antenna: best Displayed by HD-1 and HD-2.
		4. Use Ethereal to verify the WCO antenna field.	WRMs send WCO with the antenna field (Word 3, bits 04-05) set to Antenna best (10).	(W3) 09 00 00 00
	Verify WRM-1 transmits on Antenna 1.	5. Execute Table 6-21. Antenna Configuration Telnet Test, Test Case # 1, steps 3 through 8.	[See Telnet Test]	Ant 1 = 20.1 dBm Ant 2 = -5 dBm
	Verify WRM-2 receives on "best" antenna.	6. Execute Table 6-21. Antenna Configuration Telnet Test, Test Case # 3, steps 4 through 11.	[See Telnet Test]	All packets received on antenna 2 with attenuator on antenna 1. All packets received on antenna 1 with attenuator on antenna 2.

Antenna Configuration IP Packet-by-Packet Test

Table 6-24. Antenna Configuration IP Packet-by-Packet Test

#	Description	Test Steps	Expected Results	Actual Results
	Initialization	1. Use the test setup shown in Figure 6-2. WRMs with Power Meter and Attenuator Test Setup, with the initial condition of no power meter or attenuator attached. 2. Execute IP initialization procedure in Section 6.2.3.2 on both HD/WRM setups.	N/A	N/A
1.	Set WRM-1 and WRM-2 *antenna* to *1* using PBP control.	1. Use the HD-1 and HD-2 API Testers to set the *antenna* to *1* and transmit one packet with PBP control 2. Use Ethereal to verify the WTXO antenna field.	API Testers send WTXO with antenna field (Word 4, bits 20-21) set to Antenna 1 (00).	(W4) FF FF 01 00 1111 1111 1111 1111 0000 0001 0000 0000
	Verify WRM-1 and WRM-2 configuration.	3. Use the HD-1 and HD-2 API Testers to get the WRM configuration.	API Testers display antenna configuration as Antenna 1.	Antenna = 1
	Verify WRM-1 transmits on Antenna 1.	4. Execute Table 6-21. Antenna Configuration Telnet Test, Test Case # 1, steps 3 through 8, except transmit packets with PBP control.	[See Telnet Test]	Record results in Table 6-25

#	Description	Test Steps	Expected Results	Actual Results
	Verify WRM-2 receives on Antenna 1.	5. Execute Table 6-21. Antenna Configuration Telnet Test, Test Case # 1, steps 9 through 15.	[See Telnet Test]	Record results in Table 6-26
2.	Set WRM-1 and WRM-2 *antenna* to *2* using PBP control.	1. Use the HD-1 and HD-2 API Testers to set the *Antenna* to *2* and transmit one packet with PBP control. 2. Use Ethereal to verify the WTXO antenna field.	API Testers sends WTXO with antenna field (Word 4, bits 20-21) set to Antenna 2 (01).	(W4) FF FF 05 00 1111 1111 1111 1111 0000 0101 0000 0000
	Verify WRM-1 and WRM-2 configuration.	3. Use the HD-1 and HD-2 API Testers to get the WRM configuration.	API Tester displays antenna configuration as Antenna 2.	Antenna = 2
	Verify WRM-1 transmits on Antenna 2.	4. Execute Table 6-21. Antenna Configuration Telnet Test, Test Case # 2, steps 3 through 8, except transmit packets with PBP control.	[See Telnet Test]	Record results in Table 6-27
	Verify WRM-2 receives on Antenna 2.	5. Execute Table 6-21. Antenna Configuration Telnet Test, Test Case # 2, steps 9 through 14.	[See Telnet Test]	Record results in Table 6-28
3.	Set WRM-1 and WRM-2 *antenna* to *best* using PBP control.	1. Use the HD-1 and HD-2 API Testers to set the *Antenna* set to *best* and transmit one packet with PBP control. 2. Use Ethereal to verify the WTXO antenna field.	API Tester sends WTXO with antenna field (Word 4, bits 20-21 set to Antenna best (10).	(W4) FF FF 09 00 1111 1111 1111 1111 0000 1001 0000 0000
	Verify WRM-1 and WRM-2 configuration.	3. Use the HD-1 and HD-2 API Testers to get the WRM configuration.	API Tester displays antenna configuration as Antenna best.	Antenna = best
	Verify WRM-1 transmits on Antenna 1.	4. Execute Table 6-21. Antenna Configuration Telnet Test, Test Case # 1, steps 3 through 8, except transmit packets with PBP control.	[See Telnet Test]	Record results in Table 6-29
	Verify WRM-2 receives on “best” antenna.	5. Execute Table 6-21. Antenna Configuration Telnet Test, Test Case # 3, steps 4 through 11.	[See Telnet Test]	Record results in Table 6-30

Table 6-25. Antenna 1 Configuration IP Packet-by-Packet Tx Test Results

	Expected Results	Actual Results
Antenna 1 Power Measured	20 dBm	20.1 dBm
Antenna 2 Power Measured	<= 0 dBm	-5.3 dBm

Table 6-26. Antenna 1 Configuration IP Packet-by-Packet Rx Test Results

	Expected Results	Actual Results
HD-2 Ethereal WRXO fixed value fields results.	WRM-2 sends WRXOs with the C field (Word 1, bit 00) set to copy (1), Class field (Word 1, bits 01-02) set to debugging and measurement (10), Option field (Word 1, bits 03-07) set to 26, Length field (Word 1, bits 08-15) set to 36, and RSV field (Word 9, bits 18-31) set to 0.	(W1) DA 24 FF B5 1101 1010 0010 0100 1111 1111 1011 0101 (W9) 00 00 00 00
HD-2 Ethereal WRXO antenna field results.	WRM-2 sends WRXOs with the antenna field (Word 9, bits 16-17) set to antenna 1 (00).	(W9) 00 00 00 00
HD-2 API Tester receive antenna results.	API tester displays the packets are being received on antenna 1.	Most packets are received on antenna 1, however a few are reported received on antenna 2.

Table 6-27. Antenna 2 Configuration IP Packet-by-Packet Tx Test Results

	Expected Results	Actual Results
Antenna 2 Power Measured	20 dBm	19.8 dBm
Antenna 1 Power Measured	<= 0 dBm	-8 dBm

Table 6-28. Antenna 2 Configuration IP Packet-by-Packet Rx Test Results

	Expected Results	Actual Results
HD-2 Ethereal WRXO fixed value fields results.	WRM-2 sends WRXOs with the C field (Word 1, bit 00) set to copy (1), Class field (Word 1, bits 01-02) set to debugging and measurement (10), Option field (Word 1, bits 03-07) set to 26, Length field (Word 1, bits 08-15) set to 36, and RSV field (Word 9, bits 18-31) set to 0.	(W9) 00 00 40 00 0000 0000 0000 0000 0100 0000 0000 0000
HD-2 Ethereal WRXO antenna field results.	WRM-2 sends WRXOs with the antenna field (Word 9, bits 16-17) set to antenna 2 (01).	(W9) 00 00 40 00
HD-2 API Tester receive antenna results.	API tester displays the packets are being received on antenna 2.	Most packets are received on antenna 2, however a few are reported received on antenna 1.

Table 6-29. Antenna Best Configuration IP Packet-by-Packet Tx Results

	Expected Results	Actual Results
Antenna 1 Power Measured	20 dBm	20.1 dBm
Antenna 2 Power Measured	<= 0 dBm	-4.8 dBm

Table 6-30. Antenna Best Configuration IP Packet-by-Packet Rx Results

	Expected Results	Actual Results
Attenuator on antenna 1	API Tester displays packets are received on antenna 2.	All packets received on antenna 2.
Attenuator on antenna 2	API Tester displays packets are received on antenna 1.	All packets received on antenna 1.

6.3.3.2 Antenna 1 Compensation Factor

Verify the WRM response to commands to set the antenna 1 power compensation factor. The compensation factor affects the maximum output power, which is verified in Section 6.3.3.7. This command is not available with PBP control.

Antenna 1 Compensation Factor Telnet Test

Table 6-31. Antenna 1 Compensation Factor Telnet Test

#	Description	Test Steps	Expected Results	Actual Results
	Initialization.	1. Use the test setup shown in Figure 6-1. Single WRM Test Setup. 2. Execute Telnet initialization procedure in Section 6.2.3.1.	N/A	N/A
1.	Verify WRM response to *set antenna1comp -10* command.	1. Use the API Tester to send the *set antenna1comp -10* Telnet command and verify the WRM response.	API Tester displays WRM response: *Antenna 1 Comp: -10*.	Antenna 1 Comp: -10 dB
	Verify WRM response to *get antenna1comp* command.	2. Use the API Tester to send the *get antenna1comp* Telnet command and verify the WRM response.	API Tester displays WRM response: *Antenna 1 Comp: -10*	Antenna 1 Comp: -10 dB
	Repeat test for other compensation values.	3. Repeat test steps 1-2 for integer values –5, 0, 10, and 19.	API Tester displays WRM response: *Antenna 1 Comp: [value]*.	Record results in Table 6-32.

Table 6-32. Antenna 1 Compensation Factor Telnet Test Results

Antenna 1 Compensation	Expected Results		Actual Results	
	***set antenna1comp* Response**	***get antanna1comp* Response**	***set antenna1comp* Response**	***get antanna1comp* Response**
-5	-5	-5	-5 dB	-5 dB
0	0	0	0 dB	0 dB
10	10	10	10 dB	10 dB
19	19	19	19 dB	19 dB

Antenna 1 Compensation Factor IP Configuration Test

Table 6-33. Antenna 1 Compensation Factor IP Configuration Test

#	Description	Test Steps	Expected Results	Actual Results
	Initialization.	1. Use the test setup shown in Figure 6-1. Single WRM Test Setup. 2. Execute IP initialization procedure in Section 6.2.3.2	N/A	N/A
1.	Set WRM *antenna 1 comp to –10.*	1. Use the API Tester to set the WRM configuration with the *antenna 1 comp* field set to *-10*. 2. Use Ethereal to verify the WCO antenna 1 comp field.	API Tester sends WCO with antenna 1 compensation field (Word 3, bits 08-15) set to -10 (xF6).	(W3) 09 F6 00 00
	Verify WRM response to *antenna 1 comp* command.	3. Use the API Tester to get the WRM configuration and verify the response.	API Tester displays antenna 1 compensation factor as –10 dB.	10 dB
		4. Use Ethereal to verify the WCO antenna 1 comp field.	WRM sends WCO with the antenna1comp field set to -10.	(W3) 09 F6 00 00
	Repeat test for other compensation values.	5. Repeat test steps 1-4 for integer values from –5, 0, 10, and 19.	WRM sends WCO with the antenna 1comp field set to the specified value. API Tester displays antenna 1 compensation factor as the specified value.	Record results in Table 6-34.

Table 6-34. Antenna 1 Compensation Factor IP Configuration Test Results

Antenna 1 Compensation	Expected Results			Actual results		
	WCO antenna 1 compensation field		API Tester antenna 1 compensation	WCO antenna 1 compensation field		API Tester antenna 1 compensation
	set	get		set	get	
-5	-5	-5	-5	(0xFB) -5	(0xFB) -5	-5 dB
0	0	0	0	(0x00) 0	(0x00) 0	0 dB
10	10	10	10	(0x0A) 10	(0x0A) 10	10 dB
19	19	19	19	(0x13) 19	(0x13) 19	19 dB

6.3.3.3 Antenna 2 Compensation Factor

Verify the WRM response to commands to set the antenna 2 power compensation factor. The compensation factor affects the maximum output power, which is verified in Section 6.3.3.7.

Test Procedure: Repeat the procedure in Section 6.3.3.2 except substitute antenna 2 for antenna 1. WCO contains antenna 2 compensation in Word 3, Bits 16-23. Record the results in Table 6-35 and Table 6-36.

Table 6-35. Antenna 2 Compensation Factor Telnet Test Results

Antenna 2 Compensation	Expected Results		Actual results	
	***set antenna2comp* Response**	***get antanna2comp* Response**	***set antenna2comp* Response**	***get antanna2comp* Response**
-10	-10	-10	-10 dB	-10 dB
-5	-5	-5	-5 dB	-5 dB
0	0	0	0 dB	0 dB
10	10	10	10 dB	10 dB
19	19	19	19 dB	19 dB

Table 6-36. Antenna 2 Compensation Factor IP Configuration Test Results

Antenna 2 Compensation	Expected Results			Actual results		
	WCO antenna 2 compensation field		API Tester antenna 2 compensation	WCO antenna 2 compensation field		API Tester antenna 2 compensation
	set	get		set	get	
-10	-10	-10	-10	(0xF6) -10	(0xF6) -10	-10 dB
-5	-5	-5	-5	(0xFB) -5	(0xFB) -5	-5 dB
0	0	0	0	(0x00) 0	(0x00) 0	0 dB
10	10	10	10	(0x0A) 10	(0x0A) 10	10 dB
19	19	19	19	(0x13) 19	(0x13) 19	19 dB

6.3.3.4 Bandwidth

Verify the WRM supports WAVE mode operation at 10 MHz and 20MHz bandwidth for 802.11a channels. Upon switching from a WAVE channel to an 802.11a channel, verify the WRM sets the bandwidth to the current bandwidth setting.

Bandwidth Telnet Test

Test Cases:

1. 10 MHz WAVE Channel -> 802.11a Channel Change (20 MHz default bandwidth)
2. 10 MHz BW Command
3. 802.11a -> 20 MHz WAVE Channel Change
4. 20 MHz WAVE Channel -> 802.11a Channel Change
5. 20 MHz BW Command

Table 6-37. Bandwidth Telnet Test

#	Description	Test Steps	Expected Results	Actual Results
	Initialization.	1. Use the test setup shown in Figure 6-3. WRM with Spectrum Analyzer Test Setup. 2. Execute Telnet initialization procedure in Section 6.2.3.1.	N/A	N/A
1.	Change channel from 10 MHz WAVE channel to 802.11a channel.	1. Use the API Tester to send the *set fastchannel 52* Telnet command.	API Tester displays response: *Radio Frequency: 5260 MHz (IEEE 52).*	Radio Frequency: 5260 MHz (IEEE 52)
	Verify WRM sets BW to current setting (20 MHz).	2. Use the API Tester to send the *get bandwidth* Telnet command and verify the response.	API Tester displays response: *Channel Bandwidth: 20 MHz.*	Channel Bandwidth: 20 MHz
		3. Use the API Tester to continuously broadcast packets w/o PBP control. 4. Verify the channel frequency and 20 MHz BW using the spectrum analyzer.	Spectrum analyzer shows center frequency of 5260 MHz and 20 MHz BW.	Center frequency = 5260 MHz. Bandwidth = 20 MHz.
		5. Use API Tester to stop packet broadcast.	N/A	N/A
2.	Verify WRM response to *set bandwidth 10* command.	1. Use the API Tester to send the *set bandwidth 10* Telnet command and verify the response.	API Tester displays response *Channel Bandwidth: 10 MHz.*	Channel Bandwidth: 10 MHz
	Verify WRM response to *get bandwidth* command.	2. Use the API Tester to send the *get bandwidth* Telnet command and verify the response.	API Tester displays response: *Channel Bandwidth: 10 MHz.*	Channel Bandwidth: 10 MHz
	Verify 10 MHz operation.	3. Use the API Tester to continuously broadcast packets w/o PBP control. 4. Verify the 10 MHz BW using the spectrum analyzer.	Spectrum analyzer shows 10 MHz BW.	Bandwidth = 10 MHz.
		5. Use the API Tester to stop packet broadcast.	N/A	N/A

3.	Change channel from 802.11a channel to 20 MHz WAVE channel.	1. Use the API Tester to send the *set fastchannel 175* Telnet command.	API Tester displays response: *Radio Frequency: 5875 MHz (IEEE 175).*	Radio Frequency: 5875 MHz (IEEE 175)
	Verify channel and 20 MHz operation.	2. Use the API Tester to continuously broadcast packets w/o PBP control. 3. Verify the channel and 20 MHz BW using the spectrum analyzer.	Spectrum analyzer shows center frequency of 5875 MHz and 20 MHz BW.	Bandwidth = 20 MHz
		4. Use the API Tester to stop packet broadcast.	N/A	N/A
4.	Change channel from 20 MHz WAVE channel to 802.11a channel.	1. Use the API Tester to send the *set fastchannel 161* Telnet command.	API Tester displays response: *Radio Frequency: 5805 MHz (IEEE 161).*	Radio Frequency 5805 MHz (IEEE 161)
	Verify WRM sets BW to current setting (10 MHz).	2. Use the API Tester to send the *get bandwidth* Telnet command and verify the response.	API Tester displays response: *Channel Bandwidth: 10 MHz.*	Channel Bandwidth: 10 MHz
		3. Use the API Tester to continuously broadcast packets w/o PBP control. 4. Verify the channel frequency and 10 MHz BW using the spectrum analyzer.	Spectrum analyzer shows center frequency of 5805 MHz and 10 MHz BW.	Bandwidth = 10 MHz
		5. Use the API Tester to stop packet broadcast.	N/A	N/A
5.	Verify WRM response to *set bandwidth 20* command.	1. Use the API Tester to send the *set bandwidth 20* Telnet command and verify the response.	API Tester displays response *Channel Bandwidth: 20 MHz.*	Channel Bandwidth: 20 MHz
	Verify WRM response to *get bandwidth* command.	2. Use the API Tester to send the *get bandwidth* Telnet command and verify the response.	API Tester displays response: *Channel Bandwidth: 20 MHz.*	Channel Bandwidth: 20 MHz
	Verify 20 MHz operation.	3. Use the API Tester to continuously broadcast packets w/o PBP control. 4. Verify the 20 MHz BW using the spectrum analyzer.	Spectrum analyzer shows 20 MHz BW.	Bandwidth = 20 MHz
		5. Use the API Tester to stop packet broadcast.	N/A	N/A

Bandwidth IP Configuration Test

Test Cases:

1. 20 MHz BW Command
2. 10 MHz BW Command

Table 6-38. Bandwidth IP Configuration Test

#	Description	Test Steps	Expected Results	Actual Results
	Initialization.	1. Use the test setup shown in Figure 6-3. WRM with Spectrum Analyzer Test Setup. 2. Execute IP initialization procedure in Section 6.2.3.2.	N/A	N/A
1.	Set WRM configuration to 802.11a channel and *20 MHz BW*.	1. Use the API Tester to set the WRM configuration to channel 52 and *20 MHz BW*. 2. Use Ethereal to verify the WCO BW field.	API sends WCO with BW field (Word 3, bits 06-07) set to 20 MHz (01)	(W3) 09 00 00 00 0000 1001 0000 0000
	Verify WRM response to *20 MHz BW* command.	3. Use the API Tester to get the WRM configuration. 4. Use Ethereal to verify the WCO BW field.	WRM sends WCO with BW field set to 20 MHz.	(W3) 09 00 00 00
		5. Use the API Tester to verify the response.	API Tester displays bandwidth as 20 MHz.	20 MHz
		6. Use the API Tester to continuously broadcast packets w/o PBP control. 7. Verify the channel frequency and 20 MHz BW using the spectrum analyzer.	Spectrum analyzer shows center frequency of 5260 MHz and 20 MHz BW.	Center frequency = 5260 MHz Bandwidth = 20 MHz
		8. Use the API Tester to stop packet broadcast.	N/A	N/A
2.	Set WRM configuration to *10 MHz BW*.	1. Use the API Tester to set the WRM configuration to *10 MHz BW*. 2. Use Ethereal to verify the WCO BW field..	API sends WCO with BW field (Word 3, bits 06-07) set to 10 MHz (00)	(W3) 08 00 00 00 0000 1000 0000 0000
	Verify WRM response to 1*0 MHz BW* command.	3. Use the API Tester to get the WRM configuration. 4. Use Ethereal to verify the WCO BW field.	WRM sends WCO with BW field (Word 3, bits 06-07) set to 10 MHz (00)	(W3) 08 00 00 00
		5. Use the API Tester to verify the response.	API Tester displays bandwidth as 10 MHz.	10 MHz

#	Description	Test Steps	Expected Results	Actual Results
		6. Use the API Tester to continuously broadcast packets w/o PBP control. 7. Verify the channel frequency and 10 MHz BW using the spectrum analyzer.	Spectrum analyzer shows center frequency of 5260 MHz and 10 MHz BW.	Center frequency = 5260 MHz Bandwidth = 10 MHz
		8. Use the API Tester to stop packet broadcast.	N/A	N/A

Bandwidth IP Packet-by-Packet Test

Test Cases:

1. 10 MHz BW Command
2. 20 MHz BW Command

Table 6-39. Bandwidth IP Packet-by-Packet Test

#	Description	Test Steps	Expected Results	Actual Results
	Initialization.	1. Use the test setup shown in Figure 6-3. WRM with Spectrum Analyzer Test Setup. 2. Execute IP initialization procedure in Section 6.2.3.2.	N/A	N/A
1.	Set WRM configuration to 802.11a channel and *10 MHz BW* using PBP control.	1. Use the API Tester to set the WRM configuration to *channel 52* and *10 MHz BW* and transmit one packet with PBP control. 2. Use Ethereal to verify the WTXO BW field.	API sends WTXO with BW field (Word 4, bits 22-23) set to 10 MHz (00)	(W4) FF FF 08 00 1111 1111 1111 1111 0000 1000 0000 0000
	Verify WRM configuration.	3. Use the API Tester to get the WRM configuration.	API Tester displays BW as 10 MHz.	10 MHz
		4. Use the API Tester to continuously broadcast packets with PBP control. 5. Verify the channel frequency and 10 MHz BW using the spectrum analyzer.	Spectrum analyzer shows center frequency of 5260 MHz and 10 MHz BW.	Center frequency = 5260 MHz Bandwidth = 10 MHz
		6. Use the API Tester to stop packet broadcast.	N/A	N/A

2.	Set WRM configuration to *20 MHz BW* using PBP control.	1. Use the API Tester to set the WRM configuration to *20 MHz BW* and transmit one packet with PBP control. 2. Use Ethereal to verify the WTXO BW field.	API sends WTXO with BW field (Word 4, bits 22-23) set to 20 MHz (01)	(W4) FF FF 09 00 1111 1111 1111 1111 0000 1001 0000 0000
	Verify WRM configuration.	3. Use the API Tester to get the WRM configuration.	API Tester displays BW as 20 MHz.	20 MHz
		4. Use the API Tester to continuously broadcast packets with PBP control. 5. Verify the 20 MHz BW using the spectrum analyzer.	Spectrum analyzer shows 20 MHz BW.	Center frequency = 5260 MHz Bandwidth = 20 MHz
		6. Use the API Tester to stop packet broadcast.	N/A	N/A

6.3.3.5 Fastchannel

Verify the WRM supports WAVE mode operation on all WAVE and 802.11a channels.

The channel setting affects the channel bandwidth, data rate, and maximum output power.

- Bandwidth -- For WAVE channels, verify the WRM sets the channel bandwidth to 10 or 20 MHz depending on the channel number.
- Data Rate -- When switching from a 20 MHz to a 10 MHz channel using a Telnet command, verify the WRM halves the previous data rate. When switching from a 10 MHz to a 20 MHz channel, verify the WRM doubles the previous data rate.
- Maximum Output Power – Section 6.3.3.7 verifies these requirements.

Fastchannel Telnet Test

Test Cases:

1. Channel Frequency and BW Verification
2. Channel Data Rate Verification

Table 6-40. Fastchannel Telnet Test

#	Description	Test Steps	Expected Results	Actual Results
	Initialization.	1. Use the test setup shown in Figure 6-4. WRM with Spectrum Analyzer and Vector Signal Analyzer Test Setup, with antenna 1 installed (i.e., VSA is not connected) 2. Execute Telnet initialization procedure in Section 6.2.3.1.	N/A	N/A
1.	Verify WRM response to *set fastchannel 172* command.	1. Use the API Tester to send the *set fastchannel 172* Telnet command and verify the response.	API Tester displays response: *Radio Frequency: 5860 MHz (IEEE 172).*	Radio Frequency: 5860 MHz (IEEE 172)
	Verify WRM response to *get fastchannel* command.	2. Use the API Tester to send the *get fastchannel* command and verify the response.	API Tester displays WRM response: *Radio Frequency: 5860 MHz (IEEE 172).*	Radio Frequency: 5860 MHz (IEEE 172)
	Verify channel frequency and BW.	3. Use the API Tester to continuously broadcast packet traffic w/o PBP control. 4. Use Spectrum Analyzer to verify WRM is transmitting on channel 172 with 10 MHz BW.	Spectrum Analyzer shows center frequency of 5860 MHz and 10 MHz BW.	Center frequency = 5860 MHz Bandwidth = 10 MHz
		5. Use API Tester to stop packet broadcast.	N/A	N/A
	Verify frequency and BW for all remaining WAVE and 802.11a channels.	6. Repeat steps 1-5 for all WAVE and 802.11a channels listed in 7. Table 6-41 and 8. Table 6-42.	The API Tester displays the correct frequency, and channel number in accordance with Table 6-41 and Table 6-42. The spectrum analyzer verifies the correct center frequency and BW.	Record results in Table 6-41 and Table 6-42.
2.	Modify setup to support data rate verification.	1. Disconnect antenna 1 and connect to VSA to antenna 1 SMA connector.	N/A	N/A
	Verify data rate.	2. Use the API Tester to send the *set fastchannel 172* Telnet command and verify the response.	API Tester displays response: *Radio Frequency: 5860 MHz (IEEE 172).*	Radio Frequency: 5860 MHz (IEEE 172)
		3. Use the API Tester to send the *get rate* Telnet command and verify the response.	API Tester displays *Data Rate: 6.*	Data Rate: 6

#	Description	Test Steps	Expected Results	Actual Results
		4. Use the API Tester to continuously broadcast packet traffic w/o PBP control. 5. Use VSA to verify data rate. 6. Use API Tester to stop packet broadcast.	VSA shows data rate is 6 Mbps.	6 Mbps
	Verify data rate for all remaining WAVE and 802.11a channels.	7. Repeat steps 2-6 for all WAVE and 802.11a channels listed in Table 6-43 and Table 6-44.	For 10 MHz channels, the data rate is 6 (Mbps). For 20 MHz channels, the data rate is 12 (Mbps).	Record results in Table 6-43 and Table 6-44.

Table 6-41. WAVE Channel Frequency and BW Telnet Test Results

Test Channels	Expected Results			Actual Results					
	Frequency (MHz)	Channel Number	BW (MHz)	*set fastchannel*		*get fastchannel*		Spectrum analyzer	
				Freq	Channel	Freq	Channel	Freq	BW
172	5860	172	10	5960	172	5860	172	5860	10
174	5870	174	10	5870	174	5870	174	5870	10
175	5875	175	20	5875	175	5875	175	5875	20
176	5880	176	10	5880	176	5880	176	5880	10
178	5890	178	10	5890	178	5890	178	5890	10
180	5900	180	10	5900	180	5900	180	5900	10
181	5905	181	20	5905	181	5905	181	5905	20
182	5910	182	10	5910	182	5910	182	5910	10
184	5920	184	10	5920	184	5920	184	5920	10

Table 6-42. 802.11a Channel Frequency and BW Telnet Test Results

Test Channels	Expected Results			Actual Results					
	Frequency (MHz)	Channel Number	BW (MHz)	*set fastchannel*		*get fastchannel*		Spectrum analyzer	
				Freq	Channel	Freq	Channel	Freq	BW
52	5260	52	20	5260	52	5269	52	5260	20
56	5280	56	20	5280	56	5280	56	5280	20
60	5300	60	20	5300	60	5300	60	5300	20
64	5320	64	20	5320	64	5320	64	5320	20
149	5745	149	20	5745	149	5745	149	5745	20
153	5765	153	20	5765	153	5765	153	5765	20
157	5785	157	20	5785	157	5785	157	5785	20
161	5805	161	20	5805	161	5805	161	5805	20

Table 6-43. WAVE Channel Data Rate Telnet Test Results

Test Channels	Expected Results				Actual Results			
	Channel Number	Frequency (MHz)	BW (MHz)	Data Rate	*set fastchannel*		*get rate*	VSA Data Rate
					Frequency	Channel	Data Rate	
172	172	5860	10	6	5860	172	6 Mbps	6 Mbps
174	174	5870	10	6	5870	174	6 Mbps	6 Mbps
175	175	5875	20	12	5875	175	12 Mbps	12 Mbps
176	176	5880	10	6	5880	176	6 Mbps	6 Mbps
178	178	5890	10	6	5890	178	6 Mbps	6 Mbps
180	180	5900	10	6	5900	180	6 Mbps	6 Mbps
181	181	5905	20	12	5905	181	12 Mbps	12 Mbps
182	182	5910	10	6	5910	182	6 Mbps	6 Mbps
184	184	5920	10	6	5920	184	6 Mbps	6 Mbps

Table 6-44. 802.11a Channel Data Rate Telnet Test Results

Test Channels	Expected Results				Actual Results			
	Channel Number	Frequency (MHz)	BW (MHz)	Data Rate	*set fastchannel*		*get rate*	VSA Data Rate
					Frequency	Channel	Data Rate	
52	52	5260	20	12	5260	52	12 Mbps	12 Mbps
56	56	5280	20	12	5280	56	12 Mbps	12 Mbps
60	60	5300	20	12	5300	60	12 Mbps	12 Mbps
64	64	5320	20	12	5320	64	12 Mbps	12 Mbps
149	149	5745	20	12	5745	149	12 Mbps	12 Mbps
153	153	5765	20	12	5765	153	12 Mbps	12 Mbps
157	157	5785	20	12	5785	157	12 Mbps	12 Mbps
161	161	5805	20	12	5805	161	12 Mbps	12 Mbps

Fastchannel IP Configuration Test

Test Cases:

1. Channel Frequency and BW Verification

Table 6-45. Fastchannel IP Configuration Test

#	Description	Test Steps	Expected Results	Actual Results
	Initialization.	1. Use the test setup shown in Figure 6-3. WRM with Spectrum Analyzer Test Setup. 2. Execute IP initialization procedure in Section 6.2.3.2.	N/A	N/A
1.	Set WRM *channel* to *172.*	1. Use the API Tester to set the WRM configuration with the channel of 172. 2. Use Ethereal to verify the WCO channel field.	API Tester sends WCO with channel field (Word 1, bits 16-21) set to 172 (000000)	(W1) DD 14 01 43 1101 1101 0001 0100 **0000 00**01 0100 0011
	Verify WRM response to the *channel 172* command.	3. Use the API Tester to get the WRM configuration. 4. Use Ethereal to verify the WCO channel field.	WRM sends WCO with channel field (Word 1, bits 16-21) set to 172 (000000).	(W1, Byte 3) 01 **0000 00**01
		5. Use the API Tester to verify the response.	API Tester displays Channel 172 and 10 MHz BW.	Channel = 172 Bandwidth = 10 MHz

#	Description	Test Steps	Expected Results	Actual Results
	Verify channel frequency and BW.	6. Use the API Tester to continuously broadcast packet traffic w/o PBP control. 7. Use Spectrum Analyzer to verify WRM is transmitting on channel 172 with 10 MHz BW.	Spectrum Analyzer shows center frequency of 5860 MHz and 10 MHz BW.	Center frequency 5860 MHz 10 MHz
		8. Use the API Tester to stop packet broadcast.	N/A	N/A
	Verify frequency and BW for all remaining WAVE and 802.11a channels.	9. Repeat steps 1-8 for all WAVE and 802.11a channels listed in Table 6-46 and Table 6-47.	The WCO channel field values (Word 1, bits 16-21) are in accordance with Table 6-46 and Table 6-47. The spectrum analyzer shows center frequencies and BW in accordance with Table 6-46 and Table 6-47.	Record results in Table 6-46 and Table 6-47.

Table 6-46. WAVE Channel Frequency and BW IP ConfigurationTest Results

	Expected Results				Actual Results					
					Ethereal WCO Channel Field Results		API Tester Results		Spectrum Analyzer	
Test Chan	Channel Number	Frequency (MHz)	BW (MHz)	WCO Channel Field	Set WRM Config.	Get WRM Config.	Chan	BW	Freq	BW
172	172	5860	10	000000	0x01	0x01	5860	N/A	5860	10
174	174	5870	10	000001	0x05	0x05	5870	N/A	5870	10
175	175	5875	20	000010	0x09	0x09	5875	N/A	5875	20
176	176	5880	10	000011	0x0D	0x0D	5880	N/A	5880	10
178	178	5890	10	000100	0x11	0x11	5890	N/A	5890	10
180	180	5900	10	000101	0x15	0x15	5900	N/A	5900	10
181	181	5905	20	000110	0x19	0x19	5905	N/A	5905	20
182	182	5910	10	000111	0x1D	0x1D	5910	N/A	5910	10
184	184	5920	10	001000	0x21	0x21	5920	N/A	5920	10

Table 6-47. 802.11a Channel Frequency and BW IP Configuration Test Results

Test Chan	Expected Results				Actual Results					
					Ethereal WCO Channel Field Results		API Tester Results		Spectrum Analyzer	
	Channel Number	Frequency (MHz)	BW (MHz)	WCO Channel Field	Set WRM Config.	Get WRM Config.	Chan	BW	Freq	BW
52	52	5260	20	001101	0x35	0x35	52	20	5260	20
56	56	5280	20	001110	0x39	0x39	56	20	5280	20
60	60	5300	20	001111	0x3D	0x3D	60	20	5300	20
64	64	5320	20	010000	0x41	0x41	64	20	5320	20
149	149	5745	20	010001	0x45	0x45	149	20	5745	20
153	153	5765	20	010010	0x49	0x49	153	20	5765	20
157	157	5785	20	010011	0x4D	0x4D	157	20	5786	20
161	161	5805	20	010100	0x51	0x51	161	20	5805	20

Fastchannel IP Packet-by-Packet Test

Test Cases:

1. Channel Frequency and BW Verification

Table 6-48. Fastchannel IP Packet-by-Packet Test

#	Description	Test Steps	Expected Results	Actual Results
	Initialization.	1. Use the test setup shown in Figure 6-3. WRM with Spectrum Analyzer Test Setup. 2. Execute IP initialization procedure in Section 6.2.3.2.	N/A	N/A
1.	Set WRM *channel* to *172* using PBP control.	1. Use the API Tester to set the WRM configuration to *channel 172* and transmit one packet with PBP control. 2. Use Ethereal to verify the WTXO channel field.	API Tester sends WTXO with channel field (Word 1, bits 16-21) set to 172 (000000).	(W1, Byte 3) 01 0000 0001
	Verify WRM configuration.	3. Use the API Tester to get the WRM configuration.	API Tester displays channel 172.	172
		4. Use the API Tester to continuously broadcast packets with PBP control. 5. Verify the channel frequency and 10 MHz BW using the spectrum analyzer.	Spectrum analyzer shows center frequency of 5860 MHz and 10 MHz BW.	Center Frequency = 5860 MHz Bandwidth = 10 MHz

#	Description	Test Steps	Expected Results	Actual Results
		6. Use the API Tester to stop packet broadcast.	N/A	N/A
	Verify frequency and BW for all remaining WAVE and 802.11a channels.	7. Repeat steps 1-6 for all WAVE and 802.11a channels listed in Table 6-49 and Table 6-50.	The WTXO channel field values (Word 1, bits 16-21) are in accordance with Table 6-49 and Table 6-50. The spectrum analyzer shows center frequencies and BW in accordance with Table 6-49 and Table 6-50.	Record results in Table 6-49 and Table 6-50.

Table 6-49. WAVE Channel Frequency and BW IP Packet-by-Packet Test Results

Test Chan	Expected Results				Actual Results			
	Channel Number	Frequency (MHz)	BW (MHz)	WTXO Channel Field	Ethereal WTXO Channel Field Results	API Tester Results	Spectrum Analyzer Results	
						Channel	Freq	BW
172	172	5860	10	000000	0x01	172	5860	10
174	174	5870	10	000001	0x05	174	5870	10
175	175	5875	20	000010	0x09	175	5875	20
176	176	5880	10	000011	0x0D	176	5880	10
178	178	5890	10	000100	0x11	178	5890	10
180	180	5900	10	000101	0x15	180	5900	10
181	181	5905	20	000110	0x19	181	5905	20
182	182	5910	10	000111	0x1D	182	5910	10
184	184	5920	10	001000	0x21	184	5920	10

Table 6-50. 802.11a Channel Frequency and BW IP Packet-by-Packet Test Results

Test Chan	Expected Results				Actual Results			
	Channel Number	Frequency (MHz)	BW (MHz)	WTXO Channel Field	Ethereal WTXO Channel Field Results	API Tester Results	Spectrum Analyzer Results	
						Channel	Freq	BW
52	52	5260	20	001101	0x35	52	5260	20
56	56	5280	20	001110	0x39	56	5280	20
60	60	5300	20	001111	0x3D	60	5300	20
64	64	5320	20	010000	0x41	64	5320	20
149	149	5745	20	010001	0x45	149	5745	20
153	153	5765	20	010010	0x49	153	5765	20
157	157	5785	20	010011	0x4D	157	5785	20
161	161	5805	20	010100	0x51	161	5805	20

6.3.3.6 Fragment Threshold

Verify the WRM supports setting the MAC packet fragmentation length threshold. The valid range of values is 256 to 2346 bytes.

Test Cases:

1. No fragmentation.
2. One packet fragmented into two packets.
3. One packet fragmented into three packets.

Fragment Threshold Telnet Test

Table 6-51. Fragment Threshold Telnet Test

#	Description	Test Steps	Expected Results	Actual Results
	Initialization	1. Use test setup shown in Figure 6-6. WRM with Vector Signal Analyzer Test Setup. 2. Execute the Telnet initialization procedure in Section 6.2.3.1.	N/A	N/A
1.	Verify WRM does not fragment when MAC	1. Use the API Tester to send the *get fragmentthreshold* Telnet command.	API Tester displays response: *Fragment Threshold: 2346*	

#	Description	Test Steps	Expected Results	Actual Results
	packet size is less than fragment threshold.	2. Use the API Tester to enter a destination MAC address and transmit a single 1400 byte data packet w/o PBP control. 3. Use the VSA to display the MAC payload size.	VSA displays MAC payload size of 1456 bytes. (This MAC payload size accounts for 28 bytes of MAC header, 20 bytes of IP header, 8 bytes of layer 2 header, and 1400 bytes of data payload.)	
2.	Verify WRM fragments one packet into two packets when MAC packet size exceeds fragment threshold.	1. Use the API Tester to send the *set fragmentthreshold 1000* Telnet command.	API Tester displays response: *Fragment Threshold: 1000*	
		2. Use the API Tester to transmit a single 1400 byte data packet w/o PBP control. 3. Use the VSA to display the MAC payload size.	VSA displays two MAC packets, one with payload size of 1056 and another with payload size of 456 bytes.	
3.	Verify WRM fragments one packet into three packets when MAC packet size exceeds fragment threshold.	1. Use the API Tester to send the *set fragmentthreshold 500* Telnet command.	API Tester displays response: *Fragment Threshold: 500*	
		2. Use the API Tester to transmit a single 1400 byte data packet w/o PBP control. 3. Use the VSA to display the MAC payload size.	VSA displays three MAC packets, two with payload size of 556and a third with payload size of 456 bytes.	

Fragment Threshold IP Configuration Test

Table 6-52. Fragment Threshold IP Configuration Test

#	Description	Test Steps	Expected Results	Actual Results
	Initialization	1. Use test setup shown in Figure 6-6. WRM with Vector Signal Analyzer Test Setup. 2. Execute the IP initialization procedure in Section 6.2.3.2.	N/A	N/A
1.	Verify WRM does not fragment when MAC packet size is less than fragment threshold.	1. Use the API Tester to get the WRM configuration and verify the *Fragment Threshold.*	API Tester displays Fragment Threshold of 2346 bytes.	
		2. Use the API Tester to enter a destination MAC address and transmit a single 1400 byte data packet w/o PBP control. 3. Use the VSA to display the MAC payload size.	VSA displays MAC payload size of 1456 bytes.	

#	Description	Test Steps	Expected Results	Actual Results
2.	Verify WRM fragments one packet into two packets when MAC packet size exceeds fragment threshold.	1. Use the API Tester to set the *Fragment Threshold* to *1000* bytes. 2. Use Ethereal to verify the WCO Fragment Threshold field.	API Tester sends WCO with Fragmentation Threshold field (word 2, bits 0-15) set to 1000 (x03E8).	
		3. Use the API Tester to transmit a single 1400 byte data packet w/o PBP control. 4. Use the VSA to display the MAC payload size.	VSA displays two MAC packets, one with payload size of 1056 and another with payload size of 456bytes.	
3.	Verify WRM fragments one packet into three packets when MAC packet size exceeds fragment threshold.	1. Use the API Tester to set the *Fragment Threshold* to *500* bytes. 2. Use Ethereal to verify the WCO Fragmentation Threshold field.	API Tester sends WCO with Fragmentation Threshold field (word 2, bits 0-15) set to 500 (x01F4).	
		3. Use the API Tester to transmit a single 1400 byte data packet w/o PBP control. 4. Use the VSA to display the MAC payload size.	VSA displays three MAC packets, two with payload size of 556and a third with payload size of 456 bytes.	

Fragment Threshold IP Packet-by-Packet Test

Table 6-53. Fragment Threshold IP Packet-by-Packet Test

#	Description	Test Steps	Expected Results	Actual Results
	Initialization	1. Use test setup shown in Figure 6-6. WRM with Vector Signal Analyzer Test Setup. 2. Execute the IP initialization procedure in Section 6.2.3.2.	N/A	N/A
1.	Verify WRM does not fragment when MAC packet size is less than fragment threshold.	1. Use the API Tester to get the WRM configuration and verify the *Fragment Threshold.*	API Tester displays Fragment Threshold of 2346 bytes.	
		2. Use the API Tester to enter a destination MAC address and transmit a single 1400 byte data packet with PBP control. 3. Use the VSA to display the MAC payload size.	VSA displays MAC payload size of 1472 bytes. (This MAC payload size accounts for 28 bytes of MAC header, 20 bytes of IP header, 8 bytes of layer 2 header, 16 bytes of IP options, and 1400 bytes of data payload.)	

#	Description	Test Steps	Expected Results	Actual Results
2.	Verify WRM fragments one packet into two packets when MAC packet size exceeds fragment threshold.	1. Use the API Tester to set the *Fragment Threshold* to *1000* bytes and transmit a single 1400 byte data packet with PBP control. 2. Use Ethereal to verify the WTXO Fragment Threshold field.	API Tester sends WTXO with Fragmentation Threshold field (word 2, bits 0-15) set to 1000 (x03E8).	
		3. Use the VSA to display the MAC payload size.	VSA displays two MAC packets, one with payload size of 1072and another with payload size of 472 bytes.	
3.	Verify WRM fragments one packet into three packets when MAC packet size exceeds fragment threshold.	1. Use the API Tester to set the *Fragment Threshold* to *500* bytes. 2. Use Ethereal to verify the WTXO Fragment Threshold field.	API Tester sends WTXO with Fragmentation Threshold field (word 2, bits 0-15) set to 500 (x01F4).	
		3. Use the API Tester to transmit a single 1400 byte data packet w/o PBP control. 4. Use the VSA to display the MAC payload size.	VSA displays three MAC packets, two with payload size of 572 and a third with payload size of 472 bytes.	

6.3.3.7 Power

Power Level

Verify the WRM supports transmitting at power levels up to nominally 20 dBm, or higher if available. The valid range is 0 to 20 dBm in 1 dB increments or full for maximum power. (Full power may or may not be higher than 20 dBm.)

Test Cases:

1. Antenna 1 Output Power at SMA Connector
2. Antenna 2 Output Power at SMA Connector

Power Level Telnet Test

Table 6-54. Power Level Telnet Test

#	Description	Test Steps	Expected Results	Actual Results
	Initialization	1. Use test setup shown in Figure 6-5. WRM with Power Meter Test Setup, with power meter connected to antenna 1 SMA connector. 2. Execute the Telnet initialization procedure in Section 6.2.3.1.	N/A	N/A
1.	Verify WRM response to *set power 0* command.	1. Use API Tester to send the *set power 0* Telnet command and verify the response. .	API Tester displays response: *Transmit Power: 0.*	Transmit Power: 0dBm
	Verify WRM response to *get power* command.	2. Use API Tester to send the *get power* Telnet command and verify the response.	API Tester displays response: *Transmit Power: 0.*	Transmit Power: 0dBm
	Verify output power level.	3. Use API Tester to continuously broadcast packet traffic w/o PBP control. 4. Measure the transmit power at the antenna 1 SMA connector using the power meter.	Power meter displays antenna 1 power measurement = 0 dBm +/- 1 dB.	0 dBm
		5. Use API Tester to stop packet broadcast.	N/A	N/A
	Verify 1-20 dBm in 1 dB increments, and full.	6. Repeat steps 1-5 for all power settings from 1 to 20 dBm in 1 dB increments, and “full”.	API Tester displays response: Transmit Power: xx, where xx is the specified level. Power meter displays specified power within +\- 1 dB. For “full”, the power is 20 dBm +2/-1 dB.	Record results in Table 6-55.
2.	Verify output power levels on antenna 2.	1. Use the API Tester to send the *set antenna 2* Telnet command and verify the response.	API Tester displays response: *Antenna: 2.*	Antenna: 2
		2. Connect power meter to the antenna 2 SMA connector. 3. Repeat Test Case # 1 for all power settings from 0 to 20 dBm in 1 dB increments, and “full”.	API Tester displays response: Transmit Power: xx, where xx is the specified level. Power meter displays specified power within +/- 1 dB. For “full”, the power is 20 dBm +2/-1 dB.	Record results in Table 6-56.

Table 6-55. Antenna 1 Output Power Level Telnet Test Results

Power Level (dBm)	Expected Results			Actual Results		
	***set power* Response**	***get power* Response**	**Power Meter Reading**	***set power* Response**	***get power* Response**	**Power Meter Reading**
1	1	1	1	1 dBm	1 dBm	-0.15 dBm
2	2	2	2	2 dBm	2 dBm	2.5 dBm
3	3	3	3	3 dBm	3 dBm	3.9 dBm
4	4	4	4	4 dBm	4 dBm	4.5 dBm
5	5	5	5	5 dBm	5 dBm	5.9 dBm
6	6	6	6	6 dBm	6 dBm	6.8 dBm
7	7	7	7	7 dBm	7 dBm	8.2 dBm
8	8	8	8	8 dBm	8 dBm	9.0 dBm
9	9	9	9	9 dBm	9 dBm	11.0 dBm
10	10	10	10	10 dBm	10 dBm	11.9 dBm
11	11	11	11	11 dBm	11 dBm	12.5 dBm
12	12	12	12	12 dBm	12 dBm	13.7 dBm
13	13	13	13	13 dBm	13 dBm	14.6 dBm
14	14	14	14	14 dBm	14 dBm	15.5 dBm
15	15	15	15	15 dBm	15 dBm	16.5 dBm
16	16	16	16	16 dBm	16 dBm	17.4 dBm
17	17	17	17	17 dBm	17 dBm	18.3 dBm
18	18	18	18	18 dBm	18 dBm	19.0 dBm
19	19	19	19	19 dBm	19 dBm	19.5 dBm
20	20	20	20	20 dBm	20 dBm	20.1 dBm
full	full	full	20	full	full	20.5 dBm

Table 6-56. Antenna 2 Output Power Level Telnet Test Results

Power Level (dBm)	Expected Results			Actual Results		
	***set power* Response**	***get power* Response**	**Power Meter Reading**	***set power* Response**	***get power* Response**	**Power Meter Reading**
0	0	0	0	0 dBm	0 dBm	-0.7 dBm
1	1	1	1	1 dBm	1 dBm	-0.7 dBm
2	2	2	2	2 dBm	2 dBm	2.0 dBm
3	3	3	3	3 dBm	3 dBm	3.3 dBm
4	4	4	4	4 dBm	4 dBm	3.9 dBm
5	5	5	5	5 dBm	5 dBm	5.3 dBm
6	6	6	6	6 dBm	6 dBm	6.4 dBm
7	7	7	7	7 dBm	7 dBm	7.5 dBm
8	8	8	8	8 dBm	8 dBm	8.5 dBm
9	9	9	9	9 dBm	9 dBm	10.4 dBm
10	10	10	10	10 dBm	10 dBm	11.4 dBm
11	11	11	11	11 dBm	11 dBm	12.0 dBm
12	12	12	12	12 dBm	12 dBm	13.0 dBm
13	13	13	13	13 dBm	13 dBm	14.3 dBm
14	14	14	14	14 dBm	14 dBm	15.1 dBm
15	15	15	15	15 dBm	15 dBm	16.1 dBm
16	16	16	16	16 dBm	16 dBm	17.2 dBm
17	17	17	17	17 dBm	17 dBm	17.9 dBm
18	18	18	18	18 dBm	18 dBm	18.7 dBm
19	19	19	19	19 dBm	19 dBm	19.2 dBm
20	20	20	20	20 dBm	20 dBm	19.8 dBm
full	full	full	20	full	full	20.1 dBm

Power Level IP Configuration Test

Table 6-57. Power Level IP Configuration Test

#	Description	Test Steps	Expected Results	Actual Results
	Initialization	1. Use test setup shown in Figure 6-5. WRM with Power Meter Test Setup, with the power meter connected to the antenna 1 SMA connector. 2. Execute the IP initialization procedure in Section 6.2.3.2.	N/A	N/A
1.	Set WRM *power level* to *0* dBm.	1. Use the API Tester to set the WRM configuration with the *power level* at *0 dBm*. 2. Use Ethereal to verify the WCO Tx power field.	API Tester sends WCO with Tx power field (Word 1, bits 22-27) set to 0 (000000).	(W1) DD 14 1**0 0**3 1101 1101 0001 0100 0001 00**00 0000** 0011
	Verify WRM response to the *power level 0* command.	3. Use the API Tester to get the WRM configuration. 4. Use Ethereal to verify the WCO Tx power field.	WRM sends WCO with Tx power field (Word 1, bits 22-27) set to 0.	(W1, Bytes 3-4) 10 03
		5. Use the API Tester to verify the response.	API Tester displays *Power Level 0 dBm*.	0 dBm
	Verify output power level.	6. Use the API Tester to continuously broadcast packet traffic w/o PBP control. 7. Use the power meter to measure the power level.	Power meter displays antenna 1 power measurement = 0 dBm +/- 1 dB.	-0.1 dBm
		8. Use the API Tester to stop packet broadcast.	N/A	N/A
	Verify 1-20 dBm in 1 dB increments, and full.	9. Repeat steps 1-8 for all power settings from 1 to 20 dBm in 1 dB increments, and "full".	WCO Tx Power field contains the specified power level or all 1s for "full". API Tester displays *Power Level: xx*, where xx is the specified level. Power meter displays specified power within +/- 1 dB. For "full", the power is 20 dBm +2/-1 dB.	Record results in Table 6-58.
2.	Verify output power levels on antenna 2.	1. Use the API Tester to set the WRM configuration with the antenna set to 2. 2. Use the API Tester to get the WRM configuration.	API Tester displays *Antenna 2.*	Antenna = 2

#	Description	Test Steps	Expected Results	Actual Results
		3. Connect power meter to the antenna 2 SMA connector. 4. Repeat Test Case # 1 for all power settings from 0 to 20 dBm in 1 dB increments, and "full".	WCO Tx power field contains the specified power level or all 1s for "full". API Tester displays *Power Level: xx*, where xx is the specified level. Power meter displays specified power within +/- 1 dB. For "full", the power is 20 dBm +2/-1 dB.	Record results in Table 6-59.

Table 6-58. Antenna 1 Output Power Level IP Configuration Test Results

Power Level (dBm)	Expected Results				Actual Results			
	WCO Tx Power field		API Tester Power Level	Power Meter Reading	WCO Tx Power field (Word 1, bits 22-27)		API Tester Power Level	Power Meter Reading
	set	get			set	get		
1	000001	000001	1	1	01	01	1 dBm	0.0 dBm
2	000010	000010	2	2	02	02	2 dBm	2.6 dBm
3	000011	000011	3	3	03	03	3 dBm	4.0 dBm
4	000100	000100	4	4	04	04	4 dBm	4.5 dBm
5	000101	000101	5	5	05	05	5 dBm	5.8 dBm
6	000110	000110	6	6	06	06	6 dBm	6.8 dBm
7	000111	000111	7	7	07	07	7 dBm	8.3 dBm
8	001000	001000	8	8	08	08	8 dBm	9.1 dBm
9	001001	001001	9	9	09	09	9 dBm	11.0 dBm
10	001010	001010	10	10	0A	0A	10 dBm	12.3
11	001011	001011	11	11	0B	0B	11 dBm	12.6 dBm
12	001100	001100	12	12	0C	0C	12 dBm	13.8 dBm
13	001101	001101	13	13	0D	0D	13 dBm	14.7 dBm
14	001110	001110	14	14	0E	0E	14 dBm	15.6 dBm
15	001111	001111	15	15	0F	0F	15 dBm	16.6 dBm
16	010000	010000	16	16	10	10	16 dBm	17.3 dBm
17	010001	010001	17	17	11	11	17 dBm	18.5 dBm
18	010010	010010	18	18	12	12	18 dBm	19.0 dBm

Power Level (dBm)	Expected Results				Actual Results			
	WCO Tx Power field		API Tester Power Level	Power Meter Reading	WCO Tx Power field (Word 1, bits 22-27)		API Tester Power Level	Power Meter Reading
	set	get			set	get		
19	010011	010011	19	19	13	13	19 dBm	19.5 dBm
20	010100	010100	20	20	14	14	20 dBm	20.1 dBm
full	111111	111111	full	20	3F	3F	full	20.5 dBm

Table 6-59. Antenna 2 Output Power Level IP Configuration Test Results

Power Level (dBm)	Expected Results				Actual Results			
	WCO Tx Power field		API Tester Power Level	Power Meter Reading	WCO Tx Power field (Word 1, bits 22-27)		API Tester Power Level	Power Meter Reading
	set	get			set	get		
0	000000	000000	0	0	00	00	0 dBm	-0.7 dBm
1	000001	000001	1	1	01	01	1 dBm	-0.7 dBm
2	000010	000010	2	2	02	02	2 dBm	1.9 dBm
3	000011	000011	3	3	03	03	3 dBm	3.3 dBm
4	000100	000100	4	4	04	04	4 dBm	4.0 dBm
5	000101	000101	5	5	05	05	5 dBm	5.3 dBm
6	000110	000110	6	6	06	06	6 dBm	6.5 dBm
7	000111	000111	7	7	07	07	7 dBm	7.7 dBm
8	001000	001000	8	8	08	08	8 dBm	8.5 dBm
9	001001	001001	9	9	09	09	9 dBm	10.4 dBm
10	001010	001010	10	10	0A	0A	10 dBm	11.3 dBm
11	001011	001011	11	11	0B	0B	11 dBm	12.0 dBm
12	001100	001100	12	12	0C	0C	12 dBm	13.0 dBm
13	001101	001101	13	13	0D	0D	13 dBm	14.3 dBm
14	001110	001110	14	14	0E	0E	14 dBm	15.1 dBm
15	001111	001111	15	15	0F	0F	15 dBm	16.1 dBm
16	010000	010000	16	16	10	10	16 dBm	17.1 dBm
17	010001	010001	17	17	11	11	17 dBm	18.0 dBm
18	010010	010010	18	18	12	12	18 dBm	18.6 dBm
19	010011	010011	19	19	13	13	19 dBm	19.2 dBm

Power Level (dBm)	Expected Results				Actual Results			
	WCO Tx Power field		API Tester Power Level	Power Meter Reading	WCO Tx Power field (Word 1, bits 22-27)		API Tester Power Level	Power Meter Reading
	set	get			set	get		
20	010100	010100	20	20	14	14	20 dBm	19.8 dBm
full	111111	111111	full	20	3F	3F	full	20.1 dBm

Power Level IP Packet-by-Packet Test

Table 6-60. Power Level IP Packet-by-Packet Test

#	Description	Test Steps	Expected Results	Actual Results
	Initialization	1. Use test setup shown in Figure 6-5. WRM with Power Meter Test Setup, with the power meter connected to the antenna 1 SMA connector. 2. Execute the IP initialization procedure in Section 6.2.3.2.	N/A	N/A
1.	Set WRM *power level* to *0* dBm using PBP control.	1. Use the API Tester to set the WRM configuration *power level* to *0 dBm* and transmit one packet with PBP control. 2. Use Ethereal to verify the WTXO Tx power field.	API Tester sends WTXO with Tx power field (Word 1, bits 22-27) set to 0 (000000).	(W1) D9 10 1**0 0**3 1101 1001 0001 0000 0001 00**00 0000** 0011
	Verify WRM configuration.	3. Use the API Tester to get the WRM configuration.	API Tester displays *Power Level 0 dBm*.	0 dBm
	Verify output power level.	4. Use the API Tester to continuously broadcast packet traffic with PBP control. 5. Use the power meter to measure the power level.	Power meter displays antenna 1 power measurement = 0 dBm +/- 1 dB.	-0.7 dBm
		6. Use API Tester to stop packet broadcast	N/A	N/A
	Verify 1-20 dBm in 1 dB increments, and full.	7. Repeat steps 1- 6 for all power settings from 1 to 20 dBm in 1 dB increments, and "full".	WTXO field contains the specified power level or all 1s for "full". API Tester displays *Power Level: xx*, where xx is the specified level. Power meter displays specified power within +/- 1 dB. For "full", the power is 20 dBm +2/-1 dB.	Record results in Table 6-61.

#	Description	Test Steps	Expected Results	Actual Results
2.	Verify output power levels on antenna 2.	1. Use the API Tester to set the WRM configuration with the antenna set to 2.	N/A	Antenna = 2
		2. Connect power meter to the antenna 2 SMA connector. 3. Repeat Test Case # 1 for all power settings from 0 to 20 dBm in 1 dB increments, and "full".	WTXO field contains the specified power level or all 1s for "full". API Tester displays *Power Level: xx*, where xx is the specified level. Power meter displays specified power within +/- 1 dB. For "full", the power is 20 dBm +2/-1 dB.	Record results in Table 6-62.

Table 6-61. Antenna 1 Output Power Level IP Packet-by-Packet Test Results

Power Level (dBm)	Expected Results			Actual Results		
	WTXO Tx Power field	API Tester Power Level	Power Meter Reading	WTXO Tx Power field (W1, bits 22-27)	API Tester Power Level	Power Meter Reading
1	000001	1	1	0x01	1 dBm	0.0 dBm
2	000010	2	2	0x02	2 dBm	2.7 dBm
3	000011	3	3	0x03	3 dBm	4.0 dBm
4	000100	4	4	0x04	4 dBm	4.8 dBm
5	000101	5	5	0x05	5 dBm	6.1 dBm
6	000110	6	6	0x06	6 dBm	6.9 dBm
7	000111	7	7	0x07	7 dBm	8.1 dBm
8	001000	8	8	0x08	8 dBm	9.1 dBm
9	001001	9	9	0x09	9 dBm	10.9 dBm
10	001010	10	10	0x0A	10 dBm	11.7 dBm
11	001011	11	11	0x0B	11 dBm	12.6 dBm
12	001100	12	12	0x0C	12 dBm	13.7 dBm
13	001101	13	13	0x0D	13 dBm	14.6 dBm
14	001110	14	14	0x0E	14 dBm	15.4 dBm
15	001111	15	15	0x0F	15 dBm	16.4 dBm
16	010000	16	16	0x10	16 dBm	17.2 dBm

Power Level (dBm)	Expected Results			Actual Results		
	WTXO Tx Power field	API Tester Power Level	Power Meter Reading	WTXO Tx Power field (W1, bits 22-27)	API Tester Power Level	Power Meter Reading
17	010001	17	17	0x11	17 dBm	18.4 dBm
18	010010	18	18	0x12	18 dBm	18.9 dBm
19	010011	19	19	0x13	19 dBm	19.4 dBm
20	010100	20	20	0x14	20 dBm	20.0 dBm
full	111111	full	20	0x3F	full	20.5 dBm

Table 6-62. Antenna 2 Output Power Level IP Packet-by-Packet Test Results

Power Level (dBm)	Expected Results			Actual Results		
	WTXO Tx Power field	API Tester Power Level	Power Meter Reading	WTXO Tx Power field (W1, bits 22-27)	API Tester Power Level	Power Meter Reading
0	000000	0	0	0x00	0 dBm	-0.7 dBm
1	000001	1	1	0x01	1 dBm	-0.6 dBm
2	000010	2	2	0x02	2 dBm	2.1 dBm
3	000011	3	3	0x03	3 dBm	3.4 dBm
4	000100	4	4	0x04	4 dBm	3.9 dBm
5	000101	5	5	0x05	5 dBm	5.5 dBm
6	000110	6	6	0x06	6 dBm	6.2 dBm
7	000111	7	7	0x07	7 dBm	7.4 dBm
8	001000	8	8	0x08	8 dBm	8.4 dBm
9	001001	9	9	0x09	9 dBm	10.4 dBm
10	001010	10	10	0x0A	10 dBm	11.4 dBm
11	001011	11	11	0x0B	11 dBm	12.4 dBm
12	001100	12	12	0x0C	12 dBm	13.3 dBm
13	001101	13	13	0x0D	13 dBm	14.1 dBm
14	001110	14	14	0x0E	14 dBm	15.1 dBm
15	001111	15	15	0x0F	15 dBm	16.1 dBm
16	010000	16	16	0x10	16 dBm	17.0 dBm
17	010001	17	17	0x11	17 dBm	17.8 dBm

Power Level (dBm)	Expected Results			Actual Results		
	WTXO Tx Power field	API Tester Power Level	Power Meter Reading	WTXO Tx Power field (W1, bits 22-27)	API Tester Power Level	Power Meter Reading
18	010010	18	18	0x12	18 dBm	18.5 dBm
19	010011	19	19	0x13	19 dBm	19.1 dBm
20	010100	20	20	0x14	20 dBm	19.7 dBm
full	111111	full	20	0x3F	full	20.1 dBm

WAVE Channel Power Limiting

Verify the WRM limits the transmit power at the SMA connector for WAVE channels so the maximum allowable level at the antenna input will not be exceeded. The maximum allowable antenna input power is a function of unit mode and channel. The maximum allowable power at the SMA connector is a function of the maximum allowable antenna input power and the antenna compensation factor.

Test Cases:

1. Power Limiting at Antenna 1 SMA Connector
2. Power Limiting at Antenna 2 SMA Connector

RSU Power Limiting Telnet Test

Table 6-63. RSU Power Limiting Telnet Test

#	Description	Test Steps	Expected Results	Actual Results
	Initialization	1. Use the test setup shown in Figure 6-5. WRM with Power Meter Test Setup, with the power meter connected to the antenna 1 SMA connector. 2. Execute Telnet initialization procedure in Section 6.2.3.1.	N/A	N/A
1.	Set the WRM unit mode to RSU.	1. Use the API Tester to send the *set unitmode RSU* Telnet command and verify the response.	API Tester displays response: *Unit Mode: RSU.*	Unit Mode: RSU

#	Description	Test Steps	Expected Results	Actual Results
	Set the channel, antenna compensation factor, and power setting.	2. Use the API Tester to send the *set channel 172* Telnet command. 3. Use the API Tester to send the *set antenna1comp 0* Telnet command. 4. Use the API Tester to send the *set power 10* Telnet command. 5. Use the API Tester to verify the response for the above commands.	API Tester displays response: *Radio Frequency: 5860 MHz (IEEE 172).* API Tester displays response: *Antenna1comp: 0.* API Tester displays response: *Transmit Power: 10.*	Radio Frequency: 5860 MHz (IEEE 172) Antenna 1 Comp: 0 dB Transmit Power: 10 dBm
	Verify the output power level at the SMA antenna connector.	6. Use the API Tester to continuously broadcast packets w/o PBP control. 7. Measure the transmit power at the antenna 1 SMA connector using the power meter.	Power meter displays antenna 1 power = 10 dBm +/- 1 dB.	12.1 dBm
		8. Use the API Tester to stop packet broadcast.	N/A	N/A
	Verify the output power levels for other parameter settings.	9. Repeat steps 2-8 using the combinations of channel, antenna compensation factor, and power levels listed in Table 6-64.	See Table 6-64.	Record results in Table 6-64.
2.	Set the antenna to 2.	1. Use the API Tester to send the *set antenna 2* Telnet command and verify the response. 2. Connect the power meter to the antenna 2 SMA connector.	API Tester display response: *Antenna: 2.*	Antenna: 2
	Verify the output power levels.	3. Execute Test Case # 1, steps 2-9 using the combinations of channel, antenna compensation factor, and power levels listed in Table 6-65. Measure output power at the antenna 2 SMA connector.	See Table 6-65.	Record results in Table 6-65.

Table 6-64. RSU Power Limiting at Antenna 1 Telnet Test Results

Channel	Ant. Input Limit (dBm)	Antenna Comp.	Power	Expected Results (dBm)	Actual Results (dBm)				
					Channel 172	Channel 174	Channel 176	Channel 178	Channel 184
172, 174, 176, 178,	28.8	0	10	10	12.1	12.1	12.0	12.1	12.0
			15	15	16.7	16.4	16.3	16.4	16.5
			20	20	20.5	20.2	20.1	20.1	20.2
		10	10	10	12.1	12.1	11.7	11.8	11.8

Channel	Ant. Input Limit (dBm)	Antenna Comp.	Power	Expected Results (dBm)	Actual Results (dBm)				
					Channel 172	**Channel 174**	**Channel 176**	**Channel 178**	**Channel 184**
184			15	15	16.7	16.4	16.3	16.4	16.5
			20	19	19.8	19.6	19.4	19.5	19.6
		19	10	10	12.1	11.9	11.8	11.8	11.8
			15	10	12.1	11.8	11.7	11.7	11.7
			20	10	12.1	11.8	11.7	11.8	11.7
					Channel 175	**Channel 180**	**Channel 181**	**Channel 182**	
175, 180, 181, 182	10.0	-10	0	0	-0.1	0.1	-0.1	0.0	
			10	10	11.2	12.4	11.5	12.4	
			20	20	19.5	20.4	19.7	20.5	
		-5	0	0	-0.3	0.0	0.1	0.0	
			10	10	11.3	12.1	11.4	12.1	
			20	15	15.9	16.6	16.2	16.8	
		0	0	0	-0.2	0.0	0.0	0.0	
			10	10	11.2	12.1	11.3	12.1	
			20	10	11.2	12.1	11.6	12.1	

Table 6-65. RSU Power Limiting at Antenna 2 Telnet Test Results

Channel	Ant. Input Limit (dBm)	Antenna Comp.	Power	Expected Results (dBm)	Actual Results (dBm)				
					Channel 172	Channel 174	Channel 176	Channel 178	Channel 184
172, 174, 176, 178, 184	28.8	0	10	10	11.3	10.7	11.3	11.3	10.5
			15	15	16.1	15.5	16.0	16.1	15.2
			20	20	19.8	19.2	19.8	19.9	19.1
		10	10	10	11.2	10.8	11.2	11.3	10.5
			15	15	16.0	15.5	16.0	16.0	15.2
			20	19	19.1	18.7	19.2	19.2	18.4
		19	10	10	11.3	10.7	11.3	11.3	10.5
			15	10	11.3	10.7	11.3	11.3	10.5
			20	10	11.3	10.7	11.3	11.3	10.5
					Channel 175	**Channel 180**	**Channel 181**	**Channel 182**	
175, 180, 181, 182	10.0	-10	0	0	-1.0	-0.9	-1.2	-1.2	
			10	10	10.4	11.1	10.0	10.6	
			20	20	18.9	19.3	18.4	19.0	
		-5	0	0	-0.9	-0.8	-1.4	-1.2	
			10	10	10.4	11.0	10.2	10.5	
			20	15	15.0	15.7	14.8	15.4	
		0	0	0	-1.0	-1.0	-1.3	-1.3	
			10	10	10.5	11.0	10.0	10.5	
			20	10	10.5	11.0	10.0	10.6	

RSU Power Limiting IP Configuration Test

Table 6-66. RSU Power Limiting IP Configuration Test

#	Description	Test Steps	Expected Results	Actual Results
	Initialization	1. Use the test setup shown in Figure 6-5. WRM with Power Meter Test Setup, with the power meter connected to the antenna 1 SMA connector. 2. Execute IP initialization procedure in Section 6.2.3.2.	N/A	N/A
1.	Set the WRM *unit mode* to *RSU*.	1. Use the API Tester to set the WRM unit mode to RSU. 2. Use the API Tester to get the current WRM configuration and verify the response.	API Tester displays unit mode as RSU.	RSU
	Set the channel, antenna compensation factor, and power setting.	3. Use the API Tester to set the WRM configuration to channel 172, antenna1 compensation as 0 and power level as 10. 4. Use the API Tester to get the WRM configuration and verify the response for the above commands.	API Tester displays channel 172, antenna1 compensation as 0, and power level as 10.	Channel = 172 Antenna 1 Comp = 0 Tx Power = 10 dBm
	Verify the power output level at the SMA antenna connector.	5. Use the API Tester to continuously broadcast packets w/o PBP control. 6. Measure the transmit power at the antenna 1 SMA connector using the power meter.	Power meter displays antenna 1 power = 10 dBm +/- 1 dB.	12.0 dBm
	Verify the power output level for other parameter settings.	7. Repeat steps 3-6 using the combinations of channel, antenna compensation factor, and power levels listed in Table 6-67.	See Table 6-67.	Record results in Table 6-67.
2.	Set the antenna to 2.	1. Use the API Tester to set the antenna to 2. 2. Use API Tester to get the WRM configuration and verify the response. 3. Connect the power meter to the antenna 2 SMA connector.	API Tester displays antenna 2.	Antenna = 2
	Verify the output power levels.	4. Execute Test Case # 1, steps 3-7 using the combinations of channel, antenna compensation factor, and power levels listed in Table 6-68. Measure output power at the antenna 2 SMA connector.	See Table 6-68.	Record results in Table 6-68.

Table 6-67. RSU Power Limiting at Antenna 1 IP Configuration Test Results

Channel	Ant. Input Limit (dBm)	Antenna Comp.	Power	Expected Results (dBm)	Actual Results (dBm)				
					Channel 172	Channel 174	Channel 176	Channel 178	Channel 184
172, 174, 176, 178, 184	28.8	0	10	10	12.0	11.7	11.9	11.9	11.8
			15	15	16.5	16.3	16.0	16.0	16.1
			20	20	20.4	20.1	19.9	20.0	20.0
		10	10	10	12.2	11.6	11.7	11.8	11.6
			15	15	16.6	16.4	16.3	16.2	16.5
			20	19	19.7	19.3	19.1	19.2	19.6
		19	10	10	12.0	11.9	11.6	11.7	11.8
			15	10	11.9	11.8	11.7	11.8	11.6
			20	10	12.0	11.8	11.5	11.6	11.7
					Channel 175	**Channel 180**	**Channel 181**	**Channel 182**	
175, 180, 181, 182	10.0	-10	0	0	-0.3	0.1	-0.1	0.1	
			10	10	11.2	12.0	11.3	12.2	
			20	20	19.3	20.1	19.5	20.4	
		-5	0	0	-0.3	0.0	-0.2	0.1	
			10	10	11.2	12.1	11.4	12.0	
			20	15	15.7	16.4	15.8	16.5	
		0	0	0	-0.3	0.1	-0.3	0.1	
			10	10	11.2	12.2	11.1	12.0	
			20	10	11.2	12.2	11.1	12.0	

Table 6-68. RSU Power Limiting at Antenna 2 IP Configuration Test Results

Channel	Ant. Input Limit (dBm)	Antenna Comp.	Power	Expected Results (dBm)	Actual Results (dBm)				
					Channel 172	Channel 174	Channel 176	Channel 178	Channel 184
172, 174, 176, 178, 184	28.8	0	10	10	10.4	10.9	11.3	11.4	10.3
			15	15	15.3	15.6	16.0	16.1	15.1
			20	20	18.8	19.2	19.8	19.8	19.0
		10	10	10	10.4	11.2	11.3	11.7	10.4
			15	15	15.2	15.5	16.1	16.0	15.2

Channel	Ant. Input Limit (dBm)	Antenna Comp.	Power	Expected Results (dBm)	Actual Results (dBm)				
					Channel 172	**Channel 174**	**Channel 176**	**Channel 178**	**Channel 184**
			20	19	18.0	18.7	19.2	19.1	18.3
		19	10	10	10.2	10.8	11.2	11.2	10.6
			15	10	10.3	10.9	11.3	11.3	10.4
			20	10	10.2	11.0	11.2	11.4	10.4
					Channel 175	**Channel 180**	**Channel 181**	**Channel 182**	
175, 180, 181, 182	10.0	-10	0	0	-1.1	-1.1	-1.3	-1.3	
			10	10	10.5	10.9	10.1	10.7	
			20	20	18.7	19.3	18.4	18.9	
		-5	0	0	-1.1	-1.0	-1.3	-1.5	
			10	10	10.3	11.3	10.0	10.4	
			20	15	15.1	16.0	14.8	15.4	
		0	0	0	-1.0	-1.0	-1.4	-1.4	
			10	10	10.3	10.9	10.0	10.4	
			20	10	10.3	10.9	10.0	10.5	

RSU Power Limiting Packet-by-Packet IP Test

Table 6-69. RSU Power Limiting Packet-by-Packet IP Test

#	Description	Test Steps	Expected Results	Actual Results
	Initialization	1. Use the test setup shown in Figure 6-5. WRM with Power Meter Test Setup, with the power meter connected to the antenna 1 SMA connector. 2. Execute IP initialization procedure in Section 6.2.3.2.	N/A	N/A
1.	Set the WRM *unit mode* to *RSU*, channel, antenna compensation factor, and power setting for use by PBP control.	1. Use the API Tester to set the antenna 1 compensation to 0 using IP Configuration. 2. Use the API Tester to set the WRM *unit mode* to *RSU*, channel to 172, and power level as 10.	N/A	N/A
	Verify the power output level at the SMA antenna connector.	3. Use the API Tester to continuously broadcast packets with PBP control. 4. Measure the transmit power at the antenna 1 SMA connector using the power meter.	Power meter displays antenna 1 power = 10 dBm +/- 1 dB.	12.0 dBm
		5. Use the API Tester to stop packet broadcast.	N/A	N/A
	Verify the power output level for other parameter settings.	6. Repeat steps 1-5 using the combinations of channel, antenna compensation factor, and power levels listed in 7. Table 6-70.	See Table 6-70.	Record results in Table 6-70.
2.	Set the antenna to 2.	1. Use the API Tester to set the antenna to 2 for PBP control.	N/A	
	Verify the output power levels.	2. Execute Test Case # 1, steps 1-6 using the combinations of channel, antenna compensation factor, and power levels listed in Table 6-71. Measure output power at the antenna 2 SMA connector.	See Table 6-71.	Record results in Table 6-71.

Table 6-70. RSU Power Limiting at Antenna 1 Packet-by-Packet IP Test Results

Channel	Ant. Input Limit (dBm)	Antenna Comp.	Power	Expected Results (dBm)	Actual Results (dBm)				
					Channel 172	Channel 174	Channel 176	Channel 178	Channel 184
172, 174, 176, 178, 184	28.8	0	10	10	12.0	11.7	11.8	11.9	11.9
			15	15	16.4	16.1	16.2	16.1	16.3
			20	20	20.2	20.1	20.0	20.0	20.1
		10	10	10	12.0	11.7	11.8	11.8	11.8
			15	15	16.4	16.3	16.3	16.1	16.5
			20	19	19.7	19.6	19.3	19.5	19.6
		19	10	10	12.0	11.8	11.8	11.9	11.9
			15	10	12.1	12.0	11.7	11.8	11.8
			20	10	12.2	11.9	11.7	11.8	11.8
					Channel 175	**Channel 180**	**Channel 181**	**Channel 182**	
175, 180, 181, 182	10.0	-10	0	0	-0.3	0.1	0.0	0.0	
			10	10	11.2	12.3	11.6	12.3	
			20	20	19.4	20.3	19.8	20.4	
		-5	0	0	-0.3	0.1	0.0	0.1	
			10	10	11.3	12.0	11.5	12.1	
			20	15	15.7	16.4	16.0	16.5	
		0	0	0	-0.3	0.1	-0.1	0.1	
			10	10	11.3	12.1	11.6	12.2	
			20	10	11.3	12.0	11.6	12.1	

Table 6-71. RSU Power Limiting at Antenna 2 Packet-by-Packet IP Test Results

Channel	Ant. Input Limit (dBm)	Antenna Comp.	Power	Expected Results (dBm)	Actual Results (dBm)				
					Channel 172	Channel 174	Channel 176	Channel 178	Channel 184
172, 174, 176, 178, 184	28.8	0	10	10	10.3	11.0	11.3	11.3	10.8
			15	15	15.1	15.5	15.9	15.9	15.2
			20	20	18.7	19.2	19.7	19.7	19.0
		10	10	10	10.4	10.7	11.5	11.4	10.7
			15	15	15.0	15.6	16.0	15.9	15.1
			20	19	18.1	18.6	19.1	19.1	18.3
		19	10	10	10.3	10.7	11.2	11.2	10.7
			15	10	10.3	10.7	11.2	11.2	10.7
			20	10	10.3	10.7	11.2	11.2	10.7
					Channel 175	**Channel 180**	**Channel 181**	**Channel 182**	
175, 180, 181, 182	10.0	-10	0	0	-0.9	-1.0	-1.3	-1.4	
			10	10	10.3	10.9	10.0	10.5	
			20	20	18.9	19.3	18.4	18.9	
		-5	0	0	-0.9	-0.9	-1.3	-1.5	
			10	10	10.4	10.9	10.0	10.9	
			20	15	15.1	15.7	14.7	15.2	
		0	0	0	-0.9	-1.0	-1.3	-1.3	
			10	10	10.5	10.8	10.4	10.7	
			20	10	10.5	10.9	10.4	10.8	

OBU Power Limiting Telnet Test

Table 6-72. OBU Power Limiting Telnet Test

#	Description	Test Steps	Expected Results	Actual Results
	Initialization	1. Use the test setup shown in Figure 6-5. WRM with Power Meter Test Setup, with the power meter connected to the antenna 1 SMA connector. 2. Execute Telnet initialization procedure in Section 6.2.3.1.	N/A	N/A
1.	Set the WRM unit mode to OBU.	1. Use the API Tester to send the *set unitmode OBU* Telnet command and verify the response.	API Tester displays response: *Unit Mode: OBU.*	Unit Mode: OBU
	Set the channel, antenna compensation factor, and power setting.	2. Use the API Tester to send the *set channel 172* Telnet command. 3. Use the API Tester to send the *set antenna1comp –5* Telnet command. 4. Use the API Tester to send the *set power 9* Telnet command. 5. Use the API Tester to verify the response for the above commands.	API Tester displays response: *Radio Frequency: 5860 MHz (IEEE 172).* API Tester displays response: *Antenna1comp: -5.* API Tester displays response: *Transmit Power: 9.*	Radio Frequency: 5860 MHz (IEEE 172) Antenna 1 Comp: -5 Transmit Power: 9 dBm
	Verify the output power level at the SMA antenna connector.	6. Use the API Tester to continuously broadcast packets. 7. Measure the transmit power at the antenna 1 SMA connector using the power meter.	Power meter displays antenna 1 power = 9dBm +/- 1 dB.	11.0 dBm
		8. Use the API Tester to stop packet broadcast.	N/A	N/A
	Verify the output power level for other parameter settings.	9. Repeat steps 2-8 using the combinations of channel, antenna compensation factor, and power levels listed in Table 6-73.	See Table 6-73.	Record results in Table 6-73.
2.	Set the antenna to 2.	1. Use the API Tester to send the *set antenna 2* Telnet command and verify the response. 2. Connect the power meter to the antenna 2 SMA connector.	API Tester display response: *Antenna: 2.*	Antenna: 2
	Verify output power levels.	3. Execute Test Case # 1, steps 2-9 using the combinations of channel, antenna compensation factor, and power levels listed in Table 6-74. Measure output power at the antenna 2 SMA connector.	See Table 6-74.	Record results in Table 6-74.

Table 6-73. OBU Power Limiting at Antenna 1 Telnet Test Results

Channel	Ant. Input Limit (dBm)	Antenna Comp.	Power	Expected Results (dBm)	Actual Results (dBm)				
					Channel 172	Channel 174	Channel 176	Channel 178	Channel 184
172, 174, 176, 178, 184	28.8	0	10	10	12.0	11.6	11.8	11.8	11.8
			15	15	16.6	16.1	16.0	16.4	16.8
			20	20	20.4	20.1	19.9	20.0	20.1
		10	10	10	11.9	12.0	11.4	11.9	11.8
			15	15	16.7	16.2	15.9	16.2	16.3
			20	19	19.5	19.4	19.2	19.3	19.6
		19	10	10	12.0	12.1	11.7	11.8	11.9
			15	10	12.1	12.0	11.8	11.9	11.9
			20	10	12.2	11.9	11.8	11.9	12.0
					Channel 175				
175	10.0	-10	0	0	-0.3				
			10	10	11.0				
			20	20	19.3				
		-5	0	0	-0.3				
			10	10	11.3				
			20	15	15.7				
		0	0	0	-0.3				
			10	10	11.0	**Channel 180**	**Channel 181**	**Channel 182**	
			20	10	11.0				
180, 181, 182	20.0	0	10	10		12.0	11.5	12.3	
			15	15		16.8	15.8	16.6	
			20	20		20.1	19.5	20.2	
		5	10	10		12.0	11.6	12.1	
			15	15		16.4	16.0	16.6	
			20	15		16.5	15.9	16.5	
		10	10	10		12.2	11.6	12.0	
			15	10		12.2	11.6	12.0	
			20	10		12.2	11.5	12.1	

Table 6-74. OBU Power Limiting at Antenna 2 Telnet Test Results

Channel	Ant. Input Limit (dBm)	Antenna Comp.	Power	Expected Results (dBm)	Actual Results (dBm)				
					Channel 172	Channel 174	Channel 176	Channel 178	Channel 184
172, 174, 176, 178, 184	28.8	0	10	10	10.6	11.0	11.2	11.5	10.8
			15	15	15.2	15.7	16.0	16.3	15.4
			20	20	18.6	19.0	19.7	19.9	19.0
		10	10	10	10.5	10.6	11.1	11.6	10.7
			15	15	14.9	15.3	15.8	16.1	15.1
			20	19	18.0	18.6	19.0	19.3	18.4
		19	10	10	10.5	10.7	11.3	11.7	10.4
			15	10	10.5	10.8	11.3	11.8	10.4
			20	10	10.5	10.7	11.3	11.4	10.4
					Channel 175	**Channel 180**	**Channel 181**	**Channel 182**	
175	10.0	-10	0	0	-1.2				
			10	10	10.4				
			20	20	18.7				
		-5	0	0	-1.1				
			10	10	10.5				
			20	15	15.0				
		0	0	0	-1.1				
			10	10	10.5				
			20	10	10.5				
180, 181, 182	20.0	0	10	10		11.0	10.1	10.5	
			15	15		16.1	15.0	15.3	
			20	20		19.4	18.4	19.0	
		5	10	10		11.0	10.0	10.5	
			15	15		15.6	15.0	15.3	
			20	15		15.6	15.1	15.2	
		10	10	10		10.9	10.5	10.6	
			15	10		10.9	10.5	10.6	
			20	10		10.9	10.5	10.5	

OBU Power Limiting IP Configuration Test

Table 6-75. OBU Power Limiting IP Configuration Test

#	Description	Test Steps	Expected Results	Actual Results
	Initialization	1. Use the test setup shown in Figure 6-5. WRM with Power Meter Test Setup, with the power meter connected to the antenna 1 SMA connector. 2. Execute IP initialization procedure in Section 6.2.3.2.	N/A	N/A
1.	Set the WRM *unit mode* to *OBU*.	1. Use the API Tester to set the WRM *unit mode* to *OBU*. 2. Use the API Tester to get the current WRM configuration and verify the response.	API Tester displays unit mode as OBU.	Unit Mode = OBU
	Set the channel, antenna compensation factor, and power setting.	3. Use the API Tester to set the WRM configuration to channel 172, antenna1 compensation as 0 and power level as 10. 4. Use the API Tester to get the WRM configuration and verify the response for the above commands.	API Tester displays channel 172, antenna1 compensation as 0 and power level as 10.	Channel = 172 Antenna 1 Comp = 0 Tx Power = 10
	Verify the output power level at the SMA antenna connector.	5. Use the API Tester to continuously broadcast packets w/o PbP control. 6. Measure the transmit power at the antenna 1 SMA connector using the power meter.	Power meter displays antenna 1 power = 10 dBm +/- 1 dB.	12.0 dBm
		7. Use the API Tester to stop packet broadcast.	N/A	N/A
	Verify the output power level for other parameter settings.	8. Repeat steps 3-7 using the combinations of channel, antenna compensation factor, and power levels listed in 9. Table 6-76.	See Table 6-76.	Record results in Table 6-76
2.	Set the antenna to 2.	1. Use the API Tester to set the antenna to 2. 2. Use API Tester to get the WRM configuration and verify the response. 3. Connect the power meter to the antenna 2 SMA connector.	API Tester displays antenna 2.	Antenna = 2

#	Description	Test Steps	Expected Results	Actual Results
	Verify output power levels.	4. Execute Test Case # 1, steps 3-8 using the combinations of channel, antenna compensation factor, and power levels listed in **Table 6-77**. Measure output power of antenna 2 instead of antenna 1.	See **Table 6-77**.	Record results in **Table 6-77**

Table 6-76. OBU Power Limiting at Antenna 1 IP Configuration Test Results

Channel	Ant. Input Limit (dBm)	Antenna Comp.	Power	Expected Results (dBm)	Actual Results (dBm)				
					Channel 172	Channel 174	Channel 176	Channel 178	Channel 184
172, 174, 176, 178, 184	28.8	0	10	10	12.0	11.9	11.5	11.9	11.8
			15	15	16.8	16.5	16.2	16.1	16.3
			20	20	20.2	20.1	19.9	20.0	20.1
		10	10	10	12.0	11.8	11.8	11.7	11.8
			15	15	16.5	16.2	16.1	16.4	16.3
			20	19	19.8	19.5	19.2	19.3	19.4
		19	10	10	12.2	12.0	11.8	11.6	11.8
			15	10	12.2	12.0	11.6	11.6	11.8
			20	10	12.0	12.0	11.7	11.6	11.7
					Channel 175	**Channel 180**	**Channel 181**	**Channel 182**	
175	10.0	-10	0	0	-0.4				
			10	10	11.0				
			20	20	19.3				
		-5	0	0	-0.4				
			10	10	11.1				
			20	15	15.7				
		0	0	0	-0.4				
			10	10	11.1				
			20	10	11.1				
180, 181, 182	20.0	0	10	10		12.0	11.4	12.0	
			15	15		16.5	15.7	16.7	
			20	20		20.3	19.6	20.3	
		5	10	10		11.9	11.4	12.0	
			15	15		16.6	15.9	16.7	
			20	15		16.5	16.0	16.7	
		10	10	10		12.1	11.3	12.2	
			15	10		12.1	11.3	12.2	
			20	10		12.1	11.5	12.1	

Table 6-77. OBU Power Limiting at Antenna 2 IP Configuration Test Results

Channel	Ant. Input Limit (dBm)	Antenna Comp.	Power	Expected Results (dBm)	Actual Results (dBm)				
					Channel 172	Channel 174	Channel 176	Channel 178	Channel 184
172, 174, 176, 178, 184	28.8	0	10	10	10.2	10.5	11.4	11.4	10.7
			15	15	14.9	15.2	15.8	16.3	15.2
			20	20	18.5	19.0	19.6	19.9	18.9
		10	10	10	10.2	10.5	11.2	11.2	10.4
			15	15	14.9	15.3	16.0	16.0	15.0
			20	19	17.9	18.5	18.9	19.2	18.3
		19	10	10	10.3	10.5	11.3	11.3	10.6
			15	10	10.3	10.5	11.3	11.3	10.6
			20	10	10.4	10.5	11.4	11.3	10.6
					Channel 175	**Channel 180**	**Channel 181**	**Channel 182**	
175	10.0	-10	0	0	-1.2				
			10	10	10.2				
			20	20	18.6				
		-5	0	0	-1.1				
			10	10	10.2				
			20	15	14.9				
		0	0	0	-1.1				
			10	10	10.2				
			20	10	10.2				
180, 181, 182	20.0	0	10	10		11.2	10.2	10.7	
			15	15		15.7	14.8	15.4	
			20	20		19.4	18.5	18.9	
		5	10	10		11.2	10.2	10.6	
			15	15		15.6	14.7	15.6	
			20	15		15.9	14.8	15.5	
		10	10	10		11.2	10.2	10.7	
			15	10		11.1	10.3	10.6	
			20	10		11.1	10.3	10.7	

6.3.3.8 Data Rate

Verify the WRM supports all data rates specified by ASTM E2213-03 for channels operating with a 10 MHz bandwidth. Verify the WRM supports all data rates specified by IEEE 802.11a for channels operating with a 20 MHz bandwidth.

Test Cases:

1. 10 MHz Data Rates
2. 20 MHz Data Rates

Data Rate Telnet Test

Table 6-78. Data Rate Telnet Test

#	Description	Test Steps	Expected Results	Actual Results
	Initialization.	1. Use the test setup shown in Figure 6-6. WRM with Vector Signal Analyzer Test Setup. 2. Execute Telnet initialization procedure in Section 6.2.3.1.	N/A	N/A
1.	Verify WRM response to *set rate 3* command.	1. Use the API Tester to send the *set rate 3* command and verify the response.	API Tester displays response: *Data Rate: 3*	Data Rate: 3
	Verify the WRM response to *get rate* command.	2. Use the API Tester to send the *get rate* Telnet command and verify the response.	API Tester displays response: *Data Rate: 3.*	Data Rate: 3
	Verify WRM operation.	3. Use the API Tester to continuously broadcast packets w/o PBP control. 4. Use VSA to verify WRM is transmitting at the 3 Mbps data rate.	VSA shows WRM is transmitting at 3 Mbps.	3 Mbps
		5. Use the API Tester to stop packet broadcast.	N/A	N/A
	Verify all remaining 10 MHz data rates.	6. Repeat steps 1-5 for all data rates listed in Table 6-79.	API Tester displays WRM response showing selected data rate. VSA verifies data rate is correct.	Record results in Table 6-79
2.	Switch to 20 MHz channel.	1. Use API Tester to send command *set fastchannel 52* and verify the response.	API Tester displays response: *Radio Frequency: 5260 MHz (IEEE 52).*	Radio Frequency: 5260 (IEEE 52)
	Verify all 20 MHz data rates.	2. Repeat Test Case # 1, steps 1-5 for all data rates listed in Table 6-80.	API Tester displays WRM response showing selected data rate. VSA verifies data rate is correct.	Record results in Table 6-80

Table 6-79. 10MHz Channel Data Rate Telnet Test Results

Data Rate	Expected Results			Actual Results		
	set data rate	***get data rate***	**VSA**	***set data rate***	***get data rate***	**VSA**
4.5	4.5	4.5	4.5	4.5	4.5	4.5 Mbps
6	6	6	6	6	6	6 Mbps
9	9	9	9	9	9	9 Mbps
12	12	12	12	12	12	12 Mbps
18	18	18	18	18	18	18 Mbps
24	24	24	24	24	24	24 Mbps
27	27	27	27	27	27	27 Mbps

Table 6-80. 20MHz Channel Data Rate Telnet Test Results

Data Rate	Expected Results			Actual Results		
	set data rate	***get data rate***	**VSA**	***set data rate***	***get data rate***	**VSA**
6	6	6	6	6	6	6 Mbps
9	9	9	9	9	9	9 Mbps
12	12	12	12	12	12	12 Mbps
18	18	18	18	18	18	18 Mbps
24	24	24	24	24	24	24 Mbps
36	36	36	36	36	36	36 Mbps
48	48	48	48	48	48	48 Mbps
54	54	54	54	54	54	54 Mbps

Data Rate IP Configuration Test

Table 6-81. Data Rate IP Configuration Test

#	Description	Test Steps	Expected Results	Actual Results
	Initialization.	1. Use the test setup shown in Figure 6-6. WRM with Vector Signal Analyzer Test Setup. 2. Execute IP initialization procedure in Section 6.3.1.2.	N/A	N/A
1.	Set WRM *rate* to *3*.	1. Use the API Tester to set the WRM configuration with a rate of 3. 2. Use Ethereal to verify the WCO rate field.	API Tester sends WCO with rate field (Word 1, Bits 28-31) set to 0001.	(W1) DD 14 11 41 1101 1101 0001 0100 0001 0001 0100 0001
	Verify the WRM rate configuration.	3. Use the API Tester to get the WRM configuration. 4. Use Ethereal to verify WCO rate field.	WRM sends WCO with rate field (Word 1, Bits 28-31) set to 0001.	(W1) DD 14 11 41
		5. Use the API Tester to verify the WRM configuration.	API Tester displays 3 Mbps.	Data rate = 3
	Verify WRM operation.	6. Use the API Tester to continuously broadcast packets w/o PBP control. 7. Use VSA to verify WRM is transmitting at the 3 Mbps data rate.	VSA shows WRM is transmitting at 3 Mbps.	VSA shows 3 Mbps
		8. Use API Tester to stop packet broadcast.	N/A	N/A
	Verify all remaining 10 MHz data rates.	9. Repeat steps 1-8 for all data rates listed in Table 6-82.	WCOs contain rate values in accordance with Table 6-82. API Tester displays WRM response showing selected data rate. VSA verifies data rate is correct.	Record results in Table 6-82.
2.	Switch to 20 MHz channel.	1. Use API Tester to send command set the WRM configuration to channel 52. 2. Use the API Tester to get the WRM configuration.	API Tester displays channel 52.	052 (5260 MHz) – 802.11a
	Verify all 20 MHz data rates.	3. Repeat Test Case # 1, steps 1-8 for all data rates listed in Table 6-83.	WCOs contain rate values in accordance with Table 6-83. API Tester displays WRM response showing selected data rate. VSA verifies data rate is correct.	Record results in Table 6-83.

Table 6-82. 10 MHz Channel Data Rate IP Configuration Test Results

Data Rate	Expected Results				Actual Results			
	WCO rate field		API Tester	VSA	WCO rate field		API Tester	VSA
	Set	Get			Set	Get		
4.5	0010	0010	4.5	4.5	0010	0010	4.5	4.5 Mbps
6	0011	0011	6	6	0011	0011	6	6 Mbps
9	0100	0100	9	9	0100	0100	9	9 Mbps
12	0101	0101	12	12	0101	0101	12	12 Mbps
18	0110	0110	18	18	0110	0110	18	18 Mbps
24	0111	0111	24	24	0111	0111	24	24 Mbps
27	1000	1000	27	27	1000	1000	27	27 Mbps

Table 6-83. 20 MHz Channel Data Rate IP Configuration Test Results

Data Rate	Expected Results				Actual Results			
	WCO rate field		API Tester	VSA	WCO rate field		API Tester	VSA
	Set	Get			Set	Get		
6	0001	0001	6	6	0001	0001	6	6 Mbps
9	0010	0010	9	9	0010	0010	9	9 Mbps
12	0011	0011	12	12	0011	0011	12	12 Mbps
18	0100	0100	18	18	0100	0100	18	18 Mbps
24	0101	0101	24	24	0101	0101	24	24 Mbps
36	0110	0110	36	36	0110	0110	36	36 Mbps
48	0111	0111	48	48	0111	0111	48	48 Mbps
54	1000	1000	54	54	1000	1000	54	54 Mbps

Data Rate IP Packet-by-Packet Test

Table 6-84. Data Rate IP Packet-by-Packet Test

#	Description	Test Steps	Expected Results	Actual Results
	Initialization.	1. Use the test setup shown in Figure 6-6. WRM with Vector Signal Analyzer Test Setup. 2. Execute IP initialization procedure in Section 6.3.1.2.	N/A	N/A
1.	Set WRM *rate to 3* using PBP control.	1. Use the API Tester to set the WRM configuration with a *rate* of *3* and transmit one packet with PBP control. 2. Use Ethereal to verify the WTXO rate field.	API Tester sends WTXO with Data Rate field (Word 1, Bits 28-31) set to 0001.	(W1) D9 10 11 41 1101 1001 0001 0000 0001 0001 0100 0001
	Verify WRM configuration.	3. Use the API Tester to get the WRM configuration.	API Tester displays data rate of 3 Mbps.	3 Mbps
	Verify WRM data rate.	4. Use the API Tester to continuously broadcast packets. 5. Use VSA to verify WRM is transmitting at 3 Mbps.	VSA shows WRM is transmitting at 3 Mbps.	3 Mbps
		6. Use the API Tester to stop packet broadcast.	N/A	N/A
	Verify remaining 10 MHz rates.	7. Repeat steps 1-6 for all data rates listed in Table 6-85.	WTXO rate field values are in accordance with Table 6-85. VSA verifies WRM is transmitting at correct rate.	Record results in Table 6-85.
2.	Switch to 20 MHz channel.	1. Use API Tester to set the WRM configuration to channel 52. 2. Use the API Tester to get the WRM configuration and verify the response.	API Tester displays channel 52.	052 (5260 MHz) – 802.11a
	Verify all 20 MHz data rates.	3. Repeat Test Case # 1, steps 1-6 for all data rates listed in Table 6-86.	WTXO rate field values are in accordance with Table 6-86. VSA verifies WRM is transmitting at correct rate.	Record results in Table 6-86.

Table 6-85. 10MHz Channel Data Rate IP Packet-by-Packet Test Results

Data Rate	Expected Results			Actual Results		
	WTXO rate field	API Tester	VSA	WTXO rate field	API Tester	VSA
4.5	0010	4.5	4.5	0010	4.5	4.5 Mbps
6	0011	6	6	0011	6	6 Mbps
9	0100	9	9	0100	9	9 Mbps
12	0101	12	12	0101	12	12 Mbps
18	0110	18	18	0110	18	18 Mbps
24	0111	24	24	0111	24	24 Mbps
27	1000	27	27	1000	27	27 Mbps

Table 6-86. 20MHz Channel Data Rate IP Packet-by-Packet Test Results

Data Rate	Expected Results			Actual Results		
	WTXO rate field	API Tester	VSA	WTXO rate field	API Tester	VSA
6	0001	6	6	0001	6	6 Mbps
9	0010	9	9	0010	9	9 Mbps
12	0011	12	12	0011	12	12 Mbps
18	0100	18	18	0100	18	18 Mbps
24	0101	24	24	0101	24	24 Mbps
36	0110	36	36	0110	36	36 Mbps
48	0111	48	48	0111	48	48 Mbps
54	1000	54	54	1000	54	54 Mbps

6.3.3.9 RTS Threshold

Verify the WRM supports setting the RTS threshold. The valid range of values is 256 to 2346 bytes. For these tests, the step attenuators are setup to provide a 10dB difference between the two WRM transmit power levels. This allows the test operator to identify the origin of packet transmissions captured by the Vector Signal Analyzer.

Test Cases:

1. No RTS on Service Channel when RTS Threshold is set higher than MAC packet length.
2. RTS/CTS performed on Service Channel when RTS Threshold is set lower than MAC packet length.
3. No RTS on Control Channel.

RTS Threshold Telnet Test

Table 6-87. RTS Threshold Telnet Test

#	Description	Test Steps	Expected Results	Actual Results
	Initialization	1. Use test setup shown in Figure 6-9. WRMs with Step Attenuators and Vector Signal Analyzer Test Setup. 2. Execute the Telnet initialization procedure in Section 6.2.3.1 on both HD/WRM setups. 3. Adjust step attenuator connected to WRM-1antenna to 20 dB. 4. Adjust step attenuator connected to WRM-2 antenna to 30 dB.	N/A	N/A
1.	Verify WRM does not perform RTS/CTS on Service Channel when MAC packet size is less than RTS threshold.	1. Use the HD-1 API Tester to send the *set fastchannel 172* Telnet command.	HD-1 API Tester displays response: *Radio Frequency: 5860 MHz (IEEE 172).*	Radio Frequency: 5860 (IEEE 172)
		2. Use the HD-2 API Tester to send the *set fastchannel 172* Telnet command.	HD-2 API Tester displays response: *Radio Frequency: 5860 MHz (IEEE 172).*	Radio Frequency 5860 (IEEE 172)
		3. Use the HD-1 API Tester to send the *get rtsthreshold* Telnet command.	HD-1 API Tester displays response: *RTS Threshold: 2346*	RTS/CTS Threshold: 2346
		4. Use the HD-2 API Tester to get the MAC address of WRM-2.	HD-2 API Tester displays the MAC address of WRM-2.	F2:AB:B9:06:F8:BC

#	Description	Test Steps	Expected Results	Actual Results
		5. Use the HD-1 API Tester to transmit a single 1400 byte data packet w/o PBP control to WRM-2 MAC address. 6. Use the VSA to display the data packet transmission.	VSA displays WRM-1 data packet transmitted at 0dBm, followed by short WRM-2 ACK transmitted at –10dBm.	Data packet transmitted at +2 dBm. ACK transmitted at –10 dBm.
2.	Verify WRM performs RTS/CTS on Service Channel when MAC packet size exceeds RTS threshold.	1. Use the HD-1 API Tester to send the *set fastchannel 172* Telnet command.	HD-1 API Tester displays response: *Radio Frequency: 5860 MHz (IEEE 172).*	Radio Frequency: 5860 MHz (IEEE 172)
		2. Use the HD-2 API Tester to send the *set fastchannel 172* Telnet command.	HD-2 API Tester displays response: *Radio Frequency: 5860 MHz (IEEE 172).*	Radio Frequency: 5860 MHz (IEEE 172)
		3. Use the HD-1API Tester to send the *set rtsthreshold 1000* Telnet command.	HD-1 API Tester displays response: *RTS Threshold: 1000*	RTS/CTS Threshold: 1000
		4. Use the HD-1 API Tester to transmit a single 1400 byte data packet w/o PBP control to WRM-2 MAC address. 5. Use the VSA to display the data packet transmission.	VSA displays short WRM-1 RTS transmitted at 0 dBm, followed by short WRM-2 CTS transmitted at –10 dBm, followed WRM-1 data packet transmitted at 0dBm, followed by short WRM-2 ACK transmitted at –10dBm.	RTS transmitted at +2 dBm. CTS transmitted at –10 dBm. Data transmitted at +2 dBm. ACK transmitted at –10 dBm.
3.	Verify WRM does not perform RTS/CTS on Control Channel even though MAC packet size exceeds RTS threshold.	1. Use the HD-1 API Tester to send the *set fastchannel 178* Telnet command.	HD-1 API Tester displays response: *Radio Frequency: 5890 MHz (IEEE 178).*	Radio Frequency: 5890 (IEEE178)
		2. Use the HD-2 API Tester to send the *set fastchannel 178* Telnet command.	HD-2 API Tester displays response: *Radio Frequency: 5890 MHz (IEEE 178).*	Radio Frequency: 5890 (IEEE 178)
		3. Use the HD-1API Tester to send the *set rtsthreshold 1000* Telnet command.	HD-1 API Tester displays response: *RTS Threshold: 1000*	RTS/CTS Threshold: 1000
		4. Use the HD-1 API Tester to transmit a single 1400 byte data packet w/o PBP control to WRM-2 MAC address. 5. Use the VSA to display the data packet transmission.	VSA displays WRM-1 data packet transmitted at 0dBm, followed by short WRM-2 ACK transmitted at –10dBm.	Data transmitted at +2 dBm. ACK transmitted at –10 dBm.

RTS Threshold IP Configuration Test

Table 6-88. RTS Threshold IP Configuration Test

#	Description	Test Steps	Expected Results	Actual Results
	Initialization	1. Use test setup shown in Figure 6-9. WRMs with Step Attenuators and Vector Signal Analyzer Test Setup. 2. Execute the IP initialization procedure in Section 6.3.1.2 on both HD/WRM setups. 3. Adjust step attenuator connected to WRM-1antenna to 20 dBm. 4. Adjust step attenuator connected to WRM-2 antenna to 30 dBm.	N/A	N/A
1.	Verify WRM does not perform RTS/CTS on Service Channel when MAC packet size is less than RTS threshold.	1. Use the HD-1 API Tester to set the WRM channel to 172.	HD-1 API Tester displays Channel 172.	172 (5860 MHz) – WAVE
		2. Use the HD-2 API Tester to set the WRM channel to 172.	HD-2 API Tester displays Channel 172.	172 (5860 MHz) – WAVE
		3. Use the HD-1 API Tester to get the WRM configuration and verify the *RTS Threshold*	API Tester displays RTS Threshold of 2346 bytes.	RTS Threshold 1000
		4. Use the HD-2 API Tester to get the MAC address of WRM-2.	HD-2 API Tester displays the MAC address of WRM-2.	46:87:1A:9C:FB:29
		5. Use the HD-1 API Tester to transmit a single 1400 byte data packet w/o PBP control to WRM-2 MAC address. 6. Use the VSA to display the data packet transmission.	VSA displays WRM-1 data packet transmitted at 0dBm, followed by short WRM-2 ACK transmitted at –10dBm.	Data transmitted at +2 dBm. ACK transmitted at –10 dBm.
2.	Verify WRM performs RTS/CTS on Service Channel when MAC packet size exceeds RTS threshold.	1. Use the HD-1 API Tester to set the WRM channel to 172.	HD-1 API Tester displays Channel 172.	172 (5860 MHz) – WAVE
		2. Use the HD-2 API Tester to set the WRM channel to 172.	HD-2 API Tester displays Channel 172.	172 (5860 MHz) – WAVE
		3. Use HD-1 API Tester to set the RTS Threshold to 1000 bytes. 4. Use Ethereal to verify the WCO RTS Threshold field.	API Tester sends WCO with RTS Threshold field (Word 2, bits 16-31) set to 1000 (x03E8).	(W2) 09 2A **03 E8**

#	Description	Test Steps	Expected Results	Actual Results
		5. Use the HD-1 API Tester to transmit a single 1400 byte data packet w/o PBP control to WRM-2 MAC address. 6. Use the VSA to display the data packet transmission.	VSA displays short WRM-1 RTS transmitted at 0 dBm, followed by short WRM-2 CTS transmitted at –10 dBm, followed WRM-1 data packet transmitted at 0dBm, followed by short WRM-2 ACK transmitted at –10dBm.	RTS at +2 dBm, CTS at –10 dBm, Data at +2 dBm, ACK at –10 dBm.
3.	Verify WRM does not perform RTS/CTS on Control Channel even though MAC packet size exceeds RTS threshold.	1. Use the HD-1 API Tester to set the WRM channel to 178.	HD-1 API Tester displays Channel 178.	178 (5890 MHz) – WAVE
		2. Use the HD-2 API Tester to set the WRM channel to 178.	HD-2 API Tester displays Channel 178.	Channel = 178
		3. Use HD-1 API Tester to set the RTS Threshold to 1000 bytes. 4. Use Ethereal to verify the WCO RTS Threshold field.	API Tester sends WCO with RTS Threshold field (Word 2, bits 16-31) set to 1000 (x03E8).	(W2) 09 2A **03 E8**
		5. Use the HD-1 API Tester to transmit a single 1400 byte data packet w/o PBP control to WRM-2 MAC address. 6. Use the VSA to display the data packet transmission.	VSA displays WRM-1 data packet transmitted at 0dBm, followed by short WRM-2 ACK transmitted at –10dBm.	Data at +2 dBm, ACK at –10 dBm.

Table 6-89. RTS Threshold IP Packet-by-Packet Test

#	Description	Test Steps	Expected Results	Actual Results
	Initialization	1. Use test setup shown in Figure 6-9. WRMs with Step Attenuators and Vector Signal Analyzer Test Setup. 2. Execute the IP initialization procedure in Section 6.3.1.2 on both HD/WRM setups. 3. Adjust step attenuator connected to WRM-1antenna to 20 dBm. 4. Adjust step attenuator connected to WRM-2 antenna to 30 dBm.	N/A	N/A
1.	Verify WRM does not perform RTS/CTS on Service Channel when MAC packet size is less than RTS threshold.	1. Use the HD-2 API Tester to get the MAC address of WRM-2.	HD-2 API Tester displays the MAC address of WRM-2.	B2:E7:74:5E:40:32
		2. Use HD-2 API Tester to change channel to 172.	N/A	N/A
		3. Use the HD-1 API Tester to transmit a single 1400 byte data packet with RTS Threshold set to 1500, on channel 172, with PBP control to WRM-2 MAC address. 4. Use Ethereal to verify the WTXO RTS Threshold field.	API Tester sends WTXO with RTS Threshold field (Word 2, bits 16-31) set to 1500 (x05DC).	(W2) 09 2A 05 DC
		5. Use the VSA to display the data packet transmission.	VSA displays WRM-1 data packet transmitted at 0dBm, followed by short WRM-2 ACK transmitted at –10dBm.	Data at +2 dBm, ACK at –10 dBm
		6. Use the API Tester to stop packet transmission.	N/A	N/A
2.	Verify WRM performs on Service Channel RTS/CTS when MAC packet size exceeds RTS threshold.	1. Use the HD-1 API Tester to transmit a single 1400 byte data packet with RTS Threshold set to 1000, on channel 172, with PBP control to WRM-2 MAC address. 2. Use Ethereal to verify the WTXO RTS Threshold field.	API Tester sends WTXO with RTS Threshold field (Word 2, bits 16-31) set to 1000 (x03E8).	(W2) 09 2A 03 E8

#	Description	Test Steps	Expected Results	Actual Results
		3. Use the VSA to display the data packet transmission.	VSA displays short WRM-1 RTS transmitted at 0 dBm, followed by short WRM-2 CTS transmitted at –10 dBm, followed WRM-1 data packet transmitted at 0dBm, followed by short WRM-2 ACK transmitted at –10dBm.	RTS at +2 dBm. CTS at –10 dBm, Data at +2 dBm, ACK at –10 dBm
		4. Use the API Tester to stop packet transmission.	N/A	N/A
3.	Verify WRM does not perform RTS/CTS on Control Channel even though MAC packet size exceeds RTS threshold.	1. Use the HD-2 API Tester to get the MAC address of WRM-2.	HD-2 API Tester displays the MAC address of WRM-2.	16:2C:C8:DF:50:66
		2. Use the API Tester to transmit a single 1400 byte data packet with RTS Threshold set to 1000, on channel 178, with PBP control to WRM-2 MAC address. 3. Use Ethereal to verify the WTXO RTS Threshold field.	API Tester sends WTXO with RTS Threshold field (Word 2, bits 16-31) set to 1000 (x03E8).	(W2) 09 2A 03 E8
		4. Use the VSA to display the data packet transmission.	VSA displays WRM-1 data packet transmitted at 0dBm, followed by short WRM-2 ACK transmitted at –10dBm.	Data at +2 dBm, ACK at –10 dBm.
		5. Use the API Tester to stop packet transmission	N/A	N/A

6.3.4 Status Reporting

6.3.4.1 Configuration Parameters

Verify the WRM reports the configuration parameters. See Section 6.3.1.1 for a verification of the Telnet *get config* command. The IP Configuration tests throughout this test plan verify the WRM Configuration information obtained with the IP interface.

6.3.4.2 Hardware Version

Verify the WRM reports the hardware version. This command is only available through the Telnet interface.

Table 6-90. Hardware Version Telnet Test

#	Description	Test Steps	Expected Results	Actual Results
	Initialize.	1. Use the test setup shown in Figure 6-1. Single WRM Test Setup. 2. Execute Telnet initialization procedure in Section 6.2.3.1.	N/A	N/A
1.	Verify the WRM response to the *get hardware* command.	1. Use the API Tester to send the *get hardware* Telnet command and verify the WRM response.	API Tester displays response: [See Note below table]	revisions: mac 5.8 phy 4.4 analog 3.6 PCI Vendor ID: 0x168c, Device ID: 0x13 Sub Vendor ID: 0x168c, Sub Device ID: 0x13

Note: WRM response is of the following format:

revisions: mac 5.7 phy 4.2 analog 3.6

PCI Vendor ID: 0x168c, Device ID: 0x13

Sub Vendor ID: 0x168c, Sub Device ID: 0x13

6.3.4.3 RSSI

Verify the WRM reports the RSSI in dBm. The RSSI is available through the Telnet and IP Packet-by-Packet interfaces.

RSSI Telnet Test

Table 6-91. RSSI Telnet Test

#	Description	Test Steps	Expected Results	Actual Results
	Initialize.	1. Use the test setup shown in Figure 6-7. WRMs with Cable Connection. 2. Execute Telnet initialization procedure in Section 6.2.3.1 on both HD/WRM setups.	N/A	N/A
1.	Set the antenna configuration to 1.	1. Use the HD-1 and HD-2 API Testers to send the *set antenna 1* command and verify the response.	API Testers display response *Antenna: 1*.	Antenna: 1
	Verify the WRM-1 response to the *get rssi* command.	2. Adjust the WRM-2 output power and the attenuators so the input level at the WRM-1 SMA connector will be ~ –30 dBm when WRM-2 is transmitting. 3. Use the HD-2 API Tester to continuously broadcast packets with PBP control. 4. Use the HD-1 API Tester to send the *get rssi* Telnet command and verify the WRM response. 5. Use the HD-2 API Tester to stop the packet broadcast.	API Tester displays response: *rssi: -30* (+/- 1 dB)	RSSI = -30 dBm
	Verify the WRM-1 response over range of RSSI levels.	6. Repeat steps 2-5 varying the input level at the WRM-1 SMA connector from –40 to –90 dBm in 10 dB steps.	API Tester displays response: *rssi: xxx* (+/- 1 dB), where xxx is the input level.	Record the results in Table 6-92

Table 6-92. RSSI Telnet Test Results

WRM-1 SMA Input Level	HD-1 *get rssi*	
	Expected Results	Actual Results
-40	-40	-41 dBm
-50	-50	-50 dBm
-60	-60	-61 dBm
-70	-70	-70 dBm
-80	-80	-80 dBm
-90	-90	-91 dBm

RSSI IP Packet-by-Packet Test

Table 6-93. RSSI IP Packet-by-Packet Test

#	Description	Test Steps	Expected Results	Actual Results
	Initialize.	1. Use the test setup shown in Figure 6-7. WRMs with Cable Connection. 2. Execute IP initialization procedure in Section 6.3.1.2 on both HD/WRM setups.	N/A	N/A
1.	Set antenna configuration.	1. Use the HD-1 and HD-2 API Testers to set the antenna configuration to 1. 2. Use the HD-1 and HD-2 API Testers to get the WRM configuration.	API Testers display antenna configuration as 1.	Antenna = 1
	Verify the WRM-1 provides the RSSI to HD-1.	3. Adjust the WRM-2 output power and the attenuators so the input level at the WRM-1 SMA connector will be ~ –30 dBm when WRM-2 is transmitting. 4. Use the HD-2 API Tester to broadcast one packet with PBP control. 5. Use the HD-1 Ethereal to verify the WRXO RSSI field.	WRM send WRXO with the RSSI field (Word 1, bits 16-31) to –30 (0xFFE2) +/- 1 dB	(W1) DA 24 **FF E2**
		6. Use the API Tester to verify the RSSI.	API Tester displays RSSI of –30 (+/- 1 dB)	-30 dBm
	Verify the WRM-1 response over range of RSSI levels.	7. Repeat steps 3-6 varying the WRM-1 input level from –40 to –90 dBm in 10 dB steps.	WRM sends WRXO with the RSSI field (Word 1, bits 16-31) to the input level (+/- 1 dB)	Record results in Table 6-94.

Table 6-94. RSSI IP Packet-by-Packet Tests and Results

WRM-1 SMA Input Level	Expected Results		Actual Results	
	WRXO RSSI field	API Tester	WRXO RSSI field	API Tester
-40	1111111111011000 (xFFD8)	-40	FF D7 (-41 dBm)	-41 dBm
-50	1111111111001101 (xFFCE)	-50	FF CF (-49 dBm)	-49 dBm
-60	1111111111000100 (xFFC4)	-60	FF C2 (-62 dBm)	-62 dBm
-70	1111111110111010 (xFFBA)	-70	FF BB (-69 dBm)	-69 dBm
-80	1111111110110000 (xFFB0)	-80	FF B1 (-79 dBm)	-79 dBm
-90	1111111110100110 (xFFA6)	-90	FF A7 (-89 dBm)	-89 dBm

6.3.4.4 Software Version

Verify the WRM reports the software version. This command is only available through the Telnet interface.

Table 6-95. Software Version Telnet Test

#	Description	Test Steps	Expected Results	Actual Results
	Initialize.	1. Use the test setup shown in Figure 6-1. Single WRM Test Setup. 2. Execute Telnet initialization procedure in Section 6.2.3.1.	N/A	N/A
1.	Verify the WRM response to the *version* command.	1. Use the API Tester to send the *version* Telnet command and verify the WRM response.	API Tester displays response: *AP software: 3.1.0.358* *WRM software: x.x* *mmm dd yyy, hh:mm:ss*	AP software: 3.1.0.358 WRM software: 1.9 Jul 16 2004, 11:28:11

6.4 WRM Functional Specification Tests

This section specifies tests to verify requirements in the WRM Functional Specification that were not verified during the WRM Interface Specification Tests.

6.4.1 Power-Up Initialization

Upon power-up, verify the WRM initializes to the last saved configuration. The WRM saves its configuration whenever it is commanded to WAVEdefault parameters (through either a Telnet command or IP command) or upon a Telnet command changing a parameter value.

Table 6-96. Power-Up Initialization Test

#	Description	Test Steps	Expected Results	Actual Results
	Initialize.	1. Use the test setup shown in Figure 6-1. Single WRM Test Setup. 2. Execute Telnet initialization procedure in Section 6.2.3.1.	N/A	N/A
1.	Verify power up initialization to WAVE default parameters.	1. Cycle power on the WRM. 2. Use the API Tester to send the *get config* Telnet command.	API Tester displays configuration data including default parameter values listed in Table 6-3.	Configuration data matches default values listed in the table.
	Modify the configuration using Telnet commands.	3. Use API Tester to send the following commands and display WRM response: • *set unitmode RSU* • *set servicemode private* • *set antenna 1* • *set antenna1comp 2* • *set antenna2comp –4* • *set fastchannel 52* • *set bandwidth 10* • *set rate 12* • *set fragmentthreshold 300* • *set rtsthreshold 400* • *set power 10*	API Tester displays WRM responses echoing new settings.	API Tester echoes Telnet command settings.
	Verify power up initialization to modified parameters.	4. Cycle power on the WRM. 5. Use the API Tester to send the *get config* Telnet command.	API Tester displays WRM responses echoing step 3 settings.	API Tester reports all parameter values matching the values set in step 3.
	Set WRM to default parameters using a Telnet command.	6. Use the API Tester to send the *set WAVEdefault* command and verify response.	API Tester displays response: *WAVEdefault*. WRM reboots.	WRM rebooted
	Verify power up to default parameters	7. Cycle power on the WRM. 8. Use the API Tester to send the *get config* Telnet command.	API Tester displays configuration data including default parameter values listed in Table 6-3.	Configuration data matches default values listed in the table.
	Modify the configuration using IP config commands.	9. Send the same set of commands as in step 3.	See step 3.	API Tester displays IP configuration parameter settings.
	Set WRM to default parameters using an IP Config command.	10. Use the API Tester to send an IP default configuration request.	N/A	N/A

#	Description	Test Steps	Expected Results	Actual Results
	Verify power up initialization to default parameters.	11. Use the API to get the WRM configuration using an IP command.	API Tester displays WRM configuration showing default parameter values listed in Table 6-3.	Configuration data matches default values listed in the table.

6.4.2 MAC Address

Verify when the WRM is operating in RSU mode, it uses the stored MAC address. Verify when the WRM is operating in OBU mode, it generates a random MAC address when it powers up. The MAC address may only be obtained through the IP Configuration interface.

Table 6-97. MAC Address Test

#	Description	Test Steps	Expected Results	Actual Results
	Initialization.	1. Use the test setup shown in Figure 6-1. Single WRM Test Setup. 2. Execute IP initialization procedure in Section 0.	N/A	N/A
1.	Get MAC address (WRM is in OBU mode).	1. Use the API Tester to get the WRM configuration. 2. Use Ethereal to verify the WCO MAC address.	WRM sends WCO with MAC address (Word 4, bits 00-31, and Word 5, bits 00-15)	(W4) DA 21 3F CF (W5) 9D 5D 00 00
		3. Use the API Tester to verify the WRM configuration.	API Tester displays MAC address equivalent to WCO contents.	API Tester displays MAC Address: DA:21:3F:CF:9D:5D
	Verify WRM generates new address on subsequent power up.	4. Cycle power on the WRM. 5. Use the API Tester to get the WRM configuration and display the MAC address.	API Tester displays a different MAC address than in step 3.	API Tester displays MAC Address: B2:1B:26:90:6C:5A
2.	Configure WRM to RSU mode, cycle power, and get MAC address.	1. Use the API Tester to send the *set unitmode RSU* Telnet command. 2. Cycle power on the WRM. 3. Use the API Tester to get the WRM configuration. 4. Use Ethereal to verify the WCO MAC address.	WRM sends WCO with MAC address (Word 4, bits 00-31, and Word 5, bits 00-15)	(W4) 00 03 7F BF (W5) 0D F4 00 00
		5. Use the API Tester to verify the WRM configuration.	API Tester displays MAC address equivalent to WCO contents.	API Tester displays MAC Address: 00:03:7F:BF:0D:F4

#	Description	Test Steps	Expected Results	Actual Results
	Verify WRM uses same MAC address on subsequent power up.	6. Cycle power on the WRM. 7. Use the API Tester to get the WRM configuration and display the MAC address.	API Tester displays the same MAC address as in step 5.	API Tester displays MAC Address: 00:03:7F:BF:0D:F4

6.4.3 802.11 Management Frames

Verify the WRM does not transmit any IEEE 802.11 [3] management frames. Upon receiving a management frame, verify the WRM acknowledges the frame but does not take action based on its contents.

Table 6-98. 802.11 Management Frames Test

#	Description	Test Steps	Expected Results	Actual Results
	Initialization.	1. Use the test setup shown in Figure 6-3. WRM with Spectrum Analyzer Test Setup. 2. Execute IP initialization procedure in Section 0.	N/A	N/A
1.	Verify WRM does not transmit any IEEE 802.11 management frames.	1. Use spectrum analyzer to verify WRM is not transmitting.	Spectrum analyzer displays flat line, indicating no data is being transmitted.	Spectrum analyzer does not indicate any data transmissions.
		2. Use the API Tester to continuously broadcast packets. 3. Use the spectrum analyzer to verify the WRM transmissions.	Spectrum analyzer displays wave patterns indicating data is being transmitted.	Spectrum analyzer displays patterns indicating data is being transmitted.
		4. Use the API Tester to stop packet broadcast. 5. Use the spectrum analyzer to verify the WRM is not transmitting.	Spectrum analyzer displays flat line, indicating no data is being transmitted.	Spectrum analyzer does not indicate any data transmissions.

6.4.4 802.11 DATA Frames

Verify the WRM constructs MAC frames in accordance with IEEE 802.11. The MAC frames contains address fields which must be set as follows:

1. Basic Service Set Identification (BSSID) – this field shall be set to all 0s.

2. Source Address – this field shall be set to the WRM MAC address.
3. Destination Address – Broadcast MAC address or destination address provided by HD.

The WRM shall always set the Power Management, More Data, and Wired Equivalent Privacy (WEP) fields to 0. For data frames, verify the subtype is set to data.

Table 6-99. Data Tx/Rx Test

#	Description	Test Steps	Expected Results	Actual Results
	Initialization.	1. Use the test setup shown in Figure 6-8. Dual WRMs. 2. Execute IP initialization procedure in Section 0 on both HD/WRM setups.	N/A	N/A
1.	Get HD-2 MAC address.	1. Use the HD-2 API Tester to get the local MAC address.	API Tester displays local MAC address.	HD-2 MAC Address: BE:C3:65:83:10:A5
	Transmit and receive data frames.	2. Use the HD-2 API Tester to transmit one packet with PBP control with a broadcast destination address. 3. Use the HD-1 Ethereal to verify the WRXO MAC Header field.	WRM sends WRXO with MAC Header field (see 802.11, Chapter for format). Verify BSSID is all 0s, Source Address is the HD-2 MAC address, Destination Address is the Broadcast MAC address. Verify the Power Management, More Data, and WEP fields are 0. Verify the subtype is data (0000)	BSSID: 00 00 00 00 00 00 Source Address: BE:C3:65:83:10:A5 Destination Address: FF FF FF FF FF FF Power Mgmt = 0 More Data = 0 WEP = 0 Subtype = 0000
		4. Use the HD-2 API Tester to transmit one packet with PBP control with a unicast destination address. 5. Use the HD-1 Ethereal to verify the WRXO MAC Header field.	WRM sends WRXO with MAC Header field values the same as in step 3 except the Destination Address is the specified unicast address.	Destination Address: 5A:39:8D:31:EA:18

6.4.5 WRM Reconfiguration Time

Verify the WRM reconfigures to new settings, other than wireless mode changes, within 5 ms.

Table 6-100. WRM Reconfiguration Time Test

#	Description	Test Steps	Expected Results	Actual Results
	Initialization.	1. Use the test setup shown in Figure 6-6. WRM with Vector Signal Analyzer Test Setup. 2. Execute IP initialization procedure in Section 6.3.1.2 on both HD/WRM setups.	N/A	N/A
1.	Set up WRM configurations and VSA, and start recording data transmissions on the VSA.	1. Use API Tester to configure WRM Configuration #1 to channel 174, 6Mbps data rate, 20dBm Tx power, and to transmit 1000 byte data packets 5 times every 10ms. 2. Use API Tester to configure WRM Configuration #2 to channel 175, 12Mbps data rate, 10dBm Tx power, and to transmit 1000 byte data packets 10 times every 10ms. 3. Use API Tester to configure WRM Configuration #3 to channel 176, 6Mbps data rate, 20dBm Tx power, and to transmit 1000 byte data packets 5 times every 10ms. 4. Setup the VSA to display at least 30ms of time domain information, including WRM channel, Tx power, and data rate. Use the API Tester to broadcast continuously by repeatedly cycling through the above WRM configurations. .	VSA displays data packet transmissions.	VSA displays packet transmissions.

#	Description	Test Steps	Expected Results	Actual Results
	Verify the WRM reconfigures within 5ms.	5. Watch on the VSA for indication that the WRM has changed channel, Tx power, and data rate, switching from WRM configuration #1 to WRM configuration #2. 6. Pause the real-time display on the VSA to make a time measurement. 7. Use the VSA to measure the time between the stop and restart of data as recorded on the VSA.	The VSA indicates that the time between stop and restart of data is 5ms or less.	2.8ms reconfiguration time measured for transition from configuration 1-> configuration 2. 3.3ms reconfiguration time measured for transition from configuration 2 -> configuration 3. 3.2ms reconfiguration time measured for transition from configuration 3 -> configuration 1.
	Verify new WRM configuration.	8. Use the VSA to measure the channel value at the time data stopped and at the time data restarted.	Within this 5ms time period the VSA displays a change in channel from 174 to 175.	Frequency changed from 5870 MHz (IEEE 174) to 5875 MHz (IEEE 175) in 2.8ms.
		9. Use the VSA to measure the Tx power level at the time data stopped and at the time data restarted.	Within this 5ms time period the VSA displays a change in Tx power from 20dBm to 10dBm.	Tx power changed from 20dBm to 10dBm in 2.8ms.
		10. Use the VSA to measure the data rate at the time data stopped and at the time data restarted.	Within this 5ms time period the VSA displays a change in data rate from 6Mbps to 12Mbps. *Note: this test result will depend on the ability of the VSA to demodulate the first packet following the channel, power, and data rate change.*	Data rate changed from 6Mbps to 12Mbps in 2.8ms.

6.5 WRM Network Tests

6.5.1 Single Transmitter with Multiple Receivers

6.5.1.1 Broadcast Addressing

Single-Channel Operation Test

This test verifies single-channel operation with broadcast messages.

- Four WRMs operating on the same channel:
  - One WRM broadcasting 50 byte data bursts every 100ms.
  - Three WRMs set up to receive.
- Test operator verifies data is received at all three receiving stations.

Table 6-101. Broadcast Addressing Single Channel Operation Test

#	Description	Test Steps	Expected Results	Actual Results
	Initialization.	1. Configure four test setups, each one configured as shown in Figure 6-1. Single WRM Test Setup. 2. Execute IP initialization procedure in Section 6.2.3.2 on all HD/WRM setups.	N/A	N/A
1.	Verify WRMs receive the data	1. Use HD-1 API Tester to repeatedly broadcast a 50-byte data packet every 100 ms w/o PBP control. 2. Use the HD-2, HD-3, and HD-4 API Testers to verify data is being received at each WRM.	API Testers for HD-2, HD-3, and HD-4 display received data packet information.	HD-2, 3, & 4 report data packets received.
		3. Allow packet broadcasting to continue for 60 seconds. 4. Use HD-1 API Tester to stop packet broadcast.	API Testers for HD-2, HD-3, and HD-4 stop displaying received data packet information, and indicate receipt of ~600 packets (or 10 packets times the # of seconds the test ran).	HD-1 transmitted 603 packets. HD-2 received 603 packets. HD-3 received 603 packets. HD-4 received 603 packets.

Multi-Channel Operation Test

This test verifies multi-channel operation and transmitter channel switching with broadcast messages.

- One station broadcasting data bursts and changing to one of three channels every 5 seconds.
- Three stations set up to receive on three unique channels.
- Test operator verifies data is received on each receiving station only on the corresponding channel.

Table 6-102. Broadcast Addressing Multi-Channel Operation Test

#	Description	Test Steps	Expected Results	Actual Results
	Initialization.	1. Configure four test setups, each one configured as shown in Figure 6-1. Single WRM Test Setup. 2. Execute IP initialization procedure in Section 6.2.3.2 on all HD/WRM setups.	N/A	N/A
1.	Tune WRMs to test channels.	1. Use HD-2 API Tester to set the WRM configuration with the channel of 172. 2. Use HD-3 API Tester to set the WRM configuration with the channel of 176. 3. Use HD-4 API Tester to set the WRM configuration with the channel of 181. 4. Use the API Testers to confirm the WRM configurations.	Each API Tester confirms the corresponding WRM is set to the correct channel.	HD-2 channel = 172. HD-3 channel = 176. HD-4 channel = 181.
	Set up PBP configurations.	5. Use HD-1 API Tester to create three PBP configurations: • One configuration to broadcast a unique 50-byte data packet on channel 172, • A second configuration to broadcast a unique 50-byte data packet on channel 176, • A third configuration to broadcast a unique 50-byte data packet on channel 181.	N/A	N/A
	Broadcast data bursts.	6. Use HD-1 API Tester to repeatedly cycle through the three PBP configurations every 1 second.	N/A	N/A

#	Description	Test Steps	Expected Results	Actual Results
	Verify WRMs receive the data	7. Use the HD-2, HD-3, and HD-4 API Testers to verify the data received at each WRM is correct for the corresponding receive channel.	API Testers for HD-2, HD-3, and HD-4 only display received data packet information corresponding to the channel to which they are tuned.	API Testers on each HD only report receiving data packets on the channel they are tuned to.
		8. Allow PBP transmissions continue cycling for 60 seconds. 9. Use HD-1 API Tester to stop PBP Transmissions.	API Testers for HD-2, HD-3, and HD-4 stop displaying received data packet information, and indicate receipt of ~20 packets (or 1 packet for each 3 seconds the test was run).	Each HD reported receiving 20 packets.

Directed Addressing

Single-Channel Operation Test

This test verifies single-channel operation with directed (unicast) destination MAC addresses.

- One station transmitting alternate data bursts to specific MAC addresses every 5 seconds.
- Three stations with unique MAC addresses set up to receive.
- Test operator verifies appropriately addressed data is received at the receiving stations.

Table 6-103. Directed Addressing Single-Channel Operation Test

#	Description	Test Steps	Expected Results	Actual Results
	Initialization.	1. Configure four test setups, each one configured as shown in Figure 6-1. Single WRM Test Setup. 2. Execute IP initialization procedure in Section 6.2.3.2 on all HD/WRM setups.	N/A	N/A
1.	Get MAC addresses.	1. Use the HD-2, HD-3, and HD-4 API Testers to get the MAC address of each corresponding WRM.	API Testers report the corresponding MAC addresses.	HD-2 MAC Address: 9A:2B:E2:49:7E:77 HD-3 MAC Address: 4A:CD:15:E4:B9:46 HD-4 MAC Address: AA:1F:A4:17:A8:84
	Set up PBP configurations	2. Use HD-1 API Tester to create three PBP configurations: • One configuration to transmit a unique 50-byte data packet to MAC address of WRM-2, • A second configuration to transmit a unique 50-byte data packet to MAC address of WRM-3, • A third configuration to transmit a unique 50-byte data packet to MAC address of WRM-4.	N/A	N/A
	Transmit data bursts.	3. Use HD-1 API Tester to repeatedly cycle through the three PBP configurations at 100ms intervals.	N/A	N/A
	Verify WRMs receive the data	4. Use the HD-2, HD-3, and HD-4 API Testers to verify the data being received at each WRM is correct for the corresponding MAC address.	API Testers for HD-2, HD-3, and HD-4 only display received data packet information corresponding to their MAC address.	API Tester on each HD reported receiving only data specifically addressed to their respective MAC addresses.

#	Description	Test Steps	Expected Results	Actual Results
		5. Allow packet transmissions to continue for 60 seconds. 6. Use HD-1 API Tester to stop packet transmissions.	API Testers for HD-2, HD-3, and HD-4 stop displaying received data packet information, and indicate receipt of ~200 packets (or 10 packets for each 3 seconds the test was run).	HD-1 transmitted 694 packets in ~69 seconds. HD-2 received 232 packets. HD-3 received 231 packets. HD-4 received 231 packets.

Multi-Channel Operation Test

This test verifies multi-channel operation and channel switching with directed (unicast) destination MAC addresses.

- One station transmitting data bursts to specific MAC addresses on specific channels, switching channels every 5 seconds.
- Three stations with unique MAC addresses set up to receive on three unique channels.
- Test operator verifies appropriately addressed data is received on the correct channel at the receiving stations.

Table 6-104. Directed Addressing Multi-Channel Operation Test

#	Description	Test Steps	Expected Results	Actual Results
	Initialization.	1. Configure four test setups, each one configured as shown in Figure 6-1. Single WRM Test Setup. 2. Execute IP initialization procedure in Section 6.2.3.2 on all HD/WRM setups.	N/A	N/A
1.	Get MAC addresses.	1. Use the HD-2, HD-3, and HD-4 API Testers to get the MAC address of each corresponding WRM.	API Testers report the corresponding MAC addresses.	HD-2 MAC Address: 9A:2B:E2:49:7E:77 HD-3 MAC Address: 4A:CD:15:E4:B9:46 HD-4 MAC Address: AA:1F:A4:17:A8:84

#	Description	Test Steps	Expected Results	Actual Results
	Tune WRMs to test channels.	2. Use HD-2 API Tester to set the WRM configuration with the channel of 172. 3. Use HD-3 API Tester to set the WRM configuration with the channel of 176. 4. Use HD-4 API Tester to set the WRM configuration with the channel of 181. 5. Use the API Testers to confirm the WRM configurations	Each API Tester confirms the corresponding WRM is set to the correct channel.	HD-2 channel = 172. HD-3 channel = 176. HD-4 channel = 181.
	Set up PBP configurations	6. Use HD-1 API Tester to create three PBP configurations: • one configuration to transmit a unique 50-byte data packet, on channel 172, at 20dBm power level, to MAC address of WRM-2, • a second configuration to transmit a unique 50-byte data packet, on channel 176, at 15 dBm power level, to MAC address of WRM-3, • a third configuration to transmit a unique 50-byte data packet, on channel 181, at 10 dBm power level, to MAC address of WRM-4.	N/A	N/A
	Transmit data bursts.	7. Use HD-1 API Tester to repeatedly cycle through the three PBP configurations at 100ms intervals.	N/A	N/A
	Verify WRMs receive the data	8. Use the HD-2, HD-3, and HD-4 API Testers to verify the data being received at each WRM is correct for the corresponding MAC address and channel.	API Testers for HD-2, HD-3, and HD-4 only display received data packet information corresponding to their MAC address and channel.	Data received on HD-2, 3, & 4 is correct for their respective MAC addresses.

#	Description	Test Steps	Expected Results	Actual Results
		9. Allow PBP transmissions to continue for 60 seconds. 10. Use HD-1 API Tester to stop PBP transmissions.	API Testers for HD-2, HD-3, and HD-4 stop displaying received data packet information, and indicate receipt of ~200 packets (or 10 packets for each 3 seconds the test was run).	HD-1 transmitted 600 packets in 60 seconds. HD-2 received 200 packets. HD-3 received 20 packets. HD-4 received 20 packets.

6.5.2 Multiple Transmitters with Multiple Receivers Test

This test verifies channel contention situations, with multiple transmitters and receivers operating on the same channel.

- Six WRMs operating on the same channel:
  - Three WRMs using directed MAC addressing to transmit data to three different receivers.
  - Three WRMs with unique MAC addresses set up to receive.
- Test operator verifies appropriately addressed data is received at the receiving stations.

Table 6-105. Multiple Transmitters with Multiple Receivers Test

#	Description	Test Steps	Expected Results	Actual Results
	Initialization.	1. Configure six test setups, each one configured as shown in Figure 6-1. Single WRM Test Setup. 2. Execute IP initialization procedure in Section 6.2.3.2 on all HD/WRM setups.	N/A	N/A
1.	Get MAC addresses.	1. Use the HD-4, HD-5, and HD-6 API Testers to get the MAC address of each corresponding WRM.	API Testers report the corresponding MAC addresses.	HD-4 MAC Address: 9A:2B:E2:49:7E:77 HD-5 MAC Address: 4A:CD:15:E4:B9:46 HD-6 MAC Address: AA:1F:A4:17:A8:84

#	Description	Test Steps	Expected Results	Actual Results
	Set up PBP configurations	2. Use HD-1 API Tester to create one PBP configuration to transmit a unique 1000-byte data packet 40 times every 100ms on channel 178 to MAC address of WRM-4. 3. Use HD-2 API Tester to create one PBP configuration to transmit a unique 1000-byte data packet 5 times every 100ms on channel 178 to MAC address of WRM-5. 4. Use HD-3 API Tester to create one PBP configuration to transmit a unique 1000-byte data packet 5 times every 100ms on channel 178 to MAC address of WRM-6.	N/A	N/A
	Transmit data bursts.	5. Use HD-1, HD-2, and HD-3 API Testers to repeatedly transmit their PBP configurations.	N/A	N/A
	Verify WRMs receive the data	6. Use the HD-4, HD-5, and HD-6 API Testers to verify the data being received at each WRM is correct for the corresponding MAC address.	API Testers for HD-4, HD-5, and HD-6 only display received data packet information corresponding to their MAC address.	HD-4, 5, & 6 display only receive data corresponding to their MAC addresses.
		7. Allow PBP transmissions to continue for 180 seconds. 8. Use HD-1, HD-2, and HD-3 API Testers to stop PBP transmissions.	API Testers for HD-4, HD-5, and HD-6 stop displaying received data packet information.	HD-4, 5, & 6 stop reporting received data packets.
		9. Use the HD-5 and HD-6 API Testers to verify data received at each WRM.	API Testers for HD-5 and HD-6 indicate receipt of ~150 packets (or 1 packet for each 15 seconds the test was run).	HD-1 transmitted 100560 packets. HD-4 received 64413 packets. HD-2 transmitted 12580 packets. HD-5 received 12579 packets. HD-3 transmitted 10530 packets. HD-6 received 10530 packets.

6.6 Requirement/Test Cross-Reference Matrix

Section Number	Requirement	Test Procedure
3.3.1	The WRM shall support the commands and responses described in the WRM Interface Specification.	6.3
3.3.1	Upon receiving a command to change to a new wireless mode followed by a reboot command, the WRM shall begin operation in the new mode within 10 seconds after receiving the reboot command.	6.3.2.1
3.3.1	Upon receiving a command to change any parameter other than wireless mode, the WRM shall reconfigure to the new setting within 5 ms.	6.4.5
3.3.2.1	The WRM shall support transmit and receive on a single antenna (antenna 1 or 2), and shall also support an antenna "best" mode. The antenna configuration is settable by the HD.	6.3.3.1
3.3.2.2	The WRM shall be able to tune to any WAVE channel as specified by ASTM E2213-03, and any US 802.11a channel as specified by IEEE 802.11a.	6.3.3.5
3.3.2.2	For WAVE channels, the WRM shall support operation at the bandwidth (10 or 20 MHz) specified by ASTM E2213-03.	6.3.3.5
3.3.2.2	For 802.11a channels, the WRM radio shall support operation with either a 10 or 20 MHz bandwidth.	6.3.3.4
3.3.2.2	The WRM shall support all data rates specified by ASTM E2213-03 for channels operating with a 10 MHz bandwidth.	6.3.3.8
3.3.2.2	The WRM shall support all data rates specified by IEEE 802.11a for channels operating with a 20 MHz bandwidth.	6.3.3.8
3.3.2.2	The channel, channel bandwidth, and data rate are settable by the HD.	6.3.3.4 6.3.3.5 6.3.3.8
3.3.2.3	The WRM shall support transmitting at an HD-settable power level up to nominally 20 dBm or higher if available.	6.3.3.7
3.3.2.3	For WAVE channels, the WRM shall limit the transmit power at the SMA connector so the maximum allowable level at the antenna input, as specified by ASTM E2213-03, will not be exceeded.	6.3.3.7.2
3.3.3.1	Upon power-up, the WRM shall initialize to the last stored configuration. The WRM will save its configuration approximately every minute if any changes have occurred.	6.4.1
3.3.2.2	When the WRM is operating in RSU mode, it shall use the last stored MAC address. When the WRM is operating in OBU mode, it shall generate a random MAC address when it powers up and whenever it is commanded by the HD to switch from RSU to OBU mode.	6.4.2

Section Number	Requirement	Test Procedure
3.3.3.3	The WRM shall construct MAC frames in accordance with IEEE 802.11. The MAC frames contain address fields which shall be set as follows: 1. Basic Service Set Identification (BSSID) – shall be set to all 0s. 2. Source Address – shall be set to the WRM MAC address. 3. Destination Address – Broadcast MAC address. The WRM shall always set the Power Management, More Data, and Wired Equivalent Privacy (WEP) fields to 0.	6.4.4
3.3.3.3	The WRM shall perform fragmentation as required to limit the size of any MAC frames to less than or equal to the MAC fragmentation threshold.	6.3.3.6
3.3.3.4	The WRM shall not transmit any IEEE 802.11 management frames. Upon receiving a management frame, the WRM shall acknowledge the frame but not take action based on its contents.	6.4.3
3.3.3.5	On non-control channels, the WRM shall support the use of 802.11 RTS, CTS, and ACK control frames. The WRM shall not transmit any other type of control frame.	3.3.9
3.3.3.5	When transmitting on a non-control channel, the WRM shall send an RTS frame only if the MAC frame length exceeds the RTS/CTS threshold.	6.3.3.9
3.3.3.6	The WRM shall support the use of 802.11 data frames with the subtype data. The WRM shall not transmit any other type of data frame.	6.4.4

7 ACCEPTANCE TEST REPORT

This document summarizes the results of executing the WAVE Radio Module (WRM) Acceptance Test Plan (ATP) (Chapter 6) for the WRM delivered in accordance with the VSC Project: Preliminary Requirements for Second Generation WAVE Radio Module [Section 1.2].

7.1 Scope

Denso conducted all tests specified in the ATP and recorded the results to complete the ATP document. The completed ATP comprises Chapter 6 in this document.

7.2 Test Equipment

The following test equipment was used to complete the ATP:

Description	Model Number
Attenuators	Various values, including 10 dB, 20 dB, 30 dB, and 50 dB fixed attenuators, and a step attenuator.
Power Meter	Gigatronics 8651A meter with 80701 sensor head.
Spectrum Analyzer	HP 8563E
Vector Signal Analyzer	HP 4352B

7.3 ATP Result Summary

Denso conducted all tests as outlined in the ATP on July 16-20, with the exception of the fragment threshold test in Section 3.3.6. The WRM does not currently support fragmentation in WAVE mode. All tests passed, with the exception of some test steps conducted within the Antenna Configuration and Power tests. The following table presents a summary of the ATP Test Results.

Paragraph	Test	Results		
		Telnet	IP Configuration	PbP
6.3.1	WAVEdefault	Pass	Pass	N/A
6.3.2.1	Wireless Mode	Pass	N/A	N/A
6.3.2.2	Service Mode	Pass	Pass	Pass
6.3.2.3	Unit Mode	Pass	Pass	Pass
6.3.3.1	Antenna Configuration	Fail (See Comment 1)	Fail (See Comment 1)	Fail (See Comment 1)

Paragraph	Test	Results		
		Telnet	**IP Configuration**	**PbP**
6.3.3.2	Antenna 1 Compensation Factor	Pass	Pass	N/A
6.3.3.3	Antenna 2 Compensation Factor	Pass	Pass	N/A
6.3.3.4	Bandwidth	Pass	Pass	Pass
6.3.3.5	Fastchannel	Pass		
6.3.3.6	Fragmentation			
6.3.3.7	Power	Fail (See Comment 2)	Fail (See Comment 2)	Fail (See Comment 2)
6.3.3.8	Data Rate	Pass	Pass	Pass
6.3.3.9	RTS Threshold	Pass	Pass	Pass
6.3.4.1	Configuration Parameters	Pass	Pass	N/A
6.3.4.2	Hardware Version	Pass	N/A	N/A
6.3.4.3	RSSI	Pass	N/A	Pass
6.3.4.4	Software Version	Pass	N/A	N/A
6.4.1	Power-up Initialization	Pass	Pass	N/A
6.4.2	MAC Address	Pass		
6.4.3	802.11 Management Frames	Pass		
6.4.4	802.11 Data Frames	Pass		
6.4.5	WRM Reconfiguration Time	Pass		
6.5.1.1	Single Transmitter with Multiple Receiver – Broadcast Addressing	Pass		
6.5.1.2	Single Transmitter with Multiple Receiver – Directed Addressing	Pass		
6.5.2	Multiple Transmitters with Multiple Receivers	Pass		

Test Result Comments:

1. When antenna 1 or antenna 2 is selected, most packets are received on the selected antenna, but the API Tester reports some packets also being received on the non-selected antenna. See 7.3.1 for more details.
2. Some output power measurements were outside the +/- 1dB margin. See 7.3.2 for more details.

7.3.1 Antenna Configuration Tests

Subsequent to the ATP, extended Antenna Configuration testing was performed to more accurately quantify the ratio of packets received on the non-selected antenna to those received on the selected antenna. These tests were run with broadcasted packets (no acknowledgements) and strong RSSI. In all cases greater than 98% of the transmitted packets were received.

7.3.1.1 No Attenuation on Selected Antenna

Testing was performed with no attenuation between the WRM SMA connectors and the antennas. When antenna 1 was selected, 99% of the received packets were correctly received on antenna 1, with the remaining 1% received on antenna 2. When antenna 2 was selected, 97.5% of the received packets were correctly received on antenna 2, with the remaining 2.5% received on antenna 1.

7.3.1.2 50 dB Attenuator on Selected Antenna

Testing was performed with 50 dB of attenuation between the WRM SMA connector for the selected antenna and the antenna. When antenna 1 was selected, 93% of the received packets were correctly received on antenna 1, with the remaining 7% received on antenna 2. When antenna 2 was selected, 98% of the received packets were correctly received on antenna 2, with the remaining 2% received on antenna 1.

7.3.1.3 No Antenna on Selected Antenna

Testing was performed with only a 50Ω load (no antenna) attached to the selected antenna. When antenna 1 was selected, 96% of the received packets were correctly received on antenna 1, with the remaining 4% received on antenna 2. When antenna 2 was selected, 95% of the received packets were correctly received on antenna 2, with the remaining 5% received on antenna 1.

7.3.1.4 No Antenna on Non-Selected Antenna

Testing was performed with only a 50Ω load (no antenna) attached to the non-selected antenna. When antenna 1 was selected, 97% of the received packets were correctly received on antenna 1, with the remaining 3% received on antenna 2. When antenna 2 was selected, 98% of the received packets were correctly received on antenna 2, with the remaining 2% received on antenna 1.

7.3.2 Power Tests

All output power measurements outside the proposed +/- 1dB margin are highlighted in the completed ATP. For the worst cases, power measurements fell outside the +/- 1dB margin by an additional +1.3/-0.6 dB.

The WRM unit used for performing the ATP Power Tests consistently produced between 0.5 and 1 dB lower output power levels when transmitting on antenna 2 compared to antenna 1. In general, antenna 2 posted better output power results than antenna 1.

Power Limiting Test results showed the WRM consistently and appropriately limited the transmit power. However, due to the power setting issues described above, the measured power for some settings was outside the +/- 1dB margin.

7.4 Software Issues Discovered While Testing

While executing the ATP, the software issues presented in this section were identified. All problems were reported to software developers, and corrections were implemented. The software fixes were verified by re-running appropriate sections of the ATP. The ATP includes the rerun test results.

Denso maintains the software in a configuration management tool, labels all builds used in formal tests, and tracks all changes. All API Tester issues were discovered in the build labeled VSCC version 0.1 and corrected in VSCC version 0.2. The WRM issue was discovered in the build labeled VSCC version 0.1 and corrected in VSCC version 0.2.

7.4.1 API Tester Issues

7.4.1.1 Bandwidth setting could be changed while WAVE channel is selected

The API Tester allowed the user to change the bandwidth setting while a WAVE channel was selected. Since the bandwidth setting only applies to 802.11a channels, the API Tester should not allow the user to change the bandwidth setting when a WAVE channel is selected.

The API Tester was modified to disable bandwidth changes when a WAVE channel is selected.

7.4.1.2 API Tester changed 802.11a Bandwidth setting without user issuing the change

The API Tester used the 802.11a Bandwidth field to report the selected WAVE channel's bandwidth. When changing from a 10 MHz WAVE channel to an 802.11a channel, the 10 MHz bandwidth setting was always applied to the 802.11a channel, regardless of the previous 802.11a Bandwidth setting.

The API Tester was modified to disable bandwidth reporting when a WAVE channel is selected, and only display the last 802.11a Bandwidth setting.

7.4.1.3 Telnet login not consistently successful on power up or following reset

Following a Telnet WAVEdefault command, API Tester occasionally reported “WRM Get Configuration Communication Error or not in WAVE mode”. Each time this error message was displayed by the API Tester, the user issued a Telnet Config Command. The API Tester then reported incorrect login in the Telnet window.

The API Tester was modified to detect login failures on the Telnet interface and to retry the Telnet login.

7.4.1.4 WRM configuration not consistently retrieved on power up or following reset

Following an IP Reset WAVE Default command, API Tester occasionally reported “WRM Get Configuration Communication Error or not in WAVE mode”. Each time this error message was displayed by the API Tester, the user issued an IP Get Current Configuration Command. The API Tester then reported the current configuration without reporting any errors.

This issue was the result of the API Tester trying to establish communication with the WRM before the WRM completed power up or reset. The API Tester was modified to detect errors and retry when establishing communication with the WRM.

7.4.2 WRM Issue

7.4.2.1 IP Reset WAVE Default did not consistently reset WRM parameters to defaults

While running the ATP, the IP Configuration WAVE default command did not always reset the parameters to the default settings.

Under certain circumstances the WRM software did not recognize that parameters had been changed from the default configuration, so the parameter values were not being reset to the default values. The WRM software was modified to correct this issue.

A-1 TERMS, ACRONYMS, AND ABBREVIATIONS

Acronym	Term
AC	Alternating Current
ACK	Acknowledgement
ADC	Analog-to-Digital Converter
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
ANT	Antenna
AP	Access Point
API	Application Programming Interface
AR	Atheros
ASTM	American Society for Testing and Materials
ATP	Acceptance Test Plan
BDA	Bi-Directional Amplifier
BPSK	Binary Phase Shift Keying
BSSID	Basic Service Set Identification
BW	Bandwidth
CFR	Code of Federal Regulations
CLA	Cigarette Lighter Adapter
CLI	Command Line Interface
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance
CTS	Clear to Send
DAC	Digital-to-Analog Converter
dB	Decibel
dBi	Decibel Isotropic
dBm	Decibel Milliwatts
DC	Direct Current
DSRC	Dedicated Short Range Communications
EIRP	Equivalent Isotropically Radiated Power
EJTAG	Enhanced Joint Test Action Group (a standard defined by MIPS Technologies)
EVM	Error Vector Magnitude
FCC	Federal Communications Commission
FEC	Forward Error Correction
FIPS	Federal Information Processing Standard
FLASH	A type of nonvolatile memory that can be erased and reprogrammed
GHz	Gigahertz
GPIO	General Purpose Input Output
GUI	Graphical User Interface

HD	Host Device
Hz	Hertz
ICE	In-Circuit Emulator
IEEE	Institute of Electrical and Electronics Engineers
IHL	IP Header Length
IP	Internet Protocol
LAN	Local Area Network
LED	Light Emitting Diode
MAC	Medium Access Control
Mbps	Megabits per Second
MHz	Megahertz
MII	Media Independent Interface
MIPS	Reference to MIPS Technologies
N/A	Not Applicable
N/A	Not Applicable
NDA	Non-Disclosure Agreement
ns	Nanoseconds
OBU	On Board Unit
OFDM	Orthogonal Frequency Division Multiplexing
OS	Operating System
PBP	Packet-by-Packet
PCB	Printed Circuit Board
PCF	Point Control Function
PCI	Peripheral Component Interconnect
PER	Packet Error Rate
PHY	Physical Layer
ppm	Parts per Million
QAM	Quadrature Amplitude Modulation
QPSK	Quaternary Phase Shift Keying
RF	Radio Frequency
RFC	Request for Comment
RMS	Root Mean Square
RS-232	A mature serial data interface standard
RSSI	Received Signal Strength Indicator
RSU	Road Side Unit
RSV	Reserved
RTOS	Real-Time Operating System
RTS	Request to Send
RX	Receiver

Rx	Receive
SDRAM	Synchronous Dynamic Random Access Memory
SM	Service Mode
SMA	Subminiature Version A (a high frequency RF connector)
SOW	Statement Of Work
SSID	Service Set ID
SW	Software
TBD	To Be Determined
TCP	Transport Control Protocol
TKIP	Temporal Key Integrity Protocol
TX	Transmitter
Tx	Transmit
UART	Universal Asynchronous Receiver-Transmitter
UM	Unit Mode
UNII	Unlicensed National Information Infrastructure
VSA	Vector Signal Analyzer
VSC	Vehicle Safety Communications
VSCC	Vehicle Safety Communications Consortium
WAVE	Wireless Access in Vehicular Environments
WCO	WAVE Configuration Option
WCRO	WAVE Configuration Request Option
WEP	Wired Equivalent Privacy (original 802.11 data encryption standard)
WRM	WAVE Radio Module
WRXO	WAVE Rx Option
WTXO	WAVE Tx Option

A-2 REFERENCES

[1] ASTM E2213-03 Standard Specification for Telecommunications and Information Exchange Between Roadside and Vehicle Systems – 5 GHz Band Dedicated Short Range Communications (DSRC) Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

[2] IEEE 802.11a, 1999 Edition, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. High-speed Physical Layer in the 5 GHz band.

[3] ANSI/IEEE 802.11 - 1999 (Reaff 2003), Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications.

[4] CFR Title 47—Telecommunication, CHAPTER I--FEDERAL COMMUNICATIONS COMMISSION , PART 90--PRIVATE LAND MOBILE RADIO SERVICES

[5] Atheros AR5002AP-X Product Sheet, not dated

[6] Atheros AR5002 Family Chipset Product Sheet, not dated

[7] Hirose U.FL Series Miniature RF Coaxial Connectors (and cables), dated January 2004

[8] CUI Inc. DPS050240-P5 120V/5V AC-DC Power Converter, dated April 2002

[9] Internet Engineering Task Force RFC 854 Telnet Protocol Specification, dated May 1983.

[10] Internet Engineering Task Force RFC 791 Internet Protocol, dated September, 1981.

Appendix F:
Testing System

TABLE OF CONTENTS

1 Background 1-1

2 Preliminary Requirements 2-1

2.1 Introduction 2-1

2.2 Development Requirements 2-1

2.3 Applications 2-2

2.3.1 On-Board Unit (OBU) Test Application 2-2

2.3.2 OBU Test and RSU Test Common Requirements 2-4

3 Application Message Specification 3-1

3.1 Introduction 3-1

3.1.1 Scope 3-1

3.1.2 Application Interfaces 3-1

3.1.3 GPS Receiver Interface 3-2

3.1.4 Vehicle Bus Interface 3-2

3.1.5 Traffic Signal Interface 3-2

3.1.6 WAVE Radio Module Interface 3-2

3.2 Message Definitions 3-3

3.2.1 Common Message Header 3-3

3.2.2 OBU V2V Safety Message 3-4

3.2.3 RSU Traffic Signal Message 3-6

4 Testing System Specification and Architecture 4-1

4.1 Introduction 4-1

4.1.1 Scope 4-1

4.2 Architecture 4-1

4.2.1 Overview 4-1

4.2.2 External Interfaces 4-1

4.2.3 User Interface 4-2

4.2.4 Test Control 4-4

4.3 Class Descriptions 4-6
4.3.1 Class Descriptions 4-7
4.4 Data 4-25
4.4.1 Structures 4-25
4.4.2 Global Variables 4-27
4.5 Design Goals and Constraints 4-29
4.5.1 Design Methodology 4-29
4.5.2 MFC, Standard Library Usage 4-29
4.5.3 ANSI Compliance 4-29
4.5.4 Memory Management 4-29
4.5.5 Naming Conventions 4-29
4.6 Modifications and Enhancements 4-29
4.6.1 Changing Over the Air Formats 4-29
4.6.2 Changing Data Logging 4-30
4.6.3 Changing Test Types 4-30
4.6.4 Changing T9App Configuration Loading / Saving 4-30
4.6.5 Changing CAN messages 4-31

5 Validation Results 5-1

5.1 Introduction 5-1
5.1.1 Scope 5-1
5.2 Test Configurations 5-1
5.2.1 WAVE Radio Module Network Connection 5-1
5.2.2 Test Setups 5-1
5.2.3 Initialization 5-3
5.2.4 Software Builds 5-6
5.3 GUI Parameter Tests 5-6
5.3.1 WRM Configuration Screen 5-6
5.3.2 Comm Parameters Screen 5-9
5.3.3 Test Options Screen 5-14
5.3.4 Traffic Signal Information Screen 5-17
5.3.5 Test Display Screen 5-20
5.3.6 GUI Configuration Recording, Persistence 5-25

5.4 Interface Tests 5-26
5.4.1 GPS Receiver Interface Tests 5-26
5.4.2 Vehicle Bus Interface Tests 5-30
5.4.3 Traffic Signal Interface Tests 5-39
5.5 Requirement/Test Cross Reference Matrix 5-45
5.5.1 Task 9 Software Requirement Verification 5-45
5.5.2 Common Message Header Verification 5-48
5.5.3 OBU Message Verification 5-48
5.5.4 RSU Message Verification 5-49

6 Appendix 6-1

6.1 Terms, Acronyms, and Abbreviations 6-1
6.2 References 6-3
6.3 Task 9 Device CAN Input Messages 6-3
6.3.1 Vehicle Velocity Message 6-3
6.3.2 Vehicle Acceleration Message 6-4
6.3.3 Vehicle Devices Message 6-5
6.4 Traffic Signal Interface 6-5
6.4.1 Initial Request/Response State 6-6
6.4.2 Periodic Request/Response State 6-6
6.5 Preliminary Vehicle-to-Vehicle Common Message Set 6-9
6.6 Task 9 Application Users' Guide 6-11
6.6.1 Introduction 6-11
6.6.2 Scope 6-11
6.6.3 Setup Procedures 6-11
6.6.4 Operating Instructions 6-14
6.6.5 Troubleshooting 6-25

TABLE OF FIGURES

Figure 2-1. Task 9 Device in the OBU Test Application Configuration 2-2
Figure 2-2. Task 9 Device in the RSU Test Application Configuration 2-3
Figure 3-1. OBU Interfaces 3-1
Figure 3-2. RSU Interfaces 3-2
Figure 3-3. Common Message Header Format 3-3
Figure 3-4. OBU V2V Safety Message Format 3-5
Figure 3-5. RSU Traffic Signal Message Format (Part 1 of 2) 3-7
Figure 3-6. RSU Traffic Signal Message Format (Part 2 of 2) 3-8
Figure 4-1. T9App Architecture 4-1
Figure 4-2. T9App External Interfaces 4-2
Figure 4-3. Configuration Dialogs Screen Shots 4-3
Figure 4-4. Test Display Dialog Screen Shot 4-3
Figure 4-5. T9App Test Execution Architecture (UML Diagram) 4-5
Figure 5-1. Generic Test Setup 5-2
Figure 5-2. OBU Test Setup 5-2
Figure 5-3. RSU Test Setup 5-3
Figure 6-1. Common Setup 6-11
Figure 6-2. OBU Setup 6-13
Figure 6-3. RSU Setup 6-14
Figure 6-4. T9App Main Screen Layout 6-15
Figure 6-5. WRM Configuration Screen Layout 6-15
Figure 6-6. Comm Parameters Screen Layout 6-16
Figure 6-7. Test Options Screen Layout 6-18
Figure 6-8. Traffic Signal Information Screen Layout 6-19
Figure 6-9. Location Information Screen Dialog Box 6-19
Figure 6-10. Test Display Screen Layout 6-20
Figure 6-11. Sample OBU Logfile 6-23
Figure 6-12. Excel Text Import Wizard 6-24
Figure 6-13. Worksheet Selection 6-24
Figure 6-14. Imported Logfile 6-25

Figure 6-15. COM Port Conflict Error Message 6-26
Figure 6-16. GPS Port Initialization Error Message 6-26
Figure 6-17. Traffic Signal Port Initialization Error Message 6-27
Figure 6-18. CAN Bus Initialization Error Message Box 6-27

TABLE OF TABLES

Table 2-1. Definitions Used Throughout the Document 2-1
Table 3-1. Common Message Header Field Descriptions 3-4
Table 3-2. OBU V2V Safety Message Discrete Field Definitions 3-6
Table 3-3. RSU Traffic Signal Message Discrete Field Definitions 3-9
Table 4-1. T9App Dialog Class Summary 4-4
Table 4-2. T9App Class Summary 4-6
Table 4-3. CCanControl Methods and Attributes 4-8
Table 4-4. CCanMsg Methods and Attributes 4-8
Table 4-5. CCommParams Methods and Attributes 4-9
Table 4-6. CDeviceDatabase Methods and Attributes 4-10
Table 4-7. CGpsControl Methods and Attributes 4-11
Table 4-8. CGpsPosition Methods and Attributes 4-11
Table 4-9. CLocationInfo Methods and Attributes 4-12
Table 4-10. CSerialPort Class Methods and Attributes 4-15
Table 4-11. CSignalControl Methods and Attributes 4-15
Table 4-12. CSignalControl State Machine Events 4-16
Table 4-13. CSignalInfo Methods and Attributes 4-17
Table 4-14. CTestLog Methods and Attributes 4-18
Table 4-15. CTestStatusDialog Methods and Attributes 4-18
Table 4-16. CTestStatusDialog Processes 4-19
Table 4-17. CVehicleInfo Methods and Attributes 4-20
Table 4-18. CWaveDeviceInfo Methods and Attributes 4-22
Table 4-19. CWrmControl Methods and Attributes 4-23
Table 4-20. CWrmMsg Methods and Attributes 4-24
Table 4-21. GPS Location Structure 4-25

Table 4-22. Test Header Structure 4-25
Table 4-23. Stopping Location Structure 4-26
Table 4-24. Common Message Structure 4-26
Table 4-25. OBU VTV Message 4-26
Table 4-26. RSU TS Message 4-27
Table 4-27. T9 App Globals 4-27
Table 4-28. WAVE API Globals 4-28
Table 4-29. PCAN USB Globals 4-28
Table 5-1. OBU Initialization Procedure 5-3
Table 5-2. RSU Initialization Procedure 5-4
Table 5-3. Communication Parameters Initial Values 5-4
Table 5-4. Test Options Initial Values 5-5
Table 5-5. Traffic Signal Parameters Initial Values 5-5
Table 5-6. WRM and T9App Software Versions 5-6
Table 5-7. WRM Configuration Screen Results 5-7
Table 5-8. WRM Configuration Data Elements 5-9
Table 5-9. Comm Parameters Screen Low Parameter Values 5-10
Table 5-10. Comm Parameters Screen Low Parameter Results 5-10
Table 5-11. Comm Parameters Screen Data Elements 5-11
Table 5-12. Comm Parameters Screen Mid Parameter Values 5-11
Table 5-13. Comm Parameters Screen Mid Parameter Results 5-12
Table 5-14. Comm Parameters Screen High Parameter Values 5-13
Table 5-15. Comm Parameters Screen High Parameter Results 5-13
Table 5-18. Test Options Screen Parameter Values 5-14
Table 5-19. Test Options Screen Case 1 Results 5-15
Table 5-20. Test Options Data Elements 5-16
Table 5-21. Test Options Screen Case 2 Results 5-16
Table 5-22. Test Options Screen Case 3 Results 5-17
Table 5-23. Traffic Signal Information Screen Results 5-18
Table 5-24. Traffic Signal Message Data Elements 5-19
Table 5-25. Distance, Heading Test GPS Data 5-21
Table 5-26. Distance, Heading Test Parameter Values 5-21
Table 5-27. Distance, Heading Test Results 5-21

Table 5-28. RSU – RSU Bearing Test GPS Data 5-22
Table 5-29. RSU – RSU Bearing Test Parameter Values 5-22
Table 5-30. RSU – RSU Bearing Test Results 5-23
Table 5-31. OBU – OBU Relative Heading Test Parameters 5-24
Table 5-32. OBU – OBU Relative Heading Test Results 5-25
Table 5-33. GUI Configuration Recording, Persistence Results 5-26
Table 5-34. Common Message Header GPS Data Test Results 5-27
Table 5-35. Common Message Header GPS Data Elements 5-27
Table 5-36. OBU GPS Interface Test Results 5-28
Table 5-37. OBU V2V Safety Message GPS Data Elements 5-28
Table 5-38. RSU GPS Interface Test Results 5-30
Table 5-39. RSU Traffic Signal Message GPS Data Elements 5-30
Table 5-40. Vehicle Velocity Settings (Low-Value) 5-31
Table 5-41. Vehicle Acceleration Settings (Low-Value) 5-31
Table 5-42. Vehicle Devices Settings (Low-Value) 5-32
Table 5-43. Vehicle Interface Low-Value Test Results 5-32
Table 5-44. OBU V2V Safety Message Vehicle Data Elements 5-33
Table 5-45. Vehicle Velocity Settings (Mid-Value) 5-34
Table 5-46. Vehicle Acceleration Settings (Mid-Value) 5-34
Table 5-47. Vehicle Devices Settings (Mid-Value) 5-34
Table 5-48. Vehicle Interface Mid-Value Test Results 5-35
Table 5-49. Vehicle Velocity Settings (High-Value) 5-35
Table 5-50. Vehicle Acceleration Settings (High-Value) 5-36
Table 5-51. Vehicle Devices Settings (High-Value) 5-36
Table 5-52. Vehicle Interface High-Value Test Results 5-36
Table 5-53. Vehicle Devices Settings 5-37
Table 5-54. Vehicle Interface Test Results 5-37
Table 5-56. Vehicle Devices Settings 5-38
Table 5-57. Vehicle Interface Test Results 5-38
Table 5-58. Vehicle Devices Settings 5-38
Table 5-60. Vehicle Interface Test Results 5-38
Table 5-61. Traffic Signal Long Initial Response, Fast Polling Results 5-39
Table 5-62. Short Initial Response, Slow Polling Results 5-40

Table 5-63. Traffic Signal Active Phase 1 and 5 Parameters 5-41
Table 5-64. Traffic Signal Active Phase 1 and 5 Results 5-41
Table 5-65. RSU Traffic Signal Message Data Elements 5-41
Table 5-66. Traffic Signal Active Phase 2 and 6 Parameters 5-42
Table 5-67. Traffic Signal Active Phase 2 and 6 Results 5-42
Table 5-69. Traffic Signal Active Phase 3 and 7 Parameters 5-43
Table 5-70. Traffic Signal Active Phase 3 and 7 Results 5-43
Table 5-71. Traffic Signal Active Phase 4 and 8 Parameters 5-44
Table 5-72. Traffic Signal Active Phase 4 and 8 Results 5-44
Table 5-73. Task 9 Software Requirement Cross Reference 5-45
Table 5-74. Common Message Header Field Verification 5-48
Table 5-75. OBU Message Verification 5-48
Table 5-76. RSU Message Verification 5-49
Table 6-1. Comm Parameters Screen Field Definitions 6-16
Table 6-2. Test Option Screen Field Definitions 6-18
Table 6-3. Traffic Signal Information Screen Field Definitions 6-19
Table 6-4. Test Display Screen Field Definitions 6-21
Table 6-5. Logfile Record Types 6-22

1 Background

The WAVE radio modules developed under Task 6D include the capability for hardware and software operation at 5.9 GHz, closely compliant with available lower layer DSRC standards. The WAVE radio modules also include a well-documented Applications Programming Interface (API) that includes access to many of the functions available in the DSRC lower layers. The development of a common computing platform was necessary to support future VSCC testing and evaluation of functionalities being specified in the upper layer standards. This common computing platform was also required for simulating transmissions from traffic signal controllers, as well as interfacing with these controllers to transmit traffic signal data in real time.

The next generation testing system developed under Task 9 interfaces with automotive network systems, traffic signal controllers and research computers. As well, the system supports enhanced data acquisition capabilities, both for recording pertinent test-related information, and for acquiring and recording automotive network data pertinent to the testing in Task 10. Due to the wide range of anticipated testing uses, the next generation test system was designed to function as a portable system with flexible system interfaces to plug into relevant automotive networks, traffic signal controllers and research computers, as required.

The preliminary testing of communications functionalities necessary for the development of prototype vehicle safety applications depended upon access to proprietary in-vehicle networks and systems, as well as access to the DSRC communications capabilities. The API on the WAVE radio modules was also designed to be available for direct access by the proprietary on-board computing systems of VSCC member companies. Development of software on these proprietary systems to support this data integration and functionality testing represented an additional development activity that was necessary to enable Task 10 testing and evaluation.

The contents of Chapters 3-5 and portions of Chapter 6 of this report were prepared by the identified contractor, Denso LA Laboratories, in conjunction with the VSCC. The materials prepared by Denso comprised a number of separate specifications and reports. These were integrated into Chapters 3-6 of this report with minor editorial and formatting revisions.

This project was completed successfully within the necessary short time constraints imposed by the Task 10 testing requirements. The Task 9 software was delivered in time, and in sufficient working order, to support the final phases of the Task 10 testing, including real time vehicle bus data transfer between vehicles of different manufacturers, as well as real time traffic controller data transmission from intersection locations to vehicles in motion.

2 Preliminary Requirements

The preliminary requirements presented in this chapter represent the starting point for the development of the Task 9 software, thus are represented in the future tense. These preliminary requirements were subsequently refined under an iterative process between Denso and the VSCC in order to complete the detailed specifications described later in this report.

2.1 Introduction

The Task 9 test software and Task 9 device will be used to support testing for VSC task 10. The task 10 testing will involve running scenario specific tests involving two or more vehicles and collecting data for analysis of each test.

The primary roles of the Task 9 device shall be to:

- Interface between a vehicle communication bus or a roadside device and the Wave Radio Module (WRM) so that the WRM can transmit information from a vehicle or roadside device to neighboring vehicles.
- Receive and decode incoming messages from the WRM transmitted from surrounding vehicles or roadside devices.
- Record information sent to and information received from other devices through the WRM.
- Allow an interface to change WRM parameters and application-specific communication parameters.

Table 2-1 refers to commonly used terms and their definitions.

Table 2-1. Definitions Used Throughout the Document

Test Scenario Parameters	communication parameters to be set according to the test scenario defined in task 10
Wave Radio Module (WRM)	configurable radio module provided as a work output from VSC Task 6D

2.2 Development Requirements

The Task 9 device shall be the existing laptop computers currently used as part of the VSC communications test kit, with Windows operating system installed. The software to be developed by the supplier for VSC Task 9 shall be configured to operate on the Task 9 device. The deliverables for Task 9 shall include validation of correct functional operation of developed software on the Task 9 device, plus all source code, development environments and any necessary licensing so that members of the VSC consortium can freely modify the source code to perform specific tasks and create new applications.

2.3 Applications

The Task 9 software shall have the capability to run one application at a time with the Task 9 device being configurable to easily choose amongst a set of preloaded applications.

As part of this task, the supplier developing the Task 9 software shall provide two basic applications for use on the Task 9 device. The on-board unit (OBU) test application will be used in a vehicle and will wirelessly broadcast vehicle parameters and decode incoming packets containing surrounding vehicle parameters. The roadside unit (RSU) test application will be used near a roadway infrastructure device such as a traffic signal and will broadcast traffic signal information. The next two subsections discuss these two applications and the unique requirements of each. The last subsection discusses common requirements of these applications.

2.3.1 On-Board Unit (OBU) Test Application

Figure 2-1 shows the basic physical connections the OBU Test application will utilize.

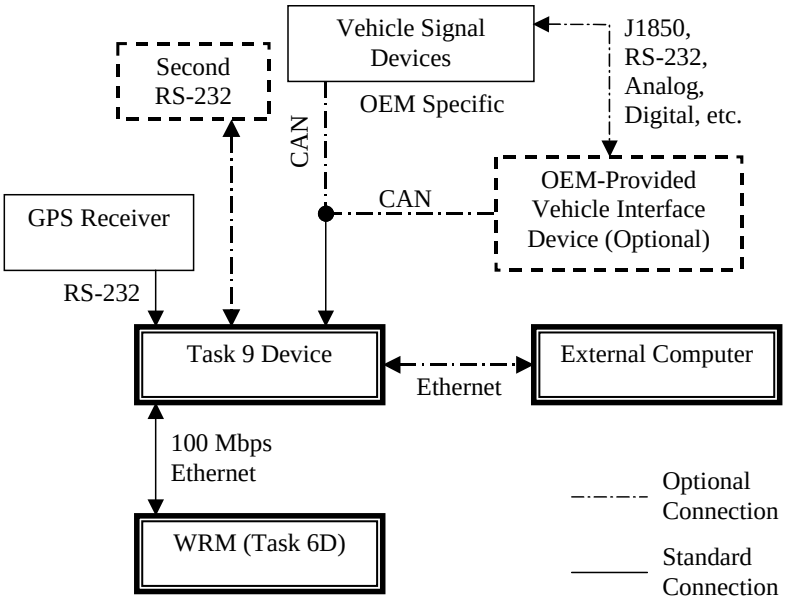


Figure 2-1. Task 9 Device in the OBU Test Application Configuration

2.3.1.1 OEM Vehicle Interface

In the OBU test application, the Task 9 device shall use a Controller Area Network (CAN) bus to receive messages with vehicle information such as vehicle speed, brake position, acceleration, etc. The format of the information received on the CAN bus is defined in Section 6.3.

The OEM Vehicle Interface software shall be written so that OEMs may modify the source code to achieve an alternative mapping from CAN message identifiers and formats to vehicle data.

2.3.1.2 Wireless Data Output

The OBU test application shall periodically issue commands to the WRM to transmit the latest GPS and vehicle information wirelessly. The periodicity of the transmitted information shall be adjustable through the control user interface and shall allow periods at least as small as 10 milliseconds. The format of the data sent wirelessly is defined in Section 3.2.2.

2.3.1.3 Roadside Unit (RSU) Test Application

Figure 2-2 shows the basic physical connections the RSU test application will utilize.

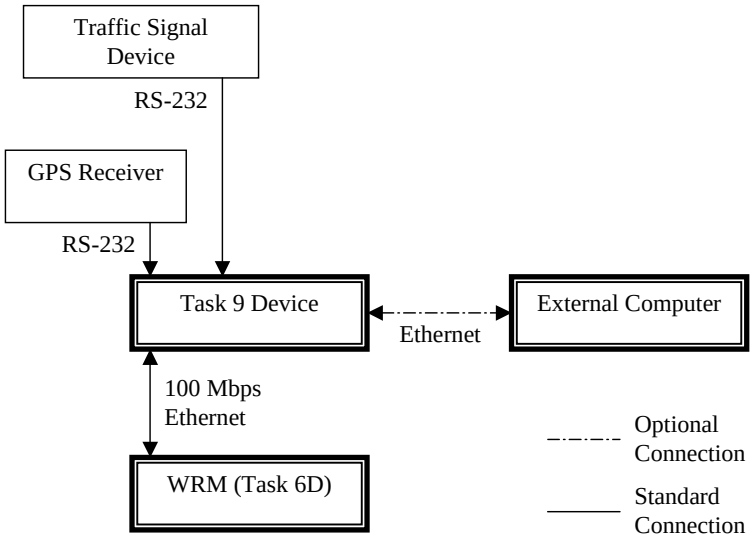


Figure 2-2. Task 9 Device in the RSU Test Application Configuration

2.3.1.4 Traffic Signal Device Interface

The RSU test application shall decode traffic signal information from an RS-232 connection. The format of the information contained on the RS-232 connection is defined in Section 6.4.

2.3.1.5 Wireless Data Output

The RSU test application shall periodically issue commands to the WRM to transmit traffic signal information wirelessly. The periodicity of the transmitted information shall be adjustable through the control user interface and shall allow periods at least as small as 10 milliseconds.

The format and content of the data sent wirelessly, including GPS and traffic signal information from the RS-232 connection on the Task 9 device, is defined in Section 3.2.3.

2.3.1.6 Application Display

Control User Interface

The RSU test application shall be configurable so that the user has the capability to modify constant parameters for the traffic signal information. Example constant parameters that may require adjustment via the control user interface include location of the intersection, directionality, stopping locations, number of lanes, etc. The constant parameters that require adjustment will be defined by the members of the VSC consortium.

2.3.2 OBU Test and RSU Test Common Requirements

2.3.2.1 GPS Receiver Interface

In the OBU test application, the Task 9 device shall use an RS-232 port to receive ASCII messages formatted in the National Maritime Electronics Association (NMEA) 0183 standard. At a minimum, the GPS receiver will be configured to output the “GPGGA” and "GPVTG" strings defined by NMEA 0183. The application shall parse these messages to get the GPS data required in other parts of this document.

2.3.2.2 Interface to WRM

Telnet Interface to WRM

The WRM can be controlled via a telnet interface. For this reason, the Task 9 device shall have a telnet client allowing a user to connect to the WRM for manual configuration.

IP API Interface to WRM

The IP API interface to the WRM consists largely of get, set, send, and transmit commands supplied to calling applications through an API supplied with the WRM. The API utilizes an Ethernet connection to send packets to the WRM issuing commands. The API uses the IP Options field of the IP Header to send the commands.

The API has been implemented and tested utilizing a Microsoft Windows operating system. The supplier developing the Task 9 software will be responsible interfacing with the API on the Task 9 device. The source code for the API will be written utilizing Berkeley Sockets.

In the case where the WRM hardware becomes available but the API has not yet been ported, telnet commands to the WRM may be used to statically configure the WRM which will allow testing of other functionality.

2.3.2.3 Wireless Data Output

In addition to the data content sent from the OBU test and RSU test applications, each data packet shall also contain the following:

- *Sender ID* (either preset OR randomized at start of test)
- Common *Message ID* (to be defined by VSCC members)
- *Message Count* (incrementing short unsigned integer)
- *Broadcast Power*
- Operating System Time (nanoseconds)
- *State of Data Logging* (i.e., logging active, logging inactive)
- *Latitude, Longitude, Height* (ellipsoidal)
- *GPS Seconds in Week* (conversion from UTC time to GPS Seconds in Week) (set *GPS Seconds in Week* to zero for devices with no GPS receiver attached)
- *Heading* (from GPS receiver)

2.3.2.4 Data Logging

By default, the Task 9 device shall record all data sent and all data received from surrounding devices via the WRM. In addition, the Task 9 device shall record reception parameters, timing, and statistics associated with each data packet. The recorded reception parameters include:

- Receiver Signal Strength Indicator (*RSSI*)
- *Distance to Sender* (using valid GPS coordinates of sender and receiver)
- *Heading to Sender* (using valid GPS coordinates of sender and receiver)
- Current *GPS Seconds in Week* of receiver
- *Latitude, Longitude, Height* (ellipsoidal) of receiver
- *Heading* (from GPS receiver)
- *Speed* (meters/second, via CAN from host vehicle if receiver)

The Task 9 device shall contain enough storage space to record eight hours of data with five communicating devices in the immediate area transmitting a 100 byte packet once every 100 milliseconds. The 100 byte packet does not include overhead introduced by the storage medium nor does it include the size of the reception parameters.

Members of the VSC consortium plan to modify the OBU test and RSU test applications to support specific application development in the potential future VSC projects. The supplier of the Task 9 software shall write the OBU test and RSU test applications in such a way as to provide a mechanism allowing recording of additional data.

All parameters controllable from the control user interface shall be recorded.

2.3.2.5 Application Display

The Task 9 device shall have a monitor/display and data entry device (such as a keyboard) allowing the user to configure the applications and observe their run-time status.

Control User Interface

The applications shall retain the value of all parameters controllable from the control user interface during a “normal” power cycle.

The control user interface shall allow the user to configure the applications to transmit wirelessly through the WRM upon application execution. This implies the application will also be decoding CAN and/or serial data as appropriate for the application.

The control user interface shall allow the user to adjust all WRM communication parameters described in the WRM interface specification.

The control user interface shall display the IP address of the Task 9 device at the Ethernet port connected to the WRM.

The OBU test and RSU test applications shall each provide a display for configuring the communication parameters. The display shall allow the user to adjust the following communication parameters inherent to the application:

- Periodicity of message transmission
- Size of message being transmitted (append data to standard message using same message ID)
- Destination IP address (as a default, this should be the broadcast IP address)

The OBU test and RSU test applications shall have the ability to initiate, suspend, or terminate a test. The test shall consist of the OBU test or RSU test applications transmitting and recording data as described in previous sections. The length of the test shall be controllable via the control user interface. The user shall be able to control the length of the test by specifying the number of packets sent or the number of seconds of test time. During a test, the Task 9 device shall record data as outlined in sections above.

The OBU test and RSU test applications shall have the ability to specify a filename for recorded test data. The format for the filename shall be <Test Name>_<Test Run>_<GPS Date> where:

- <Test Name> is a field entered by the user
- <Test Run> is an automatically incrementing number incremented after a test has ended (i.e., terminated by the user, maximum number off packet sent, test time exceeded)
- <GPS Date> is derived from the local GPS information.

Real-Time Interface

The OBU test and RSU test applications shall each have an active visual display that shows other Task 9 devices that have communicated with the host Task 9 device. The display shall support at least 10 other Task 9 devices and update the information displayed at least once per second. The text on the display should be easily readable in a vehicular environment. For each device, the following shall be displayed:

- Sender ID
- State of Data Logging
- Most recent Message Count
- Distance to Sender
- Relative Heading to Sender = Heading to Sender (from GPS differencing) – Heading (only to be calculated when host vehicle speed > 5 m/s)
- RSSI
- Speed

3 Application Message Specification

3.1 Introduction

This chapter provides the Message Specification for the Wireless Access in Vehicular Environments (WAVE) application which was developed in accordance with the requirements in Chapter 2.

3.1.1 Scope

This Task 9 Application (T9App) Message Specification describes the format and content of the OBU and RSU message data sent by the T9App to the WAVE Radio Module (WRM) for wireless transmission. The requirements in this document were derived from the requirements in Chapter 2, the Preliminary Vehicle-To-Vehicle Common Message Set (defined in Section 6.5), and the VSCC-defined OBU and RSU message formats defined Sections 6.3 and 6.4.

3.1.2 Application Interfaces

This section describes the T9App interfaces. Figure 3-1 and Figure 3-2 illustrate the OBU and RSU configurations. For the OBU, the T9App inputs data from a GPS receiver and vehicle bus. For the RSU, the T9App inputs data from a GPS receiver (optional) and traffic signal. The T9App extracts selected data, formats the messages defined in Chapter 3.2, and sends the messages to the WRM. The subparagraphs below describe the relevant data transferred over each interface.

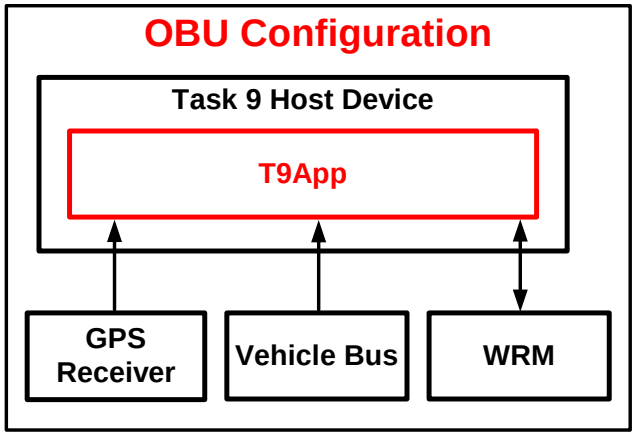


Figure 3-1. OBU Interfaces

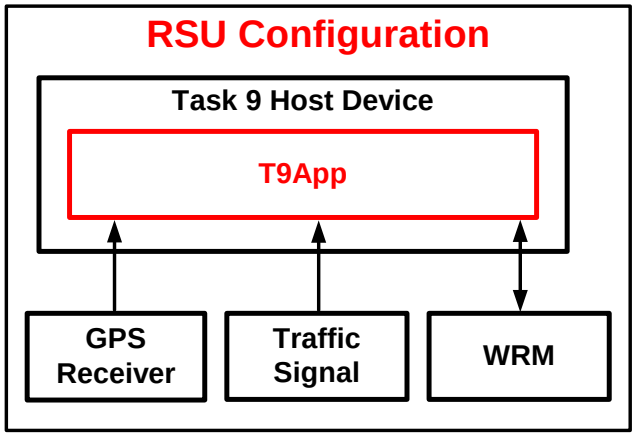


Figure 3-2. RSU Interfaces

3.1.3 GPS Receiver Interface

The T9App receives GPS messages formatted in accordance with the National Maritime Electronics Association (NMEA) 0183 standard [1] over an RS-232 interface. The T9App uses information from the Global Positioning System Fix Data (GPGGA) and Global Positioning Track Made Good and Ground Speed (GPVTG) strings. It obtains date and time from either the UTC Date / Time and Local Time Zone Offset (GPZDA) or the Recommended Minimum Specific GPS/Transit Data string. The T9App operates with GPS receivers that output either string or both.

3.1.4 Vehicle Bus Interface

The T9App receives vehicle data formatted in accordance with Section 6.3 definitions over a Controller Area Network (CAN) bus. The T9App uses information from the Vehicle Velocity, Vehicle Acceleration, and Vehicle Devices messages.

3.1.5 Traffic Signal Interface

The T9App receives a traffic signal message formatted in accordance with the Traffic Signal Interface Specification in Section 6.4 over an RS-232 interface.

3.1.6 WAVE Radio Module Interface

The T9App interfaces to the WRM in accordance with the WRM Interface Specification [2]. The T9App sends the OBU and RSU messages to the WRM as the IP Frame Payload.

3.2 Message Definitions

This section specifies the format of the common message header (which precedes all messages) and the OBU and RSU messages.

3.2.1 Common Message Header

Figure 3-3 illustrates the common message header format and the source of the data in each of the fields. Table 3-1 provides a description of each of the fields.

Byte \ Bit	8	7	6	5	4	3	2	1(lsb)	SOURCE
1	Packet Length MSByte								Calculated value
2	GPS Seconds in Week MSNybble				Packet Length LSNybble (LSBit = 1 Byte)				
3	GPS Seconds in Week …								Calculated from GPS,GPZDA
4	GPS Seconds in Week LSByte								or GPRMC
5	GPS Longitude MSByte								GPS, GPGGA
6	"								
7	"								
8	GPS Longitude LSByte (LSBit = 10**-7 decimal degrees; signed)								
9	GPS Latitude MSByte								GPS, GPGGA
10	"								
11	"								
12	GPS Latitude LSByte (LSBit = 10**-7 decimal degrees; signed)								
13	GPS Altitude MSByte								GPS, GPGGA
14	Altitude (LSBit = 1 cm; unsigned; offset by +1 km)								
15	Unused				Altitude, LSNybble				
16	GPS Heading MSByte								GPS, GTVTG (True Heading)
17	GPS Heading (LSBit = 0.01 degrees; signed; 0 degrees = North)								
18	Sender ID MSByte								Default value or user input
19	Sender ID LSByte								
20	Message Count MSByte								Calculated value
21	Message Count LSByte								
22	Unused		Log	Tx Power (LSBit = 1 dBm)					User input (Log, Tx power)
23	OS Time MSByte								OS High Precision Timer
24	"								
25	"								
26	"								
27	"								
28	"								
29	OS Time LSByte (LSBit = 1 nanosecond)								

Figure 3-3. Common Message Header Format

Table 3-1. Common Message Header Field Descriptions

Field Name	Description
Packet Length	Total packet length including common message header and message body (i.e., OBU message or RSU message, plus the user-specified number of fill bytes).
GPS Seconds in Week	Number of seconds since the beginning of the week. The range is 0 to 604,799. For units without a GPS receiver, this field is set to 0.
GPS Longitude, Latitude, Altitude	Position information received from the GPS receiver. The altitude is the height above ellipsoid.
GPS Heading	True heading information received from the GPS receiver. This field is set to 0 in RSU messages.
Sender ID	Sender ID of the source of the message. The range is 0 to 65535.
Message Count	Number of messages sent during the current test. The first message is sent with a message count of 1 and the count is incremented in subsequent messages. The count rolls over when it is incremented past 65535.
OS Time	Timestamp from OS clock. The precision and accuracy of the time will vary based on the host device. For the current T9app implementation, the precision will not be accurate to nanoseconds. The timestamp begins at an arbitrary value at the beginning of a test. It rolls over approximately every 28 months.
Log	Logging status. 1 = logging enabled. 0 = logging disabled.
Tx Power	Transmit power setting of the message sender. The range of values is 0 to 20, or 31. A value of 0 to 20 indicates the power setting in dBm. A value of all 1s (i.e., 31) indicates full power.

3.2.2 OBU V2V Safety Message

Figure 3-4 illustrates the SAE V2V Safety Message format that will be used as the OBU message. All signed values are two's complement unless otherwise noted. The figure also lists the source of the data that the T9App will use to populate the message fields Table 3-2 provides definitions for fields with discrete integer values.

Byte \ Bit	8	7	6	5	4	3	2	1(lsb)	SOURCE
1	Message Type								Set to 0
2	Temporary ID MSByte								WRM MAC Address
3	Temporary ID...								
4	Temporary ID...								
5	Temporary ID...								
6	Temporary ID...								
7	Temporary ID LSByte								
8	Precision Indicator (Meaning TBD)								Set to 0
9	Longitude of center of vehicle MSByte								GPS, GPGGA
10	"								
11	"								
12	Longitude LSByte (LSBit = 10^{-7} decimal degrees; signed)								
13	Latitude of center of vehicle MSByte								GPS, GPGGA
14	"								
15	"								
16	Latitude LSByte (LSBit = 10^{-7} decimal degrees; signed)								
17	Altitude of center of vehicle MSByte								GPS, GPGGA
18	Altitude (LSBit = 1 cm; unsigned; offset by +1 km)								
19	Unused				Altitude LSNybble				
20	UTC Time MSByte								GPS, GPZDA or GPRMC
21									
22	Number of milliseconds since Jan. 1, 2004 at 00:00:00								
23									
24	UTC Time LSByte (LSBit = 0.001 seconds)								
25	Heading MSByte								GPS. GPVTG (True Heading)
26	Heading (LSBit = 0.01 degrees; signed; 0 degrees = North)								
27	Vehicle Speed MSByte								CAN, Vehicle Velocity Msg
28	Vehicle Speed LSByte (LSBit = 0.01 m/s; unsigned)								
29	Lateral Acceleration MSByte								CAN, Vehicle Acceleration Msg
30	Longitudinal Acceleration MSNybble				Lateral Acceleration LSNybble (LSBit = 0.01 m/s^2; signed)				CAN, Vehicle Acceleration Msg
31	Longitudinal Acceleration LSByte (LSBit = 0.01 m/s^2; signed)								
32	Yaw Rate MSByte								CAN, Vehicle Velocity Msg
33	Yaw Rate LSByte (LSBit = 0.01 deg/sec; signed)								
34	Throttle Position (LSBit = 0.5% open; unsigned)								CAN, Vehicle Devices Msg
35	Brake Applied Status				Brake Applied Pressure				CAN, Vehicle Devices Msg
36	Steering Wheel Angle MSByte								CAN, Vehicle Devices Msg
37	Steering Wheel Angle LSByte (LSBit = 0.02 degrees; signed)								
38	Headlights		Turn Signal/Hazard Signal		Traction Control State		Anti-Lock Brake State		CAN, Vehicle Devices Msg
39	Unused				System Health				CAN, Vehicle Devices Msg
40	Vehicle Length MSByte								Set to 0
41	Vehicle Width (Upper 2 bits)		Vehicle Length (Lower 6 bits; LSBit = 1 cm; unsigned)						
42	Vehicle Width LSByte (LSBit = 1 centimeter)								Set to 0

Figure 3-4. OBU V2V Safety Message Format

Table 3-2. OBU V2V Safety Message Discrete Field Definitions

Byte	Field Name	Description
35	Brake Applied Status	0000 = All off XXX1 = Left front XX1X = Left rear X1XX = Right front 1XXX = Right rear 1111 = All on
35	Brake Applied Pressure	0000 = Not equipped 0001 = Minimum braking pressure 0010 … 1111 = Maximum braking pressure
38	Headlights	00 = Off 01 = Daytime running lights 10 = On 11 = Brights
38	Turn Signal/Hazard Signal	00 = Off 01 = Left turn signal 10 = Right turn signal 11 = Hazard signal
38	Traction Control State	00 = Not equipped 01 = Off 10 = On 11 = Engaged
38	Anti-Lock Brake State	00 = Not equipped 01 = Off 10 = On 11 = Engaged
39	System Health	0000 = No faults detected 0001 = Specific error codes … 1111 = "

3.2.3 RSU Traffic Signal Message

Figure 3-5 and Figure 3-6 illustrate the VSCC defined RSU Traffic Signal Message format that will be used as the RSU message. All signed values are two's complement unless otherwise noted. The figure also lists the source of the data that the T9App will use to populate the message fields. Table 3-3 provides definitions for fields with discrete integer values.

Byte \ Bit	8	7	6	5	4	3	2	1(lsb)	SOURCE
1	Message Type								Set to 1
2	Temporary ID MSByte								WRM MAC Address
3	Temporary ID...								
4	Temporary ID...								
5	Temporary ID...								
6	Temporary ID...								
7	Temporary ID LSByte								
8	Precision Indicator (Meaning TBD)								Set to 0
9	Longitude of RSU GPS Antenna MSByte								GPS, GPGGA or GUI
10	"								
11	"								
12	Longitude LSByte (LSBit = 10^{-7} decimal degrees; signed)								
13	Latitude of RSU GPS Antenna MSByte								GPS, GPGGA or GUI
14	"								
15	"								
16	Latitude LSByte (LSBit = 10^{-7} decimal degrees; signed)								
17	Altitude of RSU GPS Antenna MSByte								GPS, GPGGA or GUI
18	Altitude LSByte (LSBit = 1 cm; unsigned; offset by +1 km)								
19	Unused				Altitude LSNybble				
20	UTC Time MSByte								GPS, GPZDA or GPRMC
21									0 if no GPS
22	Number of milliseconds since Jan. 1, 2004 at 00:00:00								
23									
24	UTC Time LSByte (LSBit = 0.001 seconds)								
25	Longitude of Stopping Location #1 MSByte								GUI
26	"								
27	"								
28	Longitude LSByte (LSBit = 10^{-7} decimal degrees; signed)								
29	Latitude of Stopping Location #1 MSByte								GUI
30	"								
31	"								
32	Latitude LSByte (LSBit = 10^{-7} decimal degrees; signed)								
33	Altitude of Stopping Location #1 MSByte								GUI
34	Altitude LSByte (LSBit = 1 cm; unsigned; offset by +1 km)								
35	Unused				Altitude LSNybble				
36	Directionality of Stopping Location #1 MSByte								GUI
37	Directionality LSByte (LSBit = 0.01 degrees; signed; 0 degrees = North)								
38	Current State of Traffic Light at Stopping Location #1								Traffic Signal
39	Time Left in Current State of Traffic Light at Stopping Location #1 MSByte								Traffic Signal
40	Time Left LSByte (LSBit = 0.001 seconds) (This field is invalid if current state is red.)								
41	Duration of Yellow State at Stopping Location #1 MSByte								GUI
42	Yellow State Duration LSByte (LSBit = 0.001 seconds)								
43	Longitude of Stopping Location #2 MSByte								GUI
44	"								
45	"								
46	Longitude LSByte (LSBit = 10^{-7} decimal degrees; signed)								
47	Latitude of Stopping Location #2 MSByte								GUI
48	"								
49	"								
50	Latitude LSByte (LSBit = 10^{-7} decimal degrees; signed)								

Figure 3-5. RSU Traffic Signal Message Format (Part 1 of 2)

51	Altitude of Stopping Location #2 MSByte	GUI
52	Altitude LSByte (LSBit = 1 cm; unsigned; offset by +1 km)	
53	Unused / Altitude LSNybble	
54	Directionality of Stopping Location #2 MSByte	GUI
55	Directionality LSByte (LSBit = 0.01 degrees; signed; 0 degrees = North)	
56	Current State of Traffic Light at Stopping Location #2 (See Below)	Traffic Signal
57	Time Left in Current State of Traffic Light at Stopping Location #2 MSByte	Traffic Signal
58	Time Left LSByte (LSBit = 0.001 seconds) (This field is invalid if current state is red.)	
59	Duration of Yellow State at Stopping Location #2 MSByte	GUI
60	Yellow State Duration LSByte (LSBit = 0.001 seconds)	
61	Longitude of Stopping Location #3 MSByte	GUI
62	"	
63	"	
64	Longitude LSByte (LSBit = 10^{-7} decimal degrees; signed)	
65	Latitude of Stopping Location #3 MSByte	GUI
66	"	
67	"	
68	Latitude LSByte (LSBit = 10^{-7} decimal degrees; signed)	
69	Altitude of Stopping Location #3 MSByte	GUI
70	Altitude LSByte (LSBit = 1 cm; unsigned; offset by +1 km)	
71	Unused / Altitude LSNybble	
72	Directionality of Stopping Location #3 MSByte	GUI
73	Directionality LSByte (LSBit = 0.01 degrees; signed; 0 degrees = North)	
74	Current State of Traffic Light at Stopping Location #3 (See Below)	Traffic Signal
75	Time Left in Current State of Traffic Light at Stopping Location #3 MSByte	Traffic Signal
76	Time Left LSByte (LSBit = 0.001 seconds) (This field is invalid if current state is red.)	
77	Duration of Yellow State at Stopping Location #3 MSByte	GUI
78	Yellow State Duration LSByte (LSBit = 0.001 seconds)	
79	Longitude of Stopping Location #4 MSByte	GUI
80	"	
81	"	
82	Longitude LSByte (LSBit = 10^{-7} decimal degrees; signed)	
83	Latitude of Stopping Location #4 MSByte	GUI
84	"	
85	"	
86	Latitude LSByte (LSBit = 10^{-7} decimal degrees; signed)	
87	Altitude of Stopping Location #4 MSByte	GUI
88	Altitude LSByte (LSBit = 1 cm; unsigned; offset by +1 km)	
89	Unused / Altitude LSNybble	
90	Directionality of Stopping Location #4 MSByte	GUI
91	Directionality LSByte (LSBit = 0.01 degrees; signed; 0 degrees = North)	
92	Current State of Traffic Light at Stopping Location #4 (See Below)	Traffic Signal
93	Time Left in Current State of Traffic Light at Stopping Location #4 MSByte	Traffic Signal
94	Time Left LSByte (LSBit = 0.001 seconds) (This field is invalid if current state is red.)	
95	Duration of Yellow State at Stopping Location #4 MSByte	GUI
96	Yellow State Duration LSByte (LSBit = 0.001 seconds)	

Figure 3-6. RSU Traffic Signal Message Format (Part 2 of 2)

Table 3-3. RSU Traffic Signal Message Discrete Field Definitions

Byte	Field Name	Description
36, 56, 74, and 92	Current State of Traffic Light	0 = Green 2 = Yellow 3 = Red

4 Testing System Specification and Architecture

4.1 Introduction

This chapter provides the Software Design Document for the Wireless Access in Vehicular Environments (WAVE) application developed in accordance with the requirements in Chapter 2.

4.1.1 Scope

This section describes the architecture, classes, data structures, and design goals of the Task 9 Application (T9App). It also provides the guidance for implementing future enhancements.

4.2 Architecture

4.2.1 Overview

Figure 4-1 illustrates the T9App architecture. The T9App consists of the WAVETest.exe, the WaveAPI.DLL and the PCAN_USB.DLL. Denso developed the software for the WAVETest.exe and WaveAPI.DLL. Grid Connect supplied the PCAN_USB.DLL with their USB Controller Area Network (CAN) adapter.

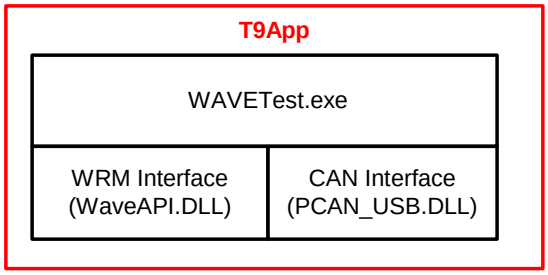


Figure 4-1. T9App Architecture

4.2.2 External Interfaces

Figure 4-2 illustrates the T9App external interfaces. The T9App interfaces to a GPS receiver, a vehicle bus (OBU only), a traffic signal (RSU only), and the Wave Radio Module (WRM). The subparagraphs below describe the software supporting each of these interfaces.

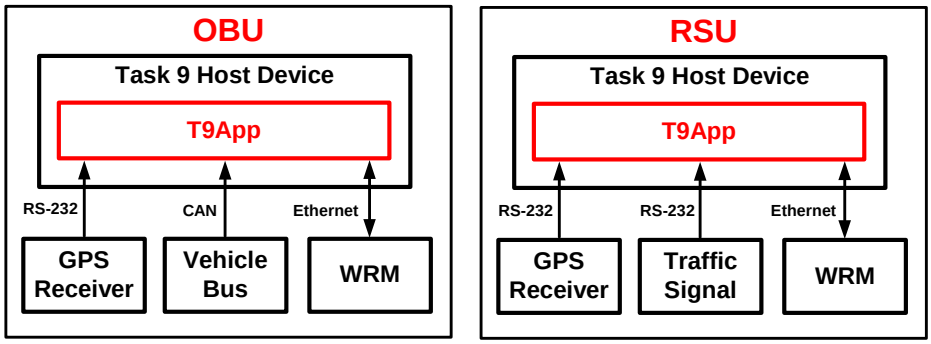


Figure 4-2. T9App External Interfaces

4.2.2.1 GPS/Traffic Signal Interface

The T9App interfaces to the GPS and Traffic Signal using the standard Microsoft Windows serial port drivers.

4.2.2.2 Vehicle Bus Interface

The T9App interfaces to the vehicle bus using the PCAN_USB.DLL supplied by Grid Connect. The Task 9 Host Device (HD) must also have the Grid Connect PCAN_USB.SYS driver installed.

4.2.2.3 WRM Interface

The T9App interfaces to the WRM using the WaveAPI.DLL originally developed for VSCC under Task 6D.

4.2.3 User Interface

4.2.3.1 Screen Shots

The T9App User Interface is a collection of configuration dialogs and a real time Test Display dialog screen. See Figure 4-3 for screen shots of the configuration dialogs and Figure 4-4 for the Test Display dialog.

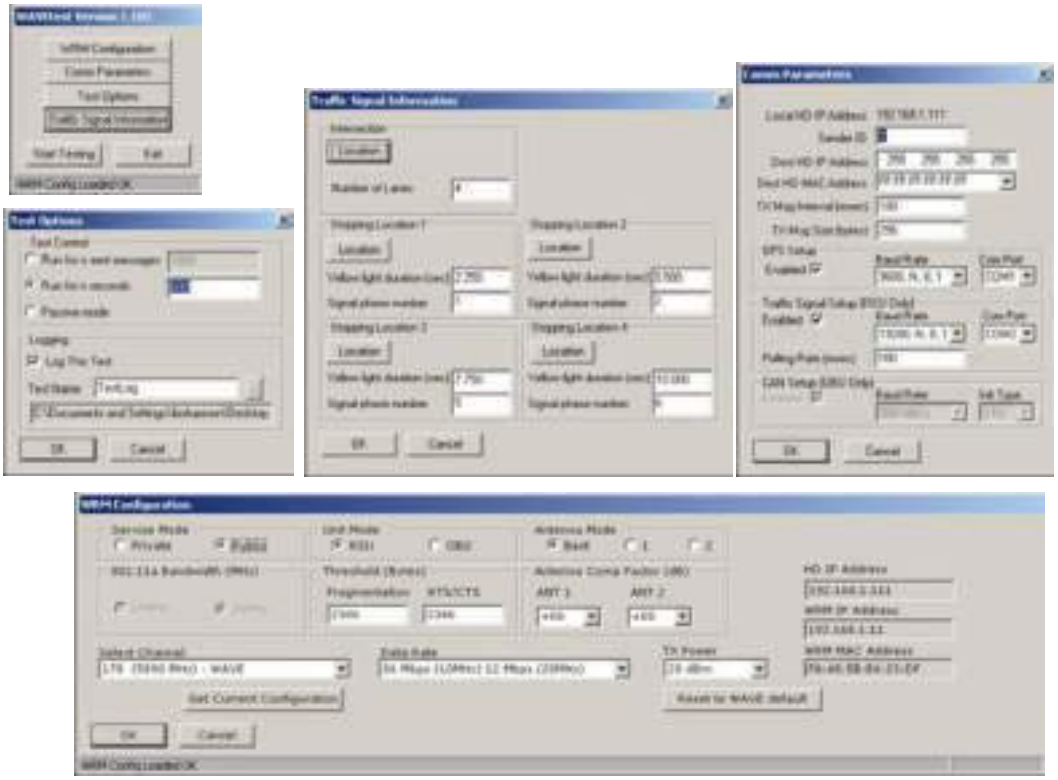


Figure 4-3. Configuration Dialogs Screen Shots

Figure 4-4. Test Display Dialog Screen Shot

4.2.3.2 T9App Dialog to Class Relationships

Table 4-1 summarizes the classes for the main application and the dialogs. For all dialogs, a Microsoft Foundation Class (MFC) based GUI class controls the display, data entry, and range checking. For configuration dialogs, a second information class (generic class type) stores the data in a portable manner.

Table 4-1. T9App Dialog Class Summary

Dialog/App	GUI Class	Information Class
Main Windows App	CWaveTestApp	N/A
Main Dialog	CWaveTestDlg	N/A
WRM Configuration Dialog	CVSCCGUIDlg	CWrmControl
Comm Parameters Dialog	CCommParamDialog	CCommParams
Test Options Dialog	CTestOptionsGui	CTestOptions
Traffic Signal Information Dialog	CRsuParamtersDialog	CSignalInfo
Location Information Dialog	CLocationDialog	CLocationInfo
Test Display Dialog	CTestStatusDialog	N/A

4.2.4 Test Control

4.2.4.1 Class Architecture

The CTestStatusDialog class controls test execution. Figure 4-5 illustrates the high level architecture in a Unified Modeling Language (UML) format (see www.uml.org for more information). The CTestStatusDialog class owns control classes for each hardware interface (i.e., CGpsControl, CSignalControl, CWrmControl, and CCanControl). The CSerialPort class manages the serial ports for the GPS and Traffic Signal interfaces.

The ThisDevice object maintains local device information and the CDeviceDB class maintains OBU or RSU message data received from each unique sender ID. The CTestLog class writes the test log.

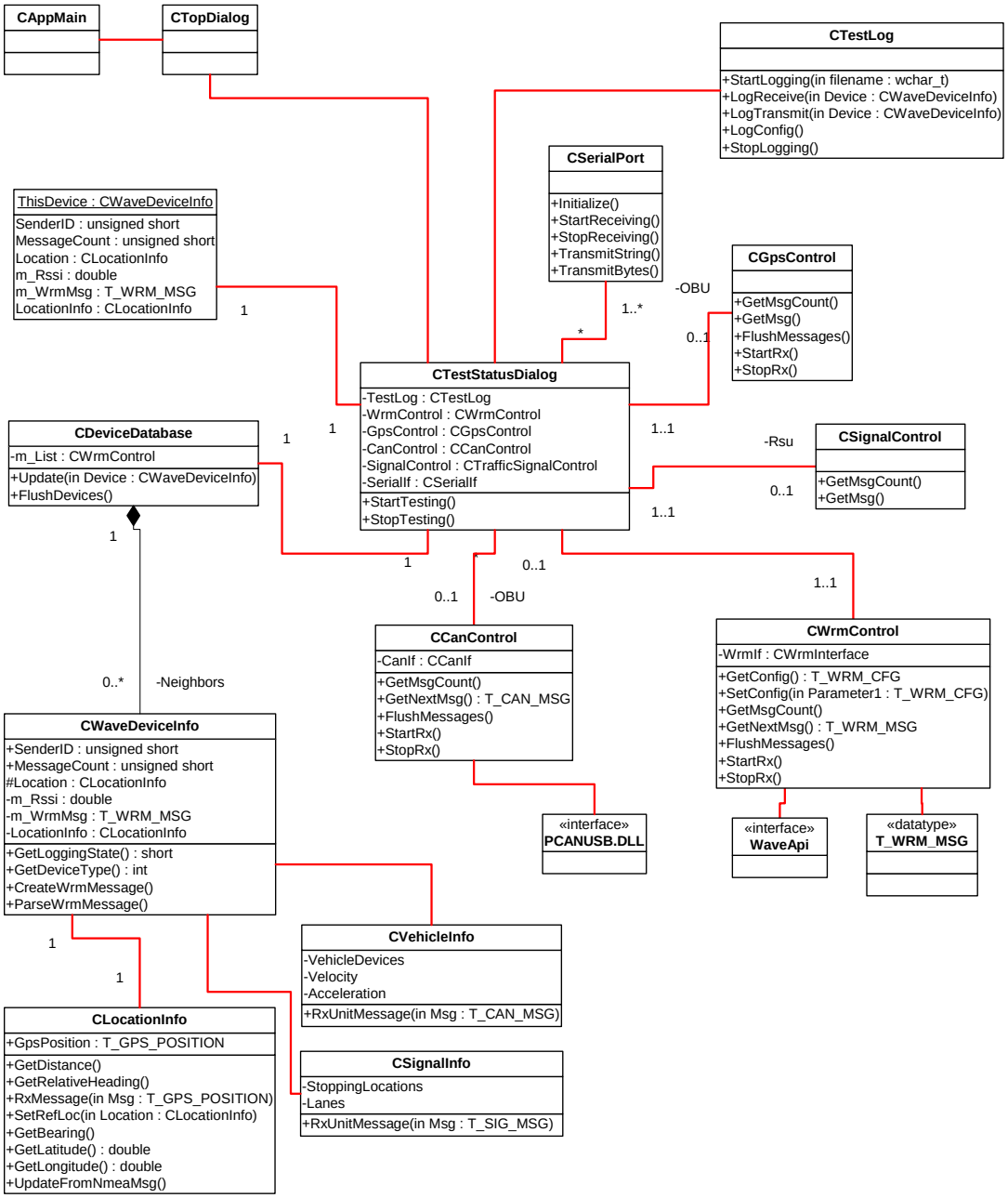


Figure 4-5. T9App Test Execution Architecture (UML Diagram)

4.2.4.2 Test Processing

The CTestStatusDialog object maintains three timers, a Tx Message Interval Timer, a Screen Refresh Timer, and an optional Traffic Signal Service Timer. The T9App sets the Tx Message Interval Timer to the user-entered value on the Comm Parameters screen. The Screen Refresh Timer is always set to one second. The T9App sets the Traffic Signal Service Timer to the user-entered value on the Comm Parameters screen.

Upon expiration of the Tx Message Interval Timer, the CTestStatusDialog object processes all of the messages received from the GPS and Vehicle Bus since the last timer expiration. It formats the OBU or RSU message from the latest information and sends the message to the WRM for transmission and to the CTestLog object for logging. It also processes all messages received from the WRM. It sends the data along with the required reception parameters (e.g., RSSI, timestamp) to the CDeviceDatabase object for entry in the database and to the CTestLog object for logging.

Upon expiration of the Screen Refresh Timer, the T9App queries the CDeviceDatabase and updates the Test Display dialog with the latest information received from remote devices, in order of first unit to the last. The T9App also updates the local device information and current testing statistics.

Upon expiration of the Traffic Signal Service Timer, the T9App sends out its periodic refresh message and updates its traffic signal information with all messages received since the last timer expiration.

The timer processing continues until the user-defined test completion criteria is met, or until the user presses the quit button.

4.3 Class Descriptions

Table 4-2. T9App Class Summary lists the classes used for test execution along with their type and purpose. The class types are control, container, and processing. Some classes are both container and processing. Control classes abstract an underlying API and provide a C++ interface for the T9App architecture. Container classes provide wrapper functions for getting and setting various T9App data stores and messages. Processing classes use a combination of control and/or container classes to implement application functionality and features.

Table 4-2. T9App Class Summary

Class	Class Type	Purpose
CCanControl	Control	Uses PCANUSB.DLL to read messages from CAN bus, queues CAN messages for processing.
CCanMsg	Container	Wraps CAN messages received from CAN I/F.
CCommParams	Container	Holds communication related test parameters.
CDeviceDatabase	Container	Holds list of remote devices from which messages were received during a test run.
CGpsControl	Control	Reads and queues GPS NMEA messages.
CGpsPosition	Container	Wraps and parses NMEA message data.
CLocationInfo	Container/Processing	Performs navigation calculations and data store for location related information.

Class	Class Type	Purpose
CSerialPort	Processing	Provides a C++ wrapper for the Microsoft Standard Serial Port Library, and provides a thread based event handler w/ dispatch. The GPS and Traffic Signal Control modules use this class.
CSignalControl	Control	Reads / polls and queues traffic signal messages.
CSignalInfo	Container	Holds traffic signal stopping location and current state information.
CTestLog	Processing	Logs all transmitted and received data.
CTestOptions	Container	Holds test options related parameters.
CTestStatusDialog	Main Control / Processing	Runs test case and displays test status.
CVehicleInfo	Container	Holds all vehicle related information.
CWaveDeviceInfo	Container	Provides master container for all WAVE device information, OBU and RSU. Also holds generic WAVE device information, not specific to RSU or OBU.
CWrmControl	Control	Reads/queues and transmits WRM messages.
CWrmMsg	Container/Processing	Provides generic wrapper for transmitting WRM messages, also provides parsing and encoding functions for over the air formats.

4.3.1 Class Descriptions

The following subparagraphs summarize each T9App class, and describe each class's public methods and attributes.

4.3.1.1 Class CCanControl

The CCanControl class encapsulates the CAN USB interface. It starts a receive processing thread, and buffers CAN messages in real time for deferred processing. See Table 4-3 for details.

Table 4-3. CCanControl Methods and Attributes

Method/Attribute	Description
unsigned int GetCanBusPollingInterval();	Returns value of the CanBusPollingInterval.
CCanMsg& GetNextRx();	Retrieves the head of the message list. If the list is empty, the results are undefined.
int GetRxCount();	Returns message count of CAN message list.
int Init(int CanBaud, int CanFrame);	Attempts to initialize CAN Interface via the PCAN_USB DLL. Returns error codes if unable to load or initialize DLL.
BOOL InitRxThread();	Creates and starts execution of thread to check for and receive CAN messages from PCAN_USB.DLL. Places received messages into the message list.
SetCanBusPollingInterval(unsigned int interval);	Sets the interval to check the CAN bus status.
StopRxThread();	Stops the receive thread; preserves all unprocessed CAN messages in the queue.
BOOL m_Initialized;	Tracks current init state of underlying CAN Interface DLL.

4.3.1.2 Class CCanMsg

The CCanMsg class encapsulates a Rx CAN message. It parses all supported CAN messages (currently 3), and fills out a preconfigured CVehicleInfo object when the Update () method is called. See Table 4-4 for details.

Table 4-4. CCanMsg Methods and Attributes

Method/Attribute	Description
TPCANMsg* GetRxPacket()	Gets next CAN message.
SetTheVehicle(CVehicleInfo* Vehicle)	Sets the vehicle object that will be accessed when the UpdateVehicle method is called to parse the CAN Messages.
UpdateVehicle	Parses the privately held CAN message and calls the appropriate set methods in the preconfigured Vehicle object for each data item read from the CAN message.

4.3.1.3 Class CCommParams

The CCommParams class owns the communication parameters for the T9App. The config dialogs access the members of this class pre-test, and the test status dialog uses this class to set up the test run. See Table 4-5 for details.

Table 4-5. CCommParams Methods and Attributes

Method/Attribute	Description
BYTE* GetDestMacAddress(); SetDestMacAddress(BYTE a1,BYTE a2, BYTE a3, BYTE a4, BYTE a5,BYTE a6);	Gets or sets Destination MAC address.
friend ostream &operator<<(ostream&, const CCommParams&); friend istream &operator>>(istream&, CCommParams&); PrintHeaders(ostream &output); bool ConfigLoaded();	These methods support saving, loading, and logging of the configuration.
USHORT GetTrafficSignalPollRate(); SetTrafficSignalPollRate(USHORT rate);	Gets traffic signal polling rate.
SetHostIpAddress(BYTE a1, BYTE a2, BYTE a3, BYTE a4); GetHostIpAddress(BYTE *a1, BYTE *a2, BYTE *a3, BYTE *a4); CString& GetHostIpAddressString();	Sets and gets the Host IP Address parameters – the T9App automatically gets the IP address from the OS.
SetDestIpAddress(unsigned long); GetDestIpAddress(BYTE*a1, BYTE *a2, BYTE *a3, BYTE *a4); GetDestIpAddress(BYTE* address); unsigned long GetDestIpAddress(); CString& GetDestIpAddressString();	Sets and gets the Destination IP address.

unsigned short GetSenderId();
int SetSenderId(CString& val);
SetSenderId(USHORT val);
CString& GetSenderIdString();
	Gets and sets the Sender ID for the over the air message header.

int GetMessageRateMsec();
int SetMessageRateMsec(CString& val);
SetMessageRateMsec(int val);
CString& GetMessageRateMsecString();
	Gets and sets the rate at which messages are sent over the air.

int SetMessageSize(CString& val); SetMessageSize(int val); CString& GetMessageSizeString();	Sets the minimum over the air message size. The T9App automatically increases this value to the actual message size if it is too low.
ResetDefaults();	Resets all values to defaults.

Method/Attribute	Description
unsigned int m_CanBaudIndex; unsigned int m_CanInitType; BOOL m_CanEnabled;	CAN I/F initialization parameters.
unsigned int m_GpsBaudIndex; unsigned int m_GpsPort; BOOL m_GpsEnabled;	GPS Serial Port initialization parameters.
unsigned int m_TrafficSignalBaudIndex; unsigned int m_TrafficSignalPort; BOOL m_TrafficSignalEnabled; USHORT m_TrafficSignalPollRate;	Traffic Signal initialization parameters.

4.3.1.4 Class CDeviceDatabase

The CDeviceDatabase class maintains an up-to-date list of all remote WAVE devices from which messages were received. This class contains 2 CLists, 1 for OBUs and 1 for RSUs. See Table 4-6 for details.

Table 4-6. CDeviceDatabase Methods and Attributes

Method/Attribute	Description
ResetDatabase()	Iterates thru OBU and RSU lists and removes each item.
CList<CWaveDeviceInfo, CWaveDeviceInfo&> m_RsuList; CList<CWaveDeviceInfo, CWaveDeviceInfo&> m_ObuList;	CList Template, holds a list of references to OBU/ RSU class WAVE devices
void UpdateRemoteDevice(CWaveDeviceInfo& NewDevice);	Updates the remote device list by adding the device or updating the data. This function is called each time an over the air message is received and successfully parsed into a new CWaveDeviceInfo object.

4.3.1.5 Class CGpsControl

The CGPSControl class processes National Maritime Electronics Association (NMEA) format messages from a GPS device plugged into a local configurable serial port. The CTestStatusDialog (CDialog) object owns the serial port class, due to serial class implementation. The CTestStatusDialog forwards all messages from the serial port to this class for actual processing. See Table 4-7 for details.

Table 4-7. CGpsControl Methods and Attributes

Method/Attribute	Description
BOOL Initialize(CWnd* pPortOwner, int port, int baudindex);	Called by the object owner to attempt to initialize the serial port, returns FALSE if initialization fails.
OnCommunication, OnErrDetected, OnRxFlagDetected	Called by TestStatusDialog when rx char, error, or rxflag event is received.
void ProcessMessages();	Processes the first message the GPS Control class may have in its list.
Void SetLocalDevice(CWaveDeviceInfo *Device);	Sets the device to be updated when the NMEA messages are parsed. .
StartRxThread();	Starts the serial ports receive thread, if the serial port initialized without error.
StopRxThread();	Stops the serial ports receive thread, used when testing is paused or terminated.
CSerialPort* m_Serial;	Pointer to serial object controlled by this class.

4.3.1.6 Class CGpsPosition

The CGpsPosition class represents a decoded GPS position, and provides methods to decode NMEA messages into a GPS position. Each local WAVE device's ClocationInfo will have a corresponding CGpsPosition object. See Table 4-8 for details.

Table 4-8. CGpsPosition Methods and Attributes

Method/Attribute	Description
UpdateFromNmeaMsg(CString &data);	Given the NMEA message in a string, this method fills out the details of the GPS Position and sets the appropriate m_Received_XXX flags.
double m_Heading;	GPS Heading.
BOOL m_Received_GGA;	Holds flag that is set to true if this object processed a NMEA GPGGA message. Note more than one received flag may be set during life of this object.
BOOL m_Received_RMC;	Holds flag that is set to true if this object processed a NMEA GPRMC message. Note more than one received flag may be set during life of this object.
BOOL m_Received_VTG;	Holds flag that is sets to true if this object processed a NMEA GPVTG message. Note more than one received flag may be set during life of this object.

Method/Attribute	Description
BOOL m_Received_ZDA;	Set to true if this object processed a NMEA GPZDA message. Note more than one received flag may be set during life of this object.
double m_utc;	Parsed UTC Time in fixed point format: Hhmmss.ss
double m_latitude;	Parsed Latitude of position, ddmm.mmm
char m_latNS;	Parsed Latitude North/South qualifier. Either ‘N’ or ‘S’
double m_longitude;	Parsed Longitude of position, ddmm.mmm
char m_longEW;	Parsed Longitude east/west qualifier. Either ‘E’ or ‘W’
int m_fixQual;	Parsed fix quality.
int m_sats;	Parsed number of satellites in view
double m_hdop;	Parsed relative accuracy of horizontal position.
double m_altitude;	Parsed units above mean sea level.
char m_altUnits;	Parsed units qualifier for altitude. ‘M’ for meters.
double m_hogae;	Parsed height of geoid above WGS84 ellipsoid (HOGAE) in meters.
char m_hogUnits;	Parsed units qualifier for HOGAE. ‘M’ for meters, this is the units for the m_hogae
char m_csum[1];	Parsed NMEA checksum used by program to check for GPS transmission errors. Not currently implemented.
CString m_utctime;	UTC Time in String format.
int m_month, m_day, m_year;	Parsed UTC month, day, and year.
int m_hours, m_minutes, m_seconds, m_hundreths;	Parsed UTC hours, minutes, seconds, and hundredths.

4.3.1.7 Class CLocationInfo

The CLocationInfo class owns a GPS position and provides navigational calculations and formatting retrieval methods for working with location information. See Table 4-9 for details.

Table 4-9. CLocationInfo Methods and Attributes

Method/Attribute	Description
unsigned char GetAltitudeLsb();	Gets LSB part of Altitude for the over the air message.
unsigned short GetAltitudeMsb();	Gets MSB part of Altitude for the over the air message.
CString& GetAltitudeStr();	Gets Altitude.
Double GetBearing(CLocationInfo& Destination);	Computes the initial bearing from the local location to the given destination.

Method/Attribute	Description
CString& GetBearingString(CLocationInfo& Destination);	Returns the initial bearing in a formatted string, suitable for GUI display or logging.
CString& GetFormattedLatStr(); double GetLatitude();	Latitude access methods. Floating point, string.
CString& GetFormattedLongStr(); double GetLongitude();	Longitude access methods, floating point, string. Etc.
DWORD GetGpsSecondsInWeek();	Returns pre-computed GPS seconds in week. Returns zero if GPS messages containing this information haven't been received yet.
signed short GetHeadingInt();	Returns Heading in signed integer format, suitable for over the air transmission.
CString& GetHeadingStr(); unsigned short GetHeadingUINT();	Heading access methods of various combinations.
unsigned char GetPrecision();	Returns the precision of the OS timestamp.
double GetRelativeDistance(location) CString& GetRelDistanceStr(location)	Computes distance from object to given location.
double GetRelativeHeading(CLocationInfo& Location) CString& GetRelHeadingStr(CLocationInfo& Location)	Computes and returns relative heading from object to given location in different formats.

GetUTCTimeSinceJan12004(PTIME_MSEC Value);
unsigned char GetUTCTimeSinceJan12004Lsb();
unsigned long GetUTCTimeSinceJan12004Msb();
	Returns the number of milliseconds that have elapsed since UTC Time January 1st, 2004. This method uses the current UTC time retrieved from GPS receiver as the starting point. If UTC time has not been received from the GPS yet, or if the GPS is not enabled, this function returns 0 values in the TIME_MSEC structure.

PrintHeaders(ostream &output);	Outputs to stream the field labels for each element that the overloaded input and output functions read/write.
PrintHeaders(ostream &output, CString prefix);	Outputs to stream the field labels with an optional prefix for each element that the overloaded input and output functions read/write.
ResetLocationDefaults();	Resets all run-time values to zero.
SetAltitude(unsigned short msb, unsigned char lsb);	Sets Altitude.
void SetAltitude(double alt);	Sets Altitude.
int SetAltitudeStr(CString &val);	Sets Altitude.

Method/Attribute	Description
SetGpsSecondsInWeek(DWORD Seconds);	Sets GPS seconds in week..
SetHeading(double Heading); SetHeading(signed short Heading); int SetHeadingStr(CString& heading);	Sets Heading.
int SetLatitude(CString &val); SetLatitude(double val);	Sets Latitude.
int SetLongitude(CString &val); SetLongitude(double val);	Sets Longitude.
SetPrecision(unsigned char Precision);	Sets the precision of the OS timestamp.
SetUtcTimeSinceJan12004(TIME_MSEC time);	Sets UTC time from the over the message.
UpdateLocationFromGpsPosition(CString& NmeaMsg);	Updates the location from information in the NMEA message.
friend ostream &operator<<(ostream&, const CLocationInfo&);	Writes the current values of the member data to the given ostream, used for logging configuration and saving configuration.
friend istream &operator>>(istream&, CLocationInfo&);	Reads member data from the given input stream. Used to read application configuration from disk.

4.3.1.8 Class CSerialPort

The CSerialPort class encapsulates the Microsoft serial port interface with a C++ methods and a threaded state machine for handling simultaneous transmit and receive. The GPS control class and the traffic signal control class use this class. The T9App configures the serial interfaces to send all events to the CTestStatusDialog window. When the CTestStatusDialog receives events, it forwards them to the appropriate control class depending on how the user configured the serial ports. For example, if the user configured COM1 for GPS, the CTestStatusDialog forwards all COM1 port event messages to the GPS control class. See Table 4-10 for details.

Table 4-10. CSerialPort Class Methods and Attributes

Method/Attribute	Description
GetCommEvents();	Returns the configured communications event masks.
GetDCB();	Returns the device control block created at initialization.
GetWriteBufferSize();	Returns write buffer size that was specified in InitPort() call.
InitPort(PortOwner, portnr, baud, parity, databits,, stopsbits = 1, dwCommEvents, nBufferSize)	Opens the specified serial port with the specified baud rate, parity, stop bits, and tx buffer sizes.
KillThread();	Kills the comm. Port receive thread.
RestartMonitoring();	Stops and re-starts comm. port receive thread.
StartMonitoring();	Starts serial port receive thread.
StopMonitoring();	Pauses the serial port receive thread, doesn't kill it.
WriteToPort(char* string);	Adds the specified character string to the tx queue and begins transmission.
WriteToPort(unsigned char* string, unsigned int len);	Adds the specified byte buffer to the tx queue begins transmission.

4.3.1.9 Class CSignalControl

Methods and Attributes

The CSignalControl class controls a traffic signal plugged into the serial port this object has been given a reference to. See Table 4-11 for details.

Table 4-11. CSignalControl Methods and Attributes

Method/Attribute	Description
USHORT GetPollingRate();	Returns current traffic signal polling rate in milliseconds.
BOOL Initialize(CWnd *pPortOwner, int port, int baudindex);	Initializes serial port according to the given parameters. Returns false if init failed.
SetPollingRate(USHORT rate);	Sets traffic signal polling interval in milliseconds.
StartRxThread();	Starts receive thread if it isn't already running.

Method/Attribute	Description
void StateMachine(enum TS_EVENT Event, void *data);	Traffic Signal state machine entry point. When the traffic signal interface is enabled, the state machine must be clocked by calling this function a tick event parameter and tick interval value as a data. When serial data is received, this function must be called with TSE_RX_DATA event, and a character in data portion.
StopRxThread();	Stops the receive thread if it is running.
TransmitPeriodicRequest();	Transmits poll message to traffic signal.
CSerialPort* m_Serial;	Serial port this object controls.

State Machine

The CSignalControl implements the Traffic Signal Interface with a simple state machine. The state machine implements the initialization sequence in accordance with the timing requirements. Table 4-12 lists the events processed by state machine and describes each event.

Table 4-12. CSignalControl State Machine Events

Event	Description
TSE_NONE	No event.
TSE_INIT_OK	Initialization sequence succeeded.
TSE_RX_DATA	Serial port has received a character.
TSE_TX_DATA	Serial port TX has completed.
TSE_RX_FLAG	Serial port RX flag indicated.
TSE_ERROR	Serial port error indicated.
TSE_CTS	Serial port clear to send indication.
TSE_TICK	Owner is indicating that time has elapsed.
TSE_PROCESS	Indicates queued messages should be processed.
TSE_SHUTDOWN	Owner is shutting down.

4.3.1.10 Class CSignalInfo

The CSignalInfo class contains the traffic signal information. The CWaveDeviceInfo owns this object which contains valid data for a RSU. See Table 4-13 for details.

Table 4-13. CSignalInfo Methods and Attributes

Method/Attribute	Description

unsigned short GetDurationOfYellowLightMsec(int signal);
unsigned short GetSignalPhaseNumber(int signal);
unsigned char GetSignalState(int signal);
unsigned short GetSignalStateTimeLeftMsec(int signal);
	Obtain signal information from over the air messages.

CString& GetLanesString();	Gets the number of lanes in a string format.
friend ostream &operator<<(ostream&, const CSignalInfo&); friend istream &operator>>(istream&, CSignalInfo&); PrintHeaders(ostream &output);	Writes T9App configuration to disk or to test log.
ResetSignalDefaults();	Sets all signals to red state and time left to 0.
int SetLanes(CString &lanes);	Set the number of lanes.
SetSignalState(int Phase, SIGNAL_STATE State, int SecondsLeft);	Set current signal state of a remote RSU.

unsigned char GetSignalState(int signal);
unsigned short GetSignalStateTimeLeftMsec(int signal);
unsigned short GetSignalPhaseNumber(int signal);
unsigned short GetDurationOfYellowLightMsec(int signal);
	Obtain signal information from over the air messages.

unsigned short m_SignalPhaseNumber[MAX_SIGNALS];	Configured phase number for each signal.
SIGNAL_STATE m_SignalState[MAX_SIGNALS];	Traffic light state for each signal.
unsigned short m_SignalStateTimeRemainingMsec[MAX_SIGNALS];	Configured time remaining for each signal.
CLocationInfo m_StoppingLocation[MAX_SIGNALS];	Coordinates of stopping locations.
unsigned short m_YellowLightDurationMsec[MAX_SIGNALS];	Yellow light duration for each signal

4.3.1.11 Class CTestLog

The CTestLog class writes entries to the log. It is implemented with the ANSI streams library. See Table 4-14 for details.

Table 4-14. CTestLog Methods and Attributes

Method/Attribute	Description
void LogReceive(CWrmMsg& msg, CWaveDeviceInfo& receiver);	Logs a receive entry. The function parses the message into a CWaveDeviceInfo object, queries the object values, and logs them to the current stream. The receiver information is a required parameter to enable logging of reception information.
LogTestParameters(CcommParams, CTestOptions, CwaveDeviceInfo, CwrmControl)	Writes T9App configurable parameters to current test log file.
void LogTransmit(CWrmMsg& msg);	Logs a transmit entry. The function reparses the message back into a CWaveDeviceInfo object, queries the sent values, and logs them to the current stream.
int StartLogging(CString TestName, CString Path, CString GpsDate, int pass);	Creates a candidate filename from a test name, file path, and pass number. Tries to open that filename read-only. If that filename exists, the function increments pass number and tries again until the test log filename is unique. Next, the test log filename is opened for writing and the final pass number is returned to calling function.
StopLogging();	Closes log file, forcing it to be written to disk.

4.3.1.12 Class CTestStatusDialog

Methods

Section 4.2.4 describes the CTestStatusDialog class. See Table 4-15 for the method description.

Table 4-15. CTestStatusDialog Methods and Attributes

Method/Attribute	Description
SetCommParams(CCommParams &Params);	Sets pointer to communication parameters object owned by Test App.
SetLocalDevice(CwaveDeviceInfo)	Sets local CWaveDeviceInfo information to be used for each test pass.
SetTestOptions(CTestOptions &TestOptions);	Sets pointer to test options configuration object owned by Test App.
SetWrmControl(CWrmControl *WrmControl);	Sets pointer to WRM control object owned by Test App.

Processes

Table 4-16 lists all of the threads and timers that the CTestStatusDialog class owns. The CTestStatusDialog uses timers to meet the processing requirements. The threads enable the test display to update without slowing down data events for other functions. The CTestStatusDialog starts and stops the threads and timers for each test pass.

Table 4-16. CTestStatusDialog Processes

Process Name	Purpose	Type
CcanControl.Rx_thread	Checks for the presence of a CAN message. Queues any messages into CcanControl's message list.	Polling Thread. 10 millisecond sleep between polling if CAN bus is idle. Not configurable.
CwrmControl::rx_thread	Checks for and retrieves WRM messages from WaveApi.dll.	Polling Thread. 10msec sleep between polling if WRM is idle. Not configurable.
TestStatusDialog::GpsSerial.rx_thread	Serial event handler/dispatcher.	Event Driven Thread
TestStatusDialog::ProcessMessages	Sends periodic updates. Processes all WRM RX messages, CAN messages, and GPS Messages.	Timer executes at user defined interval.
TestStatusDialog::SignalSerial.rx_thread	Serial event handler/ dispatcher.	Event Driven Thread
TestStatusDialog::StartTesting	Auto starts the first test pass when user clicks Start testing from main dialog.	10-millisecond timer single shot timer, not configurable.
TestStatusDialog::TrafficSignalPolling	Clocks the traffic signal interface state machine.	Timer executes at user defined polling rate
TestStatusDialog::UpdateDisplay	Updates GUI at a regular interval, prevents screen flashing & excessive processor utilization for GUI updates.	1-second timer, not configurable.

4.3.1.13 Class CVehicleInfo

The CVehicleInfo class contains all vehicle information. It obtains local information from the CAN bus and remote information by parsing an OBU Vehicle to Vehicle (V2V) message received over the air. Since the requirements for logging vehicle information and transmitting it over the air are slightly different, 2 methods are provided for each vehicle attribute; one for displaying it or logging to disk, and another to format values for over the air transmission. The CVehicleInfo class also provides two methods for setting values, one to set values from a received OBU message and another to set values from a CAN message (in different formats). See Table 4-17 for details.

Table 4-17. CVehicleInfo Methods and Attributes

Method/Attribute	Description
unsigned char GetBrakeInfo();	Gets the brake-applied status in upper nibble, and brake-applied pressure in lower nibble.
double GetLatAccel(); signed short GetLatAccelShort();	Gets Lateral Acceleration
Double GetLongAccel(), signed short GetLongAccelShort()	Gets Longitudinal Acceleration.
Unsigned char GetSignalAndControlStatus();	Gets: Headlight status in bits 7,6 Turn signal/hazard in bits 5,4 Traction control in bits 3,2 Anti-lock brake state in bits 1,0
double GetSteeringWheelAngle(); Signed short GetSteeringWheelAngleShort();	Gets current steering wheel angle as a signed number from -180.00 to +180.00.
unsigned char GetSystemHealth();	Gets system health bits in the lower nibble.
double GetThrottlePos();	Gets throttle position in same precision as CAN bus message format (0.5%).
unsigned short GetVehicleLength();	Gets 14 bits of vehicle length in cm.
unsigned short GetVehicleWidth();	Gets 10 bits of vehicle width in cm.
Double GetVelocity(), Unsigned int GetVelocityUINT(), CString& GetSpeedStr();	Gets current vehicle speed in meters per seconds.
double GetYawRate(); signed short GetYawRateShort();	Gets vehicle yaw rate in degrees as a signed number. LSB = 0.01 deg/sec.
ResetVehicleDefaults();	Resets all values to starting state valid.
SetBrakeInfo(BYTE BrakeInfo);	Sets the brake-applied status (in upper nibble), and the brake-applied pressure (lower nibble).
SetLatAccel(BYTE msb, BYTE lsb); SetLatAccelmmSec(BYTE msb, BYTE lsb);	"
SetLongAccel(BYTE msb, BYTE lsb); SetLongAccelmmSec(BYTE msb, BYTE lsb);	"

Method/Attribute	Description
SetSignalAndControlStatus(BYTE SignalAndControlStatus);	Sets parameters in OBU VTV message and CAN format: Headlight status in bits 7,6 Turn signal/hazard in bits 5,4 Traction control in bits 3,2 Anti-lock brake state in bits 1,0
SetSteeringWheelAngle(signed short Angle); SetSteeringWheelAngle(double Angle);	"
SetSystemHealth(BYTE SystemHealth);	Sets value from lower nibble.
SetThrottlePos(BYTE ThrottlePos);	Sets throttle position from CAN Message or OBU VTV message
SetVehicleLength(BYTE VehicleLengthMsb,BYTE VehicleLengthLsb);	Currently initialized to zero. Not settable by user or CAN message. Only the over the air message parser calls this function.
SetVehicleWidth(BYTE VehicleWidthMsb,BYTE VehicleWidthLsb);	Currently initialized to zero. Not settable by user or CAN message. Only the over the air message parser calls this function.
SetVelocity(WORD Speed); SetVelocity(BYTE msb, BYTE lsb);	2 functions to support setting this value from either a received CAN message or and OBU VTV message.
SetYawRate(signed short YawRate); SetYawRate(BYTE msb, BYTE lsb);	"
friend ostream &operator<<(ostream&, const CVehicleInfo&);	Logs and saves T9App configuration.
friend istream &operator>>(istream&, CVehicleInfo&);	"

4.3.1.14 Class CWaveDeviceInfo

The CWaveDeviceInfo class contains all information about a WAVE device, either OBU or RSU. This class provides methods to get/set all attributes including some formatting methods suitable for displaying WAVE device info on dialogs. This class has overloaded streams operators so that device information can be read or written from any streams type. This class also contains a static instance of a vehicle and a traffic signal object. This class maintains the current RSSI, Message Counts, Sender ID, and other overhead information required for each WAVE device. Note T9App uses this object for storing information about both local and remote WAVE devices. See Table 4-18 for details.

Table 4-18. CWaveDeviceInfo Methods and Attributes

Method/Attribute	Description
bool ConfigLoaded();	Set to true if a previously saved configuration file containing valid device information was loaded.
int GetDeviceType(); SetDeviceType(int type);	Gets and sets device type (OBU or RSU).
CString& GetLogStateStr(); int GetLoggingState() SetLoggingState(unsigned short val);	Gets and sets the logging state for a device.
unsigned short GetMessageCount(); CString& GetMsgCountStr(); SetMessageCount(unsigned short val);	Gets and sets the message count that is incremented by the sender and sent in the test header of over the air messages.
int GetRssi(); CString& GetRssiStr(); SetRssi(signed short val);	Gets and sets the RSSI for the device's last message.
unsigned short GetSenderId(); CString& GetSenderIdStr(); SetSenderId(unsigned short id);	Gets and sets user configured Sender ID.
unsigned char GetTxPower(); SetTxPower(unsigned char val);	Gets and sets the WRM TX power level.
IncMessageCount();	Increments the message count in case of local device. Not used for remote devices.
bool IsRsu();	Returns true if the object represents an RSU.
bool IsObu();	Returns true if the object represents an OBU.
PrintHeaders(ostream &output, CString prefix); PrintHeaders(ostream &output);	Prints headers when saving configuration or logging WaveDeviceInfo attributes. An optional prefix for custom formatting.
ResetDeviceDefaults();	Sets all values to zero.
friend ostream &operator<<(ostream&, const CWaveDeviceInfo&); friend istream &operator>>(istream&, CWaveDeviceInfo&);	Read/writes this object to a stream. Used for logging configuration to disk during testing & writing configuration to disk.
CLocationInfo m_LocationInfo;	Current GPS Location information for this vehicle or intersection (not stopping locations).
CSignalInfo m_SignalInfo;	If this device is an RSU, this object is the current signal information.

Method/Attribute	Description
CLocationInfo m_TestLocationInfo;	Test header version of our location.
CVehicleInfo m_VehicleInfo;	If this device is an OBU, this object represents the current vehicle information.
BYTE m_WrmMacAddr[2];	MAC Address of the WRM connected to the HD represented by this object.

4.3.1.15 Class CWrmControl

CWrmControl provides WRM transmit and receive capability, with a separate full time receive thread and an internal packet queue. This class also encapsulates a single use of the WAVEApi, to provide one point of control for all T9App dialogs needing access to the local WRM. This is the only object that makes WaveApi calls. See Table 4-19 for details.

Table 4-19. CWrmControl Methods and Attributes

Method/Attribute	Description
bool ConfigLoaded();	Returns whether or not loading configuration from disk file was successful, if false, a configuration file was not found.
int GetConfigFromWrm();	Gets configuration from WRM.
CWrmMsg& GetLastSent();	Gets a copy of the last message that was sent to the WaveApi, used to support logging.
CWrmMsg& GetNextRx();	Gets the oldest message received from the WRM from this object's internal message queue.
int GetRxCount();	Returns received message count.
GetWrmConfig(wrm_configuration_parameters_type *Config);	Gets the local WRM configuration.
bool InitRxThread();	Initializes and starts WRM message receive thread.
PrintHeaders(ostream &output);	Prints field headers for saving and logging this objects configurable attributes.
ResetWrm();	Resets WRM via WAVEAPI
static UINT rx_thread(LPVOID pParam);	Receive thread.
int SaveWrmConfig(wrm_configuration_parameters_type* Config);	Request the given configuration to be saved to WRM, via the WAVEApi
void SendUpdate(CWaveDeviceInfo& device);	Sends packets over the air.

Method/Attribute	Description
SetDestMacAddress(BYTE *Address);	Sets destination MAC address for over the air messages.
SetWrmConfig(wrm_configuration_parameters _type* Config);	Sets this objects internal WRM configuration structure with the passed in one.
StopRxThread();	Stops WRM message receive thread.
friend ostream &operator<<(ostream&, const CWrmControl&);	Saves and logs this object's configurable attributes.
friend istream &operator>>(istream&, CWrmControl&);	Saves and logs this object's configurable attributes.
CString m_DestIpAddress;	Current destination IP address, which is user configurable.

4.3.1.16 Class CWrmMsg

The CWrmMsg class encapsulates a sent or received WRM message. It creates an over the air formatted message from a given CWaveDeviceInfo object, or it creates a CWaveDeviceInfo object from a received over the air message. See Table 4-20 for details.

Table 4-20. CWrmMsg Methods and Attributes

Method/Attribute	Description
int ParseMessage();	Parses a received over the air message of either OBU or RSU format, and creates a valid CWaveDeviceInfo object (accessible with the m_Device attribute) if successful. Return value is the parsed size, a value of –1 indicates an error while parsing.
SetWrmIpAddr(unsigned long IpAddr);	Sets the IP address of the receiver of this message. This value is necessary for making calibration adjustments to the RSSI.
CWaveDeviceInfo m_Device;	A WAVE device info object created by a successful call to ParseMessage().
BYTE m_SourceIpString[20];	For a received CWrmMsg object, this is the sender's IP address, for sends, this value is undefined.
unsigned short m_Length;	Message size, including padding.
ULARGE_INTEGER m_TimeStamp;	For a received CWrmMsg object, this holds the parsed value of the timestamp encoded by the sender of this message. For transmit, this value is not used.

4.4 Data

4.4.1 Structures

This section describes the data structures that are common to T9App classes for control and message processing functions. Where commonality was identified in messages, these common structures were created to eliminate redundancy and reduce code size and processing overhead.

The GPS location structure (Table 4-21) is used in both OBU and RSU messages, and also in the message headers.

Table 4-21. GPS Location Structure

TGPS_LOCATION	
DWORD	Longitude;
DWORD	Latitude;
WORD	AltitudeMsb;
BYTE	AltitudeLsb:4;
BYTE	Reserved:4;

The test header structure (Table 4-22) contains the data that is prepended onto each RSU or OBU message.

Table 4-22. Test Header Structure

T_TEST_HEADER	
BYTE	LengthMsb;
BYTE	LengthLsb:4;
BYTE	GpsTimeMsb:4;
WORD	GpsTimeLsb;
GPS_LOCATION	Location;
WORD	Heading;
WORD	SenderId;
WORD	MessageCount;
BYTE	TxPower:5;
BYTE	LogEnabled:1;
BYTE	Reserved:2;
BYTE	OsTimeHi;
WORD	OsTimeMid;
DWORD	OsTimeLow;

The stopping location structure (Table 4-23) contains the data associated with each stopping location.

Table 4-23. Stopping Location Structure

T_TS_STOPPING_INFO	
GPS_LOCATION	Location;
WORD	Direction;
BYTE	SignalState;
WORD	SignalStateTimeLeft;
WORD	DurationOfYellowLight;

The common message structure contains the fields that are common to both the OBU and RSU message bodies (i.e., fields directly following the message header).

Table 4-24. Common Message Structure

T_COMMON_MSG_HEADER	
BYTE	MessageType;
BYTE	TemporaryId[2];
BYTE	PrecisionIndicator;
GPS_LOCATION	Location;
DWORD	UTCTimeMsb;
BYTE	UTCTimeLsb;

The OBU VTV message structure (Table 4-25) contains the data for the over the air message.

Table 4-25. OBU VTV Message

T_VTV_MSG	
COMMON_MSG_HEADER	CommonHeader;
WORD	Heading;
WORD	Speed;
BYTE	LatAccelMsb;
BYTE	LatAccelLsb:4;
BYTE	LongAccelMsb:4;
BYTE	LongAccelLsb;
WORD	YawRate;
BYTE	ThrottlePos;

T_VTV_MSG	
BYTE	BrakeInfo;
WORD	SteeringWheelAngle;
BYTE	SignalAndControlStatus;
BYTE	SystemHealth:4;
BYTE	Reserved:4;
BYTE	VehicleLengthMsb;
BYTE	VehicleLengthLsb:6;
BYTE	VehicleWidthMsb:2;
BYTE	VehicleWidthLsb;

The RSU TS message structure (Table 4-26) contains the data for the over the air message.

Table 4-26. RSU TS Message

T_TS_MSG	
COMMON_MSG_HEADER	CommonHeader;
TS_STOPPING_INFO	Sl1Info;
TS_STOPPING_INFO	Sl2Info;
TS_STOPPING_INFO	Sl3Info;
TS_STOPPING_INFO	Sl4Info;

4.4.2 Global Variables

This section describes the list of global scope variables and the rationale for their use.

4.4.2.1 T9App Globals

Table 4-27 lists the global variables/functions used by the T9App.

Table 4-27. T9 App Globals

Function	Rationale
Operator <<	Required to support streams overloading cleanly. Many T9App classes define global overloaded functions for streams operation. Since this function is called by methods of the C++ standard lib classes, they need to be global in scope.
Operator >>	"

4.4.2.2 WAVE API Globals

Table 4-28 lists global variables used by the WAVE API Interface implementation.

Table 4-28. WAVE API Globals

Variable	Rationale
AntennaFactorTable	The T9App reused code from the WAVE API Tester. The T9App left the code unchanged for consistency.
MaxTxPowerTable	"
FullInList	"

4.4.2.3 PCAN USB Globals

Table 4-29 lists global variables used by the PCAN USB.

Table 4-29. PCAN USB Globals

Function	Rationale
PCAN_Init g_CAN_Init;	Denso copied the implementation from Grid Connect PCAN example code, which used global scope variables.
PCAN_Close g_CAN_Close;	"
PCAN_Status g_CAN_Status;	"
PCAN_Write g_CAN_Write;	"
PCAN_Read g_CAN_Read;	"
PCAN_VersionInfo g_CAN_VersionInfo;	"
UnloadDLL	"
LoadDLL	"
check_err	"
GetFunctionAdress	"
HINSTANCE g_i_DLL;	"

4.5 Design Goals and Constraints

4.5.1 Design Methodology

The T9App is a 100% object oriented (OO) design, implemented in Microsoft C++.

4.5.2 MFC, Standard Library Usage

The T9App leverages the Microsoft Foundation Classes for its GUI elements, internal lists, strings, and multi-threading support. The T9App uses standard C/C++ libraries whenever possible. The T9App uses standard libraries for string operations, time/date functions, file access, formatting text, and synchronization.

4.5.3 ANSI Compliance

For code that doesn't use MFC support classes, the code is mostly ANSI C++ compliant, with the exception of meeting VSCC requirements that the ANSI C++ standard can't meet (e.g., high-precision timers, logging / displaying of 64bit data types).

4.5.4 Memory Management

The T9App uses automatic memory management to the extent possible. To avoid memory leaks or management problems, all classes were designed to include references to objects or the actual objects statically. Where memory is dynamically allocated, it is encapsulated in objects, and then control of these objects is passed to standard list classes, so the objects will be automatically destroyed under normal program termination.

4.5.5 Naming Conventions

The T9App Member variables, function parameters, and local variables were named to reflect the contents of the data. For example, the variable named m_Width in the *CVehicle* class will contain the width of the vehicle the object describes.

4.6 Modifications and Enhancements

This section provides guidance for making enhancements for some expected scenarios.

4.6.1 Changing Over the Air Formats

The CWrmMsg class performs over the air message creation and parsing. Modify the appropriate message structures, header or body data. These structures are:

4.6.1.1 T_TEST_HEADER

Modify this structure to add or change information in the common message header that is prepended to each over the air message. Modify the CWrmMsg::CreateTestHeader() and CWrmMsg::ParseTestHeader() to support parsing and creation.

4.6.1.2 T_COMMON_MSG_HEADER

Modify this structure to add or change information in the first fields that are identical in the OBU and RSU message (e.g., Message Type, Temporary ID). Modify the CWrmMsg::CreateCommonMsgHeader() and CWrmMsg::ParseCommonHeader() to support the modified fields.

4.6.1.3 T_VTV_MSG

Modify this structure to add or change information in the OBU V2V message. Modify the CWrmMsg::ParseVtvMessage() and CWrmMsg::CreateObuMsgFromDevInfo(). In addition, modifications to the CVehicleInfo member data may be needed.

4.6.1.4 T_TS_MSG

Modify this structure to add or change the information in the RSU TS message. Modify the CWrmMsg::CreateRsuMsgFromDevInfo() and CWrmMsg::ParseVtvMessage(). In addition, modifications to the CSignalInfo member data may be needed.

4.6.2 Changing Data Logging

To add or modify fields in the log records, modify the both record header and the record data. For example, to add the logging of a new reception parameter, modify the CTestLog::LogReceptionParametersLabels() method to add the new field name in the desired place, and then modify the CTestLog::LogReceptionParameters() method to log the new field each time a packet is received. Transmit and Receive packets all have the same system of labels and logging for each record type. (OBUTX, OBURX, RSUTX, RSURX).

4.6.3 Changing Test Types

The T9App currently supports 3 test types: run for n seconds, run for n transmits, and passive listener mode. Modify the CTestStatusDialog class, which has methods that check for test completion using the test type variable. If additional test types are defined, modify the CTestOptions class and the CTestOptionsGui Class.

4.6.4 Changing T9App Configuration Loading / Saving

Each class has its own global overloaded operators >> and << for loading and saving its configuration (for all classes that support loading/saving). To load/save additional class information, add these methods to the overloaded operator definitions to support this. Each class also has its own field labels function which must be updated so the field labels for the test log entries and configuration saving are consistent.

WaveDeviceInfo Example:

Change the stream output global overloaded function:

friend ostream &operator<<(ostream&, const CWaveDeviceInfo&)

Change the stream input global overloaded function:

friend istream &operator>>(istream&, CWaveDeviceInfo&);

Change the field labels function:

CWaveDeviceInfo::PrintHeaders

4.6.5 Changing CAN messages

To support additional or modified CAN messages, modify the CCanMsg and CVehicleInfo classes. The CCanMsg::UpdateVehicle method parses the CAN message ID, switches on this ID, and calls 1 of 3 different parsing functions, ProcessVelocityMessage, ProcessAccelMessage, and ProcessDevicesMessage. Modify the existing parsing function for changes, or add a parsing function for a new CAN message.

Each CAN message parser has a reference to a vehicle object that it updates with the contents of the CAN message. Modify the CVehicle class definition to modify or add storage variables if for the changed data. See the CVehicleInfo class description (Section 4.3.1.13) for details. If the OBU V2V message must also be modified, see Section 4.6.1.

5 Validation Results

5.1 Introduction

This chapter describes the Acceptance Test Plan (ATP) for the Task 9 Application (T9App) developed in accordance with the requirements in Chapter 2.

5.1.1 Scope

This Task 9 ATP defines the tests Denso conducted to verify compliance with the Task 9 requirements (Chapter 2), the Application Message Specification (Chapter 3), and the Traffic Signal Interface Specification (Section 6.4). The T9App also complies with the Wave Radio Module (WRM) Interface Specification [2]. The T9App re-uses the WRM interface software developed and verified as part of Task 6D. The interface requirements were not re-verified in this test. Denso submitted a test report with the results of these tests to the VSCC for approval.

5.2 Test Configurations

This section describes how to connect a host device to a WRM. It also describes the test setups and initialization procedures required by the tests specified in subsequent sections.

5.2.1 WAVE Radio Module Network Connection

Set up each Host Device (HD) and WRM as shown in Figure 5-1. Each HD and WRM must have a unique IP address. Configure the HD Internet Protocol (IP) address to 192.168.001.1xx, where xx is the WRM unit number assigned by Denso. Configure each HD with a Subnet Mask of 255.255.255.000.

5.2.2 Test Setups

5.2.2.1 Generic Test Setup

For all test setups, each HD is connected to its corresponding WRM using an Ethernet crossover cable. Each HD has the T9App and Ethereal software installed. Ethereal is a software network analyzer that may be downloaded at no charge from www.ethereal.com. The test procedures use Ethereal to verify the contents of the IP packets sent from the HD to the WRM. The WRM is powered using a wall power supply. Connect HD comm. port 1 to the VSCC supplied differential GPS (DGPS) using a standard serial cable. Configure the COM1 port settings to 9600 baud, no parity bit, 8 data bits, 1 stop bit. See Figure 5-1. For subsequent test setups, the crossover cable is not labeled, and the power supply is not shown for simplicity.

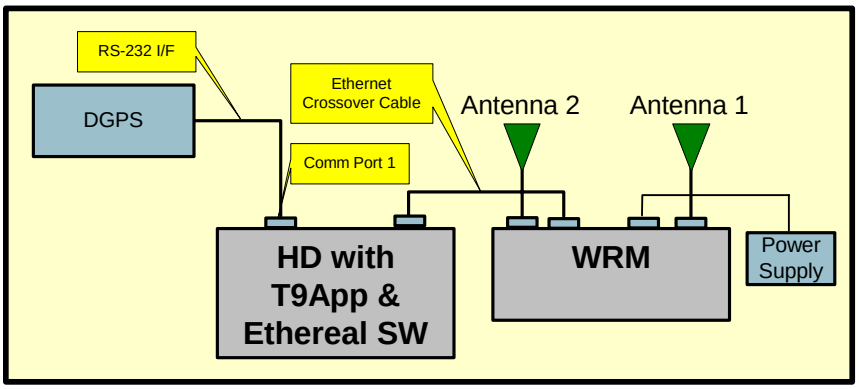


Figure 5-1. Generic Test Setup

5.2.2.2 OBU Test Setup

For OBU tests, install a Grid Connect Controller Area Network (CAN) bus adapter (see www.gridconnect.com for additional information) into the HD USB port and a second adapter into a laptop hosting the vehicle bus simulator (VBusSim) software. The VBusSim is a test application developed by Denso to verify the T9App. It enables the user to specify the CAN bus message contents. Connect the two adapters with a CAN bus cable. Verify the Peak System CAN (PCAN) software (supplied by Grid Connect) is installed on the HD. The test procedures use PCAN to verify the CAN bus message contents. See Figure 5-2.

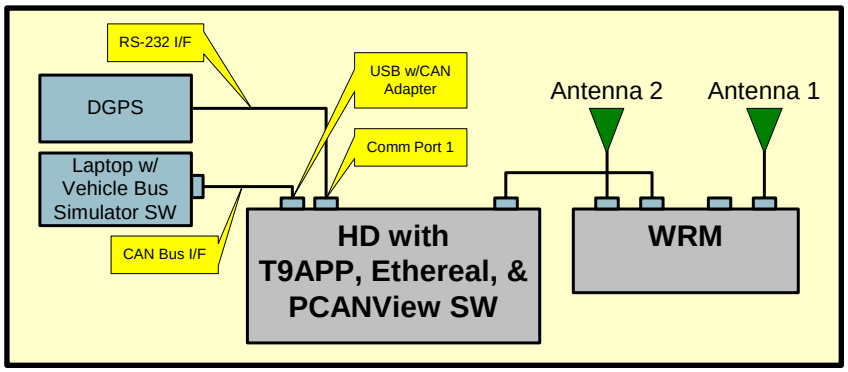


Figure 5-2. OBU Test Setup

5.2.2.3 RSU Test Setup

For RBU tests, connect HD comm port 2 to comm port 2 of a laptop hosting the traffic signal simulator (TrafSigSim) software using a standard serial cable. The TrafSigSim is a test application developed by Denso to verify the T9App. It responds to traffic signal queries and enables the user to specify the traffic signal message contents. Configure both comm ports to 19,200 bps, 8 data bits, no parity

bit, and 1 stop bit. The DGPS is not connected for some RSU tests. See Figure 5-3.

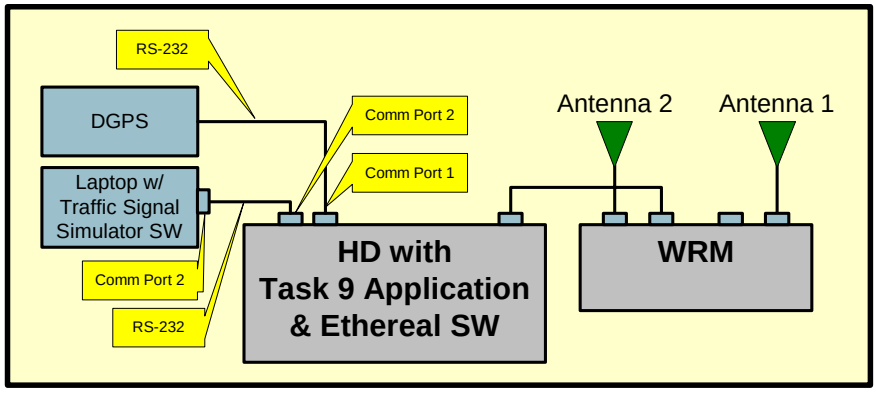


Figure 5-3. RSU Test Setup

5.2.3 Initialization

This section defines the procedures that are used to configure the hardware and software to a known state prior to starting a test. The tests in subsequent chapters refer to these procedures when required.

5.2.3.1 OBU and RSU Initialization Procedures

Table 5-1. OBU Initialization Procedure

#	Description	Test Steps	Expected Results
1.	Initialize HD.	If it is not already running, launch the T9App. If it is not already running, launch the Ethereal application.	The HD displays the T9App GUI and the Ethereal GUI.
	Initialize WRM.	On the T9App GUI, select WRM Configuration. On the WRM Configuration Screen, select Reset to WAVE default.	The WRM reboots and the T9App GUI displays the current WRM configuration.
	Initialize GUI parameters.	Initialize the T9App GUI parameters as described in Sections 5.2.3.2 and 5.2.3.3. Return to the main screen.	GUI displays entered values.
	Initialize GPS	If its not already running, turn on the GPS device and configure it up to output NMEA messages.	GPS device acquires satellite information and its GUI displays location information.
	Initialize VBusSim application.	If it is not already running, launch the VBusSim application on the connected laptop.	Laptop displays VBusSim GUI.

Table 5-2. RSU Initialization Procedure

#	Description	Test Steps	Expected Results
1.	Initialize HD.	If it is not already running, launch the T9App. If it is not already running, launch the Ethereal application.	The HD displays the T9App GUI and the Ethereal GUI.
	Initialize WRM.	On the TApp GUI, select WRM Configuration. On the WRM Configuration Screen, select Reset to WAVE default.	The WRM reboots and the Task 9 GUI displays the current WRM configuration.
	Set WRM to RSU mode.	On the WRM Configuration Screen, set the Unit Mode to RSU. Enter OK to return to the main screen. Select the WRM Configuration Screen. Confirm the unit mode is set to RSU. Enter OK to return to the main screen.	The T9App displays the unit mode as RSU.
	Initialize GUI parameters.	Initialize the GUI parameters as described in Sections 5.3, 5.4, and 5.5. Return to the main screen.	GUI displays entered values.
	Initialize GPS	If its not already running, turn on the GPS device and configure it up to output NMEA messages.	GPS device acquires satellite information and its GUI displays location information.
	Initialize Traffic Signal Simulator application.	If it is not already running, launch the Traffic Signal Simulator application on the connected laptop.	Laptop displays Traffic Signal Simulator GUI.

5.2.3.2 Communication Parameters Initialization

From the main screen, select Comm Parameters. On the Comm Parameters screen, set the parameters values as shown in Table 5-3.

Table 5-3. Communication Parameters Initial Values

Parameter	Value
Sender ID	Set to the last 3 digits of the host IP address.
Destination IP Address	255.255.255.255
Destination MAC Address	FF:FF:FF:FF:FF:FF
Message Interval (ms)	100
Message Size (bytes)	71 (OBU) or 125 (RSU)
GPS Group	Enabled (only if GPS is attached)
GPS Baud Rate	9600, N, 8, 1

Parameter	Value
GPS COM Port	COM1
Traffic Signal Setup	Enabled (RSU) or Disabled (OBU)
Traffic Signal Baud Rate	19200, N, 8, 1
Traffic Signal COM Port	COM2
Traffic Signal Polling Rate (ms)	500
CAN Setup	Enabled (OBU) or Disabled (RSU)
CAN Baud Rate	500 kbit/s
CAN Init Type	STD

5.2.3.3 Test Options Initialization

From the main screen, select Test Options. On the Test Options screen, set the parameter values as shown in Table 5-4.

Table 5-4. Test Options Initial Values

Parameter	Value
Test Control	Run for n seconds. Set seconds to 1000.
Logging	Enabled (select check box).
Test Name	ATP
Log Directory	C:\ATP

5.2.3.4 Traffic Signal Information Initialization

From the main screen, select Traffic Signal Information. On the Traffic Signal screen, set the Intersection # of Lanes to a value of four. Set the remaining parameters values as shown in Table 5-5.

Table 5-5. Traffic Signal Parameters Initial Values

	Latitude		Longitude				Yellow	Signal
Group	Degrees	Direction	Degrees	Direction	Altitude	Direction	Duration	Phase
Intersection	90	N	180	E	-1000.0	0.0	N/A	N/A
Stop Loc 1	45.9999999	N	90.9999999	E	500.01	90.99	0.00	1
Stop Loc 2	0.0000017	N	0.0000017	E	1000.25	180.0	20.001	3
Stop Loc 3	45.5	S	90.5	W	2500.50	-90.55	40.999	6
Stop Loc 4	90	S	180	W	4000.99	-179.99	65.535	8

5.2.4 Software Builds

Record the WRM software version and the T9App software version in Table 5-6.

Table 5-6. WRM and T9App Software Versions

WRM Software Version	T9App Software Version	WRM Unit Number	Tests
WAVE Radio Module Ver 1.0	Denso WAVEtest V0.1	4, 10, 2, 6	All

5.3 GUI Parameter Tests

5.3.1 WRM Configuration Screen

1. Set up a RSU configuration as described in Section 5.2 (without the GPS receiver connected) and execute the RSU initialization procedure in Table 5-2.
2. Set up an OBU configuration as described in Section 5.2 and execute the OBU initialization procedure in Table 5-1.
3. On both the RSU and OBU WRM Configuration Screen, set the Tx power to 0 dBm, and record the WRM MAC address in Table 5-7.
4. Start an Ethereal session on both the RSU and OBU to log Ethernet activity sent from the HDs to the WRMs.
5. On the T9App main screen for both the RSU and OBU, select start testing. Record the RSSI value from the Test Display Screen in Table 5-7.
6. Allow the test to run for a minimum of 10 seconds, and then stop testing on both the RSU and OBU.
7. Stop recording Ethernet activity on the RSU and OBU Ethereal.
8. Open a Telnet session from the RSU and OBU HDs to the associated WRM. Use a Get RSSI Telnet command to get the RSSI of the last received packet. Verify these RSSI values match the RSSI values recorded from the GUIs.
9. Open the T9App log file on the RSU and OBU side. Verify the logged values match the values in Table 5-7 and record the results.
10. Use Ethereal on the RSU and OBU side to verify the IP data fields listed in Table 5-8 match the values in Table 5-7 and record the results.
11. Repeat steps 3-10 with power settings of 10 dBm, and full power, and record the results in Table 5-7.

Table 5-7. WRM Configuration Screen Results

Unit	Parameter	Expected Results			Actual Results		
		GUI	Log	Ethereal	GUI	Log	Ethereal
RSU	WRM MAC Address	MAC Address	MAC Address	MAC Address	86:D9: FB:B1: 26:1C	Pass	Pass
	RSSI (OBU Tx power setting = 0 dBm)	+/- 2 dB from RSSI Telnet value	+/- 2 dB from RSSI Telnet value	N/A	-55	-55	N/A
	Telnet Get RSSI (OBU Tx power setting = 0 dBm)	-55					
	OS Time (Message Timestamp)	N/A	Increments by ~ 100,000,000 in each message.	Increments by ~ 100,000,000 in each message.	N/A	Pass	Pass
	Message Type	N/A	0x01	0x01	N/A	0x01	0x01
	Temporary ID	N/A	RSU WRM MAC Address	RSU WRM MAC Address	N/A	Pass	Pass
	RSUTX Tx Power (setting = 0 dBm)	N/A	0	00000	N/A	0	Pass
	OBURX Tx Power (setting = 0 dBm)	N/A	0	00000	N/A	0	Pass
	RSSI (OBU Tx power setting = 10 dBm)	+/- 2 dB from RSSI Telnet value	+/- 2 dB from RSSI Telnet value	N/A	-44	-44	N/A
	Telnet Get RSSI (OBU Tx power setting = 10 dBm)	-45					
	RSUTX Tx Power (setting = 10 dBm)	N/A	10	01010	N/A	10	01010
	OBURX Tx Power (setting = 10 dBm)	N/A	10	01010	N/A	10	01010
	RSSI (OBU Tx power setting = full)	+/- 2 dB from RSSI Telnet value	+/- 2 dB from RSSI Telnet value	N/A	-37	-37	N/A

Unit	Parameter	Expected Results			Actual Results		
		GUI	**Log**	**Ethereal**	**GUI**	**Log**	**Ethereal**
	Telnet Get RSSI (OBU Tx power setting = full)	-39					
	RSUTX Tx Power (setting = full)	N/A	31	11111	N/A	31	11111
	OBURX Tx Power (setting = full)	N/A	31	11111	N/A	31	11111
OBU	WRM MAC Address	MAC Address	MAC Address	MAC Address	B2:FE: 95:10: 1B:77	Pass	Pass
	RSSI (RSU Tx power setting = 0 dBm)	+/- 2 dB from RSSI Telnet value	+/- 2 dB from RSSI Telnet value	N/A	-59	-59	N/A
	Telnet Get RSSI (RSU Tx power setting = 0 dBm)	-57					
	OS Time (Message Timestamp)	N/A	Increments by ~ 100,000,000 in each message.	Increments by ~ 100,000,000 in each message.	N/A	Pass	Pass
	Message Type	N/A	0x00	0x00	N/A	0x00	0x00
	Temporary ID	N/A	OBU WRM MAC Address	OBU WRM MAC Address	N/A	Pass	Pass
	OBUTX Tx Power (setting = 0 dBm)	N/A	0	00000	N/A	0	00000
	RSURX Tx Power (setting = 0 dBm)	N/A	0	00000	N/A	0	00000
	RSSI (RSU Tx power setting = 10 dBm)	+/- 2 dB from RSSI Telnet value	+/- 2 dB from RSSI Telnet value	N/A	-47	-49	N/A
	Telnet Get RSSI (RSU Tx power setting = 10 dBm)	-48					
	OBUTX Tx Power (setting = 10 dBm)	N/A	0	01010	N/A	10	01010

Unit	Parameter	Expected Results			Actual Results		
		GUI	Log	Ethereal	GUI	Log	Ethereal
	RSURX Tx Power (setting = 10 dBm)	N/A	0	01010	N/A	10	01010
	RSSI (RSU Tx power setting = full)	+/- 2 dB from RSSI Telnet value	+/- 2 dB from RSSI Telnet value	N/A	-37	-37	N/A
	Telnet Get RSSI (RSU Tx power setting = full)	-39					
	OBUTX Tx Power (setting = full)	N/A	31	11111	N/A	31	11111
	RSURX Tx Power (setting = full)	N/A	31	11111	N/A	31	11111

Table 5-8. WRM Configuration Data Elements

Data Element	Length (bits)	IP Data Frame Byte #	IP Data Frame Bits
OS Time	56	23-29	All
Message Type	8	30	1-8
Temporary ID	48	31-36	All
Tx Power of Sender	5	22	1-5

5.3.2 Comm Parameters Screen

1. Set up a RSU configuration as described in Section 5.2.2.3 (without the GPS receiver connected) and execute the RSU initialization procedure in Table 5-2.
2. Set up an OBU configuration as described in Section 5.2.2.2 and execute the OBU initialization procedure in Table 5-1.

5.3.2.1 Comm Parameters Screen Low-Value Tests

1. On both the RSU and OBU Comm Parameters Screen, set the values as shown in Table 5-9 and enter OK.
2. Start an Ethereal session on both the RSU and OBU to log Ethernet activity sent from the HDs to the WRMs.
3. On the T9App main screen for both the RSU and OBU, select start testing.
4. Verify the GUI values match the values in Table 5-10 and record the results.
5. Allow the test to run for a minimum of 10 seconds, and then stop testing on both the RSU and OBU.

6. Stop recording Ethernet activity on both the RSU and OBU Ethereal.
7. Open the T9App log file on the RSU and OBU (Rx) side. Verify the logged values match the values in Table 5-10 and record the results.
8. Use Ethereal (on the RSU-side HD) to verify the RSU Traffic Signal Message IP data fields listed in Table 5-11 match the values in Table 5-10 and record the results. (**Note**: The Destination IP Address is part of the IP Frame, and the number of bytes for the Message Size must be counted.)

Table 5-9. Comm Parameters Screen Low Parameter Values

Parameter	Value
Destination IP Address	IP Address of other HD
Message Interval (msec)	10
Message Size (Bytes)	71 (OBU) or 125 (RSU)
Sender ID	0 (OBU) or 1 (RSU)

Table 5-10. Comm Parameters Screen Low Parameter Results

		Expected Results			Actual Results		
Unit	**Parameter**	**GUI**	**Log**	**Ethereal**	**GUI**	**Log**	**Ethereal**
RSU	Destination IP Address	N/A	N/A	OBU IP Address	N/A	N/A	Pass
	Message Interval	N/A	~100 RSUTX entries/sec	N/A	N/A	100 msgs in 1.046 seconds	N/A
	Packet Length	N/A	125 (RSUTX) 71 (OBURX)	0x07D	N/A	125 71	0x07D 0x047
	Message Size	N/A	N/A	125 bytes	N/A	N/A	125
	Sender ID	1 (RSU) 0 (OBU)	1 (RSUTX), 0 (OBURX)	0x0001	1 0	1 0	0x0001 0x0000
OBU	Destination IP Address	N/A	N/A	RSU IP Address	N/A	N/A	Pass
	Message Interval	N/A	~100 OBUTX entries/sec	N/A	N/A	100 msgs in 1.044 seconds	N/A

Unit	Parameter	Expected Results			Actual Results		
		GUI	Log	Ethereal	GUI	Log	Ethereal
	Packet Length	N/A	71 (OBUTX) 125 (RSURX)	0x047	N/A	71 125	0x047 0x07D
	Message Size	N/A	N/A	71 bytes	N/A	N/A	71
	Sender ID	0 (OBU) 1 (RSU)	0 (OBUTX) 1 (RSURX)	0x0000	0 1	0 1	0x0000 0x0001

Table 5-11. Comm Parameters Screen Data Elements

Data Element	Length (bits)	IP Data Frame Byte #	IP Data Frame Bits
Packet Length	12	1	1-8
		2	1-4
Sender ID	16	18-19	All

5.3.2.2 Comm Parameters Screen Mid-Value Tests

1. Repeat step 1 of Section 5.3.2.1, using the Comm Parameter Values in Table 5-12.
2. Repeat steps 2-8 of Section 5.3.2.1, verifying the values and recording the results in Table 5-13.

Table 5-12. Comm Parameters Screen Mid-Parameter Values

Parameter	Value
Destination IP Address	255.255.255.255
Message Interval (msec)	100
Message Size (Bytes)	500
Sender ID	255 (OBU) or 256 (RSU)

Table 5-13. Comm Parameters Screen Mid-Parameter Results

Unit	Parameter	Expected Results			Actual Results		
		GUI	Log	Ethereal	GUI	Log	Ethereal
RSU	Destination IP Address	N/A	N/A	255.255. 255.255	N/A	N/A	255.255. 255.255
	Message Interval	N/A	~10 RSUTX entries/sec	N/A	N/A	10 msgs in 0.902 seconds	N/A
	Packet Length	N/A	500 (RSUTX) 500 (OBURX)	0x1F4	N/A	500 500	0x1F4
	Message Size	N/A	N/A	500 bytes	N/A	N/A	500
	Sender ID	256 (RSU) 255 (OBU)	256 (RSUTX) 255 (OBURX)	0x0100	256 255	256 255	0x0100 0x00FF
OBU	Destination IP Address	N/A	N/A	255.255. 255.255	N/A	N/A	255.255. 255.255
	Message Interval	N/A	~10 OBUTX entries/sec	N/A	N/A	10 msgs in 0.908 seconds	N/A
	Packet Length	N/A	500 (OBUTX) 500 (RSURX)	0x1F4	N/A	500 500	0x1F4
	Message Size	N/A	N/A	500 bytes	N/A	N/A	500
	Sender ID	255 (OBU) 256 (RSU)	255 (OBUTX) 256 (RSURX)	0x00FF	255 256	255 256	0x00FF 0x0100

5.3.2.3 Comm Parameters Screen High-Value Tests

1. Repeat step 1 of Section 5.3.2.1, using the Comm Parameter Values in Table 5-14.
2. Repeat steps 2-8 of Section 5.3.2.1, verifying the values and recording the results in Table 5-15.

Table 5-14. Comm Parameters Screen High-Parameter Values

Parameter	Value
Destination IP Address	255.255.255.255
Message Interval (msec)	1000
Message Size (Bytes)	1200
Sender ID	65534 (OBU) or 65535 (RSU)

Table 5-15. Comm Parameters Screen High-Parameter Results

Unit	Parameter	Expected Results			Actual Results		
		GUI	Log	Ethereal	GUI	Log	Ethereal
RSU	Destination IP Address	N/A	N/A	255.255. 255.255	N/A	N/A	255.255. 255.255
	Message Interval	N/A	~1 RSUTX entry/sec	N/A	N/A	1.000 msgs/sec	N/A
	Packet Length	N/A	1200 (RSUTX) 1200 (OBURX)	0x4B0	N/A	1200 1200	0x4B0
	Message Size	N/A	N/A	1200 bytes	N/A	N/A	1200
	Sender ID	65535 (RSU) 65534 (OBU)	65535 (RSUTX) 65534 (OBURX)	0xFFFF	65535 65534	65535 65534	0xFFFF 0xFFFE
OBU	Destination IP Address	N/A	N/A	255.255. 255.255	N/A	N/A	255.255. 255.255
	Message Interval	N/A	~1 OBUTX entry/sec	N/A	N/A	1.000 msgs/sec	N/A
	Packet Length	N/A	1200 (OBUTX) 1200 (RSURX)	0x4B0	N/A	1200 1200	0x4B0
	Message Size	N/A	N/A	1200 bytes	N/A	N/A	1200
	Sender ID	65534 (OBU) 65535 (RSU)	65534 (OBUTX) 65535 (RSURX)	0xFFFE	65534 65535	65534 65535	0xFFFE 0xFFFF

5.3.3 Test Options Screen

1. Set up a RSU configuration as described in Section 5.2.2.3 (without the GPS receiver connected) and execute the RSU initialization procedure in Table 5-2.
2. Set up an OBU configuration as described in Section 5.2.2.2 and execute the OBU initialization procedure in Table 5-1.
3. On both the RSU and OBU Test Options Screen, set the values as shown in Case 1 of Table 5-16 and enter OK.
4. Start an Ethereal session to log Ethernet activity between the RSU HD and the WRM.
5. On the T9App main screen for both the RSU and OBU, select start testing.
6. While the test is running, hit the Pause button on both the RSU and OBU.
7. Verify the message counts stop incrementing on both the RSU and OBU GUI.
8. Verify Ethereal is not detecting messages being sent or received.
9. Once the test has been paused for at least 5 seconds, hit the Resume button on the RSU and OBU.
10. Verify the GUI values match the values Table 5-17 and record the results.
11. For Test Case 1 and 2, wait until the test completes. For Test Case 3, wait 80 seconds and then hit the Quit button on both the RSU and OBU.
12. Stop recording Ethernet activity on Ethereal.
13. Open the T9App log file on the RSU and OBU side. Verify the logged values match the values in Table 5-17 and record the results.
14. Use Ethereal to view the IP data fields listed in Table 5-18 and verify the fields match the values in Table 5-17 and record the results.
15. Repeat steps 3-11 for Cases 2 and 3 in Table 5-16 and record the results in Table 5-19 and Table 5-20.

Table 5-16. Test Options Screen Parameter Values

Parameter	Values		
	Case 1	**Case 2**	**Case 3**
Test Control	Run for n sent messages. Set # of messages to 1000.	Run for n seconds. Set # of seconds to 50.	Run for n seconds. Set # of seconds to 100.
Logging	Enabled	Enabled	Disabled
Test Name	ATP	ATP	N/A
Log Directory	C:\ATP	C:\ATP	N/A

Table 5-17. Test Options Screen Case 1 Results

Unit	Parameter	Expected Results			Actual Results		
		GUI	Log	Ethereal	GUI	Log	Ethereal
RSU	Message Count (test running)	Increments from 1 to # of messages sent or received.	RSUTX and OBURX increments from 1 to # of messages sent or received.	Increments from 1 to # of messages sent	Pass	Pass	Pass
	Message Count (test paused)	Message counts stop incrementing.	N/A	No messages being sent.	Pass	N/A	Pass
	Test Run	Last test run # + 1.	N/A	N/A	Pass	N/A	N/A
	Messages Sent	1000	N/A	N/A	Pass	N/A	N/A
	Seconds elapsed	~100	N/A	N/A	99	N/A	N/A
	Log	N/A	1	1	N/A	1	1
	Logfile name	N/A	c:\ATP\ATP_[test run]_mmddyyyy.txt	N/A	N/A	Pass	N/A
OBU	Message Count (test running)	Increments from 1 to # of messages sent or received.	OBUTX and RSURX increments from 1 to # of messages sent or received.	Increments from 1 to # of messages sent	Pass	Pass	Pass
	Message Count (test paused)	Message counts stop incrementing.	N/A	No messages being sent.	Pass	N/A	Pass
	Test Run	Last test run # + 1.	N/A	N/A	Pass	N/A	N/A
	Messages Sent	1000	N/A	N/A	Pass	N/A	N/A
	Seconds elapsed	~100	N/A	N/A	99	N/A	N/A
	Log	N/A	1	1	N/A	1	1
	Logfile name	N/A	c:\ATP\ATP_[test run]_mmddyyyy.txt	N/A	N/A	Pass	N/A

Table 5-18. Test Options Data Elements

Data Element	Length (bits)	IP Data Frame Byte #	IP Data Frame Bits
Message Count	16	20-21	All
Log	1	22	6

Table 5-19. Test Options Screen Case 2 Results

Unit	Parameter	Expected Results			Actual Results		
		GUI	Log	Ethereal	GUI	Log	Ethereal
RSU	Message Count (test running)	Increments from 1 to # of messages sent or received.	RSUTX and OBURX increments from 1 to # of messages sent or received.	Increments from 1 to # of messages sent	Pass	Pass	Pass
	Message Count (test paused)	Message counts stop incrementing .	N/A	No messages being sent.	Pass	N/A	Pass
	Test Run	Last test run # + 1.	N/A	N/A	Pass	N/A	N/A
	Messages Sent	~500	N/A	N/A	499	N/A	N/A
	Seconds elapsed	50	N/A	N/A	50	N/A	N/A
	Log	N/A	1	1	N/A	1	1
	Logfile name	N/A	c:\ATP\ATP_[test run]_mmddyyyy.txt	N/A	N/A	Pass	N/A
OBU	Message Count (test running)	Increments from 1 to # of messages sent or received.	OBUTX and RSURX increments from 1 to # of messages sent or received.	Increments from 1 to # of messages sent	Pass	Pass	Pass
	Message Count (test paused)	Message counts stop incrementing .	N/A	No messages being sent.	Pass	N/A	Pass
	Test Run	Last test run # + 1.	N/A	N/A	Pass	N/A	N/A
	Messages Sent	~500	N/A	N/A	499	N/A	N/A
	Seconds elapsed	50	N/A	N/A	50	N/A	N/A
	Log	N/A	1	1	N/A	1	1

Unit	Parameter	Expected Results			Actual Results		
		GUI	Log	Ethereal	GUI	Log	Ethereal
	Logfile name	N/A	c:\ATP\ATP_[test run]_mmddyyyy.txt	N/A	N/A	Pass	N/A

Table 5-20. Test Options Screen Case 3 Results

Unit	Parameter	Expected Results			Actual Results		
		GUI	Log	Ethereal	GUI	Log	Ethereal
RSU	Message Count	Increments from 1 to # of messages sent or received.	N/A	Increments from 1 to # of messages sent	Pass	N/A	Pass
	Test Run	"N/A"	N/A	N/A	"N/A"	N/A	N/A
	Messages Sent	~800	N/A	N/A	Pass	N/A	N/A
	Seconds elapsed	80	N/A	N/A	80	N/A	N/A
	Log	N/A	N/A	0	N/A	N/A	0
	Logfile name	N/A	No logfile generated	N/A	N/A	Pass	N/A
OBU	Message Count	Increments from 1 to # of messages sent or received.	N/A	Increments from 1 to # of messages sent	Pass	N/A	Pass
	Test Run	"N/A"	N/A	N/A	"N/A"	N/A	N/A
	Messages Sent	~800	N/A	N/A	Pass	N/A	N/A
	Seconds elapsed	80	N/A	N/A	Pass	N/A	N/A
	Log	N/A	N/A	0	N/A	N/A	0
	Logfile name	N/A	No logfile generated	N/A	N/A	Pass	N/A

5.3.4 Traffic Signal Information Screen

1. Set up a RSU configuration as described in Section 5.2.2.3 (without the GPS receiver connected) and execute the RSU initialization procedure in Table 5-2.
2. Set up an OBU configuration as described in Section 5.2.2.2 and execute the OBU initialization procedure in Table 5-1.
3. Start an Ethereal session to log Ethernet activity between the RSU HD and the WRM.

4. On the T9App main screen for both the RSU and OBU, select start testing.
5. Verify the GUI values match the values in Table 5-21 for RSU (Tx) and OBU (Rx) sides, and record the results.
6. Allow the test to run for a minimum of 5 seconds, and then stop testing on both the RSU and OBU.
7. Stop recording Ethernet activity on Ethereal.
8. Open the T9App log file on the RSU (Tx) and OBU (Rx) side. Verify the logged values match the values in Table 5-21 and record the results.
9. Use Ethereal (on the RSU-side HD) to view the RSU Traffic Signal Message IP data fields listed in Table 5-22. Verify the fields match the values in Table 5-21 and record the results.

Table 5-21. Traffic Signal Information Screen Results

		Expected Results			Actual Results				
Group	**Parameter**	**GUI**	**Log**	**Ethereal**	**Tx GUI**	**Tx Log**	**Ethereal**	**Rx GUI**	**Rx Log**
Intersection	Latitude	90.0	90.0	0x35A4E900	90	90	Pass	90	90
	Longitude	180.0	180.0	0x6B49D200	180	180	Pass	180	180
	Altitude	N/A	-1000.0	0x00000	N/A	-1000	Pass	N/A	-1000
	Number of Lanes	N/A	4	N/A	N/A	4	N/A	N/A	N/A
Stop Loc 1	Latitude	N/A	45.9999999	0x1B6B0AFF	N/A	45.9999999	Pass	N/A	45.9999999
	Longitude	N/A	90.9999999	0x363D7F7F	N/A	90.9999999	Pass	N/A	90.9999999
	Altitude	N/A	500.01	0x249F1	N/A	500.01	Pass	N/A	500.01
	Direction	N/A	90.99	0x238B	N/A	90.99	Pass	N/A	90.99
	Yellow Duration	N/A	0.0	0x0000	N/A	0	Pass	N/A	0
Stop Loc 2	Latitude	N/A	0.0000017	0x00000011	N/A	0.0000017	Pass	N/A	0.0000017
	Longitude	N/A	0.0000017	0x00000011	N/A	0.0000017	Pass	N/A	0.0000017
	Altitude	N/A	1000.25	0x30D59	N/A	1000.25	Pass	N/A	1000.25
	Direction	N/A	180.0	0x4650	N/A	180	Pass	N/A	180
	Yellow Duration	N/A	20.001	0x4E21	N/A	20.001	Pass	N/A	20.001
Stop Loc 3	Latitude	N/A	-45.5	0xE4E14040	N/A	-45.5	Pass	N/A	-45.5
	Longitude	N/A	-90.5	0xCA0ECBC0	N/A	-90.5	Pass	N/A	-90.5
	Altitude	N/A	2500.50	0x55762	N/A	2500.5	Pass	N/A	2500.5

Group	Parameter	Expected Results			Actual Results				
		GUI	Log	Ethereal	Tx GUI	Tx Log	Ethereal	Rx GUI	Rx Log
	Direction	N/A	-90.55	0xDCA1	N/A	-90.55	Pass	N/A	-90.55
	Yellow Duration	N/A	40.999	0xA027	N/A	40.999	Pass	N/A	40.999
Stop Loc 4	Latitude	N/A	-90.0	0xCA5B1700	N/A	-90	Pass	N/A	-90
	Longitude	N/A	-180.0	0x94B62E00	N/A	-180	Pass	N/A	-180
	Altitude	N/A	4000.99	0x7A183	N/A	4000.99	Pass	N/A	4000.99
	Direction	N/A	-179.99	0xB9B1	N/A	-179.99	Pass	N/A	-179.99
	Yellow Duration	N/A	65.535	0xFFFF	N/A	65.535	Pass	N/A	65.535

Table 5-22. Traffic Signal Message Data Elements

Data Element		Length (bits)	IP Data Frame Byte #	IP Data Frame Bits
Intersection	Longitude	32	38-41	All
	Latitude	32	42-45	All
	Altitude	20	46-47	All
			48	1-4
Stop Loc 1	Longitude	32	54-57	All
	Latitude	32	58-61	All
	Altitude	20	62-63	All
			64	1-4
	Direction	16	65-66	All
	Yellow Duration	16	70-71	All
Stop Loc 2	Longitude	32	72-75	All
	Latitude	32	76-79	All
	Altitude	20	80-81	All
			82	1-4
	Direction	16	83-84	All
	Yellow Duration	16	88-89	All

Data Element		Length (bits)	IP Data Frame Byte #	IP Data Frame Bits
Stop Loc 3	Longitude	32	90-93	All
	Latitude	32	94-97	All
	Altitude	20	98-99	All
			100	1-4
	Direction	16	101-102	All
	Yellow Duration	16	106-107	All
Stop Loc 4	Longitude	32	108-111	All
	Latitude	32	112-115	All
	Altitude	20	116-117	All
			118	1-4
	Direction	16	119-120	All
	Yellow Duration	16	124-125	All

5.3.5 Test Display Screen

5.3.5.1 Distance Calculation, OBU Heading Test

1. Set up a RSU configuration as described in Section 5.2.2.3 (without the GPS receiver connected) and execute the RSU initialization procedure in Table 5-2.
2. Set up an OBU configuration as described in Section 5.2.2.2 and execute the OBU initialization procedure in Table 5-1.
3. Record the GPS device readings in Table 5-23.
4. On the RSU Traffic Signal Parameters screen, set the intersection location values as shown in Case 1 of Table 5-24.
5. Calculate the distance between the RSU and OBU side by entering the GPS readings as the source, and the RSU Traffic Signal Intersection Location as the destination on the web site http://jan.ucc.nau.edu/~cvm/latlongdist.html.
6. On the T9App main screen for both the RSU and OBU, select start testing.
7. Verify the GUI values match the values in Table 5-25 and record the results.
8. Stop the test.
9. Open the T9App log file on the RSU and OBU side. Verify the logged values match the values in Table 5-25 and record the results.
10. Repeat steps 4-9 for Cases 2 and 3 in Table 5-24 and record the results in Table 5-25.

Table 5-23. Distance, Heading Test GPS Data

Parameter	GPS Device Readings
Longitude	-117.2275
Latitude	33.1333
Altitude	161.7 m

Table 5-24. Distance, Heading Test Parameter Values

Parameter Group	Parameter	Values		
		Case 1	Case 2	Case 3
RSU Traffic Signal Intersection Location	Latitude	Same as GPS latitude reading	GPS latitude reading + 0.0003 degrees	GPS latitude reading - 0.0015 degrees
	Longitude	Same as GPS longitude reading	GPS longitude reading + 0.0003 degrees	GPS longitude reading - 0. 0015 degrees
	Altitude	Same as GPS altitude reading	Same as GPS altitude reading	Same as GPS altitude reading

Table 5-25. Distance, Heading Test Results

Test Case	Parameter	Expected Results		Actual Results			
		GUI	Log	RSU GUI	RSU Log	OBU GUI	OBU Log
1	Distance to Sender as calculated by web site		0				
	Distance to Sender	Same as web site +/- 5 meters.	Same as web site +/- 5 meters.	4.3 m	4.3 m	4.3m	4.3 m
	OBU Heading	Fluctuating Value	Fluctuating Value	Pass	Pass	N/A	N/A
2	Distance to Sender as calculated by web site		43.6 m				
	Distance to Sender	Same as web site +/- 5 meters.	Same as web site +/- 5 meters.	43.1 m	43.1 m	43.1 m	43.1 m
3	Distance to Sender as calculated by web site		217.8 m				
	Distance to Sender	Same as web site +/- 5 meters.	Same as web site +/- 5 meters.	218.5 m	218.5 m	218.5 m	218.5 m

5.3.5.2 RSU – RSU Bearing Test

1. Set up a RSU configuration as described in Section 5.2.2.3 (with the GPS receiver connected) and execute the RSU initialization procedure in Table 5-2.
2. Set up a second RSU configuration as described in Section 5.2.2.3 (without the GPS receiver connected) and execute the RSU initialization procedure in Table 5-2.
3. Record the GPS device readings in Table 5-26.
4. On the RSU #2 Traffic Signal Parameters screen, set the intersection location values as shown in Case 1 of Table 5-27.
5. Calculate the bearing between the RSUs using the Excel spreadsheet Task9Bearing.xls (spreadsheet generated by Denso). Enter the GPS readings for RSU #1, and the RSU Traffic Signal Intersection Location for RSU # 2 in Table 5-28.
6. On the T9App main screen for both the RSUs, select start testing.
7. Verify the GUI values match the values Table 5-28 and record the results.
8. Stop the test.
9. Open the T9App log file for both RSUs. Verify the logged values match the values in Table 5-28 and record the results.
10. Repeat steps 3-9 for Cases 2, 3, and 4 in Table 5-27 and record the results in Table 5-28.

Table 5-26. RSU – RSU Bearing Test GPS Data

Parameter	GPS Device Readings
Longitude	-117.2275
Latitude	33.1333
Altitude	161.7 m

Table 5-27. RSU – RSU Bearing Test Parameter Values

Parameter Group	Parameter	Value			
		Case 1	Case 2	Case 3	Case 4
RSU Traffic Signal Intersection Location	Latitude	GPS latitude reading + 0.0015 degrees	Same as GPS latitude reading	GPS latitude reading + 0.0015 degrees	GPS latitude reading -0.0015 degrees
	Longitude	Same as GPS longitude reading	GPS longitude reading + 0.0015 degrees	GPS longitude reading + 0.0015 degrees	GPS longitude reading -0.0015 degrees

Parameter Group	Parameter	Value			
		Case 1	**Case 2**	**Case 3**	**Case 4**
	Altitude	Same as GPS altitude reading	Same as GPS altitude reading	Same as GPS altitude reading	Same as GPS altitude reading

Table 5-28. RSU – RSU Bearing Test Results

Test Case	Parameter	Expected Results		Actual Results	
		GUI	**Log**	**GUI**	**Log**
1	Bearing from RSU #1 to RSU #2 calculated by spreadsheet.		0		
	Bearing from RSU #2 to RSU #1 calculated by spreadsheet.		180		
	RSU # 1 display/log	Same as spreadsheet +/- 2 degrees.	Same as spreadsheet +/- 2 degrees.	-0.7	-0.7
	RSU # 2 display/log	Same as spreadsheet +/- 2 degrees.	Same as spreadsheet +/- 2 degrees.	179.3	179.3
2	Bearing from RSU #1 to RSU #2 calculated by spreadsheet.		-90		
	Bearing from RSU #2 to RSU #1 calculated by spreadsheet.		90		
	RSU # 1 display/log	Same as spreadsheet +/- 2 degrees.	Same as spreadsheet +/- 2 degrees.	-91.4	-91.4
	RSU # 2 display/log	Same as spreadsheet +/- 2 degrees.	Same as spreadsheet +/- 2 degrees.	88.6	88.6
3	Bearing from RSU #1 to RSU #2 calculated by spreadsheet.		-39.9		
	Bearing from RSU #2 to RSU #1 calculated by spreadsheet.		140.1		
	RSU # 1 display/log	Same as spreadsheet +/- 2 degrees.	Same as spreadsheet +/- 2 degrees.	-41.1	-41.1
	RSU # 2 display/log	Same as spreadsheet +/- 2 degrees.	Same as spreadsheet +/- 2 degrees.	138.9	138.9
4	Bearing from RSU #1 to RSU #2 calculated by spreadsheet.		140.1		

Test Case	Parameter	Expected Results		Actual Results	
		GUI	Log	GUI	Log
	Bearing from RSU #1 to RSU #2 calculated by spreadsheet.		-39.9		
	RSU # 1 display/log	Same as spreadsheet +/- 2 degrees.	Same as spreadsheet +/- 2 degrees.	141.2	141.2
	RSU # 2 display/log	Same as spreadsheet +/- 2 degrees.	Same as spreadsheet +/- 2 degrees.	-38.8	-38.8

5.3.5.3 OBU – OBU Relative Heading Test

1. Set up an OBU configuration (with a GPS connected) as described in Section 5.2.2.2 and execute the OBU initialization procedure in Table 5-1.
2. Set up a second OBU configuration (without a GPS connected) as described in Section 5.2.2.2 and execute the OBU initialization procedure in Table 5-1.
3. On the OBU # 1 VBusSim GUI, set the CAN bus message parameters as shown in Case 1 of Table 5-29.
4. On the T9App main screen for both OBUs, select start testing.
5. Verify the OBU # 1 GUI values match the values in Table 5-30 and record the results.
6. Stop the test.
7. Repeat steps 3-6 for Cases 2 and 3 in Table 5-29 and record the results in Table 5-30.

Table 5-29. OBU – OBU Relative Heading Test Parameters

Parameter Group	Parameter	Values		
		Case 1	Case 2	Case 3
OBU Vehicle Velocity Message	Vehicle Speed	5.00 m/s	5.01 m/s	400.00 m/s
	Vehicle Speed Availability	1	1	1

Table 5-30. OBU – OBU Relative Heading Test Results

Test Case	Parameter	Expected Results	Actual Results
		GUI	GUI
1	OBU 1 relative heading to OBU # 2	0	"N/A"
2	OBU 1 relative heading to OBU # 2	Fluctuating Value	Fluctuating Value
3	OBU 1 relative heading to OBU # 2	Fluctuating Value	Fluctuating Value

5.3.6 GUI Configuration Recording, Persistence

1. Set up a RSU configuration as described in Section 5.2.2.3 (without the GPS receiver connected) and execute the RSU initialization procedure in Table 5-2.
2. Set up an OBU configuration as described in Section 5.2.2.2 and execute the OBU initialization procedure in Table 5-1.
3. On the T9App main screen for both the RSU and OBU, select start testing.
4. Allow the test to run for a minimum of 5 seconds, and then stop testing on both the RSU and OBU.
5. Open the T9App log file on the RSU (Tx) and OBU (Rx) side. Verify the logged values in the Config entries match the values in Table 5-31 and record the results.
6. Close the T9App and cycle power on both the RSU and OBU HDs. Re-open the T9App on both the RSU and OBU.
7. Repeat steps 3-5 and record the results in Table 5-31.

Table 5-31. GUI Configuration Recording, Persistence Results

Test Step	Screen	Expected Results	Actual Results	
		Log	RSU Log	OBU Log
5	Communication Parameters	See Table 5-3.	Pass	Pass
	Test Options	See Table 5-4.	Pass	Pass
	Traffic Signal Parameters	See Table 5-5.	Pass	All zeros
7	Communication Parameters	See Table 5-3.	Pass	Pass
	Test Options	See Table 5-4.	Pass	Pass
	Traffic Signal Parameters	See Table 5-5.	Pass	All zeros

5.4 Interface Tests

5.4.1 GPS Receiver Interface Tests

5.4.1.1 Common Message Header – GPS Data Tests

1. Set up an OBU configuration as described in Section 5.2.2.2 and execute the OBU initialization procedure in Table 5-1, without launching the VBusSim application.
2. Start the GPS and allow it to acquire satellite information and update its display.
3. Record the GPS device readings in Table 5-32.
4. Start an Ethereal session to log Ethernet activity between the HD and the WRM.
5. On the OBU T9App main screen, select start testing.
6. Allow the T9App test to run for at least 5 seconds.
7. Stop recording Ethernet activity on Ethereal.
8. Convert the time recorded on the GPS device to the number of seconds since the start of the week. Convert this value to hex to verify the “GPS seconds in week” value captured by Ethereal.
9. Use Ethereal to view the IP data fields indicated in Table 5-33 and record the values. Convert the hex values to decimal and verify the data corresponds to the GPS device values in Table 5-32. Record the results.

Table 5-32. Common Message Header GPS Data Test Results

Parameter	GPS Device Readings	Ethereal Results (decimal)
Longitude	-117.2275	-1163886040
Latitude	33.1333	331333293
Altitude	162.5m	116250
Time	21:24:50	249906

Table 5-33. Common Message Header GPS Data Elements

Data Element	Length (bits)	IP Data Frame Byte #	IP Data Frame Bits	Value (Hex)
GPS Seconds in Week	20	2	5-8	0x3
		3-4	All	0xD032
Longitude	32	5-8	All	0XBA208228
Latitude	32	9-12	All	0x13BFBEAD
Altitude	20	13-14	All	0x1C61
		15	1-4	0xA

5.4.1.2 OBU GPS Interface Tests

1. Set up a RSU configuration as described in Section 5.2.2.3, without the GPS receiver connected. Execute the RSU initialization procedure in Table 5-2, without launching Ethereal or TrafSigSim applications.
2. Set up an OBU configuration as described in Section 5.2.2.2 and execute the OBU initialization procedure in Table 5-1, without launching the VBusSim application.
3. Start the GPS and allow it to acquire satellite information and update its display.
4. Record the GPS device readings in Table 5-34.
5. Start an Ethereal session to log Ethernet activity between the OBU HD and the OBU WRM.
6. On the T9App main screen for both RSU and OBU, select start testing.
7. Allow the test to run for at least 5 seconds.
8. Stop recording Ethernet activity on Ethereal.
9. Open the T9App log file on the OBU side and verify the logged GPS values match the values recorded by the GPS device. Verify the logged values in both the OBUTX entries and the RSURX log entries. In the OBUTX entries,

the GPS data is logged as the transmitted data. In the RXURX entries, the GPS data is logged as the receiver information. Record the results in Table 5-34.

10. Use Ethereal (on the OBU HD) to view the IP data fields indicated in Table 5-35 and record the values. Convert the hex values to decimal and verify the data corresponds to the GPS device values in Table 5-34. Record the results.
11. Convert the time recorded on the GPS device to the number of seconds since the start of the week. Use this calculated value to verify the OBU and RSU logged values for GPS seconds in the week. Convert this value to hex to verify the GPS seconds in the week value sent from the OBU, as captured by Ethereal.
12. Open the T9App log file on the RSU side and verify the logged GPS values in the OBURX entries match the values recorded by the GPS device. Record the results in Table 5-34.

Table 5-34. OBU GPS Interface Test Results

Parameter	GPS Device Readings	Actual Results			
		OBU Log		Ethereal	RSU Log OBURX
		OBUTX	RSURX		
Longitude	-117.2275	-117.2275	180	1172274637	-117.2275
Latitude	33.1333	33.1333	90	331333189	33.1333
Altitude	163.3 m	163.3	-1000	116330	163.3
Time	02:37:59	268679	268679	268679	268679

Table 5-35. OBU V2V Safety Message GPS Data Elements

Data Element	Length (bits)	IP Data Frame Byte #	IP Data Frame Bits	Value (Hex)
Longitude	32	38-41	All	0xBA20820F
Latitude	32	42-45	All	0x13BFBE45
Altitude	20	46-47	All	0x1C66
		48	1-4	0xA
# of seconds in week	40	2	5-8	0x4
		3-4	All	0x1987

5.4.1.3 RSU GPS Interface Tests

1. Set up a RSU configuration as described in Section 5.2.2.3 and execute the RSU initialization procedure in Table 5-2, without launching the Ethereal application.
2. Set up an OBU configuration as described in Section 5.2.2.2 without the GPS receiver connected. Execute the OBU initialization procedure in Table 5-1, without launching Ethereal or VBusSim applications.
3. Start the GPS and allow it to acquire satellite information and update its display.
4. Record the GPS device readings in Table 5-36.
5. Start an Ethereal session to log Ethernet activity between the RSU HD and the RSU WRM.
6. On the T9App main screen for both RSU and OBU, select start testing.
7. Review the T9App GUI on both the RSU and OBU to verify the RSU longitude and latitude values match the values recorded by the GPS device. Record the results in Table 5-36.
8. Allow the test to run for at least 5 seconds.
9. Stop recording Ethernet activity on Ethereal.
10. Open the T9App log file on the RSU side and verify the logged GPS values in both the RSUTX and OBURX entries match the values recorded by the GPS device. In the RSUTX entries, the GPS data is logged as the transmitted data. In the OBURX entries, the GPS data is logged as the receiver information. Record the results in Table 5-36.
11. Use Ethereal (on the RSU HD) to view the IP data fields indicated in Table 5-37 and record the values. Convert the hex values to decimal and verify the data corresponds to the GPS device values in Table 5-36. Record the results.
12. Convert the time recorded on the GPS device to the number of seconds since the start of the week. Use this calculated value to verify the OBU and RSU logged values for GPS seconds in the week. Convert this value to hex to verify the GPS seconds in the week value sent from the OBU, as captured by Ethereal.
13. Open the T9App log file on the OBU side and verify the logged GPS values in the RSURX entries match the values recorded by the GPS device. Record the results in Table 5-36.

Table 5-36. RSU GPS Interface Test Results

Parameter	GPS Device Readings	Actual Results				
		RSU GUI	RSU Log	Ethereal	RSU GUI	RSU Log (RSURX)
Longitude	-117.2275	-117.2275	-117.2275	1172274755	-117.2275	-117.2275
Latitude	33.1333	33.1333	33.1333	331333183	33.1333	33.1333
Altitude	163.3 m	N/A	166.6	117240	N/A	166.6
Time	02:57:00	N/A	269962	269962	N/A	269962

Table 5-37. RSU Traffic Signal Message GPS Data Elements

Data Element	Length (bits)	IP Data Frame Byte #	IP Data Frame Bits	Value (Hex)
Longitude	32	38-41	All	0xBA2081BD
Latitude	32	42-45	All	0x13BFBE3F
Altitude	20	46-47	All	0x1C9F
		48	1-4	0x8
# of seconds in week	40	2	5-8	0x4
		3-4	All	0x2383

5.4.2 Vehicle Bus Interface Tests

The tests in this section will verify low, mid and high values for all vehicle speed, yaw rate, lateral and longitudinal acceleration, throttle position, and steering wheel angle. The remaining discrete field values will also be verified.

1. Set up a RSU configuration as described in Section 5.2.2.3, without connecting the GPS receiver. Execute the RSU initialization procedure in Table 5-2 without launching the Ethereal or TrafSigSim applications.
2. Set up an OBU configuration as described in Section 5.2.2.2 (without the GPS receiver connected) and execute the OBU initialization procedure in Table 5-1.

5.4.2.1 Vehicle Bus Interface Low-Value Tests

1. Start an Ethereal session on the OBU HD to log Ethernet activity between the HD and the WRM.
2. Use the VBusSim to set the Vehicle Velocity settings as indicated in Table 5-38 and use PCAN to verify the Vehicle Velocity settings.
   Table 5-39 and use PCAN to verify the Vehicle Acceleration settings.
3. Use VBusSim to set the Vehicle Devices settings as indicated in Table 5-40 and use PCAN to verify the Vehicle Devices settings.

4. On the T9App main screen for both RSU and OBU, select start testing. Allow the test to run for a minimum of 10 seconds and then stop testing.
5. Stop recording Ethernet activity on Ethereal.
6. Review the T9App GUI on both the OBU and RSU to verify the displayed values match the expected GUI values in Table 5-41 and record the results.
7. Open the T9App log file on the OBU HD and verify the logged values in the OBUTX entries match the expected OBU log values in Table 5-41. Verify the vehicle speed is also logged in the RSURX entries as the receiver information. Record the results.
8. Use Ethereal (on the OBU HD) to view the IP data fields indicated in Table 5-42 and record the values in Table 5-41. Verify the Ethereal values match the expected values in Table 5-41.
9. Open the T9App log file on the RSU HD and verify the logged values in the OBURX entries match the expected RSU log values in Table 5-41. Record the results.

Table 5-38. Vehicle Velocity Settings (Low-Value)

			PCAN Results			
			Expected		Actual	
Parameter	**Setting**	**Availability Indicator**	**Setting**	**Availability Indicator**	**Setting**	**Availability Indicator**
Vehicle Speed	0	1	0	1	0	1
Yaw Rate	-179.999	1	0xB9B1	1	0xB9B1	1

Table 5-39. Vehicle Acceleration Settings (Low-Value)

			PCAN Results			
			Expected		Actual	
Parameter	**Setting**	**Availability Indicator**	**Setting**	**Availability Indicator**	**Setting**	**Availability Indicator**
Lateral Acceleration	-2.05	1	0xF7FE	1	0xF7FE	1
Longitudinal Acceleration	-2.05	1	0xF7FE	1	0xF7FE	1

Table 5-40. Vehicle Devices Settings (Low-Value)

Parameter	Setting	Availability Indicator	PCAN Results			
			Expected		Actual	
			Setting	Availability Indicator	Setting	Availability Indicator
Throttle Position	0	1	0	1	0	1
Brake Applied Status	0	1	0	1	0	1
Brake Applied Pressure	0	1	0	1	0	1
Steering Wheel Angle	-179.98	1	0xB9B2	1	0xB9B2	1
Headlights	0	1	0	1	0	1
Turn Signal/Hazard Signal	0	1	0	1	0	1
Traction Control State	0	1	0	1	0	1
Anti-Lock Brake State	0	1	0	1	0	1
System Health	0	1	0	1	0	1

Table 5-41. Vehicle Interface Low-Value Test Results

Parameter	Expected Results			Actual Results				
	GUI	Log	Ethereal	OBU GUI	OBU Log	Ethereal	RSU GUI	RSU Log
Vehicle Speed	0 m/s	0	0		0	0	0	0
Yaw Rate	N/A	-179.99	0xB9B1	N/A	-179.99	0xb9b1	N/A	-179.99
Lateral Acceleration	N/A	-2.05	0xF33	N/A	-2.04	0xF34	N/A	-2.04
Longitudinal Acceleration	N/A	-2.05	0xF33	N/A	-2.04	0xF34	N/A	-2.04
Throttle Position	N/A	0	0	N/A	0	0	N/A	0
Brake Applied Status	N/A	0	0	N/A	0	0	N/A	0
Brake Applied Pressure	N/A	0	0	N/A	0	0	N/A	0
Steering Wheel Angle	N/A	-179.98	0xDCD9	N/A	-179.98	0xdcd9	N/A	-179.98
Headlights	N/A	0	0	N/A	0	0	N/A	0
Turn Signal/Hazard Signal	N/A	0	0	N/A	0	0	N/A	0
Traction Control State	N/A	0	0	N/A	0	0	N/A	0
Anti-Lock Brake State	N/A	0	0	N/A	0	0	N/A	0
System Health	N/A	0	0	N/A	0	0	N/A	0

Table 5-42. OBU V2V Safety Message Vehicle Data Elements

Data Element	Length (bits)	IP Data Frame Byte #	IP Data Frame Bits
Vehicle Speed	16	56	1-8
		57	1-8
Lateral Acceleration	12	58	1-8
		59	1-4
Longitudinal Acceleration	12	59	5-8
		60	1-8
Yaw Rate	16	61-62	All
Throttle Position	8	63	1-8
Brake Applied Status	4	64	5-8
Brake Applied Pressure	4	64	1-4
Steering Wheel Angle	16	65-66	All
Headlights	2	67	7-8
Turn Signal/Hazard Signal	2	67	5-6
Traction Control State	2	67	3-4
Anti-lock Brake State	2	67	1-2
System Health	4	68	1-4

5.4.2.2 Vehicle Bus Interface Mid-Value Tests

1. Repeat steps 1-6 of section 5.4.2.1, using the Vehicle Velocity settings in Table 5-43, the Vehicle Acceleration settings in Table 5-44, and the Vehicle Devices settings in Table 5-45.
2. Repeat steps 7-10 of section 5.4.2.1, verifying the values and recording the results in Table 5-46.

Table 5-43. Vehicle Velocity Settings (Mid-Value)

Parameter	Setting	Availability Indicator	PCAN Results			
			Expected		Actual	
			Setting	Availability Indicator	Setting	Availability Indicator
Vehicle Speed	2.55	1	0x00FF	1	0x00FF	1
Yaw Rate	2.55	1	0x00FF	1	0x00FF	1

Table 5-44. Vehicle Acceleration Settings (Mid-Value)

Parameter	Setting	Availability Indicator	PCAN Results			
			Expected		Actual	
			Setting	Availability Indicator	Setting	Availability Indicator
Lateral Acceleration	0	1	0x0000	1	0x0000	1
Longitudinal Acceleration	0	1	0x0000	1	0x0000	1

Table 5-45. Vehicle Devices Settings (Mid-Value)

Parameter	Setting	Availability Indicator	PCAN Results			
			Expected		Actual	
			Setting	Availability Indicator	Setting	Availability Indicator
Throttle Position	7.5	1	0x0F	1	0x0F	1
Brake Applied Status	1	1	0x1	1	0x1	1
Brake Applied Pressure	7	1	0x7	1	0x7	1
Steering Wheel Angle	0	1	0x0000	1	0x0000	1
Headlights	1	1	0x1	1	0x1	1
Turn Signal/Hazard Signal	1	1	0x1	1	0x1	1
Traction Control State	1	1	0x1	1	0x1	1
Anti-Lock Brake State	1	1	0x1	1	0x1	1

Table 5-46. Vehicle Interface Mid-Value Test Results

Parameter	Expected Results			Actual Results				
	GUI	Log	Ethereal	Tx GUI	Tx Log	Ethereal	Rx GUI	Rx Log
Vehicle Speed	2.55 m/s	255	0x00FF	2.55	2.55	00FF	2.55	2.55
Yaw Rate	2.55 m/s	255	0x00FF	N/A	2.55	00FF	N/A	2.55
Lateral Acceleration	N/A	0	0x000	N/A	0	000	N/A	0
Longitudinal Acceleration	N/A	0	0x000	N/A	0	000	N/A	0
Throttle Position	N/A	7.5	0x0F	N/A	7.5	0F	N/A	7.5
Brake Applied Status	N/A	1	0x1	N/A	1	1	N/A	1
Brake Applied Pressure	N/A	7	0x7	N/A	7	7	N/A	7
Steering Wheel Angle	N/A	0	0x0000	N/A	0	0000	N/A	0
Headlights	N/A	1	0x1	N/A	1	1	N/A	1
Turn Signal/Hazard Signal	N/A	1	0x1	N/A	1	1	N/A	1
Traction Control State	N/A	1	0x1	N/A	1	1	N/A	1
Anti-Lock Brake State	N/A	1	0x1	N/A	1	1	N/A	1

5.4.2.3 Vehicle Bus Interface High-Value Tests

1. Repeat steps 1-6 of section 5.4.2.1, using the Vehicle Velocity settings in Table 5-47, the Vehicle Acceleration settings in Table 5-48, and the Vehicle Devices settings in Table 5-49.
2. Repeat steps 7-10 of section 5.4.2.1, verifying the values and recording the results in Table 5-50.

Table 5-47. Vehicle Velocity Settings (High-Value)

Parameter	Setting	Availability Indicator	PCAN Results			
			Expected		Actual	
			Setting	Availability Indicator	Setting	Availability Indicator
Vehicle Speed	655.35	1	0xFFFF	1	0xFFFF	1
Yaw Rate	179.99	1	0x464F	1	0x464F	1

Table 5-48. Vehicle Acceleration Settings (High-Value)

Parameter	Setting	Availability Indicator	PCAN Results			
			Expected		Actual	
			Setting	Availability Indicator	Setting	Availability Indicator
Lateral Acceleration	2.04	1	0x07F8	1	0x07F8	1
Longitudinal Acceleration	2.04	1	0x07F8	1	0x07F8	1

Table 5-49. Vehicle Devices Settings (High-Value)

Parameter	Setting	Availability Indicator	PCAN Results			
			Expected		Actual	
			Setting	Availability Indicator	Setting	Availability Indicator
Throttle Position	100	1	0xC8	1	0xC8	1
Brake Applied Status	2	1	0x2	1	0x2	1
Brake Applied Pressure	15	1	0xF	1	0xF	1
Steering Wheel Angle	179.98	1	0x464E	1	0x464E	1
Headlights	2	1	0x2	1	0x2	1
Turn Signal/Hazard Signal	2	1	0x2	1	0x2	1
Traction Control State	2	1	0x2	1	0x2	1
Anti-Lock Brake State	2	1	0x2	1	0x2	1

Table 5-50. Vehicle Interface High-Value Test Results

Parameter	Expected Results			Actual Results				
	GUI	Log	Ethereal	Tx GUI	Tx Log	Ethereal	Rx GUI	Rx Log
Vehicle Speed	655.35 m/s	655.35	0xFFFF	655.35	655.35	0xFFFF	655.35	655.35
Yaw Rate	N/A	179.99	0x464F	N/A	179.99	0x464F	N/A	179.99
Lateral Acceleration	N/A	2.047	0x0CC	N/A	2.04	0x0CC	N/A	2.04
Longitudinal Acceleration	N/A	2.047	0x0CC	N/A	2.04	0x0CC	N/A	2.04
Throttle Position	N/A	100	0xC8	N/A	100	0xC8	N/A	100
Brake Applied Status	N/A	2	0x2	N/A	2	0x2	N/A	2
Brake Applied Pressure	N/A	15	0xF	N/A	15	0xF	N/A	15

Parameter	Expected Results			Actual Results				
	GUI	Log	Ethereal	Tx GUI	Tx Log	Ethereal	Rx GUI	Rx Log
Steering Wheel Angle	N/A	179.98	0x2327	N/A	179.98	0x2327	N/A	179.98
Headlights	N/A	2	0x2	N/A	2	0x2	N/A	2
Turn Signal/Hazard Signal	N/A	2	0x2	N/A	2	0x2	N/A	2
Traction Control State	N/A	2	0x2	N/A	2	0x2	N/A	2
Anti-Lock Brake State	N/A	2	0x2	N/A	2	0x2	N/A	2

5.4.2.4 Vehicle Bus Interface Discrete-Value Tests

1. Repeat steps 1, 2, 5, & 6 of section 5.4.2.1, using the Vehicle Devices settings in Table 5-51.
2. Repeat steps 7-10 of section 5.4.2.1, verifying the values and recording the results in Table 5-52.

Table 5-51. Vehicle Devices Settings

Parameter	Setting	Availability Indicator	PCAN Results			
			Expected		Actual	
			Setting	Availability Indicator	Setting	Availability Indicator
Brake Applied Status	4	1	0x4	1	0x4	1
Headlights	3	1	0x3	1	0x3	1
Turn Signal/Hazard Signal	3	1	0x3	1	0x3	1
Traction Control State	3	1	0x3	1	0x3	1
Anti-Lock Brake State	3	1	0x3	1	0x3	1

Table 5-52. Vehicle Interface Test Results

Parameter	Expected Results		Actual Results		
	Log	Ethereal	Tx Log	Ethereal	Rx Log
Brake Applied Status	4	0x4	4	0x4	4
Headlights	3	0x3	3	0x3	3
Turn Signal/Hazard Signal	3	0x3	3	0x3	3
Traction Control State	3	0x3	3	0x3	3
Anti-Lock Brake State	3	0x3	3	0x3	3

3. Repeat steps 1, 2, 5, & 6 of section 5.4.2.1, using the Vehicle Devices setting in Table 5-53.
4. Repeat steps 7-10 of section 5.4.2.1, verifying the values and recording the results in Table 5-54.

Table 5-53. Vehicle Devices Settings

Parameter	Setting	Availability Indicator	PCAN Results			
			Expected		Actual	
			Setting	Availability Indicator	Setting	Availability Indicator
Brake Applied Status	8	1	0x8	1	0x8	1

Table 5-54. Vehicle Interface Test Results

Parameter	Expected Results		Actual Results		
	Log	Ethereal	Tx Log	Ethereal	Rx Log
Brake Applied Status	8	0x8	8	0x8	8

5. Repeat steps 1, 2, 5, and 6 of section 5.4.2.1, using the Vehicle Devices setting in Table 5-55.
6. Repeat steps 7-10 of section 5.4.2.1, verifying the values and recording the results in Table 5-56.

Table 5-55. Vehicle Devices Settings

Parameter	Setting	Availability Indicator	PCAN Results			
			Expected		Actual	
			Setting	Availability Indicator	Setting	Availability Indicator
Brake Applied Status	15	1	0xF	1	0xF	1

Table 5-56. Vehicle Interface Test Results

Parameter	Expected Results		Actual Results		
	Log	Ethereal	Tx Log	Ethereal	Rx Log
Brake Applied Status	15	0xF	F	0xF	F

5.4.3 Traffic Signal Interface Tests

5.4.3.1 Initialization/Polling Test

1. Set up a RSU configuration as described in Section 5.2.2.3 and execute the RSU initialization procedure in Table 5-2.

Fast Polling Test

1. On the T9App Comm Parameters screen, set the traffic signal polling interval to 100 milliseconds.
2. On the T9App main screen, select start testing.
3. On the TrafSigSim screen, verify it receives the 22 byte initialization sequence:
   04 41 30 31 05 10 02 55 25 01 01 10 03 17 51 04 61 30 31 05 10 30
4. Verify the TrafSigSim responds with 10 30 10 31 followed by the specified amount of other data.
5. Verify the TrafSigSim receives nothing for at least a full second.
6. Verify the TrafSigSim receives a periodic polling query of: 04 61 30 31 05 10 30, and responds with a traffic signal message (contents to be verified in other tests).
7. Stop the test on the T9App.

Table 5-57. Traffic Signal Long Initial Response, Fast Polling Results

	TrafSigSim Results	
Parameter	**Expected**	**Actual**
Initialization Sequence	See step 3.	Passed. Received expected results
Initialization Response	See step 4. (83 bytes of other data may follow.)	Passed. TrafSigSim responded with 10 30 10 31. No additional data followed the initialization response.
Delay between receiving initialization and polling sequence	≥ 1 second.	Passed. Delay ~= 1 second
Polling query	See step 6.	Passed. Received periodic query
Polling interval	~100 milliseconds	Passed. Polling rate is ~100 ms.

Slow Polling Test

1. On the T9App Comm Parameters screen, set the traffic signal polling interval to 1000 milliseconds.
2. Repeat steps 2-7 of Section 5.4.3.1 and record the results in Table 5-58.
3. Reset the T9App traffic signal polling interval to 100 milliseconds.

Table 5-58. Short Initial Response, Slow Polling Results

	TrafSigSim Results	
Parameter	**Expected**	**Actual**
Initialization Sequence	See Section 5.4.3.1, step 3.	Passed.
Initialization Response	See Section 5.4.3.1, step 4 followed by 0 bytes of other data.	Passed. TrafSigSim responded with 10 30 10 31. No additional data followed the initialization response.
Delay between receiving initialization and polling sequence	$\geq$ 1 second.	Passed. Delay ~= 1 second
Polling query	See Section 5.4.3.1, step 6.	Passed. Received periodic query
Polling interval	~1000 milliseconds	Passed. Polling rate is ~1000 ms

5.4.3.2 Traffic Signal Message Processing

1. Set up a RSU configuration as described in Section 5.2.2.3 (without the GPS receiver connected) and execute the RSU initialization procedure in Table 5-2.
2. Set up an OBU configuration as described in Section 5.2.2.2 and execute the OBU initialization procedure in Table 5-1.

Traffic Signal Message, Active Phase 1 and 5

1. Configure the TrafSigSim parameters and verify the results as shown in

Table 5-59.

2. Start an Ethereal session to log Ethernet activity between the HD and the WRM on the RSU HD.
3. On the T9App main screen for both the RSU and OBU, select start testing.
4. Allow the test to run for a minimum of 5 seconds, and then stop testing on both the RSU and OBU.
5. Stop recording Ethernet activity on Ethereal.
6. Open the T9App log file on the RSU (Tx) and OBU (Rx) side. Verify the logged values match the Log values in Table 5-60 and record the results.
7. Use Ethereal (on the RSU HD) to view the RSU Traffic Signal Message IP data fields listed in Table 5-61 and record the values in Table 5-60. Verify the Ethereal values match the expected values in Table 5-60.

Table 5-59. Traffic Signal Active Phase 1 and 5 Parameters

Parameter	Setting	TrafSig Results			
		Expected		Actual	
		Byte	Value	Byte	Value
State of active phase on ring 1	Green	5	0x00	5	0x00
State of active phase on ring 2	Green	25	0x00	25	0x00
Active Phases	1, 5	44	0x11	44	0x11
Seconds left in the currently active phase of ring 1	1	12	0x01	12	0x01
Seconds left in the currently active phase of ring 2	1	32	0x01	32	0x01

Table 5-60. Traffic Signal Active Phase 1 and 5 Results

Parameter	Expected Results		Actual Results		
	Log	Ethereal	Tx Log	Ethereal	Rx Log
Current State of Traffic Light at Stop Loc 1 (Phase 1)	0	0x00	0	Byte 67= 0x00	0
Time Left in Current State at Stop Loc 1	1.000	0x03E8	1	Byte 68/69 = 0x03e8	1
Current State of Traffic Light at Stop Loc 2 (Phase 3)	3	0x03	3	Byte 85 = 0x03	3
Time Left in Current State at Stop Loc 2	0	0x0000	0	Byte 86/87 = 0x0000	0
Current State of Traffic Light at Stop Loc 3 (Phase 6)	3	0x03	3	Byte 103 = 0x03	3
Time Left in Current State at Stop Loc 3	0	0x0000	0	Byte 104/105 = 0x0000	0
Current State of Traffic Light at Stop Loc 4 (Phase 8)	3	0x03	3	Byte 121 = 0x03	3
Time Left in Current State at Stop Loc 4	0	0x0000	0	Byte 122/123 = 0x0000	0

Table 5-61. RSU Traffic Signal Message Data Elements

Data Element	Length (bits)	IP Data Frame Byte #	IP Data Frame Bits
Current State of Traffic Light at Stop Loc 1	8	67	All
Time Left in Current State at Stop Loc 1	16	68-69	All
Current State of Traffic Light at Stop Loc 2	8	85	All
Time Left in Current State at Stop Loc 2	16	86-87	All
Current State of Traffic Light at Stop Loc 3	8	103	All

Data Element	Length (bits)	IP Data Frame Byte #	IP Data Frame Bits
Time Left in Current State at Stop Loc 3	16	104-105	All
Current State of Traffic Light at Stop Loc 4	8	121	All
Time Left in Current State at Stop Loc 4	16	122-123	All

Traffic Signal Message, Active Phase 2 and 6

1. Repeat step 1 of Section 5.4.3.2, using the Traffic Signal settings in Table 5-62.
2. Repeat steps 2-7 of Section 5.4.3.2, verifying the values and recording the results in Table 5-63.

Table 5-62. Traffic Signal Active Phase 2 and 6 Parameters

Parameter	Setting	TrafSig Results			
		Expected		Actual	
		Byte	Value	Byte	Value
State of active phase on ring 1	Yellow	5	0x02	5	0x02
State of active phase on ring 2	Yellow	25	0x02	25	0x02
Active Phases	2, 6	44	0x22	44	0x22
Seconds left in the currently active phase of ring 1.	20	12	0x14	12	0x14
Seconds left in the currently active phase of ring 2.	20	32	0x14	32	0x14

Table 5-63. Traffic Signal Active Phase 2 and 6 Results

Parameter	Expected Results		Actual Results		
	Log	Ethereal	Tx Log	Ethereal	Rx Log
Current State of Traffic Light at Stop Loc 1 (Phase 1)	3	0x03	3	Byte 67= 0x03	3
Time Left in Current State at Stop Loc 1	0	0x0000	0	Byte 68/69 = 0x0000	0
Current State of Traffic Light at Stop Loc 2 (Phase 3)	3	0x03	3	Byte 85 = 0x03	3
Time Left in Current State at Stop Loc 2	0	0x0000	0	Byte 86/87 = 0x0000	0
Current State of Traffic Light at Stop Loc 3 (Phase 6)	2	0x02	2	Byte 103 = 0x02	2
Time Left in Current State at Stop Loc 3	20.000	0x4E20	20	Byte 104/105 = 0x4E20	20

Parameter	Expected Results		Actual Results		
	Log	Ethereal	Tx Log	Ethereal	Rx Log
Current State of Traffic Light at Stop Loc 4 (Phase 8)	3	0x03	3	Byte 121 = 0x03	3
Time Left in Current State at Stop Loc 4	0	0x0000	0	Byte 122/123 = 0x0000	0

Traffic Signal Message, Active Phase 3 and 7

1. Repeat step 1 of Section 5.4.3.2, using the Traffic Signal settings in Table 5-64.
2. Repeat steps 2-7 of Section 5.4.3.2, verifying the values and recording the results in Table 5-65.

Table 5-64. Traffic Signal Active Phase 3 and 7 Parameters

Parameter	Setting	TrafSig Results			
		Expected		Actual	
		Byte	Value	Byte	Value
State of active phase on ring 1	Green	5	0x00	5	0x00
State of active phase on ring 2	Green	25	0x00	25	0x00
Active Phases	3, 7	44	0x44	44	0x44
Seconds left in the currently active phase of ring 1.	40	12	0x28	12	0x28
Seconds left in the currently active phase of ring 2.	40	32	0x28	32	0x22

Table 5-65. Traffic Signal Active Phase 3 and 7 Results

Parameter	Expected Results		Actual Results		
	Log	Ethereal	Tx Log	Ethereal	Rx Log
Current State of Traffic Light at Stop Loc 1 (Phase 1)	3	0x03	3	Byte 67= 0x03	3
Time Left in Current State at Stop Loc 1	0	0x0000	0	Byte 68/69 = 0x0000	0
Current State of Traffic Light at Stop Loc 2 (Phase 3)	0	0x00	0	Byte 85 = 0x00	0
Time Left in Current State at Stop Loc 2	40.000	0x9C40	40	Byte 86/87 = 0x9C40	40
Current State of Traffic Light at Stop Loc 3 (Phase 6)	3	0x03	3	Byte 103 = 0x03	3
Time Left in Current State at Stop Loc 3	0	0x0000	0	Byte 104/105 = 0x0000	0

Parameter	Expected Results		Actual Results		
	Log	Ethereal	Tx Log	Ethereal	Rx Log
Current State of Traffic Light at Stop Loc 4 (Phase 8)	3	0x03	3	Byte 121 = 0x03	3
Time Left in Current State at Stop Loc 4	0	0x0000	0	Byte 122/123 = 0x0000	0

Traffic Signal Message, Active Phase 4 and 8

1. Repeat step 1 of Section 5.4.3.2, using the Traffic Signal settings in Table 5-66.
2. Repeat steps 2-7 of Section 5.4.3.2, verifying the values and recording the results in Table 5-67.

Table 5-66. Traffic Signal Active Phase 4 and 8 Parameters

Parameter	Setting	TrafSig Results			
		Expected		Actual	
		Byte	Value	Byte	Value
State of active phase on ring 1	Yellow	5	0x02	5	0x02
State of active phase on ring 2	Yellow	25	0x02	25	0x02
Active Phases	4,8	44	0x88	44	0x88
Seconds left in the currently active phase of ring 1.	65	12	0x41	12	0x41
Seconds left in the currently active phase of ring 2.	65	32	0x41	32	0x41

Table 5-67. Traffic Signal Active Phase 4 and 8 Results

Parameter	Expected Results		Actual Results		
	Log	Ethereal	Tx Log	Ethereal	Rx Log
Current State of Traffic Light at Stop Loc 1 (Phase 1)	3	0x03	3	Byte 67= 0x03	3
Time Left in Current State at Stop Loc 1	0	0x0000	0	Byte 68/69 = 0x0000	0
Current State of Traffic Light at Stop Loc 2 (Phase 3)	3	0x03	3	Byte 85 = 0x03	3
Time Left in Current State at Stop Loc 2	0	0x0000	0	Byte 86/87 = 0x0000	0
Current State of Traffic Light at Stop Loc 3 (Phase 6)	3	0x03	3	Byte 103 = 0x03	3
Time Left in Current State at Stop Loc 3	0	0x0000	0	Byte 104/105 = 0x0000	0

Parameter	Expected Results		Actual Results		
	Log	Ethereal	Tx Log	Ethereal	Rx Log
Current State of Traffic Light at Stop Loc 4 (Phase 8)	65.000	0x00	2	Byte 121 = 0x02	2
Time Left in Current State at Stop Loc 4	0	0x0FDE8	65	Byte 122/123 = 0xFDE8	65

5.5 Requirement/Test Cross Reference Matrix

5.5.1 Task 9 Software Requirement Verification

These are a summary of requirements gleaned from Chapter 2.

Table 5-68. Task 9 Software Requirement Cross Reference

Section Number	Requirement	Test Procedure
3	The Task 9 software shall have the capability to run one application at a time with the Task 9 device being configurable to easily choose amongst a set of preloaded applications. The On-board Unit (OBU) Test application will be used in a vehicle and will wirelessly broadcast vehicle parameters and decode incoming packets containing surrounding vehicle parameters. The Roadside Unit (RSU) Test application will be used near a roadway infrastructure device such as a traffic signal and will broadcast traffic signal information.	All tests, by inspection.
3.1 OBU Application Requirements		
3.1.1	In the OBU Test application, the Task 9 device shall use a Controller Area Network (CAN) bus to receive messages with vehicle information such as vehicle speed, brake position, acceleration, etc.	5.4.2
3.1.2	The OBU Test application shall periodically issue commands to the WRM to transmit the latest GPS and vehicle information wirelessly.	5.4.1.2
3.1.2	The periodicity of the transmitted information shall be adjustable through the control user interface and shall allow periods at least as small as 10 milliseconds.	5.3.2
3.2 RSU Application Requirements		
3.2.1	The RSU Test application shall decode traffic signal information from an RS-232 connection.	5.4.3
3.2.2	The RSU Test application shall periodically issue commands to the WRM to transmit traffic signal information wirelessly.	5.3.2
3.2.2	The periodicity of the transmitted information shall be adjustable through the control user interface and shall allow periods at least as small as 10 milliseconds.	5.3.2
3.2.3.1	The RSU Test application shall be configurable so that the user has the capability to modify constant parameters for the traffic signal information.	5.3.4

Section Number	Requirement	Test Procedure
3.3 OBU and RSU Test Common Requirements		
3.3.1	In the OBU Test application, the Task 9 device shall use an RS-232 port to receive ASCII messages formatted in the National Maritime Electronics Association (NMEA) 0183 standard. The application shall parse these messages to get the GPS data required in other parts of this document.	5.4.1.2
3.3.3	In addition to the data content sent from the OBU Test and RSU Test applications, each data packet shall also contain the following:	(N/A)
	Sender ID (either preset OR randomized at start of test)	5.3.2
	Common *Message ID* (to be defined by VSCC members)	5.3.1
	Message Count (incrementing short unsigned integer)	5.3.3
	Broadcast Power	5.3.1
	Operating System Time (nanoseconds)	5.3.1
	State of Data Logging (i.e., logging active, logging inactive)	5.3.3
	Latitude, Longitude, Height (ellipsoidal)	5.4.1.1
	GPS Seconds in Week (conversion from UTC time to GPS Seconds in Week)(set *GPS Seconds in Week* to zero for devices with no GPS receiver attached)	5.4.1.1
	Heading (from GPS receiver)	5.4.1.1
3.3.4	By default, the Task 9 device shall record all data sent and all data received from surrounding devices via the WRM.	5.3, 5.4
3.3.4	In addition, the Task 9 device shall record reception parameters, timing, and statistics associated with each data packet. The recorded reception parameters include:	(N/A)
	Receiver Signal Strength Indicator (*RSSI*)	5.3.1
	Distance to Sender (using valid GPS coordinates of sender and receiver)	5.3.5.1
	Heading to Sender (using valid GPS coordinates of sender and receiver)	5.3.5.3
	Current *GPS Seconds in Week* of receiver	5.4.1
	Latitude, Longitude, Height (ellipsoidal) of receiver	5.4.1
	Heading (from GPS receiver)	5.4.1
	Speed (meters/second, via CAN from host vehicle if receiver)	5.4.2
3.3.4	All parameters controllable from the control user interface shall be recorded.	5.3.6
3.3.5.1	The applications shall retain the value of all parameters controllable from the control user interface during a “normal” power cycle.	5.3.6
3.3.5.1	The control user interface shall allow the user to configure the applications to transmit wirelessly through the WRM upon application execution. This implies the application will also be decoding CAN and/or serial data as appropriate for the application.	5.3, 5.4
3.3.5.1	The control user interface shall allow the user to adjust all WRM communication parameters described in the WRM interface specification.	Tested in Task 6D
3.3.5.1	The control user interface shall display the IP address of the Task 9 device at the Ethernet port connected to the WRM.	5.3.2

Section Number	Requirement	Test Procedure
3.3.5.1	The OBU Test and RSU Test applications shall each provide a display for configuring the communication parameters. The display shall allow the user to adjust the following communication parameters inherent to the application: Periodicity of message transmission Size of message being transmitted (append data to standard message using same message ID) Destination IP address (as a default, this should be the broadcast IP address)	5.3.2
3.3.5.1	The OBU Test and RSU Test applications shall have the ability to initiate, suspend, or terminate a test. The test shall consist of the OBU Test or RSU Test applications transmitting and recording data as described in previous sections.	5.3.2
3.3.5.1	The length of the test shall be controllable via the control user interface. The user shall be able to control the length of the test by specifying the number of packets sent or the number of seconds of test time. During a test, the Task 9 device shall record data as outlined in sections above.	5.3.3
3.3.5.1	The OBU Test and RSU Test applications shall have the ability to specify a filename for recorded test data. The format for the filename shall be <Test Name>_<Test Run>_<GPS Date> where: <Test Name> is a field entered by the user <Test Run> is an automatically incrementing number incremented after a test has ended (i.e., terminated by the user, maximum number off packet sent, test time exceeded) <GPS Date> is derived from the local GPS information.	5.3.3
3.3.5.1	The OBU Test and RSU Test applications shall each have an active visual display that shows other Task 9 devices that have communicated with the host Task 9 device. The display shall support at least 10 other Task 9 devices and update the information displayed at least once per second. The text on the display should be easily readable in a vehicular environment.	5.3.5
3.3.5.1	For each device, the following shall be displayed:	(N/A)
	Sender ID	5.3.2
	State of Data Logging (Requirement deleted during Denso/VSCC Telecon)	N/A
	Most recent *Message Count*	5.3.3
	Distance to Sender	5.3.5.1
	Relative Heading to Sender = *Heading to Sender* (from GPS differencing) – *Heading* (only to be calculated when host vehicle speed > 5 m/s)	5.3.5.3
	RSSI	5.3.1
	Speed	5.4.2

5.5.2 Common Message Header Verification

Table 5-69. Common Message Header Field Verification

Field Name	Verification Test
Packet Length	5.3.2
GPS Seconds in Week	5.4.1.1
GPS Longitude	5.4.1.1
GPS Latitude	5.4.1.1
GPS Altitude	5.4.1.1
GPS Heading	5.4.1.1
Sender ID	5.3.2
Message Count	5.3.2
Log	5.3.2
Tx Power	5.3.1
OS Time	5.3.1

5.5.3 OBU Message Verification

Table 5-70. OBU Message Verification

Field Name	Verification Test
Message Type	5.3.1
Temporary ID	5.3.1
Precision Indicator	N/A
Longitude of center of vehicle	5.4.1.2
Latitude of center of vehicle	5.4.1.2
Altitude of center of vehicle	5.4.1.2
UTC Time	5.4.1.2
Heading	5.4.1.2
Vehicle Speed	5.4.2
Lateral Acceleration	5.4.2
Longitudinal Acceleration	5.4.2
Yaw Rate	5.4.2
Throttle Position	5.4.2
Brake Applied Status	5.4.2
Brake Applied Pressure	5.4.2
Steering Wheel Angle	5.4.2

Field Name	Verification Test
Headlights	5.4.2
Turn Signal/Hazard Signal	5.4.2
Traction Control State	5.4.2
Anti-Lock Brake State	5.4.2
Vehicle Length	N/A
Vehicle Width	N/A

5.5.4 RSU Message Verification

Table 5-71. RSU Message Verification

Field Name	Verification Test
Message ID	5.3.1
Temporary ID	5.3.1
Precision Indicator	N/A
Longitude of RSU GPS Antenna	5.3.4, 0
Latitude of RSU GPS Antenna	5.3.4, 0
Altitude of RSU GPS Antenna	5.3.4, 0
UTC Time	5.4.1.3
Longitude of Stopping Location # 1	5.3.4
Latitude of Stopping Location # 1	5.3.4
Altitude of Stopping Location # 1	5.3.4
Directionality of Stopping Location # 1	5.3.4
Current State of Traffic Light at Stopping Location # 1	5.4.3.2
Time Left in Current State of Traffic Light at Stopping Location # 1	5.4.3.2
Duration of Yellow State at Stopping Location # 1	5.3.4
Longitude of Stopping Location # 2	5.3.4
Latitude of Stopping Location # 2	5.3.4
Altitude of Stopping Location # 2	5.3.4
Directionality of Stopping Location # 2	5.3.4
Current State of Traffic Light at Stopping Location # 2	5.4.3.2
Time Left in Current State of Traffic Light at Stopping Location # 2	5.4.3.2
Duration of Yellow State at Stopping Location # 2	5.3.4
Longitude of Stopping Location # 3	5.3.4
Latitude of Stopping Location # 3	5.3.4
Altitude of Stopping Location # 3	5.3.4
Directionality of Stopping Location # 3	5.3.4

Field Name	Verification Test
Current State of Traffic Light at Stopping Location # 3	5.4.3.2
Time Left in Current State of Traffic Light at Stopping Location # 3	5.4.3.2
Duration of Yellow State at Stopping Location # 3	5.3.4
Longitude of Stopping Location # 4	5.3.4
Latitude of Stopping Location # 4	5.3.4
Altitude of Stopping Location # 4	5.3.4
Directionality of Stopping Location # 4	5.3.4
Current State of Traffic Light at Stopping Location # 4	5.4.3.2
Time Left in Current State of Traffic Light at Stopping Location # 4	5.4.3.2
Duration of Yellow State at Stopping Location # 4	5.3.4

6 Appendix

6.1 Terms, Acronyms, and Abbreviations

Acronym	Definition
API	Application Programming Interface
ATP	Acceptance Test Plan
CAN	Controller Area Network
Comm	Communication
CTS	Clear to Send
DB	Decibel
DBi	Decibel Isotropic
DBm	Decibel Milliwatts
DBm	Decibel Milliwatts
Deg	Degrees
deg/sec	Degrees per Second
DGPS	Differential GPS
DLL	Dynamic Link Library
GPGGA	Global Positioning System Fix Data
GPRMC	Global Positioning Recommended Minimum Specific GPS/Transit Data
GPS	Global Positioning System
GPVTG	Global Positioning Track Made Good and Ground Speed
GPZDA	Global Positioning UTC Date / Time and Local Time Zone Offset
GUI	Graphical User Interface
HD	Host Device
I/F	Interface
IP	Internet Protocol
Kbps	Kilobits per Second
Lsb	Least Significant Bit
LSB	Least Significant Byte
LSBit	Least Significant Bit
LSByte	Least Significant Byte
LSNybble	Least Significant Nybble
M	Meters

Acronym	Definition
m/s	Meters per Second
MAC	Medium Access Control
Mbps	Megabits per Second
MFC	Microsoft Foundation Class
MHz	Megahertz
Ms	Milliseconds
MSB	Most Significant Byte
MSByte	Most Significant Byte
Msec	Milliseconds
N/A	Not Applicable
NMEA	National Maritime Electronics Association
OBU	On Board Unit
OBURX	On Board Unit Receive Log Entry
OBUTX	On Board Unit Transmit Log Entry
OS	Operating System
PCAN	Peak System Controller Area Network Software
PCAP	Packet Capture
RSSI	Received Signal Strength Indicator
RSU	Road Side Unit
RSURX	Road Side Unit Receive Log Entry
RTS	Request to Send
Rx	Receive
RXUTX	Road Side Unit Transmit Log Entry
SAE	Society of Automotive Engineers
Sec	Seconds
STD	Standard
Stop Loc	Stopping Location
T9App	Task 9 Application
TCP	Transport Control Protocol
TrafSigSim	Traffic Signal Simulator
Tx	Transmit
UML	Unified Modeling Language
USB	Universal Serial Bus
UTC	Coordinated Universal Time
UTC	Universal Coordinated Time

Acronym	Definition
V2V	Vehicle to Vehicle
VBusSim	Vehicle Bus Simulator
VSC	Vehicle Safety Communications
VSCC	Vehicle Safety Communications Consortium
WAVE	Wireless Access in Vehicular Environments
WRM	WAVE Radio Module

6.2 References

[1] NMEA 0183 Interface Standard, dated January 2002.

[2] Chapter 5, Vehicle Safety Communications Project, Task 6D: WAVE Radio Module, Final Task Report, September 27, 2004.

6.3 Task 9 device CAN input messages

This appendix outlines the CAN messages that the OBU Test application shall decode.

Parameters for the physical setup and messages will be:

- ISO 11898 Physical Layer
- 500 kilobits/second
- Standard 11-bit message IDs (not extended 29-bit)
- All signed values are twos-complement unless otherwise noted.

6.3.1 Vehicle Velocity Message

Message ID: 300 (hexadecimal)

Data Bytes: 8

Bit / Byte	8	7	6	5	4	3	2	1(lsb)
1	Vehicle Speed MSByte							
2	Vehicle Speed LSByte (LSBit = 0.01 m/s; unsigned)							
3	Yaw Rate MSByte							
4	Yaw Rate LSByte (LSBit = 0.01 deg/sec; signed)							
5	Unused						Signal Availability Indicator (See Below)	

Byte 5:

Depending on Vehicle/Application some signals might not be available. A '1' indicates the signal is available and valid. A '0' indicates the signal is unavailable or otherwise invalid.

Bit	Signal
1	Vehicle Speed
2	Yaw Rate

6.3.2 Vehicle Acceleration Message

Message ID: 301 (hexadecimal)

Data Bytes: 8

Bit / Byte	8	7	6	5	4	3	2	1(lsb)
1	Lateral Acceleration MSByte							
2	Lateral Acceleration LSByte (LSBit = 0.001 m/s; signed)							
3	Longitudinal Acceleration MSByte							
4	Longitudinal Acceleration LSByte (LSBit = 0.001 m/s; signed)							
5	Unused						Signal Availability Indicator (See Below)	

Byte 5:

Depending on Vehicle/Application some signals might not be available. A '1' indicates the signal is available and valid. A '0' indicates the signal is unavailable or otherwise invalid.

Bit	Signal
1	Lateral Acceleration
2	Longitudinal Acceleration

6.3.3 Vehicle Devices Message

Message ID: 302 (hexadecimal)

Data Bytes: 7

Bit / Byte	8	7	6	5	4	3	2	1(lsb)
1	Throttle Position (LSBit = 0.5% open; unsigned)							
2	Brake Applied Status					Brake Applied Pressure		
3	Steering Wheel Angle MSByte							
4	Steering Wheel Angle LSByte (LSBit = 0.01 degrees; signed)							
5	Headlights (Meaning TBD)		Turn Signal/Hazard Signal (Meaning TBD)		Traction Control State (Meaning TBD)		Anti-Lock Brake State (Meaning TBD)	
6	Unused				System Health (Meaning TBD)			
7	Signal Availability Indicator (See Below)							

Byte 7:

Depending on Vehicle/Application some signals might not be available. A '1' indicates the signal is available and valid. A '0' indicates the signal is unavailable or otherwise invalid.

Bit	Signal
1	Throttle Position
2	Brake Applied Status
3	Steering Wheel Angle
4	Anti-Lock Brake State
5	Traction Control State
6	Turn Signal/Hazard Signal
7	Headlights
8	System Health

6.4 Traffic Signal Interface

This appendix specifies the format of the RS-232 messages that need to be exchanged in order to get traffic signal information into the Task 9 device.

Parameters for the physical setup and messages will be:

- 19,200 Baud
- 8 data bits
- No parity bit
- 1 stop bit

The communication between the Task 9 device and the traffic signal device shall consist of a series of requests and responses. The Task 9 device shall make requests and the traffic signal device will respond with data. There are two types of request/response pairs: initial and periodic.

6.4.1 Initial Request/Response State

The Task 9 device shall prepare the traffic signal controller for the periodic state by first transmitting the following sequence of 22 bytes (all bytes specified in hexadecimal format):

```
04 41 30 31  05 10 02 55  25 01 01 10  03 17 51 04
61 30 31 05  10 30
```

The Task 9 device shall then expect these four bytes to be transmitted from the traffic signal controller as a response:

```
10 30 10 31
```

There may also be an 83 byte data message following this response. These 83 bytes shall be ignored and discarded.

The Task 9 device shall then wait a full second before advancing to the periodic state.

6.4.2 Periodic Request/Response State

After leaving the "Initial State" the Task 9 device shall stay in the "Periodic State" for the duration of the program. The "Periodic State" shall consist of the Task 9 device repeatedly transmitting a request to the traffic signal device and the Task 9 device validating and parsing each response.

The Task 9 device shall execute the request by transmitting the following sequence of 7 bytes (all bytes specified in hexadecimal format) with a user-selectable period between 100 and 1000 milliseconds (with 100 milliseconds being the default):

```
04 61 30 31 05 10 30
```

The Task 9 device shall then expect the traffic signal controller to respond with a message that is at least 83 bytes long (with a maximum length of 100 bytes). Before validating and parsing the message it shall be searched for occurrences of the byte 0x10 in consecutive positions in the message. For every sequence of 0x10's one of them shall be extracted and discarded from the message. For example, if the received bytes were:

```
10 02 25 01 00 0B 1B 2A 2E 30 00 10 10 FF FF FF
FF FF FF FF FF 00 10 10 00 02 00 0B 1B 2A 2E 30
00 1A FF FF FF FF FF FF FF FF 00 1A 00 44 00 00
00 00 00 00 00 BB 00 00 00 00 00 00 00 00 00 00
00 44 00 00 FF 00 00 00 00 00 7F FF 00 00 00 00
10 03 2F 51 04
```

They would become this:

```
10 02 25 01 00 0B 1B 2A 2E 30 00 10 FF FF FF FF
FF FF FF FF 00 10 00 02 00 0B 1B 2A 2E 30 00 1A
FF FF FF FF FF FF FF FF 00 1A 00 44 00 00 00 00
00 00 00 BB 00 00 00 00 00 00 00 00 00 00 00 44
00 00 FF 00 00 00 00 00 7F FF 00 00 00 00 10 03
2F 51 04
```

after the "stuffed 0x10's" extraction.

Once this extraction has been performed the message shall be considered valid if it meets the following criteria:

1. It is exactly 83 bytes long.
2. It begins with the bytes 0x10 and 0x02 in that order.
3. It ends with the byte 0x04.

Once a message is determined to be valid then data shall be parsed from it. The following table shows the relevant bytes and their meanings:

Byte Number	Meaning
1	Header byte - constant 0x10
2	Header byte - constant 0x02
5	The current state of the active phase on ring 1: 0x00 = Green 0x02 = Yellow 0x03 = Red
25	The current state of the active phase on ring 2: 0x00 = Green 0x02 = Yellow 0x03 = Red
44	Active phases – one bit for each phase (1 – active, 0 – not active). Example: 0001 0001 – phases 1 and 5 are active 0010 0100 – phases 3 and 6 are active
46	Next active phases (format the same as "active phases").
12	Seconds left in the current state of the currently active phase of ring 1.
32	Seconds left in the current state of the currently active phase of ring 2.
83	End-of-message byte – constant 0x04

A **phase** can be thought of as a single flow of traffic through an intersection. An **active phase** is one that potentially has a non-red light. Any phase that is not active has a red light. The eight phases are divided into two groups of four phases called **rings**. Phases 1-4 make up ring 1 and phases 5-8 make up ring 2. Only 1 phase on each ring can be active simultaneously.

6.5 Preliminary Vehicle-to-Vehicle Common Message Set

Byte \ Bit	8	7	6	5	4	3	2	1(lsb)
1	Message Type (See Below)							
2	Temporary ID MSByte							
3	Temporary ID...							
4	Temporary ID...							
5	Temporary ID...							
6	Temporary ID...							
7	Temporary ID LSByte							
8	Precision Indicator (Meaning TBD)							
9	Longitude of center of vehicle MSByte							
10	"							
11	"							
12	Longitude LSByte (LSBit = 10^{-7} decimal degrees; signed)							
13	Latitude of center of vehicle MSByte							
14	"							
15	"							
16	Latitude LSByte (LSBit = 10^{-7} decimal degrees; signed)							
17	Altitude of center of vehicle MSByte							
18	Altitude (LSBit = 1 cm; unsigned; offset by +1 km)							
19	Unused				Altitude LSNybble			
20	UTC Time MSByte							
21								
22	Number of milliseconds since Jan. 1, 2004 at 00:00:00							
23								
24	UTC Time LSByte (LSBit = 0.001 seconds)							
25	Heading MSByte							
26	Heading (LSBit = 0.01 degrees; signed; 0 degrees = North)							
27	Vehicle Speed MSByte							
28	Vehicle Speed LSByte (LSBit = 0.01 m/s; unsigned)							
29	Lateral Acceleration MSByte							
30	Longitudinal Acceleration MSNybble				Lateral Acceleration LSNybble (LSBit = 0.01 m/s^2; signed)			
31	Longitudinal Acceleration LSByte (LSBit = 0.01 m/s^2; signed)							
32	Yaw Rate MSByte							
33	Yaw Rate LSByte (LSBit = 0.01 deg/sec; signed)							
34	Throttle Position (LSBit = 0.5% open; unsigned)							
35	Brake Applied Status (See Below)				Brake Applied Pressure (See Below)			
36	Steering Wheel Angle MSByte							
37	Steering Wheel Angle LSByte (LSBit = 0.02 degrees; signed)							
38	Headlights (See Below)		Turn Signal/Hazard Signal (See Below)		Traction Control State (See Below)		Anti-Lock Brake State (See Below)	
39	Unused				System Health (See Below)			
40	Vehicle Length MSByte							
41	Vehicle Width (Upper 2 bits)		Vehicle Length (Lower 6 bits; LSBit = 1 cm; unsigned)					
42	Vehicle Width LSByte (LSBit = 1 centimeter)							

NOTE: this represents the data format for the message set as delivered to the applications

MSByte - Most Significant Byte (8 bits)
LSByte - Least Significant Byte (8 bits)
LSNybble - Least Significant Nybble (4 bits)

All signed values are twos complement unless otherwise noted.

Message Type (From byte 1)	
0	Vehicle-to-Vehicle Message Version 1.0
1 - 255	Undefined

Brake Applied Status (From byte 35)	
0000	All Off
XXX1	Left Front
XX1X	Left Rear
X1XX	Right Front
1XXX	Right Rear
1111	All On

Brake Applied Pressure (From byte 35)	
0000	Not equipped
0001	Minimum braking pressure
0010	…
1111	Maximum braking pressure

Headlights (From byte 38)	
00	Off
01	Daytime Running Lights
10	On
11	Brights

Turn Signal/Hazard Signal (From byte 38)	
00	Off
01	Left Turn Signal
10	Right Turn Signal
11	Hazard Signal

Traction Control State (From byte 38)	
00	Not equipped
01	Off
10	On
11	Engaged

Anti-Lock Brake State (From byte 38)	
00	Not equipped
01	Off
10	On
11	Engaged

System Health (From byte 39)	
0000	No faults detected
0001	Specific error codes
…	"
1111	"

6.6 Task 9 Application Users' Guide

6.6.1 Introduction

This section provides the User's Guide for the Wireless Access in Vehicular Environments (WAVE) application delivered in accordance with the requirements in Chapter 2.

6.6.2 Scope

This User's Guide describes the setup, operating instructions, and troubleshooting procedures for the Task 9 Application (T9App). The T9App may be configured to operate in an OBU or RSU mode to support testing of vehicle safety scenarios.

6.6.3 Setup Procedures

6.6.3.1 Common Setup

This section describes the setup procedures that apply to both the OBU and RSU. It describes the WRM Setup, Host Device (HD) Configuration, Software Installation, and differential GPS (DGPS) setup. Figure 6-1 illustrates the configuration.

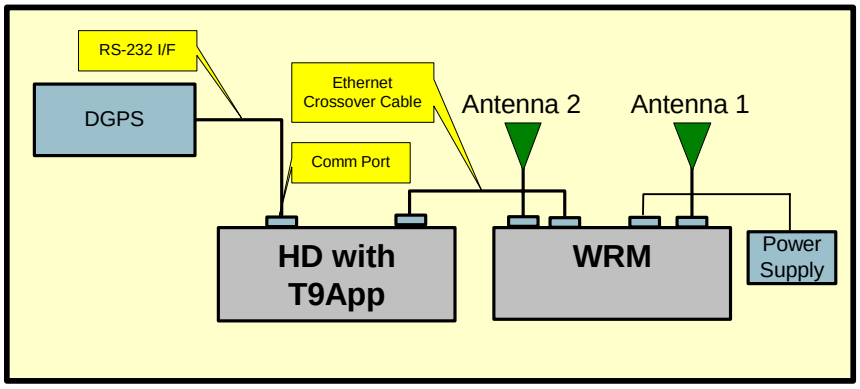


Figure 6-1. Common Setup

6.6.3.2 WRM Setup

Connect the HD to the WRM using one of the following methods:

- Use an Ethernet crossover cable to connect the HD Ethernet port directly to the WRM Ethernet port. If the HD is running Windows 2000 or Windows XP, a standard Ethernet cable may be used.

- Use standard Ethernet cables to connect the HD and WRM through a hub or Ethernet switch.

Supply power to the WRM using either the wall power supply (120V/5V AC-DC converter) or the vehicle power supply (12V/5V DC-DC converter with cigarette lighter adapter). For subsequent test setups, the crossover cable is not labeled, and the power supply is not shown for simplicity.

6.6.3.3 Host Device Configuration

Configure the HD IP address to an address of the format 192.168.001.xxx with Subnet Mask of 255.255.255.000. For communication to succeed, the HD IP address must be different from the WRM IP address (which is labeled on the WRM when it is delivered, and should not be changed by the user).

Each WRM has a unique IP address of the format 192.168.001.0xx, where xx is the DENSO assigned unit number. Each HD IP address needs to be unique as well. DENSO recommends adding 100 to the last set of digits in the WRM IP address to get the HD IP address. For example, if the WRM IP address is 192.168.001.013 then set the Host IP address to 192.168.001.113.

Windows IP Configuration Example

If the HD is a PC running the Windows XP operating system, use the following procedure to configure the HD IP address.

- From the Host PC's Start menu, choose Control Panel and then Network Connections.
- Right click on the Local Area Connection icon that belongs to the Ethernet controller connected to the WRM and select Properties.
- Within the Local Area Connection Properties dialog box, choose Internet Protocol (TCP/IP) and click Properties.
- Click the radio button corresponding to "Use the following IP address".
- Configure the Host IP address to (192.168.001.xxx) for the Ethernet connection in the Internet Protocol (TCP/IP) Properties dialog box. For example, if the WRM IP address is 192.168.001.013 then set the Host IP address to 192.168.001.113.
- Set the subnet mask to 255.255.255.0.
- Accept the settings and close the Internet Protocol Properties dialog box.
- The HD is now configured to communicate with the WRM.

6.6.3.4 Software Installation

Run the WAVETestInstall.exe program to install the T9App software. On the Customer Information screen, enter your User Name and Company Name. The installation places the program executable and dynamic link library files in the

appropriate directory (C:\Program Files\DENSO\WAVE Test\WAVE Test vx.x). The installation also places a WAVE Test vx.x (i.e., T9App) shortcut on your computer's Desktop. Double-clicking this icon will start the program. The program can also be started from the Windows Start button by selecting Programs and then WAVE Test vx.x.

The T9App program utilizes the Windows packet capture (PCAP) libraries, which must be installed separately. If the PCAP software was installed previously (e.g., as part of the API Tester installation), it does not need to be reinstalled. DENSO will supply the PCAP installation executable as part of the T9App delivery. It is also available from http://winpcap.polito.it.

6.6.3.5 GPS Setup

Connect a HD comm port to the DGPS using a standard serial cable (by default, the T9App uses comm port 1). Configure the comm port settings to the settings being used by the DGPS using the T9App Comm Parameters screen (see Section 6.6.4.4). The default T9App and CSI Wireless DGPS settings are 9600 baud, no parity bit, 8 data bits, and 1 stop bit. For the RSU, use of the DGPS is optional.

On some computers running Windows XP, the OS mistakenly interprets the DGPS as a serial track ball and loss of mouse control results. If this occurs, use the OS to disable the bogus track ball. From the Start menu, select Control Panel, and then System. Select the Hardware tab and then Device Manager. Right click on the device and disable it.

6.6.3.6 OBU Setup

Figure 6-2 illustrates the OBU setup. For the vehicle bus interface, install the Controller Area Network (CAN) bus drivers from the disk or CD supplied by Grid Connect (see www.gridconnect.com for additional information). Install a Grid Connect adapter into a HD USB port. VSCC must supply the cable to connect the adapter to the vehicle bus.

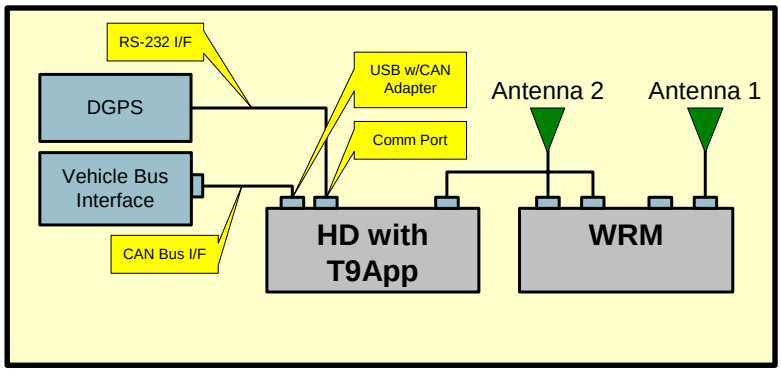


Figure 6-2. OBU Setup

6.6.3.7 RSU Setup

Figure 6-3 illustrates the RSU setup. Connect a HD comm port to the traffic signal controller using a standard serial cable (by default, the T9App uses comm port 2). Use the T9App Comm Parameters Screen (see Section 6.6.4.4) to configure the comm port settings. The default T9App settings are 19,200 baud, no parity bit, 8 data bits, and 1 stop bit.

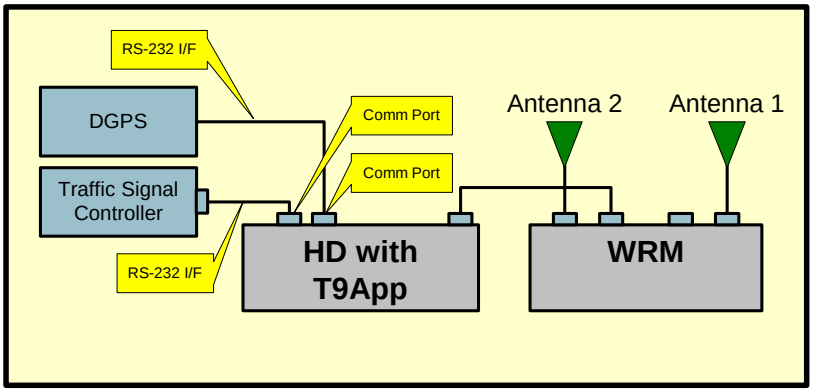


Figure 6-3. RSU Setup

6.6.4 Operating Instructions

6.6.4.1 Overview

The T9App provides the following functionality:

- User configuration of test parameters
- WRM configuration
- Transmission and reception of messages formatted in accordance with the Task 9 Application Message Specification defined in Section 6.5.
- Real-time display of WAVE network status
- Logging of configuration parameters and message traffic
- Operation in OBU or RSU mode
- Interface to DGPS receiver and CAN vehicle bus for OBU operation
- Interface to DGPS receiver and traffic signal controller for RSU operation

6.6.4.2 Main Screen

Figure 6-4 shows the T9App Main Screen Layout. It enables the user to access four screens (i.e., WRM Configuration, Comm Parameters, Test Options, and

Traffic Signal Information) to set up the test configuration. After setup, press the "Start Testing" button to begin test execution.

Figure 6-4. T9App Main Screen Layout

6.6.4.3 WRM Configuration Screen

The WRM Configuration Screen enables the user to configure the WRM parameters or reset the WRM configuration to the default settings. Figure 6-5 shows the WRM Configuration Screen layout. Refer to the WRM Interface Specification 0 for a detailed description of the parameter options and their default values. The unit mode setting specifies whether the T9App and WRM operate in RSU or OBU mode. The T9App limits the available options for Tx power to settings that are valid for the current channel, unit mode, and antenna compensation factor. Refer to the WRM Interface Specification for a description of the valid power settings. After selecting the desired settings, press the OK button to configure the WRM and exit the screen, or Cancel to leave the WRM configuration unchanged. Use the Get Current Configuration button to refresh the screen with the current WRM settings.

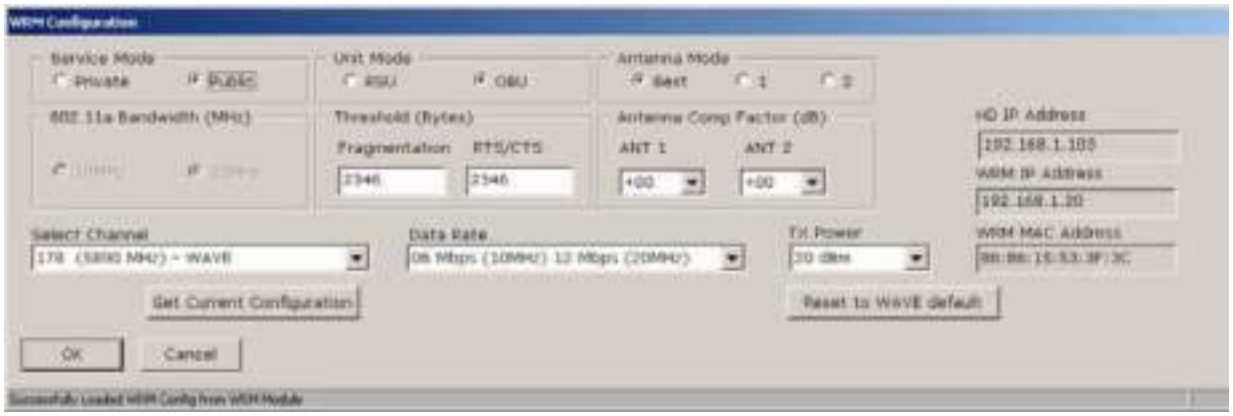


Figure 6-5. WRM Configuration Screen Layout

6.6.4.4 Comm Parameters Screen

The Comm Parameters Screen enables the user to configure communication parameters for over the air message transmission and device interfaces. Figure 6-6 shows the Comm Parameters Screen layout and Table 6-1. Comm Parameters Screen Field Definitions provides the field definitions.

Figure 6-6. Comm Parameters Screen Layout

Table 6-1. Comm Parameters Screen Field Definitions

Group	Field	Description
N/A	Local HD IP Address	See Section 6.6.3.3 for instructions on how to set the Host Device IP Address using OS capabilities.
	Sender ID	Set to the ID to be sent in the common message header.
	Destination HD IP Address	Set to 255.255.255.255 for broadcast IP addressing, or to the destination HD IP address for unicast IP addressing.
	Destination WRM MAC Address	Set to all FFs for broadcast MAC addressing, or to the destination WRM MAC address for unicast IP addressing. Note that OBUs automatically regenerate a new random MAC address whenever they are reset or power cycled.

Group	Field	Description
	Tx Message Interval	Set to the transmit interval for the OBU V2V Safety Message or the RSU Traffic Signal Message.
	Tx Message Size.	Set to the desired message size. The T9App adds fill bytes to the end of the message if needed to reach the specified size. The T9App ignores this parameter if it is less than the size of the OBU or RSU message.
GPS Setup	Enabled	Check the box if a GPS receiver is attached.
	Baud Rate	Set the baud rate to match the GPS Receiver configuration.
	Com Port	Set to the port on which the GPS Receiver is attached.
Traffic Signal Setup	Enabled	Check the box if a Traffic Signal Controller device is attached.
	Baud Rate	Set the baud rate to match the Traffic Signal Controller configuration.
	Com Port	Set to the port on which the Traffic Signal Controller is attached.
CAN Setup	Enabled	Check the box if a CAN bus is attached.
	Baud Rate	Set the baud rate to match the CAN bus configuration.
	Init Type	Set to standard (STD).

6.6.4.5 Test Options Screen

The Test Options Screen enables the user to configure the test duration and logging. Figure 6-7 shows the Test Options Screen layout and Table 6-2 provides the field definitions.

Figure 6-7. Test Options Screen Layout

Table 6-2. Test Option Screen Field Definitions

Group	Field	Description
Test Control	Run for n sent messages	Check the radio button and enter the total number of messages to be sent during the test.
	Run for n seconds	Check the radio button and enter the number of seconds the test should run.
	Passive mode	Check the radio button to run in passive mode. The T9App will not transmit any messages, but will display and log received messages. After starting the test, the test will continue to run until the user presses the Quit button.
Logging	Log this Test	Check the box to generate a logfile for the test. Uncheck the box if no logfile is required.
	Test Name	Enter the test name for the logfile. Browse to the desired directory by pressing the "…" button. The T9App will generate a logfile at the specified location with the name [Test Name]_[Test Run]_mmddyyyy.txt. The T9App will set the Test Run number to 1 for the first test of the day for this test name and location and automatically increment it for all subsequent tests.

6.6.4.6 Traffic Signal Information Screen

The Traffic Signal Information Screen enables the user to configure the static traffic signal information. Figure 6-8 shows the Traffic Signal Information screen layout and Figure 6-9 shows the Location Information dialog box that is displayed when any of the Location buttons are pushed. If the RSU has a GPS receiver attached, the RSU will use the GPS information as the intersection location rather than the user entered values. Table 6-3 provides the field definitions.

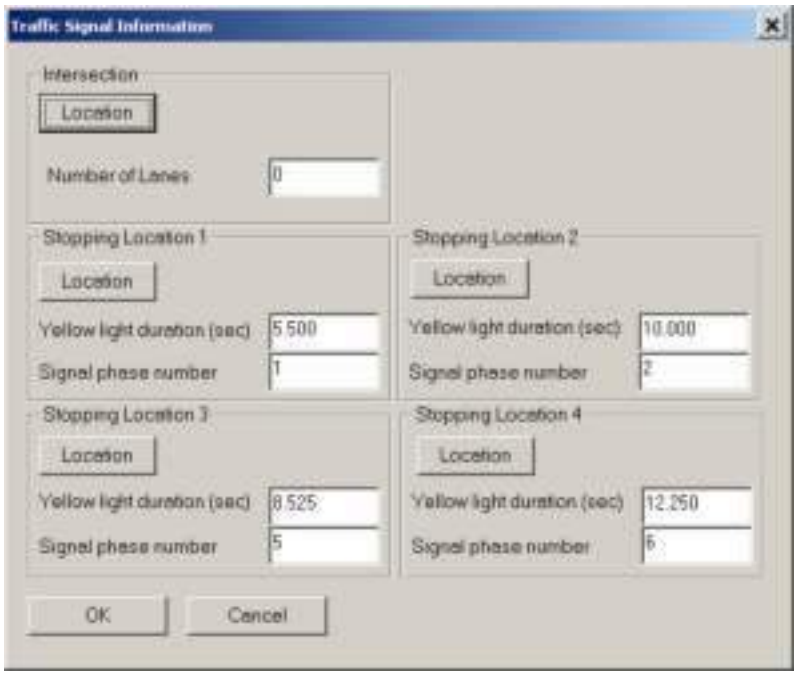


Figure 6-8. Traffic Signal Information Screen Layout

Figure 6-9. Location Information Screen Dialog Box

Table 6-3. Traffic Signal Information Screen Field Definitions

Group	Field	Description
Intersection	Number of Lanes	Set to the number of lanes in the intersection.
Stopping locations 1-4	Yellow light duration	Set to the duration of the yellow light.
	Signal phase number	Set to a number in the range of 1 to 8. Each stopping location should have a different signal phase number.

Group	Field	Description
Location Information Dialog Box	Latitude	Set to the latitude of the intersection or stopping location. Enter northern latitudes as positive numbers and southern latitudes as negative numbers.
	Longitude	Set to the longitude of the intersection or stopping location. Enter northern longitudes as positive numbers and southern longitudes as negative numbers..
	Altitude	Set to the altitude (height above ellipsoid).
	Direction	Set to the direction. 0 represents north. Enter eastern directions as positive numbers and western directions as negative numbers.

6.6.4.7 Test Display Screen

The Test Display Screen provides a real time display of the WAVE network status. The Test Display screen also enables the user to pause and resume a test, or to quit a test. Figure 6-10 shows the Test Display Screen layout and Table 6-4 provides the field definitions.

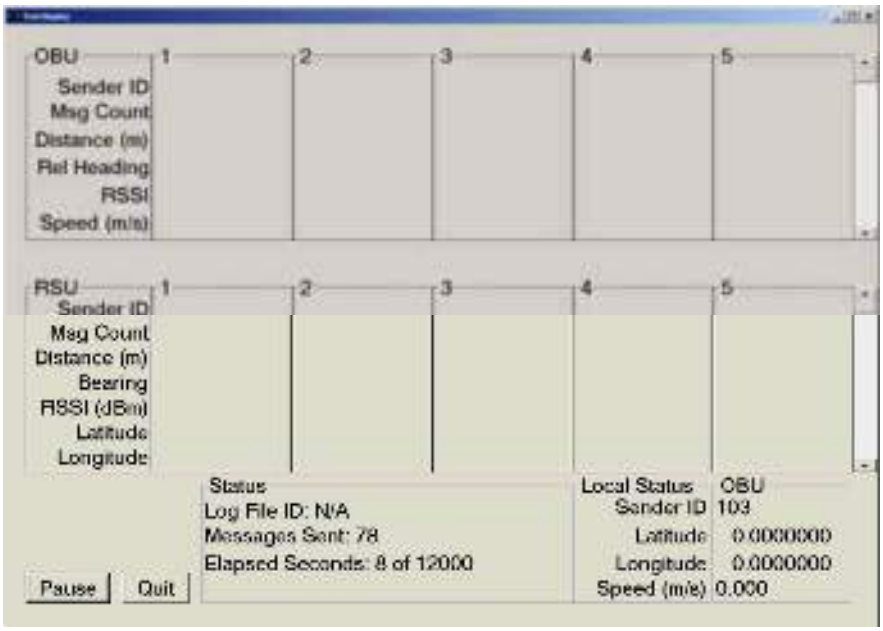


Figure 6-10. Test Display Screen Layout

Table 6-4. Test Display Screen Field Definitions

Group	Field	Description
OBU	Sender ID	Displays the sender ID of the OBU.
	Msg Count	Displays the number of messages received from the OBU since the beginning of the test.
	Distance	Displays the distance to the OBU.
	Rel Heading	Displays the relative heading to the OBU (i.e., bearing from the local OBU to the remote OBU minus the remote OBU's heading) if the local unit is an OBU. Displays the remote OBU's heading if the local unit is an RSU.
	RSSI	Displays the received signal strength of the last message received from the OBU.
	Speed	Displays the speed of the OBU obtained from the CAN bus.
RSU	Sender ID	Displays the sender ID of the RSU.
	Msg Count	Displays the number of messages received from the RSU since the beginning of the test.
	Distance	Displays the distance to the RSU.
	Bearing	Displays the bearing to the RSU.
	RSSI	Displays the received signal strength of the last message received from the RSU. The T9App automatically adjusts the RSSI by a known offset prior to display or logging, based on the WRM IP address. DENSO measured this offset prior to shipment. If the IP address is changed, an incorrect offset or no offset may be applied.
	Latitude	Displays the latitude of the RSU.
	Longitude	Displays the longitude of the RSU.
Control	Pause Button	Pauses the current testing. The T9App stops the screen updates log generation, and changes the button label to "Resume".
	Resume Button	Resumes a paused test. The T9App resumes the screen updates and log generation, and changes the button label to "Pause".
	Quit Button	Quits the current test. The T9App stops the screen updates, closes the logfile, and exits to the main screen. The logfile contains the log entries generated up to the time the test was stopped.

Group	Field	Description
Status	Log File ID	Displays the current test ID that will be used in the log file name. The T9App sets this number to 1 for the first logged run of the day and automatically increments it during the day. The T9App resets the test number to 1 if the test name or log directory is changed on the Test Options Screen (see Section 6.6.4.5). TheT9App does not increment the test number for tests that are not logged.
	Messages Sent	Displays the number of messages sent since the beginning of the test. If the Test Control selection on the Test Options Screen (see Section 6.6.4.5) is "Run for n sent messages", the T9App displays Messages Sent as "x of n".
	Seconds Elapsed	Displays the elapsed time since the beginning of the test. This does not include any time during which the test was paused. If the Test Control selection on the Test Options Screen (see Section 6.6.4.5) is "Run for n seconds", the T9App displays Seconds Elapsed as "x of n".
Local	Sender ID	Displays the Sender ID of the local unit.
	Latitude	Displays the latitude of the local unit.
	Longitude	Displays the longitude of the local unit.
	Speed	Displays the speed of the local unit obtained from the CAN bus (applicable for OBUs only).

6.6.4.8 Logfile Usage

Logfile Contents

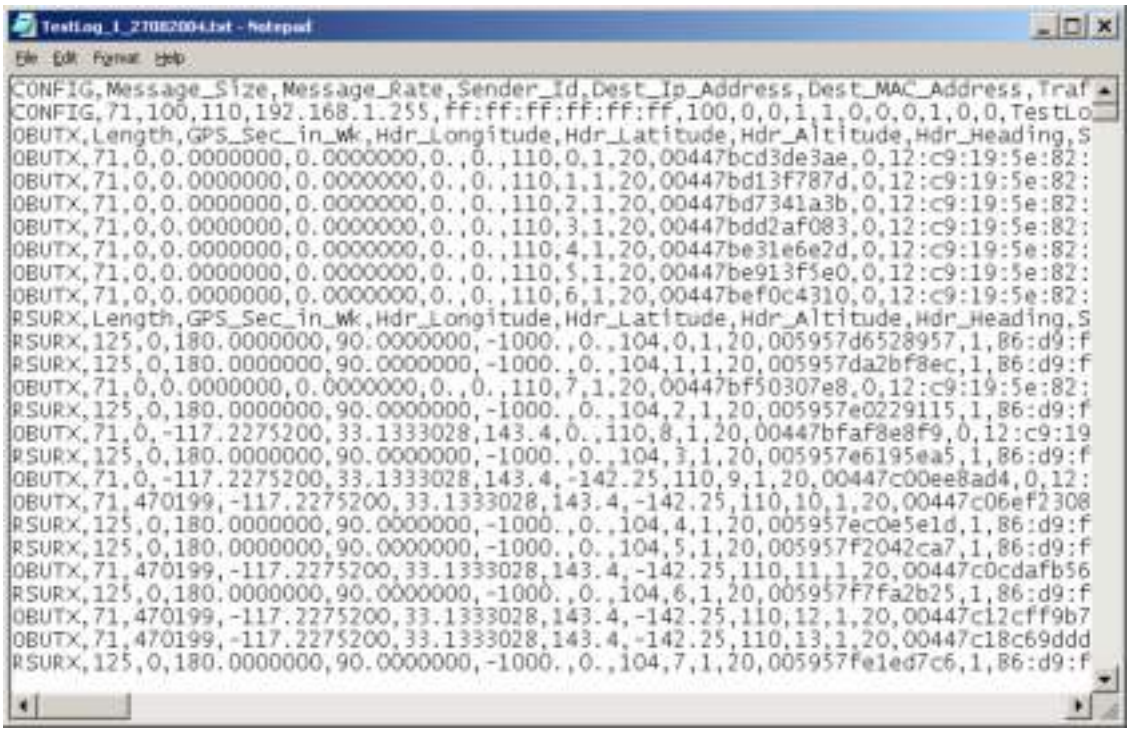
If the user requests logging on the Test Options Screen (see Section 6.6.4.5), the T9App generates a logfile with configuration information and entries for each message sent and received. Table 6-5. Logfile Record Types describes each of the log record types, and indicates whether or not they appear in an OBU or RSU log.

Table 6-5. Logfile Record Types

Record Type	Contents	OBU Log	RSU Log
CONFIG	Records the configuration data entered by the user on the T9App GUI.	√	√
OBUTX	Records data sent over the air by the local unit when the unit is operating in OBU mode.	√	
OBURX	Records data received from a remote OBU.	√	√
RSUTX	Records data sent over the air by the local unit when the unit is operating in RSU mode.		√
RSURX	Records data received from a remote RSU.	√	√

The T9App writes a heading record before the first record of each type. The heading record contains the names of all of the fields for the record type. The T9App writes a CONFIG record at the beginning of the test. When operating as an OBU, it writes an OBUTX record whenever it transmits a message. When operating as a RSU, it writes a RSUTX record whenever it transmits a message. All units log all received messages as OBURX or RSURX records, depending on the type of the sending unit.

Figure 6-11 shows the contents of a sample OBU logfile. The first two rows are a CONFIG heading record followed by a CONFIG data record. The third row is an OBUTX heading record, followed by seven OBUTX data records. Next is an RSURX heading record followed by two RSURX data records.



```
CONFIG,Message_Size,Message_Rate,Sender_Id,Dest_Ip_Address,Dest_MAC_Address,Traf
CONFIG,71,100,110,192.168.1.255,ff:ff:ff:ff:ff:ff,100,0,0,1,1,0,0,0,1,0,0,TestLo
OBUTX,Length,GPS_Sec_in_Wk,Hdr_Longitude,Hdr_Latitude,Hdr_Altitude,Hdr_Heading,S
OBUTX,71,0,0.0000000,0.0000000,0.,0.,110,0,1,20,00447bcd3de3ae,0,12:c9:19:5e:82:
OBUTX,71,0,0.0000000,0.0000000,0.,0.,110,1,1,20,00447bd13f787d,0,12:c9:19:5e:82:
OBUTX,71,0,0.0000000,0.0000000,0.,0.,110,2,1,20,00447bd7341a3b,0,12:c9:19:5e:82:
OBUTX,71,0,0.0000000,0.0000000,0.,0.,110,3,1,20,00447bdd2af083,0,12:c9:19:5e:82:
OBUTX,71,0,0.0000000,0.0000000,0.,0.,110,4,1,20,00447be31e6e2d,0,12:c9:19:5e:82:
OBUTX,71,0,0.0000000,0.0000000,0.,0.,110,5,1,20,00447be913f5e0,0,12:c9:19:5e:82:
OBUTX,71,0,0.0000000,0.0000000,0.,0.,110,6,1,20,00447bef0c4310,0,12:c9:19:5e:82:
RSURX,Length,GPS_Sec_in_Wk,Hdr_Longitude,Hdr_Latitude,Hdr_Altitude,Hdr_Heading,S
RSURX,125,0,180.0000000,90.0000000,-1000.,0.,104,0,1,20,005957d6528957,1,86:d9:f
RSURX,125,0,180.0000000,90.0000000,-1000.,0.,104,1,1,20,005957da2bf8ec,1,86:d9:f
OBUTX,71,0,0.0000000,0.0000000,0.,0.,110,7,1,20,00447bf50307e8,0,12:c9:19:5e:82:
RSURX,125,0,180.0000000,90.0000000,-1000.,0.,104,2,1,20,005957e0229115,1,86:d9:f
OBUTX,71,0,-117.2275200,33.1333028,143.4,0.,110,8,1,20,00447bfaf8e8f9,0,12:c9:19
RSURX,125,0,180.0000000,90.0000000,-1000.,0.,104,3,1,20,005957e6195ea5,1,86:d9:f
OBUTX,71,0,-117.2275200,33.1333028,143.4,-142.25,110,9,1,20,00447c00ee8ad4,0,12:
OBUTX,71,470199,-117.2275200,33.1333028,143.4,-142.25,110,10,1,20,00447c06ef2308
RSURX,125,0,180.0000000,90.0000000,-1000.,0.,104,4,1,20,005957ec0e5e1d,1,86:d9:f
RSURX,125,0,180.0000000,90.0000000,-1000.,0.,104,5,1,20,005957f2042ca7,1,86:d9:f
OBUTX,71,470199,-117.2275200,33.1333028,143.4,-142.25,110,11,1,20,00447c0cdafb56
RSURX,125,0,180.0000000,90.0000000,-1000.,0.,104,6,1,20,005957f7fa2b25,1,86:d9:f
OBUTX,71,470199,-117.2275200,33.1333028,143.4,-142.25,110,12,1,20,00447c12cff9b7
OBUTX,71,470199,-117.2275200,33.1333028,143.4,-142.25,110,13,1,20,00447c18c69ddd
RSURX,125,0,180.0000000,90.0000000,-1000.,0.,104,7,1,20,005957fe1ed7c6,1,86:d9:f
```

Figure 6-11. Sample OBU Logfile

6.6.4.9 Importing a Logfile into Excel

One method of converting the logfile into a more easily readable format is to import it into Excel. The procedure for this is as follows:

1. Open Excel.
2. Use the open file command and select the desired logfile. Excel will display the Text Import Wizard, step 1 of 3. Leave the default settings, select Next and step 2 of 3 will be displayed.
3. On step 2, check the box to indicate comma is a delimiter and then select Finish. See Figure 6-12.

Figure 6-12. Excel Text Import Wizard

4. Excel will now display the logfile in a worksheet. Push the select all button (above the "1" and to the left of "A"). Excel will highlight all of the cells as shown in Figure 6-13.

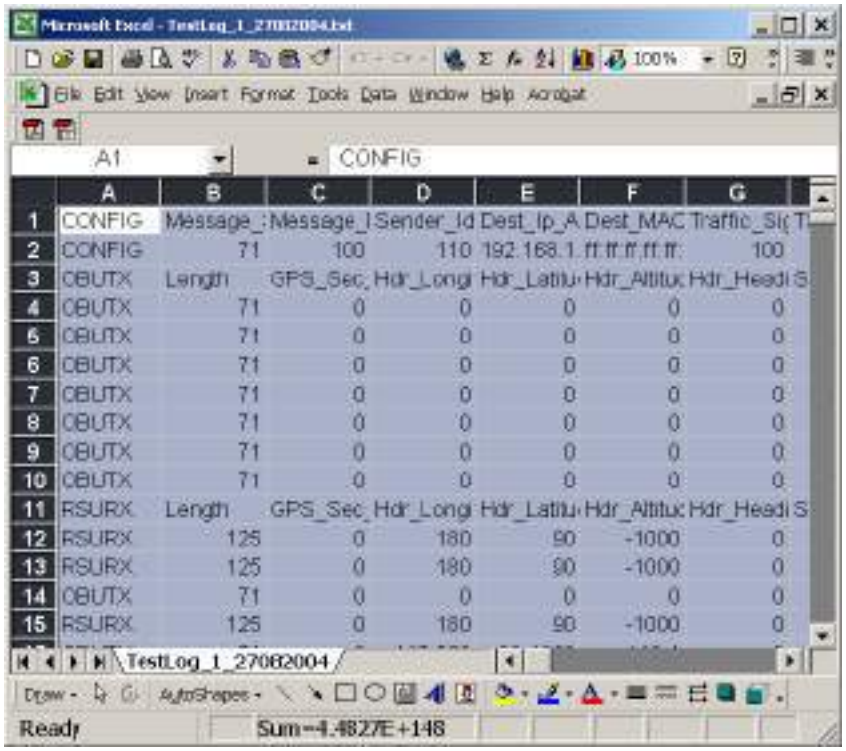
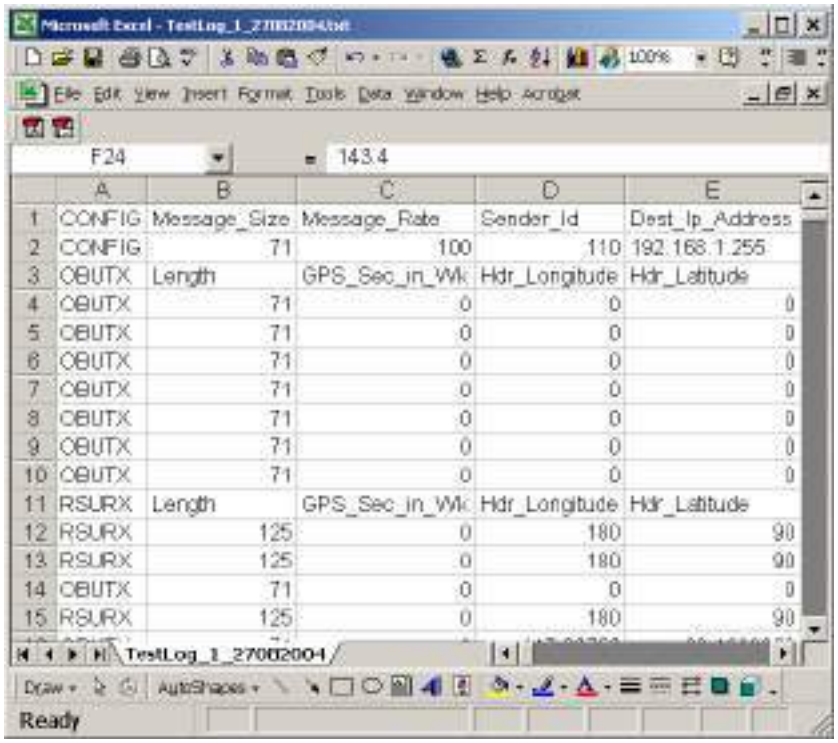


Figure 6-13. Worksheet Selection

5. From the menu, select Format, Column, AutoFit Selection. The logfile will now be displayed in a more easily read format. See Figure 6-14.



	A	B	C	D	E
1	CONFIG	Message_Size	Message_Rate	Sender_Id	Dest_Ip_Address
2	CONFIG	71	100	110	192.168.1.255
3	OBUTX	Length	GPS_Sec_in_Wk	Hdr_Longitude	Hdr_Latitude
4	OBUTX	71	0	0	0
5	OBUTX	71	0	0	0
6	OBUTX	71	0	0	0
7	OBUTX	71	0	0	0
8	OBUTX	71	0	0	0
9	OBUTX	71	0	0	0
10	OBUTX	71	0	0	0
11	RSURX	Length	GPS_Sec_in_Wk	Hdr_Longitude	Hdr_Latitude
12	RSURX	125	0	180	90
13	RSURX	125	0	180	90
14	OBUTX	71	0	0	0
15	RSURX	125	0	180	90

Figure 6-14. Imported Logfile

6.6.5 Troubleshooting

This chapter describes the error messages generated by the T9App and how to resolve them.

6.6.5.1 WRM Communication

The T9App attempts to retrieve the current WRM configuration upon startup. If it is successful, it displays the message "WRM Config loaded OK" at the bottom of the main screen. If it is unable to retrieve the configuration, it displays the message "Unable to init WRM API". If this message appears, check the following.

1. Verify the HD and WRM Ethernet interfaces are connected with the correct cabling.
2. Verify the WRM is powered on.
3. Verify the WRM is in WAVE mode. Use a Telnet command to change the mode from 802.11a to WAVE if necessary.

6.6.5.2 GPS and Traffic Signal Communication

The GPS and Traffic Signal serial port configurations are set using the Comm Parameters Screen (see Section 6.6.4.4). If both are enabled, they must use different COM ports. If the same port is selected for both devices, the T9App displays the message box shown in Figure 6-16 when the user attempts to exit the screen. To eliminate the error, select different COM ports for each device, or disable the setup for one of the devices.

Figure 6-15. COM Port Conflict Error Message

6.6.5.3 GPS Communication

The T9App attempts to initialize the selected GPS serial port at the beginning of each test when GPS setup is enabled on the Comm Parameters screen. If it is unable to initialize the port, it displays the message box shown in Figure 6-16.

Figure 6-16. GPS Port Initialization Error Message

If this message box appears, check the following.

1. Verify the selected COM port exists on the host device (check the number of ports available using the OS).
2. Verify the GPS is connected to the selected port.
3. Verify no other application is using the COM port (e.g., Hyperterm).
4. Reboot the machine if the above steps do not resolve the issue. The COM port may be hung from use by a previous application.

If the T9App does not appear to be receiving GPS data, verify the serial port settings on the GPS receiver match the T9App settings.

6.6.5.4 Traffic Signal Communication

The T9App attempts to initialize the selected Traffic Signal port at the beginning of each test when operating in RSU mode and Traffic Signal setup is enabled on

the Comm Parameters Screen. If it is unable to initialize the port, it displays the message box shown in Figure 6-17.

Figure 6-17. Traffic Signal Port Initialization Error Message

If this message box appears, check the following.

1. Verify the selected COM port exists on the host device (check the number of ports available using the OS).
2. Verify the Traffic Signal is connected to the selected port.
3. Verify no other application is using the COM port (e.g., HyperTerminal).
4. Reboot the machine if the above steps do not resolve the issue. The COM port may be hung from use by a previous application.

If the T9App does not appear to be receiving Traffic Signal data, verify the serial port settings on the Traffic Signal controller match the T9App settings.

6.6.5.5 CAN Bus Communication

The T9App attempts to initialize the CAN bus when operating in OBU mode and CAN setup is enabled on the Comm Parameters Screen. If it is unable to initialize the bus, it displays the message box shown in Figure 6-18. Select OK to continue the test without using the CAN interface. This is equivalent to unchecking the CAN setup box on the Comm Parameters Screen (see Section 6.6.4.4) Select Cancel to return to the main screen without executing the test.

Figure 6-18. CAN Bus Initialization Error Message Box

If this message box appears and the CAN bus should be operational, check the following.

1. Verify the Grid Connect CAN bus drivers are installed on the host device.
2. Verify the CAN bus settings for baud rate and init type on the Comm Parameters Screen are valid for the current setup.
3. Verify the Grid Connect USB adapter is plugged into the host device.

4. Verify the cable is connected between the Grid Connect adapter and the vehicle.
5. Verify no other CAN application is running on the same machine (e.g., Grid Connect's PCAN View)

Appendix G: Field Testing and Evaluation of WAVE/DSRC Communications Functionalities

TABLE OF CONTENTS

1 OVERVIEW 1

1.1 GOALS 1
1.2 TEST PLAN 2
1.2.1 Transmission Characteristics at Intersections 2
1.2.2 Intersection Controller Data Exchange 11
1.2.3 Vehicle Data Exchange 12

2 TEST RESULTS FOR INTERSECTIONS 15

2.1 INTERSECTION TESTING 15
2.1.1 Baseline Evaluation and Test Equipment Verification 17
2.1.2 Oakwood Boulevard & Michigan Avenue 19
2.1.3 Crooks Road & Big Beaver Road 23
2.1.4 Santa Clara Street & Market Street 26
2.1.5 Hillview Avenue & Hanover Street 28
2.1.6 Woodward Avenue & I-696 Service Drive 30
2.1.7 El Camino Real & 5th Avenue 33
2.1.8 Woodside Road & Churchill Avenue 35
2.1.9 Country Club Drive & 12 Mile Road 36
2.1.10 Auburn Road & Squirrel Road 39
2.1.11 Sand Hill Road & Whiskey Hill Road 44
2.1.12 Long Lake Road & Lahser Road 46
2.1.13 Quarton Road & Lahser Road 49
2.1.14 Skyline Boulevard & Woodside Road 51
2.1.15 Page Mill Road & Deer Creek Road 52
2.1.16 Squirrel Road & Long Lake Road 54
2.2 COMPARISONS WITH THE OPEN ENVIRONMENT BASELINE DATA 59
2.3 SUMMARY 61

3 INTERSECTION TESTING USING A SYNCHRONIZED TRAFFIC CONTROLLER 63

3.1 BACKGROUND AND TEST SET-UP 63
3.1.1 Traffic Signal Controller Interface 64
3.1.2 Choice of Intersection 65
3.1.3 Test Preparations 67
3.2 FULL POWER TRANSMIT TESTING AND 5.9 GHZ DSRC INTERSECTION CHARACTERIZATION 68
3.2.1 Performance Characterization 69
3.2.2 Traffic Signal Controller Phase and Timing 77

3.3 REDUCED POWER TRANSMIT TESTING AND 5.9 GHZ DSRC INTERSECTION CHARACTERIZATION 81
3.3.1 Test Results at 12 dBm Transmit Power Setting 81
3.3.2 Test Results at 6 dBm Transmit Power Setting 83
3.3.3 Test Results at 3 dBm Transmit Power Setting 85
3.4 VEHICLE-VEHICLE AND VEHICLE-INFRASTRUCTURE TESTING AND RESULTS 87
3.5 SUMMARY 91

4 VEHICLE-TO-VEHICLE COMMUNICATIONS RESULTS USING THE WAVE RADIO MODULES 93

4.1 VEHICLE-TO-VEHICLE COMMUNICATIONS PERFORMANCE AT MILFORD PROVING GROUNDS 93
4.1.1 Test for Omni-directional Coverage & Vehicle Signals 94
4.1.2 Lead Vehicle Brake Test 98
4.1.3 Test for Maximum Communication Range 101
4.1.4 Test for Communication Performance Under High Relative Speed 103
4.1.5 Test for Communication Range Under Low Transmit Power 105
4.1.6 Test for Communication Performance Under High Data Rate 106
4.2 VEHICLE-TO-VEHICLE COMMUNICATIONS PERFORMANCE ON I-96 FREEWAY AND M-5 RAMP 108
4.2.1 Test Conducted on I-96 West 109
4.2.2 Test Conducted on I-96 East 113
4.2.3 Test Conducted on M-5 Ramp to 12 Mile Road 117
4.3 SUMMARY 121

TABLE OF FIGURES

FIGURE 1. CONTROLLER TEST SITE AT ORCHARD LAKE ROAD AND 10 MILE ROAD 11
FIGURE 2. SEVEN VEHICLE CARAVAN WITH CAN CONNECTIVITY HIGHLIGHTED 14
FIGURE 3. RSU AT DETROIT AREA TEST LOCATION 16
FIGURE 4. RSU AT PALO ALTO AREA TEST LOCATION 16
FIGURE 5. RSU AT DETROIT AREA TEST LOCATION 16
FIGURE 6. RSU AT PALO ALTO AREA TEST LOCATION 16
FIGURE 7. RSU EQUIPMENT VERIFICATION AT MILFORD PROVING GROUND 18
FIGURE 8. AERIAL VIEW OF THE OAKWOOD/MICHIGAN INTERSECTION 19
FIGURE 9. AERIAL VIEW OVERLAID WITH COLOR-CODED RSSI VALUES 20
FIGURE 10. VIEWS FROM THE OAKWOOD/MICHIGAN INTERSECTION 21
FIGURE 11. CTK PLOTS OF THE OAKWOOD/MICHIGAN INTERSECTION 22
FIGURE 12. RSSI PLOT OF THE CROOKS/BIG BEAVER INTERSECTION 23
FIGURE 13. VIEWS OF THE CROOKS/BIG BEAVER INTERSECTION 24
FIGURE 14. CTK PLOTS OF THE CROOKS/BIG BEAVER INTERSECTION 25
FIGURE 15. AERIAL VIEW OF SANTA CLARA/MARKET INTERSECTION 26
FIGURE 16. RSSI PLOT AND VIEWS OF MARKET/SANTA CLARA INTERSECTION 27
FIGURE 17. CTK PLOT OF THE MARKET STREET TEST ROUTE 27
FIGURE 18. RSSI PLOT FOR THE HANOVER TEST ROUTE 28
FIGURE 19. VIEWS OF THE HILLVIEW/HANOVER INTERSECTION 29
FIGURE 20. CTK PLOT FOR THE HANOVER TEST ROUTE 29
FIGURE 21. WOODWARD/I-696 SERVICE DRIVE INTERSECTION 30
FIGURE 22. RSSI PLOT OF THE WOODWARD/I-696 SERVICE DRIVE INTERSECTION 31
FIGURE 23. VIEWS AND CTK PLOT OF THE I-696 SERVICE DRIVE TEST ROUTE 31
FIGURE 24. VIEW AND CTK PLOT FOR THE WOODWARD TEST RUN 32
FIGURE 25. RSSI PLOT FOR EL CAMINO REAL/5TH AT 100% POWER (20 DBM) 33
FIGURE 26. RSSI PLOT FOR EL CAMINO/5TH AT 50% POWER (17 DBM) 34
FIGURE 27. RSSI FOR EL CAMINO/5TH AT 10% POWER (10 DBM) 34
FIGURE 28. RSSI PLOT AND VIEWS OF THE WOODSIDE TEST RUN 35
FIGURE 29. CTK PLOT FOR THE HILLSIDE TEST RUN 36
FIGURE 30. RSSI PLOT FOR THE COUNTRY CLUB/12 MILE INTERSECTION 36
FIGURE 31. VIEWS AND CTK PLOT FOR EASTBOUND 12 MILE TEST RUN 37
FIGURE 32. VIEWS AND CTK PLOTS FOR 1) WEST TO SOUTH, 2) NORTH TO EAST TEST ROUTES . 38
FIGURE 33. RSSI PLOT FOR AUBURN/SQUIRREL TEST RUNS 39
FIGURE 34. VIEWS AND CTK PLOT FOR THE SOUTHBOUND SQUIRREL TEST RUN 40
FIGURE 35. VIEWS AND CTK PLOT FOR THE SOUTHBOUND SQUIRREL TEST RUN 41
FIGURE 36. VIEWS AND CTK PLOT FOR THE EASTBOUND AUBURN TEST RUN 42
FIGURE 37. VIEWS AND CTK PLOT FOR THE WESTBOUND SQUIRREL TEST RUN 43
FIGURE 38. RSSI PLOT FOR SAND HILL TEST ROUTE 44
FIGURE 39. VIEWS AND CTK PLOT FOR THE SAND HILL TEST RUN 45
FIGURE 40. RSSI PLOT AND VIEWS FOR THE LONG LAKE/LAHSER TEST ROUTE 47
FIGURE 41. CTK PLOTS FOR THE LONG LAKE/LAHSER INTERSECTION 48
FIGURE 42. RSSI PLOT FOR THE QUARTON TEST ROUTE 49
FIGURE 43. VIEWS AND CTK PLOTS FOR THE QUARTON TEST ROUTES 50
FIGURE 44. RSSI PLOT FOR THE SKY LINE TEST ROUTE 51

FIGURE 45. VIEWS AND CTK PLOT FOR THE SKYLINE TEST RUN 52
FIGURE 46. RSSI PLOT AND VIEWS FOR THE PAGE MILL TEST ROUTE 53
FIGURE 47. CTK PLOT FOR THE PAGE MILL TEST RUN 53
FIGURE 48. RSSI PLOT FOR THE SQUIRREL AND LONG LAKE TEST ROUTES 54
FIGURE 49. VIEWS AND CTK PLOT FOR NORTHBOUND SQUIRREL TEST RUN 55
FIGURE 50. VIEWS AND CTK PLOT FOR THE SOUTHBOUND SQUIRREL TEST RUN 56
FIGURE 51. VIEWS AND CTK PLOT FOR THE WESTBOUND LONG LAKE TEST RUN 57
FIGURE 52. VIEWS AND CTK PLOT FOR THE EASTBOUND LONG LAKE TEST RUN 58
FIGURE 53. DATA COMPARISON OF OAKWOOD/MICHIGAN AND MILFORD PROVING GROUNDS ... 59
FIGURE 54. DATA COMPARISON OF CROOKS/BIG BEAVER AND MILFORD PROVING GROUNDS 60
FIGURE 55. EPAC M30 63
FIGURE 56. ORCHARD LAKE ROAD – SOUTHBOUND DIRECTION 65
FIGURE 57. 10 MILE ROAD – EASTBOUND DIRECTION 66
FIGURE 58. ORCHARD LAKE ROAD – NORTHBOUND DIRECTION 66
FIGURE 59. 10 MILE ROAD – WESTBOUND DIRECTION 67
FIGURE 60. EASTBOUND 10 MILE RD. PACKETS RECEIVED, RANGE AND RSSI 70
FIGURE 61. WESTBOUND 10 MILE RD. PACKETS RECEIVED, RANGE AND RSSI 70
FIGURE 62. SOUTHBOUND ORCHARD LAKE. PACKETS RECEIVED, RANGE AND RSSI 71
FIGURE 63. NORTHBOUND ORCHARD LAKE. PACKETS RECEIVED, RANGE AND RSSI 71
FIGURE 64. EASTBOUND 10 MILE RD. PACKETS RECEIVED, RANGE AND RSSI WITHIN 250 M RANGE OF INTEREST FOR SAFETY APPLICATIONS 72
FIGURE 65. NUMBER OF OUTAGES AND LENGTH IN EASTBOUND DIRECTION WITHIN 250 M 72
FIGURE 66. WESTBOUND 10 MILE RD. PACKETS RECEIVED, RANGE AND RSSI WITHIN 250 M RANGE OF INTEREST FOR SAFETY APPLICATIONS 73
FIGURE 67. NUMBER OF OUTAGES AND LENGTH IN WESTBOUND DIRECTION WITHIN 250 M 73
FIGURE 68. SOUTHBOUND 10 MILE RD. PACKETS RECEIVED, RANGE AND RSSI WITHIN 250 M RANGE OF INTEREST FOR SAFETY APPLICATIONS 74
FIGURE 69. NUMBER OF OUTAGES AND LENGTH IN SOUTHBOUND DIRECTION WITHIN 250 M 74
FIGURE 70. NORTHBOUND 10 MILE RD. PACKETS RECEIVED, RANGE AND RSSI WITHIN 250 M RANGE OF INTEREST FOR SAFETY APPLICATIONS 75
FIGURE 71. NUMBER OF OUTAGES AND LENGTH IN NORTHBOUND DIRECTION WITHIN 250 M 75
FIGURE 72. RSSI LEVEL AND PACKET RECEPTION IN ALL DIRECTIONS AND MULTIPLE LANES AT ORCHARD LAKE AND 10 MILE ROAD WITHIN 250 M OF RSU LOCATION 76
FIGURE 73. CUMULATIVE NUMBER OF OUTAGES AND RESPECTIVE LENGTH OF TIME AT ORCHARD LAKE AND 10 MILE ROAD WITHIN 250 M OF RSU LOCATION 77
FIGURE 74. DISTANCE, VEHICLE SPEED AND SIGNAL STATE FOR AN EASTBOUND RUN 78
FIGURE 75. SIGNAL STATE AND TIME TO NEXT STATE AS RECEIVED BY OBU 79
FIGURE 76. ONE-SECOND QUANTIZATION OF TIME TO NEXT STATE AS RECEIVED BY OBU 79
FIGURE 77. ORCHARD LAKE & 10 MILE RD INTERSECTION. CURRENT SIGNAL STATE AS RECEIVED BY THE OBU FROM THE RSU 80
FIGURE 78. EASTBOUND 10 MILE RD. PACKETS RECEIVED, RANGE AND RSSI @ 12 DBM 81
FIGURE 79. WESTBOUND 10 MILE RD. PACKETS RECEIVED, RANGE AND RSSI @ 12 DBM 82
FIGURE 80. RSU TO THE LEFT OF TRUCK BEING OBSTRUCTED FROM OBU 83
FIGURE 81. WESTBOUND 10 MILE RD. PACKETS RECEIVED, RANGE AND RSSI @ 6 DBM 84
FIGURE 82. EASTBOUND 10 MILE RD. PACKETS RECEIVED, RANGE AND RSSI @ 6 DBM 84
FIGURE 83. WESTBOUND 10 MILE RD. PACKETS RECEIVED, RANGE AND RSSI @ 3DBM 85

FIGURE 84. EASTBOUND 10 MILE RD. PACKETS RECEIVED, RANGE AND RSSI @ 3 DBM..... 86
FIGURE 85. RSSI VERSUS RANGE AT VARIOUS POWER SETTINGS..... 87
FIGURE 86. ONE RSU AND TWO OBUS CROSSING PATHS TESTING. GM-OBU TRAVELING EASTBOUND, FORD-OBU TRAVELING SOUTHBOUND. 89
FIGURE 87. ONE RSU AND TWO OBUS CROSSING PATHS TESTING. GM-OBU TRAVELING WESTBOUND, FORD-OBU TRAVELING NORTHBOUND. 90
FIGURE 88. RANGE FROM RSU, VEHICLE SPEED AND BRAKING INFORMATION AS RECEIVED BY GM-OBU AND FORD-OBU WHILE TRAVELING ON INTERSECTION CROSSING PATHS 91
FIGURE 89. LEGEND FOR VEHICLES 93
FIGURE 90. TEST TRACK AT MPG 94
FIGURE 91. TEST SCENARIO NO. 4.1.1 94
FIGURE 92. DISTANCE AND RSSI CALCULATED FROM DATA RECEIVED BY GM26 95
FIGURE 93. SPEED AND BRAKE STATUS OF FORD28 RECEIVED BY GM26 96
FIGURE 94. YAW RATE OF FORD28 RECEIVED BY GM26 96
FIGURE 95. LONGITUDINAL ACCELERATION OF FORD28 RECEIVED BY GM26 97
FIGURE 96. LATERAL ACCELERATION OF FORD28 RECEIVED BY GM26..... 97
FIGURE 97. NUMBER OF PACKETS FROM FORD28 RECEIVED BY GM26 98
FIGURE 98. TEST SCENARIO NO. 4.1.2 98
FIGURE 99. DISTANCE AND RSSI CALCULATED FROM DATA RECEIVED BY FORD28..... 99
FIGURE 100. SPEED FROM DATA RECEIVED BY FORD28 100
FIGURE 101. LONGITUDINAL ACCELERATION FROM DATA RECEIVED BY FORD28 100
FIGURE 102. NUMBER OF PACKETS FROM GM26 RECEIVED BY FORD28 101
FIGURE 103. TEST SCENARIO NO. 4.1.3 101
FIGURE 104. DISTANCE AND RSSI CALCULATED FROM DATA RECEIVED BY FORD28..... 102
FIGURE 105. NUMBER OF PACKETS FROM GM26 RECEIVED BY FORD28 103
FIGURE 106. DISTANCE AND RSSI CALCULATED FROM DATA RECEIVED BY FORD28..... 104
FIGURE 107. NUMBER OF PACKETS FROM GM26 RECEIVED BY FORD28 104
FIGURE 108. DISTANCE AND RSSI CALCULATED FROM DATA RECEIVED BY FORD28..... 105
FIGURE 109. NUMBER OF PACKETS FROM GM26 RECEIVED BY FORD28 106
FIGURE 110. DISTANCE AND RSSI CALCULATED FROM DATA RECEIVED BY FORD28..... 107
FIGURE 111. NUMBER OF PACKETS FROM GM26 RECEIVED BY FORD28 107
FIGURE 112. SEVEN VEHICLE CARAVAN..... 108
FIGURE 113. DISTANCES CALCULATED FROM DATA RECEIVED BY FORD28..... 110
FIGURE 114. SPEED AND BRAKE STATUS RECEIVED BY FORD28 110
FIGURE 115. YAW RATE RECEIVED BY FORD28..... 111
FIGURE 116. LONGITUDINAL ACCELERATION RECEIVED BY FORD28 111
FIGURE 117. LATERAL ACCELERATION OF RECEIVED BY FORD28..... 112
FIGURE 118. NUMBER OF PACKETS FROM OTHER VEHICLES RECEIVED BY FORD28..... 112
FIGURE 119. DISTANCES CALCULATED FROM DATA RECEIVED BY FORD28..... 114
FIGURE 120. SPEED AND BRAKE STATUS RECEIVED BY FORD28 114
FIGURE 121. YAW RATE RECEIVED BY FORD28..... 115
FIGURE 122. LONGITUDINAL ACCELERATION RECEIVED BY FORD28 115
FIGURE 123. LATERAL ACCELERATION OF RECEIVED BY FORD28..... 116
FIGURE 124. NUMBER OF PACKETS FROM OTHER VEHICLES RECEIVED BY FORD28..... 116
FIGURE 125. DISTANCES CALCULATED FROM DATA RECEIVED BY FORD28..... 118
FIGURE 126. SPEED AND BRAKE STATUS RECEIVED BY FORD28 118

FIGURE 127. YAW RATE RECEIVED BY FORD28 119
FIGURE 128. LONGITUDINAL ACCELERATION RECEIVED BY FORD28 119
FIGURE 129. LATERAL ACCELERATION OF RECEIVED BY FORD28 120
FIGURE 130. NUMBER OF PACKETS FROM OTHER VEHICLES RECEIVED BY FORD28 120

TABLE OF TABLES

TABLE 1. OAKWOOD/MICHIGAN AND CROOKS/BIG BEAVER INTERSECTION 3
TABLE 2. SANTA CLARA/MARKET AND HILLVIEW/HANOVER INTERSECTION 4
TABLE 3. WOODWARD/I-696 SERVICE DRIVE AND EL CAMINO REAL/5TH AVENUE INTERSECTION 5
TABLE 4. WOODSIDE/CHURCHILL AND COUNTRY CLUB/12 MILE INTERSECTION 6
TABLE 5. AUBURN/SQUIRREL AND SAND HILL/WHISKEY HILL INTERSECTION 7
TABLE 6. LONG LAKE/LAHSER AND QUARTON/LAHSER INTERSECTION 8
TABLE 7. SKYLINE/WOODSIDE AND PAGE MILL/DEER CREEK INTERSECTION 9
TABLE 8. SQUIRREL & LONG LAKE INTERSECTION 10
TABLE 9. RSU MESSAGE 64
TABLE 10. WRM CONFIGURATION FOR RSU MESSAGE (FULL DBM) 68
TABLE 11. WRM CONFIGURATION FOR RSU MESSAGE (12DBM) 81
TABLE 12. WRM CONFIGURATION FOR RSU MESSAGE (6 DBM) 83
TABLE 13. WRM CONFIGURATION FOR RSU MESSAGE (3 DBM) 85
TABLE 14. PARAMETERS FOR TEST SCENARIO NO. 4.1.1 94
TABLE 15. PARAMETERS FOR TEST SCENARIO NO. 4.1.2 98
TABLE 16. PARAMETERS FOR TEST SCENARIO NO. 4.1.3 101
TABLE 17. PARAMETERS FOR TEST SCENARIO NO. 4.2.1 109
TABLE 18. PARAMETERS FOR TEST NO. 4.2.2 113
TABLE 19. PARAMETERS FOR TEST SCENARIO NO. 4.2.3 117

1 OVERVIEW

1.1 Goals

The overall goal of the activities described in this appendix was to test and evaluate communications functionalities for potential vehicle safety implementations, in order to continue pre-competitive research into the feasibility of using 5.9 GHz DSRC to enable and enhance vehicle safety systems and applications. Throughout this testing, the main focus was on evaluating communications data necessary to establish feasibility and to enable the future design and development of two potential vehicle safety applications – traffic signal violation warning and emergency electronic brake lights. Communication scenarios were developed that would support early prototype vehicle safety applications in order to evaluate communications requirements. As used herein, communication scenarios include transmissions between a roadside unit (RSU) and an on-board unit (OBU), as well as OBU-to-OBU, relevant to potential safety applications in real-world environments. The activities focused on data collection and analysis in preparation for the full functionality prototype development of prospective vehicle safety applications.

For the RSU to OBU case, the goal within this task was to work towards implementation requirements for interfacing with existing infrastructure traffic control equipment to effectively establish vehicle safety applications. Part of this work consisted of cooperation with local road authorities to understand the hurdles of an installed, safety-specific test RSU as required for the traffic signal violation warning prototype application scenario. In addition, arrangements were made to send test data from roadside locations in real-world intersection locations using a programmed controller box.

For the OBU to OBU case, the major focus was on the implementation of the standard vehicle message set being developed by SAE to support vehicle-to-vehicle safety applications such as emergency electronic brake lights. A test plan was developed and conducted for both test track and public roadway environments. The goal of the testing in this portion of the task was to evaluate available DSRC standards for communications reliability, update rate, and range under vehicle-to-vehicle operations.

The collected data under Task 10 served two purposes:

- To begin to assess the viability of DSRC communications in real-world conditions.
- To provide raw data as a basis for potential future safety application algorithm development in a simulation environment.

1.2 Test Plan

Three types of testing were identified as requiring additional attention above and beyond that testing accomplished within the scope of Task 4:

- **Transmission Characteristics at Intersections –** Although some Task 4 testing took place in public road settings, a great deal of the testing was conducted at test track facilities, and no specific efforts were aimed at identifying troublesome/unique intersections or determining expected performance at these junctures.

- **Intersection Controller Data Exchange –** Task 3 identified theoretical information that might be sent from an intersection controller, but no actual controller broadcast tests had been attempted during Task 4 testing due to hardware constraints. Investigating the hurdles of such information exchange was seen as crucial to enable future application development.

- **Vehicle Data Exchange –** Task 4 provided extensive vehicle-to-vehicle testing, but the packets consisted mostly of random filler, and provided no instantaneous information from the vehicle's electrical architecture and sensors. Proving the ability to exchange such information between manufacturers was seen as crucial to enable future application development.

1.2.1 Transmission Characteristics at Intersections

Various intersections in the Detroit and San Francisco Bay areas were selected for their unique characteristics in order to gain a better understanding of how these variations affect DSRC communications. For the sake of expediency, the Task 4 Communication Test Kits (CTKs) and the Task 6C antennas were used as an improvised roadside unit, with a few modifications to the antenna mounting arrangement. Though the Task 6C antennas were designed for vehicle mounting, their omni-directional functionality was deemed to be desirable for determining the general transmission characteristics of a CTK broadcasting from one of the corners at each selected intersection. The investigation focused on plotting the relative received signal strength of transmissions sent from the stationary RSU and received on portable test equipment carried in a moving vehicle.

A number of intersections in both the Palo Alto and Detroit teams were evaluated using the improvised RSU equipment. The specific intersections evaluated covered a broad range of roadway geometries, structural/terrain occlusions, and traffic environments. The pages that follow (Tables 1-8) identify the selected intersections and describe the features that are of particular interest. The findings from these evaluations are presented in Section 2 of this appendix.

Location	Setting/Traffic	Configuration	Obstructions	Illustration
Oakwood Boulevard & Michigan Avenue Dearborn, MI	Urban area normally experiences heavy daytime traffic	2 lanes in each direction and a center lane for left turns at the intersection Oakwood Blvd rises to the north and crests a small hill. It descends to the south, bending out of sight around a corner	Densely packed buildings and tree-lined sidewalks A concrete buttressed railroad overpass to the south on Oakwood Blvd	
Crooks Road & Big Beaver Road Troy, MI	Urban area continually full of moving traffic during the daytime hours	3 lanes each way eastbound and westbound on Big Beaver Road, separated by medial strip Fewer lanes of traffic in the north and southbound directions on Crooks Road	Buildings nearby (a few with 10 floors or more), but the buildings are far removed by large parking lots Small trees and bushes on the media strip	

Table 1. Oakwood/Michigan and Crooks/Big Beaver Intersection

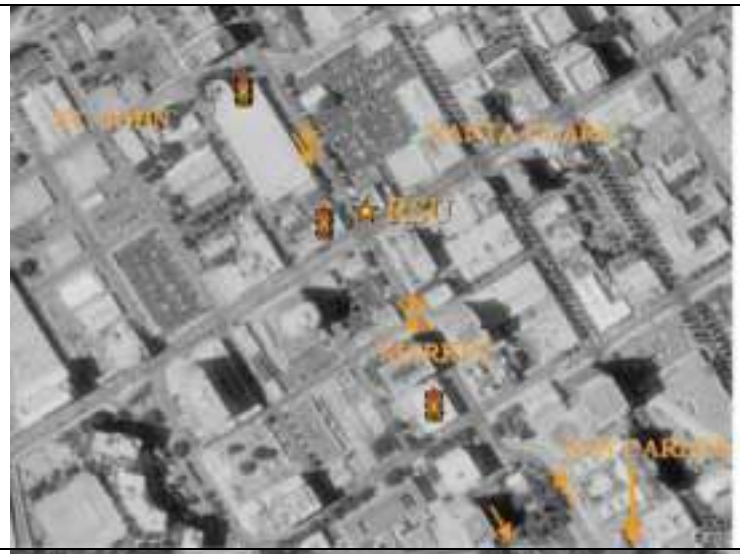
Location	Setting/Traffic	Configuration	Obstructions	Illustration
Santa Clara Street & Market Street San Jose, CA	Urban area with heavy traffic during the time of the testing	2 lanes in each direction and a center lane for left-turns at the intersection.	There are closely packed high rises and trees along both sides of Market Street.	
Hillview Avenue & Hanover Street Palo Alto, CA	Urban area with light traffic during daytime	Both Hillview and Hanover have a single lane in both directions and a center lane for left-turns at the intersection	The north end of Hanover is slightly uphill and the south end has a 90-degree bend to the west	

Table 2. Santa Clara/Market and Hillview/Hanover Intersection

Location	Setting/Traffic	Configuration	Obstructions	Illustration
Woodward Avenue & I-696 Service Drive Huntington Woods, MI	Urban area with medium to heavy traffic during the day	4 lanes in the southbound direction and 5 lanes in the westbound direction, both include a left turn lane	Line of sight on southbound Woodward is blocked by terrain and trees along the curve in the road Vehicles pass beneath an overhanging parking garage just before the intersection	
El Camino Real & 5th Avenue Atherton, CA	Suburban area with medium traffic during the time of the testing	El Camino has three lanes for each direction and two additional lanes for left-turning onto 5th 5th has two lanes for each direction and one left turn lane for southbound El Camino	A moderate amount of trees and buildings are along both sides of El Camino and the south-end is slightly curved	

Table 3. Woodward/I-696 Service Drive and El Camino Real/5th Avenue Intersection

Location	Setting/Traffic	Configuration	Obstructions	Illustration
Woodside Road & Churchill Avenue Redwood City, CA	Suburban area with medium traffic during the daytime	Woodside has two lanes in both directions and Churchill has one in both directions Woodside has a left turn lane with a traffic light at the Churchill intersection	There are plenty of trees along both sides of Woodside Both directions on Woodside away from the intersection have uphill slopes, and the south end is slightly curved to the west	
Country Club Drive & 12 Mile Road Farmington Hills, MI	Suburban area with light to heavy traffic conditions depending on the time of day	Eastbound 12 Mile has 2 lanes and a right turn lane. Westbound 12 Mile has 2 lanes and a left turn lane Country Club Drive has 2 lanes in each direction separated by a median strip	Country Club Drive has an obstructed line of sight to the RSU due to several trees Vehicles traveling East on 12 Mile Road also have obstructed line of sight due to trees	

Table 4. Woodside/Churchill and Country Club/12 Mile Intersection

Location	Setting/Traffic	Configuration	Obstructions	Illustration
Auburn Road & Squirrel Road West Bloomfield, MI	Suburban area with light traffic during the time of testing	Auburn Road has two lanes in each direction Squirrel Road has 1 lane in each direction and a center left turn lane	Squirrel Road curves suddenly just north of the intersection and the line of sight is blocked by terrain along the curving roadway	
Sand Hill Road & Whiskey Hill Road Menlo Park, CA	Suburban area with medium traffic conditions. Sand Hill runs relatively north-south, and Whiskey Hill intersects Sand Hill at an angle, coming from the north-east	There is a triangle-shaped median with stop sign in the middle of the intersection, separating Sand Hill from two branches of traffic that move southbound on Whiskey Hill	There are a number of tall trees and shrubs There are up-hill grades in both directions on Sand Hill going away from the intersection	

Table 5. Auburn/Squirrel and Sand Hill/Whiskey Hill Intersection

Location	Setting/Traffic	Configuration	Obstructions	Illustration
Long Lake Road & Lahser Road Bloomfield Hills, MI	Suburban area. Long Lake Road has a steady amount of residential traffic during the daytime hours Lahser Road has slower, sparser traffic than Long Lake Road	Long Lake Road has two lanes of traffic in the east and westbound directions North and southbound Lahser Road has one lane of traffic in both directions	Trees and bushes encircle the intersection and block line-of-sight in at least one, if not all, directions A hill north of the intersection prevents line-of-sight to the traffic light until about 150m from the intersection	
Quarton Road & Lahser Road Auburn Hills, MI	Suburban area with medium traffic during the time of testing	Aside from left and right turn lanes at the intersection, these roads are limited to one lane of traffic in either direction	Considerable foliage close to the shoulder of the roads Quarton rises to a hill about 200m to the east, and to the west, the road bends, disappearing from view within ~100m	

Table 6. Long Lake/Lahser and Quarton/Lahser Intersection

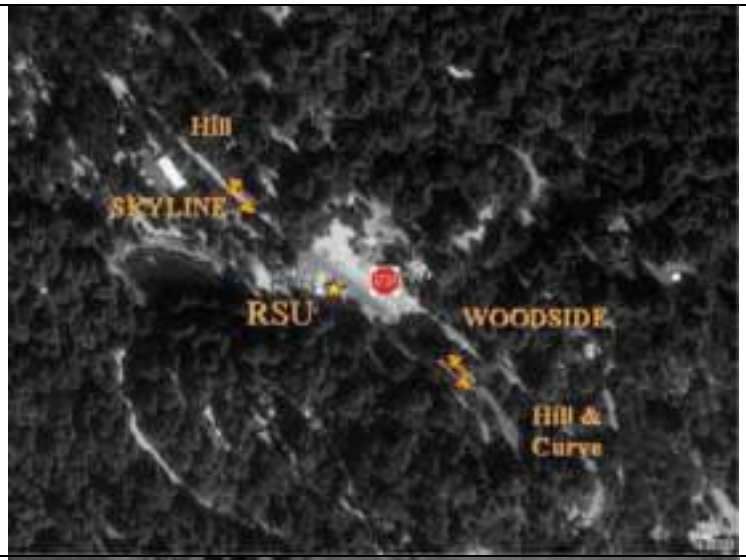
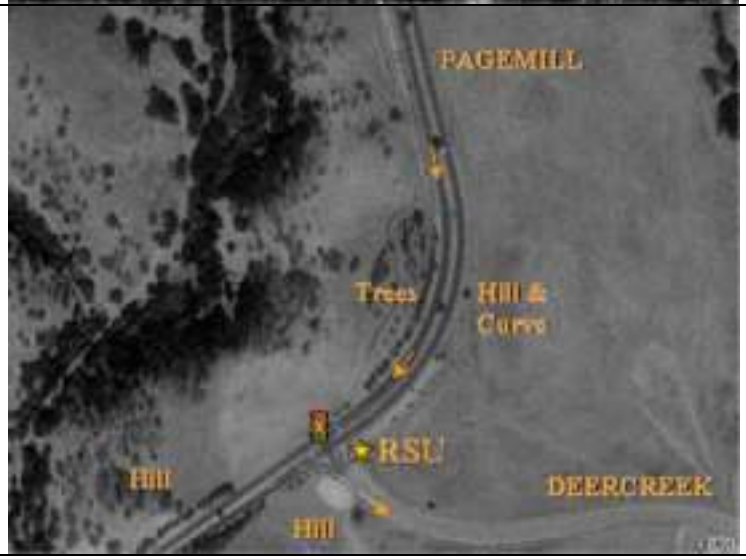
Location	Setting/Traffic	Configuration	Obstructions	Illustration
Skyline Boulevard & Woodside Road Redwood City, CA	Suburban area with light traffic during the daytime	Both Skyline and Woodside have a single lane in both directions There are stop signs on Woodside at the intersection, but none on Skyline	Both directions on Skyline have uphill slopes and the southeastern end gradually curves to the south. Dense foliage throughout the area and surrounding the intersection.	
Page Mill Road & Deer Creek Road Palo Alto, CA	Rural area with medium traffic during the daytime	Both roads have two lanes in both directions Page Mill has a left turn lane with a traffic light at the Deer Creek intersection	Southbound Page Mill Road curves slowly toward the southwestern direction and goes uphill There are trees along the curve of Page Mill Road	

Table 7. Skyline/Woodside and Page Mill/Deer Creek Intersection

Location	Setting/Traffic	Configuration	Obstructions	Illustration
Squirrel Road & Long Lake Road Bloomfield Hills, MI	Suburban area with light traffic during the time of the testing	1 lane in either direction for both roads, with left and right turn lanes at the intersection to accommodate the extreme curves of Long Lake Road	Squirrel Road has overhead foliage, as well as hills, both of which descend in the southbound direction Long Lake Road has terrain and foliage along the curving roadway that eventually blocks the direct line of sight to the intersection	

Table 8. Squirrel & Long Lake Intersection

1.2.2 Intersection Controller Data Exchange

After identifying applications in Task 3 that would utilize information sent from an intersection controller, a feasibility study covering this type of information exchange was seen as crucial to enable future application development. The Task 9 testing system was designed to interface with such a controller for this purpose. Rather than connecting the test equipment to a traffic signal controller that actually controls traffic lights, it was decided that it should be connected to a second controller to be purchased by the VSCC. This second controller could be programmed with exactly the same timing as the actual controller, eliminating any risk of inadvertent interference.

The choice of which signalized intersection to run the tests could be based on factors such as the previous establishment of a cooperative atmosphere between the VSCC and the Road Commission of Oakland County (RCOC), and also the elimination of those locations where the dynamic control of the traffic lights changes the signal timing. Testing at such an intersection would add another dimension of complexity that was beyond the scope of this preliminary feasibility study. The intersection chosen for the test was Orchard Lake Road and 10 Mile Road in Farmington, Michigan (Figure 1). The traffic signal controller shown in the inset of Figure 1 was programmed by the RCOC to use exactly the same timing as the controller at the selected intersection.

Figure 1. Controller Test Site at Orchard Lake Road and 10 Mile Road

The following tests were chosen for the traffic controller investigation:

- **Communication Performance Assessment:** A test to assess the communication performance at the intersection by comparing the amount of packets received with the amount of those sent

- **Traffic Signal Status Plot:** Plotting the instantaneous traffic status with respect to the location where the moving test vehicle receives the data

- **Reduced Power Transmit Testing:** A set of tests to investigate transmission power control by running successive trials at power levels of 12, 6, and 3 dBm

- **Vehicle-Vehicle and Vehicle-Infrastructure Testing:** An analysis that considers whether communications can be established and maintained between two OBU vehicles traveling on perpendicular legs of an intersection with a relatively low building density in the near vicinity

Section 3 of this report describes the results of these investigations.

1.2.3 Vehicle Data Exchange

Several vehicle-to-vehicle communication tests were conducted to evaluate the WAVE Radio Modules (WRMs) that were developed in Task 6D. This testing would also feature the wireless exchange of CAN data between different vehicle makes. In order to vary the circumstances of the evaluation, the locations chosen for testing included the Milford Proving Grounds, the I-96 freeway, and the M-5 ramp to Twelve Mile Road, all in Michigan.

At the beginning of the Task 10 activity, it was noted that interfacing between the DSRC test equipment and an on-vehicle CAN bus could most readily be achieved by leveraging prior work completed within the CAMP project. It was determined that testing could be conducted using a Jaguar XKR developed by Ford for the EDMap project, and two Buick LeSabres developed by GM for the ACAS project. Other vehicles (all shown in Figure 2) would participate in a number of the tests and be capable of receiving the CAN vehicle signals broadcasted over the DSRC Control Channel. The following tests were selected for this phase of the vehicle-to-vehicle communications evaluation:

- **Test for Omni-Directional Coverage:** One test vehicle travels in a circle around a second vehicle to verify 360º coverage and overall signal reception.

- **Lead Vehicle Brake Test:** A braking test for two vehicles traveling in the same direction, intended to clarify the potential of DSRC to prevent rear-end collisions.

- **Test for Maximum Vehicle Range:** A slow-moving test to determine the maximum communication ranges and to identify if there are null zones for vehicle-to-vehicle communications.

- **Test for Communication Performance Under High Vehicle Speed:** A test to determine if there is degradation in communication performance under high relative speed conditions (70 mph for vehicles traveling in opposite directions).

- **Test for Communication Range Under Low Transmit Power:** A test to determine the reduction in communication range under low Transmit Power conditions.

- **Test for Communication Performance Under High Data Rate:** a test to determine the degradation in communication performance under high Data Rate transmissions (increased from 6 to 27 Mbps).

- **Vehicle-to-Vehicle Communications Testing:** A series of tests conducted on the I-96 freeway and the M-5 ramp in Michigan in order to evaluate communications performance on freeways

The results of these tests are described in Section 4 of this appendix.

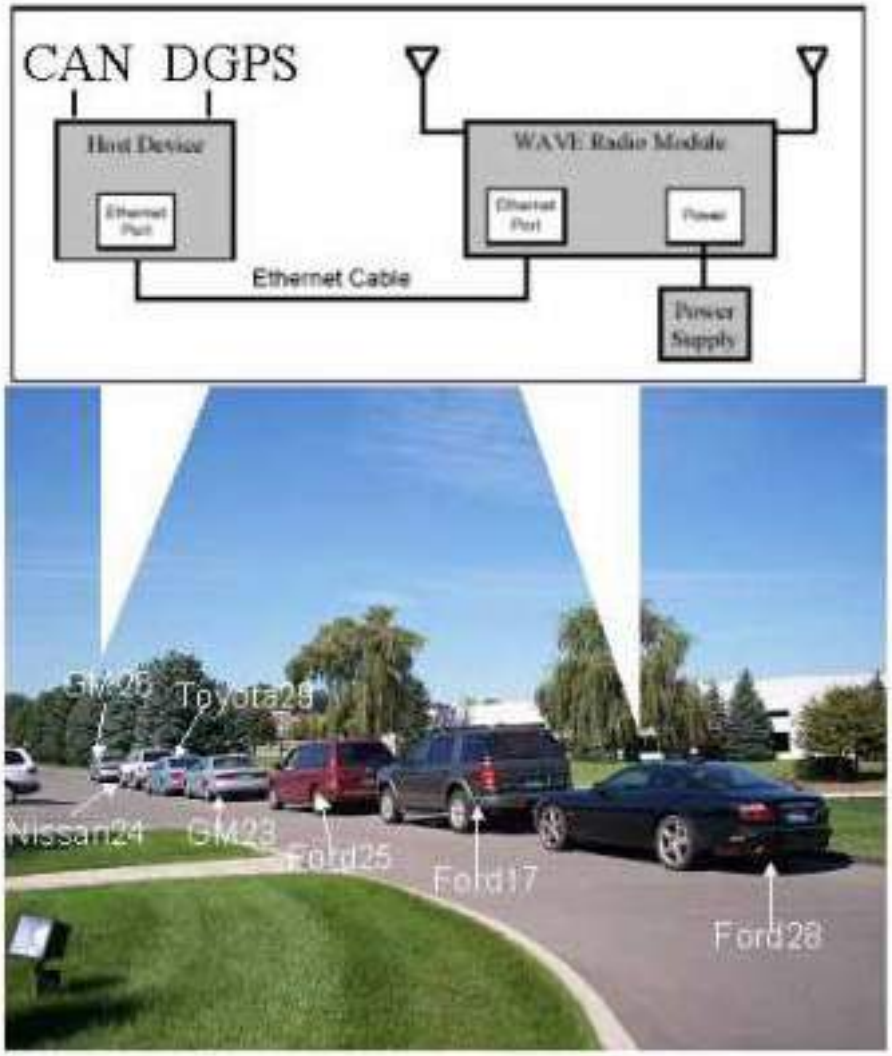


Figure 2. Seven Vehicle Caravan with CAN Connectivity Highlighted

2 TEST RESULTS FOR INTERSECTIONS

The Task 10 field-testing program was carried out for the most part on public roadways, with some baseline studies and equipment verifications conducted using the test track facilities at GM's Milford Proving Grounds. All intersection testing with portable equipment placed near the edge of each thoroughfare was conducted with prior approval from the public jurisdictions that were responsible for the intersections. The testing followed the planning set forth in Section 1.2 of this report, with the intention of investigating several remaining issues that were not covered within the Task 4 test scope.

2.1 Intersection Testing

In determining the appropriate equipment needed to carry out the Task 10 intersection tests, the antennas developed by M/A-COM during the Task 6C effort were applied to a test setup that satisfied potential height and placement characteristics of a DSRC roadside unit (RSU). In order to satisfy the objectives of the Task 10 testing, improvised RSUs were assembled as illustrated in Figures 3-6.

The Task 6C antenna was inverted and suspended approximately 10 feet above the roadside by means of a cross member attached to telescoping poles anchored into a heavy base plate. Transmitting both outward and towards the ground, the elevated antenna was basically mounted upside down in order to cover nearly the same vehicle-accessible area that the antenna normally would if mounted on an automobile.

- For the testing conducted in the Detroit area, the M/A-COM roof mount units were selected, which required the addition of a 1m diameter metalized foam disk to provide the ground plane necessary to produce the proper antenna radiation pattern.

- For the testing conducted in the Palo Alto area, the M/A-COM mirror mount units were utilized, which did not require a similar ground plane.

- It should be noted that these antennas were designed to provide broadcast coverage from the exterior of an automobile, and therefore the radiation patterns from the test setups were not optimized for RSU operation, but did serve as a consistent means to compare broadcast characteristics across a broad range of intersections.

The Communication Test Kits (CTKs) from Task 4 were utilized to acquire the intersection testing data. The laptop computer, running the latest version of test software under Linux (V3.0.4), was mounted on a platform attached to the telescoping poles so that signal losses in the cables to the antennas would be minimized. The GPS antenna was placed nearby on the ground, typically in a position where interference from various objects (antenna ground plane, intersection features, test personnel, etc.) would be minimized. As such, there is often a minor

offset of a few meters between the actual RSU broadcast location and the recorded GPS coordinates. Also visible in the following figures is a portable battery pack, which was used to power the GPS receiver unit.

Figure 3. RSU at Detroit Area Test Location
Figure 4. RSU at Palo Alto Area Test Location
Figure 5. RSU at Detroit Area Test Location
Figure 6. RSU at Palo Alto Area Test Location

Unless otherwise specified, Detroit area test parameters were set as follows for each data set reported:

- Broadcast frequency: 5.8GHz
- Broadcast power level: 100%
- Update rate: 10Hz
- Packet size: 500B
- Data rate: 6 Mbps

The San Francisco Bay area test parameters can be categorized into two parts: Testing with the Linux CTK software and testing with the Task 9 software. All of the Bay area tests were conducted with the Linux CTK software, with the exception of those that took place at the El Camino Real and 5th Avenue intersection, which utilized the VSCC Task 9 software. All testing with the Linux CTK had the following settings:

- Broadcast frequency: 5.8GHz
- Broadcast power level: 100%
- Update rate: 10 Hz
- Packet size: 500 bytes
- Data rate: 6 Mbps
- 10 feet height for the RSU antenna.

The testing with the Task 6D and Task 9 application had slightly different settings:

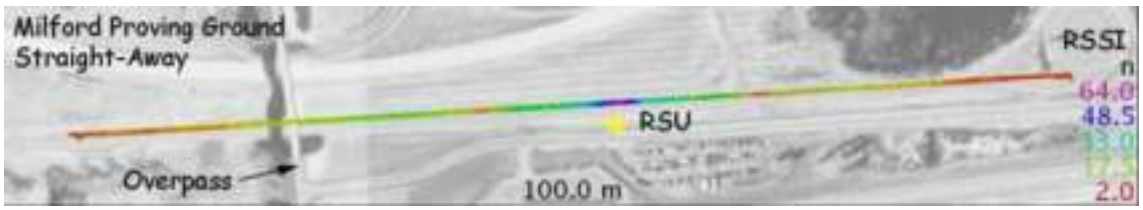
- Broadcast frequency: 5.89GHz
- Broadcast power levels: 100%, 50%, and 10%
- Data rate: 6 Mbps

In general, multiple test runs were completed for each directional approach to the intersection that was evaluated. After the test runs were completed, the test data was analyzed and evaluated. A cumulative summary for all directional approaches that we tested was then prepared, as well as individual summaries for each directional approach undertaken.

2.1.1 Baseline Evaluation and Test Equipment Verification

Prior to performing tests at actual intersections, a variety of data was acquired at the Milford Proving Grounds. Previous experience had indicated that variability existed between some of the CTKs. This motivated the investigation of the communications performance of the CTKs, with both old and new antenna designs, and in the absence of traffic and obstructions. Figures 7 shows a sample of the data obtained while driving an out-and-back circuit on the long straight-away track.

The upper portion of Figure 7 serves to illustrate a new data visualization tool that is used to present test results. Received packets are overlaid upon an aerial photo of the testing site, with each packet being color-coded to reflect the value of the Received Signal Strength Indicator (RSSI). All of the RSSI plots in this report were generated using publicly available visualization software provided by Adam Schneider.



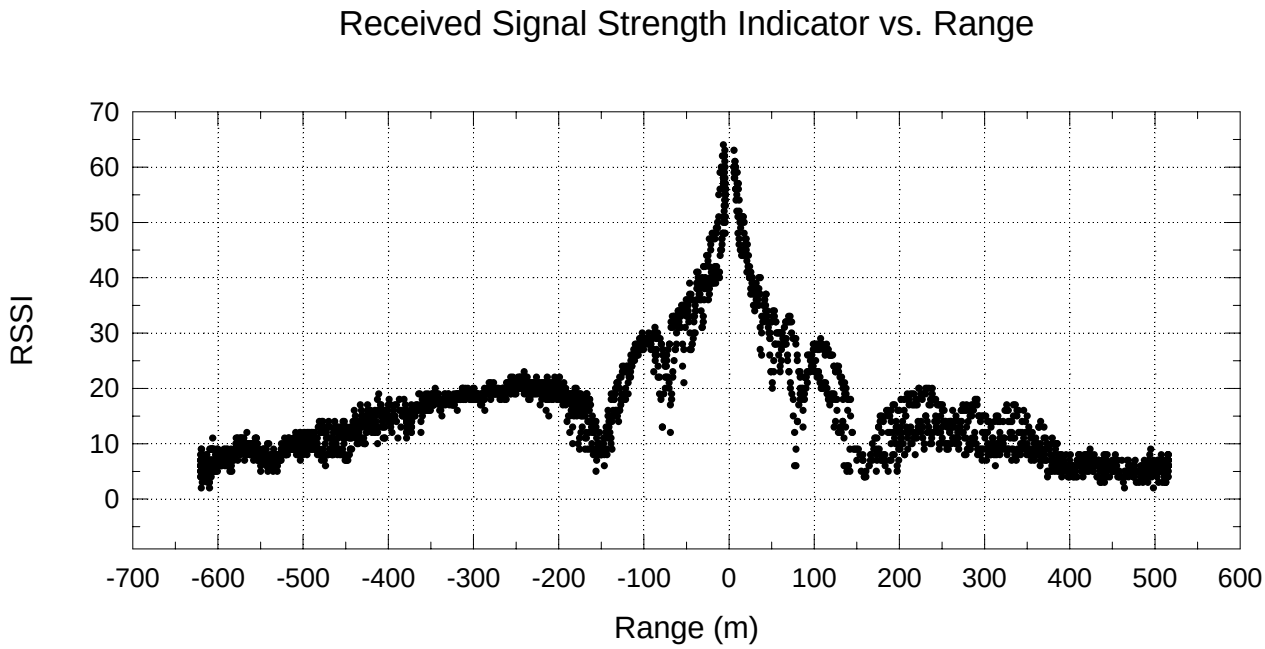


Figure 7. RSU Equipment Verification at Milford Proving Ground

The lower portion of Figure 7 plots RSSI as a function of range from the improvised RSU, with data to the west arbitrarily plotted as negative range values and data to the east as positive range values. It was observed that there were local minima in the RSSI at ranges corresponding to ~75m and ~150m, which reflected the geometry of the radio propagation for the setup, an anticipated phenomenon described in detail within the "Multipath Considerations" chapter of Appendix C. Although the data to the west and east are not entirely symmetric, they are very nearly so, with the small differences likely due to the asymmetries built into the test stand and those due to the ground terrain, including the overpass to the west.

Based upon a variety of data sets similar to the one shown above, it was determined to be appropriate to use the new M/A-COM antennas for sending and receiving. Additionally, some variability between test kits was documented, and thus it was important, for the purposes of comparing results, to use the exact same equipment in all subsequent tests. As such, each component of the setup was carefully labeled and used for the entirety of the Detroit area testing.

After demonstrating adequate performance of the improvised test equipment, similar data was gathered at the intersections that were outlined in Section 1.2.1. The sections that follow describe the findings at each of these intersections.

2.1.2 Oakwood Boulevard & Michigan Avenue

Five lanes extend out from this signalized intersection in each of four directions, and the intersection normally experiences heavy daytime traffic. For all of the data acquired, the RSU remained positioned on the southeast corner of the intersection, from which reasonable line of sight was provided in each direction of traffic (Figure 8).

Figure 8. Aerial View of the Oakwood/Michigan Intersection

Oakwood Boulevard rises to the north and crests a small hill roughly a block and a half from the intersection. To the south, it descends, passing beneath a concrete buttressed railroad overpass and then bends out of sight around a corner. A mix of low buildings and parking lots characterizes this stretch of road, and there is relatively little vegetation of consequence. West of the intersection, Michigan Avenue also rises slightly for a block and a half, beyond which line of sight to the RSU is lost. Densely packed buildings and tree-lined sidewalks are present along this segment of road. To the east of the intersection, the road descends uniformly and there are fewer buildings and roadside obstructions.

The test vehicle received data from the RSU while driving along each direction of travel at the intersection. Figure 9 shows the same overhead view of the intersection, but the received packets from the test runs are overlaid upon the aerial photo, with each packet color-coded to correspond with the value of the Received Signal Strength Indicator (RSSI). The RSSI values are listed in the lower left portion of the figure, and as expected, the highest values are found where the test vehicle travels in closest proximity to the RSU.

Figure 9. Aerial View Overlaid with Color-Coded RSSI Values

Proceeding northbound on Oakwood Boulevard in medium density traffic, only 3 packets were dropped at distances to the RSU less than 100m. While reception on the northbound side was entirely consistent with the apparent line of sight to the hillcrest, considerable reception was obtained on the southbound side well beyond line of sight, despite the drop in elevation to pass under the railroad tracks and the subsequent bend present in the road. Clearly, there were reflected signals present due to the physical structures involved. Note that although the GPS signal was lost under the railroad overpass, radio data was still being acquired. Reversing the direction and driving southbound produced similar results, with only 4 packets lost within ~100m of the intersection (Figure 10).

Figure 10. Views from the Oakwood/Michigan Intersection

Heading eastbound on Michigan Avenue in very dense traffic, 3 packets were lost within ~100m of the intersection. While waiting at a red light at the intersection one block west of the RSU, a mere 8 packets were dropped, despite the tightly packed arrangement of vehicles. The westbound direction had a slightly extended range (relative to the eastbound heading), presumably due to the better geometric line of sight to the vehicle. In this case, 2 packets were dropped within ~100m of the intersection. Figure 11 shows the CTK diagrams of the packet reception versus distance. The results demonstrate that packets can be received near this intersection under heavy traffic conditions and with an RSU situated in a less-than-optimal position.

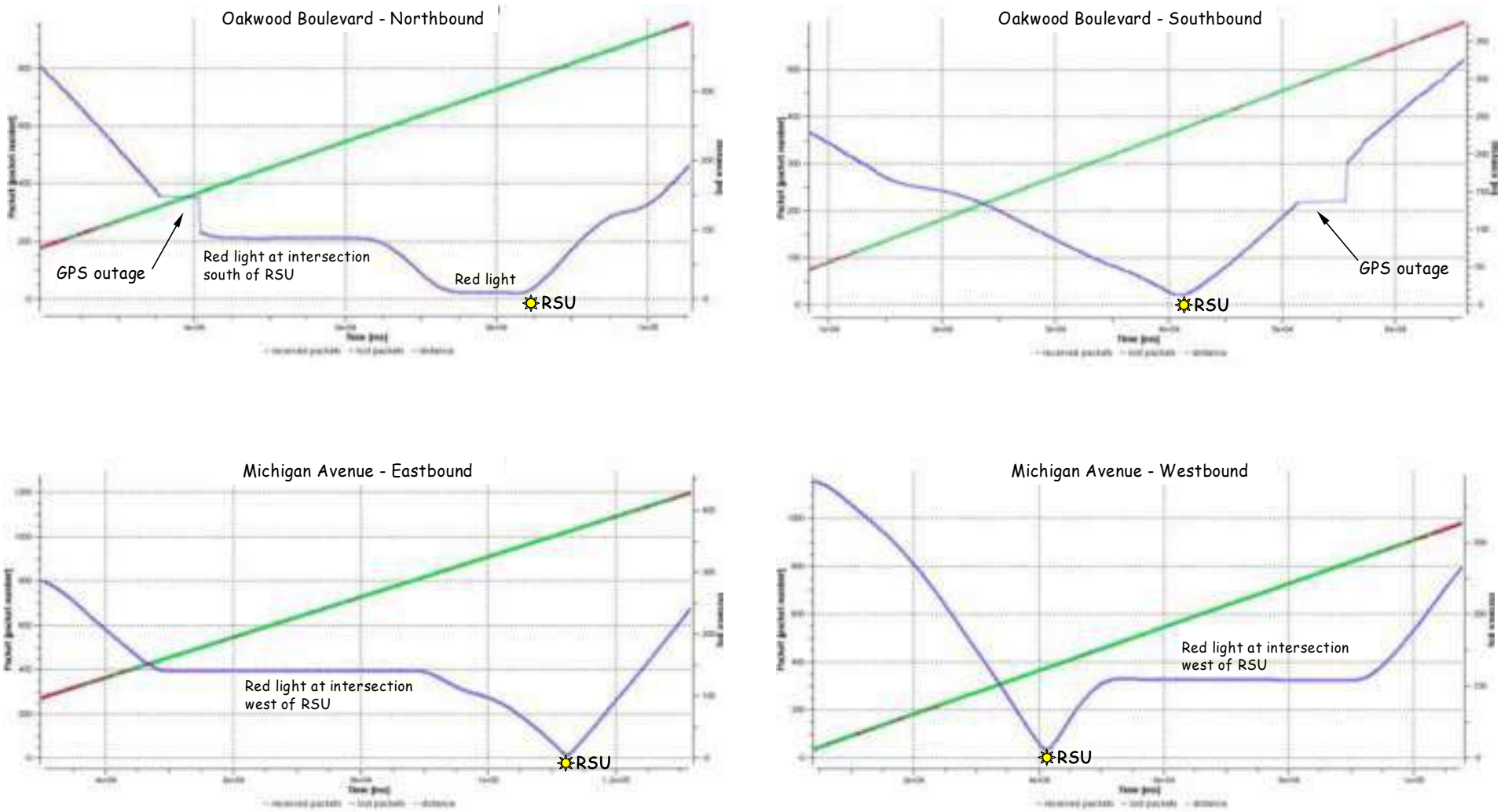


Figure 11. CTK Plots of the Oakwood/Michigan Intersection

2.1.3 Crooks Road & Big Beaver Road

This intersection has three lanes of traffic in the east and westbound directions, and these lanes are continually full of moving traffic during the daytime hours. The north and southbound directions on Crooks Road also have several lanes of traffic, but are not separated by the medial strip (with small trees and bushes) that is found on Big Beaver Road.

Foliage on the medial strip occasionally blocked the line of sight for the RSU, as shown by dropped packets indicated by callouts (1) in Figure 12. One method to help address this issue might be to package the RSU in the traffic light or at a similar height.

Buildings encircle the intersection - some, although not all, are quite tall - but are far removed from the intersection by large parking lots. The RSU was placed on the medial strip on the eastern side of the intersection, and was moved from north to south as necessary to provide best line of sight for each individual data set.

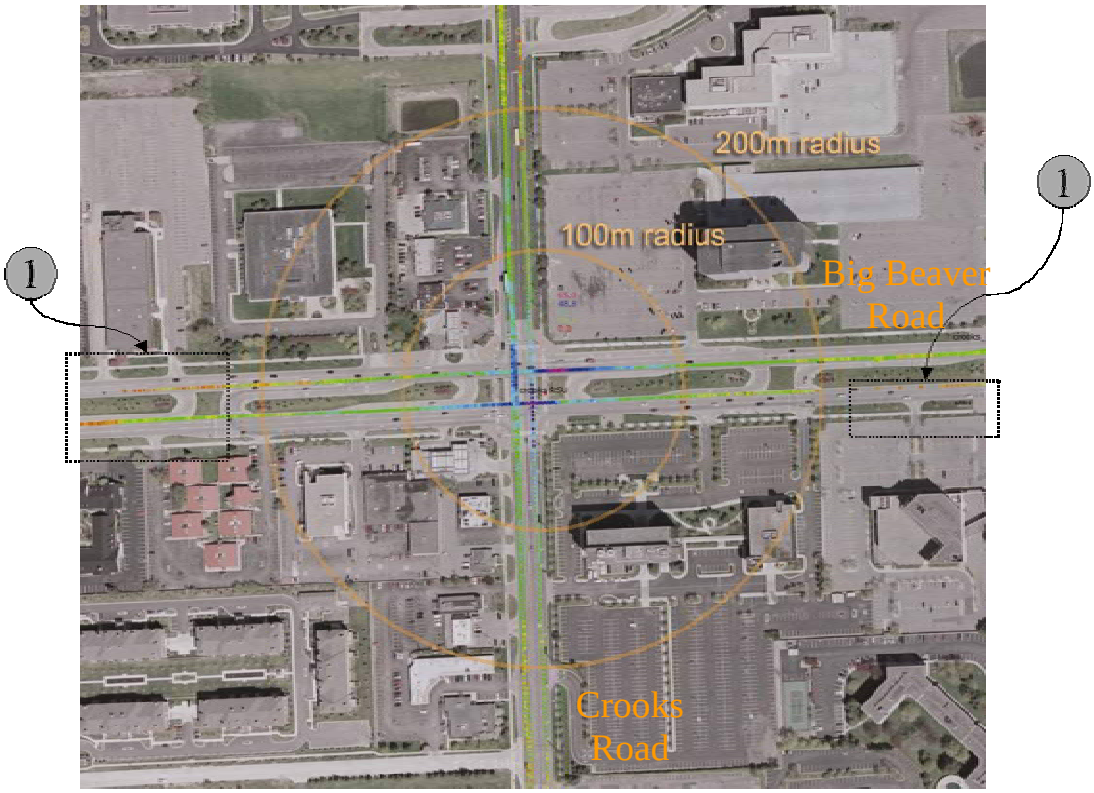


Figure 12. RSSI Plot of the Crooks/Big Beaver Intersection

Traveling northbound on Crooks Road, the test vehicle was stopped at a traffic light 200m beyond the intersection of interest and, meanwhile, traffic behind the receiver was interfering with the signal. This would not be a concern for an intersection-based application since the vehicle had already proceeded through the intersection.

In the other directions of travel (Figure 13), line-of-sight interference caused a low RSSI at a significant distance from the intersection. Yet most of the packets were still received, as shown by callouts in Figure 14. The packets dropped in (2) would not be a concern since the vehicle had already proceeded through the intersection.

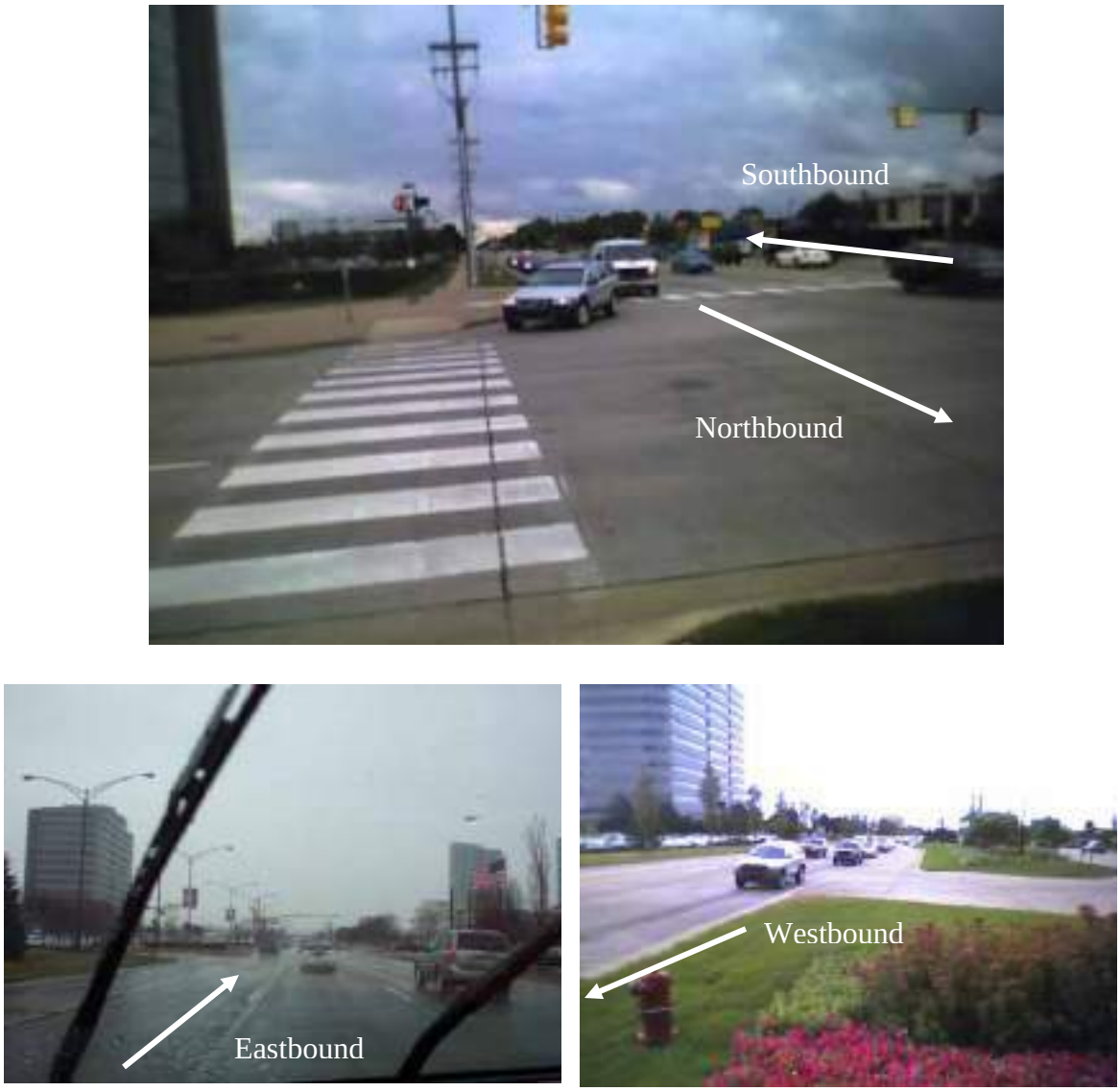


Figure 13. Views of the Crooks/Big Beaver Intersection

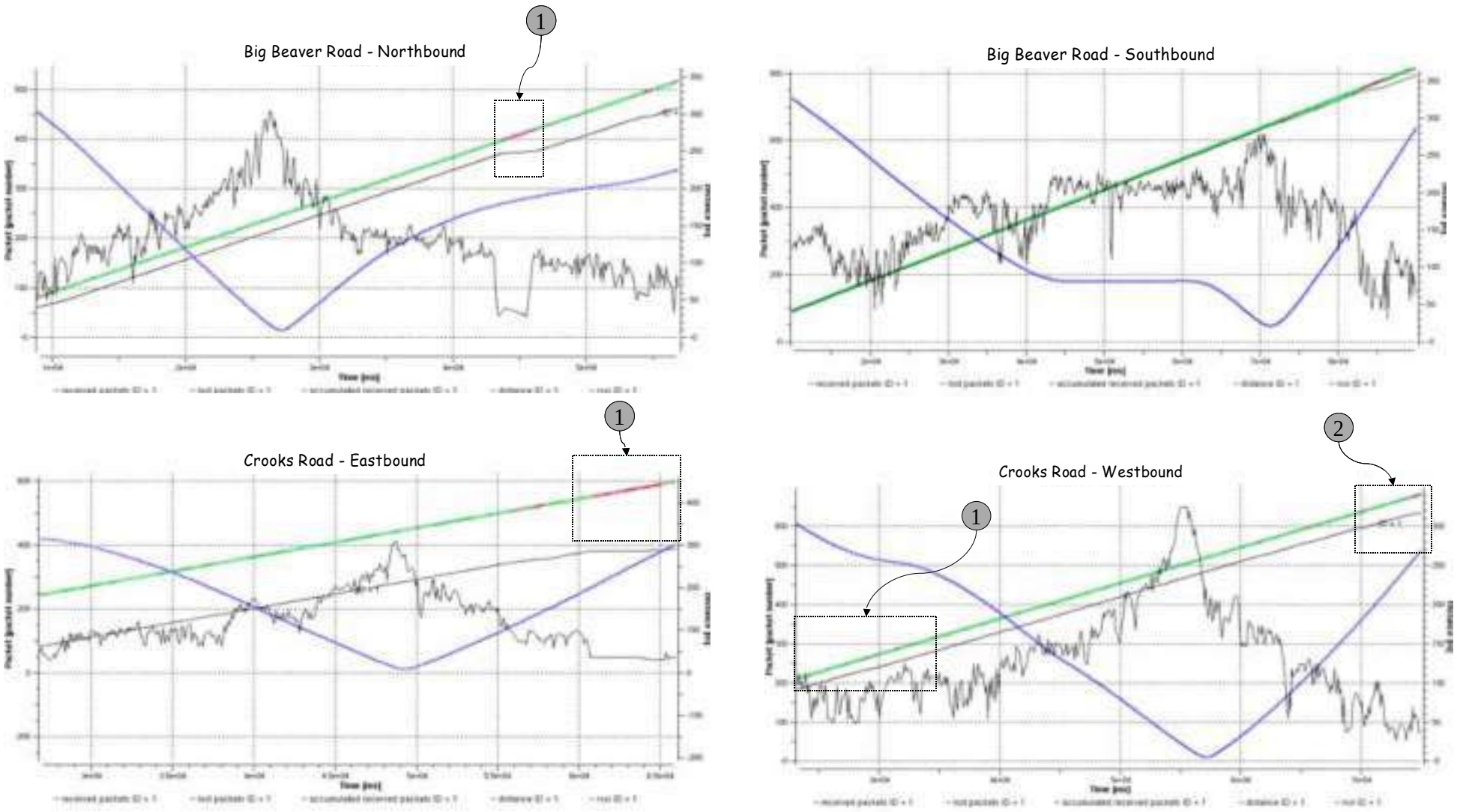


Figure 14. CTK Plots of the Crooks/Big Beaver Intersection

2.1.4 Santa Clara Street & Market Street

The intersection of Santa Clara and Market in San Jose had heavy traffic during the time of the testing (Figure 15). Both Santa Clara and Market Streets have double lanes in both directions. There are trees and closely packed high rises along both sides of Market. There is a traffic light at the intersection and both roads have a center lane for left-turns at the intersection. The RSU was placed on the northeastern side of the intersection to provide line-of-sight to north and southbound traffic on Market Street.

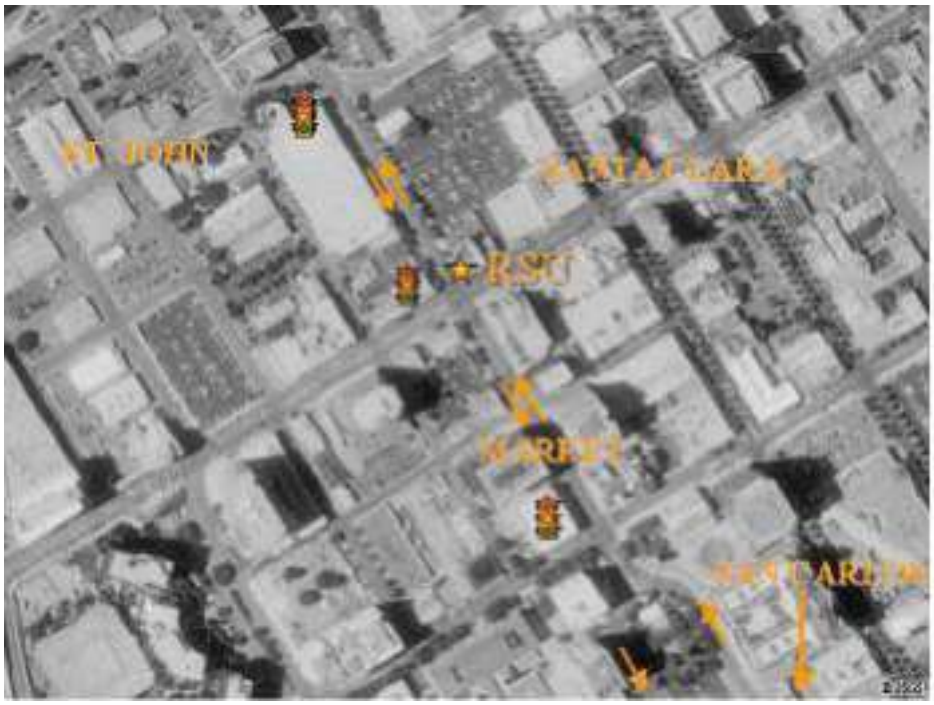


Figure 15. Aerial View of Santa Clara/Market Intersection

The intersection of Santa Clara and Market has closely packed high rises all around. The test car started off near the RSU (intersection) and traveled north onto Market (Figures 16 and 17). It turned back at St. John and passed the RSU. Then it turned back again at San Carlos and returned to the RSU.

Packets were dropped frequently along the test route due to heavy traffic and no line-of-sight between the RSU and the OBU. One possible method to improve the packet reception at this type of intersection would be to position the RSU at a higher height to improve the line-of-sight between the sending and receiving antennas.

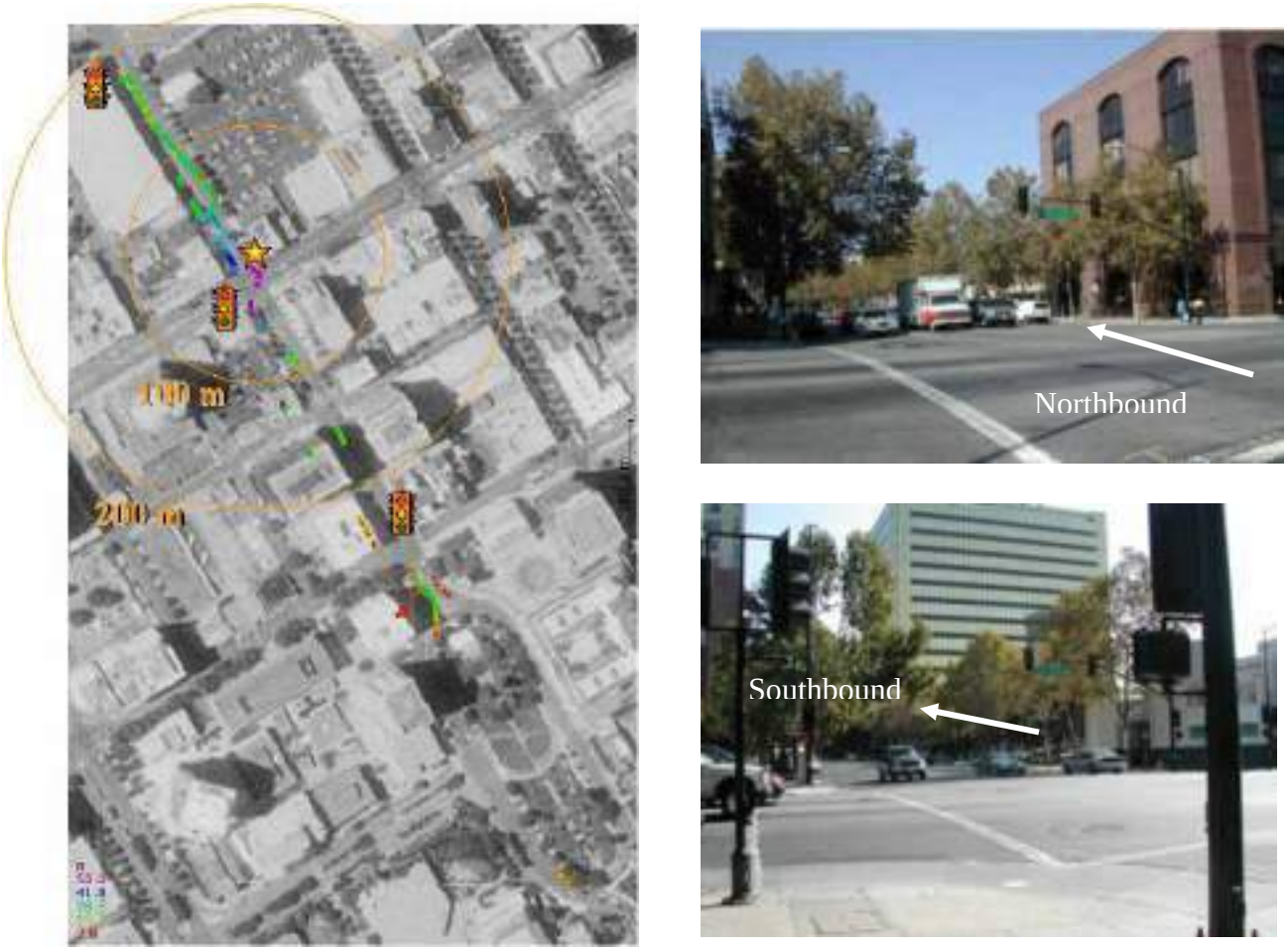


Figure 16. RSSI Plot and Views of Market/Santa Clara Intersection

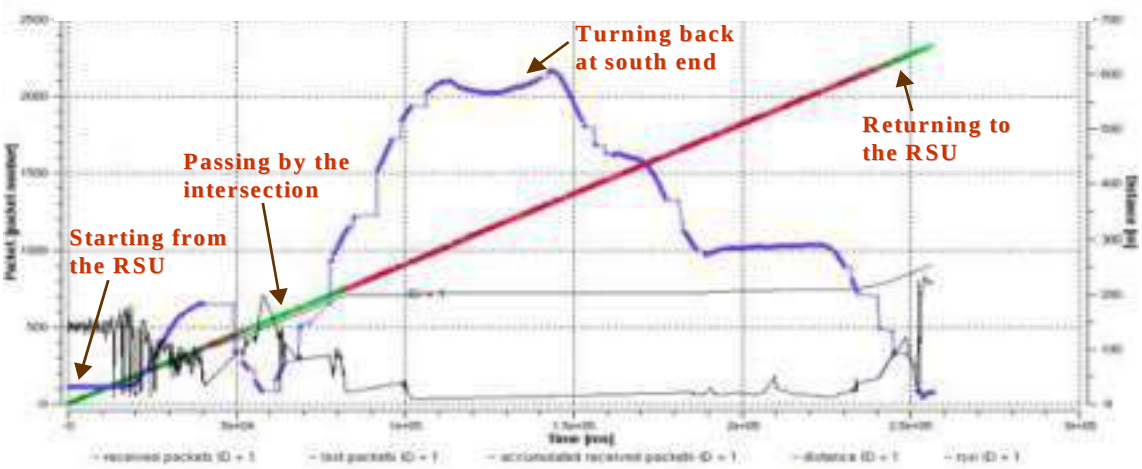


Figure 17. CTK Plot of the Market Street Test Route

2.1.5 Hillview Avenue & Hanover Street

The intersection of Hillview and Hanover in Palo Alto has light traffic during the daytime. Both Hillview and Hanover have a single lane in both directions. The north end of Hanover is slightly uphill and the south end has a 90º bend to the west. There are many trees and office buildings along both sides of Hanover. There is a traffic light at the intersection and both roads have a center lane for left-turns at the intersection. The RSU was placed on the western side of the tee-junction to provide line-of-sight to the north and southbound traffic on Hanover (Figure 18).

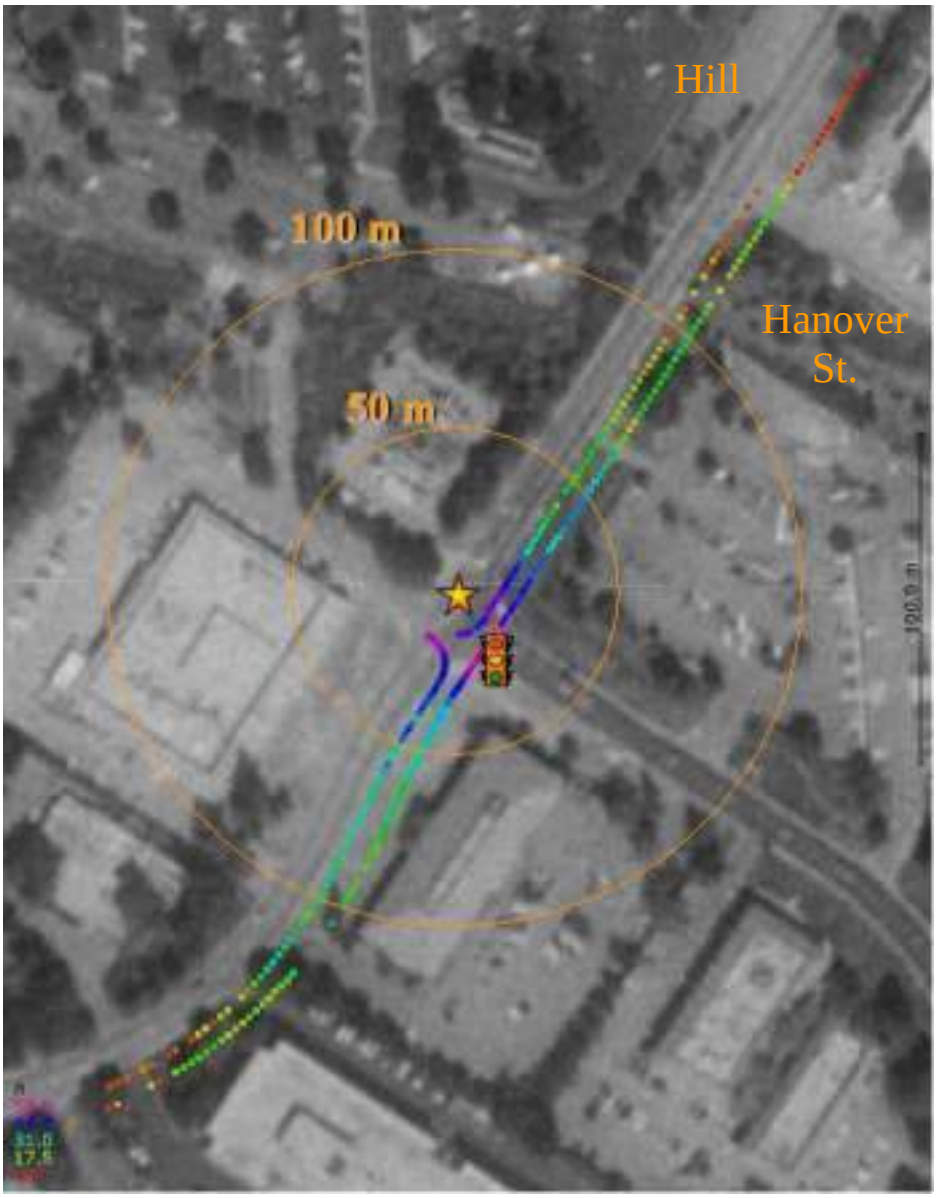


Figure 18. RSSI Plot for the Hanover Test Route

The test car started off from the RSU onto southbound Hanover (Figures 19 and 20). It turned back after the curve, then passed through the intersection. It continued and went slightly uphill on northbound Hanover. It finally turned back ~300m away from the intersection and returned to the RSU. Occasionally the hill or objects and terrain along the edge of the curving Hanover Road obscured the line-of-sight.

Figure 19. Views of the Hillview/Hanover Intersection

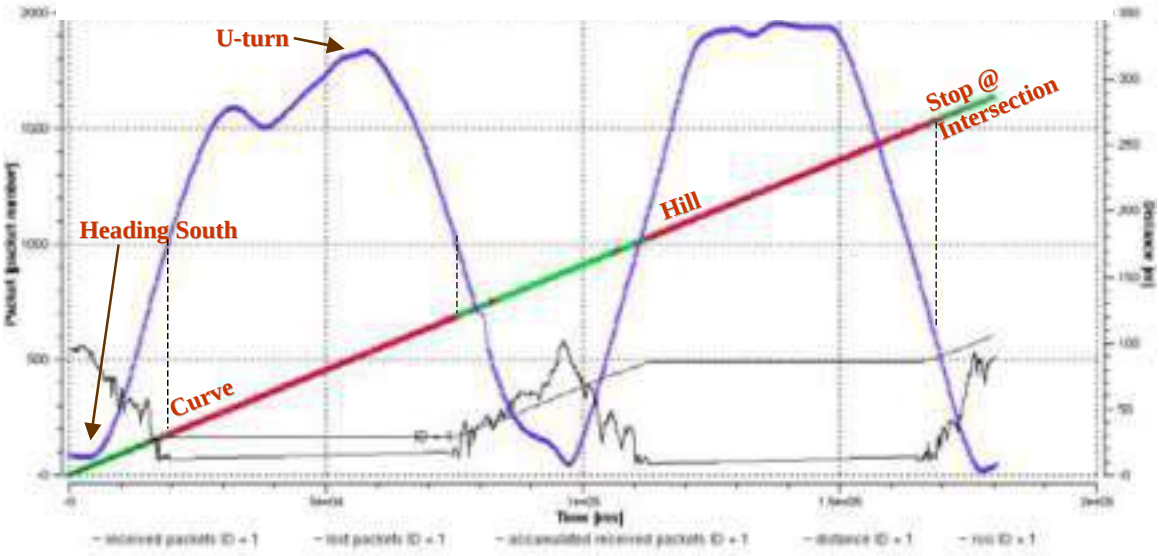


Figure 20. CTK Plot for the Hanover Test Route

2.1.6 Woodward Avenue & I-696 Service Drive

This intersection has four lanes in the southbound direction and five lanes in the westbound direction, and both directions include a left turn lane (Figure 21). There is medium to heavy traffic during the day. The traffic from southbound Woodward Avenue branches off, passing under a large overhanging parking garage before reaching the traffic signal on the I-696 service drive where the RSU is located. In addition to the parking structure, there are numerous other features that might impact communications, including a water tower, below-surface-level freeways along both test roads, and a number of concrete overpasses.

Figure 21. Woodward/I-696 Service Drive Intersection

Although there appeared to be a significant amount of obstructions at this intersection, reception results were much better than anticipated, as shown in Figure 22. Note that reception of the GPS signal was blocked while the vehicle was under the parking garage in test run #2, and the packets that were received during this portion of the test were plotted at the point where the GPS signal was reestablished. This run was concluded when the vehicle turned left onto the eastbound I-696 service drive.

Figure 22. RSSI Plot of the Woodward/I-696 Service Drive Intersection

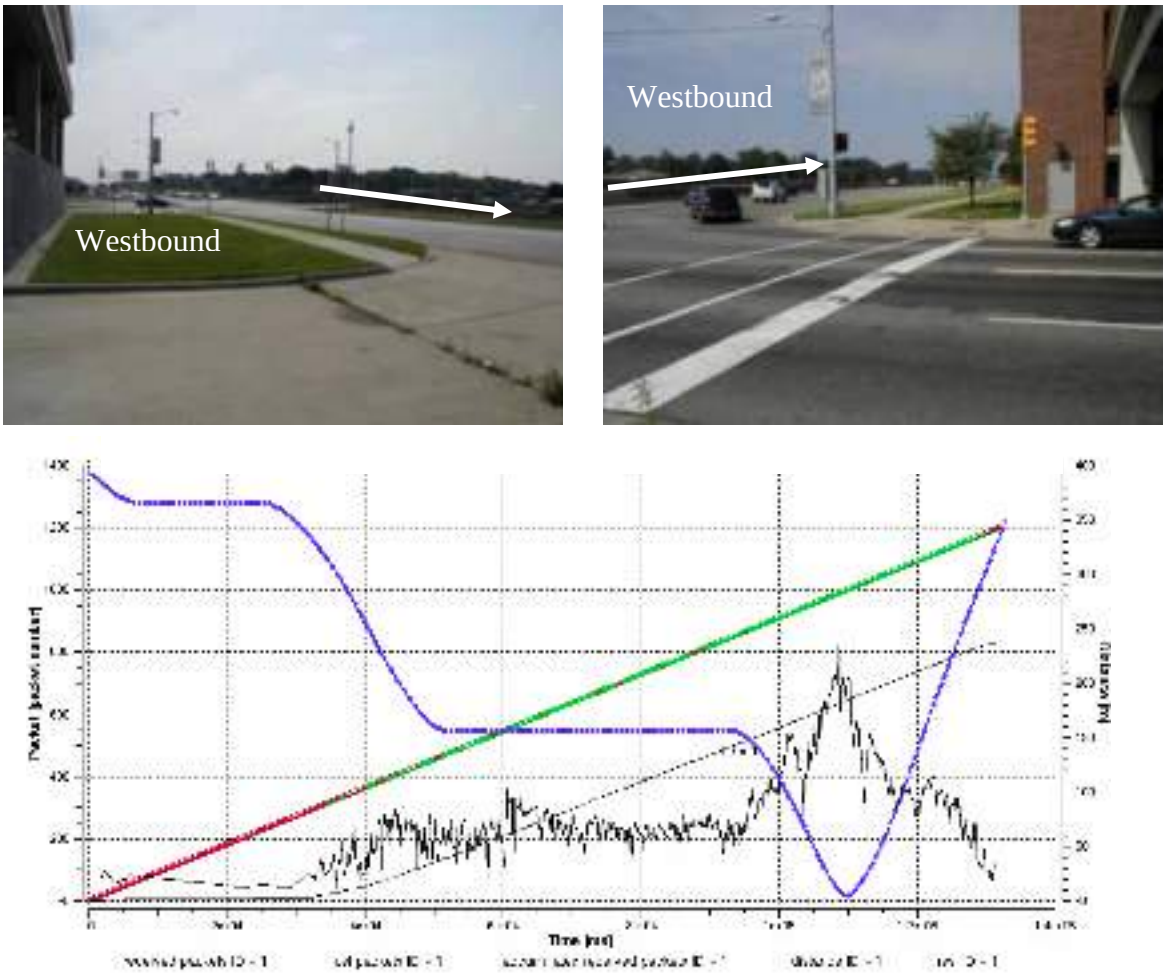


Figure 23. Views and CTK Plot of the I-696 Service Drive Test Route

For westbound I-696 Service Drive (Figures 22 and 23), packets were initially blocked by heavy traffic at a significant distance from the RSU. The cumulative packet reception rate as the vehicle approached the intersection from 250m was 85 percent, and the rate from 100m was 100 percent.

For southbound Woodward Avenue and its exit road to the I-696 service drives (Figures 22 and 24), packets were initially lost due to blockage of terrain and foliage alongside the curving roadway. Surprisingly, packet reception began at a distance of approximately 300m while line-of-side was still blocked. As the vehicle passed beneath the parking structure, the GPS signal was lost but packets continued to be received. GPS reception resumed when the vehicle moved beyond the parking structure. The test was concluded when the vehicle turned around the corner and onto the eastbound I-696 service drive. The cumulative packet reception rate as the vehicle approached the intersection from 250m was 89 percent, and the rate from 100m was 99 percent.

Figure 24. View and CTK Plot for the Woodward Test Run

2.1.7 El Camino Real & 5th Avenue

The intersection of El Camino and 5th in Atherton had medium traffic during the time of the testing. El Camino has three lanes in each direction and two additional lanes for left-turning onto 5th. 5th has two lanes in each direction and one left turn lane for southbound El Camino. A moderate amount of trees and buildings are along both sides of El Camino and the south-end is slightly curved. There is a traffic light at the intersection. The RSU was placed on the northeastern corner of the tee-junction to provide line-of-sight to north and southbound traffic on El Camino, as well as traffic on 5th. The testing was done at three power levels: 100 percent, 50 percent, and 10 percent.

The test car traveled westbound on 5th, right-turned onto El Camino and headed north. It turned back at approximately 400m away from the RSU. It went past 5th and continued along southbound El Camino. Then it turned back again at about 400m away and returned to the intersection. It right-turned onto 5th and turned back at about 200m away. In the 100 percent power test, the reception is shown in Figure 25. There were occasional dropped GPS signals and packets due to trees and no line-of-sight.

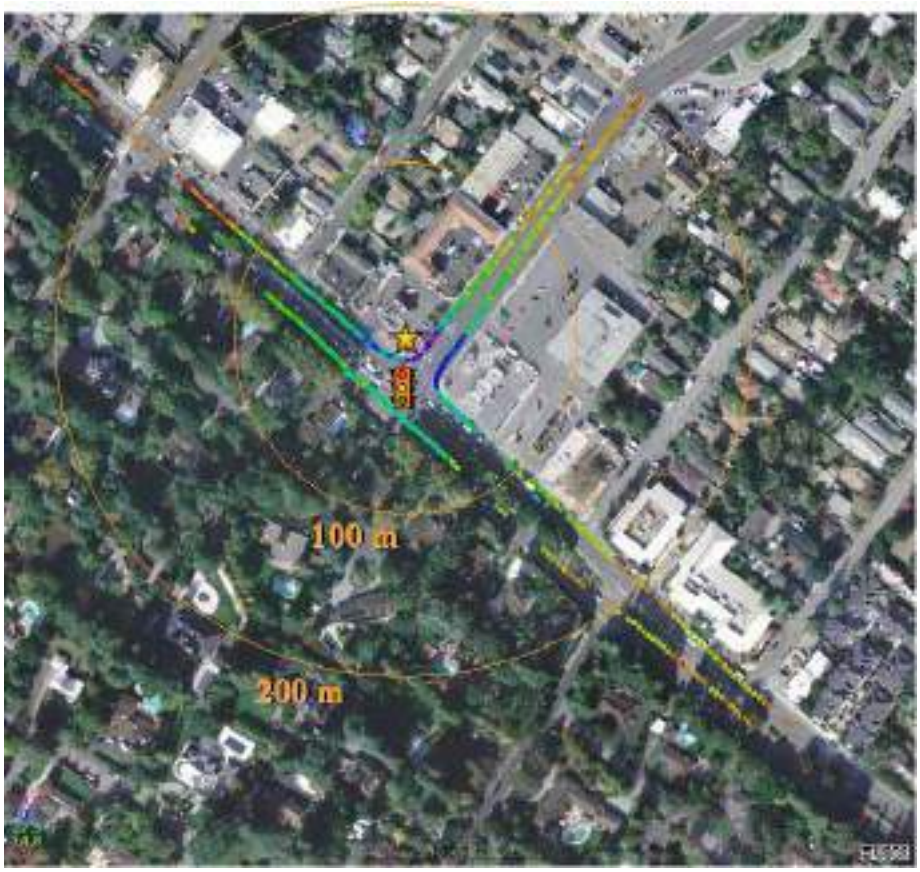


Figure 25. RSSI Plot for El Camino Real/5th at 100% Power (20 dBm)

In the 50 percent power test (Figure 26), there were less packets received and they had slightly lower RSSI values, compared with the results at 100 percent power. The receiver could not detect as many packets as it could in the case of 100 percent power. In the 10 percent power test (Figure 27), there were even less packets received and they had even lower RSSI values, compared with results at 50 percent power. The receiver could not detect as many packets as it could in the case of 50 percent power.

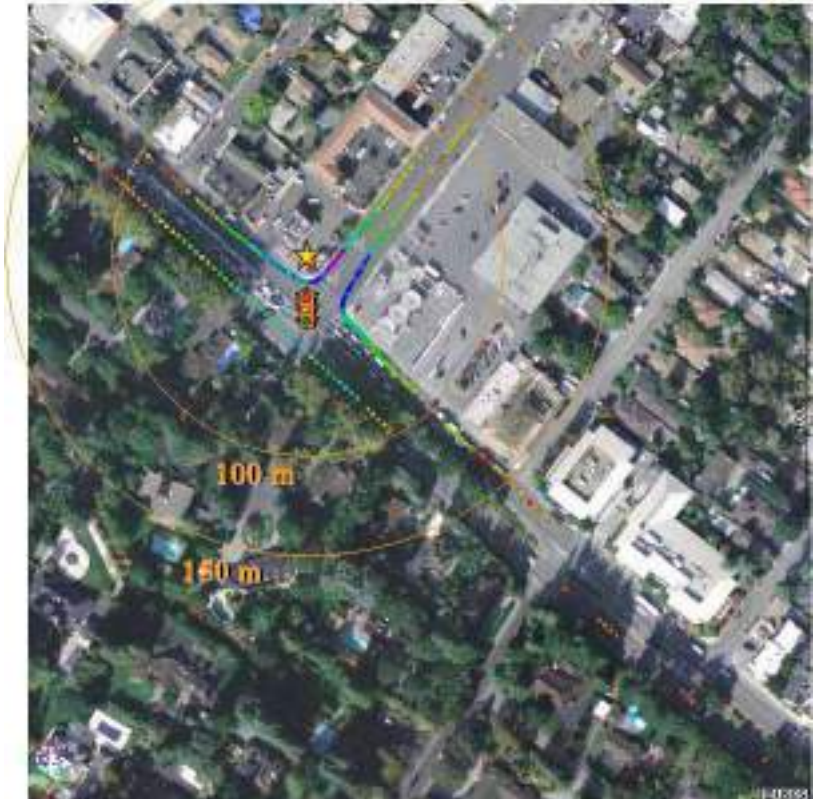


Figure 26. RSSI Plot for El Camino/5th at 50% Power (17 dBm)
Figure 27. RSSI for El Camino/5th at 10% Power (10 dBm)

2.1.8 Woodside Road & Churchill Avenue

The intersection of Woodside and Churchill in Redwood City has medium traffic during daytime. Woodside has two lanes for both directions and Churchill has one for both directions. Both directions on Woodside away from the intersection have up-hills and the south end is slightly curved to the west. There are many trees along both sides of Woodside. Woodside has a left turn lane with a traffic light at the Churchill intersection. The RSU was placed on the northeastern corner to provide line-of-sight to north and southbound traffic on Woodside (Figure 28).

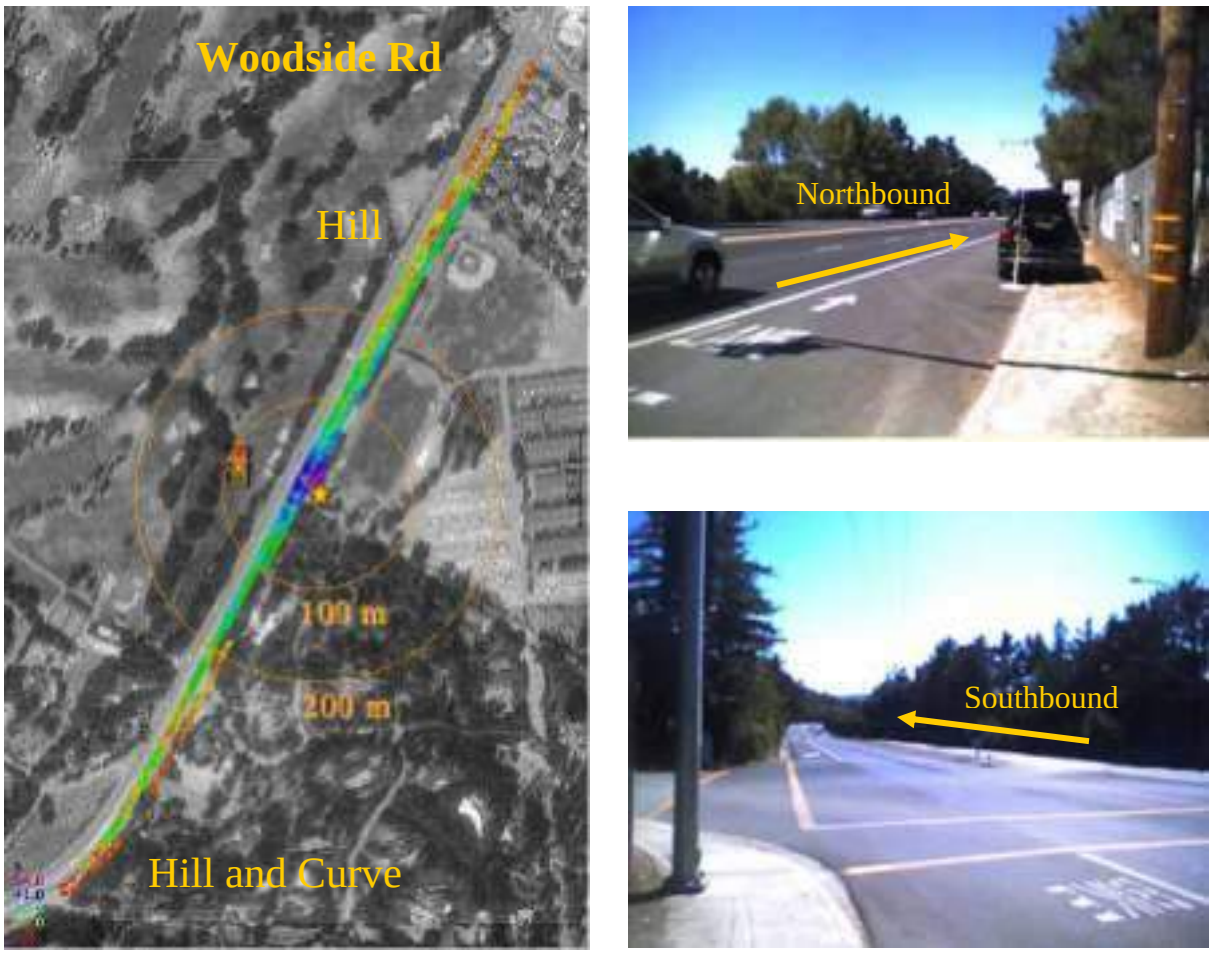


Figure 28. RSSI Plot and Views of the Woodside Test Run

The test car received signals except at locations where the line-of-sight was obscured by hills or road curvature (Figures 28 and 29). Reception faded at both ends of the test route (~500m away).

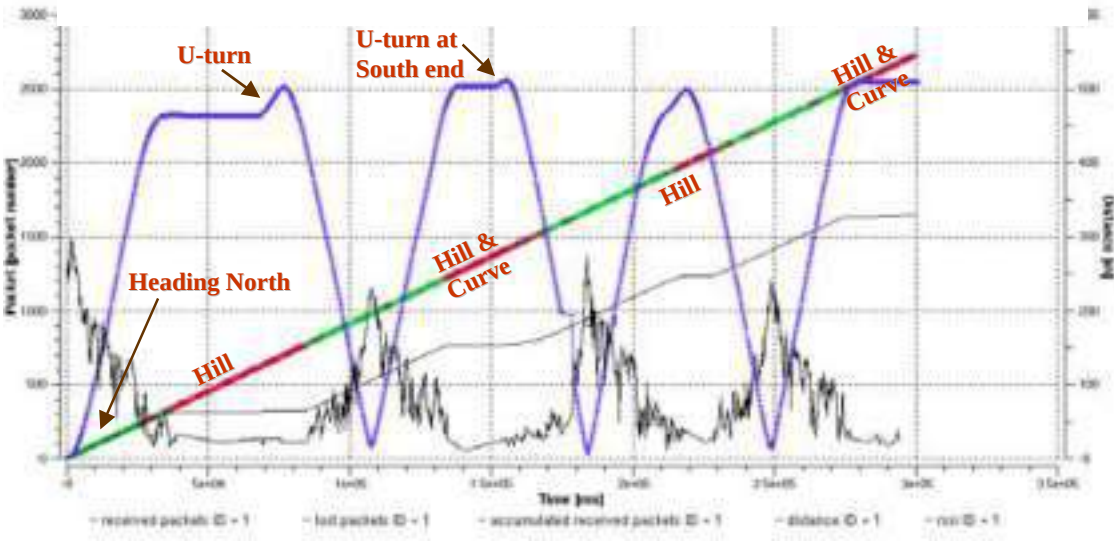


Figure 29. CTK Plot for the Hillside Test Run

2.1.9 Country Club Drive & 12 Mile Road

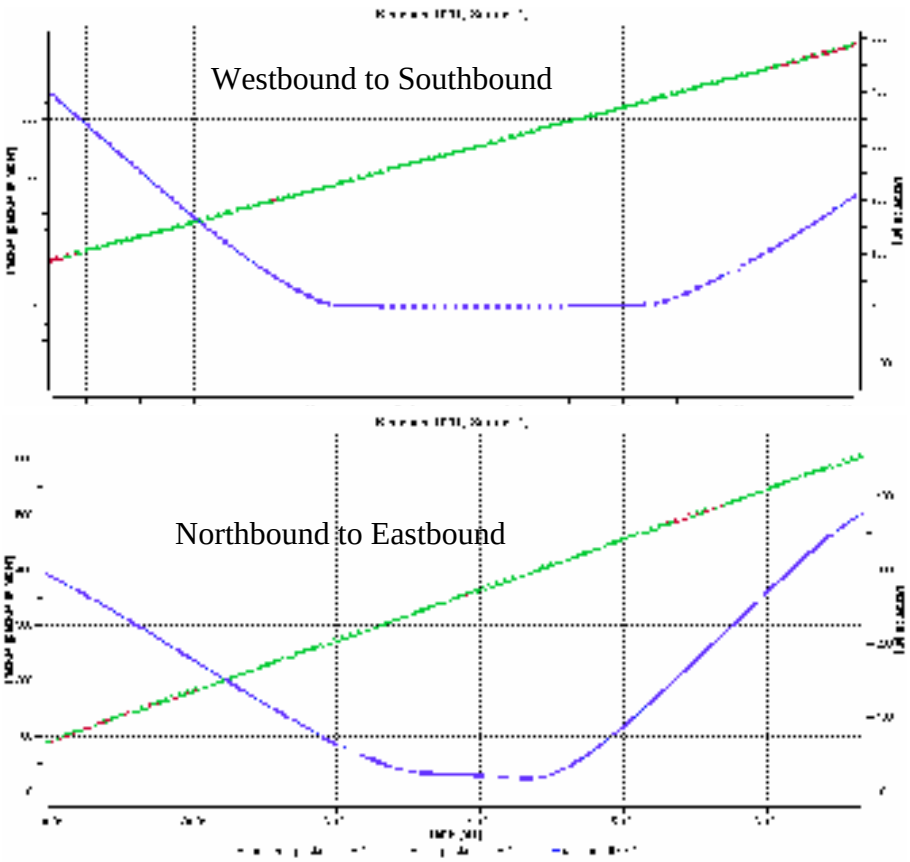
Eastbound 12 Mile has 2 lanes and a right turn lane. Westbound 12 Mile has 2 lanes and a left turn lane, and this intersection experiences light to heavy traffic conditions depending on the time of day. Vehicles traveling East on 12 mile have an obstructed line of sight to the RSU due to trees located on the median strip due to trees. Country Club Drive has 2 lanes in each direction separated by a median strip. This road also has an obstructed line of sight to the RSU due to several trees.

Figure 30. RSSI Plot for the Country Club/12 Mile Intersection

The test vehicle first traveled eastbound on 12 Mile Road straight past the RSU (Figure 30). A few packets were lost at around 200 m on either side of the RSU, possibly due to blockages from trees.

Figure 31. Views and CTK Plot for Eastbound 12 Mile Test Run

Next, the test vehicle U-turned and headed westbound on 12 Mile Road back toward the RSU (Figure 31). The vehicle turned southbound onto Country Club Drive and passed the RSU. Packets were lost going southbound while moving away from RSU due to blockages from trees. The test vehicle then turned around and headed northbound on Country Club Drive, turning right at the intersection past the RSU onto eastbound 12 Mile Road. A few packets are lost going both north and east due to blockages from trees (Figure 32).



East Test Routes

2.1.10 Auburn Road & Squirrel Road

This intersection had light traffic during the time of testing. Auburn Road has two lanes in each direction, while Squirrel Road has one lane in each direction and a center left turn lane. Squirrel Road curves suddenly just north of the intersection, and line-of-sight to the RSU is blocked by terrain along the curving roadway. Even though line-of-sight was obstructed from the RSU, the vehicle traveling northbound on Squirrel Road communicated with the RSU for distances far beyond the line of sight (Figure 33).

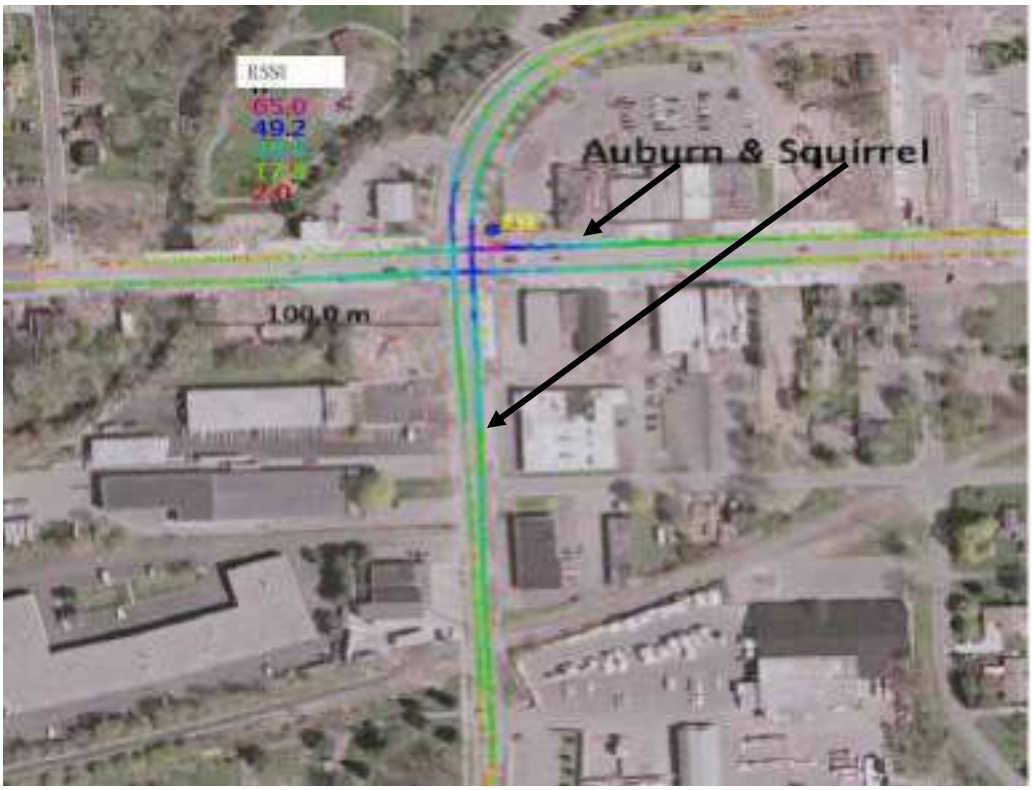
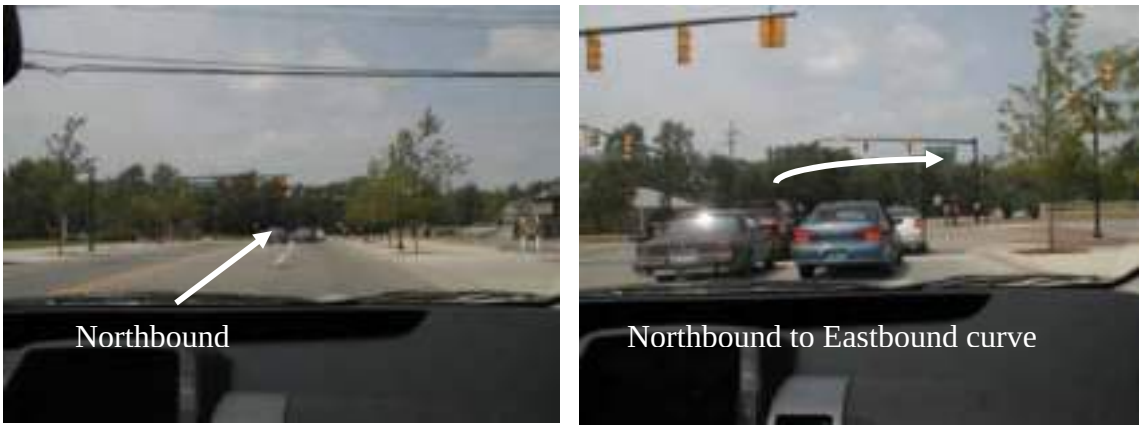


Figure 33. RSSI Plot for Auburn/Squirrel Test Runs

Traveling northbound on Squirrel Road, 100 percent of packets were received starting at about 275 m since there is clear LOS in this direction on Squirrel Road (Figure 34). Packets were eventually lost due to blockage of terrain alongside the curving roadway on the south side of Squirrel Road. Packet reception ended at a distance of approximately 130m with line-of-sight blocked.



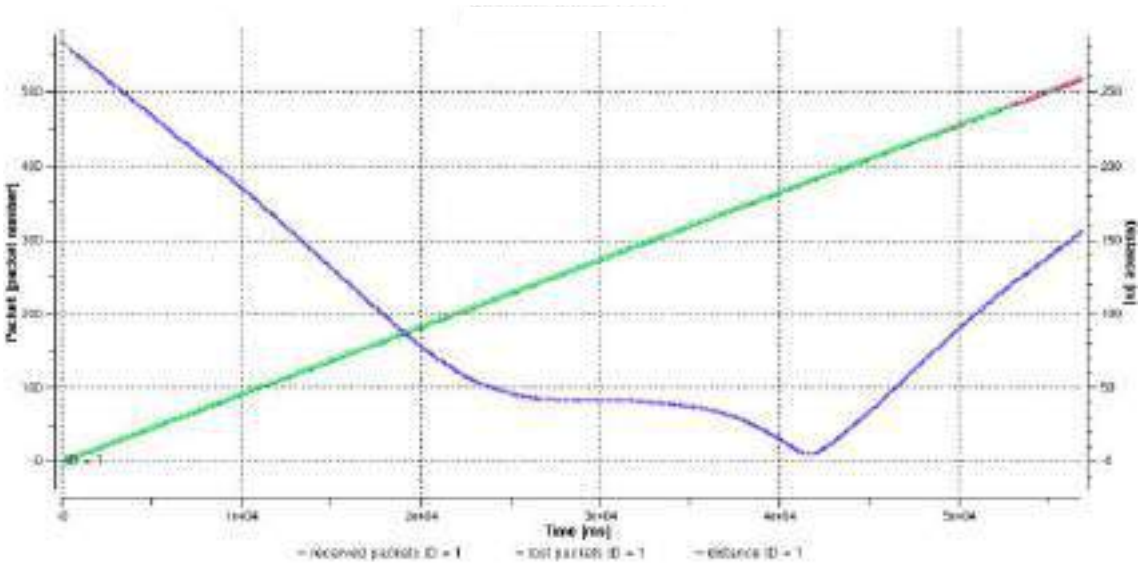


Figure 34. Views and CTK Plot for the Southbound Squirrel Test Run

Traveling southbound, packets were initially lost due to blockage of terrain alongside the curving roadway on the south side of Squirrel Road (Figure 35). Packet reception began at a distance of

approximately 175m while line-of-sight was still blocked. As the vehicle passed the intersection, a large truck blocked the LOS between the RSU and OBU, causing some intermittent communication loss. The test was concluded when the communications between the RSU and OBU was lost at distance of 300 m.

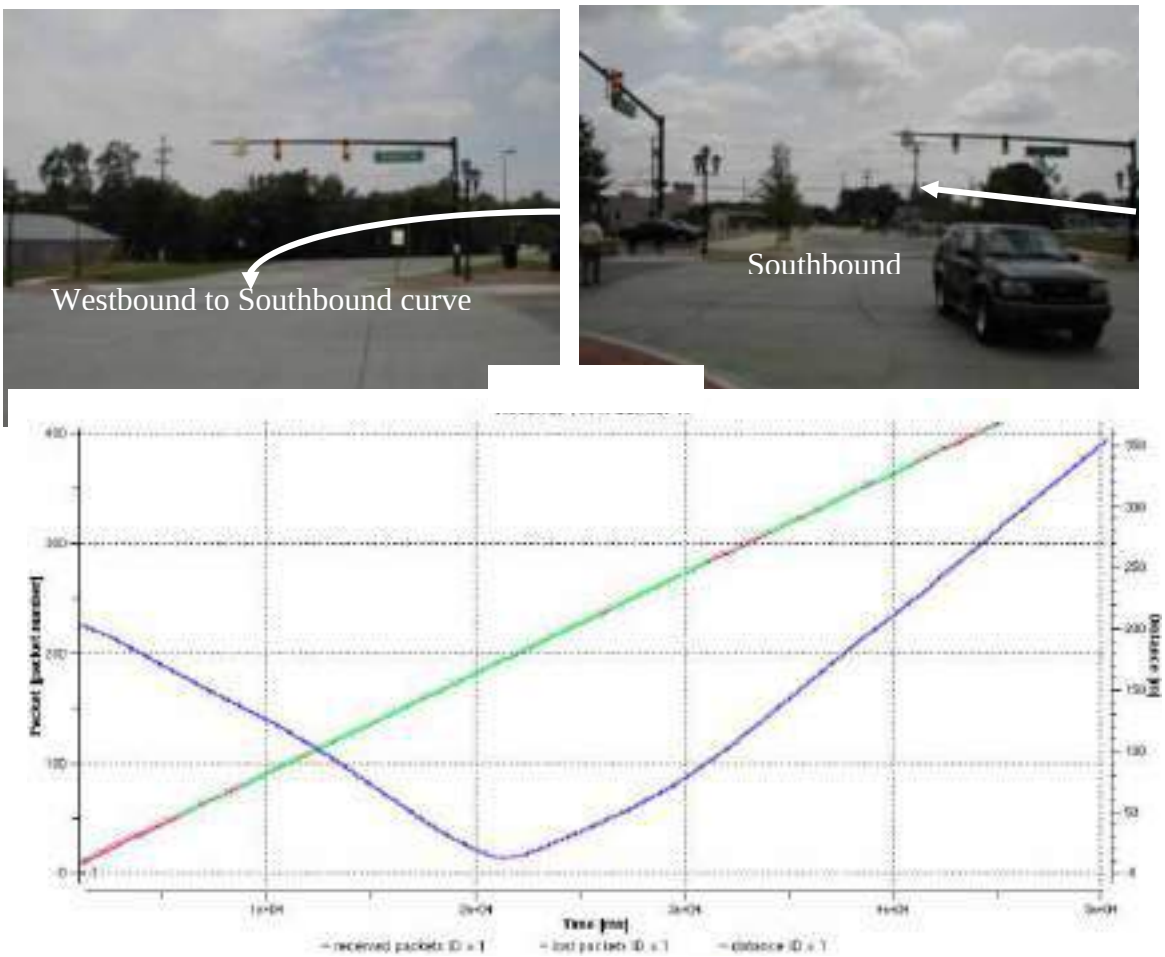


Figure 35. Views and CTK Plot for the Southbound Squirrel Test Run

Eastbound on Auburn Road, the test vehicle initially received 100 percent of the packets at about 200 m since there is clear LOS going in this direction (Figure 36). Trees and parked vehicles obstruct the line of sight and communication beyond 200m.

Figure 36. Views and CTK Plot for the Eastbound Auburn Test Run

Traveling westbound on Auburn Road, packets were received well up to about 200 m on either side of the RSU going in this direction. Packets were lost for a short duration due to LOS blockage by a large white truck (Figure 37).

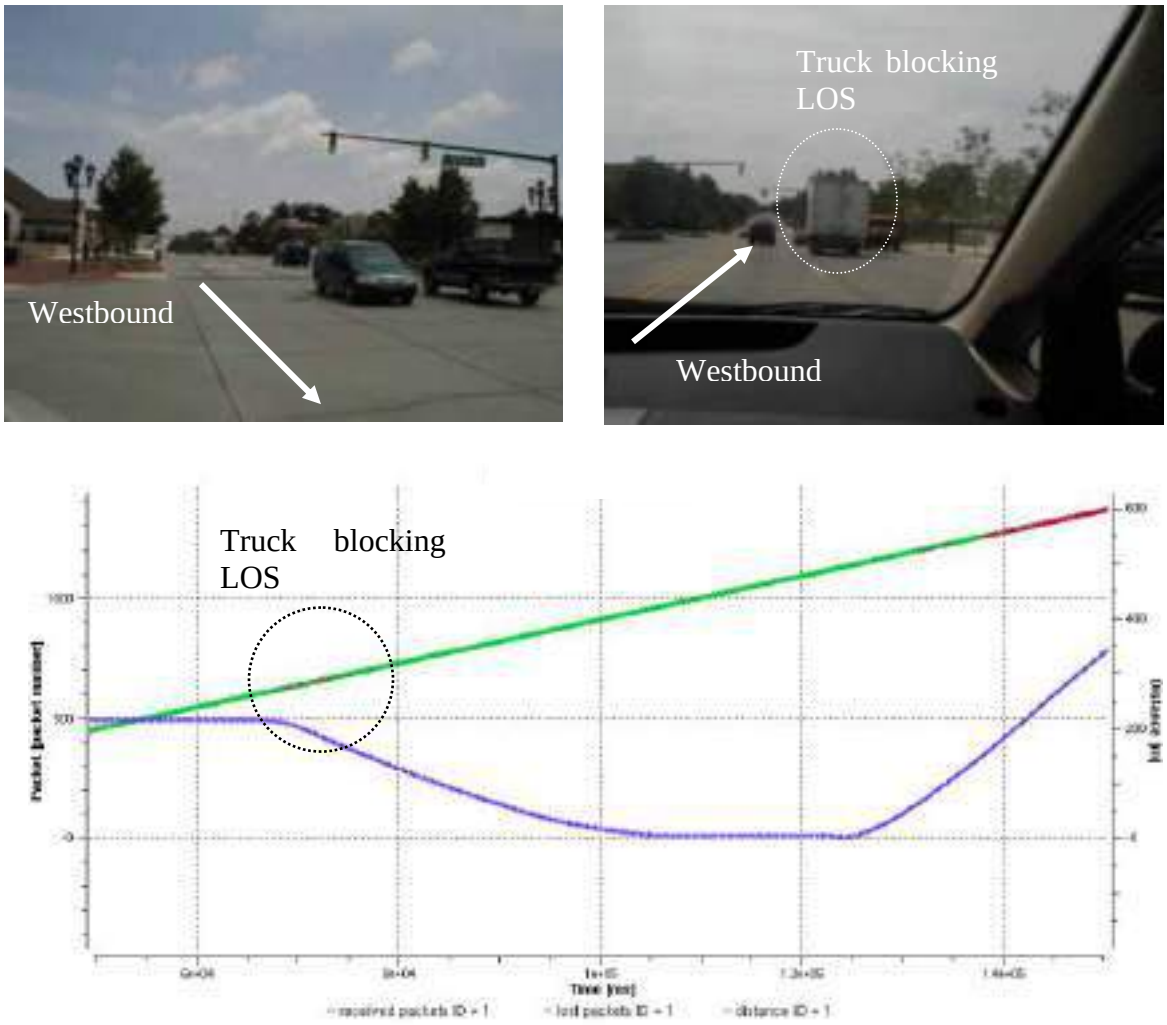


Figure 37. Views and CTK Plot for the Westbound Squirrel Test Run

2.1.11 Sand Hill Road & Whiskey Hill Road

This portion of Sand Hill runs relatively north-south, and Whiskey Hill intersects Sand Hill at an angle, coming from the north-east. The intersection of Whiskey Hill and Sand Hill does not have a traffic signal. There is a triangle-shaped median in the middle of the intersection, separating Sand Hill from two branches of traffic that run southbound on Whiskey Hill. Traffic on Whiskey Hill that will continue south yields to and merges with southbound traffic on Sand Hill. Traffic on Whiskey Hill that will turn north onto Sand Hill has a stop sign. The intersection is a relative low-point - there are up-hills in both directions on Sand Hill going away from the intersection. Whiskey Hill also rises from the level of the intersection. There are few buildings nearby, though there are a number of tall trees and shrubs (Figure 38).

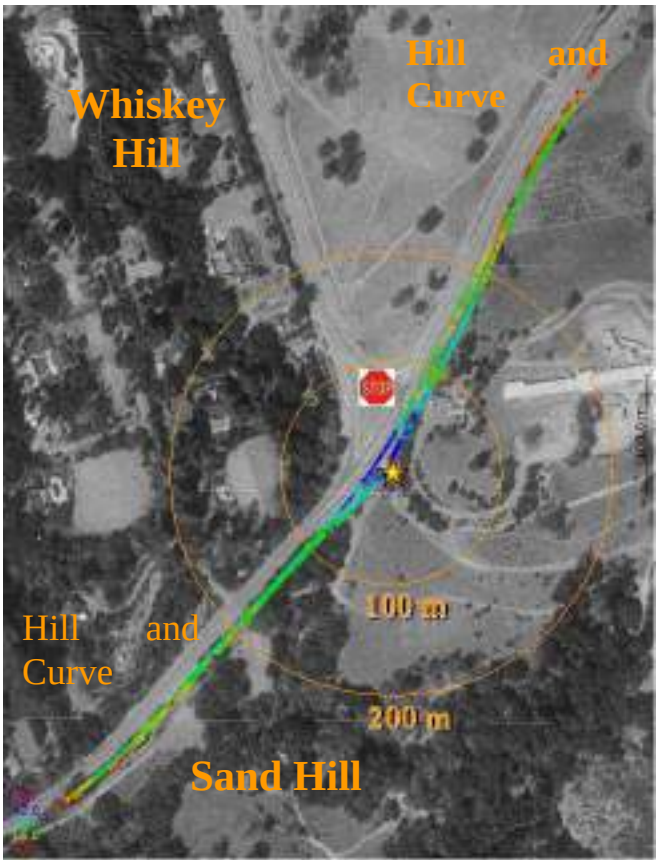


Figure 38. RSSI Plot for Sand Hill Test Route

The test car started from the RSU (intersection) and traveled northbound on Sand Hill. It turned back and passed thru the RSU. Then it turned back again and returned to the RSU. Occasional packets were dropped due to the long distance or no line-of-sight from RSU to OBU (Figure 39).

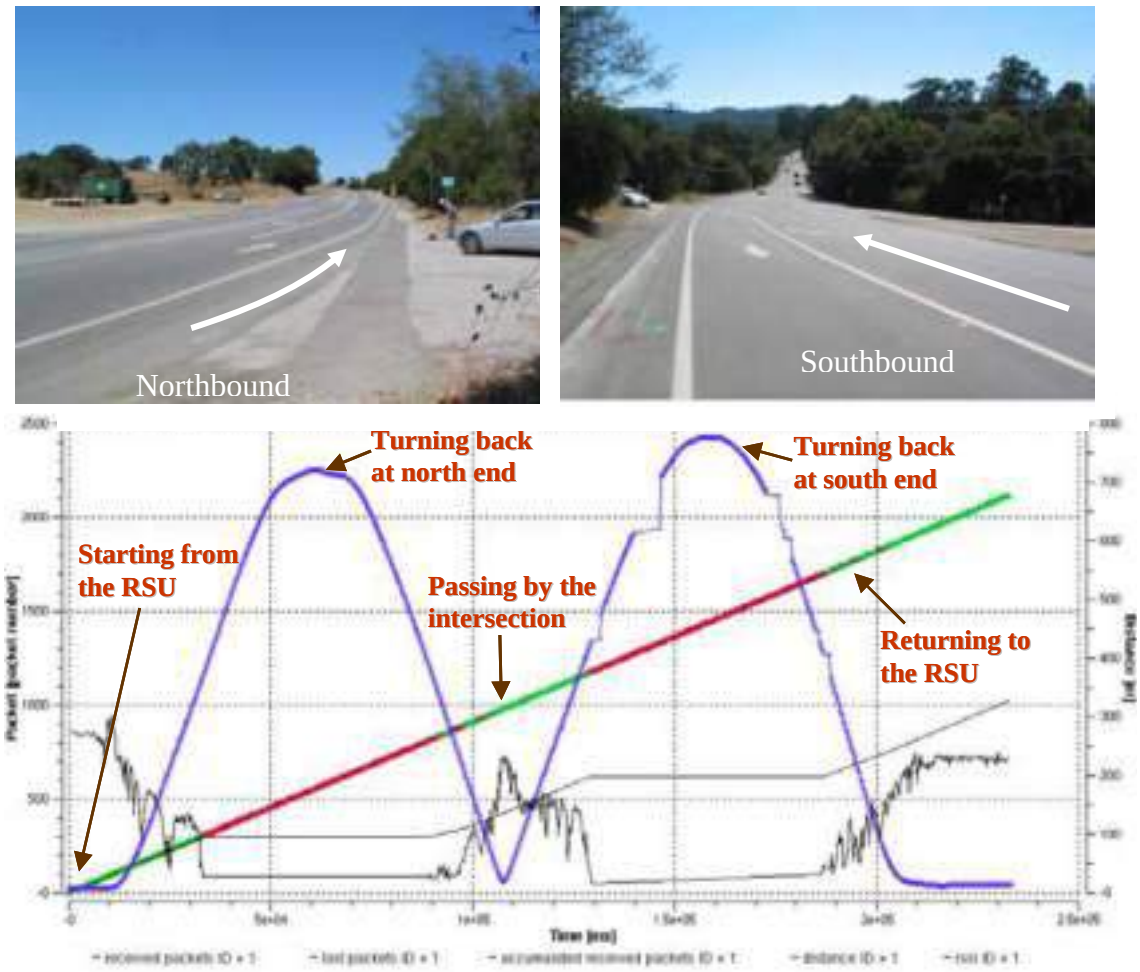


Figure 39. RSSI Plot for Sand Hill Test Route

2.1.12 Long Lake Road & Lahser Road

The intersection has two lanes of traffic in the east and westbound directions that have a steady amount of residential (non-commercial) traffic during the daytime hours. The north and southbound directions on Lahser Road have only one lane of traffic in each direction, and slower, sparser traffic than Long Lake. Trees encircle the intersection and block line-of-sight in at least one -- if not all -- directions depending upon the position of the RSU. The RSU was placed on the southeastern corner for safety reasons. Northbound and eastbound traffic was nearly atop the RSU by the time foliage permitted line-of-sight (Figure 40). In the southbound direction, a sharp decline hill prevents line-of-sight to even the traffic light until nearly upon the light. Lost GPS (due to tree cover) does not provide an accurate distance-to-RSU, but line-of-sight to the traffic light becomes available near 150 meters from the intersection center. In all directions of travel, ground level foliage prevented line-of-sight communication (Figures 40 and 41).

Figure 40. RSSI Plot and Views for the Long Lake/Lahser Test Route

For this intersection, the two test personnel stationed at the RSU attempted to identify the first moment that the test vehicle was seen approaching the RSU, and the last moment it was seen driving away from it. These moments in time were linked with the corresponding packet number and identified in the CTK plots of Figure 41 as the estimated periods during which line-of-sight exists between the RSU and the test vehicle.

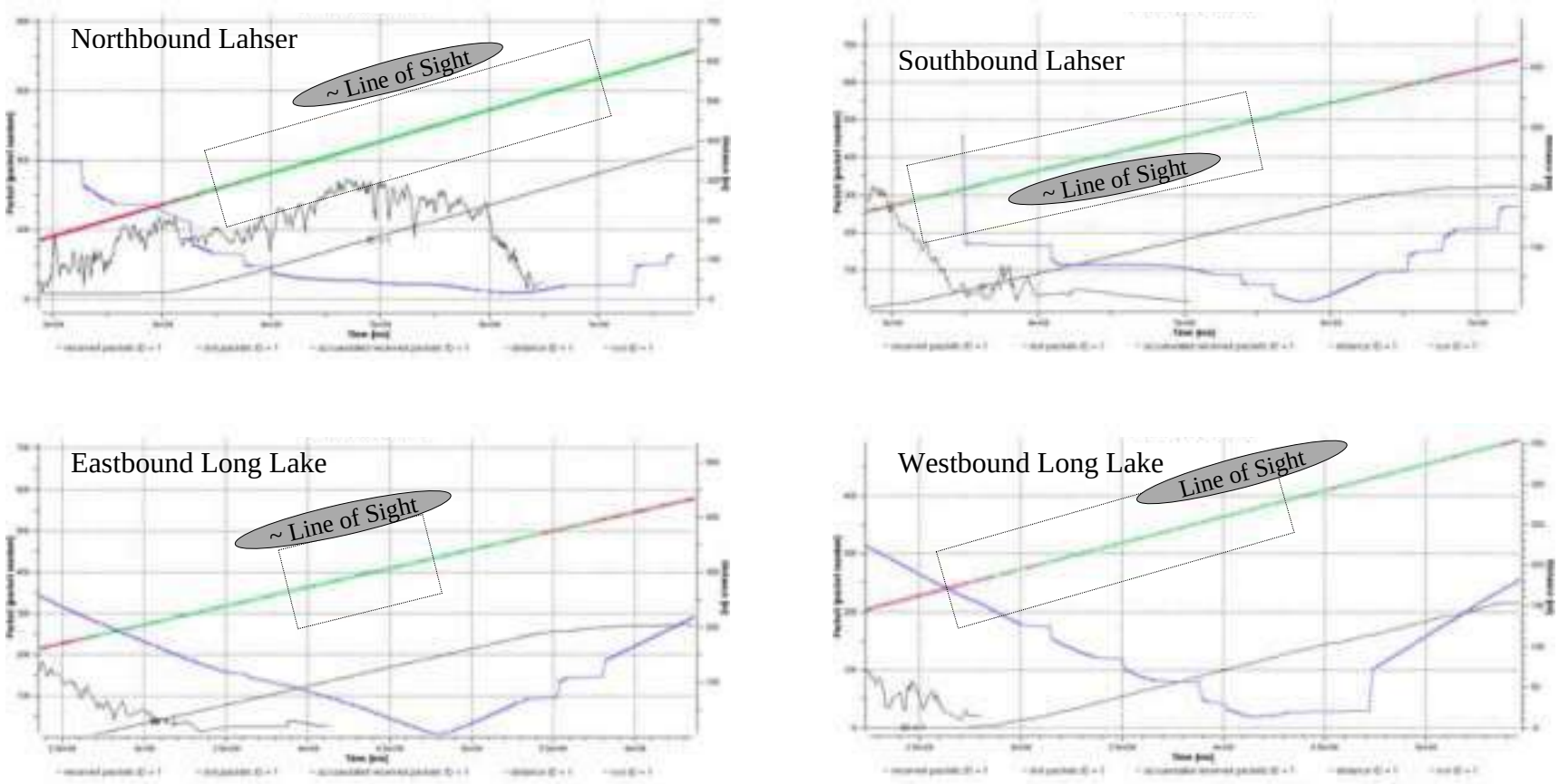


Figure 41. CTK Plots for the Long Lake/Lahser Intersection

2.1.13 Quarton Road & Lahser Road

Testing at this intersection was only performed while driving along Quarton Road due to the limited placement choices for the RSU. Aside from left and right turn lanes at the intersection, these roads are limited to one lane of traffic in either direction, and have considerable foliage close to the shoulder of the roads. Quarton rises slightly east of the intersection, cresting a hill about 200m from the RSU. On the west side, the road immediately bends to the south, disappearing from view within about 100m (Figure 42).

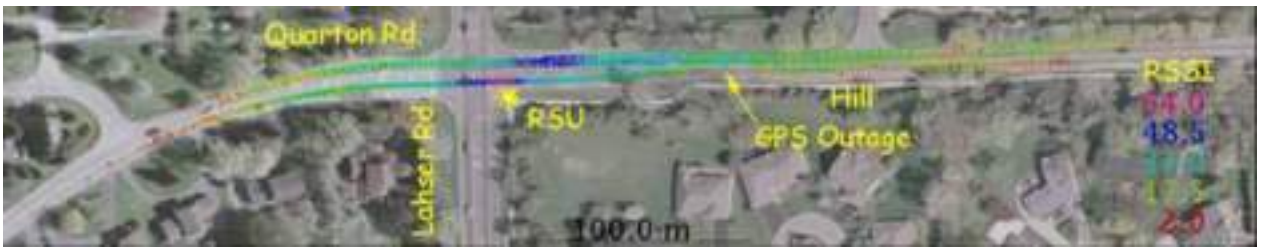
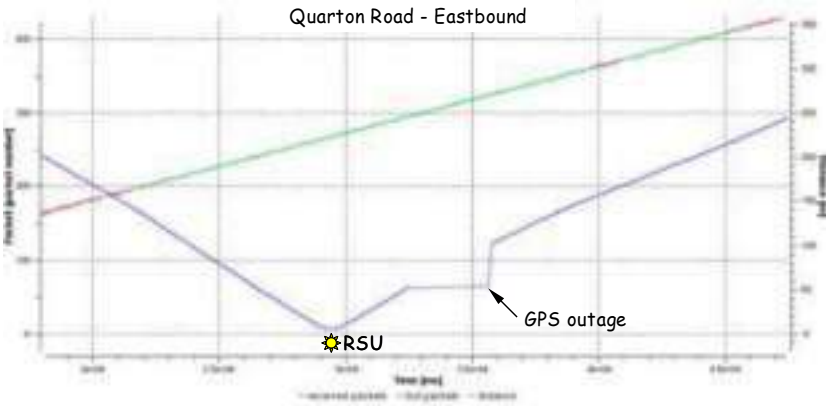


Figure 42. RSSI Plot for the Quarton Test Route

Proceeding eastbound, no packets were lost as the test vehicle approached the intersection from within 100 m (Figure 43). Approximately 50m east of the RSU, the GPS signal was temporarily lost due to an obstruction from trees along the road; however, radio reception was not affected in this region. Driving westbound, 2 packets were lost with the test vehicle within ~100m of the intersection in this case. Owing to the slightly different line of sight to the vehicle in the westbound lane, the range of radio reception was slightly different than the prior data, and there were no losses of GPS signal coverage.



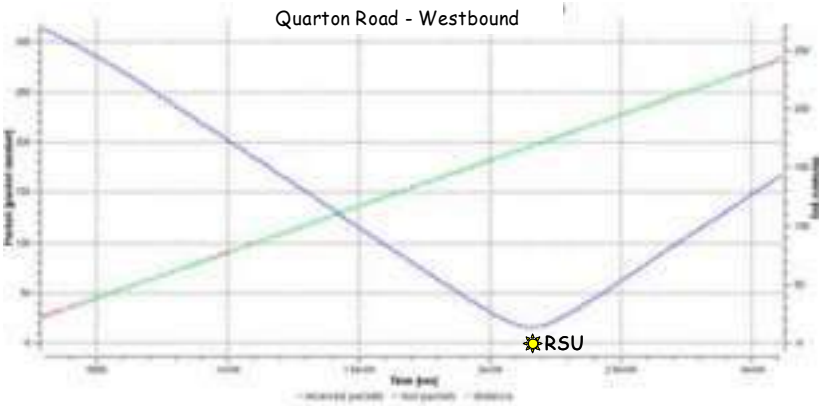


Figure 43. Views and CTK Plots for the Quarton Test Routes

2.1.14 Skyline Boulevard & Woodside Road

The intersection of Skyline and Woodside is in the hills area of Redwood City and has light traffic during daytime. Both Skyline and Woodside have a single lane in both directions. Both directions on Skyline away from the intersection have up-hills and the southeastern end is gradually curved to the south. There is dense foliage all over the hills area and surrounding the intersection. There are stop signs on Woodside at the intersection but none on Skyline. The RSU was placed on the western corner to provide line-of-sight to northwest and southeast-bound traffic on Skyline (Figure 44).

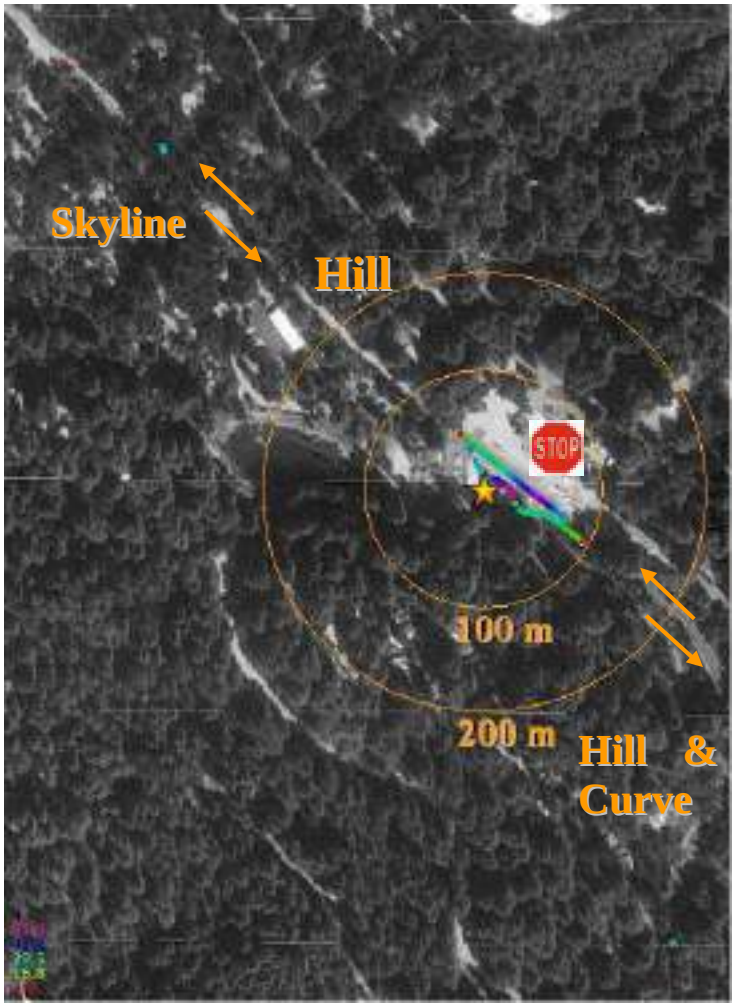


Figure 44. RSSI Plot for the Sky Line Test Route

The car started from the RSU and went southeast on Skyline (Figure 45). It turned around, went through the intersection, and turned around again and returned to the RSU. Poor GPS signals and dropped packets were recorded along the test route when the car was more than 70m away from the intersection due to heavy foliage blockage to GPS satellites and no line-of-sight from RSU to OBU at up-hills and curves.

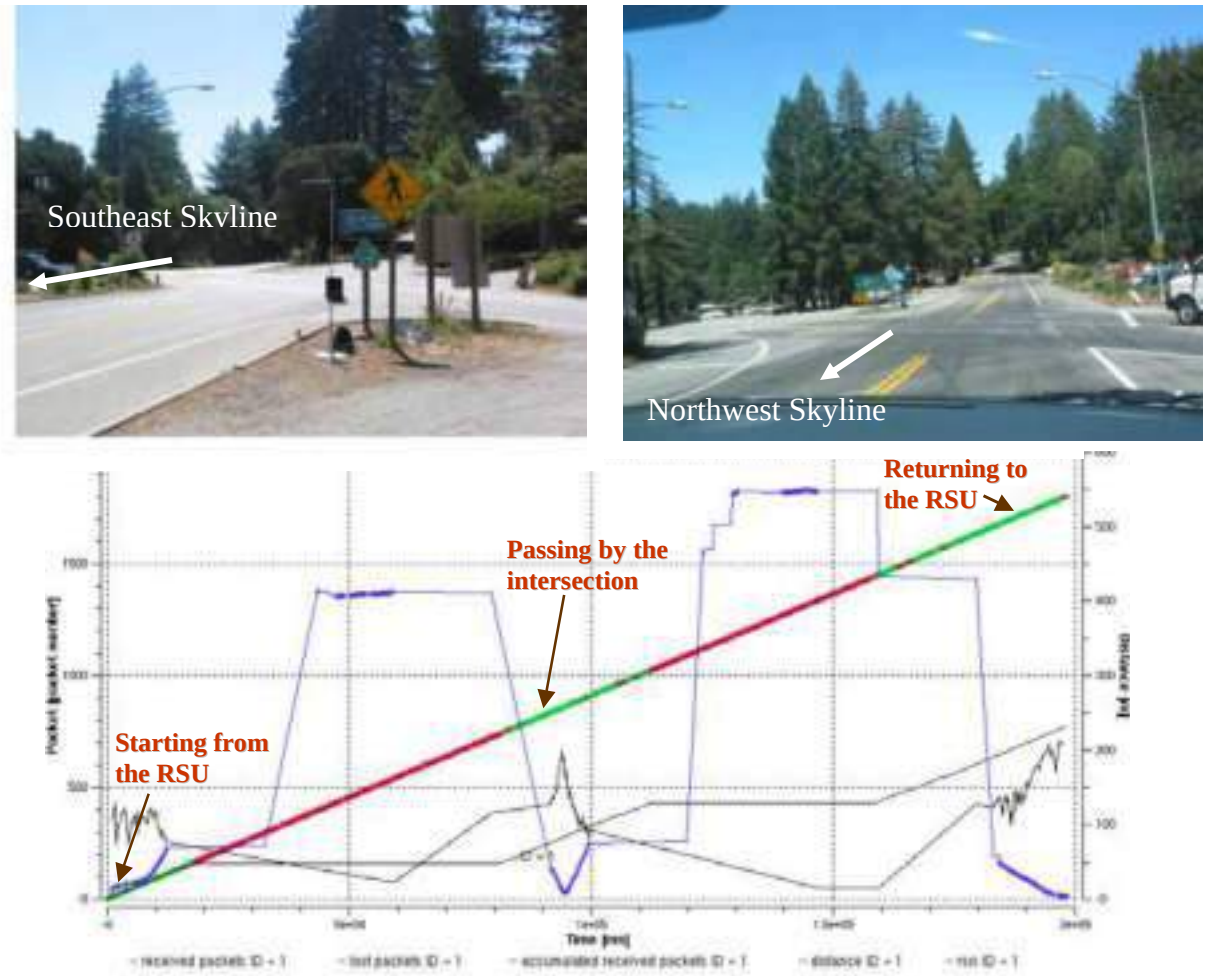


Figure 45. Views and CTK Plot for the Skyline Test Run

2.1.15 Page Mill Road & Deer Creek Road

The intersection of Page Mill and Deer Creek in Palo Alto has medium traffic during daytime. Both roads have two lanes at both directions. Southbound Page Mill curves slowly to the southwestern direction and goes uphill. There are trees along the curve. Page Mill has a left turn lane with a traffic light at the Deer Creek intersection. The RSU was placed on the eastern corner since it provided line-of-sight for the southbound and eastbound traffic (Figure 46).

The car started on Page Mill going southbound and uphill. Without line-of-sight, only few or no packets were received. There was 100 percent reception of packets as the car came out of the curve. The car turned left at the light onto Deer Creek going eastbound, and reception was blocked at close to 100m away from RSU due to no line-of-sight (obstructions such as sign posts, controller boxes etc.).

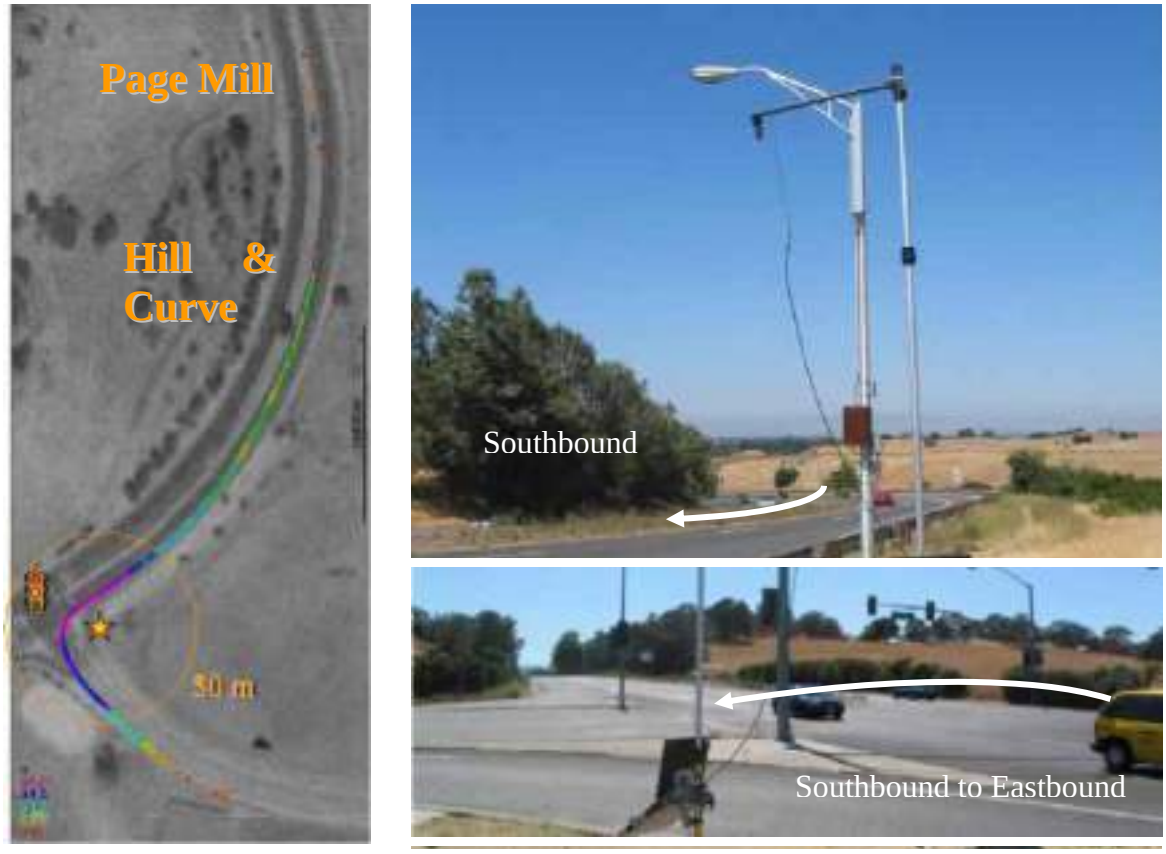


Figure 46. RSSI Plot and Views for the Page Mill Test Route

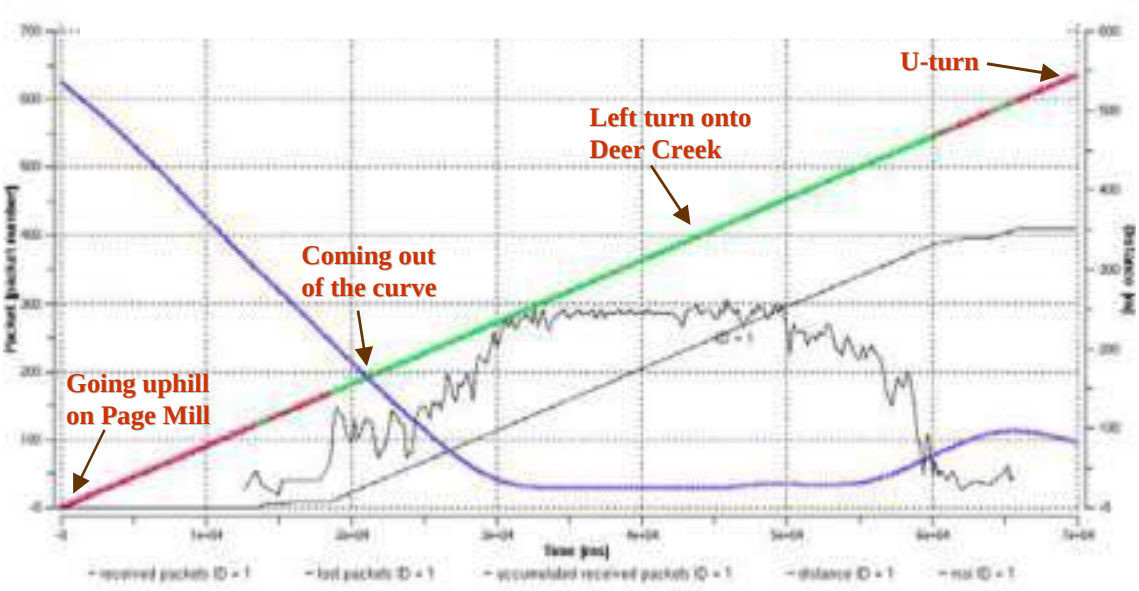


Figure 47. CTK Plot for the Page Mill Test Run

2.1.16 Squirrel Road & Long Lake Road

This intersection is characterized by single lane roads, line of sight obstructions, and overhead foliage that often blocked the GPS signal. Vehicles traveling along Squirrel Road experience two hills, both descending southbound, and vehicles traveling along Long Lake Road experience a curving roadway with the line of sight blocked by foliage and terrain along the roadside.

Packet reception for northbound and southbound travel was quickly interrupted by line of sight blockage due to Hills #1 and #2, and GPS outage along this route was prevalent due to thick foliage above the roadway (Figure 48). Packet reception for eastbound and westbound travel faded off gradually beyond 100m due to impeding terrain and foliage along the curving roadway. Infrequent GPS outages occurred due to the trees overhead.

Figure 48. RSSI Plot for the Squirrel and Long Lake Test Routes

For Squirrel Road northbound, initially packets were lost due to blockage when the test vehicle was driving up Hill #2 and/or foliage alongside the roadway (Figure 49, caption 1). The GPS signal was often blocked by overhead foliage. The vehicle stopped before the red light 20 meters from the RSU with 100 percent packet reception rate (2). Packet reception was interrupted after driving over Hill #1 on Squirrel Road (3). The GPS signal was blocked by overhead foliage.

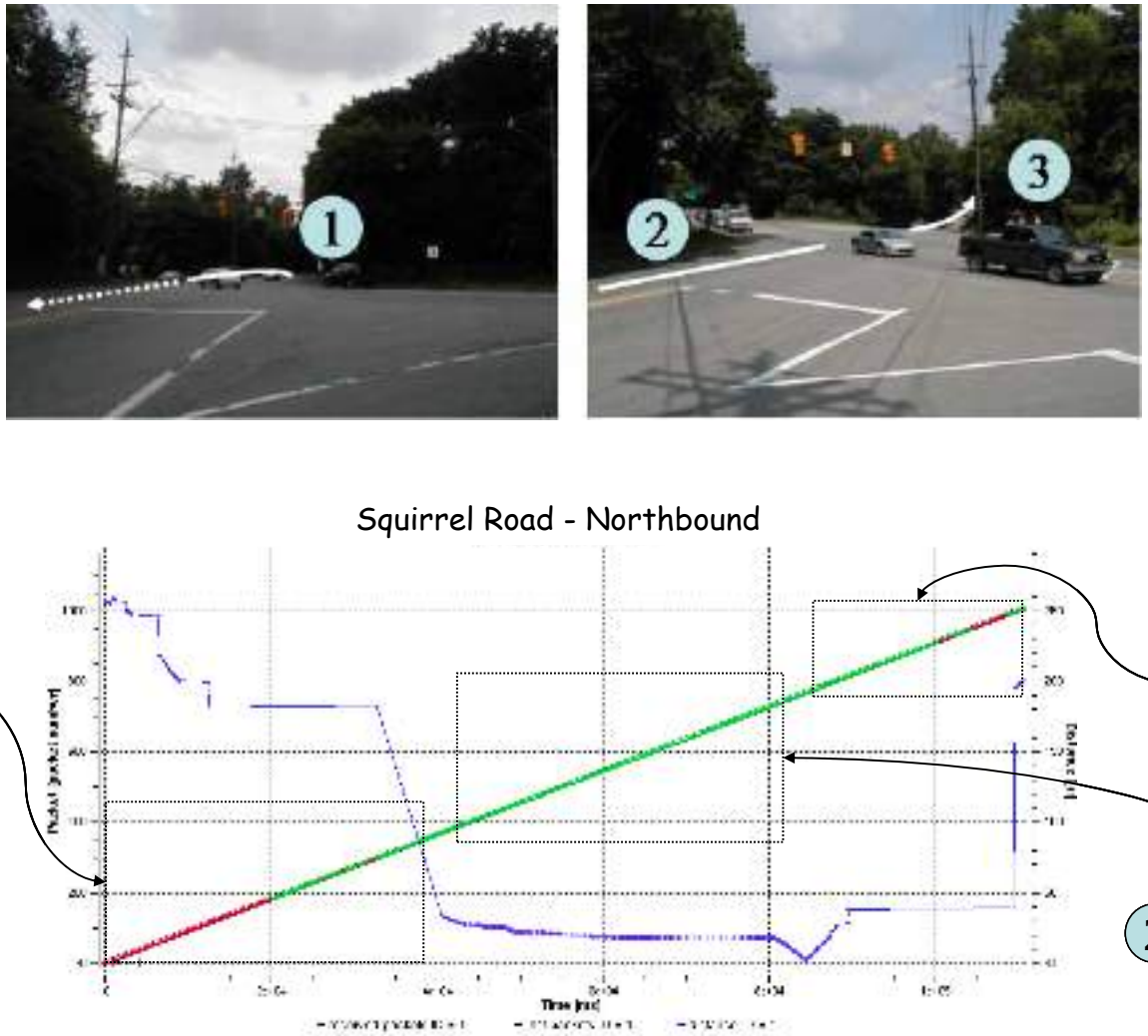
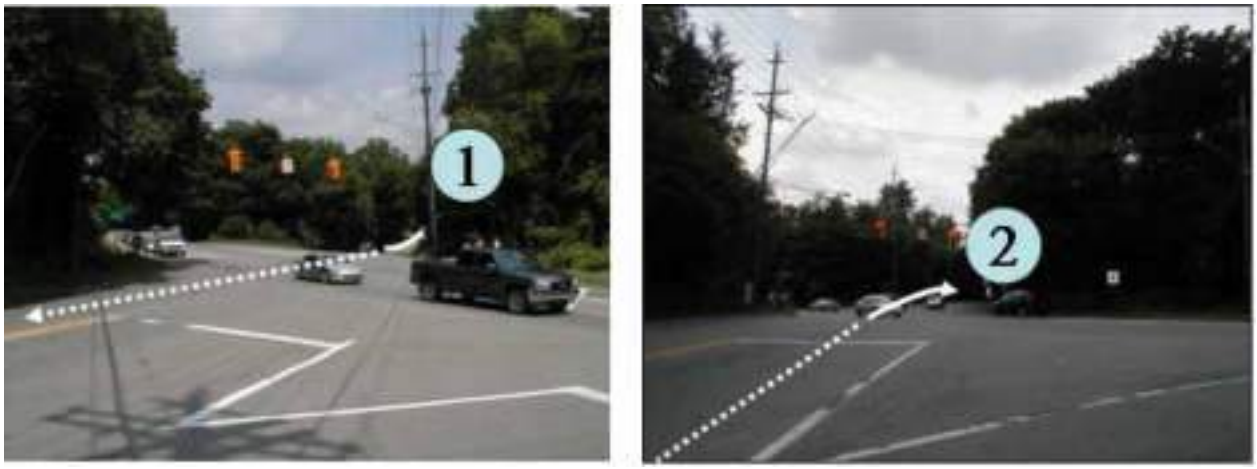


Figure 49. Views and CTK Plot for Northbound Squirrel Test Run

For Squirrel Road southbound, packet reception was initially blocked by Hill #1 and/or foliage along the roadside (Figure 50, caption 1). The GPS signal was blocked by overhead foliage. At the intersection, packet reception was excellent until the test vehicle passed over Hill #2, while the overhead foliage again blocked the GPS signal (2).



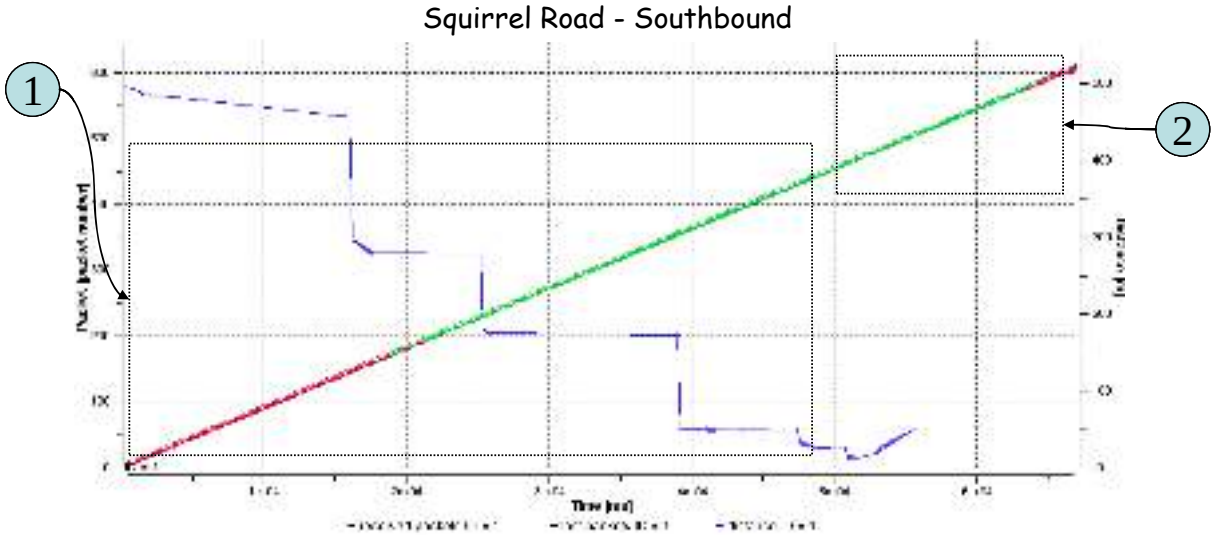
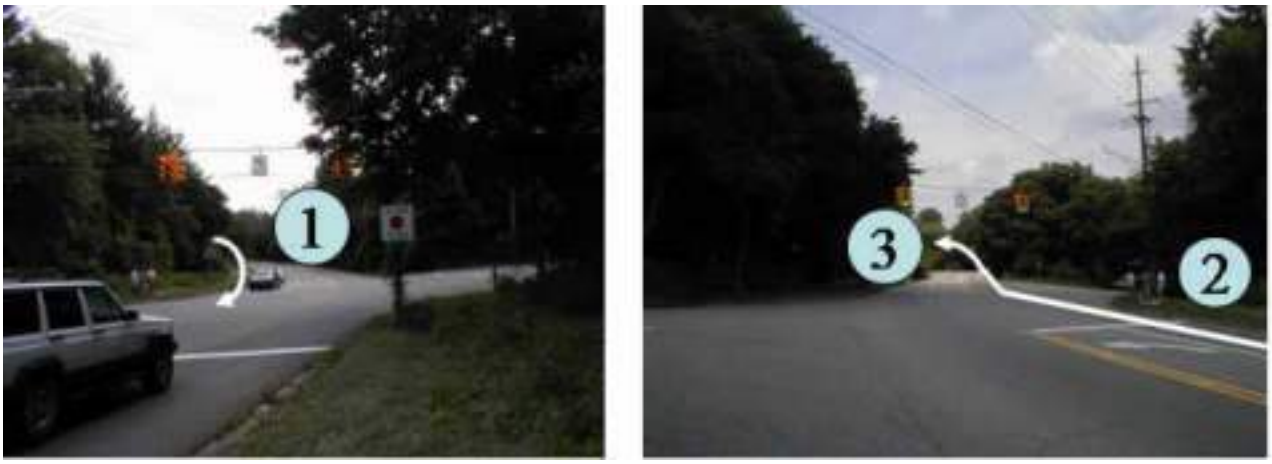


Figure 50. Views and CTK Plot for the Southbound Squirrel Test Run

For westbound Long Lake, line of sight was initially blocked by terrain and foliage along the curving roadway before packet reception becomes 100 percent as the vehicle approached from ~100 m (Figure 51, caption 1). The test vehicle stopped at the traffic signal with 100 percent packet reception (2). Intermittent packet reception and GPS outage occurred as the vehicle traveled along the curving roadway with foliage and terrain blockage (3).



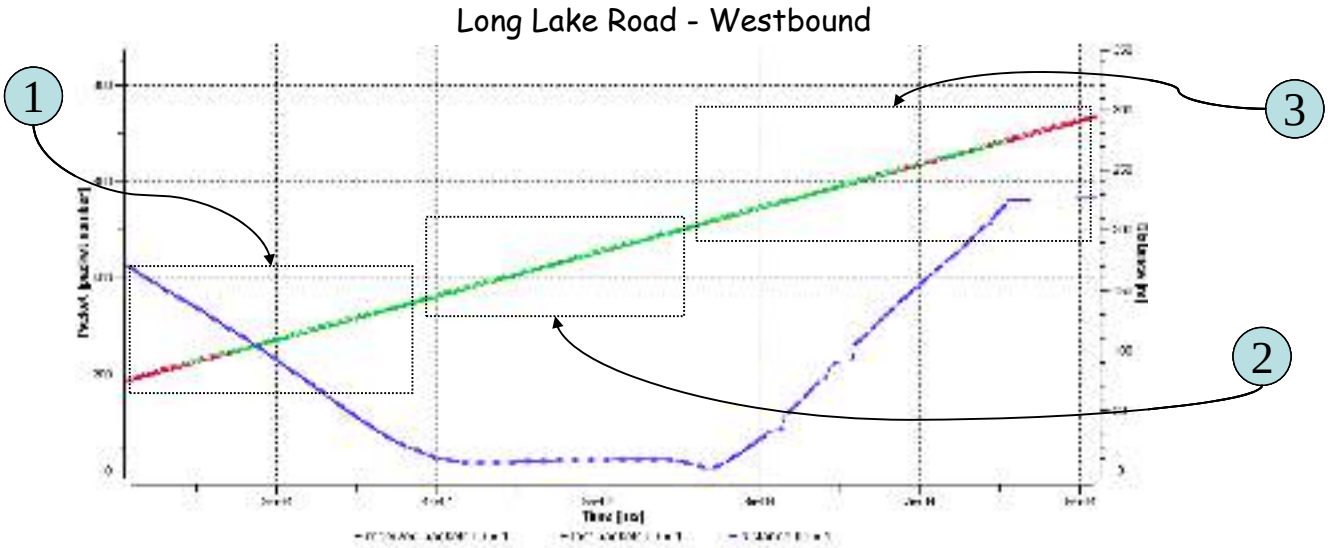


Figure 51. Views and CTK Plot for the Westbound Long Lake Test Run

For eastbound Long Lake, the line of sight was initially blocked by terrain and foliage along the curving roadway before packet reception became 100 percent as the vehicle approached from ~100 m (Figure 52, caption 1). Intermittent packet reception and GPS outage occurred as the vehicle traveled along the curving roadway with foliage and terrain blockage (2).

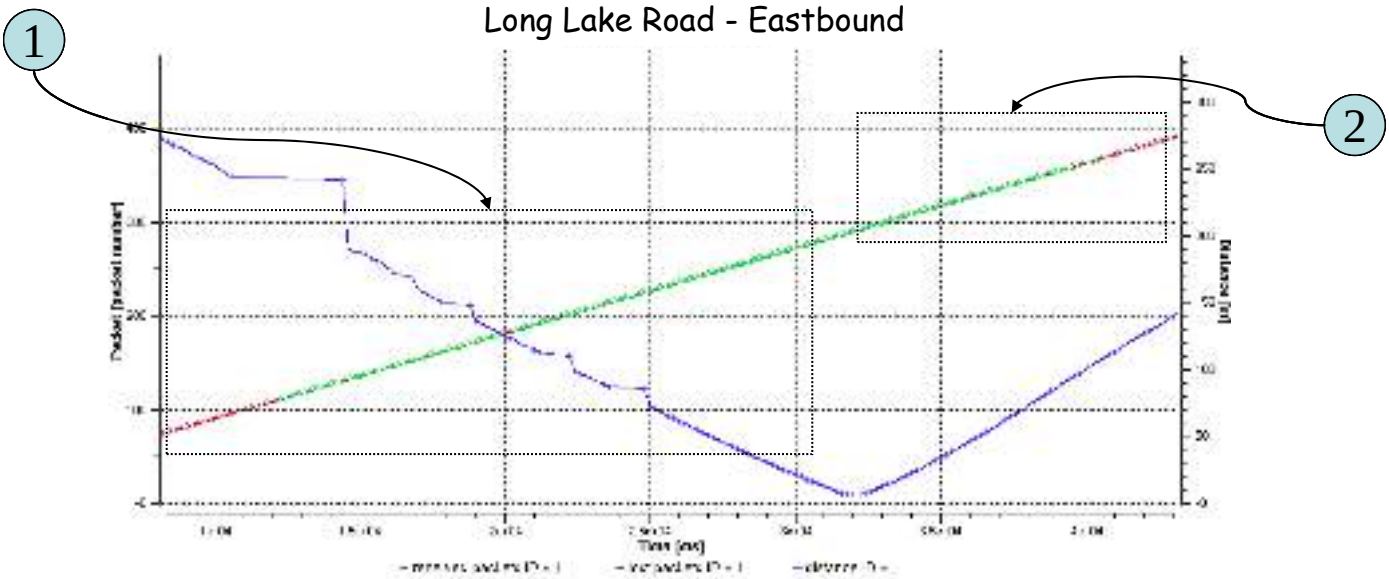


Figure 52. Views and CTK Plot for the Eastbound Long Lake Test Run

2.2 Comparisons with the Open Environment Baseline Data

Figure 53 shows the Received Signal Strength Indicator (RSSI) data from two locations superimposed. Testing at the intersection of Oakwood Boulevard and Michigan Avenue in Dearborn is superimposed upon the corresponding data acquired from the Milford Proving Grounds (MPG). To somewhat simplify the graph, data south and west of the RSU have been arbitrarily plotted on the negative axis, while data north and east of the RSU have been plotted on the positive axis.

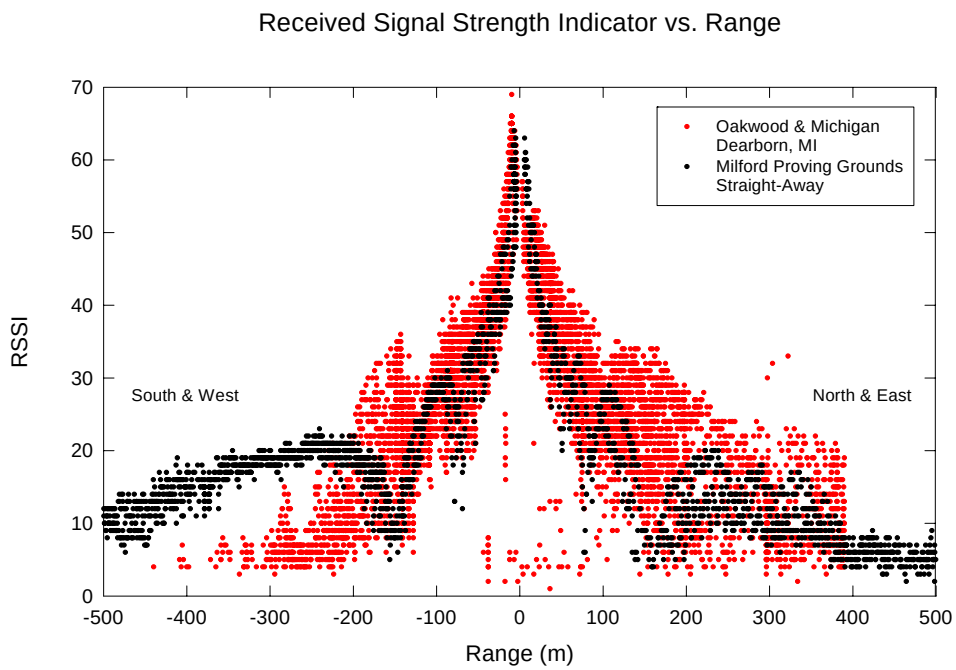


Figure 53. Data Comparison of Oakwood/Michigan and Milford Proving Grounds

There are several interesting observations to gather from this plot. The testing environment at the Oakwood and Michigan intersection is quite cluttered, both with buildings and other physical obstructions and also with very dense traffic. Despite this, over the range corresponding to line of sight between the RSU and OBU, the RSSI with distance displays essentially the same envelope with distance as that measured at the more wide open environment found at the MPG. We also observe that the nulls in the MPG data at ~75m and ~150m are not observed in the intersection testing data, presumably due to the multitude of multipath reflections created by the dense environment. Finally, there is also a much greater variability in the RSSI at a given distance in the intersection testing data, again likely due to the dense environment.

Figure 54 shows the RSSI data from the intersection of Crooks and Big Beaver Roads in Troy plotted along with the corresponding data acquired from the Milford Proving Grounds. The plots have been derived from multiple sets of runs - in the case of the intersection at Crooks and Big Beaver, 12 data sets were combined, binned into histograms of 10m intervals, and the mean RSSI values calculated. For the MPG data, four runs were compiled.

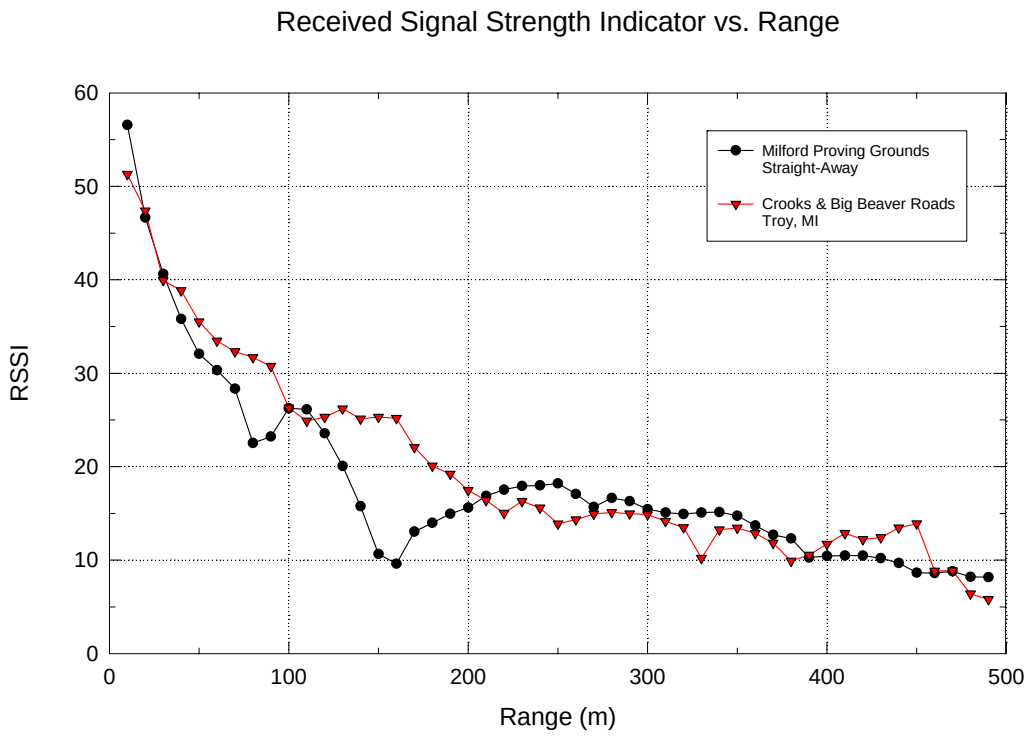


Figure 54. Data Comparison of Crooks/Big Beaver and Milford Proving Grounds

Note that the intersection at Crooks and Big Beaver is far less cluttered than the Oakwood and Michigan intersection described in the previous figure. However, as with the previous case, the key points to note are that the nulls in the MPG data at ~75m and ~150m are clearly not present in the data from the intersection testing, and that the overall shape of the RSSI with distance is the same for both the intersection and MPG testing scenarios. (Although error bars were not shown on the graph to maintain clarity, the spread in data about the mean was again far larger for the intersection scenario than for testing at MPG.) These results suggest that obstructions found in the typical intersection environment do not noticeably degrade the quality of radio reception.

2.3 Summary

Intersections in the Detroit and San Francisco Bay areas were chosen as sites for DSRC transmission characterization in order to gain a better understanding of how the unique characteristics of these intersections affect DSRC communications. All intersection testing was conducted with prior approval from the public jurisdictions responsible for the intersections. The Consortium used the Task 4 CTKs and the Task 6C antennas as improvised roadside units.

- Though not optimized for the functionality that would be expected of an RSU, the Task 4 CTKs and Task 6C antennas provided more than adequate range as demonstrated in the baseline evaluation conducted at Milford Proving Grounds (MPG). Packets were received when the test vehicle was more than 500m from the RSU, and this is well in excess of anticipated range requirements for in-vehicle safety applications.

- Open environment testing conducted at MPG also revealed that there are local minima in the RSSI at ranges corresponding to ~75m and ~150m, consistent with results found and reported in the Task 4 Report (Multipath Considerations) regarding the geometry of the radio propagation for our testing arrangement.

- All intersection testing was conducted with a single RSU broadcasting to an OBU-equipped test vehicle traveling through the thoroughfare. The effect of many OBUs attempting to transmit at the same time as the RSU is addressed in the Task 12 Simulation Report.

- The general findings from testing conducted at a representative intersection (Woodward Avenue and I-696 Service Drive in Huntington Woods, Michigan) demonstrate an 85 percent successful transmission ratio while the test vehicle was approaching the RSU from 250 m, and a 99 percent success ratio while approaching from 100m.

- In some cases, packet reception near an intersection can be blocked by heavy vehicle traffic. This situation can likely be improved upon by changing the positioning of the RSU that was used during our testing (~10’ height, etc.) so that the line-of-sight is optimized. It is likely that RSU positioning will not resolve all line-of-sight blockages between RSU and OBU antennas, especially for vehicles that are traveling behind large trucks, and this fact should be taken into consideration when designing intersection-based safety applications.

- In some cases, reception was maintained despite the fact that there was no line-of-sight between the antennas. But eventually packet reception was lost in those situations when the test vehicle moved further and further away from the RSU around a bend in the road with significant terrain and foliage blocking the view between the antennas.

- As expected, reducing the power level of the DSRC sending unit decreases the range at which packets can be received. This can be an important consideration when specifying RSU output levels.

- Downhill grades and extensive foliage can block the line-of-sight of vehicles approaching an intersection, up to the point where they are almost upon the cross street. A method of providing the RSU transmissions to these vehicles, be it through infrastructure-based repeaters or by other means, should be considered for safety critical systems.

- There were many instances when the GPS signal was lost, but packet reception between the RSU and the OBU was maintained, especially in locations near tall buildings or under extensive foliage. The prospect of maintaining adequate vehicle positioning resolution under concrete canyon or tree-laden conditions is a design issue for intersection safety system development.

- Comparing typical intersection data with similar data from the more wide-open environment found at MPG, the RSSI with distance displays essentially the same envelope. We also observed that the nulls in the MPG data at ~75m and ~150m are not observed in the intersection testing data, presumably because of multipath reflections created by the dense environment, and variability of the geometries involved during subsequent test runs. It was also noted that there is also a much greater variability in the RSSI at a given distance in the intersection testing data, again likely due to the dense environment.

3 INTERSECTION TESTING USING A SYNCHRONIZED TRAFFIC CONTROLLER

In this section the results of the testing at the Orchard Lake & 10 Mile Roads intersection are discussed and analyzed. In contrast with previous testing at various locations around the Detroit and Palo Alto areas, some of the new elements introduced for this particular intersection were:

1. Wave Radio Modules (WRM) and Task 9 Laptop were used instead of Task 4 CTKs.
2. RSU wireless message consisted of actual traffic signal controller data (phase & timing) instead of "dummy" packets.
3. All radios were configured in both transmit and receive modes, therefore the RSU was also receiving the actual dynamic data from the OBU (vehicle speed, location, etc.).

3.1 Background and Test Set-Up

Due to logistical and safety concerns, it was decided that rather than connecting the Task 9 laptop to the traffic signal controller actually controlling the traffic lights it would be connected to a second, independent controller. This second controller was programmed with exactly the same timing as the actual controller but its outputs were not connected to any traffic lights. There were several reasons for this decision:

- To eliminate any risk of interfering with the intersection traffic controller.
- To be less dependent on the local authorities for support than if we were connecting directly to intersection traffic signal controller.
- To be immune from any potential incompatibilities with the traffic signal controller installed at the intersection.

The controller used was an Eagle EPAC300 M30. It is shown in Figure 55.

Figure 55. EPAC M30

3.1.1 Traffic Signal Controller Interface

Getting the traffic signal information from the controller into the Task 9 laptop proved to be much more difficult than first anticipated. Real-time transmission of the current state of the traffic lights and the countdown to the next state are generally not a feature on most controllers.

Fortunately, with some assistance from Virginia Tech, the RS-232 output from the Eagle controller was able to be requested and read through an experimental interface. This traffic signal controller output is primarily intended to communicate with other devices running Eagle software and is not well documented. The experimental traffic signal controller interface was implemented in the Task 9 software.

Using the data received from the traffic signal controller the Task 9 software was then able to transmit the traffic signal information wirelessly. The content of the RSU message is summarized (in a simplified manner) in Table 9. More details on the RSU serial interface and message format can be found in the Appendix F.

RSU Header Message	*Message Type*	*1 byte*
	RSU I.D	*6 bytes*
	Precision indicator	*1 byte*
	Latitude, Longitude, Altitude of RSU	*11 bytes*
	UTC Time	*5 bytes*
Traffic Controller Data	*Latitude, Longitude, Altitude of Stop. Loc. #1*	*11 bytes*
	Directionality of Stop. Loc. #1	*2 bytes*
	Current State of Traffic Light at Stop. Loc. #1 (Green, Yellow, Red)	*1 byte*
	Time left in current state of Traffic Light at Stop. Loc. #1	*2 bytes*
	Duration of Yellow State at Stop. Loc. #1	*2 bytes*
	……	*…*
	Latitude, Longitude, Altitude of Stop. Loc. #4	*11 bytes*
	Directionality of Stop. Loc. #4	*2 bytes*
	Current State of Traffic Light at Stop. Loc. #4 (Green, Yellow, Red)	1 byte
	Time left in current state of Traffic Light at Stop. Loc. #4	*2 bytes*
	Duration of Yellow State at Stop. Loc. #4	*2 bytes*

Table 9. RSU message

3.1.2 Choice of Intersection

The intersection chosen for the test was Orchard Lake Road and 10 Mile Road in Farmington, Michigan. This intersection was chosen for several reasons:

- The timing of the lights is constant, i.e. there are no traffic flow sensors that cause the timing of the lights to be dynamically adapted.

- The traffic signal controller and lights installed at the intersection are owned and maintained by the Road Commission for Oakland County (RCOC) and earlier contact between VSCC and RCOC seemed to indicate the best potential for successful cooperation.

- It is reasonably close to the CAMP facility in Farmington Hills and therefore requires less logistical efforts that other intersection.

Figures 56 through 59 show the intersection from four different directions.

Figure 56. Orchard Lake Road – Southbound Direction

Figure 57. 10 Mile Road – Eastbound Direction

Figure 58. Orchard Lake Road – Northbound Direction

Figure 59. 10 Mile Road – Westbound Direction

3.1.3 Test Preparations

The independent traffic signal controller was programmed by the Road Commission for Oakland County (RCOC) to use exactly the same timing as the controller at the selected intersection (10 Mile Road and Orchard Lake Road). Specifically, the program was a fixed 70-second cycle broken down as follows:

- 28 seconds of green for Orchard Lake Road
- 5 seconds of yellow for Orchard Lake Road
- 1 second of red for all directions
- 36 second of red for Orchard Lake Road
- 30 seconds of green for 10 Mile Road
- 5 seconds of yellow for 10 Mile Road
- 1 second of red for all directions
- 34 seconds of red for 10 Mile Road

On the day of testing, the synchronization of the clocks on both controllers (the independent controller and the one installed and controlling the traffic lights at the intersection) was achieved with the assistance of a technician from RCOC. This synchronization had the effect of "matching" the timing programs in each controller and thus in theory both controllers were operating in parallel.

This synchronization of the controllers was verified in three ways*:*

1. Visually comparing the traffic light display on our controller with the state of the lights in the intersection.

2. Visually comparing the traffic light display in the Task 9 software with the state of the lights in the intersection.

3. Later in post-processing time-stamped video of the state of the lights was compared to the time-stamped output of our controller collected by the Task 9 software. They were found to be within 100 to 200 milliseconds of one another.

It is worth noting that after about an hour of testing, the two controllers were slightly out of synchronization. The controller connected to the RSU was lagging behind the installed controller. Later, it was determined that the power supply being used (an inverter running off a vehicle's 12 VDC power) to power the independent controller caused the clock to run slow. It lost about a millisecond every second. This was a steady drift and was corrected for in the data analysis.

For all the tests the RSU equipment was set up and transmitting from the southeast corner of the intersection. Also, the WRMs were configured to send and receive on the DSRC Control Channel, which is Channel 178 with a center frequency of 5890 MHz and a 10 MHz bandwidth.

3.2 Full Power Transmit Testing and 5.9 GHz DSRC Intersection Characterization

The first set of tests consisted of transmission of the RSU message Table 9 with the following WRM configuration:

Packet Length (bytes)	Message Interval (ms)	Data Rate (Mbps)	Transmit Power (dBm)
500	100	6	Full (~20 dBm)

Table 10. WRM configuration for RSU message (Full dBm)

Testing consisted of driving through the intersection in every direction and in every lane at normal traffic speeds. The RSU message received by the WRM-OBU in the vehicle was logged along with synchronized (GPS time stamp) video for post processing.

3.2.1 Performance Characterization

To assess the performance of the 5.9 DSRC technology and the WRMs in particular, the intersection data from all the runs was analyzed by calculating the ratio of received versus sent packets. It is important to note that this ratio was derived by initially considering the first and last received packet regardless of where the receptions occurred. Later on in the next section, another calculation of the successful transmission ration was performed to provide a more relevant reception percentage in the range of interest (250 m for the traffic signal violation warning application).

The summary plots depicting received packets, range from the RSU and RSSI for representative runs in every direction can be found in Figures 60 through 63. The range of communication achieved at full power setting (~20dBm) varied between 400 and 600 m. For the full range of communication, the successful transmission percentage was between 85 percent and 95 percent in all directions except for the northbound leg of the intersection where it dropped to 69 percent. In the Northbound direction (see Figure 63) a large number of packets were lost at ranges beyond 500m and this contributed to the lower ratio of 69 percent. The sporadic reception of packets at ranges beyond 500 m, which can dramatically reduce the successful transmission ratio, highlights the need to limit the range of interest when analyzing the data. In this case, the range of interest is approximately 250 m as defined by most safety applications in Task 3. Figures 64 through 71 summarized the results when the range of interest is limited to 250 m. The successful transmission ratio varies between 88 percent and 96 percent.

The communication outages experienced during testing were mainly of minimal duration (200 ms; i.e., one packet lost then communication is re-established). Longer outages of approximately one second in the eastbound and northbound data warranted a closer look and some justification. In the eastbound direction, an examination of the video collected during these runs, and the digital photographs documenting the RSU set-up, revealed that the likely cause of the repeatable one-second outage was due to a road sign obstruction of the transmitting antenna. This situation would not occur if a more optimal set-up of the antenna (high in the middle of the intersection, for example) were logistically feasible during our testing. In the northbound direction, the longer outages occurred, as expected, around the 250 m range in a hilly part of the roadway.

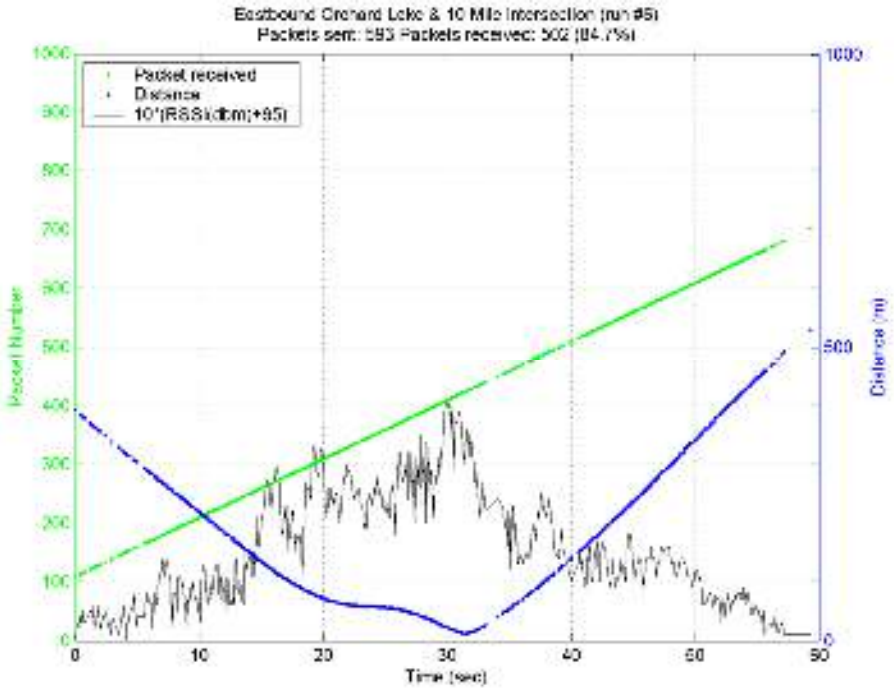


Figure 60. Eastbound 10 Mile Rd. Packets Received, Range, and RSSI

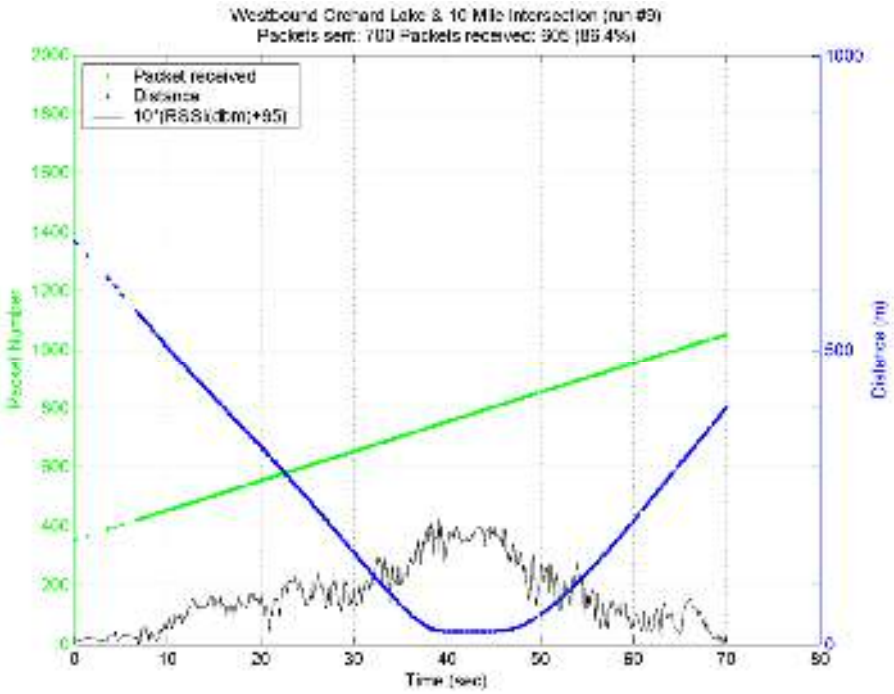


Figure 61. Westbound 10 Mile Rd. Packets Received, Range, and RSSI

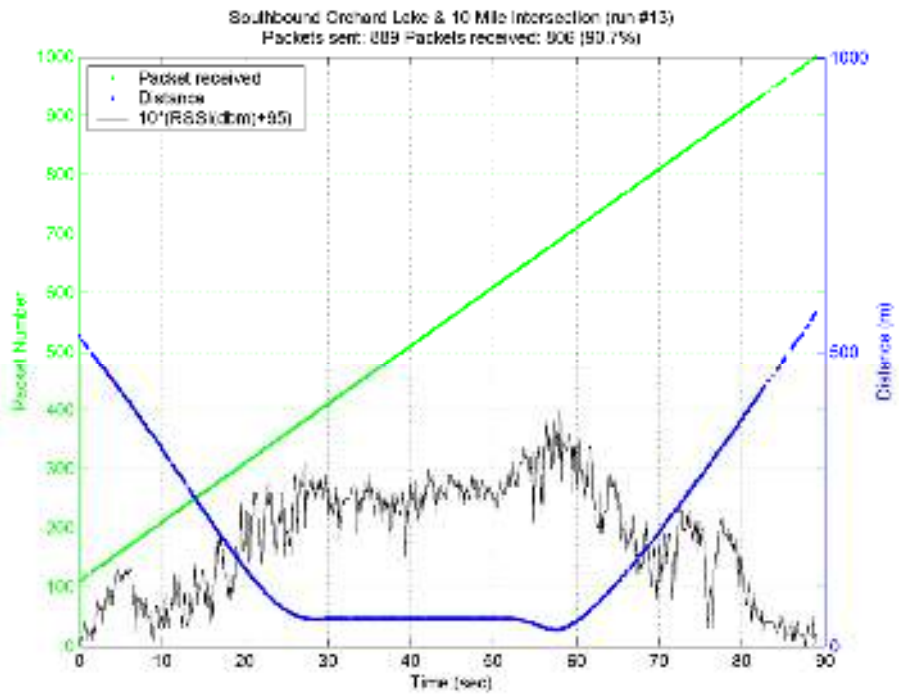


Figure 62. Southbound Orchard Lake. Packets Received, Range, and RSSI

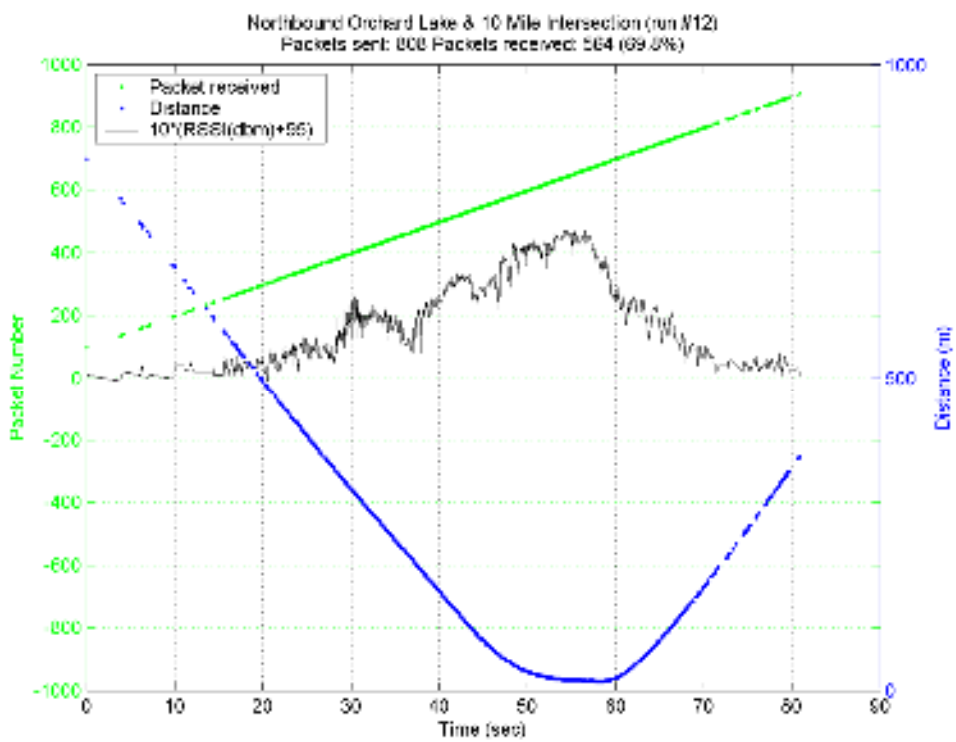


Figure 63. Northbound Orchard Lake. Packets Received, Range, and RSSI

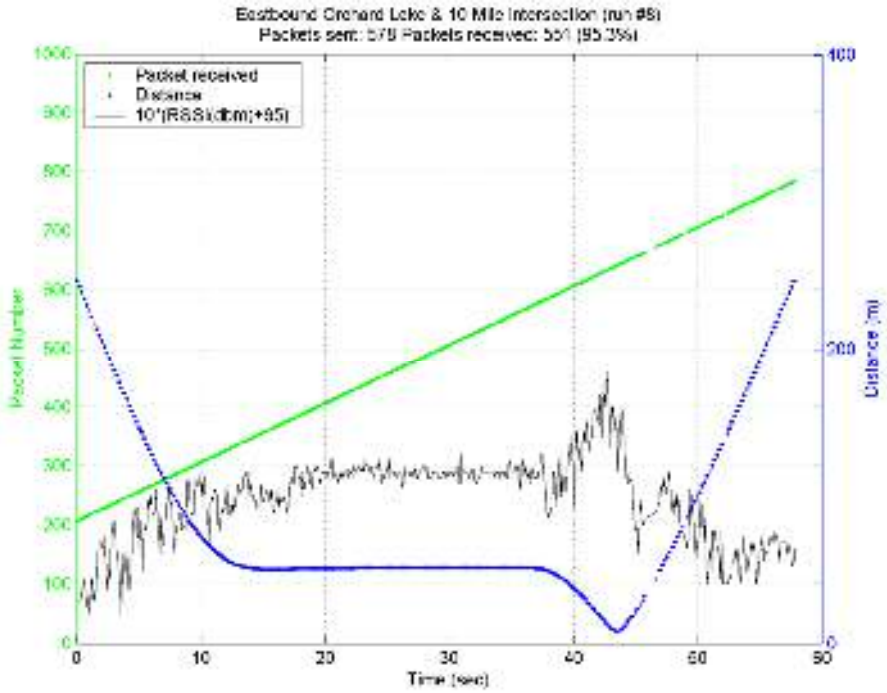


Figure 64. Eastbound 10 Mile Rd. Packets Received, Range, and RSSI Within 250 m Range of Interest for Safety Applications

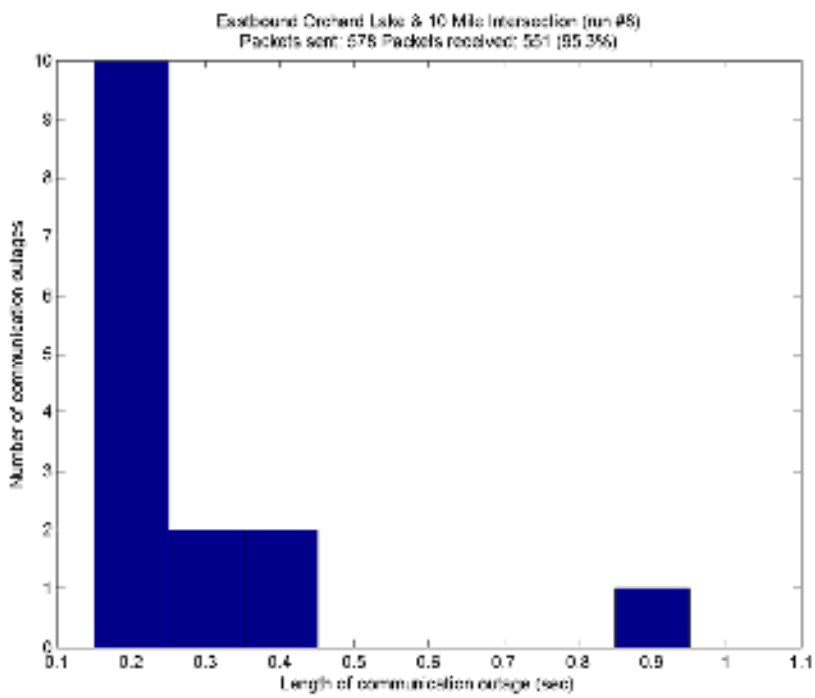


Figure 65. Number of Outages and Length in Eastbound Direction Within 250 m

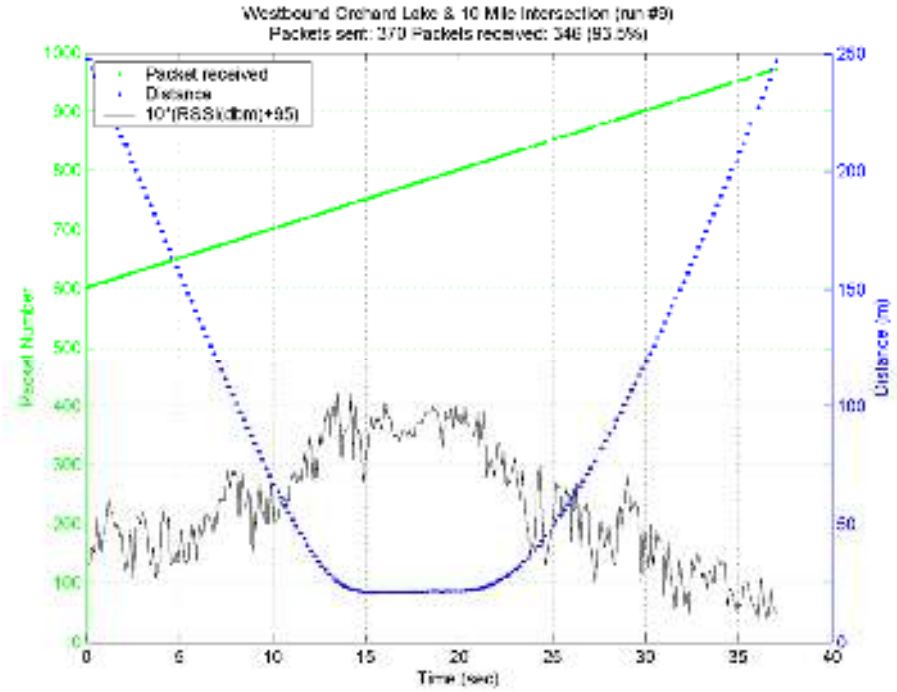


Figure 66. Westbound 10 Mile Rd. Packets Received, Range, and RSSI Within 250 m Range of Interest for Safety Applications

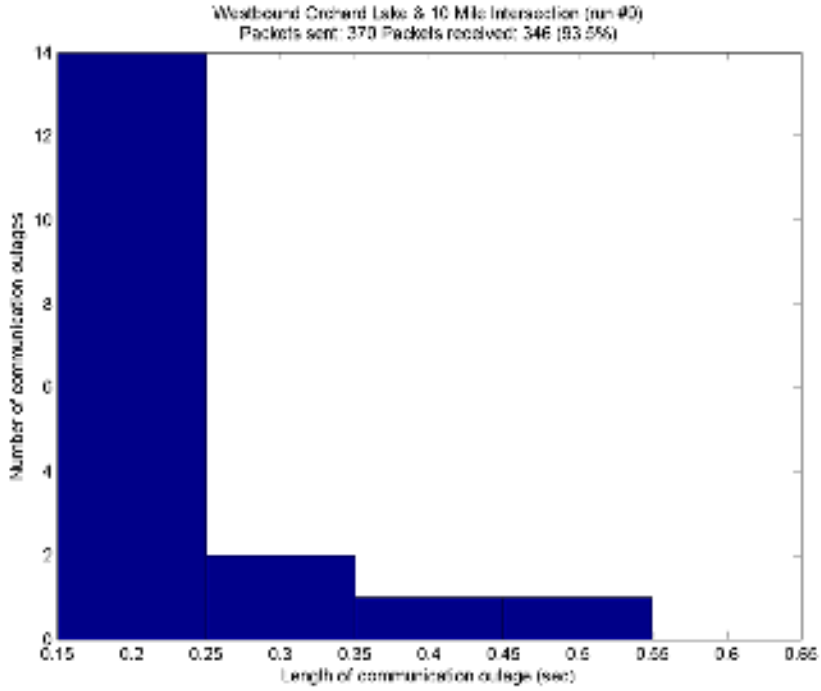


Figure 67. Number of Outages and Length in Westbound Direction Within 250 m

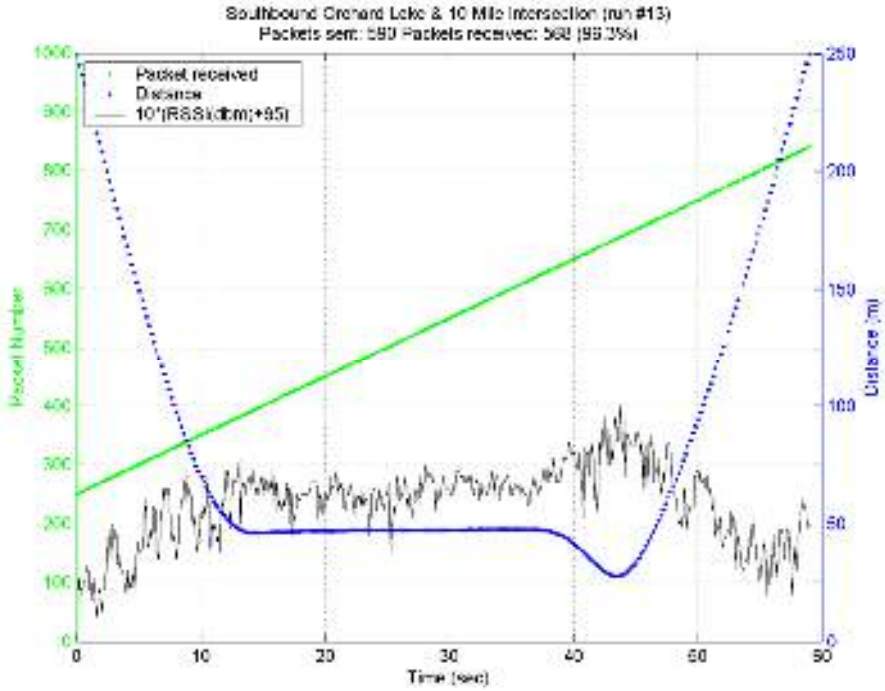


Figure 68. Southbound 10 Mile Rd. Packets Received, Range, and RSSI Within 250 m Range of Interest for Safety Applications

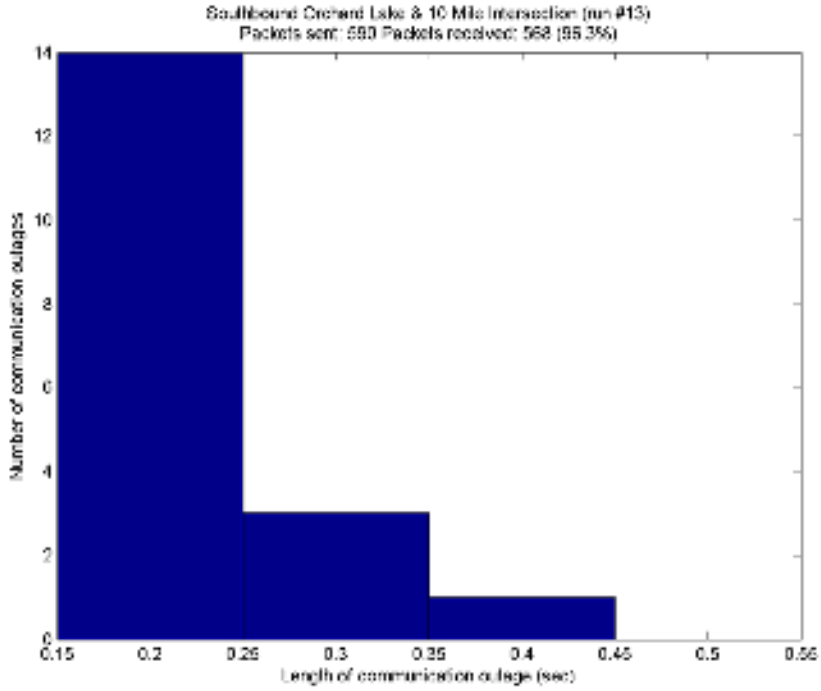


Figure 69. Number of Outages and Length in Southbound Direction Within 250 m

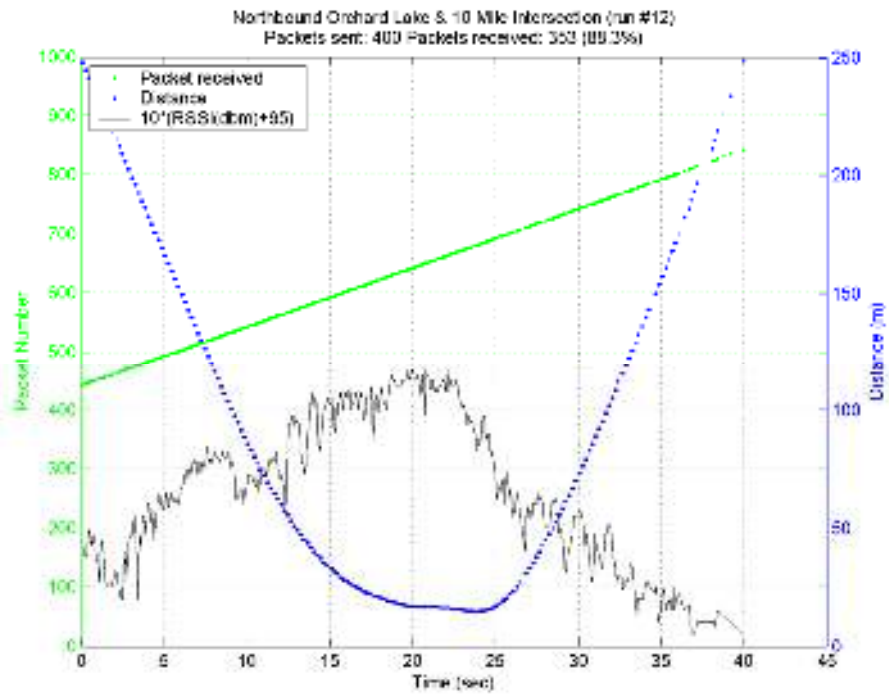


Figure 70. Northbound 10 Mile Rd. Packets Received, Range, and RSSI Within 250 m Range of Interest for Safety Applications

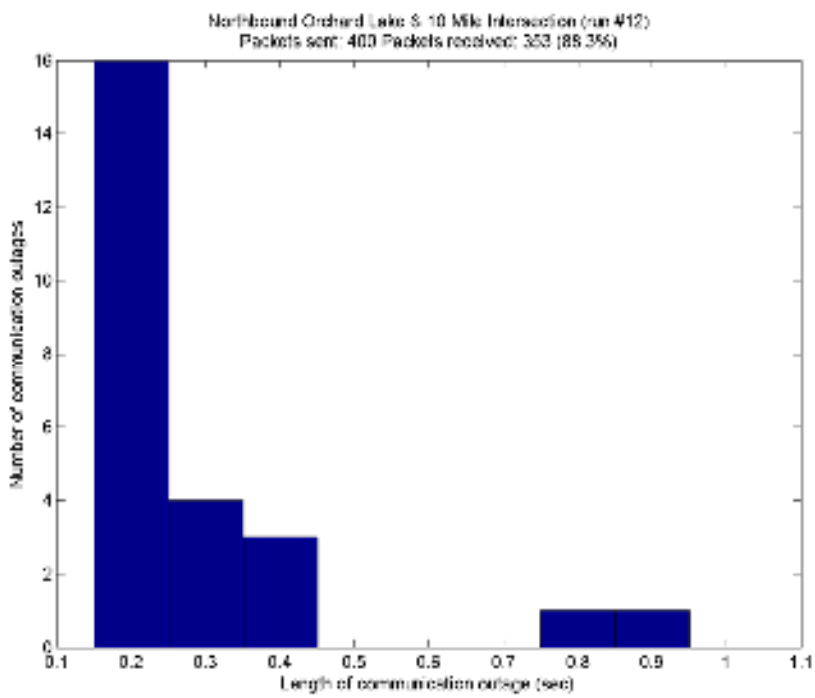


Figure 71. Number of Outages and Length in Northbound Direction Within 250 m

Figure 72. RSSI Level and Packet Reception in All Directions and Multiple Lanes at Orchard Lake and 10 Mile Road Within 250 m of RSU Location

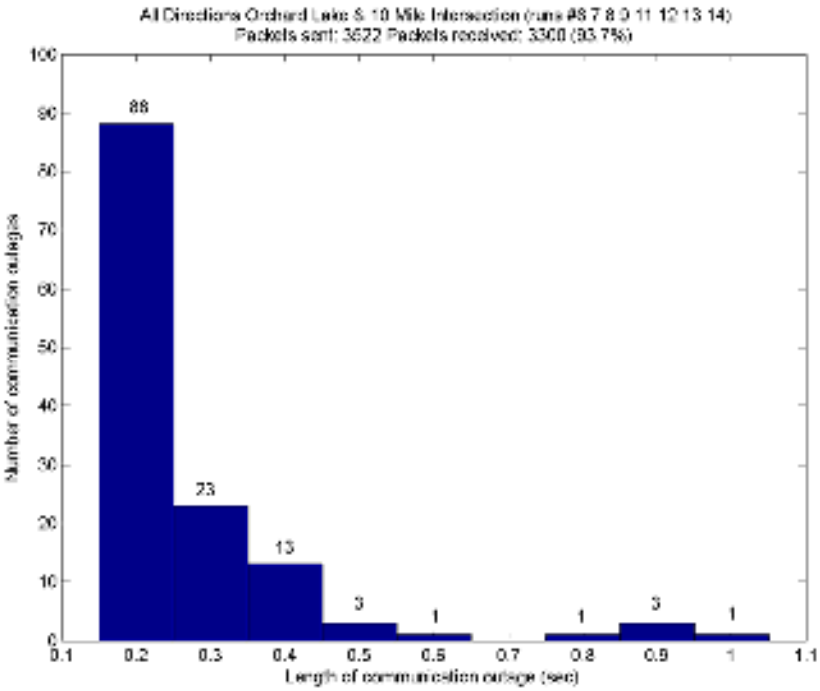


Figure 73. Cumulative Number of Outages and Respective Length of Time at Orchard Lake and 10 Mile Road Within 250 m of RSU Location

Figure 72 shows an overlay of colorized RSSI values on top of an aerial photograph of the intersection. As expected, the RSSI value was highest closer to the RSU and sporadic packet losses occurred at ranges closer to 250 m. The cumulative successful transmission ration was 93.7 percent. It is worth noting again that this was achieved under a sub-optimal RSU antenna setting (intersection corner, 10 ft above the ground) and with an inverted OBU roof-mount antenna, clearly not optimized for RSU conditions.

Figure 73 shows the cumulative number of outages from all the test runs along with their length in seconds. The most frequent outages (88) are of the minimal kind (i.e., 200 ms). This kind of outage is certainly the easiest outage to remedy with data coasting techniques. As mentioned earlier, the longer outages (around one second) are either due to hilly terrain or road sign obstructions and should be substantially reduced with proper RSU antenna placement.

In light of all the previous plots and results, it can be concluded that the RSU-OBU communication at this intersection was relatively high (above 93%) within the required range of 250 meters.

3.2.2 Traffic Signal Controller Phase and Timing

The RSU message being sent by the RSU contained, as described in Table 9, information regarding the current signal status for each direction as well as the time remaining in the current state. This information was received by the OBU as it traveled through the intersection and would have been available, in real-time, to a safety application such as traffic signal violation

warning if it were implemented on-board the vehicle. To illustrate the type of information in the RSU message that the OBU received during the multiple runs, Figure 74 shows the distance and velocity (*10) of the OBU color-coded with the received signal status. At about 325 m west of the RSU, the light turned yellow. The driver started slowing down when the light turned red at about 200 m (10-second tick mark on time line). The OBU came to a full stop before driving through the intersection when the light turned green (just beyond the 40-second tick mark on the time line). The collected data showed that the red phase lasted 34 seconds as expected for this leg of the intersection.

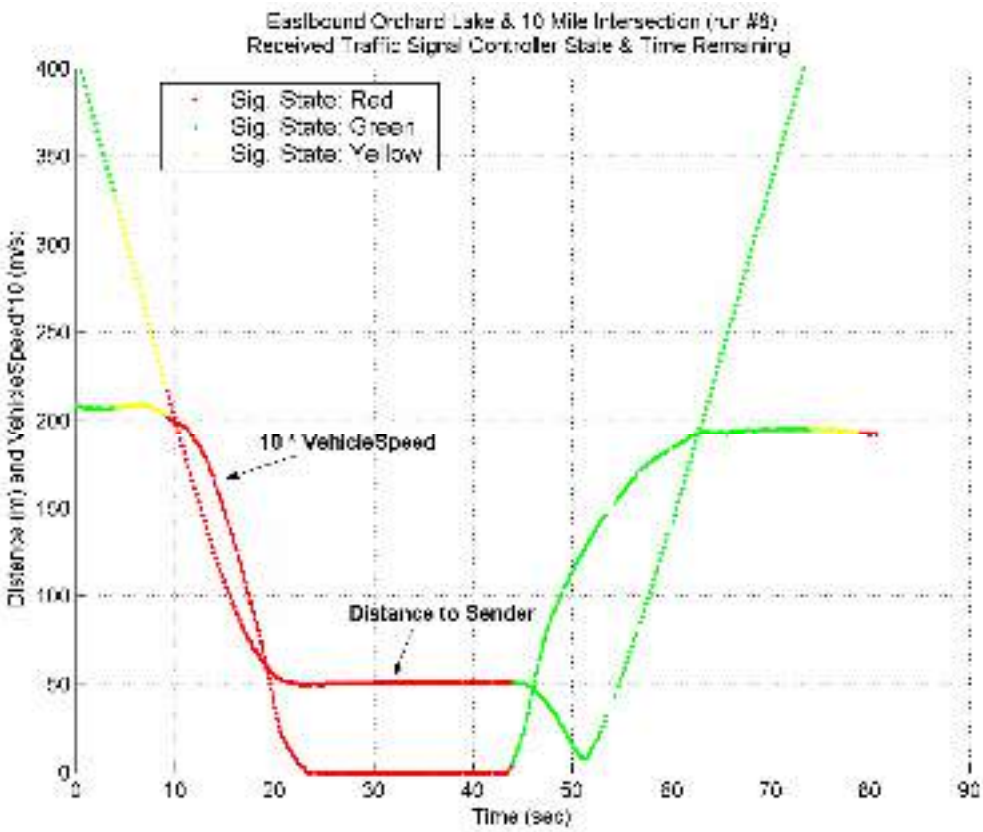


Figure 74. Distance, Vehicle Speed, and Signal State for an Eastbound Run

Figures 75 and 76 illustrate the signal state and time remaining in the eastbound direction as received by the OBU while traveling through the intersection. It is easy to notice that the resolution of the time to next state is one second, which is not adequate for anticipated safety applications. This is a limitation of the EPAC M30 serial interface. The other limitation is the inability to "poll" the data at a faster rate than 200 ms. In the case where one attempts to interface directly to the existing intersection controller with the objective of developing safety applications, special attention and effort will be required to deal with these interface issues.

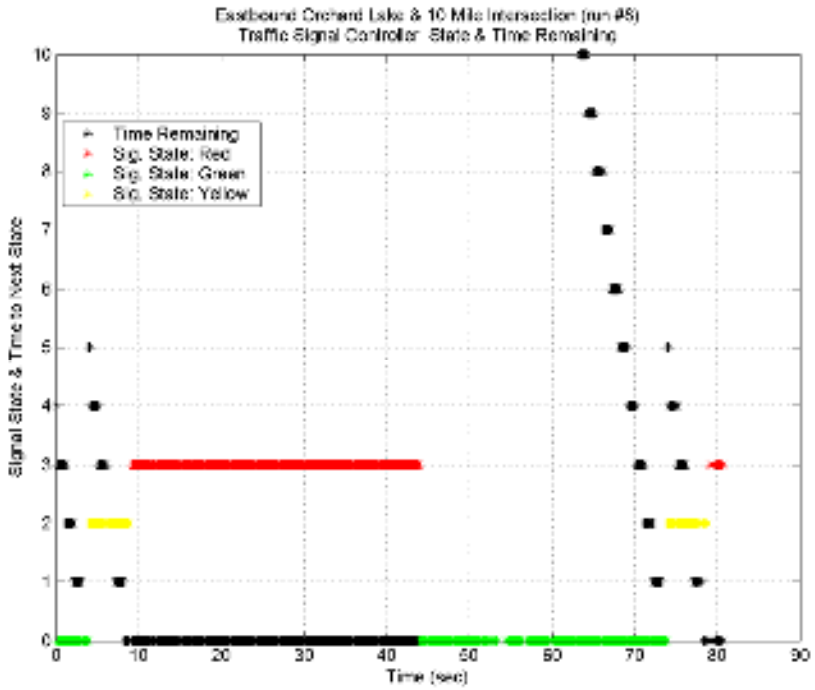


Figure 75. Signal State and Time to Next State as Received by OBU

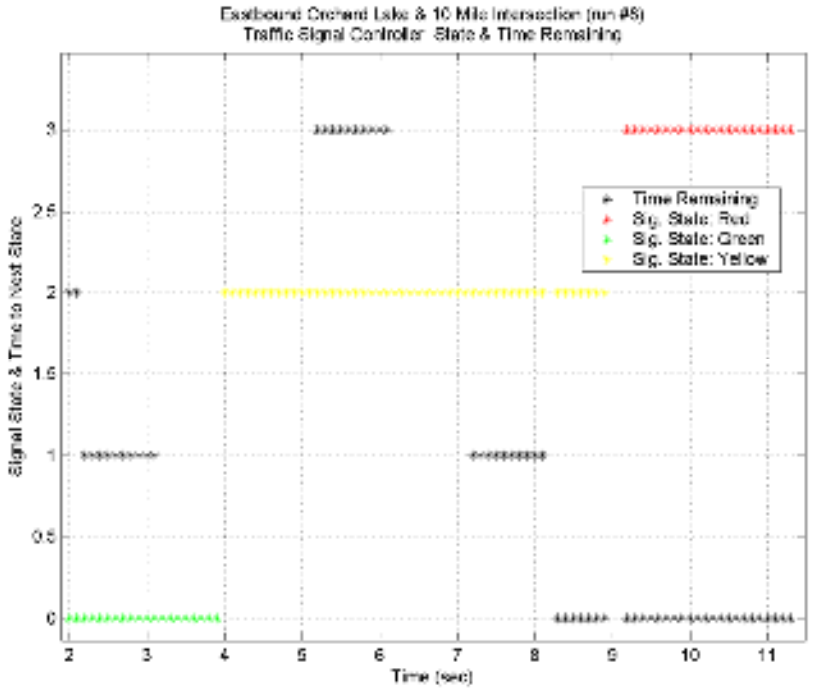


Figure 76. One-Second Quantization of Time to Next State as Received by OBU

Figure 77. Orchard Lake & 10 Mile Rd intersection. Current Signal State as Received by the OBU From the RSU

Finally, the signal state was overlaid on top of the aerial photograph of the intersection in Figure 77 to give the reader a better view of "what was received" and "when it was received" from the RSU as the OBU drives through the intersection.

3.3 Reduced Power Transmit Testing and 5.9 GHz DSRC Intersection Characterization

The next set of tests was performed at reduced transmission power levels of 12, 6 and 3 dBm. The tests were intended to explore the potential of limiting the maximum range of communication in a real-world intersection setting via power control.

3.3.1 Test Results at 12 dBm Transmit Power Setting

The following table summarizes the configuration of the RSU-WRM.

Packet Length (bytes)	*Message Interval (ms)*	*Data Rate (Mbps)*	*Transmit Power (dBm)*
500	*100*	*6*	*12 dBm*

Table 11. WRM configuration for RSU message (12dBm)

Figure 78 summarizes the data collected at the 12 dBm power level setting for an eastbound run. Compared to the results under full power setting in Figure 60, the maximum range of communication dropped approximately from 500 m to 350 m.

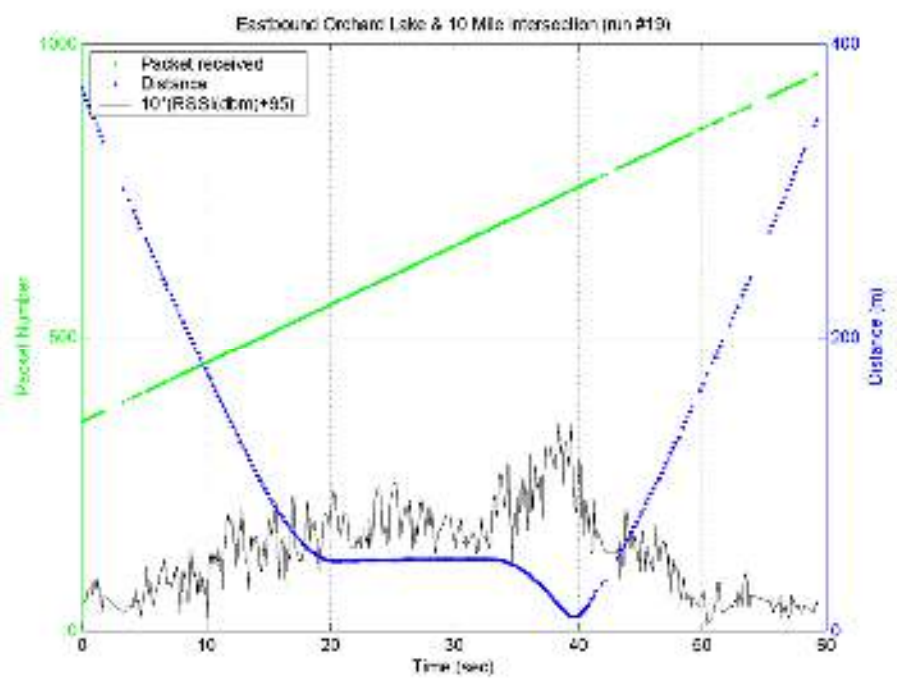


Figure 78. Eastbound 10 Mile Rd. Packets Received, Range, and RSSI @ 12 dBm

Figure 79 summarizes the data collected at the 12 dBm power level setting for a westbound run. Again, the maximum range of communication dropped from 550 m (full power setting), see Figure 61, to approximately 375 m. Note the sharp RSSI drop at 30 seconds in the time line as a truck blocked the direct line of sight between the OBU and the RSU for a full 30-second period. Both the truck and the OBU vehicle were stopped at a red light. No packets were lost during that obstruction.

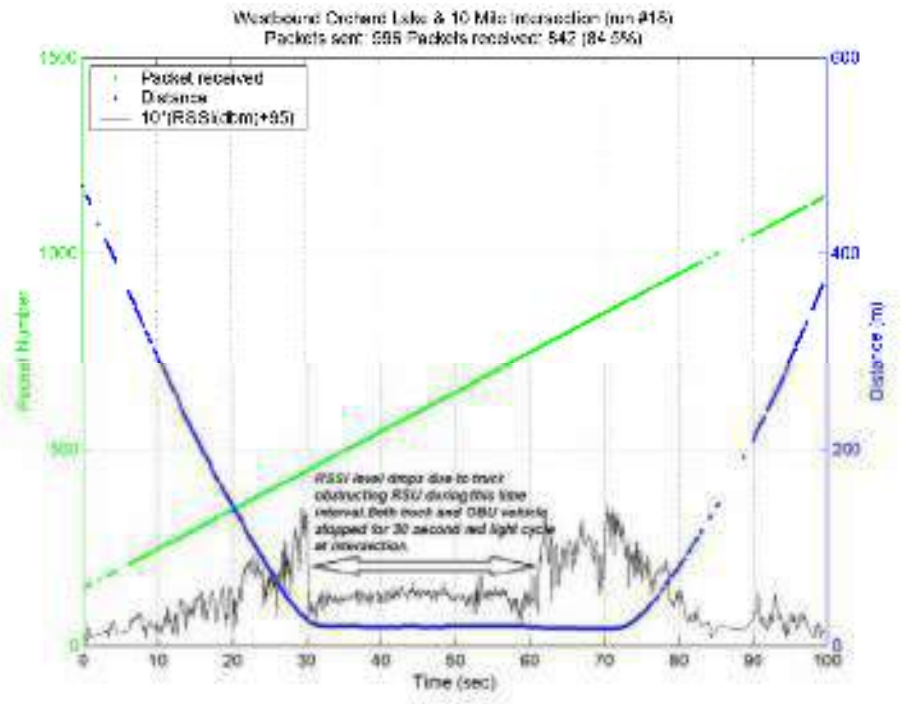


Figure 79. Westbound 10 Mile Rd. Packets Received, Range, and RSSI @ 12 dBm

Figure 80. RSU to the Left of Truck Being Obstructed From OBU

3.3.2 Test Results at 6 dBm Transmit Power Setting

The following table summarizes the configuration of the RSU-WRM.

Packet Length (bytes)	*Message Interval (ms)*	*Data Rate (Mbps)*	*Transmit Power (dBm)*
500	*100*	*6*	*6 dBm*

Table 12. WRM Configuration for RSU Message (6 dBm)

Figure 81 summarizes the data collected at the 6 dBm power level setting for a westbound run. Compared to the results under full power setting, the maximum range of communication dropped approximately from 550 m to 300 m with a substantial amount of lost packets above 150 m.

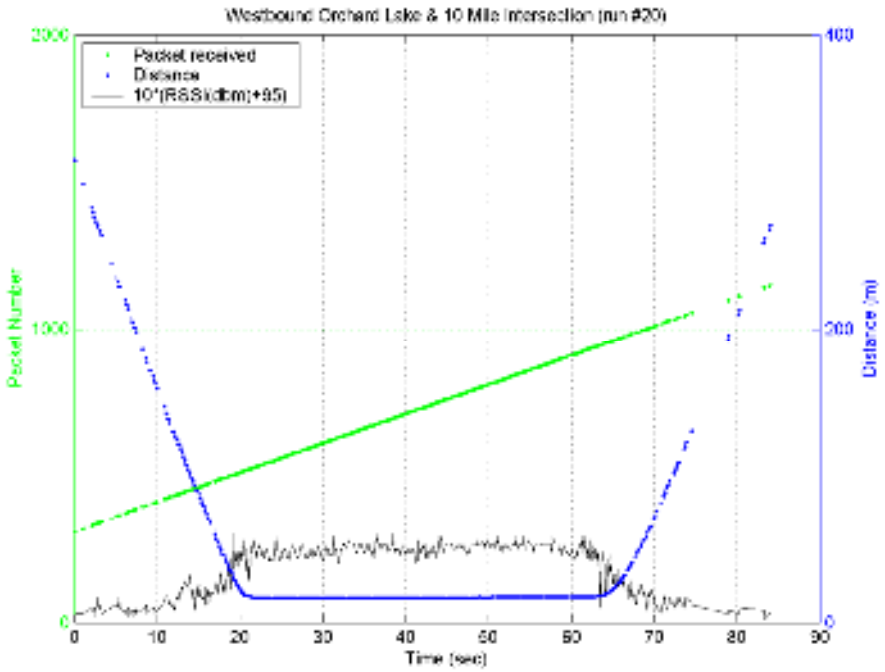


Figure 81. Westbound 10 Mile Rd. Packets Received, Range, and RSSI @ 6 dBm

Figure 82 shows the maximum range of communication around 150 m for the eastbound run.

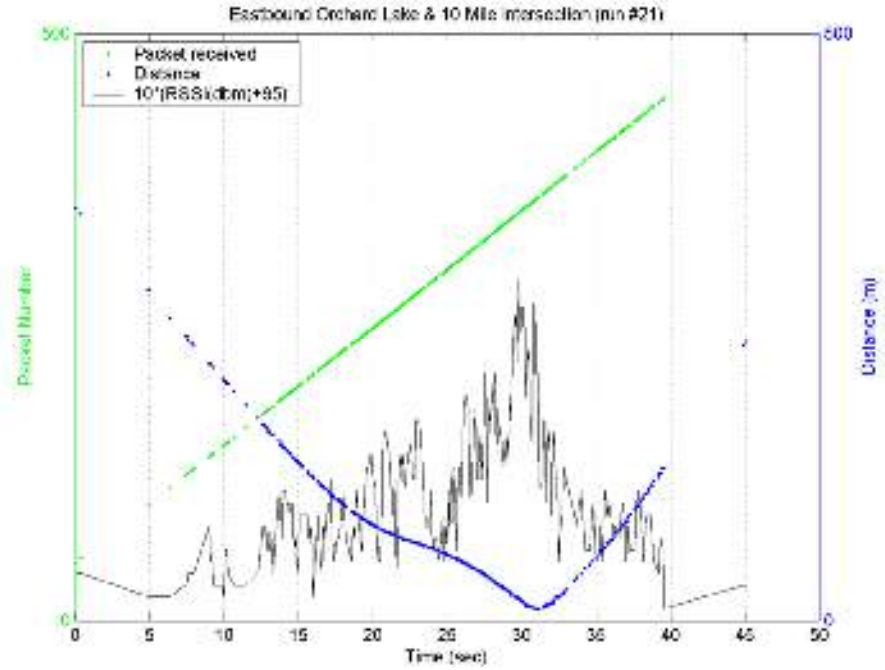


Figure 82. Eastbound 10 Mile Rd. Packets Received, Range, and RSSI @ 6 dBm

3.3.3 Test Results at 3 dBm Transmit Power Setting

The following table summarizes the configuration of the RSU-WRM:

Packet Length (bytes)	Message Interval (ms)	Data Rate (Mbps)	Transmit Power (dBm)
500	100	6	3 dBm

Table 13. WRM Configuration for RSU Message (3 dBm)

Figures 83 and 84 show a similar maximum range of communication for both the 3 dBm and the 6 dBm power settings.

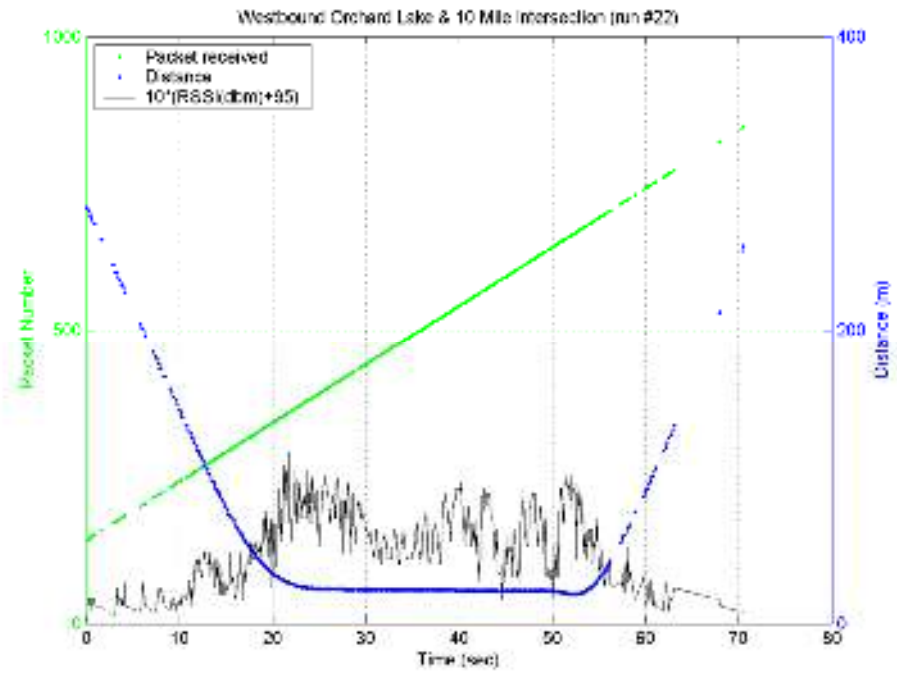


Figure 83. Westbound 10 Mile Rd. Packets Received, Range, and RSSI @ 3dBm

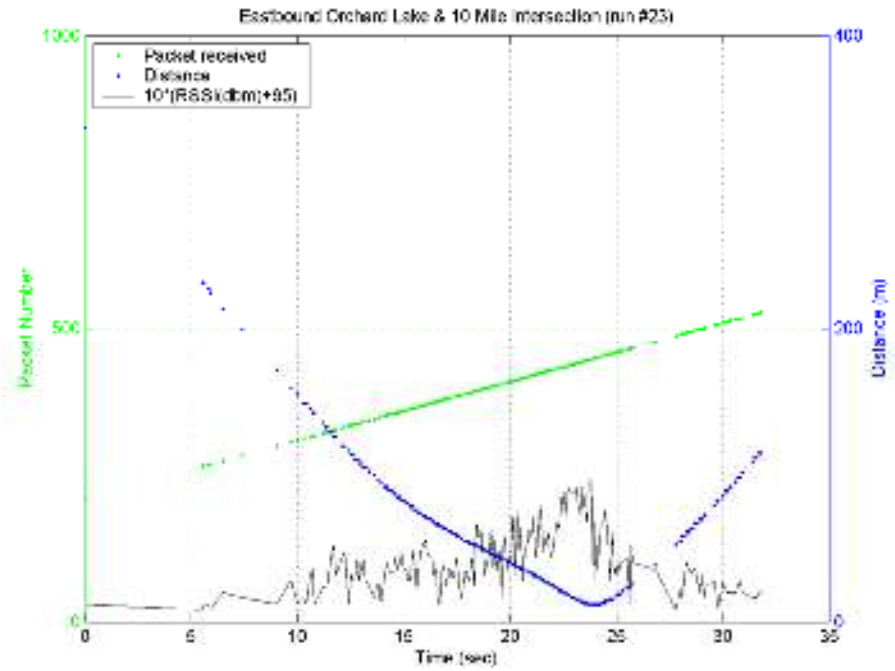


Figure 84. Eastbound 10 Mile Rd. Packets Received, Range, and RSSI @ 3 dBm

Figure 85 conveys the notion that some form of range control can be achieved at a real intersection with the proper selection of transmission power. The points on the graph are composites drawn from all of the data sets.

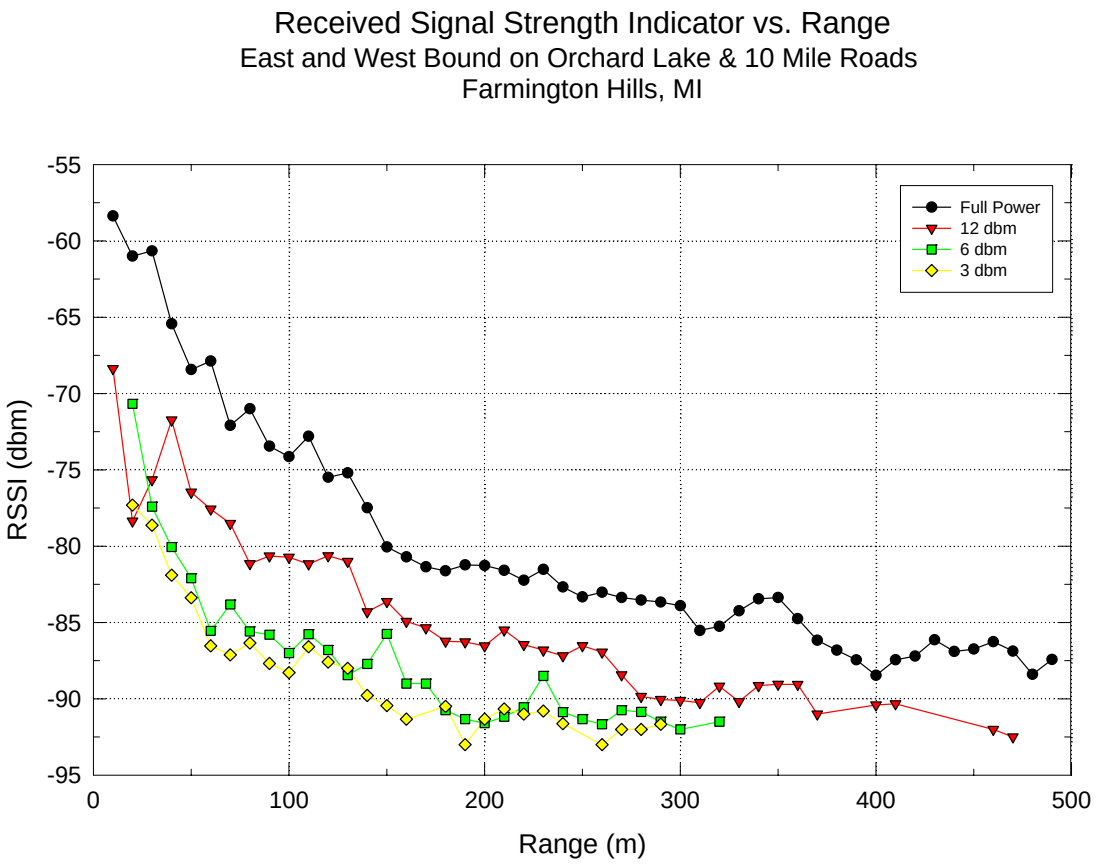


Figure 85. RSSI versus Range at Various Power Settings

3.4 Vehicle-Vehicle and Vehicle-Infrastructure Testing and Results

The final set of tests was aimed at collecting data to analyze whether communications between two OBU vehicles, traveling on perpendicular legs of the intersection, can be established before one of the OBUs enters the intersection. If so, how far away from the intersection RSU is that v2v communication initiated? It is generally assumed that in an urban intersection with high building densities, this type of v2v communication would not be possible. But since this intersection had a relatively low building density it was decided to explore this type of scenario. The transmission power on all WRMS was reconfigured to full setting (~20 dBm).

The results are illustrated in Figure 86. In this scenario a GM-OBU vehicle traveled eastbound while a Ford-OBU traveled southbound towards the RSU. The RSU was transmitting its RSU message while receiving both OBUs common vehicle message set. Both OBUs interfaced with their respective vehicle CAN buses to send out actual vehicle sensor messages such as speed, accelerations, and yaw rate.

The tracks on the figure below in the eastbound direction depict the range of the GM-OBU to the Ford-OBU as a calculated value after a successful reception of each other's messages. The range is colorized so that it is easy to determine where the vehicles were relative to each other when they successfully exchanged messages.

For example, the GM vehicle started receiving the Ford-OBU message about 100 m from the intersection (purple/blue dots), while the Ford-OBU received the GM-OBU message at about 200 m from the intersection (matching blue/purple dots). It is worth noting that because of the building on the northwest corner of the intersection no visual line of sight was available to the drivers as they approached the intersection. Examining Figure 87, where the scenario consisted of the Ford-OBU traveling northbound while the GM-OBU was traveling westbound, similar observations can be made.

Figure 88 shows that in this case, the v2v communication was established when the Ford vehicle was at ~70 m from the RSU while the GM vehicle was at ~160 m east of the RSU. Again in this case, the v2v communication was established before the actual visual line of sight between the drivers because of a building on the southeast corner of the intersection.

The data also showed that RSU message reception by both vehicles could be qualified as typical in the sense defined earlier at full power settings (beyond 500 m and above 90% within 250 m of the RSU).

Figure 86. One RSU and Two OBUs Crossing Paths Testing. GM-OBU Traveling Eastbound, Ford-OBU Traveling Southbound.

Figure 87. One RSU and Two OBUs Crossing Paths Testing. GM-OBU Traveling Westbound, Ford-OBU Traveling Northbound.

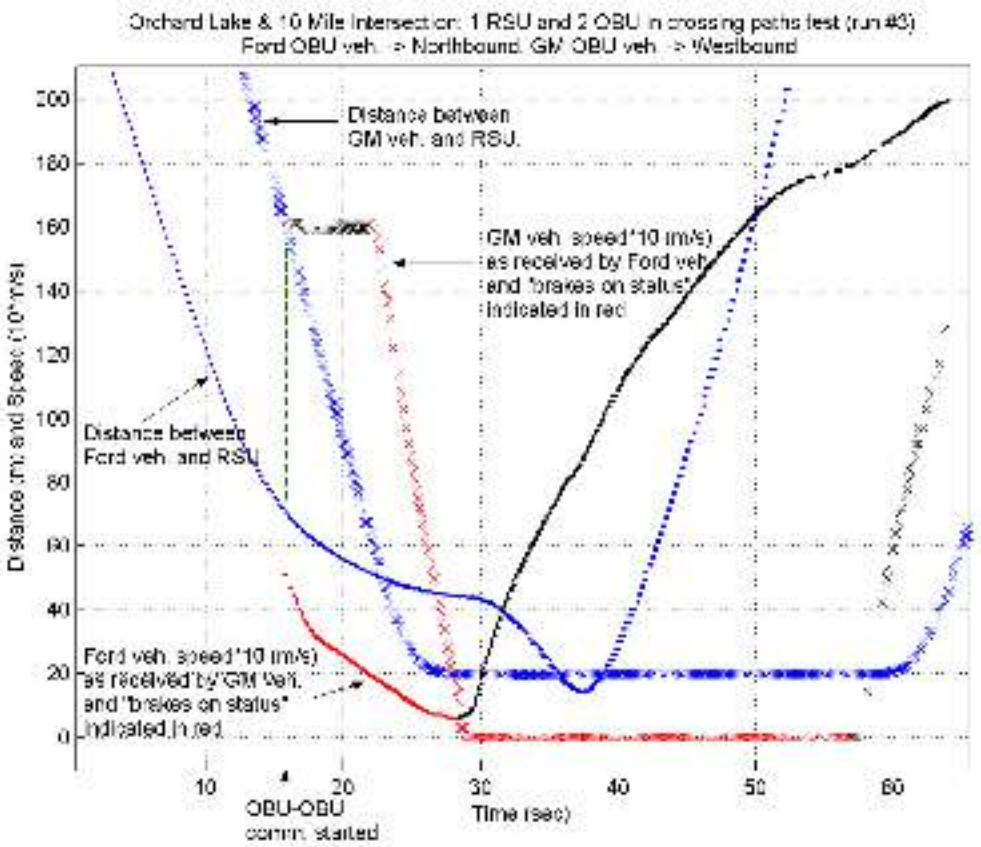


Figure 88. Range from RSU, Vehicle Speed and Braking Information as Received by GM-OBU and Ford-OBU While Traveling on Intersection Crossing Paths

3.5 Summary

In light of the testing performed at Orchard Lake and 10 Mile Road, the following conclusions can be drawn:

- The EPAC M30 traffic signal controller was successfully synchronized with the installed controller at the intersection.

- Even though the traffic controller (signal state & time remaining) was properly received by the OBU, the resolution of the time remaining (1 second) was not adequate. Interfacing to a traffic controller proved to be more challenging than expected and the final output was not adequate for anticipated safety applications. In the case of a fixed timing cycle, where there is no adaptation based on sensor feedback of vehicles in the intersection, a more precise timing could be generated, on the OBU side as part of the safety application, by initializing a timer as soon as a transition between signal states is received as part of the RSU message. However, to satisfy the 100 millisecond safety applications update rate requirement for the RSU message (instead of the 200 millisecond

achieved with the EPAC M30), the signal controller software and serial protocol would require more elaborate modifications.

- Wireless communication at 5.9 GHz at this intersection was overall characterized with a ~93% successful transmission ratio over the range of interest of 250 m.

- This performance was achieved under a sub-optimal RSU antenna setting (intersection corner, 10 ft above the ground) and with an inverted OBU roof-mount antenna, clearly not optimized for RSU conditions.

- For a safety application such as traffic signal violation warning, no major issues were uncovered as far as fulfilling the basic requirements from Task 3. No GPS outages were noticed since there are no overhead obstructions.

- Most of the outages were of the “minimal” kind, i.e. one packet loss at a time, which should be a containable type of outage.

- Some of the longer outages were merely due to obstruction (road signs, hill) and should be minimized with better (optimal) RSU antenna placement.

- Some level of maximum transmission range control can be achieved at a real-world intersection with the proper selection of transmission power.

- Finally, the limited set of tests performed for this RSU and two OBUS on crossing paths scenario and the results derived from it shows that in this intersection, communication between the two OBUs was achieved, even before visual line of sight between the drivers. It suggests that perhaps the idea of having to relay OBU messages by RSU may not necessarily be needed at some intersections. Further studies and tests are needed for this specific scenario.

4 VEHICLE-TO-VEHICLE COMMUNICATIONS RESULTS USING THE WAVE RADIO MODULES

Task 6D of the VSC project developed the WAVE Radio Modules (WRMs) that were largely compliant with the ASTM 5.9 GHz DSRC/WAVE lower layer standards specifications. Task 9 of the VSC project developed the software application that allows the user to send and receive messages using the WRMs. This application runs on a Windows Laptop and communicates with the WRM via an ethernet interface. The application has a serial interface to the DGPS Max receiver, a CAN interface to vehicle sensor data, and a serial interface to the traffic signal controller. The WRMs and the Task 9 application were developed under a subcontract with DENSO LA Labs.

Several tests were conducted to evaluate the performance of the WRMs under vehicle-to-vehicle communications scenarios. This section describes the results of the vehicle-to-vehicle communications testing conducted at the Milford Proving grounds, I-96 freeway, and the M-5 ramp to Twelve Mile Road in Michigan.

4.1 Vehicle-to-Vehicle Communications Performance at Milford Proving Grounds

The vehicle-to-vehicle communications testing was conducted using a Jaguar XKR developed by Ford for the EDMap project, and a Buick Lesabre developed by GM for the ACAS project. Software modifications were carried out on both these vehicles so that they provide the vehicle signals over the CAN interface as defined in the Task 9 application. The vehicle position information was obtained from the DGPS Max receiver that was configured to obtain differential corrections from the U.S. Coast Guard beacons. One roof mount DSRC antenna (developed under the VSC Task 6C project) was used on each of the vehicles.

The legend for the vehicles used in the testing is shown in Figure 89. An illustration of the test track used at the Milford Proving Grounds (MPG) for the testing is shown in Figure 90. In all tests the WRMs were configured to send and receive on the DSRC Control Channel, which is Channel 178 with a center frequency of 5890 MHz and a 10 MHz bandwidth.

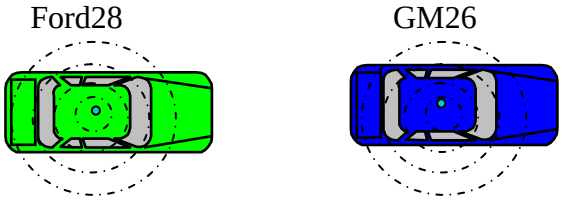


Figure 89. Legend for Vehicles

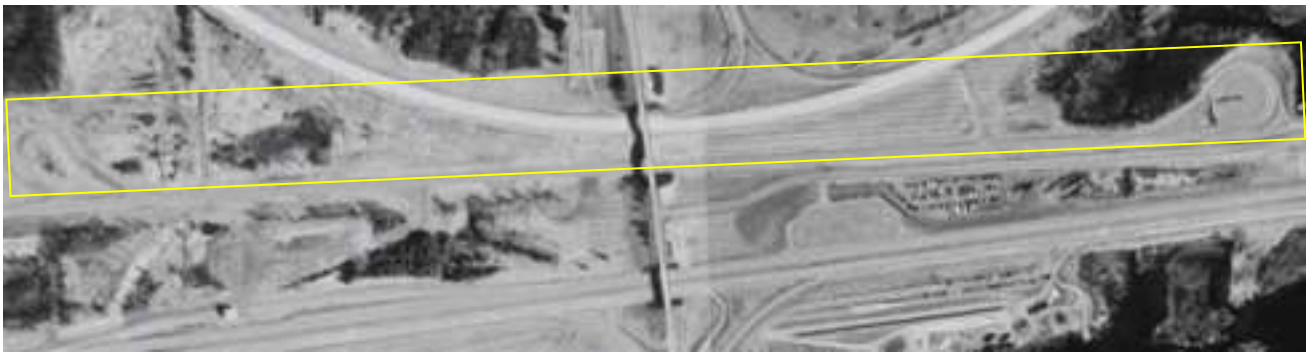


Figure 90. Test Track at MPG

4.1.1 Test for Omni-directional Coverage & Vehicle Signals

This test scenario is shown in Figure 91. The parameters for this test are shown in Table 14.

Packet Length (bytes)	*Message Interval (ms)*	*Data Rate (Mbps)*	*Transmit Power (dBm)*	*Desired Vehicle Speed (mph)*
200	*100*	*6*	*Full (~20 dBm)*	*20*

Table 14. Parameters for Test Scenario No. 4.1.1

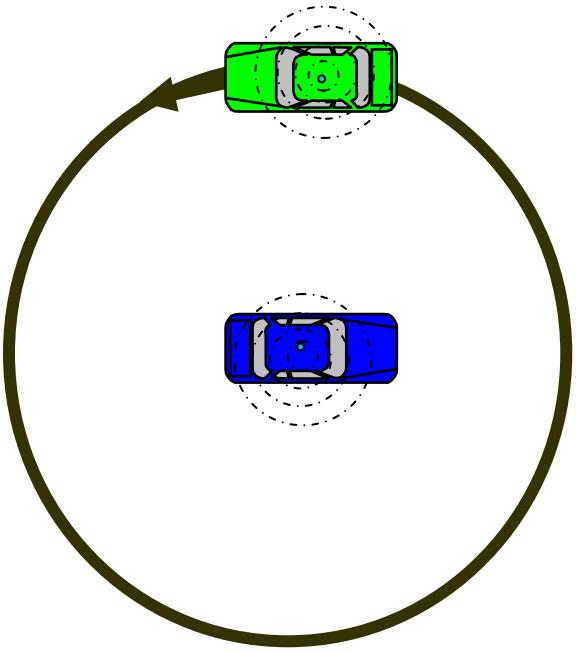


Figure 91. Test Scenario No. 4.1.1

In this test scenario, GM26 is stationary while Ford28 moves in the counter clockwise direction in a constant circular track around GM26. The WRMs on both vehicles were configured to both send and receive data. The results of this test scenario are shown in Figures 92 through 97. The distance between the vehicles was calculated from GPS data received by GM26. The distances are color-coded based on the received signal strength indicator (RSSI) values for the packets received by GM26.

Since both vehicles have been developed to provide vehicle signal data over the CAN interface to the Task 9 application, the communicated packets include actual vehicle signal data. Figure 93 shows the speed of Ford28, color-coded based on the brake status of Ford28, based on data received by GM26. Figure 94, Figure 95, and Figure 96 show the yaw-rate, longitudinal acceleration and lateral acceleration respectively of Ford28 based on data received by GM26.

The data from Figure 97 taken from a 90 second run showed that the number of packets from Ford28 received by GM26 is equal the number of packets sent by Ford28. Thus, this test scenario showed 100 percent reception and no packet loss. This demonstrated true omni-directional characteristics of the 5.9 GHz DSRC roof-mount antenna developed under Task 6 of the VSC project.

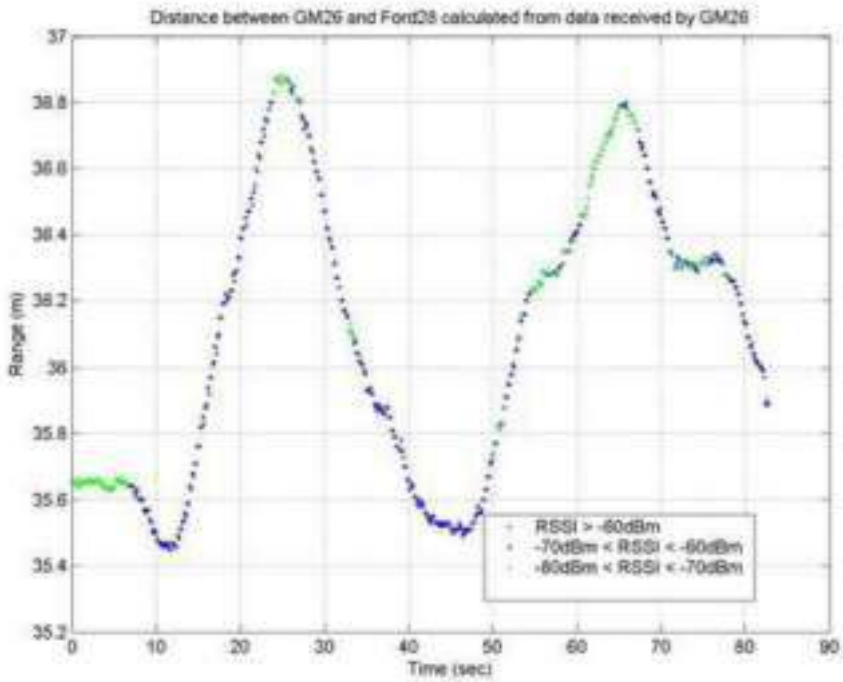


Figure 92. Distance and RSSI Calculated from Data Received by GM26

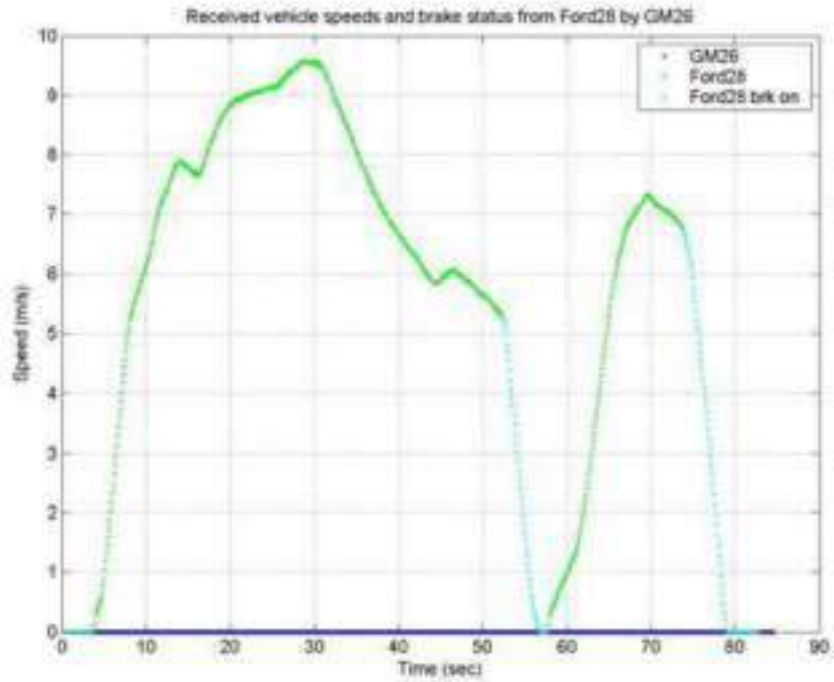


Figure 93. Speed and Brake Status of Ford28 Received by GM26

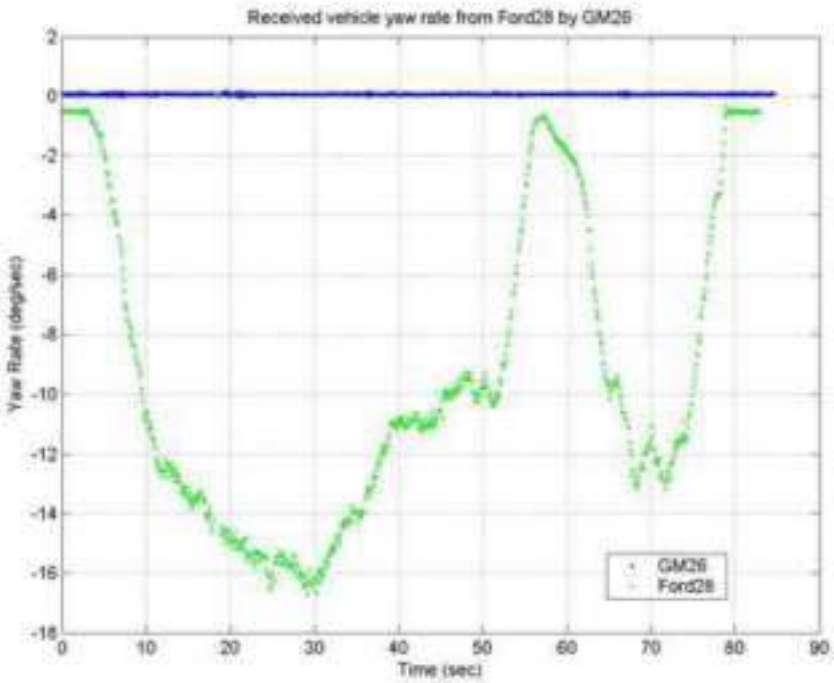


Figure 94. Yaw Rate of Ford28 Received by GM26

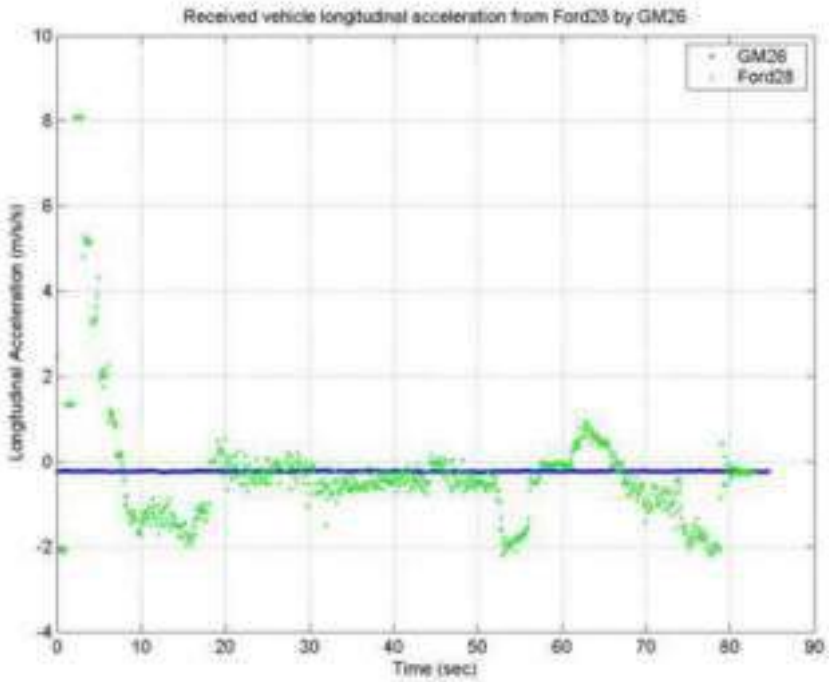


Figure 95. Longitudinal Acceleration of Ford28 Received by GM26

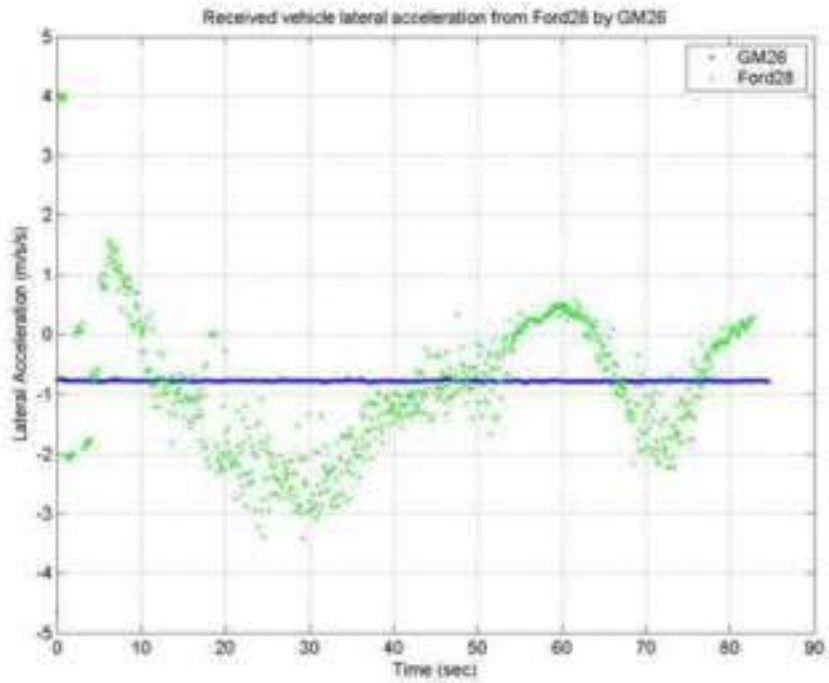


Figure 96. Lateral Acceleration of Ford28 Received by GM26

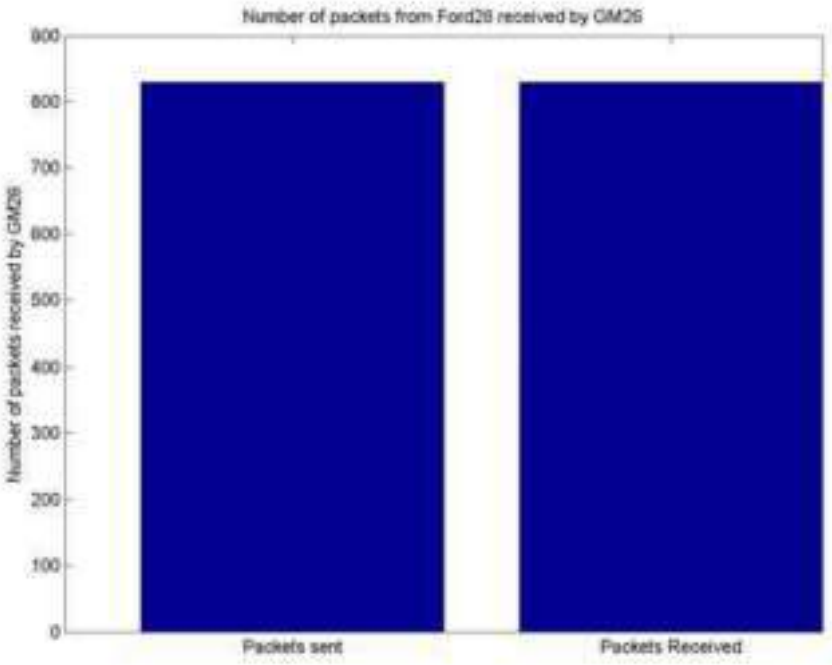


Figure 97. Number of Packets from Ford28 Received by GM26

4.1.2 Lead Vehicle Brake Test

This test scenario is shown in Figure 98. The parameters for this test are shown in Table 15.

Packet Length (bytes)	*Message Interval (ms)*	*Data Rate (Mbps)*	*Transmit Power (dBm)*	*Desired Vehicle Speed (mph)*
200	*100*	*6*	*Full (~20 dBm)*	*45*

Table 15. Parameters for Test Scenario No. 4.1.2

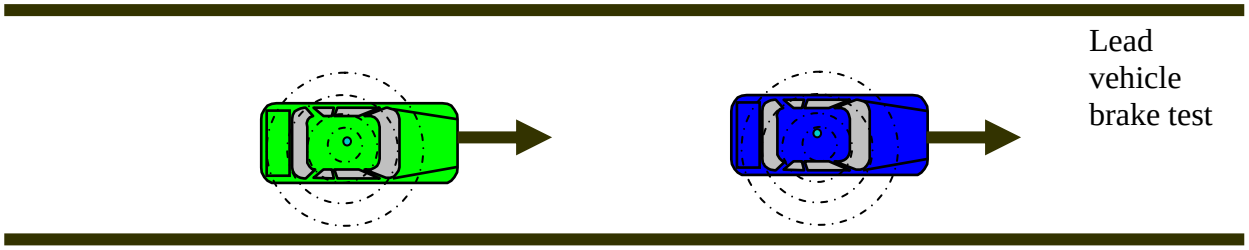


Figure 98. Test Scenario No. 4.1.2

In this test scenario, GM26 is the lead vehicle while Ford28 follows in the same longitudinal direction at about 45 mph. The lead vehicle brakes first and the following vehicle brakes in response to this. The WRMs on both vehicles were configured to both send and receive data. The results of this test scenario are shown in Figure 99 through Figure 102. The distance between the vehicles was calculated from GPS data received by Ford28. The distances are color-coded based on the received signal strength indicator (RSSI) values for the packets received by Ford28. Figures 100 and 101 show the speed and longitudinal acceleration based on data received by Ford28.

The data from Figure 102 taken from a 120 second run shows that the number of packets from GM26 received by Ford28 is equal the number of packets sent by GM26. This test scenario results showed 100 percent reception and no packet loss between the two vehicles up to ranges that exceeded 200 m. Thus, vehicle-to-vehicle communication using 5.9 GHz DSRC may potentially be used to prevent rear-end collisions between vehicles.

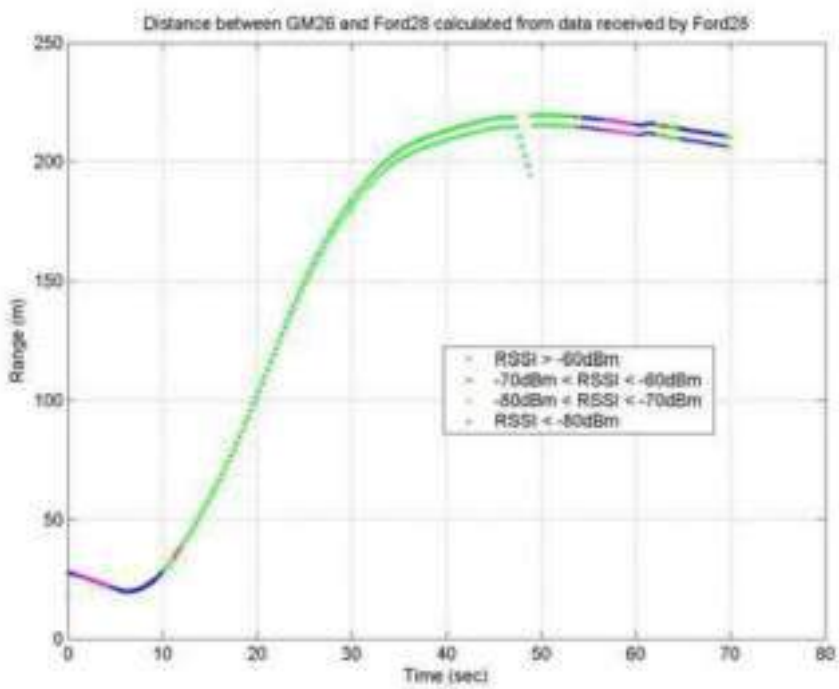


Figure 99. Distance and RSSI Calculated from Data Received by Ford28

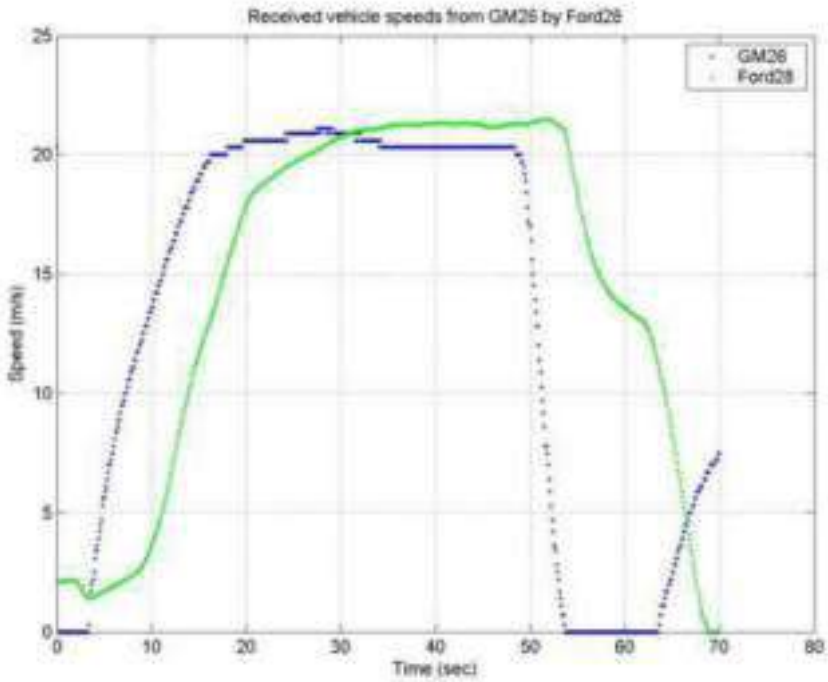


Figure 100. Speed from Data Received by Ford28

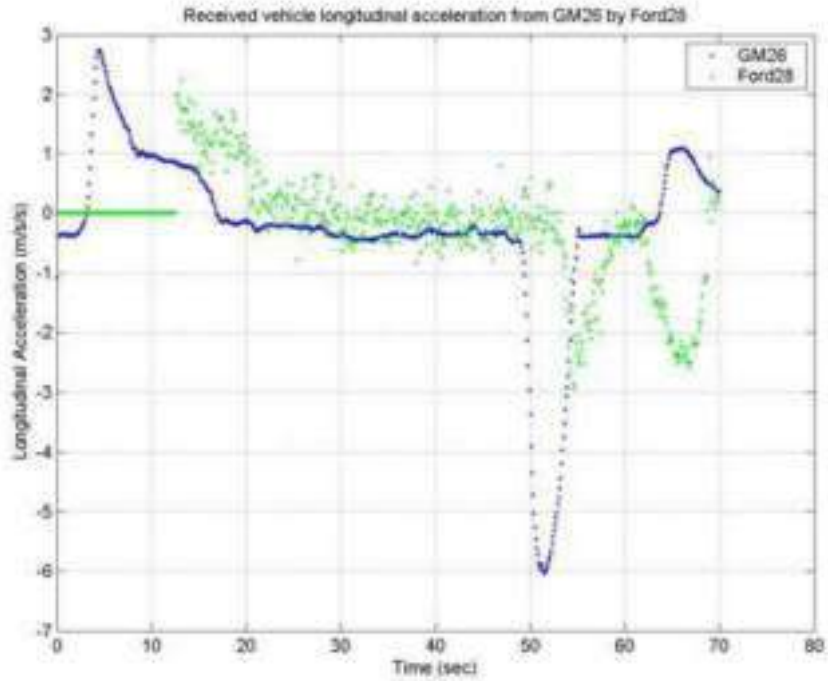


Figure 101. Longitudinal Acceleration from Data Received by Ford28

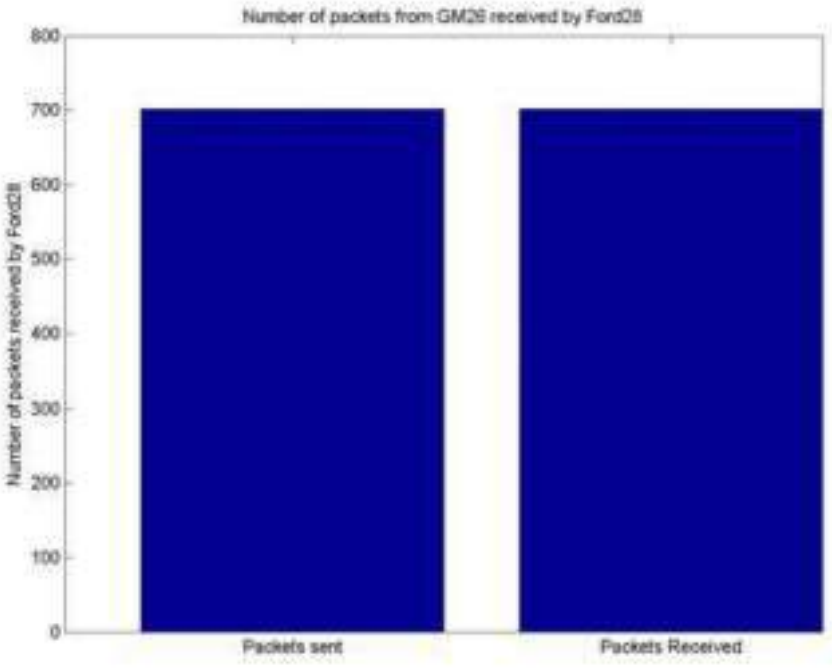


Figure 102. Number of Packets from GM26 Received by Ford28

4.1.3 Test for Maximum Communication Range

This test scenario is shown in Figure 103. The parameters for this test are shown in Table 16.

Packet Length (bytes)	*Message Interval (ms)*	*Data Rate (Mbps)*	*Transmit Power (dBm)*	*Desired Vehicle Speed (mph)*
200	*50*	*6*	*Full (~20 dBm)*	*10*

Table 16. Parameters for Test Scenario No. 4.1.3

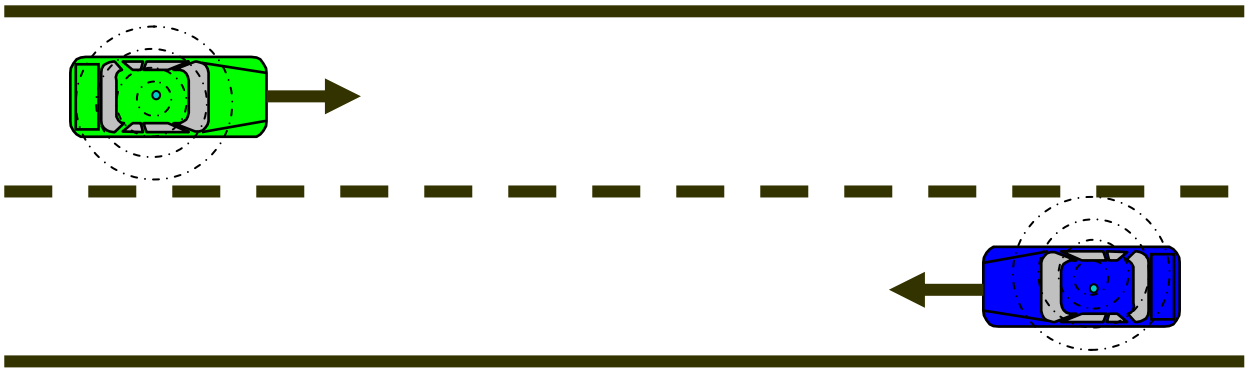


Figure 103. Test Scenario No. 4.1.3

In this test scenario, GM26 and Ford28 travel in opposite directions at about 10 mph thus yielding a relative speed of about 20 mph. This test was used to determine the maximum communication ranges and to determine if there are null zones for vehicle-to-vehicle. The WRMs on both vehicles were configured to both send and receive data. The results of this test scenario are shown in Figures 104 and 105. The distance between the vehicles was calculated from GPS data received by Ford28. The distances are color-coded based on the received signal strength indicator (RSSI) values for the packets received by Ford28.

The data from Figure 105 taken over a 100 second run showed that the number of packets from GM26 not received by Ford28 is less than 3 percent and most of the lost packets occur at distances greater than 550 m. The results of this test showed that vehicle-to-vehicle communication between the two vehicles is possible up to ranges that exceed 600 m on both directions of travel.

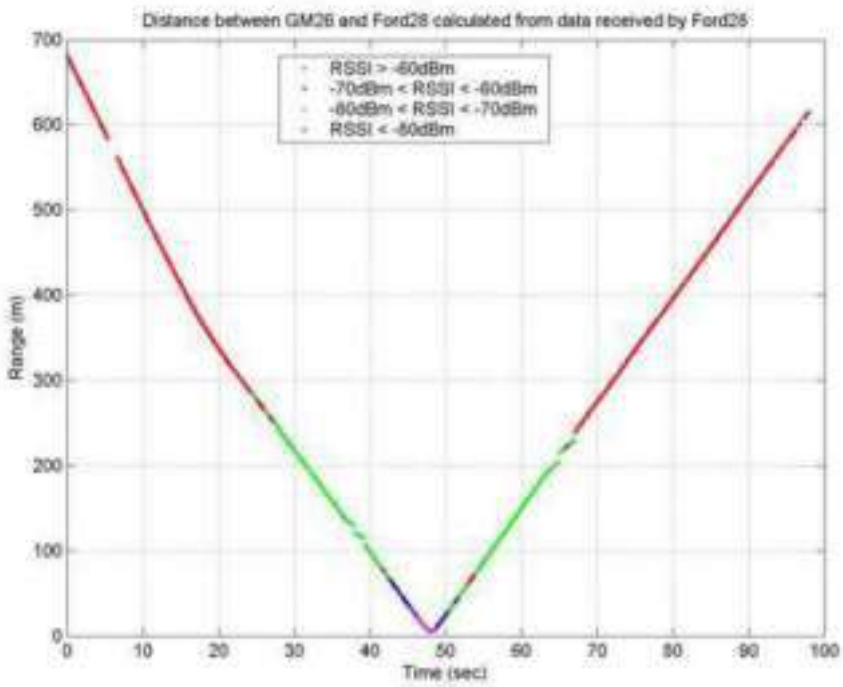


Figure 104. Distance and RSSI Calculated from Data Received by Ford28

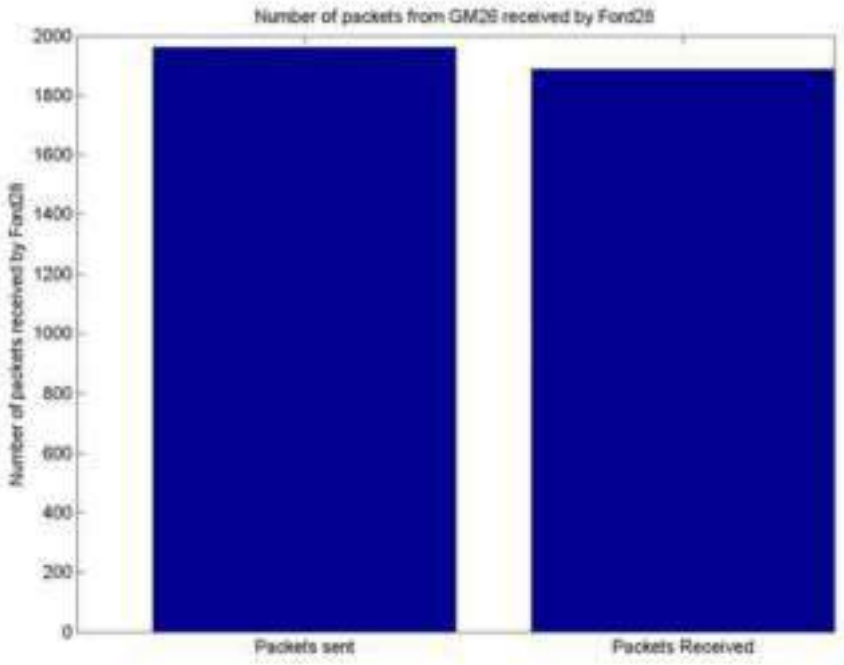


Figure 105. Number of Packets from GM26 Received by Ford28

4.1.4 Test for Communication Performance Under High Relative Speed

This test scenario is the same as shown in Figure 103. The vehicle speeds for this test have been modified to 70 mph thus yielding a relative speed of 140 mph. The other parameters for this test are shown in Table 16.

This test was used to determine if there is degradation in communication performance under high relative speed conditions for vehicle-to-vehicle. The WRMs on both vehicles were configured to both send and receive data. The results of this test scenario are shown in Figures 106 and 107. The distance between the vehicles was calculated from GPS data received by Ford28. The distances are color-coded based on the received signal strength indicator (RSSI) values for the packets received by Ford28.

By comparing the results of Test Scenario 4.1.4 with that of Test Scenario 4.1.3, the data taken over a 25 second run showed that the number of packets from GM26 that were not received by Ford28 is about 2 percent and there has been no noticeable degradation in communication performance due to high relative speed in this scenario. The results of this test showed that communication between the two vehicles is possible up to 600 m on both directions of travel even at relative speeds of about 140 mph.

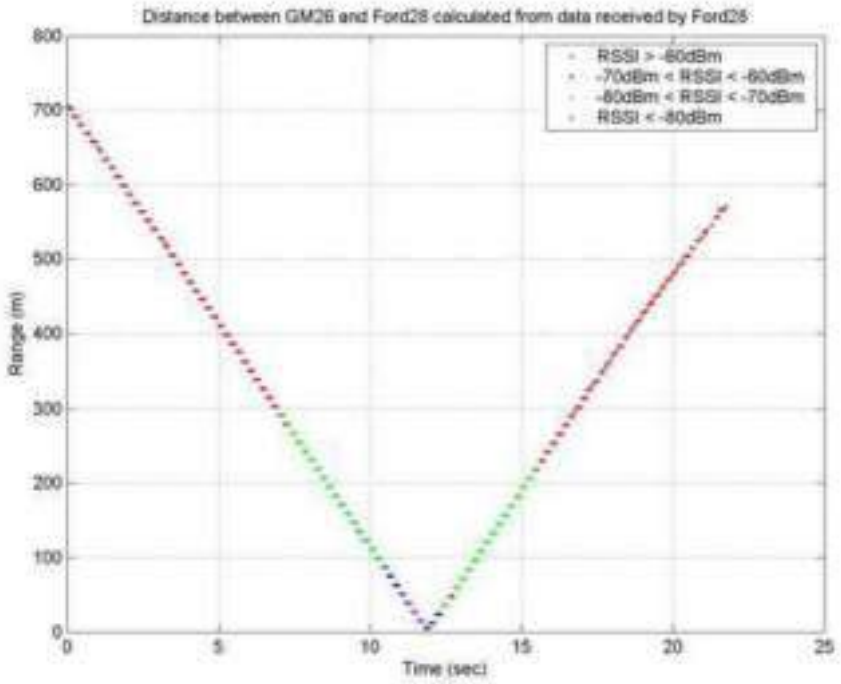


Figure 106. Distance and RSSI Calculated from Data Received by Ford28

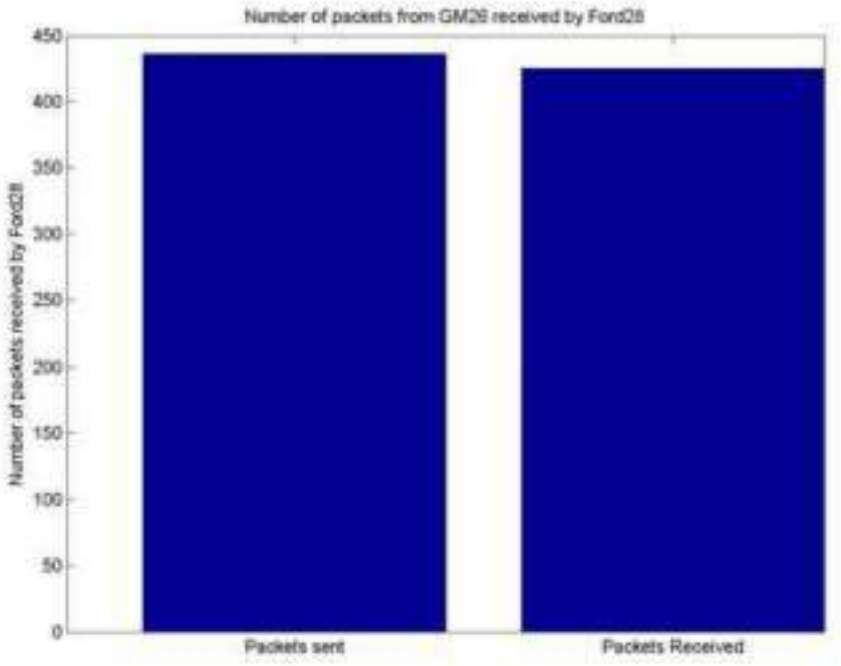


Figure 107. Number of Packets from GM26 Received by Ford28

4.1.5 Test for Communication Range Under Low Transmit Power

This test scenario is the same as in Figure 103. The WRM Transmit Power for this test has been reduced to 5 dBm in comparison to the Test Scenario 4.1.3 in which the Transmit power was set to full (~20 dBm). The other parameters for this test are shown in Table 16.

This test was used to determine the reduction in communication range under low Transmit Power conditions for vehicle-to-vehicle. The WRMs on both vehicles were configured to both send and receive data. The results of this test scenario are shown in Figure 108 and 109. The distance between the vehicles was calculated from GPS data received by Ford28. The distances are color-coded based on the received signal strength indicator (RSSI) values for the packets received by Ford28.

By comparing the results of Test Scenario 4.1.5 with that of Test Scenario 4.1.3, the data taken from a 50 second run showed that the number of packets from GM26 that were not received by Ford28 is greater than 10 percent. The communication range is about 250 m on each direction of travel, which is less that 50 percent of that obtained in Test Scenario 1.1.3 with a Transmit power of about 20 dBm. Nevertheless, the results of this test showed that, even with 5 dBm Transmit Power, vehicle-to-vehicle communication is possible between the two vehicles up to ranges of about 250 m on both directions of travel under test track conditions.

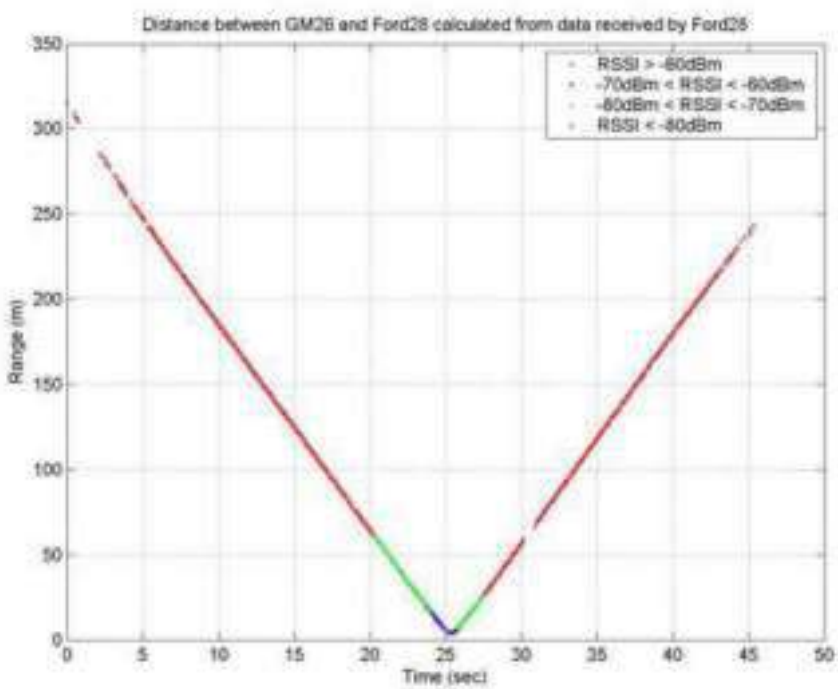


Figure 108. Distance and RSSI Calculated from Data Received by Ford28

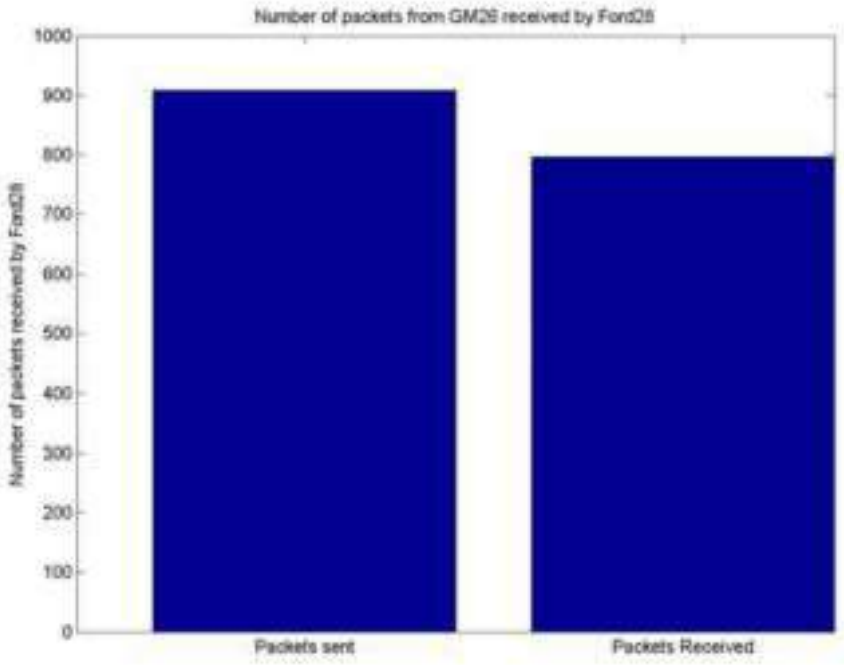


Figure 109. Number of Packets from GM26 Received by Ford28

4.1.6 Test for Communication Performance Under High Data Rate

This test scenario is the same as in Figure 103. The WRM Data Rate for this test has been increased to 27 Mbps in comparison to the Test Scenario 4.1.3 in which the Data Rate was 6 Mbps. The other parameters for this test are shown in Table 16.

This test was used to determine the degradation in communication performance under high Data Rate transmissions for vehicle-to-vehicle. The IEEE stipulates that when the data rate is increased, the transmit power from the 802.11a chipset should be reduced (a 3-4 dBm reduction in these tests) in order to maintain transmitter quality and address the packet error rate. The WRMs on both vehicles were configured to both send and receive data. The results of this test scenario are shown in Figures 110 and 111. The distance between the vehicles was calculated from GPS data received by Ford28. The distances are color-coded based on the received signal strength indicator (RSSI) values for the packets received by Ford28.

By comparing the results of Test Scenario 4.1.6 with that of Test Scenario 4.1.3, the data taken over a 35 second run showed that the number of packets from GM26 that were not received by Ford28 is greater than 15 percent packet loss. The communication range is about 200 m on each direction of travel, which is less than 35 percent of that obtained in Test Scenario 4.1.3 with a Data Rate of 6 Mbps. The results of this test suggests that, in order to have better vehicle-to-vehicle communication between the two vehicles for vehicle safety applications, the minimum DSRC Data Rate of 6 Mbps should be used, since higher Date Rates are associated with higher packet losses and reduction in communication range for the same Transmit Power setting.

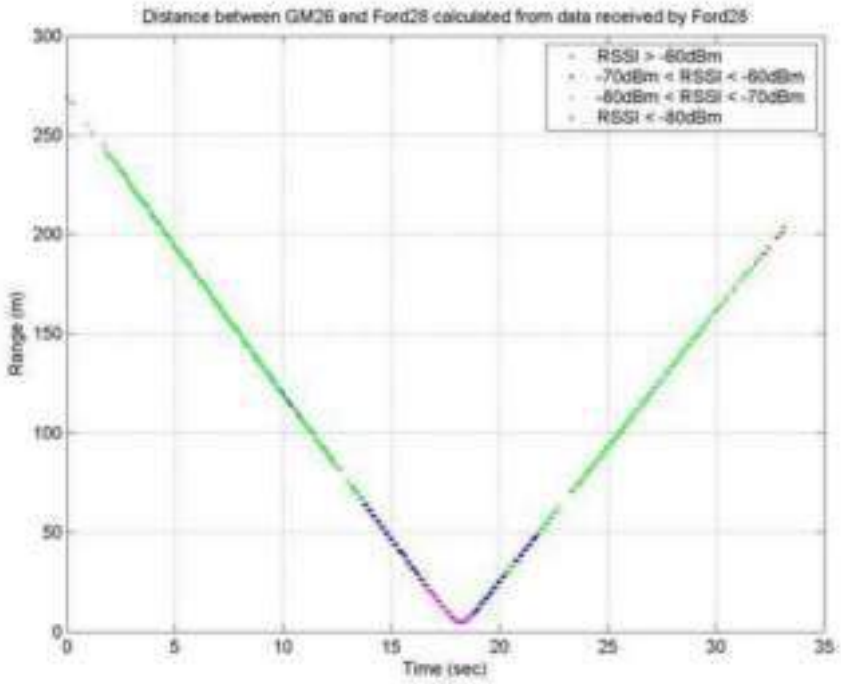


Figure 110. Distance and RSSI Calculated from Data Received by Ford28

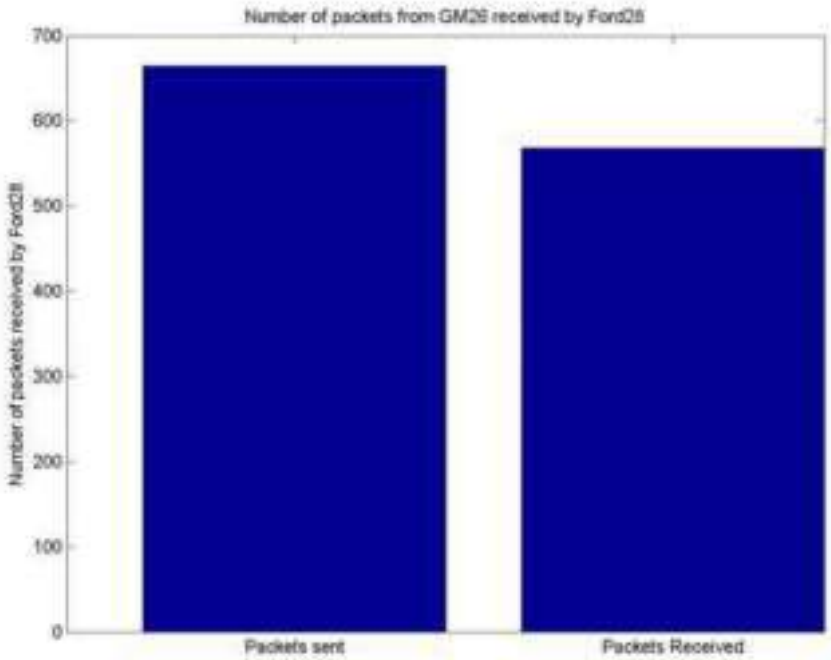


Figure 111. Number of Packets from GM26 Received by Ford28

4.2 Vehicle-to-Vehicle Communications Performance on I-96 Freeway and M-5 Ramp

Vehicle-to-vehicle communications testing was conducted on the I-96 freeway and M-5 ramp in Michigan in order to evaluate the communications performance on freeways. Seven vehicles – GM26, Nissan24, Toyota29, GM23, Ford25, Ford17 and Ford28, formed a caravan as shown in Figure 112. The caravan consisted of 4 sedans, 2 SUVs and a minivan. All seven vehicles were equipped with a DGPS Max receiver and antenna, WRM, and the Task 9 application running on a Laptop. The vehicle position information was obtained from the DGPS Max receiver that was configured to obtain differential corrections from the US Coast Guard beacons. One roof mount DSRC antenna (developed under the VSC Task 6C project) was used on the vehicles.

Three of these vehicles, Ford28 (Jaguar XKR developed by Ford for the EDMap project), GM23 and GM26 (both Buick Lesabres developed by GM for the ACAS project), had software modifications carried out so that they provided the vehicle signals over the CAN interface as defined in the Task 9 application. In all these tests, the WRMs were configured to send and receive on the DSRC Control Channel, which is Channel 178 with a center frequency of 5890 MHz and a 10 MHz bandwidth.

Figure 112. Seven Vehicle Caravan

4.2.1 Test Conducted on I-96 West

This test scenario was conducted on the I-96 west freeway close to CAMP. The parameters for this test are shown in Table 17.

Packet Length (bytes)	*Message Interval (ms)*	*Data Rate (Mbps)*	*Transmit Power (dBm)*
200	*100*	*6*	*Full (~20 dBm)*

Table 17. Parameters for Test Scenario No. 4.2.1

As shown in Figure 112, GM26 is the lead vehicle followed by Nissan24, Toyota29, GM23, Ford25, Ford17 and Ford28 respectively. The caravan was made up of 4 sedans, 2 SUVs and a minivan. The WRMs on all vehicles were configured to both send and receive data. The results for a small segment of this test scenario are shown in Figure 113 through Figure 118. Distances between Ford28 and other vehicles were calculated from V-V communication received by Ford28. The distances are color-coded based on the received signal strength indicator (RSSI) values for the packets received by Ford28.

Since three of the seven vehicles have been developed to provide vehicle signal data over the CAN interface to the Task 9 application, their communication packets include actual vehicle signal data. Figure 114 shows the speeds for a small segment of this test scenario, color-coded based on the brake status, of GM26 and GM23 using data received by Ford28. Figure 115, Figure 116, and Figure 117 show the yaw-rate, longitudinal acceleration and lateral acceleration respectively of GM26 and GM23 for a small segment of this test scenario based on data received by Ford28.

The data from Figure 118 taken over a 300 second segment of this test scenario shows that out of 3000 packets sent by each vehicle, the number of packets received by Ford28 from GM26 is 2126 (71%), the number of packets received by Ford28 from Nissan24 is 2700 (90%), the number of packets received by Ford28 from Toyota29 is 2836 (95%), the number of packets received by Ford28 from GM23 is 2756 (92%), the number of packets received by Ford28 from Ford25 is 2384 (80%), and the number of packets received by Ford28 from Ford17 is 2997 (99.9%). The packet reception from GM26 was low because there were 5 vehicles between GM26 and Ford28, two of which were sedans, 2 were SUVs and one was a minivan. Thus the line of sight may have been obstructed and the distance between them was also large for much of the test duration. The packet reception from Ford25 was low due to the luggage roof rack of the minivan, which was obstructing the antenna pattern from the roof mount antenna used on that vehicle. This shows that the communication characteristics of the 5.9 GHz DSRC roof-mount antenna can be degraded by the luggage roof rack. In general, the results of this test show that, on the freeway environment, we have vehicle-to-vehicle communication between the vehicles to 180 m range with Transmit Power of 20 dBm.

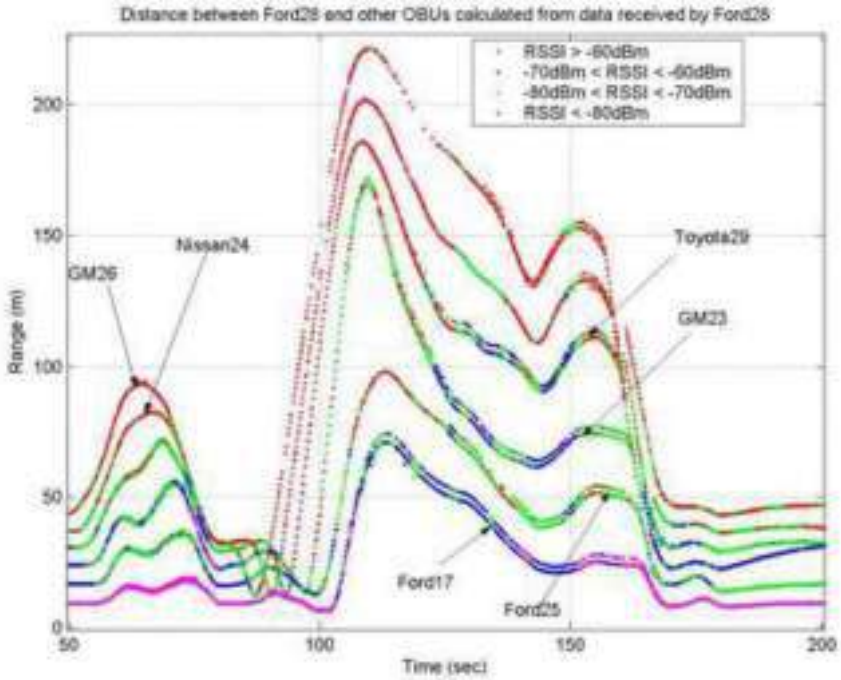


Figure 113. Distances Calculated from Data Received by Ford28

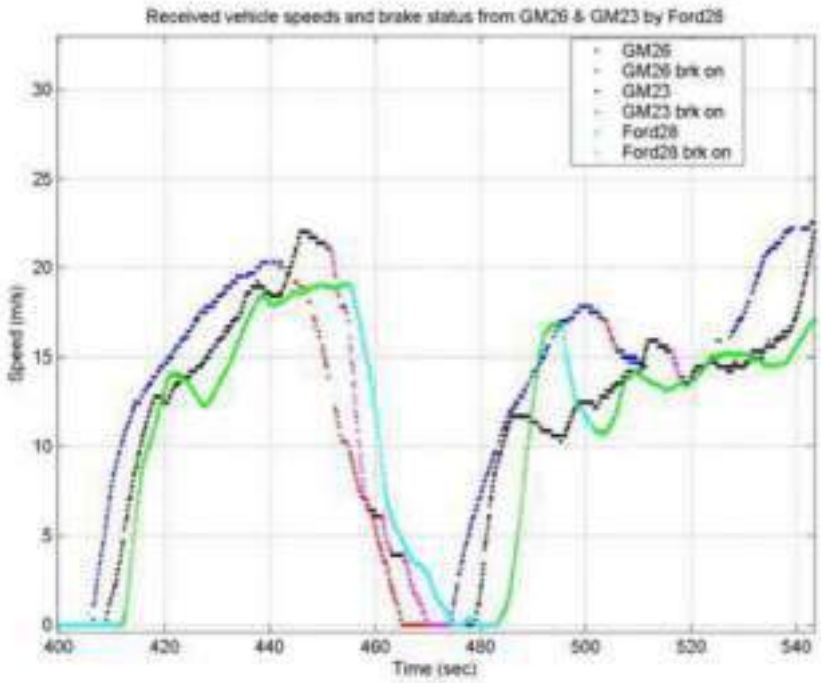


Figure 114. Speed and Brake Status Received by Ford28

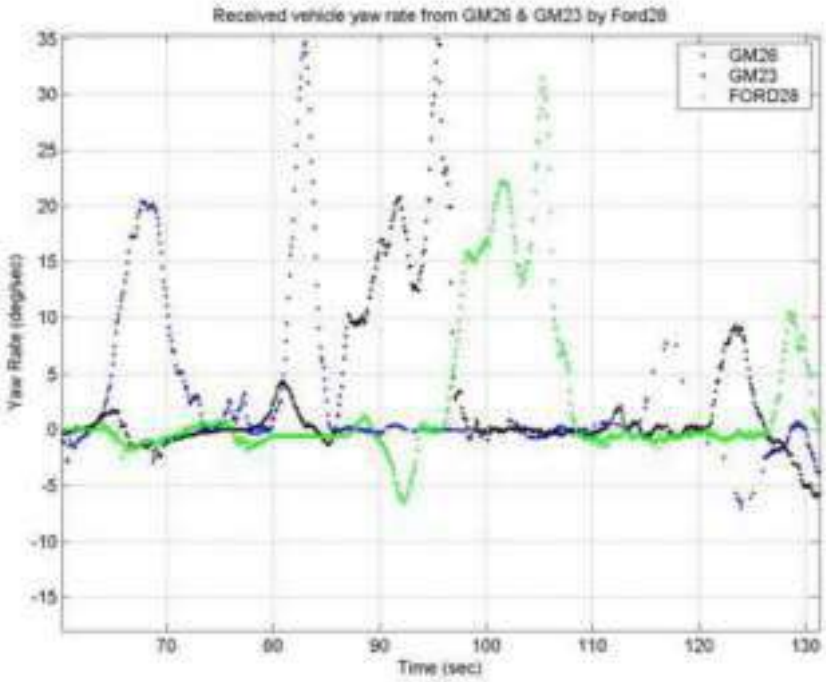


Figure 115. Yaw Rate Received by Ford28

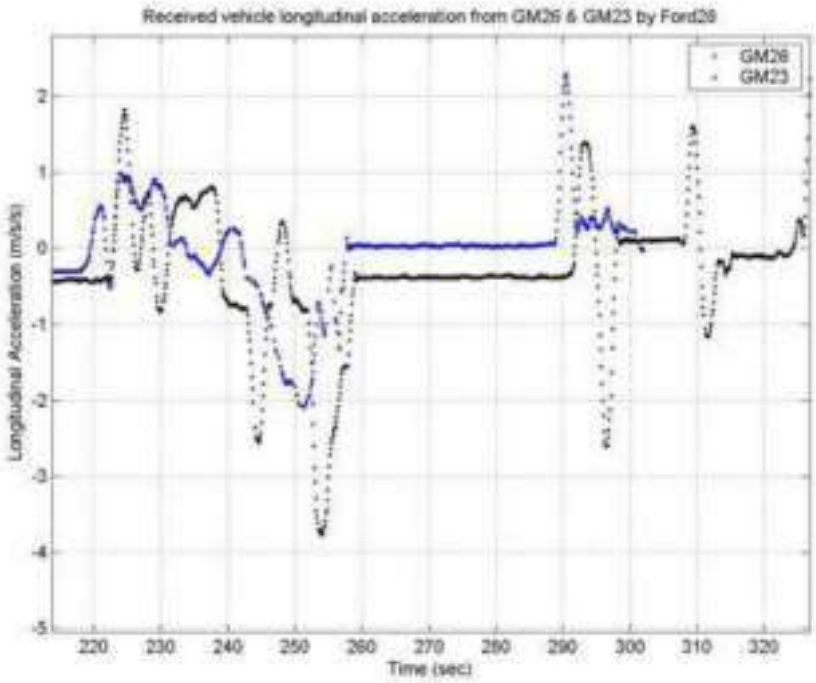


Figure 116. Longitudinal Acceleration Received by Ford28

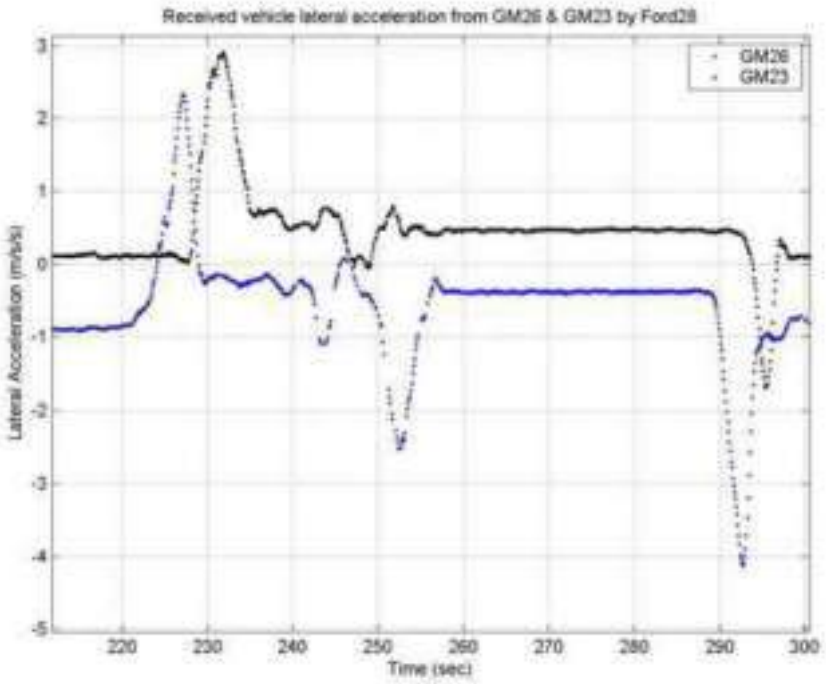


Figure 117. Lateral Acceleration of Received by Ford28

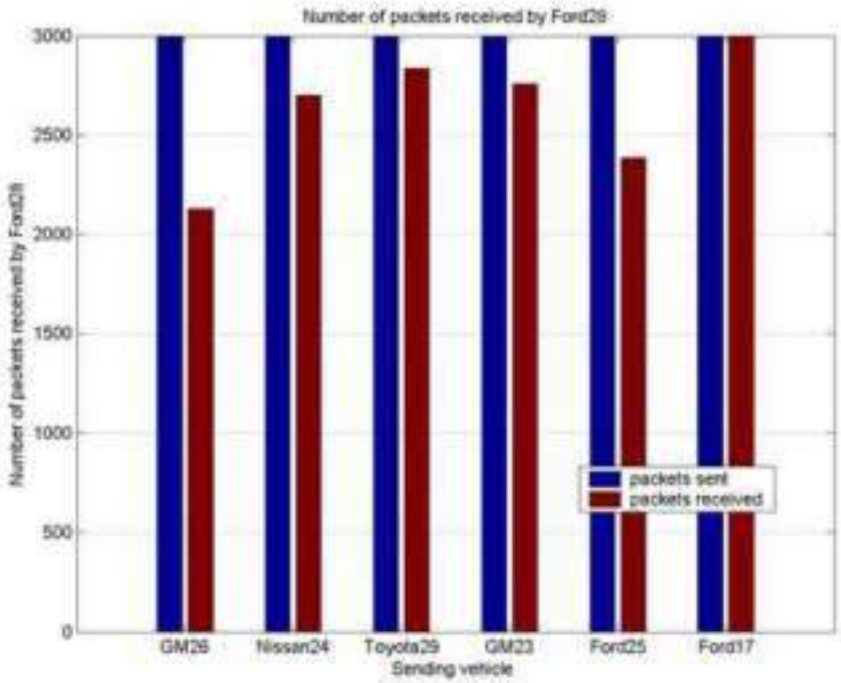


Figure 118. Number of Packets from Other Vehicles Received by Ford28

4.2.2 Test Conducted on I-96 East

This test scenario was conducted on the I-96 east freeway close to Kensington Road in Michigan. The parameters for this test are shown in Table 18. In this test, the Transmit Power was reduced to 16 dBm.

Packet Length (bytes)	*Message Interval (ms)*	*Data Rate (Mbps)*	*Transmit Power (dBm)*
200	*100*	*6*	*16*

Table 18. Parameters for Test No. 4.2.2

As shown in Figure 112, GM26 is the lead vehicle followed by Nissan24, Toyota29, GM23, Ford25, Ford17 and Ford28 respectively. The WRMs on all vehicles were configured to both send and receive data. The results for a small segment of this test scenario are shown in Figure 119 through 124. Distances between Ford28 and other vehicles were calculated from V-V communication received by Ford28. The distances are color-coded based on the received signal strength indicator (RSSI) values for the packets received by Ford28. Figure 120 shows the speeds for a small segment of this test scenario, color-coded based on the brake status, of GM26 and GM23 using data received by Ford28. Figures 121 through 123 show the yaw-rate, longitudinal acceleration and lateral acceleration respectively of GM26 and GM23 for a small segment of this test scenario based on data received by Ford28.

The data from Figure 124 taken over a 600 second segment of this test scenario shows that out of 6000 packets sent by each vehicle, the number of packets received by Ford28 from GM26 is 2957 (49%), the number of packets received by Ford28 from Nissan24 is 4543 (76%), the number of packets received by Ford28 from Toyota29 is 5124 (85%), the number of packets received by Ford28 from GM23 is 5324 (89%), the number of packets received by Ford28 from Ford25 is 4754 (79%), and the number of packets received by Ford28 from Ford17 is 5995 (99.9%). By comparing these results with that of Test Scenario 4.2.1, we find that the packet reception from GM26 is much lower in this test because the Transmit Power used for this test was reduced to 16 dBm. We also find that the packet reception from Nissan24 and Toyota29 are much lower in this test because of the lower Transmit Power used. Again, the packet reception from Ford25 was low due to the luggage roof rack of the minivan, which was obstructing the antenna pattern from the roof mount antenna used on that vehicle. In general, the results of this test showed that, on the freeway environment, vehicle-to-vehicle communication were possible between the vehicles to 150 m range with reduced Transmit Power of 16 dBm.

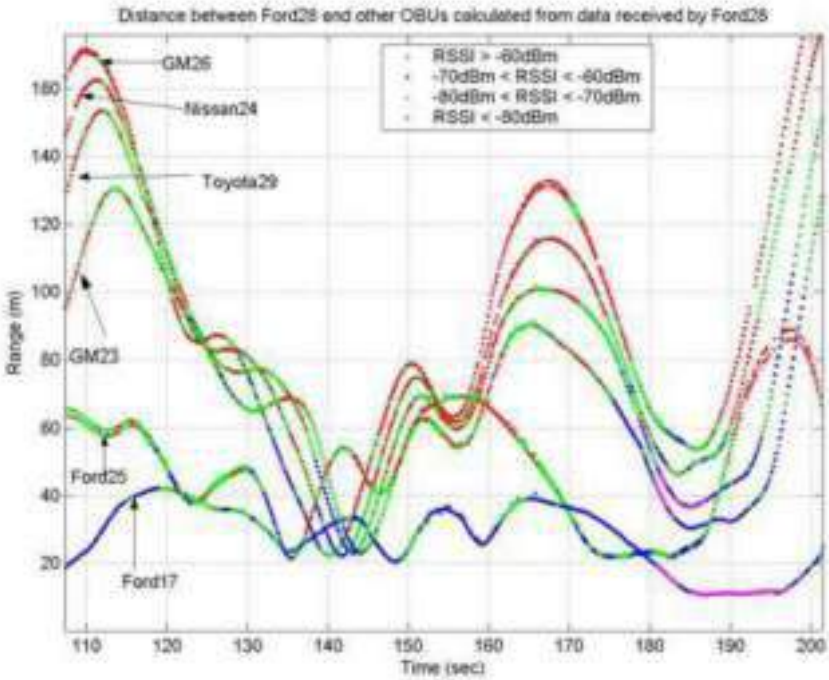


Figure 119. Distances Calculated from Data Received by Ford28

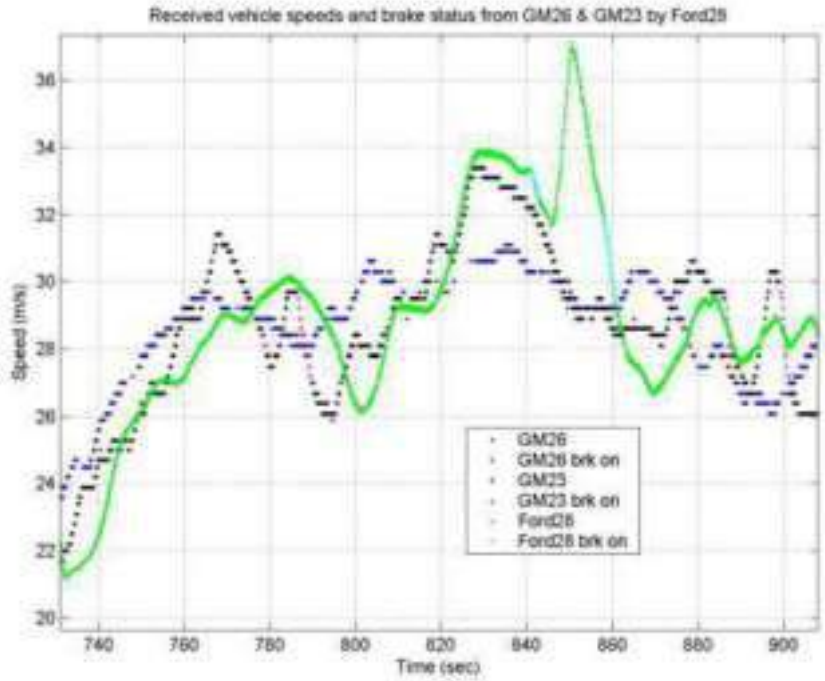


Figure 120. Speed and Brake Status Received by Ford28

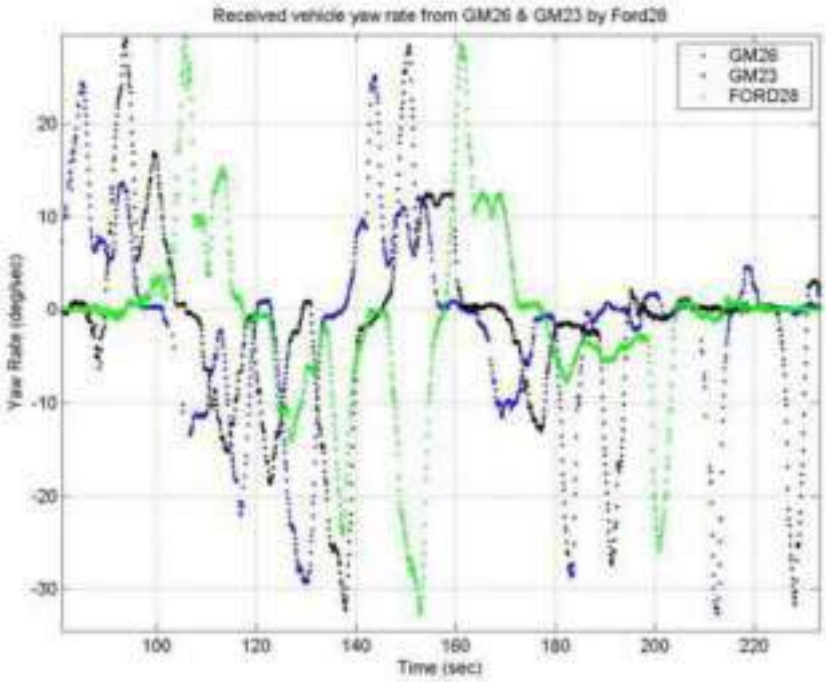


Figure 121. Yaw Rate Received by Ford28

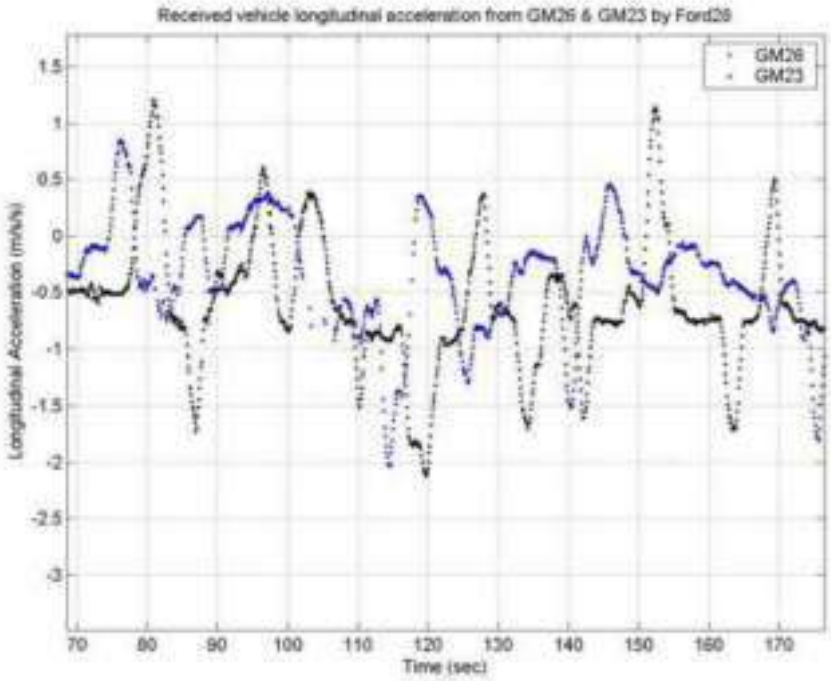


Figure 122. Longitudinal Acceleration Received by Ford28

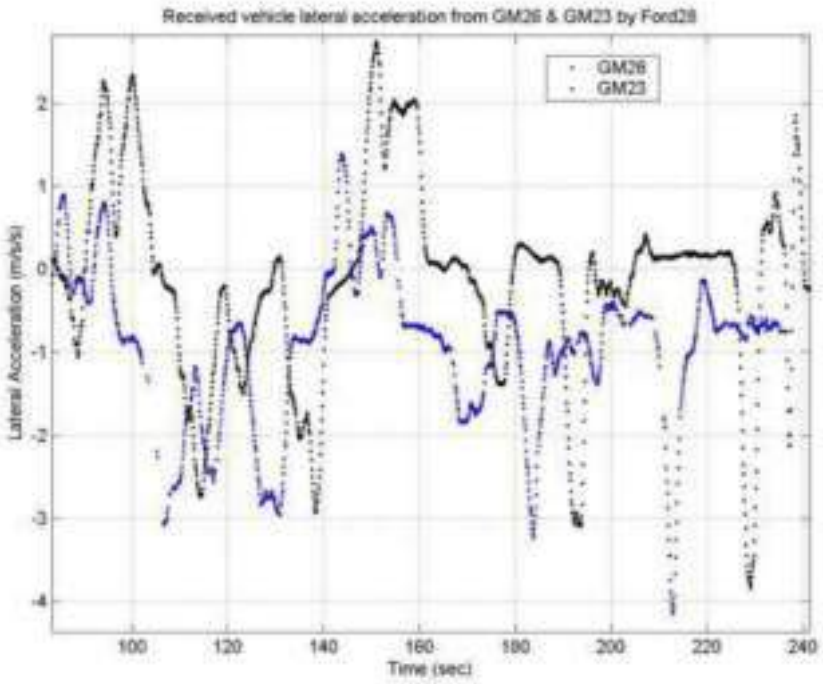


Figure 123. Lateral Acceleration of Received by Ford28

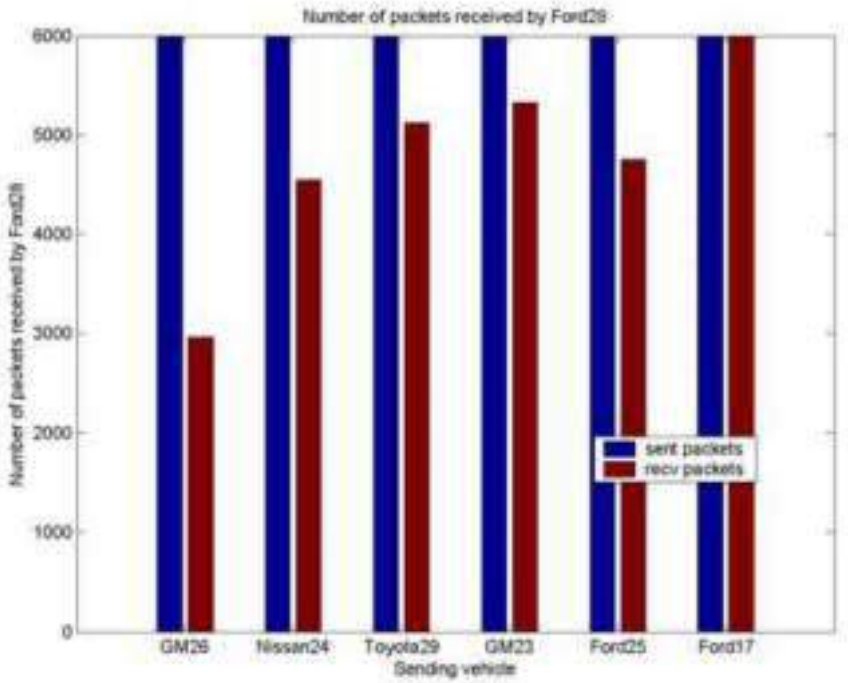


Figure 124. Number of Packets from Other Vehicles Received by Ford28

4.2.3 Test Conducted on M-5 Ramp to 12 Mile Road

This test scenario was conducted on the M-5 ramp exit to 12 Mile Road in Michigan. The parameters for this test are shown in Table 19. In this test, the Transmit Power was set to 16 dBm.

Packet Length (bytes)	*Message Interval (ms)*	*Data Rate (Mbps)*	*Transmit Power (dBm)*
200	*100*	*6*	*16*

Table 19. Parameters for Test Scenario No. 4.2.3

As shown in Figure 112, GM26 is the lead vehicle followed by Nissan24, Toyota29, GM23, Ford25, Ford17 and Ford28 respectively. The WRMs on all vehicles were configured to both send and receive data. The results for this test are shown in Figures 125 through 130. Distances between Ford28 and other vehicles were calculated from V-V communication received by Ford28. The distances are color-coded based on the received signal strength indicator (RSSI) values for the packets received by Ford28. Figure 126 shows the speeds, color-coded based on the brake status, of GM26 and GM23 using data received by Ford28. Figures 125, 126, and 127 show the yaw-rate, longitudinal acceleration and lateral acceleration respectively of GM26 and GM23 based on data received by Ford28.

The data from Figure 130 taken over a 60 second segment of this test scenario shows that out of 600 packets sent by each vehicle, the number of packets received by Ford28 from GM26 is 565 (94%), the number of packets received by Ford28 from Nissan24 is 587 (98%), the number of packets received by Ford28 from Toyota29 is 596 (99%), the number of packets received by Ford28 from GM23 is 597 (99.5%), the number of packets received by Ford28 from Ford25 is 593 (99%), and the number of packets received by Ford28 from Ford17 is 600 (100%). In general, the results of this test showed that, on the freeway ramp environment, vehicle-to-vehicle communication were possible between the vehicles to 100 m range with reduced Transmit Power of 16 dBm.

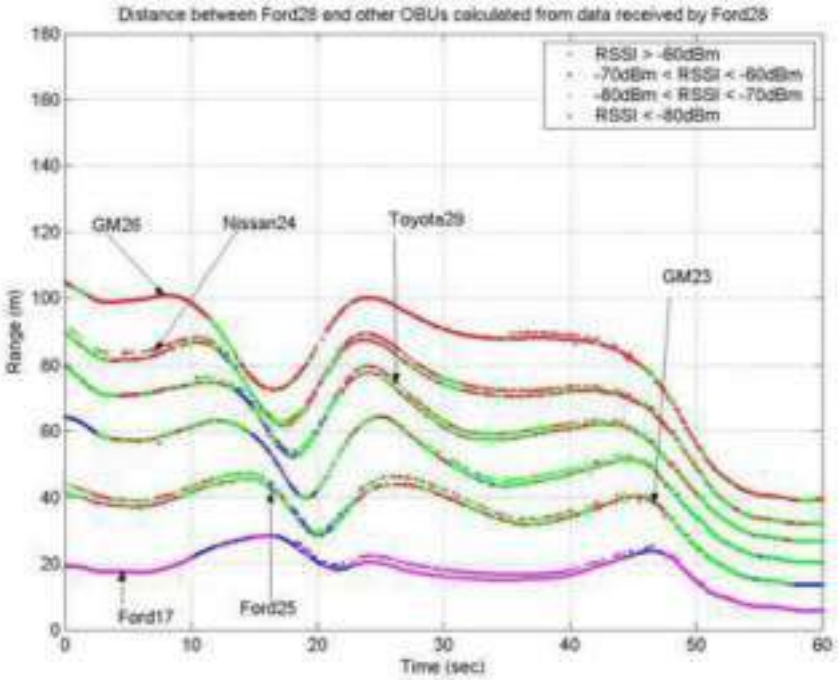


Figure 125. Distances Calculated from Data Received by Ford28

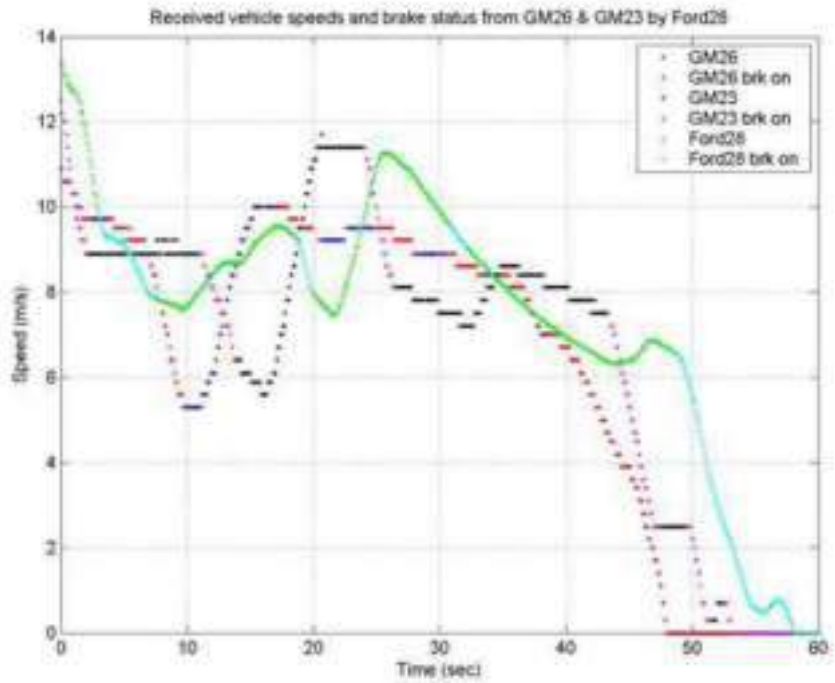


Figure 126. Speed and Brake Status Received by Ford28

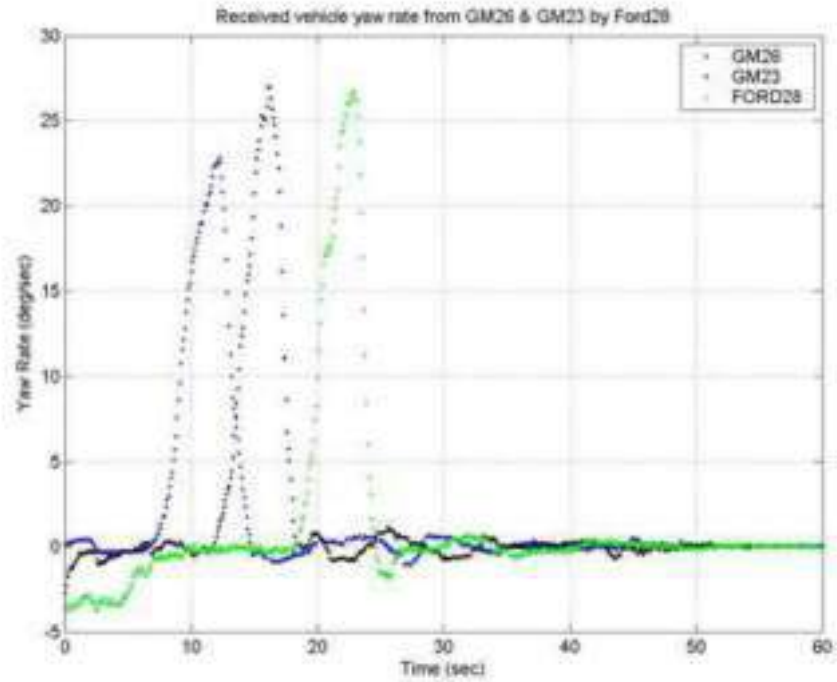


Figure 127. Yaw Rate Received by Ford28

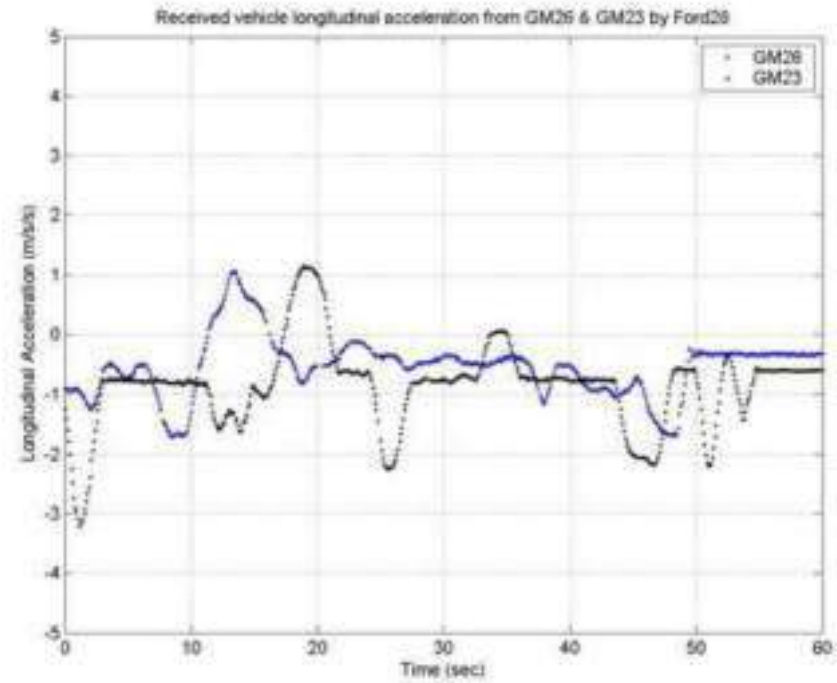


Figure 128. Longitudinal Acceleration Received by Ford28

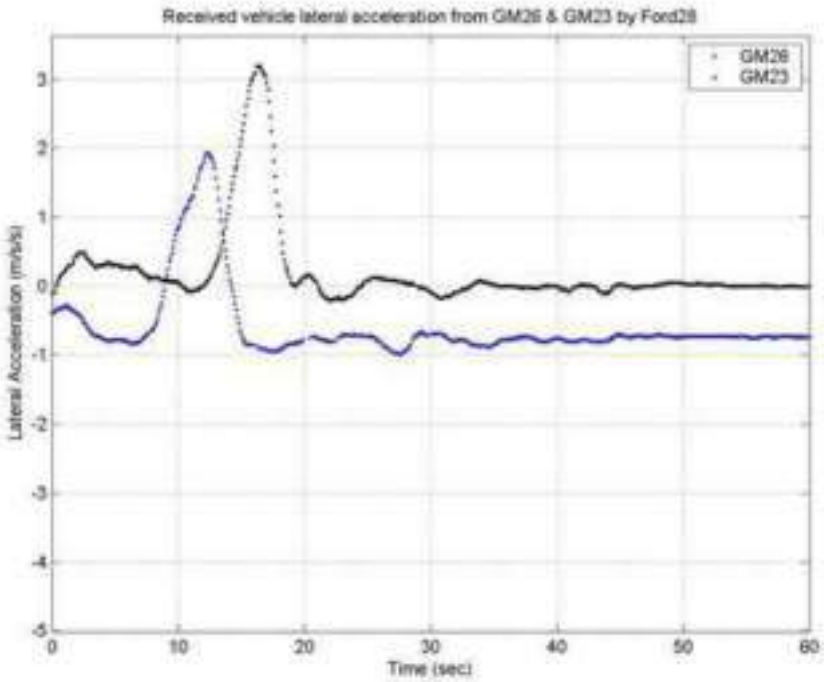


Figure 129. Lateral Acceleration of Received by Ford28

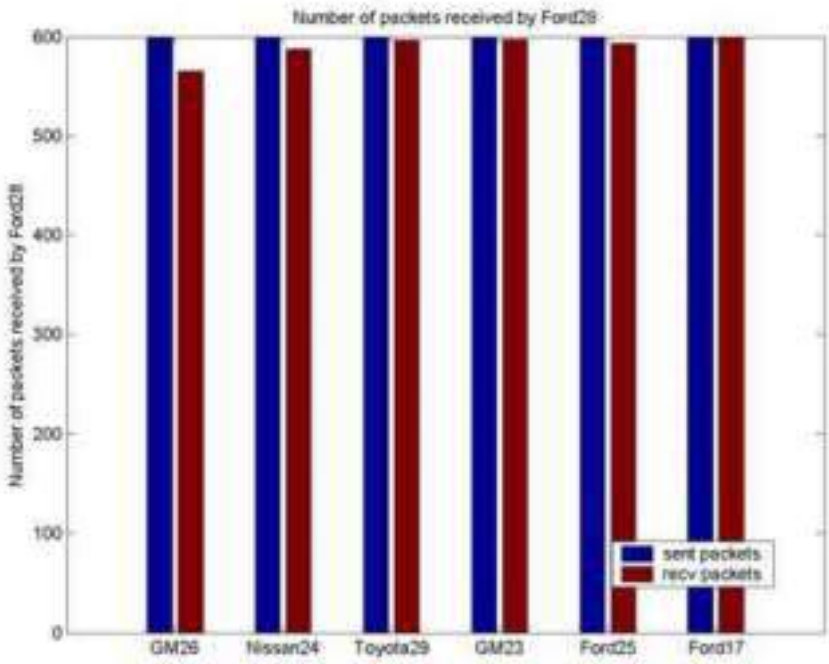


Figure 130. Number of Packets from Other Vehicles Received by Ford28

4.3 Summary

This section presented the results of the vehicle-to-vehicle communications testing conducted at the Milford Proving Grounds (MPG), I-96 freeway, and the M-5 ramp in Michigan to evaluate the performance of the Wave Radio Modules (WRMs) under vehicle-to-vehicle communications scenarios. In all the tests, the WRMs were configured to send and receive on the DSRC Control Channel, which is Channel 178 with a center frequency of 5890 MHz and a 10 MHz bandwidth.

The vehicle-to-vehicle communications testing at MPG was conducted using a Jaguar XKR developed by Ford for the EDMap project, and a Buick Lesabre developed by GM for the ACAS project. Software modifications were carried out on both these vehicles so that they provide the vehicle signals over the CAN interface as defined in the Task 9 application. Based on the V-V communications testing at MPG the following conclusions can be made:

- Results showed true omni-directional characteristics of the 5.9 GHz DSRC roof-mount antenna developed under Task 6 of the VSC project.

- Results showed 100 percent reception and no packet loss with vehicle-to-vehicle communication between the two vehicles up to ranges that exceeded 200 m in a vehicle following scenario.

- Results show that we have vehicle-to-vehicle communication between the two vehicles up to ranges that exceed 600 m on both directions of travel.

- Results showed that reducing the transmit power from 20 dBm to 5 dBm reduced the range of vehicle-to-vehicle communication to about 250 m on both directions of travel.

- Results showed that increasing the data rate from 6 Mbps to 27 Mbps was associated with higher packet losses and reduction in communication range, as expected, due to the subsequent reduction in transmit power (3-4 dBm) that takes place based on IEEE stipulations.

Vehicle-to-vehicle communications testing was conducted on the I-96 freeway and M-5 ramp in Michigan in order to evaluate the communications performance on freeways. Seven vehicles – GM26, Nissan24, Toyota29, GM23, Ford25, Ford17 and Ford28, formed a caravan as shown in Figure 112. The caravan consisted of 4 sedans, 2 SUVs and a minivan. Three of these vehicles, Ford28 (Jaguar XKR developed by Ford for the EDMap project), GM23 and GM26 (both Buick Lesabres developed by GM for the ACAS project), had software modifications carried out so that they provide the vehicle signals over the CAN interface as defined in the Task 9 application. Based on the V-V communications testing on freeways the following conclusions can be made:

- In general, the results showed that, on the freeway environment, vehicle-to-vehicle communication were possible between the vehicles to 180 m range with Transmit Power of 20 dBm.

- Results showed that the communication characteristics of the 5.9 GHz DSRC roof-mount antenna can be degraded by the luggage roof rack.

- Results showed that the packet reception can be affected because of line of sight obstructions from SUVs and minivans.

- Results showed that reducing the Transmit Power from 20 dBm to 16 dBm reduced the range of vehicle-to-vehicle communication between the vehicles to 150 m. Also the packet reception because of line of sight obstructions from SUVs and minivans can be affected severely by reduction in Transmit Power.

- In general, the results of this test showed that, on the freeway ramp environment, vehicle-to-vehicle communications were possible between the vehicles to 100 m range with reduced Transmit Power of 16 dBm.

Based on the V-V testing conducted, the communication characteristics and performance of the WRMs are promising for vehicle safety application development in the future.

Appendix H:
WAVE/DSRC Security

TABLE OF CONTENTS

1 Background 1

2 Threat Model 2

2.1 Background 2

2.2 Introduction 2

2.3 Overview of VSC for the Purpose of a Security Study 3

2.3.1 Curve Speed Warning 4
2.3.2 Traffic Signal Violation Warning 5
2.3.3 Extended Brake Lights 6
2.3.4 Other Potential Situations 6
2.3.5 VSC Unit Life Cycle 6

2.4 Desired Security Services 7

2.4.1 Message Integrity / Origin Authentication (MI /OA) 7
2.4.2 Correctness 7
2.4.3 Privacy 7
2.4.4 Robustness 8
2.4.5 Fail-Safety 8

2.5 A Strawman Security Architecture for Use in the Threat Model 9

2.5.1 Providing Communication Security 9
2.5.2 Correctness 10

2.6 Required Unit Capabilities 11

2.6.1 OBUs 11
2.6.2 RSUs 11

2.7 Attacker Capabilities 12

2.7.1 Class 1: Attackers With a Programmable Radio Transmitter/Receiver 13
2.7.2 Class 2: Attackers With Access to an Unmodified VSC Unit 14
2.7.3 Class 3: Attackers Who Have Recovered Keying Material From a VSC Unit 16
2.7.4 Class 4: 'Inside' Attackers 17
2.7.5 Some Out-of-Scope Threats 19

2.8 Containing Compromise 19

2.8.1 Proactive Containment 20
2.8.2 Discriminators for Compromised Units 20
2.8.3 Residual Capabilities of Compromised Units 20

3 Constraints 21
3.1 Introduction 21
3.2 Network Characteristics 21
3.2.1 Total Number of Units 22
3.2.2 Maximum Data Rate 22
3.2.3 Packets Per Second 22
3.2.4 Latency 22
3.2.5 Packet Loss Rate 23
3.2.6 Packet Size 23
3.3 Environmental Characteristics 23
3.3.1 Unit Size 24
3.3.2 Temperature Range 24
3.3.3 Heat Output 24
3.3.4 Power Consumption 24
3.4 Cost of Goods 25
3.4.1 RSUs 25
3.4.2 OBUs 25
3.4.3 Management Consoles 25
3.4.4 Service Consoles 25
3.4.5 Manufacturing Facilities 26
3.5 Management Costs 26
3.5.1 Investigation of Compromise 26
3.5.2 Key Infrastructure 26
3.5.3 Management of RSUs 28
4 Architecture 29
4.1 Introduction 29
4.2 Architecture Summary 29
4.3 Architectural Overview 29
4.3.1 Key Hierarchy 29
4.3.2 Communications Architecture 30
4.3.3 Message Authentication 31
4.3.4 Management, Revocation, and Updates 32
4.3.5 Fail-Open versus Fail-Closed 32

4.4 RSUs and Public Safety OBUs 32
4.4.1 Authentication Structure 33
4.4.2 Certificate Format 35
4.4.3 Registration and Certificate Issuance 37
4.4.4 Message Authentication 38
4.4.5 Propagation of Certificates 40
4.4.6 Identifying Compromised Units 40
4.4.7 Certificate Revocation 41
4.4.8 Choice of Algorithms 41
4.5 Authentication for OBU Messages 44
4.5.1 Selection Criteria 44
4.5.2 Building Blocks 46
4.5.3 Global Symmetric Keys 50
4.5.4 Public Key Signature Based Schemes 51
4.5.5 Group Signatures 62
4.5.6 Comparison of Schemes 62
5 Protocol 64
5.1 Introduction 64
5.2 Protocol Summary 64
5.3 Protocol Definition 64
5.3.1 Certificate Format 64
5.3.2 Certificate Revocation List Format 73
5.3.3 VSP Message Format 75
5.3.4 Signed Message Format 76
5.3.5 System Updates 82
5.4 Enrollment Procedures 84
5.4.1 CAs, RSUs, and PSOBUs 84
5.4.2 OBUs Certificate Initialization 86
5.5 Suggested Operating Procedures 86
5.5.1 OBU Operating Requirements 86
5.5.2 OBU CAs and Escrow Authorities 87
5.5.3 CA's Procedures 87
5.6 OBU Privacy Parameters 87
5.6.1 Choice of Work Factor for OBU Blinding 87
5.6.2 OBU Certificates 88

5.7 Opportunities for Optimization 88
5.7.1 Combined Algorithm Identifiers 88
5.7.2 Length of Fields 89
5.8 Summary of Syntax 89
6 References 97
7 Exhibit A: Analysis of ECDSA Performance 100
8 Exhibit B: Choice of Key Size 102
9 Exhibit C: The Subset Difference Algorithm 103
10 Exhibit D: Table of Acronyms 105

LIST OF TABLES

Table 1: Summary of Attacker Types and Attacks 19
Table 2: Summary of Network Constraints 23
Table 3: Summary of Environmental Constraints 25
Table 4: Message Sizes for Blind Signatures 57
Table 5: ECDSA Key Strengths and Sizes 102

LIST OF FIGURES

Figure 1: Curve Speed Warning Scenario 4
Figure 2: Traffic Signal Violation Warning Scenario 5
Figure 3: Extended Brake Lights Scenario 6
Figure 4: Strawman Key Distribution 9
Figure 5: Strawman Block Diagram 10
Figure 6: Signal/Message Conflict 15
Figure 7: Overview of Dual Authentication Structure 30
Figure 8: VSC Communications Architecture 31
Figure 9: A Protected Message 31
Figure 10: Functional Scope for RSUs and Public Safety OBUs 37

Figure 11: A Protected Message..... 38
Figure 12: A Broadcast Encryption Tree..... 46
Figure 13: Erasure Code Transmission and Reconstruction 48
Figure 14: A Trivial Code 49
Figure 15: Innocent Revocation Rates 60
Figure 16: Subset Difference Broadcast Tree..... 76
Figure 17: Subset Difference Broadcast Tree..... 103
Figure 18: Keys Assigned to Node Nl,l,r 104

1 Background

Security is an important consideration for Dedicated Short Range Communications (DSRC) that supports vehicle-safety applications. For the system to be secure, the applications must be able to trust that the communication has been received unaltered and from a known source. The communication should require a low amount of computational and communications overhead, and it must be robust in the event of individual units being compromised. Most of the vehicle-safety applications studied in the VSC project broadcast messages to all receivers, rather than directed to a given peer, which creates additional security challenges.

Communications security consultants completed the majority of technical work for this task, as well as the majority of the documentation contained in this appendix. The solutions presented in this appendix represent the recommendations of the consultants, which appear to meet the assumptions and constraints within this task. However, with the currently proposed architecture, which includes many optimizations, each message transmitted would include significant overhead, and the message signatures would take time to process once they are received. Management of a Public Key Infrastructure for RSUs would also be necessary, according to the proposed scheme. This analysis represents a foundational examination of the security question, and provides a recommendation upon which future testing may be accomplished. The overall feasibility of implementing the proposed security approach has not yet been determined.

2 Threat Model

2.1 Background

Security is a primary concern for vehicle-safety applications that are enabled or enhanced by wireless communications. This is the first in a series of sections describing the security issues associated with Vehicle Safety Communications and their possible solutions. This section focuses on the threat model, which will need to be considered by any potential design.

In this threat model, we identified four major security goals for the VSC system:

1. Message integrity/origin authentication – receivers can tell that a valid unit generated the message(s);
2. Correctness – when units generate valid messages, we can have some assurance that they were correct;
3. Privacy – it should not be possible to use VSC to remotely obtain private information about a vehicle's behavior and then tie it back to a single identified vehicle; and
4. Robustness – the system should contain mechanisms for containing misbehaving units and, where possible, continue to operate under attack.

In order to accomplish these security goals, we need to consider the kinds of attacks that might be mounted. We contemplated four basic kinds of attackers with escalating capabilities:

1. Attackers with a programmable radio transmitter/receiver;
2. Attackers with access to an un-modified VSC unit who can, therefore, control the inputs, sensors, etc.;
3. Attackers who have access to a modified VSC unit and who have obtained the keying material; and
4. "Inside" attackers who have access to records and equipment operated by the vehicle manufacturer or the VSC unit manufacturer.

Each of these attackers has a certain class of attacks that they are able to mount. In general, attackers with greater capabilities will also be able to mount a greater number of attacks, including potentially more damaging ones. However, certain kinds of attacks – such as those on the Global Positioning System (GPS) satellites and ground stations – are out of scope for this threat model. Attackers with the capability to mount such attacks can, in general, not be defended against, though there are techniques available to contain the threat they present.

We must assume throughout our design that some attacks will succeed and some units will be compromised. Thus, the design of the eventual system must incorporate this assumption as part of the threat model. One major focus of future work will be on containing compromise by detecting when it has occurred and shutting compromised units out of the VSC system.

2.2 Introduction

5.9 GHz DSRC is a wireless communications system that provides vehicle-vehicle and infrastructure-vehicle communications services. One of the anticipated major uses of this technology is for safety information such as emergency braking warnings, traffic signal violation warnings, and curve speed warnings.

Security is a primary concern in any vehicle-safety application and it is especially important when the critical data is being transmitted over the air. Without security, an attacker could tamper with

the messages being communicated and potentially cause harm. To take merely one example, an attacker who could forge messages could send false braking indicators, causing inappropriate emergency braking and perhaps crashes.

The first step in designing any security system is to determine the threat model. A threat model describes the capabilities that an attacker is assumed to be able to deploy against the system. It then attempts to predict what sorts of attacks those capabilities might enable the attacker to mount. Equally important, it specifies the forms of attack that are out of scope for the system. Nearly every security system is vulnerable to a sufficiently dedicated and resourceful attacker. The goal of security is not to provide absolute protection but to manage risk. When deciding whether to protect against an attack, the difficulty of providing that protection needs to be balanced against the seriousness of the threat and the difficulty of mounting it.

It is extremely difficult to estimate the magnitude of each threat, since the potential harm can vary widely. For example, if an attacker could impersonate an emergency vehicle, he or she could mount threats with consequences of different magnitudes. The attacker could use the communication to move quickly through traffic, convincing drivers that an emergency vehicle is approaching and causing them to move to the side of the road. This could result in delays and possibly confusion (when they do not see an emergency vehicle) for the other drivers. That same attacker could alternatively plan to preempt traffic signals in a coordinated fashion to make sure that the vehicle of an elected official, for example, would be properly placed for a terrorist attack. This scenario clearly has more serious consequences. Taking another example, if an attacker can impersonate a vehicle in an emergency braking maneuver, he or she could cause traffic jams behind them that could serve several purposes. The disturbance could simply be an amusement for the attacker, or it could be used in collaboration with other attackers to temporarily obstruct traffic arteries around a targeted city. Because the potential consequences of an attack vary so widely, they are not quantified in this report. However, some recent real-world examples may serve to highlight the need for secure communications.

In July of 2003, Kohno et al. [41] published a series of flaws in Diebold Election Systems's electronic voting system, causing some loss of confidence in e-voting and significant negative publicity for Diebold, which has remained in the news long after the initial publication. Secondly, 3M currently sells a device which allows traffic signals to be remotely controlled by public-safety vehicles. This system has no security, and consumer units that can control these intersections recently have become available [42], much to the dismay of the press and public. If VSC does not include the appropriate security, similar results are possible.

2.3 Overview of VSC for the Purpose of a Security Study

In this section, VSC is described briefly in terms pertinent to a security study. Reporting for the threat model will refer to the VSC system, as described in this section.

The VSC system will allow vehicles to communicate with each other and with infrastructure elements. Broadly speaking, this means there are two types of network elements:

Road Side Units (RSUs) – network nodes embedded in infrastructure elements such as road signs, traffic signals, etc., and

On-Board Units (OBUs) – network nodes embedded in vehicles.

In both cases, it is expected that the units will at a minimum consist of:

- A general purpose processor and associated memory;
- A radio transmitter and receiver;

- Interfaces to sensors as required; and
- A GPS receiver (for non-stationary units).

This combination of elements enables a number of safety application scenarios [1]. For purposes of analysis we will focus on three such application scenarios, which were determined to be representative of the required system capabilities. We briefly describe those scenarios here:

2.3.1 Curve Speed Warning

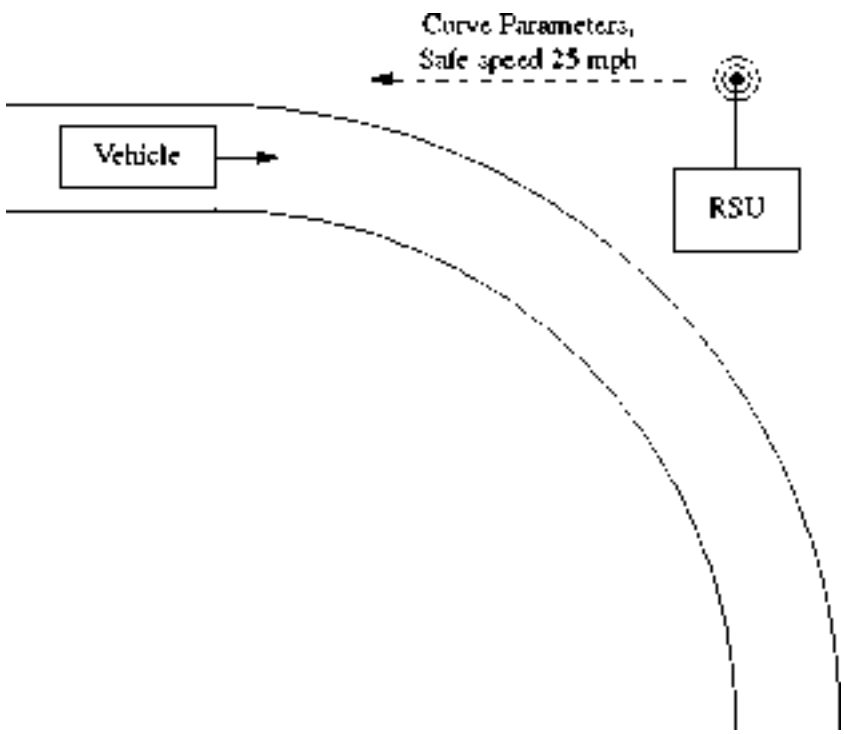


Figure 1: Curve Speed Warning Scenario

Probably the simplest VSC application scenario is *Curve Speed Warning* (CSW). It is quite common for curves in roads to have safe traversal speeds that are significantly less than the current speed limit or, at least, less than the prevailing vehicle speed. Such curves often have signs posted that warn drivers of the maximum safe speed for that curve. CSW is effectively an electronic version of such signs. Since radio transmissions can be received beyond line of sight, CSW can provide advance warning of the need to slow down.

In its simplest form, CSW could be implemented as a radio transmitter broadcasting the same speed limit as posted on the sign. As currently contemplated, it would also include the shape of the oncoming curve/curves so that the vehicle can calculate individual limits. The user interface for CSW is not specified; however for our purposes we assume that when the OBU receives a CSW signal it attempts to determine whether the vehicle is moving at a safe speed, and if not, warns the driver in some way.

2.3.2 Traffic Signal Violation Warning

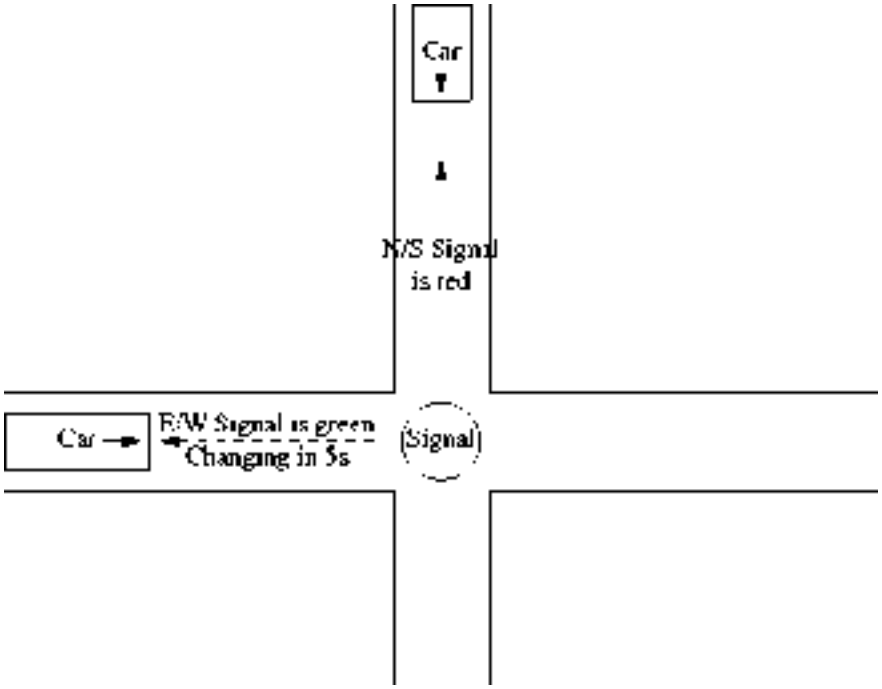


Figure 2: Traffic Signal Violation Warning Scenario

Traffic Signal Violation Warning (TSVW) acts to increase the amount of information provided by traffic signals and allow the driver to be warned if he is in danger of going through a red light. Traditional traffic signals have three modes: red, green, and yellow. The current color state provides only a limited amount of information about the time until the next state. In particular, the time from red to green and green to red is almost entirely unbounded. The TSVW application scenario provides this timing information to the vehicle, which can warn the driver when appropriate.

A TSVW RSU would likely be attached to a traffic signal. It would periodically broadcast its own location (to identify the specific traffic signal being referenced), the current state of the signal in each direction, plus the expected time until the next state and what that state will be. As with the CSW application scenario, the OBU would attempt to determine whether the vehicle was in danger of violating the traffic signal and notify the driver if so.

2.3.3 Extended Brake Lights

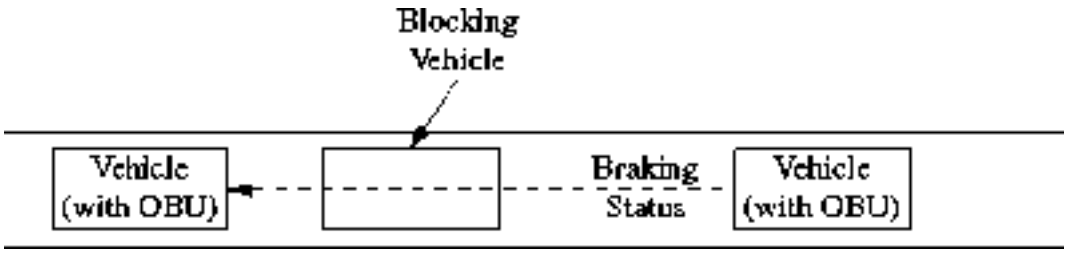


Figure 3: Extended Brake Lights Scenario

Like CSW and TSVW, *Extended Brake Lights* (EBL) extends the operational range of conventional visual signals. Unlike CSW and TSVW, EBL is a vehicle-to-vehicle application scenario rather than an infrastructure-vehicle application scenario. The purpose of EBL is to extend the range of brake light signals in emergency braking situations. Currently, drivers can see when the vehicle ahead of them is braking, but cannot see the brake lights of vehicles further down the road. In addition, brake lights are either on or they are off. They provide no information about the magnitude of the deceleration. These factors limit drivers' reaction time to emergency braking events.

The purpose of EBL is to enable improved response to such events. When a VSC-enabled vehicle detects hard braking (via brake pedal sensors, accelerometers, etc.) it broadcasts an EBL warning containing its position, velocity, acceleration, etc. When other VSC-enabled vehicles in the vicinity receive the warning, their onboard CPUs determine whether this is a potential threat and, if so, warn the driver of the situation.

Note that unlike CSW and TSVW, in which the OBUs are receivers, EBL requires the OBU to have sensors and a radio transmitter.

2.3.4 Other Potential Situations

We have mentioned two kinds of messages: vehicle-to-vehicle and infrastructure-to-vehicle. For completeness, we note that there are two other potential kinds of messages: vehicle-to-infrastructure (e.g. for traffic density measurement) or infrastructure-to-infrastructure (for coordination purposes). We do not believe that these situations introduce new security threats beyond those in the situations described above.

2.3.5 VSC Unit Life Cycle

OBUs are likely to have a simple life cycle: they are manufactured – either by the vehicle manufacturer or a subcontractor – and then installed in the vehicle. At some point during this process they are initialized with the appropriate keying material. They then require no real management other than keying material (and potentially software) updates, and deactivation under certain removal, reuse and vehicle retirement conditions. The means and criteria for deactivation are not defined in this report and need to be developed and tested via a detailed FMEA process. One exception here is public safety OBUs, which derive their authority from the agency that operates their vehicles, not the vehicle manufacturer. Their life cycle is much more

like that of RSUs, and the details of their life cycle management will be covered by a different team (see Section 2.1, entitled "Interaction With DSRC Standards Groups").

The life cycle of RSUs is more complicated than that of ordinary OBUs. The first difference is that the RSU derives its authority from the agency that operates it. Thus, RSUs will likely be initialized by the transportation agency that installs them. The second difference is that RSUs may need to be reconfigured as conditions change; for instance, a stop sign might be moved. Thus, RSUs must be field-manageable or even remotely manageable via the Internet. This management system must be constructed in such a way that only authorized agents can manage the RSU. This sort of authentication, authorization, and access control is a classic security problem with a number of known solutions.

2.4 Desired Security Services

The most basic security service that we are interested in providing is that the receiver of a VSC message obtains an accurate picture of the state of the world, as far as the transmitter knew it. It is easiest to think of this service as rejecting all messages that do not match those which would be generated by a perfect VSC unit. Imagine that each vehicle and infrastructure unit were fitted with a perfect VSC unit that always broadcast correct messages. The goal of VSC security, then, is to arrange that any given VSC receiver can reject any messages that do not match those which would have been generated by the perfect VSC unit.

We should be able to obtain this goal even in the face of attack. Attackers might have a variety of capabilities, which we consider in Section 3.7. Most likely this includes the ability to broadcast arbitrary messages and/or the ability to cause some units to lie. Thus, while we must expect that receiving units will receive bogus messages that do not match those which would be transmitted by the perfect unit, the unit should be able to reject those messages.

This general security service implies two sub-services: message integrity/origin authentication and correctness.

2.4.1 Message Integrity / Origin Authentication (MI /OA)

The purpose of MI/OA is to allow a receiving unit to determine whether messages that it receives were generated by valid VSC units and have not been tampered during transit. Clearly, if an attacker could easily generate false messages or tamper with legitimate ones, then they could cause a receiving unit to have false beliefs.

In some cases, it is also necessary for a VSC receiver to be able to determine that a series of transmissions came from the same source. For instance, a receiver might want to determine the path of a given vehicle in order to assess road conditions.

2.4.2 Correctness

Even if we assume that we have some MI/OA service, there is still the possibility that a legitimate VSC unit will lie. Thus, we want to somehow ensure that the messages transmitted by a unit reflect the state of the world, at least as far as the transmitting unit knows.

2.4.3 Privacy

A secondary but still important goal of the system is privacy. In many cases, OBUs will be transmitting information about the state of the vehicle that could be used against the owner of the vehicle. For instance, if vehicles transmit their location, speed, and identity, it would be possible for terrorists to easily collect information about the movements of public officials by deploying sensors that listened for their OBU transmissions. This type of information leakage appears likely to make the VSC system unattractive to customers. Thus, it is not acceptable, for instance, to

issue every vehicle a Public Key Infrastructure (X.509) certificate [2] which is transmitted with each message.

The privacy requirement of our design, therefore, is that to the extent to which potentially compromising information is transmitted, it should be difficult to tie that information to any particular vehicle without being in close physical proximity to the vehicle (in which case the information would be self-evident). Thus, it is likely necessary to hide the identity of the transmitting unit.

It is not clear at the present time whether complete concealment of the transmitter's identity or merely plausible deniability is required. Note that in either case, the need for privacy interacts with that for MI/OA. For instance, it is sometimes necessary to be able to determine that messages had a common origin. This needs to be done in such a way that messages can only be linked over short time windows to avoid excessive information leakage.

Note that the goal of privacy is different from that of confidentiality. In most cases, the information being broadcast is inherently public, and it is just the identity of the transmitter that needs to be kept private. At this time, the VSC research has not identified any applications that require confidentiality. If those applications are identified, then that new requirement will need to be considered during the solution stage.

2.4.4 Robustness

Another secondary security goal is robustness. It must be assumed that some units will be compromised—either subverted into generating incorrect messages or have their keying material compromised. The system should have methods of recovering from that compromise. This will most likely require ways to allow legitimate units to ignore messages from compromised units.

Another important form of robustness is the ability to withstand *denial of service* (DoS) attacks. In such attacks, an attacker attempts to stop parts of the system from functioning. He might, for instance, jam all the radios in an area or attempt to send messages to individual units to stop them from receiving or transmitting. Such attacks are notoriously difficult to defend against. Our goal will be to defend against them where possible and, at worst to avoid making them any easier.

2.4.5 Fail-Safety

A related issue is that of failure modes. It may well be the case that a receiving unit has some reason to doubt the correctness of a message, though it is not entirely sure. It is not entirely clear how such messages should be handled.

For example, in many cryptographic systems, compromised units are added to a *revocation list*. Thus, when a unit receives a message, it checks the sender identity against the revocation list and rejects the message if the sender is on the list. Revocation lists are issued on some regular schedule (monthly is common). Now, consider what happens if a unit for some reason has not yet received the current revocation list. In theory, it then cannot validate any message because it cannot check for revocation status. In practice, if the unit has a relatively recent list -- according to which the sender is valid -- then with high probability the incoming message is still valid since attacks would be statistically rare. A system that failed safe would discard such messages if the list has surpassed its expiration date, but it would have substantially less information about the world.

2.5 A Strawman Security Architecture for Use in the Threat Model

In this section, we describe a strawman security architecture. It is not intended to be a complete design and indeed has known deficiencies with respect to the security goals we have just identified. It is intended to provide a common reference point for the rest of the threat model discussion and is necessary for that purpose only.

2.5.1 Providing Communication Security

In order to provide MI/OA, we divide the world into two categories: legitimate units and all others. All legitimate units will share a single symmetric key K_i, which is valid for time period i. Messages are transmitted with an attached *Message Authentication Code* (MAC), computed using K_i. i.e., the unit transmits message M as $M||\mathrm{MAC}(K_i,M)$. Thus, a receiving unit can verify the correctness of a message via checking the MAC over M.

Each unit in the system will have a unique certified public/private key pair, but this key pair is used only for key distribution. Each group key K_i is issued by a single central authority, the *Key Distribution Center* (KDC), as shown in Figure 4. That authority only issues K_i to the units which are believed to be valid at the beginning of time period i. The KDC is usually operated by a *Security Officer* (SO) who is responsible for issuing keys and verifying that units have not been compromised.

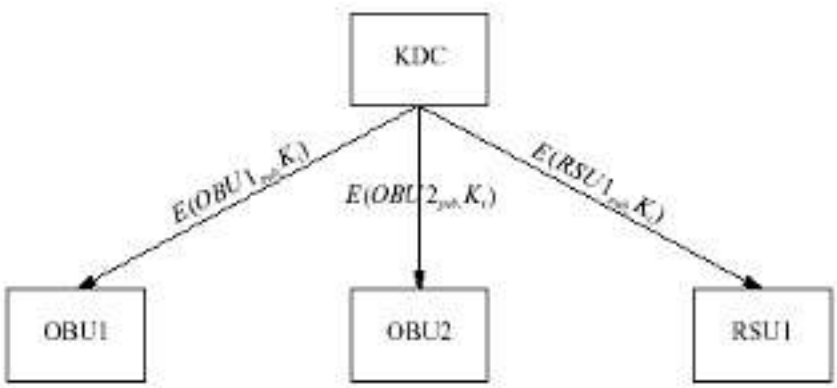


Figure 4: Strawman key distribution

It should be readily apparent that this system provides both MI/OA and privacy. As only valid units possess K_i, only they can generate valid messages and because the messages are MACed they cannot be changed in transmit. As all messages are MACed with the same common key, it is not possible to determine which messages were generated by which unit, thus privacy is provided.

In addition, this system provides a measure of robustness against compromise. Since the group key is periodically refreshed, if a unit is known to be compromised in time period i, the KDC simply does not issue it a key in time period i+1.

This strawman system is not a complete design or even necessarily the kind of security architecture that will eventually be deployed. It is provided purely as a reference point to focus discussion. The system just described has a number of known deficiencies. In particular, there is

no cryptographic way to differentiate RSUs from OBUs. Thus, an attacker who recovered the keying material from an OBU could impersonate an RSU. A hybrid system in which RSUs – which do not require privacy – are authenticated with public key cryptography could fix this problem.

2.5.2 Correctness

The system we have just described does not, however, guarantee correctness. An attacker in possession of a valid unit can extract K_i or the unit private key (through which he can obtain K_i) and can then transmit messages of his choice, posing as his unit. In order to prevent this attack, we need to harden the unit. The general idea is to enclose the sensitive portions in a tamper-resistant and tamper-evident casing, such as that specified in FIPS 140-2, levels 3-4 [3], and described below.

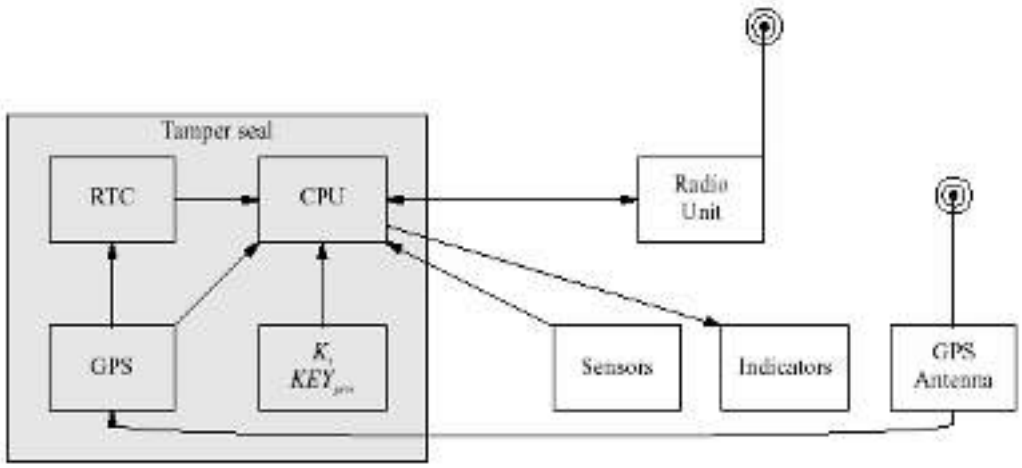


Figure 5: Strawman Block Diagram

The boundaries of the casing are an issue that will need to be decided during the full design process. For our strawman, we will consider a minimal configuration in which only the cryptographic unit, GPS receiver, a processor, and a real-time clock are embedded inside the tamper enclosure, as shown in Figure 5. The rest of the sensor modules lay outside the tamper enclosure. Therefore it is possible to convince the unit that, for instance, the user has applied the brake pedal by manipulating the appropriate sensor lead. In principle, one could place the GPS outside of the tamper enclosure as well; however, this would leave the unit with no way of independently determining the location of the unit and thus reduce correctness nearly to zero.

In general, there are two kinds of tamper seals: tamper-resistant and tamper-evident. A *tamper-resistant* seal is designed to be difficult to open and to ensure that the unit self-destructs (typically by zeroing the keying material) if an attacker attempts to open it. By contrast, a *tamper-evident* seal is simply designed to leave evidence that it has opened. Thus, if an attacker opened the unit and violated the tamper seal, it would be possible to subsequently determine this by physical inspection of the unit. For purposes of our strawman, we will assume that the seal is tamper-resistant, but that a sufficiently dedicated attacker might be able to extract the keying material.

2.6 Required Unit Capabilities

Now that we have covered each potential sample application scenario we can see that different types of units have different required capabilities. We may be able to exploit these differing requirements in our final design. We discuss those requirements here, beginning with OBUs.

2.6.1 OBUs

OBUs come in two varieties with different potential security requirements. They may either be intended for use in passenger vehicles operated by ordinary customers or they may be intended for public-safety vehicles such as ambulances and police vehicles. The requirements for these units differ both in terms of privacy and in terms of the desired degree of protection for keying material.

Protection of Keying Material

We expect that public-safety vehicles will need a higher degree of protection for their keying material. The rationale here is that public-safety vehicles will be able to create certain classes of messages that consumer vehicles cannot, e.g., "I'm an ambulance, out of the way." Clearly, forgery of such messages is especially undesirable and so public-safety OBUs need a higher degree of assurance. Some of this assurance will likely be provided by physical security around the vehicles themselves, but it is likely that the OBU will need better protection as well. Thus, public-safety OBUs might use better tamper sealing, be subject to periodic inspection, etc.

Note that in this scenario it would be desirable to somehow arrange that compromised consumer OBUs cannot be used to generate public-safety messages. The strawman system described in Section 3.5 cannot do this, because it requires the ability to verify a class of messages that the unit cannot generate. Generally, this requires public key technology, because with symmetric key, the ability to verify authenticity of a message is linked to the ability to generate valid messages.

Privacy

One goal of the overall VSC system design is to maintain privacy for traffic generated by customer OBUs. By contrast, public-safety vehicles generally do not require privacy. In fact, auditability for public safety is most likely desirable, especially if it allows easier revocation of compromised OBUs.

2.6.2 RSUs

RSUs also come in two varieties, as shown by the CSW and TSVW scenarios. The CSW RSU is a stationary unit that needs only to be able to generate the same message repeatedly.[1] By contrast the TSVW RSU is dynamically linked to the traffic signal and therefore needs a modest amount of intelligence.

Static Devices

A CSW RSU, in its simplest implementation, is a fairly dumb device and transmits the same (static) information repeatedly. Since the road it describes is stationary, it can be installed with information about the curve and never have to get any extra input. As a consequence, it does not need to have any sensors and is not vulnerable to sensor input-

[1] Note that a CS/RW RSU that adjusts its advice based on current weather conditions or observations of vehicle behavior is actually a dynamic RSU. Some applications, such as construction zone warnings, also might involve temporary movable dynamic RSUs.

based attacks. At most, it needs to be able to generate messages with new timestamps to avoid replay attacks. However it can be easily fitted with a real-time clock.

Similarly, a CSW RSU does not need to be mobile. It can always advertise the same position and curve data. In fact, it does not even need a GPS unit, since it can be programmed with its current position in an external fashion. (Although one might fit the RSU with a GPS as a fail-safe mechanism to ensure that it has been installed in the right location). For instance when the RSU is programmed with its curve speed information, it might also be programmed with its own position.

Dynamic Devices

The TSVW application scenario illustrates another kind of RSU, the dynamic RSU that transmits dynamic content. Unlike the CSW RSU, the TSVW RSU needs to know external states, in this case the traffic signal phase and timing information. It must, therefore, be able to generate some variety of messages containing different timings and phases. Like a CSW RSU, a TSVW RSU does not need to be mobile, since traffic signals are in fixed positions. However, one might imagine that some kinds of dynamic RSUs would move, e.g., construction work signals.

Common Limitations

Both kinds of RSUs share some limitations. Note that since the connection between any given RSU and its message is readily apparent, there is no requirement for RSU privacy. In addition, any given RSU only needs to be able to generate a fairly narrow class of messages. For instance, there is no need for a TSVW RSU to be able to generate messages containing maximum curve speed.

2.7 Attacker Capabilities

In the traditional *Internet Threat Model* (ITM), it is assumed that the attacker has complete control of the network but limited control of the end nodes. Rescorla and Korver write [4]:

The Internet environment has a fairly well understood threat model. In general, we assume that the end-systems engaging in a protocol exchange have not themselves been compromised. Protecting against an attack when one of the end-systems has been compromised is extraordinarily difficult. It is, however, possible to design protocols which minimize the extent of the damage done under these circumstances.

By contrast, we assume that the attacker has nearly complete control of the communications channel over which the end-systems communicate. This means that the attacker can read any PDU (Protocol Data Unit) [message] on the network and undetectably remove, change, or inject forged packets [messages] onto the wire. This includes being able to generate packets that appear to be from a trusted machine. Thus, even if the end-system with which you wish to communicate is itself secure, the Internet environment provides no assurance that packets which claim to be from that system in fact are.

Unfortunately, this model of attacker capabilities is not completely applicable to the VSC case. In particular, VSC OBUs will be very widely distributed -- in the best case, one in every vehicle -- and so we must assume that some units will become compromised. Moreover, the trust issues involved in VSC are substantially more complicated than those of traditional e-commerce systems. In ordinary Internet systems, once one has generally authenticated the peer, one can establish which messages it is permitted to send and ignore others. In the VSC system, however, there are situations where authenticated peers can send messages that are potentially legitimate but actually malicious.

In addition, it may be necessary to reconsider the assumption of complete control of the network. This assumption is not entirely realistic in the Internet setting and is less realistic in the VSC setting due to the characteristics of wireless data transmission. Depending on the security service that we are attempting to achieve, this may be an asset or a liability.

Finally, we need to consider the likelihood that the VSC system will face multiple attackers with varying capabilities. Rather than design a system that must be immune to all attackers, we shall focus on designing a system that intentionally presents different levels of security to attackers with different capabilities.

We consider four types of attackers, roughly in order of increasing capability:

1. Attackers with a programmable radio transmitter/receiver;
2. Attackers with access to an un-modified VSC unit (with an intact tamper seal), either OBU or RSU;
3. Attackers who have access to a modified VSC unit and who have obtained the keying material; and
4. "Inside" attackers who have access to records and equipment operated by the vehicle manufacturer or the VSC unit manufacturer.

In the rest of this document, we will be referring to these attackers as "Class 1", "Class 2", etc.

In the next four sections we describe each type of attacker and the type of attacks they might be able to mount. Note that we explicitly assume that attacks on the GPS satellites and base stations are outside the scope of this task. If an attacker can compromise GPS, the consequences will extend far past those on this task.

2.7.1 Class 1: Attackers with Programmable Radio Transmitters/Receivers

The most limited kind of an attacker is one with a programmable radio transmitter/receiver. This might be a modified 802.11 radio, a hand-built hardware device, or a software-defined radio. In any case, we assume that such an attacker can receive all VSC messages in his area as well as generate any number of legitimate-appearing VSC messages. He will also be able to broadcast with effectively unbounded signal power.

Class 1 attackers do not, however, have access to any VSC keying material. Thus, essentially any communications security measures whatsoever will keep them from mounting forgery attacks. However, there are still a number of attacks they could potentially mount.

Replay/Tunneling

Although a Class 1 attacker cannot craft or modify messages, they can quite easily arrange for them to appear at a different point, either in time or space. Thus, an attacker can store a message and retransmit it at a later time, amplify a message so that it appears in a distant location, or both. Protecting against this attack clearly requires that receiving units have a verifiably correct idea of where they are and what the current time is and use that to reject expired or irrelevant messages.

Denial of Service

The most straightforward attack for a Class 1 attacker to mount is a DoS attack. The simplest kind of DoS attack for such an attacker is simple radio jamming. Since a Class 1 attacker can have a network transmitter of essentially unlimited power, it is fairly straightforward to prevent all transmissions from being received. There are also a number of more sophisticated DoS attacks on 802.11 [5].

In addition, it is very easy to perform "selective jamming" on an 802.11 system: the attacker listens to enough of the message to know if he wants to let it go though. If not, he transmits during the 2nd part of the message transmission. In this way, he controls what part of the overall state gets through.

There are a large number of other potential DoS attacks. For instance, one could simply flood the network with transmissions. This will not only crowd out other valid transmissions but also potentially consume prohibitive amounts of CPU time on the receiving side as the receivers attempt to verify the transmission's validity. Finally, one could simply physically damage a unit so that it couldn't provide any service whatsoever.

RF Fingerprinting

Even a Class 1 attacker can mount a substantial privacy attack by means of *RF fingerprinting* [6]. Even in mass-produced units, radios have characteristic emissions profiles. It is generally possible to distinguish one radio transmitter from another by use of these emission profiles. Thus, an attacker who can observe the emissions of a given vehicle can then subsequently identify that vehicle by its transmissions alone. We will investigate the difficulty of this attack before the solution phase.

Remote Compromise

Even the best security implementations occasionally contain programming flaws. If those flaws are in the early message verification and processing code, then a Class 1 attacker might be able to compromise the security implementation and thus the VSC unit. Note that such an attacker could presumably only exploit code in the security layer, since it cannot generate messages that will pass the initial security checks.

A remote compromise of this type can often be used to gain control of the entire unit. In such a scenario, the attacker would effectively be a class 3 attacker, but without needing to break the tamper seal.

Remote Management

It is expected that in some cases RSUs will be remotely manageable, either via the Internet or wireless channels. In such cases, there is obviously a concern that an attacker will send false management messages. This sort of remote authorization and access control is a standard security problem with many well-known solutions. The most appropriate solution will need to be determined during the solutions phase.

2.7.2 Class 2: Attackers with Access to an Unmodified VSC Unit

Unless measures are taken to control access, it will in general be very easy for attackers to obtain VSC units. Most likely the attacker can obtain an arbitrary number of OBUs from junked vehicles but, in the most expensive case for the attacker, they can simply buy them along with a used vehicle. Initially, the price per VSC-enabled vehicle will be high (because they are newer), but the price will come down quickly if VSC units are available in most new vehicles.

Obtaining RSUs will probably be even easier, since it is assumed that they will be embedded in unattended roadside devices. Thus, our threat model needs to assume that an attacker will be able to obtain either an OBU or an RSU. In this section we consider the capabilities of a Class 2 attacker, who has a VSC unit but has not broken the tamper seals in order to compromise the CPU or keying material.

Change of Location

The most straightforward attack on an RSU is simply to move it. One might, for instance, take a stop sign transmitter and move it to another location, where it forces people to stop. This has a similar result to the tunneling attack described above, but is executed differently. It could potentially be combined with the indicator mismatch attack, described below.

Indicator Mismatch

A number of the infrastructure-to-vehicle services are designed to inform the user about the state of some piece of infrastructure. For instance, the TSVW application scenario is intended to represent the state of a traffic signal. Even if the VSC unit itself is undamaged, it is trivial for the attacker to change the state of the signal itself. For instance, one could rewire the traffic signal so it believes it is emitting a red signal but really is emitting green.

The danger here is that users of VSC might come to rely upon VSC to get information about the state of the world. To the extent that there are multiple indicators, some VSC-based and some legacy, there is a potential for damaging misunderstandings. Consider, for instance, the following scenario, shown below in Figure 6.

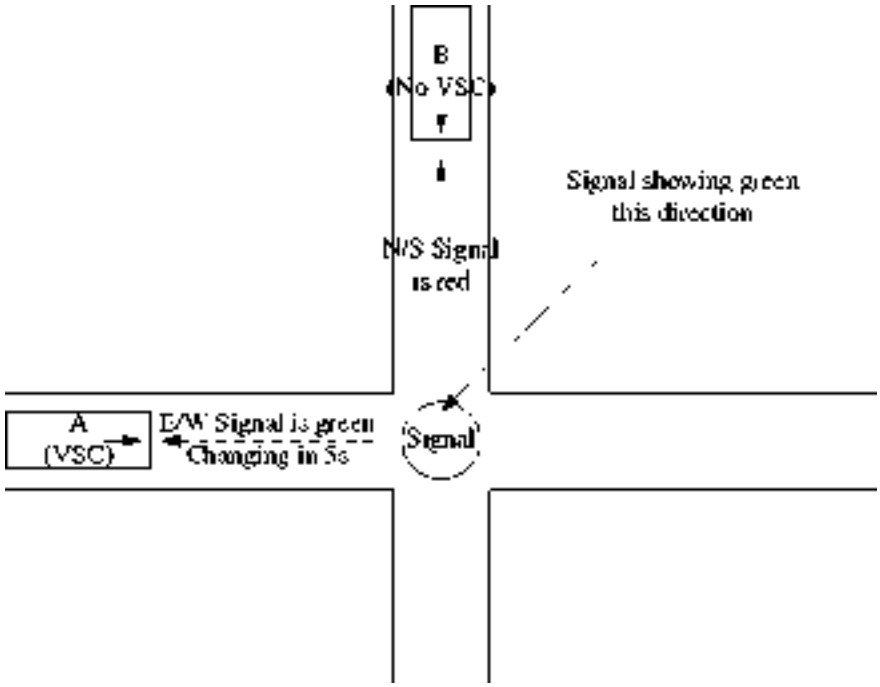


Figure 6: Signal/Message Conflict

In Figure 6, Vehicle A is VSC-enabled and Vehicle B is not. The attacker has tampered with the traffic signal so that the RSU and the actual signal are out of phase. Thus, B has a green signal and A does not see a TSVW warning. If A has a careless driver, he might rely on the fact that he has not seen the warning and not notice that the signal was in fact red. There is thus a potential for a collision. It is worth noting that this sort of scenario

can be created even without VSC, simply by wiring both indicators to be green. However, to the extent to which users trust VSC and their behavior becomes more aggressive due to the fact that they know it is active, we might expect that the problem would be worse in the case of this attack. In addition, if this attack is mounted by making both lights green, this is immediately and visibly obvious, whereas it is less obvious to detect when the VSC and visual signals conflict.

Sensor Spoofing

In our strawman design, we assume that the physical sensors (accelerometers, brake sensors, radar, etc.) are outside the tamper boundary. As these sensors often need to be in specific, physical locations this seems very likely. However, this opens up a variety of possible attacks. Provided that the attacker can generate the correct sensor inputs, he can use the VSC unit as an oracle to generate whatever false messages he desires.

A simple example of an attack using this technique can be found in the EBL service. The attacker modifies his vehicle to spoof the accelerometer and brake pedal sensors, and drives along the highway. He then waits until he is in front of the victim and sends braking signals to the OBU. The OBU, in turn, generates a valid emergency braking message over the air interface. The OBU behind the attacker receives the message, concludes it needs to brake, and informs the driver.

GPS Spoofing

Both OBUs and RSUs are potentially susceptible to a GPS-spoofing attack. Although we have assumed that the GPS is within the tamper boundary, GPS receivers rely upon radio transmissions to determine their position. With sufficient effort it may be possible to convince the GPS receiver that it is in an arbitrary location at an arbitrary time simply by supplying the correct signals to its antenna input. We will investigate the difficulty of this attack before the solution phase.

If the attacker can use the GPS to convince the VSC unit that it is in a different location or at a different time, then he can use it to generate an arbitrary number of messages with a time and date stamp of his choice. There are a large number of attacks that can be mounted via this mechanism. GPS spoofing attacks are particularly damaging when combined with sensor spoofing attacks. With GPS spoofing, an attacker can mount the fake braking attack described above but without even being in his vehicle--or with a powerful enough transmitter, even in the area.

2.7.3 Class 3: Attackers Who Have Recovered Keying Material From a VSC Unit

No matter how good a tamper seal is attached to the VSC unit, a sufficiently dedicated attacker is likely to be able to extract the keying material. In addition, an attacker might be able to exploit bugs inside the VSC unit code to compromise the unit without violating the tamper.[2] Accordingly, we need to consider attacks in which the attacker has compromised a VSC unit and recovered the private key and/or whatever temporal keying material is inside.

[2] It is not currently known how to extract the keying material of FIPS 140-1 level 4 certified tamper-resistant devices. However, it is expected that it is technically possible. Moreover, it is likely that level 4 protection will be cost prohibitive for VSC.

In general, a Class 3 attacker can mount any attack that a Class 2 attacker can mount.[3] In addition, a Class 3 attacker can generate essentially any message that the VSC unit could have generated.

Duplication

The most important capability that a Class 3 attacker has that a Class 2 attacker does not is that he is no longer subject to the constraint that he needs the VSC unit. Thus, he can easily build any number of compromised units for the one time cost of breaking a single VSC unit.

Physical Law Violations

Another capability that a Class 3 attacker has that a Class 2 attacker does not is the ability to generate completely incoherent message sets. For instance, a VSC unit can be programmed to know that time cannot run backwards, whatever the GPS input says. Similarly, the VSC unit can be programmed to know that position changes that exceed 500 mph are physically impossible and reject such input. Thus, one could conceivably program the unit with implausibility checks to refuse to generate messages that imply implausibly high velocities. The details of such filters should be investigated in future VSC-related work. By contrast, because a Class 3 attacker has access to all of the keying material, he can generate any messages he chooses, including those with implausible physical counterparts.

Increased Ability to Compromise

Another consequence of the Class 3 attacker's ability to generate any message is an increased ability to exploit programming errors in other VSC implementations. We expect that the first check that a VSC implementation will do upon receiving a message is to verify the MI/OA properties. Since other attackers have quite limited message sets they can generate, the chance that they can exploit bugs in the message processing code is fairly low. They must focus their attacks on the cryptographic code. By contrast a Class 3 attacker can always generate a message that will pass the MI/OA check and thereby exploit bugs in the message processing code.

2.7.4 Class 4: 'Inside' Attackers

The final class of attackers is referred to as "Insiders." VSC units need to be manufactured, and an attacker who is employed by the OBU/RSU manufacturer would have substantial leverage to mount additional attacks. There are actually two groups of Class 4 attackers: authorized and unauthorized. An authorized attacker would be one who was operating with the consent of the manufacturer. An unauthorized attacker would likely be a disgruntled employee. Since the capabilities afforded to an authorized insider are a superset of those offered to an unauthorized insider, we will focus our analysis on authorized insiders.

The primary additional capability that an inside attacker has is access to the KDC and the customer records. He can potentially use this to extract keying material or get a list of all units, their owners, and whatever identifying information is known. This allows him to mount a number of attacks.

---

[3] One exception here is that one could imagine placing the radio inside the tamper boundary and hope that when the tamper is violated it disables the radio or at least alters its fingerprint. In such a case, a Class 3 attacker could not mount Class 2 attacks if RF fingerprinting is used as part of the authentication system. We will not fully consider this issue here, since placing the radio inside the tamper is probably prohibitively expensive, and it is doubtful that fingerprinting technology is cost-effective to be used in every receiver.

Key Extraction

In the strawman scheme of Section 3.5, an attacker who controlled the KDC would likely be able to obtain a copy of the current group key K_i. Such an attacker would effectively have the capabilities of a Class 3 attacker. Because this sort of attack is not in the interest of the manufacturer, we assume that this sort of attack is primarily limited to unauthorized attackers. Similarly, an attacker who purchases keying material from an insider can become a Class 3 attacker.

Cryptographic Attacks on Privacy

If the OBU/RSU manufacturer maintains a database of all units manufactured and their public keys, then an authorized attacker is in a position to mount a number of attacks. In the strawman scheme described in Section 3.5, the scope of these attacks is somewhat limited. Since all units use the same group key, access to the keying material does not allow unit identification. However, the attacker could still determine a user's rough location when they request a new K_i. Depending on how often K_i is changed, this might provide fairly high-resolution information.

Some other cryptographic schemes provide much more information leakage. For instance, one commonly proposed scheme is Group Signatures [7,8]. In such schemes, there is an escrow agent that can map any signature to the private key that signed it. With such a scheme and a key-VIN database, a Class 4 attacker could potentially identify any entity.

RF Fingerprinting Database

If the manufacturer maintains an RF fingerprint of each unit, a Class 4 attacker would potentially be able to identify any unit by its fingerprint, as opposed to just tracing a given fingerprint, as a Class 1 attacker could. A database mapping fingerprint-to-VIN would be ideal for this purpose. The appropriate level of protection against this form of fingerprinting attack will need to be determined during the solutions phase.

Attacker Type	**Attack**
Class 1	Replay/tunneling Denial of service RF fingerprinting Remote compromise Remote management
Class 2	Change of location Indicator mismatch Sensor spoofing GPS spoofing
Class 3	Duplication Physical law violations Increased ability to compromise other units

Class 4	Key extraction Cryptographic attacks on privacy RF fingerprinting (with database)

Table 1: Summary of attacker types and attacks

2.7.5 Some Out Of Scope Threats

There are a number of attacks on the system that are out of scope for this task. These are described below.

Physical DoS Attacks

It is clearly possible to mount a DoS attack on any OBU or RSU simply by depriving it of power, physically damaging it, destroying it, etc. The solution to this kind of problem is physical hardening. We will not address this kind of problem here.

Radio Jamming

As discussed in Section 3.7.1, it is quite possible to build a radio transmitter that will make the entire 802.11 network-- or specific units--unusable. Since we rely on the 802.11 network, these attacks are out of scope for us.

Attacks on the GPS System Infrastructure

An attacker who could compromise the GPS satellites or base stations could easily change any unit's idea of position. We do not address security for the GPS system. At the present time, there is no way of authenticating GPS messages. However, we expect that units will need some set of heuristics to assist in detecting false GPS information. During the solutions phase we will attempt to determine some such heuristics.

Software-Based Compromise of Units

The OBUs and RSUs will contain software that processes network traffic. In many cases it is possible to mount attacks on such software that allows one to take over such systems. We advise that secure programming practices, such as those described by Viega and McGraw [9], be used when developing VSC units. As this kind of protection is a software issue and not a communications issue, it is out of scope for this task. Containing compromise of such units is, however, in scope.

Misconfiguration (Accidental or Intentional)

In many cases, RSUs must be configured when they are installed. For instance, a CSW RSU must be programmed with the characteristics of the curve that it is providing information for. In some such cases, the personnel in charge of inputting that information will make errors. Intentional misuse is also possible and should be guarded against. However, defenses against all such attacks are out of scope for this task.

2.8 Containing Compromise

Finally, we turn to the issue of dealing with compromised units. There are two basic strategies for containing compromise:

- Proactively limit the capabilities of a unit in order to minimize the effect of compromise.

- Reactively contain a compromise once it has occurred.

We consider each approach in turn. The purpose of this section is not to describe solutions but merely to explore the potential parameters of a solution and the implications of various design choices.

2.8.1 Proactive Containment

The basic principle of proactive containment is to limit capabilities. As described in Section 3.6, not all VSC units need to have the same capabilities. Since every additional capability that a unit has is a new capability that an attacker might employ, limiting unit capabilities proactively contains potential compromises. For our purposes, the two most important role separations are those of unit type and mobility.

2.8.2 Discriminators for Compromised Units

The reactive way to contain compromise is to identify and isolate compromised units. Strictly speaking, what we wish to achieve is not to *identify* compromised units but rather to isolate them. Thus, it is not necessary to identify which units have been compromised but merely to have a way to reject messages from such units in the future. Thus, what we concern ourselves with here is obtaining a *discriminator* – a piece of information which is sufficient to reject future traffic from such units. In general, however, it seems likely that such a discriminator will in fact be the unit's identity.

The problem, then, is for the Security Officer to derive a discriminator. We consider several types of information which one could potentially use for this purpose:

- Some set of messages that are deemed to be bad (apparently valid, but incorrect).
- The identity of the compromised unit (e.g., a serial number).
- The revealed private key of the compromised unit.
- The compromised unit itself, if one has physical possession of it.

Once the SO has derived a discriminator, the next stage is to somehow contain the compromised unit. There are a number of possibilities, ranging from simply telling the compromised unit to shut down (which only works with Class 2 attackers) to compiling compromised unit lists to denying the compromised units keying material. These options will be fully explored during the solution phase.

2.8.3 Residual Capabilities of Compromised Units

Our objective for containing compromised units is primarily to stop them from transmitting false information. However, compromised units will still be able to receive transmissions. As the current threat model does not include confidentiality, such attackers will have essentially the same capabilities as any Class 1 attacker.

3 Constraints

3.1 Introduction

This was the second step in the security effort for the VSC project. The first step described the VSC threat model: the capabilities of potential attackers and the types of attacks such an attacker might able to mount. This section describes the external constraints that a proposed solution must take into account.

Any engineering project is a compromise between the desirable features of the design and the constraints on it. The threat model enumerates the desired goals. This section enumerates the constraints on the design. The primary concern when introducing security is that it imposes additional overhead, for example:

- cryptographically secured messages are larger than ordinary messages
- hardened security modules are larger than ordinary computers and may consume more power
- dedicated security processors are likely to add cost to units
- security systems require management which may be expensive

A security system design must take all of the related boundary conditions into consideration if it is to be successful, or it runs the risk of being un-deployable. Note that the constraints listed below are the most accurate that the security team was able to determine, though in some cases they are accurate only to an order of magnitude. The constraints described in this section represent boundary conditions only, and must not be interpreted as specifications. They are accurate enough for this security study, but they are not meant to be used for any other purpose.

Network characteristics – The VSC security solution must operate in a network environment defined by the DSRC protocols. The solution must operate within the communications and timing parameters provided by that network.

Environmental characteristics – The VSC security solution is designed for deployment either in vehicles or as part of infrastructure devices. These environments present constraints in terms of power consumption, heat, form factor, etc.

Cost of goods – VSC units, whether *On-Board Units* (OBUs), *Road Side Units* (RSUs), or *Management Devices* (MDs) must be manufactured. The cost of goods must be kept within certain acceptable limits.

Management costs — The final VSC system will require management and maintenance, both of the system itself and of the deployed devices. Again, these costs must be kept within acceptable limits.

In the remainder of this section, we consider each form of constraint. In Section 5, which illustrates a proposed VSC architecture, we will explore options for producing a system that provides the security guarantees described in Section 3 while still meeting as many of the constraints described here as is practical.

3.2 Network Characteristics

Vehicle safety communications will be operating over an 802.11-based ad hoc wireless network. The network operates at variable data rates, ranging from 3 Mb/s to 27 Mb/s. The range of the network is approximately 300 meters in light traffic situations and 800-1000 meters without traffic or obstructions.

3.2.1 Total Number of Units

Security management overhead can depend on the number of total units in the VSC system. For our purposes (and our purposes only), we estimate that there will be on the order of 10^9 units in the United States (four times the number of vehicles in the US today) and 10^{10} units in the world as a whole (about 1.5 times the world population today). These are, of course, very approximate numbers. They are best-guesses for the order-of-magnitude number of units, and they are accurate enough for the purposes of this security task. Since the system design must consider long-term interoperability, the security system must assume full deployment, even if this constitutes overkill at first deployment; one security system for low penetrations to then be retrofitted as the deployed population grows would be difficult and/or unmanageable.

3.2.2 Maximum Data Rate

The most basic constraint that we must accept is the data rate of the channel. This presents a hard upper bound on the amount of data that must be processed by a receiving VSC unit. We assumed a maximum data rate of 6 Mb/s, which is the nominal rate of the "control channel" over which data related to safety applications will be flowing. The system should be able to handle bursts of 27 Mb/s, but need not necessarily process it all in real time.

3.2.3 Packets Per Second

An additional boundary is the number of packets per second that an implementation must have the potential to verify. Given the above network constraints, we estimate that this number is 4000 packets per second (pps) for a data rate of 27 Mb/s.[10] At 6 Mb/s, the packet rate is approximately 2500 pps. Note this need not necessarily happen in real time. Low priority messages may be handled out of order.

3.2.4 Latency

A critical question is that of latency. In order to be useful, application messages need to be delivered within a reasonably short time after they are transmitted. The exact time varies by application. Based on protocol research thus far, we assume a maximum allowable latency of 100 ms, which would include all of the time between when the data to be sent from the sending vehicle is collected and when the receiving vehicle has an opportunity to react to the received data.

However, the communications system itself introduces some latency. Thus, the total amount of latency introduced by the security layer must be less than the total allowable latency minus the communications latency. Based on results from the VSC protocol research activities, we estimate that communications latency is approximately 10 ms, and that we should conservatively design the security layer to have equivalent latency. Note that this is total latency, including both data transmission costs and data verification costs.

There may be applications developed in the future that could benefit from the VSC units' ability to route messages. In the instance of stationary RSUs, some RSUs may be physically connected to a network by wire, or occasionally through a management console, in order to receive information updates. This RSU could forward information to other RSUs within transmission range and request that the other RSU forward messages to yet another set of RSUs. In this instance, the RSU may know *a priori* which RSUs are its neighbors or will have sufficient time to discover them through some neighborhood discovery algorithm. The latency introduced during discovery and maintenance of routes in this RSU-RSU routing scenario should not impose constraints. However, packet forwarding does impose latency. We are assuming that no time-critical applications will require RSU packet forwarding.

In the case of routing among stationary OBUs, applications may include the location of a vehicle in a large airport parking lot, finding a parking spot in a crowded city, etc. The main issue is that in stationary OBU-OBU routing, the latency introduced by neighborhood discovery and maintenance again must not create a problem. We are assuming that no time-critical applications will require packet forwarding by OBUs or of OBU messages.

3.2.5 Packet Loss Rate

DSRC provides a broadcast channel with no guarantee of delivery. Therefore, we must assume that some packets will be lost. Based on simulation results so far, a broadcast's effectiveness ranges from 80% to 50% for a range from nearby to 100 meters away, under stressful but not excessive channel conditions. Of course, these numbers are highly dependent on the actual parameters in the simulation, such as transmission power, packet size, vehicle density, etc. In general, it is unlikely for a broadcast to be more than 90% successful at the intended communication range under stressful load. Conservatively, we will assume an 80% packet loss rate.

3.2.6 Packet Size

In order to maximize bandwidth usage and reduce processing overhead, we need to ensure that the security layer does not add excessive overhead to packets. Based on simulations run during the VSC protocol research activities, we assume final packet size no larger than 200 bytes for most packets, with at least 100 bytes of that used for application data. Therefore, the target is to have no more than 100 bytes of security information carried in most packets. Note that this does not mean that packets larger than 200 bytes can never be used. Larger packet sizes may be valuable for setup and management purposes. However, the typical packet size for safety messages should be less than 200 bytes.

Constraint type	**Constraint value**
Aggregate bandwidth	6 Mb/s
Maximum received packets/second	4000
Maximum allowable latency	100 ms
Maximum network latency	10 ms
Maximum packet size	200 bytes

Table 2: Summary of Network Constraints

3.3 Environmental Characteristics

The environments in which OBUs and RSUs must be deployed impose certain physical constraints. For instance, OBUs must be small enough to fit into a vehicle, must not draw too much power, etc. This section describes some potential environmental constraints for the purposes of this security study. Individual end-user requirements may differ. In general, these constraints will be different for OBUs and RSUs.

3.3.1 Unit Size

RSU

RSUs are embedded in a variety of devices. The smallest likely such device is a road sign or traffic signal. Thus, RSUs should be able to fit in a form factor approximately 30 cm x 20 cm x 10 cm. This restriction applies to the entire VSC device, including security but not including antennas. We anticipate that RSUs will be able to mount substantial antennas in order to adapt to their installation environment.

OBU

As OBUs are fitted inside the vehicle, they need to be relatively small. OBUs should be able to fit in a volume of approximately 500 cm^3. It is unlikely that they will need to be thinner than 1.5 cm. This restriction applies to the entire VSC device, including security but not including antennas.

3.3.2 Temperature Range

RSU

RSUs need to be safely deployable in the most extreme weather conditions found in roadside environments. Therefore, they should be operable in the range -40 to +85 C.

OBU

OBUs need to meet the same temperature tolerance standards as other pieces of vehicle electronics and instrumentation. In general, this is -40 to +125 C. If necessary, it may be possible to place the OBU in a protected environment, in which case the operating range would be approximately -20 to +70 C.

3.3.3 Heat Output

RSU

RSUs can typically be placed in ventilated environments. Therefore, the practical limits on RSU heat evolution are those for general purpose computers. We have somewhat arbitrarily chosen a target of 50W.

OBU

OBUs need to meet the same heat output standards as other pieces of vehicle electronics and instrumentation, which is on the order of 10W.

3.3.4 Power Consumption

RSU

RSUs generally draw less than 100 W. The peripheral equipment (e.g., sensors) usually draws far more power than the radio unit, according to industry representatives from the DSRC standardization group. As solar powered units are generally installed where plenty of sun is available, they can be assumed to have plenty of power. We have somewhat arbitrarily chosen a target of 50 W for RSUs.

OBU

OBUs must run off the vehicle battery and alternator, like any other electronic device in the vehicle. Unfortunately, acceptable power draws vary widely. We are assuming the following parameters as typical, though of course each automaker has independent

specifications. The numbers below are used only as boundary conditions and only for the purposes of this security study.

Max current draw	30-100 mA
Typical current draw 7	0% of max
Sleep mode current draw (vehicle off)	<1 mA
Supplied voltage (vehicle off)	12 V
Supplied voltage (vehicle on)	14 V
Operating voltage	9-16 V

Constraint	RSU value	OBU value
Unit size (cc)	6000	500
Temperature range (degrees C)	-40 - +85	-40 - +125
Heat output (watts)	unlimited	10
Power consumption	unlimited	30-100 mA at 14 V

Table 3: Summary of Environmental Constraints

3.4 Cost of Goods

The various devices in the system must be manufactured. The cost of these devices must be factored into the overall cost of the units in which they are embedded. This section discusses assumptions regarding those costs for the purposes of this security study only.

3.4.1 RSUs

Without security, road-side units used for currently-deployed systems such as toll collection and traffic monitoring cost about $10,000-20,000. According to members of the DSRC standards writing group, efforts are currently being made to bring the price down to approximately $200-$500 ($1000 for high-end units). Security should add less than $200 to the cost of the unit.

3.4.2 OBUs

The maximum acceptable cost of an OBU is assumed to be approximately $100, and security should add less than $50 to the cost of an OBU. Preferably, the additional cost would be less than $25.

3.4.3 Management Consoles

RSUs are expected to be field-manageable and perhaps remotely manageable. Field and office personnel will need to be issued management consoles. These management consoles need to be able to securely communicate with RSUs. The maximum cost of the management consoles should be less than $10,000.

3.4.4 Service Consoles

In some cases it may be necessary for service personnel such as auto dealers to maintain OBUs. Currently, service personnel are required to purchase substantial tooling from the manufacturers,

at costs of up to $10,000. Therefore, we believe that such OBU maintenance stations could cost up to $10,000.

3.4.5 Manufacturing Facilities

In order to avoid the construction of fake OBUs, OBUs must be manufactured in secure facilities. The security requirements for those facilities should not increase the fixed cost of facilities by more than 25 percent.

3.5 Management Costs

Any large-scale security system requires some management and this system is no exception. These management costs are borne by a variety of parties, ranging from OEMs to transit agencies. This section discusses assumptions regarding management costs for the purpose of this security study only.

3.5.1 Investigation of Compromise

Containment of compromised units is a design goal of the system. When such a compromise occurs, it is first necessary to derive a discriminator for the compromised unit. Such a discriminator can then be used to shut the compromised unit out of the system. The likely scenario is that a unit is compromised, and then the attacker uses the compromised unit maliciously. An investigation must then be mounted to derive the discriminator.

The potential cost for such an investigation is naturally dependent on the size of the attack. For a major accident, we estimate the cost to be on the order of $20,000 for the VSC portion of the investigation (and misuse of VSC would have to be suspected for it to be investigated). For traffic disruptions, we roughly estimate that if a disruption is suspected of being caused by malicious use of VSC, the cost of the investigation would be less, perhaps on the order of $5,000.

3.5.2 Key Infrastructure

OBUs are likely created with their keying material installed, making management relatively simple. However, in the proposed model, RSUs generally will be using a conventional public key infrastructure. Thus, a hierarchy of authorities will be required to certify RSUs as well as other certificate authorities. The distribution of these costs depends on the PKI architecture.

The topology of the PKI impacts on efficiency and ease of deployment. The PKI is primarily responsible for the issuance of digital certificates and revocation information. Certificate Revocation Lists (CRLs) are the most common form of revocation information. For RSUs, the naming structure is assumed to be hierarchical, based on geopolitical areas. For example, an RSU might have a name like *C=US*, *S=VA*, *L=Fairfax County*, *CN=RSU 10048*. A name like this can be accommodated under several different PKI topologies. We need to consider two major alternative architectures *hierarchical* and *flat*.

Both Public Key Infrastructure topology options are described below.

Hierarchical PKI

The PKI topology mirrors the levels in the naming hierarchy. For example, the U.S. DOT might operate a CA for the top level, issuing certificates to each of the States. Then, the States operate CAs, and they issue certificates to each of the counties and cities within the State borders. Finally, the local governments operate CAs, and they issue certificates to the RSUs.

This alternative appears to directly match the expectations of most people familiar with governmental structures. A single trust anchor is needed to represent each country. A

superior international organization could be created to serve as the top-level CA, but it would impose additional efficiency concerns.

This hierarchal structure imposes a burden on the OBU. Using the above example, four signature validations are needed to verify a message from RSU 10048. They are:

1. Validate the signature on the VA certificate with the U.S. DOT public key.
2. Validate the signature on the Fairfax County certificate with the Virginia public key.
3. Validate the signature on the RSU certificate with the Fairfax County public key.
4. Validate the signature on the message with the RSU public key.

Further, revocation information provided by each of the CA ought to be checked. If CRLs are employed, three addition signature validations are needed. Each of the CRLs ought to be small since each CA is not responsible for a large number of certificates.

Deployment requires each of the superior organizations to be operational prior to a subordinate governmental entity. Therefore, Fairfax County cannot install their first RSU until the U.S. DOT and the Commonwealth of Virginia are both fully operational.

Flat PKI

A single CA issues all of the certificates within a nation, but the naming hierarchy is unchanged. For example, the U.S. DOT operates the CA for the top level, but it accepts requests for certificates and revocations from authorized registration authorities (RAs) in each of the States, counties and cities. The process for authorizing RAs will likely follow the natural governmental structure, but once authorized, the RA can communicate directly with the CA.

All of the management concerns are transferred to the RA registration process. And, the CA is responsible for ensuring that one local government cannot request certificates that are affiliated with other jurisdictions.

This flat structure reduces the burden on the OBU. Using the above example, two signature validations are needed to verify a message from RSU 10048. They are:

1. Validate the signature on the RSU certificate with the CA public key.
2. Validate the signature on the message with the RSU public key.

Revocation checking can be problematic in this structure, since all of the revoked certificates are listed in a single CRL. While only a single signature is needed to validate the CRL, the number of entries on that CRL can become quite large. A large CRL takes significant bandwidth to download. This concern might be mitigated by performing the download at gas stations where the vehicle is stationary.

Deployment only requires the national CA to be operational. Therefore, Fairfax County cannot install their first RSU before the Commonwealth of Virginia has installed any capabilities, assuming that the registration process can be accomplished by paperwork.

This alternative has an additional concern. The national CA must be highly available. In the first alternative, the outage of any single CA has very little impact on the overall system, but in this alternative, an outage in the national CA can have major ramifications. Therefore, an architecture that includes concurrent operations from multiple physical locations is needed, making the national CA more expensive in this alternative.

3.5.3 Management of RSUs

Unlike OBUs, RSUs require substantial management. For instance, a transportation agency might want to change the settings on a curve speed warning RSU in order to accommodate changing road conditions. This sort of remote management incurs costs. In general, management will be performed by personnel with minimal computing background training, and it must be performed quickly. Reprogramming an RSU with new parameters should be possible in less than 30 minutes.

4 Architecture

4.1 Introduction

The previous two sections described the VSC threat model and system constraint assumptions. This section describes some of the possible architectural options for the VSC Security System. A full protocol based on these architectural elements is described later in Section 6 of this report.

This chapter describes the high-level security architecture that was developed to address as many of the threats identified in Activity 2 as possible, while still fitting within the constraints identified in Activity 3. The purpose of this security architecture development was to create a "cryptographic skeleton" design, showing the various communicating parties, the message flows, and the cryptographic transforms to be used.

4.2 Architecture Summary

The different privacy and security assumptions of RSUs/PSOBUs and OBUs result in different security strategies. A standard PKI strategy for RSUs/PSOBUs was assumed, and a variety of strategies for providing authentication for OBU messages were described. After much consideration, Anonymous Certificates were identified as the most promising OBU authentication strategy.

Security that meets the requirements described in the threat model imposes significant constraints. With the currently proposed architecture, which includes many optimizations, each message transmitted would include significant overhead, and the message signatures would take time to process once they are received. Management of a Public Key Infrastructure for RSUs would also be necessary, according to the proposed scheme.

Two major decisions are:

1. What PKI structure to use for RSU authentication, and
2. Which signature algorithm to use for message authentication.

ECDSA has been recommended, but it is not the only alternative. The protocol design proceeded assuming that ECDSA will be chosen, but with sufficient flexibility to allow future changes.

4.3 Architectural Overview

This section provides an overview of a proposed security architecture, which is then described in detail in subsequent sections.

4.3.1 Key Hierarchy

In order to preserve anonymity for OBUs while still allowing for fine-grained authority control for RSUs, VSC Security could use a dual authentication structure as shown in the figure below. Under this model, consumer OBUs would be authenticated via one set of mechanisms and all other units would be authenticated via another set of mechanisms. This is one possible answer proposed for the purposes of studying the implications of the model and its associated assumptions.

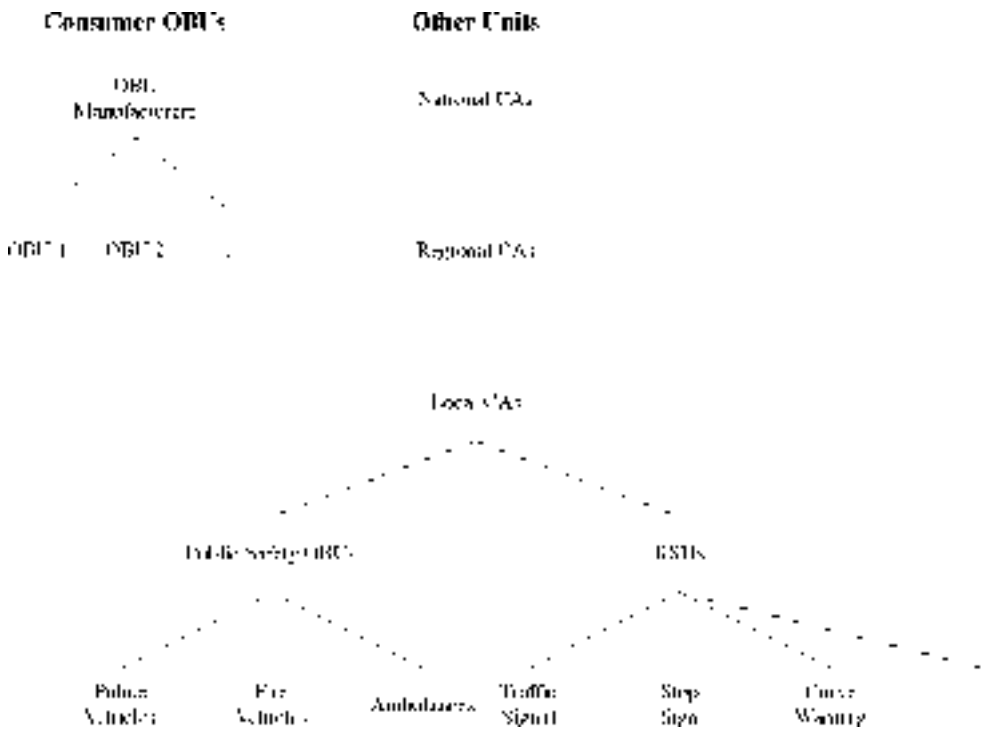


Figure 7: Overview of Dual Authentication Structure

The figure above shows the proposed dual authentication structure. OBU authentication is conceptually simple: OBU manufacturers vouch for OBUs. The RSU authentication structure is the classic hierarchical PKI which maps to the existing political authority structure. National *Certificate Authorities* (CAs) vouch for Regional CAs which vouch for Local CAs, etc. Authentication of OBUs will be done via a privacy preserving mechanism that simply vouches for the fact that the unit is a valid OBU. Authentication of RSUs and public safety OBUs will be done via traditional public key and certificate mechanisms which have been tuned to work well in the constrained VSC environment. Each level of certification is increasingly restrictive. Thus, Regional CAs can only issue certificates for their own regions, local CAs can only issue certificates for their own localities, etc. This limits the amount of damage that compromise of a single part of the authentication hierarchy can do. We describe an alternate structure for RSU authentication in Section 5.3.1.

4.3.2 Communications Architecture

Like other communication systems, VSC is structured as a series of layers, as shown in Figure 8. At the top of the stack is the Safety Application Layer, which is responsible for handling safety-related information. Next is the Security Layer, which is responsible for securing the safety messages. The bottom three layers, DSRC Messaging, 802.11 MAC (Media Access Control), and 802.11 PHY (Physical layer), take care of the actual network data transmission. Messages which are being transmitted move down the stack from the Safety Application Layer to the airwaves. Messages being received move up the stack from the airwaves to the Safety Application Layer.

[4]

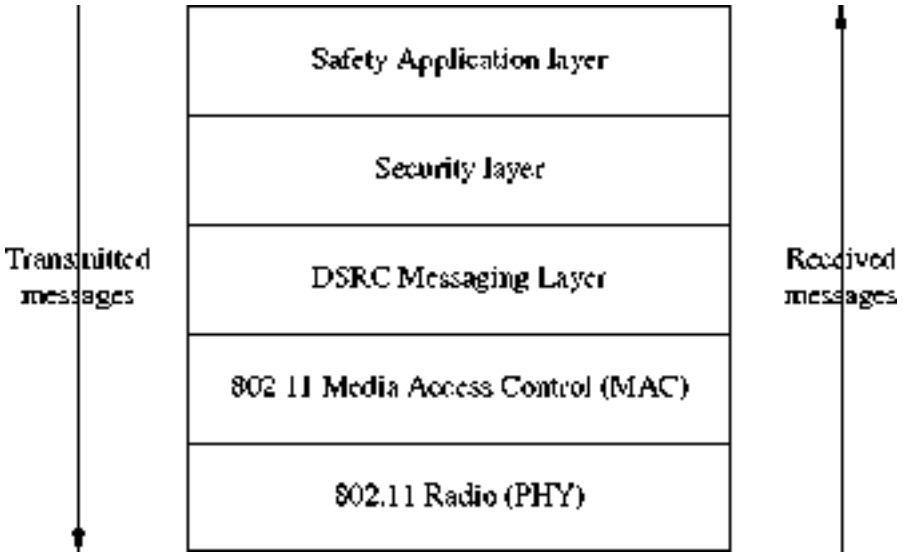


Figure 8: VSC Communications Architecture

4.3.3 Message Authentication

Once OBUs and RSUs have their keying material, they can then transmit messages using DSRC. When a unit wants to transmit a message, it first appends a timestamp and position indicator. These are derived from a trusted source and therefore must be appended by the security layer. It then applies a digital signature using its keying material and attaches the signature to the message along with some kind of key identifier (what kind of identifier depends on the architectural choices described below, but it is obviously some kind of bit string) and broadcasts the message to the receiver using DSRC. Note that we are omitting details like version numbers and algorithm and type identifiers in this presentation.

Figure 9: A protected Message

When a unit receives a message, it uses the key identifier to find the appropriate key to use for verification. The key identifier is typically either a certificate or a key index. If the former, the unit will verify the certificate. If the latter, the unit must already have the key in its cache – we

[4] Note that there has been some discussion of introducing an intermediate channel selection layer in between the 802.11 MAC and the Security Layer. The Security Layer does not provide any integrity protection for this layer.

assume for the moment that it is pre-loaded. (The following sections provide more detail on this point.) Once the key is identified, the unit uses it to verify the signature on the message using the appropriate digital signature algorithm (again, this is covered in more detail later). All of this processing happens in the Security Layer. If the signature is invalid, the message is rejected. If the signature is valid, the receiver verifies that the key used to sign it has the appropriate permissions for the kind of message received. For instance, OBUs are not allowed to send Curve Speed Warning messages. This check may also entail verifying that this keying material is valid for this location. For instance, California RSUs should not be transmitting safety information in Denver. If any of these checks fail, the message is rejected. If they all succeed, the message is accepted for processing.

4.3.4 Management, Revocation, and Updates

Any security system needs periodic updates. These may include:

- *Updated/patched code*. Even the best software inevitably has bugs. The traditional way to fix these bugs is to release new versions of the software with the bugs fixed. Uptake of such patches is slow even with general purpose computers [11] and would most likely be minimal with vehicles if driver intervention is required – people just do not think about having to upgrade their cars. Therefore, a new approach will be needed.
- *Propagation of revocation lists*. It may be necessary to publish lists of revoked (known to be compromised) units.
- *Keying material refresh*. In order to minimize the scope of compromise and the size of revocation lists, it is desirable for units to periodically obtain fresh keying material.

In order to fulfill these needs, it is necessary to have a mechanism for propagating relatively large chunks of data to users. This data would be authenticated via the same sort of mechanisms as ordinary messages, but would most likely not be structured as individual messages but rather as large files split over multiple messages in some fashion. These files will themselves be signed, using, for instance Cryptographic Message Syntax [13].

4.3.5 Fail-Open versus Fail-Closed

Because our design requires that units be periodically updated, the question arises of whether units should continue to function when they are unable to receive updates. For instance, if a unit receives a message from a unit without having a current certificate revocation list, it cannot be sure that the message is from a valid unit and must therefore decide between accepting a potentially invalid message (failing closed) and rejecting a potentially important safety message (failing open).

In this case, how to behave is an implementation decision, although the VSC protocol could require a fail-open or fail-closed behavior as a matter of policy. However, some designs inherently fail-open. For instance, if units need to periodically obtain new keys (e.g., as in the design described in Section 5.5.4.5), then they will be unable to transmit authenticated messages if they do not obtain new keying material, which could be more difficult in low-population density areas (depending on the flooding mechanism and available infrastructure). We believe that in general the system should adopt a fail-open policy. When there is a substantial question as to the validity of a message it should be rejected.

4.4 RSUs and Public Safety OBUs

RSUs and public safety OBUs have no particular anonymity requirement placed on them by the threat model and system constraint assumptions, and can therefore use a straightforward *Public*

Key Infrastructure (PKI)-style solution. PKI is not the only approach that would conceivably work, however it is a standard and well-understood security design, supporting systems as diverse as the Web e-commerce and the Department of Defense communications system. Using standard tools such as PKI allows us to avoid the risks attendant with any new security invention.

In the RSU/PSOBU PKI system, each unit has an asymmetric key pair. The public key is signed by the local CA, and the units use their private key to sign all of their messages. Certificates contain restrictions indicating what sort of messages may be signed using the corresponding key.

Note that upon initial examination it appears attractive to have RSUs do without keying material entirely and merely have them rebroadcast canned messages, e.g., "There is a stop sign at the following geographic coordinates". However, a number of RSU types (such as traffic signals) and nearly all public-safety OBUs are dynamic; they send different messages reflecting their current state. In order to support dynamic RSUs while still avoiding replay attacks, it is therefore necessary for the RSUs to have their own keying material and generate signed messages.

4.4.1 Authentication Structure

Conceptually, authority follows geographic lines of control and as one descends the certificate hierarchy, the scope of control for any given CA becomes smaller. Thus, for instance, Philadelphia would need Pennsylvania's approval (tacit or otherwise) in order to issue certificates to RSUs. This authority structure may or may not be reified in the certificate structure. In the Section 4, we considered two architectures, which we present here.

The topology of the PKI impacts on efficiency and ease of deployment. It also has political ramifications. The PKI is primarily responsible for the issuance of digital certificates and revocation information. Certificate Revocation Lists (CRLs) are the most common form of revocation information. Imagine we have an RSU which has the following place in the hierarchy:

Country	US
State	Virginia
County	Fairfax
RSU #	10048

We need to consider two major alternative architectures *hierarchical* and *flat*.

Hierarchical PKI

The PKI topology mirrors the levels in the naming hierarchy. For example, the US DOT operates a CA for the top level, issuing certificates to each of the States. Then, the States operate CAs, and they issue certificates to each of the counties and cities within the state borders. Finally, the local governments operate CAs, and they issue certificates to the RSUs.

This alternative directly matches the expectations of most people familiar with governmental structures. A single trust anchor is needed to represent each country. A superior international organization could be created to serve as the top-level CA, but it has many political issues, and it imposes additional efficiency concerns.

This hierarchal structure imposes a burden on the OBU. Using the above example, four signature validations are needed to verify a message from RSU 10048. They are:

1. Validate the signature on the VA certificate with the US DOT public key.

2. Validate the signature on the Fairfax County certificate with the VA public key.
3. Validate the signature on the RSU certificate with the Fairfax County public key.
4. Validate the signature on the message with the RSU public key.

Further, revocation information provided by each of the CA ought to be checked. If CRLs are employed, three addition signature validations are needed. Each of the CRLs ought to be small since each CA is not responsible for a large number of certificates.

Deployment requires each of the superior organizations to be operational prior to a subordinate governmental entity. Therefore, Fairfax County cannot install their first RSU until the US DOT and the Commonwealth of Virginia are both fully operational.

Flat PKI

A single CA issues all of the certificates within a nation, but the naming hierarchy is unchanged. For example, the US DOT operates the CA for the top level, but it accepts requests for certificates and revocations from authorized registration authorities (RAs) in each of the states, counties and cities. The process for authorizing RAs will likely follow the natural governmental structure, but once authorized, the RA can communicate directly with the CA.

All of the political concerns are transferred to the RA registration process. And, the CA is responsible for ensuring that one local government cannot request certificates that are affiliated with other jurisdictions.

This flat structure reduces the burden on the OBU. Using the above example, two signature validations are needed to verify a message from RSU 10048. They are:

1. Validate the signature on the RSU certificate with the CA public key.
2. Validate the signature on the message with the RSU public key.

Revocation checking can be problematic in this structure, since all of the revoked certificates are listed in a single CRL. While only a single signature is needed to validate the CRL, the number of entries on that CRL can become quite large. A large CRL takes significant bandwidth to download. This concern might be mitigated by performing the download at gas stations where the vehicle is stationary.

Deployment only requires the national CA to be operational. Therefore, Fairfax County cannot install their first RSU before the Commonwealth of Virginia has installed any capabilities, assuming that the registration process can be accomplished by paperwork.

This alternative has an additional concern. The national CA must be highly available. In the first alternative, the outage of any single CA has very little impact on the overall system, but in this alternative, an outage in the national CA can have major ramifications. Therefore, an architecture that includes concurrent operations from multiple physical locations is needed, making the national CA more expensive in this alternative.

Hybrid Alternatives

Hierarchical and flat PKI topologies represent the extremes of a continuum. Two mechanisms exemplify other points along the continuum: partitioned CRLs and indirect CRLs. Partitioned CRLs are used to ensure that CRLs never get too big. The population of certificates is divided among a group of small CRLs, and the certificate contains a pointer to the CRL that needs to be checked for revocation. For example, the first 1,000 certificates issued point to one CRL, the second 1,000 certificates point to the next CRL,

and so on. This ensures that none of the CRLs is ever larger than 1,000 entries. Of course, most should be much smaller than the maximum.

A better method of portioning the CRLs for the DSRC application is geographically. This allows an OBU to obtain and validate the CRL for a specific area as it enters it. One approach might be to partition the CRLs by ZIP code. Another approach would be to use the grid defined for the World Aeronautical Chart. Indirect CRLs allow one CA to issue the certificate and another to issue the associated CRL. In this way, a national CA could issue each certificate, but the certificate would contain a pointer to the locally-administered CRL that needs to be checked for revocation. Certification path checking is a bit more expensive than in a hierarchical PKI, but revocation is handled locally.

4.4.2 Certificate Format

Because of the packet size limitations explained in Section 4.2.6, conventional X.509 certificates [12] are unsuitable for use with VSC Security. They are excessively large and there is a large semantic gap between X.509 distinguished names and the names which make sense here. Although it is in principle possible to shoehorn VSC information into X.509 certificates, the result would be fairly unwieldy. In addition, because interoperability with conventional PKIs is not a priority and we do not anticipate using the signature algorithms that are commonly used with X.509 certificates, there is no significant advantage to using X.509 rather than a custom format.

In this section, we sketch the outlines of a certificate format for VSC Security but stop short of providing a bits-on-the wire description. VSC certificates consist of at least four data items:

- The public key of the certificate holder.
- The scope of the certificate.
- The validity window of the certificate (expiry time).
- A signature over the certificate.

The public key of the certificate holder and the signature are straightforward cryptographic data. The validity window can be easily represented in one of a large number of more or less equivalent formats (UTC time, seconds since the epoch, etc.) However, the scope requires more discussion.

Scope

In RSU/PSOBU certificates all important authorization information in a certificate must be carried in the scope field. We are concerned with two kinds of authorization information:

- Geographic – the physical regions during which this certificate may be used.
- Functional – the types of assertions that the holder of this certificate can make.

We discuss each of these kinds of scope in turn.

Geographic Scope

The purpose of geographic scope is to restrict certificates to the geographic regions for which their operators have authority. For instance, the California Transportation Agency would find it undesirable for the Illinois Transportation Agency to be able to install RSUs that broadcast information about California traffic signals, since this would mean that compromise of an RSU in Illinois would open up attacks in California. In order to

prevent this, each certificate must contain an indication of which geographic areas the certificate may be used in.

We propose that these restrictions be encoded in one of three ways:

- A radially symmetrical zone
- A polygon
- A sequence of rectangles

The specification for a radially symmetrical zone is a single lat/long coordinate specifying the center and a radius of the zone. The intention is that this mechanism is used for immovable objects like RSUs.

A polygonal restriction is a sequence of geographic locations (expressed as lat/long coordinates), which are then connected by straight lines in a connect-the-dots fashion. These points and lines define an enclosed region (or, perhaps, regions), which delineates the scope of the certificate. The certificate may speak for any point in that region. The intention is that this sort of scope will be used for CAs and PSOBUs.

A sequence of rectangles represents a middle ground between a circle and a polygon. It allows a more complex region to be defined than does a circle, but allows less complexity than a polygon and is therefore easier for a receiver to evaluate.

Note that there is some redundancy between the different representation formats. In particular, polygons can be used to emulate the other formats to a great degree. At the end of the day, experience may show that it is advisable to decide on a single format. However, initially we consider it wise to offer some variety for experiment.

In principle, this technique can be used to define the validity region to an arbitrarily fine granularity. However, in practice the need to keep message sizes down requires that the number of points be kept relatively small. This inevitably creates some areas where the certificate restrictions do not precisely match geographic boundaries. In practice, we do not anticipate this being a problem since bordering regions in general need to be able to coordinate their activities. This sort of restriction is intended primarily to proactively contain compromise between distant geographic regions. One way to produce finer grained boundaries while reducing message size is to issue multiple certificates, which together cover the entire permitted zone.

Functional Scope

It is extremely desirable to restrict the uses to which a certificate can be put. For instance, rural traffic signals are often isolated and poorly monitored. If an attacker could compromise such a signal he or she should not be able to then use it to impersonate a police car. In order to prevent this kind of attack, certificates must contain functional restrictions.

As with geographic scope, functional scope should be thought of as a tree, with restrictions becoming increasingly tight the further one moves away from the root. A proposed tree is shown in Figure 10.

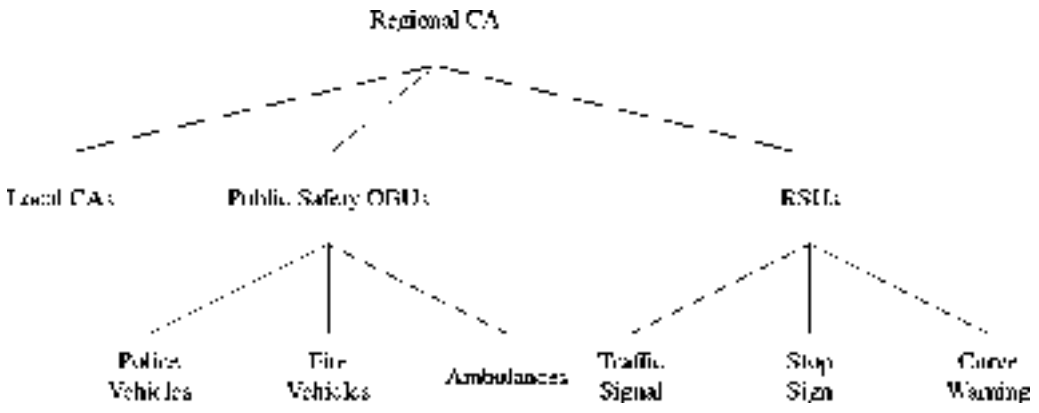


Figure 10: Functional Scope for RSUs and Public Safety OBUs

Note that it is possible – indeed likely – that a CA will sign other CAs as well as RSUs/OBUs. For instance, the California State CA might sign certificates for both the OBUs for the California Highway Patrol and for the county CAs.

No Identities

Note that unlike conventional certificates, DSRC certificates do not contain an identity string. All of the important authorization information is carried in the scope field and therefore we can save space by not including an identity payload at all.

4.4.3 Registration and Certificate Issuance

Any certificate system needs some way for units to get certificates. In VSC, these mechanisms fall into two categories: initial registration and certificate issuance.

Initial Registration

When a new PSOBU or RSU first enters the system, it is un-initialized and must be introduced to its CA. The introduction process creates a binding between some shared cryptographic credential and an entry in the CA database. For VSC, this is done one of two ways: either via direct connection or remotely. In either case, the first step is for the CA administrator to determine which permissions the unit should be allocated. This is done using non-technical mechanisms which are not specified by VSC. For instance, when initializing traffic signals, the CA administrator may be the person installing them or may communicate directly with the installer.

In the direct connection case, the unit is fitted with an interface (e.g., USB or Firewire) and the administrator physically plugs the unit into the CA. The administrator then interrogates the unit for its public key and records that key in its database, bound to the unit's identity and permissions.

In the remote case, the unit's public key (or more likely a digest of the public key) would be delivered along with the unit (for instance, embossed on the outside like a serial number). The operator of the unit would then tell the CA administrator the public key (or digest) and he would enter it into the CA database. Note that this process could also be performed via Web or some other remote access mechanism, provided that the unit operator authenticates to the CA.

Certificate Issuance

Once the initial registration has occurred, the CA can then issue certificates for the unit. The certificate permissions are controlled by whatever settings are in the CA's database. The simplest way for certificate issuance to operate is for the CA to periodically issue appropriate certificates for the public key stored in the database. Alternately, the CA might require the unit to provide a new key but authenticate the request using the initially registered key.

For RSUs, we anticipate that transit agency personnel would periodically visit the unit to install a new certificate. However, RSUs could potentially be refreshed over the Internet if network service is available. PSOBUs will likely have their certificates refreshed at their "home bases". For instance, when the vehicle is driven into the garage, it could establish a wireless connection with the local CA and get a new certificate.

4.4.4 Message Authentication

Once the keying material is established, RSU/PSOBU message authentication is accomplished by traditional digital signature techniques, in the flavor of CMS [13]. Each message has a digital signature attesting to its authenticity and an identity certificate attesting to the identity and permissions of the sending unit. The receiving unit can then verify the message and act appropriately.

Message Format

The PSOBU/RSU message format contains the following items:

- Payload type identifier
- VSC safety application information (payload)
- Locally-unique message identifier
- Timestamp
- Position
- Sender's certificate
- Signature over entire message

Note that the security system is completely blind to the contents of the safety payload. It only knows the type (for de-multiplexing on message receive). The Security Layer is simply responsible for verifying that the message is authentic. The VSC Safety Application Layer must then determine if the message is appropriate, as described in Section 5.4.4.3. Figure 11 shows such a message. The shaded sections are signed.

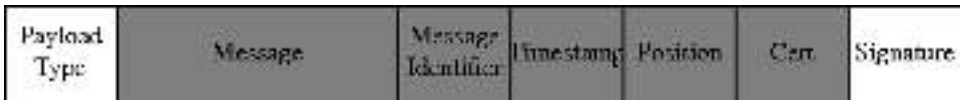


Figure 11: A protected message

Signature

When a safety message is presented to the Security Layer for processing, it must perform the following stages:

1. Generate a unique message identifier. The intent of this message identifier is to uniquely identify this message among others sent by the same unit at the same time (in cases of insufficient time granularity). This identifier can be a simple short counter or can be generated by a random number generator [14].
2. Form a temporary message consisting of the message id, the payload, and the sender's certificate.
3. Sign the temporary message.
4. Append the message signature to the temporary message to form the final message to be transmitted.
5. Pass the final message down to the DSRC Messaging Layer.

This is a fairly conventional message processing procedure, roughly analogous to that used in IPsec ESP [15].

Verification

When a unit receives a PSOBU/RSU message, it must first verify the authenticity of the message. This requires two sets of checks, one performed at the Security Layer, one performed at the Safety Application Layer. The Security Layer's job is to verify that the message is *cryptographically correct*. This means that it was correctly signed by a valid user. Verifying this requires verifying both the signature and the certification path.

Each message contains only the certificate of the sender. In order to validate that certificate, the receiver must construct a path of certificates up to a trust anchor (a certificate which is trusted because it is built into the OBU). At each stage in that path, the recipient must verify that:

- The signature on the certificate is valid.
- The restrictions on the certificate allow the current use. For instance, certificates for CAs (often called intermediate certificates) must be tagged as CAs and have the correct geographic scope for the certificate they are signing. Note that this means that the regional scope for any certificate must be entirely within the regional scope of its parent.
- The certificate is current and not expired.
- The certificate has not been revoked.

Note that units are expected to cache verified certification paths, thus reducing the burden of re-verification for new certificates. For instance, once a unit has verified the Palo Alto Police certificate, it can verify any individual police car by using the cached path, and then checking the car's individual certificate. Once the certificate has been verified, the receiving unit must then verify the message. This is a simple matter of verifying the digital signature using the public key in the certificate. The fact that a signature is valid may be cached indefinitely, however the validity of the certificates must be checked whenever a new CRL is received or the current one expires.

In order to prevent replay attacks, each message contains a timestamp which is generated inside the trust boundary of the transmitting unit. The Security Layer must maintain a list of all recently received messages (a window of 1-5 seconds is probably appropriate) and reject messages that either (1) bear timestamps outside that window or (2) have been replayed. The Safety Application Layer must also check that the position described in the message is within the geographic scope of the sender's certificate.

Once the Security Layer has verified the authenticity of the message, it passes it on to the Safety Application Layer for processing. The Safety Application Layer must then verify that the certificate that was used can be used to sign a message of this type. For instance, a Stop Sign RSU might sign a message claiming to be a Curve Speed Warning. This must be detected at the Safety Application Layer because the Security Layer does not have any visibility into the Safety messages. The Safety Layer must also verify that the message is geographically and temporally relevant (different applications have different relevance requirements). Only if all of these checks succeed is the message accepted for processing.

The intent of placing this processing in the Security Layer is to allow new applications to be deployed with their own validity requirements. An alternative design would be to have a Security Layer which accepted configurable policies for message validity. The Safety Layer could then describe which applications were to receive which policies and the Security Layer could enforce the correct policy based on the payload type field.

4.4.5 Propagation of Certificates

In order to verify a message, it is necessary to have the entire certification path up to a trust anchor. However, in general the entire path will be too large to fit into time critical messages. Therefore, there must be some mechanism to pre-load verifiers with these certificates. Because certificates are geographically restricted, there is a straightforward mechanism to arrange for certificate pre-loading. RSUs near geographic boundaries periodically broadcast the entire certification path for their region. The RSU could be Internet connected and periodically contact the CA for refreshed intermediate certificates or CRLs.

Thus, when vehicles enter a new region, they automatically acquire the new certificates and cache them. Because these messages are not time critical, they can be fairly large, up to the maximum packet size of the network. In the event that the maximum size is too small, the certificates may be spanned across multiple network packets using the technique described in Section 5.5.2.2.

4.4.6 Identifying Compromised Units

Identifying compromised RSUs and PSOBUs is relatively straightforward. We need to consider three basic cases. First, we may know the real-world identity of a compromised unit, e.g., a serial number. It is expected that CAs will keep records of which units had which key pairs, and therefore it is straightforward to revoke that particular unit and to ensure that no future certificates are issued to that unit.

In the second case, we may have captured some set of messages that are considered bad. Because certificates signed by PSOBUs and RSUs contain the certificate of the signing unit, we immediately can find the random identifier. This identifier can then be used as the key for a CA database lookup to find the real world identity of the compromised unit. That unit's certificate can then be revoked and/or the unit can not be issued any future certificates.

Finally, consider the case where an attacker compromises a unit and anonymously publishes its private key. Although the user cannot be identified, we can still identify the compromised unit in two ways. First, the private key can be used to generate the public key, which can then be looked up in CA databases. Second, the private key must be used with the associated certificate. Once the certificate is found, compromise can then be handled as in the previous case.

4.4.7 Certificate Revocation

In any PKI system, there are two basic mechanisms for dealing with compromised keying material: revocation lists and timeouts.[5] Choosing which mechanism to use is a tradeoff between the cost of propagating certificate revocation lists and the cost of refreshing keying material. Where the best tradeoff is depends on the extent of compromise – and therefore of revocation – and the required level of timeliness. Because we cannot predict *a priori* the extent of compromise, the best option is to design a system that incorporates both methods of compromise containment. When a certificate expires, it can generally be refreshed using the certificate issuance mechanisms described in Section 5.3.3. However, revocation requires a new mechanism.

Revocation lists are easy to create. They are simply a signed list of all of the non-expired keys which have been revoked. However, the lists must then be distributed. Because, like certificates, they are geographically bounded, they should be distributed at the borders of geographic regions. In the event that they are too large to fit into a single packet, they may be spanned across multiple packets, as with certificate distribution.

4.4.8 Choice of Algorithms

Although this is a traditional asymmetric key/digital signature system, a careful choice of signature algorithm nevertheless is required due to message size and performance considerations. Asymmetric signature systems differ along four dimensions that concern us:

- Signature size (S_{sig})
- Public key size (S_{pub})
- Signing time (T_{sig})
- Verification time (T_{vfy})

The first two parameters control the size of the signed messages. The second two parameters control the performance of the system, and thus directly impact latency.

Message Size

Any signed message must include:

- The certificate (size $S_{sig} + S_{pub} + S_{rest}$) where S_{rest} is the size of the identities, validity period, and restrictions and varies depending on the granularity of the geographic access controls but is constant across signature algorithms.
- The signature over the message (size S_{sig})

Thus, the minimum size for a given signed message (with an empty payload) using a conventional signature scheme is $2 \times S_{sig} + S_{pub} + S_{rest}$.

The magnitude of S_{rest} depends on the granularity of the scope restrictions in the certificate. At minimum, S_{rest} will contain a 32 bit time field. The scope field consists of a series of points defining the shape of the allowed geographic region. Each point will be approximately 8 bytes in length. Thus, a plausible value for S_{rest} is 32 bytes (four points). A radially symmetrical zone will be smaller: 8 bytes for a point and probably no more than 2 bytes for a radius. Note that S_{rest} is independent of the choice of cryptographic

[5] In principle, one could also use an online status protocol such as OCSP [16], but in practice, such mechanisms are impractical in a broadcast situation.

algorithm. In the rest of this section, we will be discussing only the size of the cryptographic portions. An additional S_{rest} bytes of overhead will always be required.

Performance

In order to send a message, the sender must perform a single digital signature, costing T_{sig}. In order to verify a message, the recipient must at a minimum verify the message signature (time T_{vfy}) and will likely have to verify at least the certificate signature (time T_{vfy}). If we assume that the rest of the signatures are cached, the total verification time is $2 \times T_{vfy}$. Thus, the total latency introduced by security is $T_{sig} + 2 \times T_{vfy}$.

Message sending throughput depends entirely on signing time. Thus, a sending unit can transmit $1/T_{sig}$ messages per second. Message receiving throughput depends on verification time. Thus, a receiving unit can receive between $1/T_{vfy}$ and $1/2*T_{vfy}$ messages per second, depending on how many of the messages are from senders whose certificates have previously been verified.

The actual performance of any algorithm depends on the processor it is running on. For reference, we quote numbers from the MIRACL library of Mike Scott running on a 450 MHz Pentium III [17]. There's nothing special about this library, except that Scott provides measurements for a large number of different algorithms, thus enabling easy performance comparisons between algorithms.

Patent Status

Finally, we must consider the patent status of each algorithm. If OEMs must license patents in order to deploy the VSC security system, then this increases their costs. We provide a description of what we know about the patent status of the algorithms we describe. This information cannot, however, replace a thorough legal search.

RSA (Rivest, Shamir, Adleman) Algorithm

RSA [18] is the world's most widely used signature algorithm. At the standard 1024 bit strength, it is fairly fast for signature (17 ms) and extremely fast for verification (.11 ms, public exponent=3). It would meet our performance targets with minimal hardware acceleration.

The RSA verification step is extremely fast since it uses small exponents, so that even a fairly small ASIC core can easily meet the latency and throughput goals for verification. Fortunately, the RSA signature goal (i.e., 5 msec latency) can also be achieved reasonably easily. For example, a new Hifn chip uses slightly less than 100K gates in a 0.13 micron CMOS process to achieve 388 RSA 1024-bit signatures/sec, running at 200 MHz. This is a latency of under 2.6 msec. The same core can perform RSA 1024-bit verifications, using a 17-bit exponent (65537), with a latency of under 0.2 msec. An area of 100K gates, when added to an existing chip, currently results in an incremental silicon cost of under $0.50 in volume. If this design were to be fabricated as a stand-alone chip, the packaging and testing costs would probably raise the per-chip cost to $2 – $4, in large volume. The power consumption of such a core, at full duty cycle, would be (very roughly) on the order of 0.25 Watts.

However, the RSA signature size is unworkably large. At 1024 bits, $S_{sig} = S_{pub} =$ 128bytes.[6] Thus, the minimal cryptographic overhead for a message is 384 bytes. It is

[6] This assumes that everyone uses the same public exponent so there is no to add it to the public key. If the exponent varies, add a few bytes overhead.

possible to aggregate multiple RSA signatures into a single signature[19] (and this requires using a non-standard form of signature) thus reducing the minimal overhead is 256 bytes, which is still likely to be too large.

There are no intellectual property costs associated with using RSA, because the patent on RSA [20] has expired.

DSA (Digital Signature Algorithm)

The other commonly used signature algorithm is the *Digital Signature Algorithm* (DSA), defined in Federal Information Processing Standard (FIPS) 186-2[21]. DSA is roughly twice as fast as RSA for signature (8.8 ms) but is far slower for verification (10.75 ms). Therefore, significant hardware acceleration would be required in order to obtain acceptable performance.

DSA signatures are 40 bytes long, but the DSA public key is as large as RSA. If a common parameter group is used, at a 1024 bit strength, S_{pub} = 128bytes. Thus, the total overhead is 208 bytes, less than RSA even with aggregation. However, since our target is 100 bytes, this is still larger than desirable.

The major computational step in a 1024-bit DSA signature is a single modular exponentiation, with a 1024-bit modulus and a 160-bit exponent. To first order, all other operations involved in the signature are only minor additions to this time. Similarly, the dominating computation cost for a 1024-bit DSA verification consists of two such exponentiations. A third-party vendor (Athena Group) currently offers a modular math core that can conservatively achieve the following latencies, running at 200MHz:

1024-bit DSA signature	0.25 msec
1024-bit DSA verify	0.50 msec

The area is about 250K gates. These numbers are all approximate and may end up slightly better or worse, depending on the silicon process and the time taken in synthesis and physical design. In any case, these performance numbers meet the desired goals, and the incremental silicon cost of such a core would be in the $1-2 range. As a stand-alone chip, the volume pricing would probably be in the $3-$6 range. The power consumption would be very roughly on the order of 0.5 W.

We know of two U.S. patents that are asserted to cover DSA. U.S. Patent 5,231,668[22] and U.S. Patent 4,995,082[23]. The '668 Patent is assigned to the United States of America and is available royalty-free. The '082 patent is not royalty-free. There has been debate about whether or not the '082 patent is required for implementations of DSA and many vendors in the US have not obtained patent licenses. A thorough analysis of this patent should be performed.

ECDSA (Elliptic Curve DSA)

As described previously, the primary problem with DSA is that the public key is too large. *Elliptic Curve DSA* (ECDSA) is effectively DSA over an elliptic curve. Elliptic curve algorithms such as ECDSA are as strong as integer algorithms such as RSA or DSA with smaller key sizes. In particular, ECDSA is roughly as fast as DSA, but at the 80-bit security level (equivalent to a 1024-bit RSA key) has only a 160-bit (20byte) key size. The signature is the same size as DSA. Thus, the minimum space overhead with ECDSA as the signature algorithm is 40 + 40 + 20 = 100 bytes. It may also be desirable to use keys stronger than 160 bits for high-level CAs, thus providing increased resistance to analytic attack.

Elliptic Curve algorithms are not as widely implemented in silicon as RSA and DSA. However, we are able to make some estimates as to performance and gate costs. We believe that we can achieve the target performance of 2000 ECDSA verifications per second using approximately 75,000 gates. This should add a cost of about $0.30 / VSC unit and consume less than 0.2 watts. See Appendix A for the reasoning behind these estimates.

Certicom has asserted a number of patents on efficient implementations of elliptic curve cryptosystems [24]. The validity of these claims themselves should be investigated and appropriate patent licensing (as necessary) pursued.

ECDSA can also be used in an "implicit certificate" mode where the public key and the signature are combined, thus reducing the space required to represent the public key. [25] This technique may be patented by Certicom. Again, we advise the pursuit of patent licensing as appropriate.

BLS (Boneh, Lynn, Shacham) Algorithm

Boneh, Lynn, and Shacham [26] describe a technique for using the Weil pairing to produce a very short signature (approximately 20 bytes). The public keys are of equivalent size. In addition, BLS signatures can be aggregated, so the minimal space overhead for security could be as low as 40 bytes. Unfortunately, BLS signature verification requires two pairings and is therefore extremely slow. Accurate numbers are not available, but our estimate is on the order of 40 ms (though two aggregated signatures can be verified at once, so this is the total overhead to verify one message). Very extensive hardware acceleration would be required to make the performance of BLS acceptable.

Algorithm Analysis Summary

We consider the best algorithm choice to be ECDSA. RSA and DSA have too large a space overhead to be practical in this application. Because BLS is very new and has only seen modest amounts of review, we do not believe it is appropriate to standardize on at this time. Thus, we recommend that ECDSA be chosen as the signature algorithm for RSUs and PSOBUs.

4.5 Authentication for OBU Messages

The situation with end user OBUs is more difficult than that with RSUs. Although the authorization problem is in principle much simpler (the OBU merely needs to establish that it is a valid OBU, rather than one with any particular set of characteristics), it is rendered much more difficult by the need to preserve privacy. In the rest of this section, we discuss the relevant criteria for deciding on a scheme and then describe a number of potential schemes for OBU authentication.

4.5.1 Selection Criteria

When deciding which approach to use for OBU message authentication, we need to consider four issues: privacy, performance (size and bandwidth), management complexity, and resistance to compromise.

Privacy

Beyond the desire for sender authentication, it is assumed in the threat model and system constraints that end user OBUs have an increased need for privacy. In this context, we are primarily concerned with two security properties:

1. *Anonymity* – it is not possible to determine a vehicle's identity from its transmissions.
2. *Unlinkability* – it is not possible to determine that multiple transmissions were from the same source.

Note that unlinkability is a stronger security property than anonymity, since a lack of anonymity automatically implies linkability.

When considering these properties, we have to be concerned with two kinds of attackers: ordinary users and insiders (Classes 1-3 versus Class 4 in the terminology of our threat model). For instance, it might be possible for OBU vendors to determine users' identities even if it is not possible for ordinary users to do so.

Performance

Authentication for end user OBUs has similar performance issues to those for RSUs and PSOBUs: time critical messages need to have small authentication tags, and both signature and verification must be quick.

Containing Compromise

As discussed in Section 5.3.6, identifying and containing compromised RSUs and PSOBUs is straightforward. Any bad message can be captured and used to identify and revoke the compromised unit. However, the requirement for privacy for end user OBUs makes containing compromise of such units more difficult. There are three important scenarios for detecting compromise and deriving a discriminator for the compromised unit.

1. The investigator captures one or more messages using the compromised unit's keying material.
2. The investigator discovers the private key of the compromised unit. This would be likely to occur if an attacker posted their private key on the Internet or if the investigator obtained a cloned unit.
3. The investigator obtains the identity (e.g., serial number) of the compromised unit, perhaps by ordinary investigative work.

Some of the schemes we will be considering allow compromise to be contained only in a subset of these scenarios.

Note that we are primarily concerned here with containing compromise by Class 3 attackers (those who have successfully broken their OBU). Class 2 attackers (those with un-tampered units) can be contained fairly simply by including a message identifier in all messages and incorporating an algorithm in each OBU that will shut down the unit on command. When a bad message is detected, an authority can broadcast via RSUs a shutdown message that says "whatever unit generated this message, shut down." One possible attack on such a shutdown command is to shield one's compromised OBU except when it is being used for live attacks. This attack can be countered by tying the shutdown command to system updates so that units must process it in order to remain active in the system.

Management Complexity

Finally, we need to consider operational issues. The number of end user OBUs will be very large and, unlike RSUs and PSOBUs, they are not directly managed by the authorizing agency, which in this case is their manufacturer under the proposed security

architecture model. Thus, management of the units becomes a serious issue. For instance, if a new software revision needs to be rolled out, some mechanism is needed for arranging that all the affected units get a copy. Additionally, when units are compromised, it may be necessary to publish revocation information. Unlike PSOBUs and RSUs, revocation information for OBUs is not geographically limited and, therefore, must propagate to all OBUs. Therein, this distribution problem is more difficult.

4.5.2 Building Blocks

The schemes described in the remainder of Section 5 of this document make use of a number of more or less standard primitives. We describe them here briefly for readers who may not be familiar with them.

Broadcast Encryption

In some of the schemes that follow, a number of OBUs share the same keying material. That keying material must be periodically refreshed, which requires the ability to send them encrypted refresh messages. This is isomorphic to a common problem encountered in the security literature: how to encrypt a single message to a large group of people with minimal overhead. The typical setting is that you have a large group of receivers of size N. You want to encrypt a message to all of these receivers with the exception of a subset of size r who are excluded. The naive way to do this is to have each receiver have a single key and separately encrypt to each receiver. This produces a very large message (linear in size N-r).

A number of superior solutions have been proposed. The current state of the art is two schemes described by Naor et al.[27]. We describe their simpler Complete Subtree scheme here.

We have a universe of N receivers, numbered from 1 to N, as in U_1, U_2, ... U_N. Imagine each user as the leaves of a binary tree, thus U_1 and U_2 are under a common interior node, as are U_3 and U_4, and so on. A small example of such a tree with $N = 4$ is shown below.

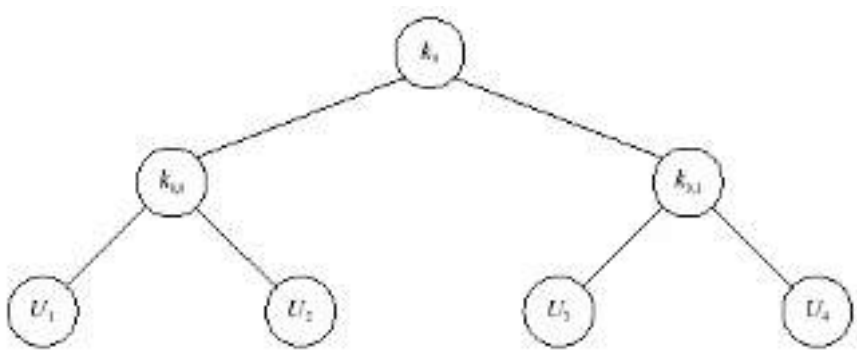


Figure 12: A broadcast encryption tree

Each node in the tree is assigned a symmetric encryption key. Each leaf (a.k.a. “unit”) is given its own key plus all the keys on its path to the root. Thus, for instance, U_1 has its own key, plus $K_{0,0}$ and K_0. In order to encrypt a message, the sender encrypts under a set of keys whose sub-trees cover the entire unrevoked set.

For instance, if no units have been excluded, the sender simply encrypts under K_0, which is known to all units. Now consider what happens if U_4 has been revoked. In that case, the sender encrypts under both $K_{0,0}$ (known to U_1 and U_2) and under U_3's key.

The efficiency of this scheme declines when a large number of units are excluded. In general, the number of separate encryptions that the sender must perform (and hence the size of the ciphertext) is $r \log (N / r)$ blocks. However, it is never any worse than the naive scheme. This scheme requires log N keys worth of storage at each receiver.

Naor et al. also describe a superior scheme called "Subset Difference". Subset difference is quite complicated and so we defer the discussion to Appendix C and simply state its properties. Subset Difference has a superior message size of $2r - 1$ blocks but the tradeoff is increased storage at each receiver of $1/2 \log^2 N$ keys. In general, message size is more critical than storage, which is relatively cheap, so the VSC team suggests encrypting using Subset Difference.

Erasure Codes

Another common problem in broadcast/multicast networking is the need to send large chunks of data in an environment where packets may be lost. In point-to-point networking, this is handled with reliable data transfer protocols such as TCP [28], but the acknowledgements required by such protocols are inconvenient in a broadcast environment. A superior approach in these environments is to use *erasure codes* [29].

The idea behind an erasure code is straightforward. Say there is a message M, which is p packets long. Instead of simply breaking it up and broadcasting it in p packets, we encode it into a group of p' packets M'_1, M'_2, ... $M'_{p'}$. The encoding is done in such a way that *any* p-sized subset of the new packets is sufficient to recover M. The sender then broadcasts all p prime packets. Any receiver that receives an appropriately sized subset has received the message.

In situations where the loss rate is known, one can simply choose an appropriately sized code and broadcast each of the p packets once. An alternative is to continuously and randomly broadcast packets. For instance, an RSU might continuously broadcast pieces of its certificate revocation list. Another possibility is to divide the fragments between a set of transmitting nodes in the system. Any unit that encounters enough other nodes will be able to reconstruct the message.

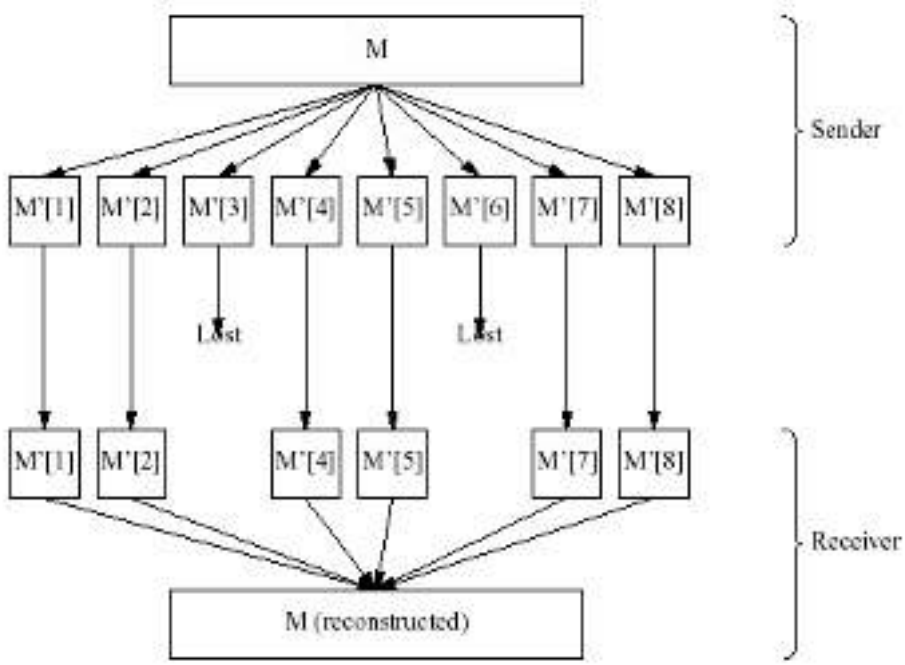


Figure 13: Erasure Code Transmission and Reconstruction

The figure above shows an example. The sender starts out with a message *M* that is 6 packets long. He then applies the encoding function to break it up into 8 packets. As long as the receiver has any 6 of those packets he can reconstruct the entire message *M*. In this case, packets 3 and 6 are lost, but the receiver gets the rest and then applies the decoding function to reconstruct *M*.

The fact that such a function exists is sort of counterintuitive and may be easier to visualize with a simple example. Imagine that we want to transmit a number from 0 to 7. This message can be encoded in three bits.

Value	Code
0	000
1	001
2	010
3	011
4	100
5	101
6	110
7	111

So, imagine that we break it up into three 2-bit messages, as shown in the figure below, so:

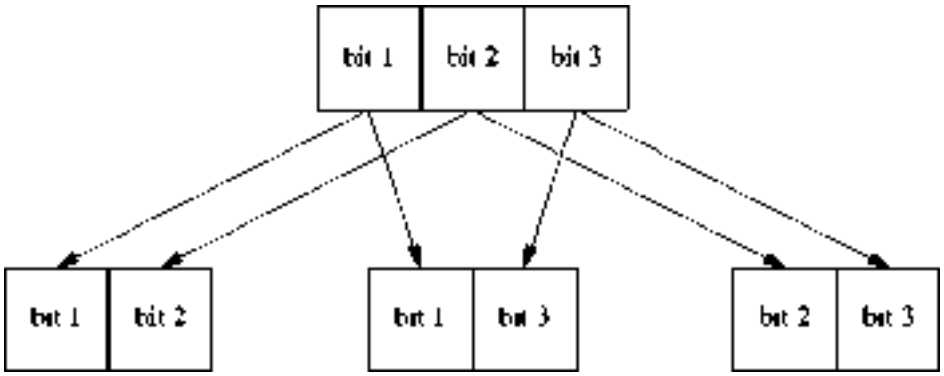


Figure 14: A Trivial Code

Thus, to encode the message 5 (101) we would transmit three packets (10,11,01). A receiver who received any two of these packets (provided he knows which one is which) can reconstruct the original message simply by reversing the encoding process. This example isn't very efficient but should be sufficient to illustrate the principle.

Patent Status

The dominant erasure code choices are subject to a large number of patents; many of which are held by Digital Fountain, Inc. We recommend that any anticipated users perform their own analysis of the patent status of this technology.

Flooding

Another issue for consideration is the distribution of files. Even if files are divided up using an erasure code scheme, the DSRC system is not one big network, but rather a series of small ad hoc loosely connected networks. Data is introduced into the system from a variety of points (typically RSUs controlled by the transmitting agent), and then must propagate to the relevant nodes. The naive solution is to have each node that receives the message rebroadcast it to all local nodes. This is obviously not optimal, and improved algorithms have been extensively studied, for instance in [22, 23]. The optimal flooding protocol for the VSC environment needs to be found/studied.

Once we assume the existence of some flooding protocol, we need to consider that there are two kinds of messages: messages that must be broadcast to all units (revocation lists, for instance) and messages that must be transmitted to only some subset of units (e.g., software updates, which only apply to units from one manufacturer). The first class of messages is *Globally Flooded* using whatever flooding algorithm is finally chosen.

The second class of messages may be transmitted by the *Limited Flooding* algorithm. Each message comes with a label (probably chosen out of a set of 100 or so), and units only listen for messages that fall into their label. For instance, software updates would be labeled by their manufacturer. This creates a set of overlay networks inside the main network each of which gets only the messages directed to it. Note that this leaks some information about unit identity, isolating it to the subset in which it is interested.

This sort of large-scale flooding network is not something that has seen extensive testing in field applications. Therefore, it is possible that there will be unpredicted problems. If such problems occur, it may be necessary to create a network of base stations that distribute data to OBUs. For instance, it would be possible to distribute updates at gas stations, where cars would be able to form a simple reliable network connection with the local RSU and download the update.

4.5.3 Global Symmetric Keys

If we want to preserve privacy, the simple approach is to have every valid OBU use the same key. Since all units have the same key, there are no additional benefits to using asymmetric cryptography. All units can simply use the same symmetric key that is then used by every unit to apply a *Message Integrity Check* (MIC) to each packet. (These are often called *Message Authentication Codes* (MAC) but we will use the term MIC to avoid conflict with the 802.11 MAC layer.) A recipient verifies a packet by recomputing the MIC and then comparing it to the message MIC.

Privacy

A global symmetric key scheme provides excellent privacy. As every message transmitted in the system is MICed with the same key, any given message could have been generated by any OBU in the system, thus providing both anonymity and unlinkability for the authentication portion of the message.

Performance

A global symmetric key scheme would have excellent performance. The only cryptographic operation in the critical path is a symmetric key MIC. MICs are very fast – approximately one million MICs/second were measured on a Pentium II/400. MICs also have extremely low space overhead – a secure MIC can be as small as 80 bits.

Compromise Containment

Compromise containment in such a scheme is handled primarily by changing the global key. Once a unit has been discovered as compromised, a new global key is generated and propagated to all uncompromised units. The key can be distributed using a standard broadcast encryption scheme as described in Section 5.5.2.1. If compromises occur frequently, key changes can be performed periodically rather than upon each compromise. Revocation lists are neither necessary nor useful for a global key scheme.

Because all messages in this system use the same keying material for authentication, it is not possible to revoke a compromised unit based purely on messages that it sends. However, if the unit's private key is published or its identity is known, it can then be revoked. The worst-case compromise scenario for a global key scheme is an attacker who compromises a single unit and then anonymously publishes the global key after every update. Because the global key is the same for everyone, it will be very difficult to track down the attacker or determine which unit was compromised. Such an attacker could potentially compromise the entire system for a long period of time. The VSC team believes that this threat is sufficiently serious that it renders a global key scheme unacceptably subject to catastrophic compromise.

There are variants of this scheme which somewhat limit the scope of compromise. For instance, you could use different keys for different geographic regions. However, because all symmetric schemes require that the sender and the recipient share keying material, they are all vulnerable to catastrophic failure to some extent.

Management Complexity

The management complexity in a global symmetric key system is produced by the need to periodically refresh keys. Any single update has the complexity of a single round of broadcast encryption, as described in Section 5.5.2.1. In the most secure implementation, this complexity would be incurred every time a unit was compromised. However, in practice, key updates would likely occur on the order of every month or so.

4.5.4 Public Key Signature Based Schemes

In order to avoid the catastrophic failure modes described in Section 5.4.3, it is necessary to use public key cryptography of some kind or another. In this section, we describe a number of approaches that use classical public key cryptography. In the next section we describe an approach that uses a newer public cryptographic primitive called "group signatures".

Simple Public Keys

At the opposite end of the spectrum from a single global key, we can issue every OBU its own key and certify it using a PKI. The manufacturer of the OBU would issue these certificates. This scheme would be very similar to that described in Section 5.3 and, as with that scheme, would make use of standard, well-understood cryptographic techniques.

Because the only important authentication in an OBU certificate is the fact that the named public key belongs to a legitimate OBU, OBU certificates can be even simpler than those provided to RSUs or PSOBUs, containing only three data items:

- The public key of the certificate holder.
- The identity of the signer of the certificate.
- A signature over the certificate.

If certificates expire, it may be desirable to have a validity period. However, the difficulties associated with obtaining new certificates suggest that it may be better to control compromise with CRLs only. In practice, however, if such a scheme were adopted it might be desirable to use the same format for both RSUs/PSOBUs and end user OBUs, and simply leave the useless slots empty or filled with some fixed data item. As we shall see, even with this system the privacy guarantees of this scheme are inadequate. We present it as a reference point against which other schemes can be compared.

Privacy

The privacy guarantees of this scheme would be quite limited. Because each message contains the certificate of the signer, it is trivial to link messages sent by the same sender, merely examine the certificate. This property is inherent in the system. One variant that improves the resistance to linkage is to issue multiple certificates to each OBU. If (say) each OBU had 1024 certificates and picked a new random certificate each hour, the ability for observers to link transmissions would be extremely limited. In order to enable compromise containment, however, the CA would need to maintain a list of which certificates have been issued to which OBU – or bind them together cryptographically. This would allow the CA to revoke all the certificates issued to an OBU once one certificate was discovered to have been misused.

This scheme can provide limited anonymity. Because the identity of the OBU is not in the certificate, ordinary attackers cannot directly discover the identity of a vehicle from

its transmissions. Of course, if such an attacker is able to independently determine the identity of the owner of the OBU, they can then link that identity to the OBU's transmissions by observation.

Anonymity against insiders is more limited. Because the manufacturer of the OBU knows which certificates were issued to which units, it is easy to work backward from any given transmission/certificate to determine which unit sent it. In principle, the CA could "forget" which units were issued which certificates, while maintaining information about other certificates were linked to it, however, it is unknown whether consumers will believe such a promise.

Performance

Performance of this system is equivalent to that described in Section 5.3. As with that system, performance is dependent on the underlying signature algorithm. Section 5.3.8 describes the performance characteristics of the candidate algorithms.

Compromise Containment

Containment of compromise in a standard PKI scheme is straightforward. As with the PKI scheme of 4, each bad message contains the certificate of the signer. It is therefore trivial to identify the public key of the responsible unit. As before, once the public key is identified, it can either be placed on a certificate revocation list or the unit can be denied a new certificate once its current certificate expires. Note that both of measures can be taken without the CA knowing the identity of the OBU that has a specific key pair. Similarly, if the private key is compromised and published, it is useless without the certificate. Once the certificate is known, revocation is performed as in the case where a message has been compromised.

Management Complexity

The primary management problem with this scheme is arranging to deliver certificates and CRLs to the OBUs. Unlike the situation in Section 5.3, end-user OBUs do not regularly connect to a single base station and, therefore, cannot get updates from that base station. In order to make this scheme work properly, certificates will need to be distributed by a flooding mechanism, such as that described in Section 5.5.2.3.

The costs for certificates and CRLs are different. Certificates must only be propagated to the appropriate OBU. Therefore, certificates can use a Restricted Flooding system. By contrast, CRLs must be propagated to all units in the system and, therefore, must use a Global Flooding system. The frequency of certificate refresh must therefore be tuned depending on the frequency of certificate revocation.

Systems have been extensively discussed where there is no certificate refresh at all, and all compromise control is done with CRLs. The advantage of such schemes is that all units must receive the same CRL, and so there is no need to partition the certificate updates between relevant units. The disadvantage of this scheme is that if revocation rates are high, CRLs can grow very large. Despite that, it appears that this is a superior approach, especially as it drastically simplifies a number of the other schemes.

Anonymous Certificates

The scheme discussed in Section 4.5.4.1 has two primary problems:

- A high level of linkability for any observer.
- A lack of anonymity against Class 4 attackers.

As discussed previously, the second property is not a necessary security requirement, but merely an artifact of the way that certification works. If the CA could somehow verifiably "forget" the binding between public key and vehicle identity, then it would be possible to construct a system without this privacy problem.

There are three major approaches for allowing certificates to be signed without creating such a binding.

1. Simple administrative policy – the CA promises to forget.
2. Blind signatures – the CA signs a certificate it cannot see.
3. Role separation between the CA and the OEM – the OEM knows the identity but does not communicate it to the CA and is not allowed to see the certificate.

The first option was discussed in the previous section. Although it is possible in principle, there is concern that users will not trust the manufacturer to avoid accidentally creating such a binding. Consequently, the remaining two alternatives are analyzed in greater detail in the sections that follow.

Blind Signatures

Blind signatures [24, 25] allow a signer to perform a digital signature on a message without knowing the message that is being signed. A blind signature on message *M* works as follows:

1. The client (in this case the OBU) uses a signature algorithm-specific blinding function *f* and a randomly generated *blinding factor B* to compute $M' = f(B,M)$. He sends *M'* to the signer.
2. The signer (in this case the CA) signs *M'* using the ordinary signature algorithm *s* and his private key *K* to produce $Sig' = s(K,M')$. He sends *Sig'* to the client.
3. The client applies the inverse blinding function f^{-1} to compute $Sig = f^{-1}(B, Sig') = s(K,M)$.

This protocol allows the CA to sign a message about which it knows nothing. In the VSC context, the OBU would generate a randomly chosen signature key and have the CA blind sign it. Thus, the OBU would obtain a certificate without having the CA know its identity.

Note that because the signer has no idea what it is signing, blind signature systems are in general vulnerable to attacks in which the client provides a bogus plaintext to the signer for signature. For instance, the OBU might generate an RSU certificate. However, this form of attack is not a concern in this context (though we will need to deal with it in the next scheme) for two reasons. First, OBUs can be initialized at the factory, where the vendor can be certain that they have not been tampered with, and that they will thus provide valid messages for signature. Second, a separate OBU-only signing key can be used for this application. Because the only meaning of such a certificate is that it belongs to an OBU, the scope of attack even for a bad unit would be sharply limited.

Role Separation

An alternative approach would be to separate the authorization to issue a certificate from the certificate issuance proper. Imagine that the CA provides the OBU manufacturer with a "signature box". When that box is physically mated to an uninitialized OBU, it will issue it a certificate. The communication between the OBU and the CA is performed over a secure channel and, therefore, the OBU manufacturer cannot learn the OBU's

certificates. Because the CA does not know the OBU's serial number, it cannot be used to de-anonymize the OBU. This is just another form of administrative control.

Multiple Certificates and Linkage

As discussed in the previous section, in order to prevent linkage of transmissions it might be desirable to issue each OBU a number of certificates. However, because the certificates are blinded, it is no longer straightforward to revoke all of an OBU's certificates when one is compromised. In order to permit this mode of operation, we need to escrow the ability to link certificates. The general idea is that each OBU certificate contains a linkage value *W*, which can be used to link it to the other certificates issued to that OBU. *W* is computed as follows:

First, each OBU generates a random symmetric key *k*. For each certificate *i* the OBU generates a cryptographically random value *r[i]* of length *w* bits.

For each certificate *i* the OBU computes the following values:

W[i] = H(k,i)

h[i] = H(0 || r[i] || W[i] || LinkageMarkerString)

e[i] = H(1 || r[i] || W[i])

B[i] = Encrypt(e[i], k)

Where *H()* is a cryptographically secure message digest. Upon certificate issuance, the *W* values are embedded in the certificate, and the *h[i], B[i]* pairs are provided to the escrow authority.

Thus, when a bad message is identified, the escrow authority can use the certificate's ^W^ value to recover the OBU's *k*, and generate the remaining *W* values. Note that this operation has been made *intentionally* expensive by the introduction of the *r[i]* value. Identifying the correct *h[i]* value requires exhaustively searching all possible values of *r[i]*, which means on average of 2^{w-1} digest operations. This feature increases the cost of linkage, thus increasing privacy. *r[I]* can be made arbitrarily large, thus making the amount of protection tunable at OBU manufacturing time.

The requirement to solve the *r[i]* "puzzle" in order to perform this linkage operation is intended to serve as a technical deterrent to casual privacy violations by making linkage expensive.

Note that as long as one of the anonymizing schemes mentioned above is used to hide the identity of any particular OBU certificate, it is not possible to de-anonymize the OBU based upon certificates alone. All that is possible is to identify other certificates belonging to the same OBU.

Privacy

The privacy of this scheme depends on whether escrowed identities are used. If they are not, then transmissions are nearly anonymous, even in the face of Class 4 attackers. However, that means that each OBU can only have one certificate and, therefore, transmissions are highly linkable.

Alternately, if multiple certificates are issued, then transmissions are no longer linkable via certificates, but identity escrowing must be employed to allow revocation of all of an OBU's certificates. The escrow authority can be separate from the OBU manufacturer, but ultimately it is straightforward to determine when two transmissions came from the same OBU (e.g., with a subpoena). However, as long as one of the de-linking schemes

mentioned above is used, it is not possible to de-anonymize the OBU via certificates alone.

Performance

Because this scheme only modifies the certificate issuing process, performance of this scheme would be generally equivalent to that described in Section 5.5.4.1, both in terms of time and space overhead. One difficulty is the choice of signature algorithm. The most common form of blind signatures is for RSA.

Compromise Containment

In general, compromise containment is done in the same fashion as that of Section 5.5.4.1. Once a compromised unit's public key is known it can be revoked.

Because the CA does not see OBU's public keys during the certificate issuance process, OBU certificates cannot be easily renewed once they expire. There are two fixes for this:

- Maintain a global certificate list, and
- Rely solely on CRLs, thereby not employing certificate expirations.

In the first strategy, OBUs would arrange to send copies of their certificates anonymously to the CA. The CA can verify that the certificates are validly signed and, if the public key has not been revoked, issue a new certificate, which is then distributed via the flooding mechanism of Section 5.5.2.3.

Without certificate expiration, CRLs may quickly grow quite large, however at the end of the day it may still be simpler to choose this approach.

Management Complexity

This scheme may introduce new management problem of maintaining the global certificate list. However, because each OBU only needs to deliver its certificate to the CA once, the problem is not particularly severe. In general, the easiest way for this to work is to have a modest number of RSUs that capture certificates and forward them onto the CA, which maintains the list. Since every message is sent with a certificate, no special cooperation is required from the OBUs.

If no global certificate list is maintained, this scheme has the same management complexity as ordinary certificates.

Anonymous Self-Enforcing Certificates

The previous two schemes allowed for linkage by the identity escrow agent. Thus, there is a risk that the identity escrow agent can be used to link any set of transmissions. Worse yet, if the identity escrow agent keeps records, then it can be used to de-anonymize transactions. We describe a complicated scheme for preventing such attacks here.

In this system, each OBU U_i has a long-term symmetric key K_i. The CA maintains a global mapping of OBU identity to K_i. In order to get a certificate, an OBU must engage in an interactive protocol with the CA. Logically, this protocol has four stages:

1. U_i demonstrates possession of K_i to the CA, perhaps by signing an initial challenge.
2. U_i generates k key pairs $I_1, I_2, \ldots I_k$.
3. The CA blind-signs certificates for all k keys. Each key has a one-day validity window.

4. U_i un-blinds the certificates.

After this exchange, U_i has k days worth of certificates. It uses one certificate per day until all the certificates have expired, at which point it must re-run the protocol to get a new batch of certificates.

Because the certificates are blind-signed and no longer contain U_i's long-term identity, it is no longer possible to revoke them based on a single bad message. In order to allow for compromise containment, we construct the key pairs so that they are self-enforcing. In DSA, ECDSA, and BLS, the private key X is 160 bits long and randomly chosen and the public key Y is computed from X. Instead of choosing X randomly, we choose it so that the top 40 bits contain the identity i of the OBU. Thus, if a private key is compromised, the identity can be extracted and no future certificates issued to U_i.

In order to ensure compliance by the OBUs (who might not put their identities in the certificates) the protocol must be more complicated. The cut-and-choose [34] technique is used to enforce OBU behavior. Thus, we replace steps 2 and 3 above with:

1. U_i generates $2k$ key pairs.
2. U_i generates $2k$ unsigned certificates, 2 for each of the k periods, using the $2k$ keys generated in step 1. Call them C_1^1, C_1^2, C_2^1, ... C_k^1, C_k^2.
3. Ui blinds each candidate certificate to get C'^1_1, C'^2_1, ... and sends the blinded certificates to the CA.
4. The CA randomly chooses one of each pair (C'^1_j, C'^2_j) and asks U_i to reveal that blinded certificate.
5. U_i sends the CA the original C_j^ls values, their blinding factors, and the corresponding private keys.
6. The CA verifies that the unblinded certificates match their blinded counterparts and that the private keys correctly contain i.
7. If all these things are true, the CA signs the other certificate in each pair and returns it to U_i. Otherwise, it adds U_i to the compromised unit list.
8. U_i unblinds the signed certificates.

This procedure is designed to minimize the probability that an OBU can get a certificate without its identity embedded. Consider what happens if the OBU omits its identity. Without loss of generality, assume that C_1^1 is improperly formatted. There is a 50% chance that the CA will ask O_i to disclose C_1^1, in which case O_i will be caught. The other half the time, the CA will choose C_1^2 in which case the attacker will have a single key, which he can use for one day without revealing his identity.

If the attacker wants to obtain more certificates with fake identities, the chance of success drops dramatically, halving with each additional false certificate requested. Thus, the probability that an attacker can obtain any significant number of untraceable keys is very low. This attack is dominated by simply compromising a unit that has just completed the key exchange protocol and, therefore, has k valid (though traceable) keys.

Privacy

As with the previous scheme, this scheme provides full anonymity for the certificates. Although the identity of the unit is known to the CA at the time of certificate issuance, there is no way to map this information to the certificate itself, as the certificate was

signed with a blind signature. Messages can still be linked within the lifetime of a single key but, as that lifetime is short, the severity of linkage is severely reduced.

Performance

The performance of messaging using this scheme is the same as that of the previous two PKI-based schemes. The management performance is worse, however, as discussed below.

Compromise Containment

Compromise containment in this scheme is worse than in the previous two schemes. First, the system cannot revoke certificates. Because the certificates are blindly signed, there is no way to determine which certificates are to be revoked. The only recourse is to not issue new certificates to the compromised unit in the future. It is not clear how severe this limitation is. If investigations take weeks to months, then the time from identification of the bad unit to key expiry might be small compared to the investigative time period.

Second, the system can only contain compromises in the second two of the three cases described in 4.5.1.3. If the private key is published, the system can use the self-enforcement property to determine the identity of the offender and not issue him future certificates. Similarly, if the system knows the identity *i* of the unit, it can simply refuse to issue it certificates in the future.

However, if the only information that is available is some set of messages generated by the compromised unit, the scheme as described provides no way to contain compromise.

Management Complexity

This scheme is much more complicated to manage than the previous two schemes. In particular, it requires a periodic interactive exchange between OBUs and the CA. This exchange consists of two round trips with sizes shown in Table 4 below.

Sender	**Message**	**Size**
OBU	*C*'s	$2kS_{sig}$
CA	request for *C* values	*k* bits
OBU	revealed *C*	$k(S_{pub} + values\ S_{sig})$
CA	signatures	kS_{sig}

Table 4: Message Sizes for Blind Signatures

In the best-case scenario of a signature and key size of 20 bytes and $k = 30$, the OBU must send 2400 bytes to the CA and the CA must respond with 600 bytes. Moreover, this is a point-to-point (not broadcast) communication, so it would be necessary to design a mechanism for OBUs to communicate reliable with CAs, which the previous schemes did not require. Because the OBUs will generally not be within direct radio contact with the CA, the DSRC network will need to provide a method for routing traffic through to the CA, probably by routing to a connection to the Internet. This requires Internet gateways in a large number of locations.

Static Combinatoric Schemes

Another approach is to use an adaptation of the cover-free broadcast encryption scheme described by Garay et al.[35]. This modification was first proposed by Jiang [36]. We have a set **R**, consisting of R key pairs and N vehicles. All public keys are known to all vehicles, and each key is assigned an index l. Each OBU U_i is assigned some random subset S_i of **R** containing n keys. We assume that vendors know which keys were assigned to each OBU, which seems like the likely case.[7]

When a unit U_i wishes to send a message M it picks a key j (for the moment, assume that the transmitting key is chosen randomly and held constant until revoked) It then signs M with R_j and then transmits the signed message $M, \{M\} R_j , j$. To verify, the receiving unit looks up key j in its local key table and verifies the signature.

Compromise is handled by *compromised key lists* (CKLs), which are globally broadcast. Whenever a bad message is detected, the key with which it was signed is added to the CKL. Units must verify that a given key is not on the CKL before accepting a message. Note that because any given unit has n keys, at minimum n bad transmissions from that unit must be observed before it can be revoked. If the attacker uses each key for the duration of the investigation, then he can use each compromised key for n investigatory periods.

The properties of this scheme depends on the chosen parameters R and n as well as the size of the system N. N is an exogenous parameter set by the number of vehicles in the system. For our purposes, we use N of 10^9 (4 times the number of vehicles in the US). Given these parameters, we can easily determine:

- The probability that any given vehicle will have a key R_l is n/R. The average number of vehicles with a given key is Nn/R.
- The probability that any given vehicle is currently using R_l is $1/R$. Therefore, the average number of vehicles using any given key R_l is N/R. Call this value C.
- Once r keys have been revoked, the probability that a given innocent unit has been covered completely revoked) is approximately $(r/R)^n$. Thus, on average, in a system of size N, $N(r/R)^n$ units will be completely revoked.
- The number of possible key subsets is approximately R^n if $n << R$.

In order for this system to work correctly, at minimum it would be preferable that no two units, U_x and U_y, have the exact same key subset. Otherwise a revocation of U_x will automatically revoke U_y and this is very undesirable. The probability of a collision is about 50% if the number of subsets is N^2. For safety, say that the number of subsets should be $10 \times N^2$, which results in $R^n = 10^{19}$ for $N = 10^9$.

Privacy

The privacy behavior of this scheme depends on the settings of n and R, which so far have only been partly constrained. In order to minimize linkability, it must be reasonably likely that two observed messages signed with the same key were not generated by the same unit. The definition of "reasonably likely" is fuzzy; semi-arbitrarily, the team deems a 50% probability that the message was generated by the same unit as “reasonably likely”.

---

[7] It is not clear how to design a system that hides this information cryptographically, as opposed to with administrative controls.

Say that the system has observed a message M with key R_l, and U_i is currently known to be using key R_l (e.g. via a previously observed message signed with R_l), then the probability that U_i generated M has as its upper bound $1/C$. In practice, the probability is far higher than this since vehicles are not homogenously distributed and tend to stay in given areas. In a closed area of size A, the probability becomes $N/AC = R/A$. In order to satisfy our linkability requirement, then, we require that $R/A < 0.5$. If we assume that the smallest area we are concerned with is 10^5 people, then $R <= 2 \times 10^5$. Since $R^n = 10^9$, the minimum value for n is 4.

One alternative is to have units choose random keys out of their available key set rather than use the same key for a long period of time. In this case, given that a unit U_i has known key R_l and the system then observes a unit using that key, then the probability that that unit is U_i is R/Nn. Again, partitioning the world into geographic areas results in the probability of that increases to AR/Nn. If $n = 4$, then R is potentially as high as 4×10^5. Note, however, that if a fresh key is chosen for each transmission, then a very small number of transmissions are enough to uniquely identify the unit, since it will quickly cycle through all its keys. Thus, each key must be retained for some moderate period of time, during which linkage is easy.

Performance

Both time and space performance of this scheme is excellent. The CPU cost is the usual cost of a digital signature. The space cost is the cost of the signature itself. Because keys are identified by indices, there is no need for certificates, thus the space overhead is roughly half that of the PKI schemes. Verification overhead is also improved because there is no need to verify a certificate, even on the first interaction.

Compromise Containment

The compromise containment scheme described here has two problems:

1. It requires that a large number of bad messages (one for each key in the unit) be observed before any given OBU is completely revoked. For instance, if $n=5$, a Class 3 attacker who had compromised the unit could mount 5 major attacks before his unit is revoked.

2. It is brittle when the number of compromised units is not very small.

The first problem is obvious, but the second requires further discussion. Recall that once r keys have been revoked, the number of revoked innocent units is approximately $N(r/R)^n$. Thus, after u units have been revoked, the number of revoked innocent units is approximately $N(un/R)^n$. The figure below shows the number of revoked innocent units for R = 100,000, some plausible values of n, with $N = 2.5 \times 10^8$, which is approximately the number of active vehicles in the United States.

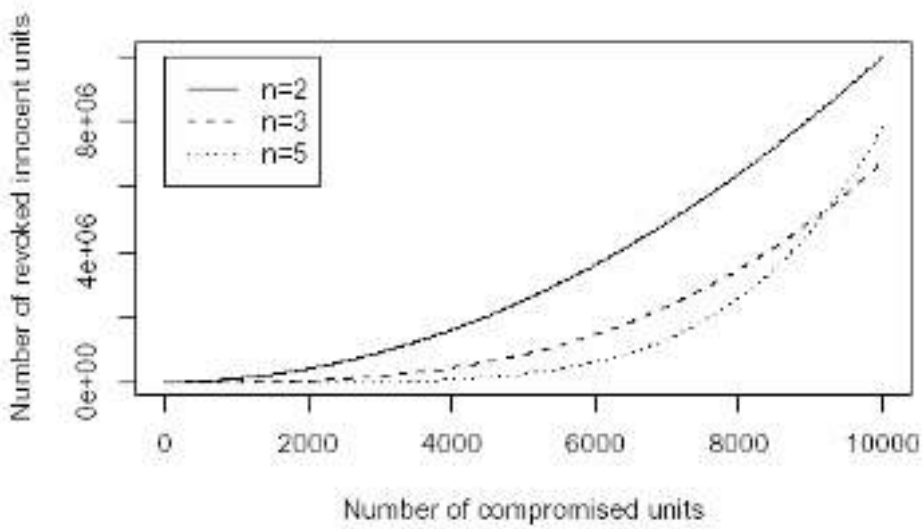


Figure 15: Innocent Revocation Rates

As is apparent above, when even small fractions of the total number of units are revoked (10,000 is only 0.004% of vehicles), the number of innocently revoked vehicles becomes completely unmanageable. Thus, a mechanism for re-keying is required. This result is not unexpected and parallels that seen by Garay et al. [35]

Management Complexity

If re-keying is not used, then management of the system is very straightforward. The only management required is distribution of CKLs, and these can be distributed by the flooding mechanism of Section 4.5.2.3. However, the management complexity of re-keying is potentially highly problematic. This topic is discussed in the next section, entitled, dynamic combinatoric schemes, which requires frequent re-keying.

Dynamic Combinatoric Schemes

Given that a re-keying mechanism is necessary for any re-keying scheme, an alternative approach is to use a dynamic combinatoric scheme with frequent re-keys, as follows. To issue keys for K time periods, generate K universes of key pairs, $\boldsymbol{R}_1$, $\boldsymbol{R}_2$, ... $\boldsymbol{R}_k$, with S keys in each set $\boldsymbol{R}_k$. Thus, within each universe $\boldsymbol{R}_k$ are keys R_k^1, R_k^2, ... R_k^S. For each time period k, the system generates S disjointed subsets of $\boldsymbol{N}$, $\boldsymbol{N}_1$, $\boldsymbol{N}_2$, ... $\boldsymbol{N}_s$ such that $\cup$ *from i* $\boldsymbol{N}_i = \boldsymbol{N}$. A unit's membership could be represented as a list of set indices. For instance, *(1,5,7)* means that the unit was in R_1 in time period 1, $\boldsymbol{R}_5$ in time period 2, and $\boldsymbol{R}_7$ in time period 3. In each time period k, all members of $\boldsymbol{N}_i$ are assigned key R_k^i. Thus, the example unit above would be given keys (R_1^1 , R_2^5 , R_3^7). As with the previous scheme, each unit gets all the public keys.

As with the static combinatoric scheme of Section 4.5.4.4, authentication is by simple digital signature. Each unit has exactly one key for any time period k and it uses that key for signature during that entire time period. If the original message is M and the unit has key R_k^i then the authenticated message is $M, i, \{M\}R_k^i$.\

Upon receipt, the recipient looks up the appropriate public key and verifies the digital signature.

Because each key is only used for a short period of time, this scheme has no support for certificate revocation. Instead, traitor tracing does revocation. Once a series of bad messages is observed, the issuing authority can figure out which unit was assigned those keys, and then refuse to issue future keys to those units. It thus takes at most k time periods from the discovery of compromise to cutting the compromised unit out of the system.

Privacy

As with the static combinatoric schemes, the privacy guarantees for this scheme depend on the system parameters, in this case S. The number of units who are using key i at any given time is N/S. Recapitulating the linkage computation from Section 5.5.4.4, the requirement becomes that $A/S > 2$ – the total number of key subsets must be smaller than the total number of vehicles in an area. For areas of $100,000$, this results in $S <= 50,000$.

Note that observation of transmissions from the same unit on multiple days quickly allows determination of the unit's true identity. In fact, this technique would likely be used to trace compromised units. However, this is of no help in linking it to future transmissions since it (almost) always shares keys with other units in the same area.

Performance

Both time and space performance of this scheme are excellent. The CPU cost is the usual cost of a digital signature. The space cost is the cost of the signature itself. Because keys are identified by indices, there is no need for certificates, thus the space overhead is roughly half that of the PKI schemes. Verification overhead is also improved because there is no need to verify a certificate, even on the first interaction. Alternately, the issuing authority can provide group certificates to key holders, thus making the message size the same as with a PKI system.

Compromise Containment

Purely refusing to issue future keys to compromised units achieves compromise containment in this scheme. Once a critical number of messages from a compromised unit have been observed (on multiple days), the identity of the unit can be determined and no future keys issued to that unit. Note that because each key is only valid for a very short time window, the attacker is forced to use multiple keys if he wants to mount a large number of attacks, thus leaking large amounts of information and enabling investigation and compromise containment.

Note that in the worst-case scenario, compromised key lists can be used to provide fast update once an offender is identified. However, given that in general the window of vulnerability is a month or so, it is doubtful that this is worth doing.

Management Complexity

The management complexity of this scheme is primarily in the need to broadcast the periodic key updates. Consider the size of an update for a single time period. This update has two parts:

1. S public keys.
2. S keys encrypted for N recipients (N/S recipients per key).

The first part of the update is of size approximately $S_{pub}\ S$ (1 megabyte for 20 byte public keys) and can be distributed by simple Global Flooding. Alternately, group certificates can be provided to OBUs along with their private keys.

The private key update is more difficult. Naively, it requires N separate encryptions, one for each OBU. However, this creates an unworkably large number of messages that must be transmitted. If the ciphertext size is the same as the key size S_{pub}, then the total ciphertext size is $S_{pub}\ N$ (approximately 2×10^{10} bytes for $N = 10^9$ and 20 byte keys. This would need to be distributed by Limited Flooding, but is still quite expensive (about 10^{11} bytes per month total).

A superior approach is to use a broadcast encryption scheme, such as that described in Section 4.5.2.1. Assuming a very high revocation rate of 1%, then the ciphertext size for each key is *0.02 times N/S* (8000 bytes for 20 byte private keys), with a total size of $4 \text{ times } 10^8$ for each time period (10^{10} bytes for a month). Ciphertext size scales linearly with the number of revoked keys, so for a more reasonable revocation rate of 0.01%, the total size would be a mere 10^8 bytes per month.

In order to enable this scheme, each unit would be constructed with its share of the broadcast encryption trees for its entire lifetime built into the unit. Each broadcast encryption tree share is of size $1/2 \log^2 N$ keys. For ordinary 128-bit symmetric keys, even if we change keys every day, 20 years worth of keying material can be stored in 25 megabytes of permanent (read-only) storage. In practice, it is unlikely that it is necessary to have either this many separate groups or change keys this frequently. In practice, a few hundred different permutations chosen at random is probably sufficient.

4.5.5 Group Signatures

The final approach to consider is *group signatures*. Group signatures are a relatively new cryptographic primitive originally proposed by David Chaum [37]. A group signature scheme has a single public key P and a large number of private keys K_i. Each member of the group is issued a single private key, which can then be used to generate signatures that verify with P. Outsiders can only verify that a signature was generated by *some* member of the group but cannot tell which member.

In general, group signature keys are distributed by a central authority. That central authority can determine which key pair generated any given signature. Although it is possible to hide the identity of any given key holder from the central authority, this capability allows the central authority to link multiple signatures by the same signer. When a key is determined to have been compromised, the central authority propagates an update to each verifier, which allows them to exclude signatures by that key.

The best published scheme is by Ateniese et al [38], and is generally known as ACJT. Unfortunately ACJT signatures are approximately seven times the size of comparable strength RSA signatures. This makes AJCT unsuitable for this purpose. Boneh and Shacham are currently devising a superior group signature scheme, that may have comparable signature size to RSA, however, it has not yet been published or widely reviewed. General security practice very strongly discourages the use of new algorithms and, therefore, the VSC team cannot recommend this algorithm for deployment in any system until it has had a year or so of public analysis. Depending on the VSC timeline, this may or may not be an attractive option.

4.5.6 Comparison of Schemes

Seven schemes have been heretofore described, however, Global Symmetric Keys and Group Signatures can be excluded immediately. Global Symmetric Keys provide unacceptably poor containment of compromise and Group Signatures provide unacceptable performance, primarily in terms of message size. Similarly, Static Combinatorics can be excluded because Dynamic Combinatorics dominates it.

The remaining schemes are:

- Simple Public Keys
- Anonymous Certificates
- Anonymous Self-Enforcing Certificates
- Dynamic Combinatorics

The choice between these four comes down to a tradeoff between privacy, management complexity, and containment of compromise.

Simple Public Keys offers the lowest management complexity, however it provides only very weak privacy protection. In the best-case scenario, where OEMs do not keep track of the binding between OBU certificates and vehicle identity, anyone who obtains access to the CA linkage database (however maintained) can use it to construct a vehicle tracking system. Once a vehicle is observed once, all of its certificates could be identified and, thus, tracking is easy. In the worst-case scenario, if the OEM maintains a vehicle/certificate binding, a vehicle can be identified from a single transmission.

Anonymous Certificates offer a slightly larger management complexity, but if certificates are never reissued (only CRLs are used) this complexity is confined to the certificate issuance process. They have similar linkage properties to Simple Public Keys but offer superior protection against the identification of vehicles -- as opposed to certificate revocation -- from a transmission. As the no-re-issuance certificate model seems likely, the VSC team believes that the increased public confidence and auditability of these schemes justifies the additional management complexity at certificate issuance time. Role separation appears to be a superior option for implementing Anonymous Certificates. The complexity of certificate re-issuance strongly suggests that having certificates not expire at all and handling compromise purely through CRLs is the best approach, although some additional work needs to be performed to identify schemes to bound the size of the CRL as the number of OBUs grows very large.

Anonymous Self-Enforcing Certificates provide superior privacy; they are not susceptible to the de-anonymizing attack described above. However, they provide inadequate compromise containment because they cannot be revoked based on transmissions but only on private key leakage. Because of these considerations, the VSC team considers Anonymous Certificates to be a superior alternative.

The only plausible alternative to Anonymous Certificates is Dynamic Combinatorics. Unlike Anonymous Certificates, it cannot be turned into a tracking system because multiple OBUs always have the same public keys. However, Dynamic Combinatorics have a much higher management load than Anonymous Certificates in that they require regular updates of keying material that must be delivered precisely to specific OBUs (rather than globally broadcast). Moreover, the updates are much larger than CRLs are likely to be. There are also concerns that this scheme would be unworkable in practice. Accordingly, the design team recommends the Anonymous Certificates approach as offering the best combination of security, privacy, and reliability. However, given the benefits and liabilities of both of these schemes, and the potential privacy risks associated with certificate linkage, we feel it would be wise to subject these schemes to a detailed assessment in the context of the large vehicle population and the well understood vehicle life cycle, and retirement process. In addition it may be advantageous to explore some combination of these schemes to manage the size and growth of the CRL, while addressing the compromise of privacy and the management of the large number of retired OBUs.

5 Protocol

5.1 Introduction

The previous section described potential architectures and provided a recommendation from the team. This chapter provides a complete description of VSC Security Protocol (VSP), the enrollment procedures, suggested policy requirements, OBU privacy parameters, opportunities for optimization, and a summary of the syntax.

5.2 Protocol Summary

With the identification and description of a security architecture that appeared to meet the needs of vehicle safety applications (see Chapter 4), a security protocol was able to be created, based upon this identified architecture. Whereas the security architecture described the cryptographic skeleton, the protocol specification describes the contents and formatting of each protocol message, as well as the behavior of each communicating endpoint. The protocol specification could therefore serve as a basis for the eventual implementation of the system. The architecture and protocol will be used to validate the requirements detailed earlier in this report by providing the DSRC standards writing group with a feasible solution. This chapter describes the security protocol that was developed in detailed protocol definition language, and ends in Section 5.8 with a complete summary of the syntax described throughout the chapter.

5.3 Protocol Definition

Security protocol is a structured approach toward providing descriptions of technical details. For clarity, the protocol is described using the protocol definition language used by TLS [43]. This section begins by describing the certificate and CRL format in the standard protocol definition language, followed by structured descriptions of the message format and a mechanism for propagation of system updates. Finally, it describes the procedures required for enrollment of new units in the system.

5.3.1 Certificate Format

Before units can authenticate to each other, they must first be issued credentials in the form of certificates. This section describes the VSP certificate format. In general, the team preferred not to invent a new certificate format, but the requirement to keep message sizes small ruled out the use of conventional certificate formats such as X.509. All VSP certificates use the same basic structure, as shown below:

```
struct {
    uint8             certificate_version;
    SubjectType       subject_type;
    CertSpecificData  type_specific_data;
    Date              expiration;
    CRLSeries         crl_series;
    SignerID          signer_id;
    PublicKey         public_key;
} UnsignedCertificate.

opaque[8]       SignerID;
uint16          CRLSeries;

struct {
    select(subject_type){
      case ca:
        CAScope     scope;
      case rsu:
        RSUScope    scope;
      case psobu:
        PSOBUScope  scope;
      case obu:
        LinkageData linkage;
      case crlsigner:
        CRLSeries   responsible_series<2^16-1>;
    }
} CertSpecificData;

enum {ca(0), rsu(1), psobu(2), obu(3), crlsigner(4), (255)} SubjectType;

uint16 Date;

struct {
    SignatureAlgorithm algorithm;

    select(algorithm){
      case ecdsa:
        ECDSAKey key;
    }
} PublicKey;
```

```
struct {
    opaque point<1..2^8-1>;
} ECPoint;

enum { ecdsa(0), (255)} SignatureAlgorithm;

struct {
    uint16              length;
    UnsignedCertificate  unsigned_certificate;
    Signature           signature;
} VSPCertificate

opaque    Signature<1 .. 2^16-1>;
```

The `certificate_version` field contains the version of the certificate format. In this version of the protocol it is 1. Note that this applies to both `UnsignedCertificate` and the `VSPCertificate` structure. Accordingly, when parsing a certificate the recipient must first read the version number in order to know how to parse the remainder of the certificate.

The `subject_type` field describes for what kind of entity the certificate is. Permissible types are `ca`(0), indicating a CA, `rsu`(1), indicating a RSU, `psobu`(2), indicating a PSOBU, `obu`(3), indicating an OBU, and `crlsigner` indicating that the holder of the certificate is authorized to sign CRLs.

The `expiration_date` field contains the last date on which the certificate is valid. This is represented in days since the UNIX epoch. Expiration occurs at midnight GMT.

The `type_specific_data` field contains information that is unique to this certificate type.

The `crl_series` field contains an integer that represents which of multiple CRLs maintained by the CA this certificate will appear on if it is ever revoked. `crl_series` only have meaning within the context of a given CA.

The `signer_id` field contains the identity of the certificate that the CA is using to vouch for this certificate. For certificates that are not trust anchors, the `signer_id` field must contain the high order 8 bytes of the SHA-1 hash of the CA's certificate. This allows for order 2^{38} CAs to exist before there is an appreciable probability of hash collision. See Section 4.4.2 for information on trust anchor certificates.

The `public_key` field contains the public key of the subject of the certificate. The `PublicKey.algorithm` field contains the algorithm for which the public key is to be used. The only currently defined algorithm is `ecdsa` (0), corresponding to the Elliptic Curve DSA algorithm specified in X9.31. Section 5.3.1.1 describes the format for elliptic curve public keys.

The length field of the Certificate structure contains the length of the remaining structure (i.e., the combined length of the `unsigned_certificate` and signature.)

The signature field contains a digital signature over the encoded `unsigned_certificate` value.

ECDSA Public Keys

In order to specify an ECDSA public key, the protocol needs to first specify a curve and a point. This is done in the following structure:

```
struct {
    NamedCurve    curve;
    ECPoint       point;
} ECDSAKey;
```

The "Curves" of the Key

Although in principle each key can have its own curve, in practice it is more efficient to select a small number of curves. This approach also has the benefit that certificates are smaller, since they do not need to contain the curve description, but only a curve identifier of type `NamedCurve`. NIST has chosen some curves that are suitable for use in Federal applications, and a subset of those curves is supported here. Additional curves can be registered in the future if needed.

```
enum {
    K-163(1),
    B-163(2),
    K-233(3),
    B-233(4),
    reserved (5..239),
      private (240..255)
} NamedCurve;
```

The `enum` names indicate the corresponding curve in the Recommended Elliptic Curves for Federal Government Use, dated July 1999. Values 240 through 255 are reserved for private use and will not be registered.

The "Point" Of The Key

The other part of an ECDSA key is the point (the public key itself). ECDSA points are expressed in the compressed format of ANSI X9.63 [50].

```
struct {
    opaque point <1..2^8-1>;
} ECPoint;
```

The ECPoint contains the byte-string representation of the point using the conversion routine of Section 4.3.6 of ANSI X9.62 [46]. All points are in a compressed representation.

CA Certificates

In addition to the standard certificate data, a CA certificate contains a scope field of type `CAScope`:

```
struct {
    ApplicationID        applications<0 .. 2^16-1>;
    SubjectType          unit_types<1 .. 2^8-1>;
    GeographicRegion     region;
} CAscope.

struct {
    ApplicationType     type;
    ApplicationSubtype  subtype;
} ApplicationID;

enum  {cert_transmit(0), crl_transmit(1), (2^16-1)} ApplicationType;
opaque ApplicationSubtype<0 .. 255>;
enum  {fragment(0), (2048)} MessageFlags;
```

The applications type indicates the application types for which this CA can issue certificates. If this field is empty, it indicates that the CA can issue certificates for any application. This type is structured.

The type field contains the major application type. This is a 16-bit field, thus allowing 65535 possible applications types. The VSCC will maintain a registry of different application types. Application types from `0xf000-0xff00` are reserved for private use but may be transmitted by production units. Types beginning with 0xff are reserved for private test networks and must not be sent by production units. Implementations must ignore message types they do not recognize.

The subtype field provides application-specific information about the message type. This data is not parsed by the VSP protocol but is assumed to be passed up to the application program. The intent is to allow certificates and messages to contain finer-grained control information than is appropriate here. For instance, application X might allow multiple message types but some units might only be able to send some of those types. All of the application types defined in this document have zero-length subtype fields.

The `unit_types` field lists the unit types (CA, RSU, PSOBU, etc.) for which this CA can issue certificates. If the `unit_types` field is empty, then it indicates that this CA can issue certificates for any unit type. This usage is not recommended.

The section “region” indicates the area in which the CA is allowed to issue certificates. It is encoded using the `GeographicRegion` type.

Encoding a Geographic Region

In VSP geographic regions are encoded using a `GeographicRegion` structure:

```
struct {
    RegionType   region_type;

    select(region_type){
      case polygon:
      PolygonalRegion    polygonal_region;
      case circle:
      CircularRegion     circular_region;
      case rectangle:
        RectangularRegion     rectangular_region<2^16-1>;
    }
}

enum {polygon(0), circle(1), rectangle(2), (255)} RegionType;
```

VSP supports a number of different region types. Currently, three are defined: polygon (0), circle (1), and rectangle (2). All region types with values < 240 must be assigned before usage. Values 240-255 will not be assigned and are reserved for private usage in test environments. Production units must not generate messages with these types:

```
PolygonalRegion       2DLocation<2^16-1>;
```

The `PolygonalRegion` type defines a region as a series of geographic points. The region is specified by connecting the points in a connect-the-dots arrangement in the order they appear. The final point is connected to the first point. The implied lines that make up the sides of the polygon must not intersect. Receiving units should verify that lines do not intersect and reject any region that does. The allowed region is the interior of the polygon.

```
struct {
    2DLocation   center;
    uint16       radius;
```

```
} CircularRegion;
```

A `CircularRegion` is simply a circle with “center” at its center and a radius of “radius” meters. The allowed region is the interior of the circle.

```
struct {
    2DLocation    upper_left;
    2DLocation    lower_right;
} RectangularRegion;
```

A `RectangularRegion` is a rectangle formed by connecting in sequence:

1. (upper_left.latitude, upper_left.longitude)
2. (lower_right.latitude, upper_left.longitude)
3. (lower_right.latitude, lower_right.longitude), and
4. (upper_left.latitude, lower_right.longitude).

Note that the `rectangular_region` value is an array of `RectangularRegion` structures. This is interpreted as a series of rectangles. The permitted region is any point within any of the rectangles.

RSU Certificates

RSU certificates contain two scope indicators. First, as with CA certificates, they contain the geographic region in which the RSU is permitted to operate. Second, they contain an indication of which types of application the RSU is permitted to send messages for:

```
struct {
    GeographicRegion      region;
    ApplicationID         applications<0 .. 2^16-1>;
} RSUScope;
```

The scope parameter is interpreted the same was as for CAs. The applications parameter contains a list of the `ApplicationIDs` that the RSU may generate. The RSU must not use this certificate to sign messages application IDs not on this list. If a recipient detects such message, it must reject it. Note that a given RSU may have multiple certificates with different application or geographic scopes. For instance, a traffic signal RSU might be enhanced to provide a maximum speed warning. It may be simpler to issue a second certificate rather than reissue the initial one. Whether to issue multiple certificates or a single certificate with multiple application IDs is a local policy issue.

PSOBU Certificates

The scope field of PSOBU certificates is effectively the same as the scope field of RSU certificates:

```
struct {
    GeographicRegion    region;
    ApplicationID       applications<0 .. 2^16-1>;
} RSUScope;

struct {
    GeographicRegion    region;
    ApplicationID       applications<0 .. 2^16-1>;
} PSOBUScope;
```

Note that it is quite likely that a PSOBU will have multiple certificates corresponding to different geographic regions. This is a straightforward way to provide permissions for a number of disjointed regions or to tile regions with a complicated boundary. The size and placement of certificate scopes is a local policy matter for the CA.

OBU Certificates

OBU certificates have some significant differences from other types of certificates. First, unlike CA, RSU, or PSOBU certificates, OBU certificates are all alike. The only meaning of an OBU certificate is "this public key belongs to an OBU". Thus, OBUs do not have any scope value, as the only important authorization is communicated by the fact that it is a certificate of type `obu`.

OBU Certificate Linkage

The anonymity of certificates presents a problem for revocation. Once a given certificate is implicated in a bad act, revoking it is straightforward. However, because each OBU has a large number of certificates, this does not substantially contain the compromise of a unit, as the attacker can simply use another one of the unit's certificates. Thus, it needs to be possible to revoke all of a unit's certificates when one is observed. The linkage field allows this mapping to be performed.

Because the ability to revoke all certificates issued together is equivalent to the ability to link transmissions from a single unit, it must be impossible for generic attackers to perform this operation--the ability to link certificates is confined to a trusted identity escrow agency. This section describes a linkage token with the appropriate properties.

We assume that the escrow authority has an ECDH key pair where the public key Y and group `g,p` is known to the OBU at certificate issuance time. We also assume an "anonymity work factor" w and that each OBU is issued n keys. Those keys are numbered from 1 to n.

1. The OBU generates a cryptographically random key k of length 256 bits.
2. For each certificate i (where i is the key number) the OBU generates a cryptographically random value r[i] of length w bits.
3. For each certificate i the OBU computes the following values:

W[i]=AES-ECB(k,i)

h[i]=SHA1(0||r[i]||W[i]||LinkageMarkerString)

e[i]=SHA1(1||r[i]||W[i])

B[i]=AES(e[i],k)

where `LinkageMarkerString` is the ASCII representation of "VSP 1.0 OBU Linkage Computation".

The encryption of B[i] is performed using the AES key wrap defined in RFC 3565[44] 128-bit AES. The first 16 bytes of e[i] are used as the AES key.

The `h[i],B[i]` pairs are encrypted under the escrow authority's public key. The exact mechanism is a local matter, however we recommend S/MIME.

The linkage value for certificate i is given as:

```
struct {
    opaque      enc_w<2^8-1>;
    uint16      i_value;
} LinkageData;
```

`enc_w` is simply the high order bytes of W[i]. Currently, implementations should use 10 byte linkage values.

`i_value` contains the i value for this specific certificate.

When an OBU certificate is implicated in bad actions, we wish to be able to revoke all the certificates issued to that OBU. In order to do that, we need k. Given a `LinkageData` value, the escrow authority can determine k using the following algorithm.

1. Decode the structure to recover `W[i]`.
2. Exhaustively search candidate `r[i]` values until one is found that produces a known `h[i]` value. Note the use of the p in the `h[i]` computation. This is intended to assist in the detection of attempts to use distributed computation networks to perform this operation.
3. Form `e[i]` and decrypt k.

In order to revoke a unit the CA simply publishes its k value on the CRL. Any receiver can easily compute the relevant `W[i]` values.

The choice of `w` is a tradeoff between work to recover from compromise and privacy protection.

CRL Signer Certificates

A certificate of type `crl_signer` indicates that the holder of this certificate is entitled to sign CRLs for this certificate authority. The `responsible_series` array contains all of the CRL series for which this CRL can sign.

5.3.2 Certificate Revocation List Format

VSP uses two kinds of CRLs, one for non-anonymous units such as CAs, RSUs, and PSOBUs and one for anonymous units such as OBUs. However, both CRLs have the same basic structure, which combines both regular CRLs and delta CRLs.

```
struct {
    uint32          length;
    UnsignedCRL     unsignedCRL;
    Signature       signature;
} OrdinaryCRL;

struct {
    CRLSeries       crl_series;
    SignerID        certificate_type;
    SubjectType     entry_type;
    uint32          crl_serial;
    Date            last_crl;
    Date            this_crl;
    Date            next_crl;
    CRLEntry        entries<2^64-1>;

    SignerInfo      signer;
} UnsignedCRL;

struct {
    select(certificate_type){
        case ca:
        case psobu:
        case rsu:
            CertificateHash  cert_hash;
        case obu:
```

```
            OBUCRLLinkage    obu_link;
        }
    } CRLEntry;
```

The `ca_id` field contains the CA for which this CRL is being issued.

The `crl_series` represents the CRL series that this CRL is for.

The `certificate_type` indicates the kind of certificates that this CRL is for.

The `crl_serial` is simply a counter that should increment by 1 for every issued CRL by that CRL issuer.

The `last_crl` and `this_crl` fields specify the time period that this CRL covers. Thus, any certificate that was revoked between `last_crl` and `this_crl` must appear on the CRL. Note that there is no requirement that the time windows represented by any two CRLs not overlap. This allows the issuance of delta CRLs or sliding window delta CRLs [45].

The `next_crl` value contains the time when the next CRL is expected to be issued. See Section 5.3.4.5.6 for discussion of the behavior of recipients with respect to CRLs.

`Entries` contains a list of the certificates that were revoked during this time period.

As usual, the signer field specifies the public key used to sign the CRL. There are two possibilities for the CRL signer:

1. It is the CA that originally issued the certificate.
2. It is a CRL signer authorized by the CA to issue CRLs.

In the latter case, the signer field must be of type certificate and the certificate must be of type `crlsigner`. That certificate must be directly signed by the original CA contained in the `signer_id`. The `responsible_series` field of the certificate must contain the value of the `crl_series` field of the CRL.

The length field of the `OrdinaryCRL` structure contains the length of the remaining structure (i.e. the combined length of the `unsigned_crl` and signature.

The signature field contains a digital signature over the encoded `unsigned_crl` value.

Partitioned CRLs

In order to keep down the size of individual CRLs, it may be desirable to maintain multiple CRL series for any given CA. Accordingly, a CA might break up the CRLs it issues into units of (say) 10000 certificates, each of which is issued on its own CRL series. Thus, a receiver would only need the relevant CRL for the certificate it was trying to verify rather than all CRLs for a given CA. The `crl_series` value is intended for this purpose. The number of CRL series and the partitioning of CRLs into a individual CRL series is a local matter for the CA, with one exception: OBUs must be randomly assigned to CRL series so that the CRL series in an OBU certificate does not leak information about the vehicle identity.

Non-Anonymous CRLs

In non-anonymous CRLs, used for all units besides OBUs, the certificates on a CRL are specified by `CertificateHash` .

```
opaque CertificateHash [10];
```

The CertificateHash must be the high order 10 bits of a SHA-1 digest of the revoked certificate.

Entries on a non-anonymous CRL must be sorted in increasing order of SHA-1 hash. Comparisons are done in big- endian format, treating the first byte of the SHA-1 hash as the most significant bit and each successive byte as less significant. This allows the receiving unit to do a binary search to determine if a certificate is on the CRL.

Anonymous CRLs

In the case where the revoked unit is an OBU, the `CRLEntry` contains an `OBUCRLLinkage` value:

```
opaque          OBUCRLLinkage <1 .. 2^8-1>;
```

The `OBUCRLLinkage` simply contains the unit key k, described in Section 5.3.1.5.1.

Note that the process of verifying whether an OBU certificate is on a CRL is modestly computationally expensive: it requires precomputing the linkage values for all the current revoked units for the value of i in the certificate. In general we expect that units that need to verify OBU signatures will have an AES accelerator. Currently available cheap AES cores can perform on the order of 108 AES operations per second and could therefore check a million revoked OBUs in .01 s. Implementations may choose to cache known to be valid certificates once this check has been performed.

5.3.3 VSP Message Format

There are two kinds of messages that are transmitted over the air in the VSC system:

- Safety messages
- Updates

However, both kinds of message have a common format:

```
enum { signed(0), (255)} MessageType;

struct {
    uint8           protocol_version;  /* 1 for this version */
    MessageType         type;
    opaque          message<2^16-1>;
} VSPMessage;
```

The `protocol_version` contains the current version of the protocol. The version described in this document is version 1, represented by the integer 1. There are no major or minor version numbers.

The type field contains the type of the message. This tells the receiving unit how to interpret the message body.

Currently the only defined types is signed (0) indicating a signed message. This leaves room for up to 254 other message types. All message types must be standardized before they may be used in real systems. Message types from 240 through 255 will not be assigned and are reserved for private usage in test environments. Production units must not generate messages with these types.

The message field is simply a block of bytes. These bytes are interpreted according to the type field. In particular, if the type field is signed then the message block is a `SignedMessage`, as specified in the next section.

5.3.4 Signed Message Format

Most of the messages in the VSP system are of type `SignedMessage`. The full PDU on the air thus looks something like the figure below:

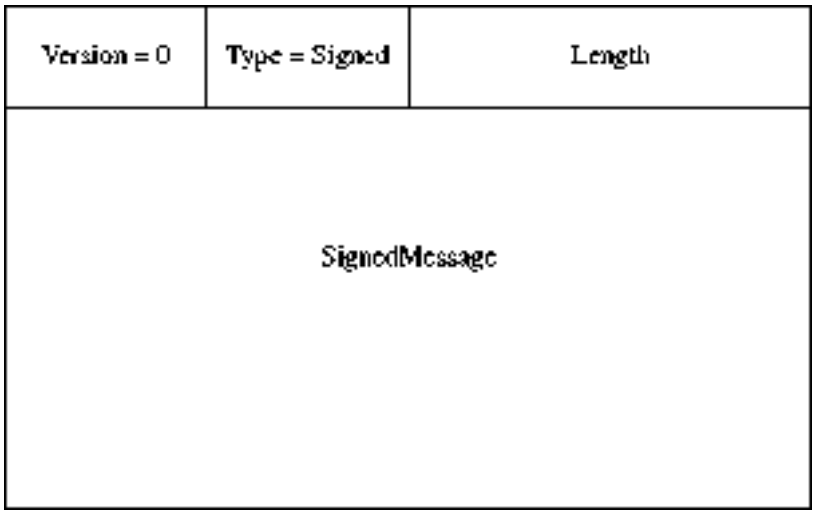


Figure 16: Subset difference broadcast tree

The specification for a `SignedMessage` is:

```
struct {
    ApplicationID    application;
    opaque           flags<0 .. 2^8-1>;
    opaque           application_data<1 .. 2^16-1>;
    opaque           message_id[2];
    Time             transmission_time;
```

```
    3DLocation      transmission_location;
    SignerInfo      signer;
} ToBeSigned;

struct {
    ToBeSigned      unsigned_message;
    Signature       signature;
} SignedMessage;

uint64          Time;
```

The application field contains the type of message being transmitted.

The flags field contains message-specific flags represented as a big-endian integer. A flag is set by `ORing` 2 flag it into the flags vector. The flags field should be the minimum necessary length. Thus, a vector where flags 2 and 5 was set would be the bytes 01 24. The only flag available is fragment (0) indicating that the message has been fragmented using the procedure specified in Section 5.3.5.4.

The `application_data` field contains the data for the application. This is not interpreted by the security protocol and is passed unchanged up to the application.

The `message_id` is a two-byte string that is unique for the `transmission_time` value.

The `transmission_time` field contains the time at which the message was generated in microseconds since the UNIX epoch (midnight, January 1, 1970).

The `transmission_location` field contains the location to which the message applies. For an OBU, this should be the current location of the unit as indicated by the GPS. An RSU, however, may "speak for" a physical unit that is not exactly in the same location as the antenna. For instance, a single RSU might broadcast messages for stop signs on four corners of an intersection. Such usages are explicitly permitted.

The signer value contains enough information to determine the keying material used to sign the message – though not necessarily the identity of the signer.

The signature block contains the digital signature itself.

Location Encoding

VSP uses lat/long/altitude coordinates to represent position, encoded in the Location structure:

```
struct {
    opaque      latitude[5];
    opaque      longitude[5];
    uint16      altitude;
```

```
} 3DLocation

struct {
    opaque      latitude[5];
    opaque      longitude[5];
} 2DLocation
```

`Latitude` and `longitude` are encoded as described in RFC 3825 [47], with a 6-bit resolution field and a 34-bit 2s complement fixed-point value. Implementations should use a resolution no less fine than 1 meter.

`Altitude` contains the an altitude position indicator in meters. All positions must use the WGS 84 [48] Datum.

Signer Info

The `SignerInfo` structure allows the recipient of a message to determine which keying material to use to authenticate the message:

```
struct {
    SignerIdentifierType    id_type;

    select (id_type) {
      case certificate:
        VSPCertificate certificate;
      case certificate_digest:
        opaque      digest[20];
    }
} SignerInfo;

enum { certificate(0), certificate_digest(1), (255)} SignerIdentifierType.
```

Currently, the `SignerInfo` may contain either a certificate or a message digest of a certificate. If the `id_type` field contains certificate (0) then the `SignerInfo` contains a certificate. If the `id_type` field contains `certificate_digest` (1) then the `SignerInfo` contains the `SignerID` corresponding to the relevant certificate.

Signature

The signature field contains the actual signature. The signature algorithm is uniquely determined by the type of the key used to generate the signature. There are no in-message indicators for signature algorithm type.

The signature is computed over the encoding of the entire `ToBeSigned` structure. Thus, for instance, if ECDSA is used as the signature algorithm the input message M to Hash(M) is the value of `unsigned_message`.

The signature value is simply a byte-string encoded in a signature algorithm-specific manner. Currently, the only algorithm so defined is ECDSA. Section 5.3.4.3.1 provides details on the use of ECDSA in VSP.

ECDSA Signatures

ECDSA signatures are performed as described in [46]. The input message is the encoded `unsigned_message` value. An ECDSA signature consists of two values r and s. These integers shall be converted into byte strings of the same length as the curve order n using the procedure of Section 4.3.1 of ANSI X9.62 [46]. The strings are padded with leading zeros to obtain the appropriate length. The strings are then concatenated to form the appropriate signature value:

```
struct {
    opaque[curve_order] r;
    opaque[curve_order] s;
} ECDSASignature;
```

Note that because the verifier knows the size of the curve, this structure can be unambiguously parsed despite the lack of length fields.

Transmission Processing

RSU and PSOBU transmission processing is straightforward:

1. Generates a random message ID.
2. Get the current position and time values.
3. Encode the `unsigned_message` value.
4. Digitally sign the `unsigned_message` value.
5. Create and encode the `SignedMessage` value.

OBU transmission processing is similar but with one important difference: the message signature must be performed in a tamper-resistant hardware security module (HSM). The `message_id, transmission_time`, and `transmission_location` values must be generated inside the HSM. Thus, the tamper-resistant module must contain a real- time clock, GPS processor, and the cryptographic keying material. This ensures that the unit cannot forge messages with arbitrary positions or timestamps.

Reception Processing

When a unit receives a `SignedMessage` it must use the following process – or its equivalent – in processing it:

1. Decode the message.
2. Check that the `transmission_time` is within the acceptable time window. If not, discard the message.
3. Check that the `transmission_position` is within the acceptable position window. If not, discard the message.
4. Look up the message in the cache of recently received messages. If the message has already been received, discard it as a replay.
5. If the sender's certificate contains a scope restriction, verify that the `message_position` is within the geographic scope of every certificate in the sender's certification path. If not, discard the message.
6. Verify that the application field in the message is consistent with the scope restriction in the certificate.
7. Verify that the sender's certificate has not been revoked. If the sender's certificate has been revoked, discard the message.
8. Verify the sender's certificate. If the sender's certificate does not verify, discard the message.
9. Verify the signature on the message. If the signature does not verify, discard the message.
10. If all the previous tests verify, pass the message up to the application layer.

Note that this process is carefully designed to minimize the number of public key operations. Thus, checks 1-7 all can be performed with minimal computational overhead. Check 8 can be cached if the same certificate is seen multiple times. Thus, the only per-message computational overhead is seen in step 9. Implementations can use any equivalent process, however this algorithm is likely to be the most efficient.

Anti-Replay

Anti-replay in VSP takes advantage of the fact that each unit has an accurate clock. Thus, the clock in the sending unit (and, therefore, the timestamps in its messages) will be closely synchronized to that of the receiving unit. The receiving unit must use the following algorithm to prevent replays.

Each receiving unit maintains an anti-replay window of size 2r; r should be at least 30 seconds. The receiver's idea of the current time is set to T. When a packet is received with timestamp t, the following procedure is followed:

1. If `t<T-r` discard the packet as out of window.
2. If `t>T+r` discard the packet as out of window.
3. If a copy of the packet is in the "already received" cache, discard the packet as a replay.
4. If the packet is accepted, add it to the already received cache and deliver it.

Every time that T advances, the already received cache should be emptied of all packets older than T-r. A ring buffer is a convenient data structure for this purpose; however, the exact choice of implementation is left up to the implementer.

Constructing the Certification Path

Certification path construction in VSP is an all-or-nothing proposition. Because messages must be processed in real time, implementations must either have the certificates on hand to verify a message or reject that message. Implementations must follow a procedure equivalent to the following algorithm, which is a form of the usual bottom up construction approach:

1. Set C equal to the current certificate and i=0
2. Set `path[i]=C`.
3. Set `i=i+1`.
4. If C is a trust anchor, the path is complete. Output path and i.
5. Parse C and extract the `signer_id` field
6. If there is a certificate in the local certificate cache such that the high order bits of `SHA1(S)` match the `signer_id`, call that certificate S. Otherwise, exit and output failure.
7. Set `C=S`.
8. Go to step 2.

The algorithm above delivers either an error or an unverified certification path of length i. Once the certificate is constructed, it must be verified, as described below. As noted before, we deliberately perform all the checks that can be performed with the unverified certification path before incurring the costs of signature verification.

Location Checks

Once the certification path is constructed, the recipient needs to verify that the location in the message is within the `GeographicScope` restrictions of the certification path. For each certificate in the path, the recipient must check that the location in the message is within that certificate's `GeographicScope`. Note that we do not require that the region permitted by each certificate be completely contained within the scope of the CA that signed that certificate. All that is necessary is that the location of the message be within the scopes of all the authorizing certificates in the certification path.

Usage Checks

The recipient must also check the usage restrictions on the certificates in the certification path. Each certificate except the end-entity `certificate path[0]` must be of type ca.

If the end-entity certificate is of type `rsu` or `psobu`, then the application field in the `UnsignedMessage` must be present in the application list in the certificate. If the end-entity certificate is of type obu the application field in the `UnsignedMessage` must be one of the applications that are permissible for OBUs. All application descriptions must describe whether they are permissible for OBUs or not. In addition, the recipient must check that the scope restrictions of the CAs in the path permit them to issue the certificates that they have issued. Thus, the application must also be permitted for each certificate in the path.

Check Certificate Cache

Recipients should maintain a cache of valid (both in terms of signature and CRL status). Implementations should check this cache prior to performing the remaining operations. A successful result allows bypassing of the remaining checks.

Certificate Revocation List Checking

Before a message is accepted, the recipient must check the appropriate Certificate Revocation List to determine whether the message was revoked at the time of message generation.

The appropriate CRL is defined as the one with a `ca_id` field that matches the certificate's `signer_id` field and a `crl_series` value that matches that in the certificate.

Once the correct CRL is identified, the recipient must then verify that the signing certificate does not appear on the CRL. For non-anonymous CRLs

, the recipient checks that the certificate hash does not appear on the CRL. For anonymous certificates, the recipient must verify that none of the linkage values in the CRL maps to the signing certificate.

As with any CRL-based system, the question arises of how to behave when the current CRL is not available. This is a particular problem in the VSP system because VSP CRLs are all push. Implementations have no ability to pull a CRL from the CA. Thus, an implementation that has been out of contact for a long period of time may get a message before getting the relevant CRL.

In order to balance the concerns of rejecting valid messages because we do not have a current CRL and of accepting invalid messages because we do not know that the signer is revoked, we recommend that recipients accept certificates for which a current CRL is not available provided that the most recent CRL is not too old. "Too old" is necessarily fuzzy, but we suggest no more than a month and no less than 50% of the time to the next CRL. For example if CRLs are issued on a monthly basis and the most recent CRL was issued on January 1. A recipient might accept certificates that were not revoked as of January 1st in the period February 1-February 14th, and perhaps through February 28th.

Checking Certificate Validity

Once all other checks have been performed, the recipient must check the validity of the signatures of each certificate in the certification path. Each certificate must be signed with the public key of the next higher-level certificate in the path.

5.3.5 System Updates

In order to maintain the VSC system, some data needs to be spread to most or all units in the system. At minimum, all units must contain a recent copy of the OBU CRL list. In addition, all units in a given geographic region need an up- to-date copy of the CRLs that correspond to RSO and PSOBU certificates that are active in that area.

VSP has two mechanisms for widespread (whether global or local) propagation of update information:

1. Broadcast by RSUs
2. Flooding by OBUs

Updates enter the system by being broadcast by an RSU. They are then picked up by OBUs, which propagate them to other OBUs as necessary. A key element of this scheme is that updates can be broken up over multiple messages in such a way that once a critical number of messages are received the entire update can be reconstructed. Section 5.3.5.3 describes this process in detail.

Initial Update Injection

System updates are generated centrally and then propagated to RSUs via mechanisms that are outside of the scope of this protocol. For example, a transportation agency might generate a CRL for its RSUs and then deliver it to the RSUs it operates via wired Internet connections. Once the transmitting RSUs obtain a new update, they transmit it to units in their local area. Section 5.3.5.3 describes the correct transmission strategy.

Update Messages

There are two currently defined types of update, CRLs (application type `crl_transmit`) and certificates (application type `cert_transmit`). In both cases, the `application_data` field of the `signed_message` is set directly to the value of the encoded CRL or certificate If the CRL or certificate is too large to fit in a single message, it must be fragmented, as described below.

Reliable Broadcast of Updates

In general, system updates will be far too large to fit in a single VSP Message structure. Thus, they must be split over multiple messages. In order to do this efficiently without requiring an acknowledgement channel, we use expandable forward error correction codes, as described in RFC 3450-3453 [49]. These codes allow split a message into pieces such that any subset of those pieces of combined size approximately that of the original message can be used to reconstruct the original message

A sender starts with a message M. It then generates and transmits a series of symbols using the following algorithm:

1. Generate a random symbol_id.
2. Compute the corresponding symbol using Ssymbol_id = FEC_encode(symbol_id,M).
3. Transmit the pair (symbol_id,Ssymbol_id).

Because the `symbol_id` is randomly generated, the sender can be stateless. As long as the `symbol_id` space is relatively large (e.g., 32 bits), the probability of symbol repetition is low. As many output symbols can be generated as the number of possible `symbol_ids`. In VSP, source symbols are transmitted using the following structure:

```
struct {
    opaque      update_digest[20];
    uint32      required_symbols;
    uint8       fec_scheme;
    uint32      source_block;
    uint32      symbol_id;
```

```
    opaque          symbol<1 .. 2^16-1>;
} EncodedSymbol;
```

`EncodedSymbol` structures are constructed using the procedure described in RFC 3450.

`update_digest` is a SHA-1 hash of the original source message, which allows recipients to disambiguate different fragments for reassembly.

`required_symbols` contains the expected number of symbols which will be required for reconstruction. This allows the recipient to know when to start reconstructing.

Transmitting Update Fragments

A transmitting unit transmits an update as a stream of `EncodedSymbol` structures. In order to prevent denial of service attacks on individual update messages, each symbol must be signed. The symbols are transmitted as `SignedMessage` objects with the appropriate application ID, either `cert` or `crl`. Before attempting to reconstruct a message, the recipient should verify the fragment certificates. This does not ensure validity of the reconstructed message but merely ensures that the fragments were not tampered with, thus avoiding reconstruction errors. The recipient must still verify the signature on the reconstructed object (e.g., certificate or CRL).

5.4 Enrollment Procedures

The first thing that a unit must do in order to transmit VSP messages is to enroll and get certified keying material. In the case of CAs, RSUs and PSOBUs, this is a fairly straightforward procedure, described in Section 5.4.1. Enrollment for OBUs is complicated by the requirement for privacy and is described in Section 5.4.2.

5.4.1 CAs, RSUs, and PSOBUs

Because CAs, RSUs and PSOBUs are authenticated via ordinary PKI-style mechanisms, enrollment of these units can be done in the conventional way. To a first order, this is a manual process: the enrolling party (the future certificate holder) presents the CA with:

Its public key

1. Its desired authorization information (scope)
2. Documentation indicating that it is entitled to the desired certificate.

The CA then decides whether to issue a certificate or not based on its internal policies. If the policy checks succeed the CA returns a certificate to the unit.

Although these processes are inherently somewhat manual, experience with PKI systems has shown that it is helpful to have standard formats for certificate signing requests (CSRs) and delivery of the return certificates. We describe those here.

Certificate Signing Requests

In order to get a certificate signed, the enrollee first generates an asymmetric key pair and uses it to construct a CertificateSigningRequest object.

```
struct {
    uint8           csr_version;
```

```
        SubjectType       type;

        CertSpecificData type_specific_data<1 .. 2^16-1>.
        PublicKey       public_key;
    } UnsignedCSR;

    struct {
        UnsignedCSR       unsigned_csr;
        Signature       signature;
    } CertificateSigningRequest;
```

The csr_version field should be set to 1 for this specification.

The subject_type should specify the desired type of certificate. Note that the value must not be obu.

The type_specific_data field should specify the desired scope. Note that this is rendered as a variable length value. This enables the enrollee to specify no scope value (by using a zero length) and let the CA insert a correct scope. Only one CertSpecificData structure should appear in this field.

The public_key field contains the public key of the enrollee.

The signature field contains a signature over the encoded unsigned_csr value using the private component corresponding to the public_key value.

Trust Anchor Certificates

In VSC, trust anchors are represented as self-signed certificates. These certificates are precisely like ordinary CA certificates except that they have a `signer_id` that consists entirely of zeros.

Certificate Issuance

Once a CA receives a CSR, it must compare it with the associated documentation (delivered in an unspecified manner) and decide whether the certificate can be issued according to the CA policies (also a local decision). If the certificate can be issued, the CA then formats the appropriate `UnsignedCertificate` structure and signs it to generate a Certificate value. Note that the CA is not bound by the enrollee's suggestion of subject type or scope. It may issue a certificate of any type or scope of its choosing. However, a CA should not generate certificates which will not result in verifiable certificate chains, e.g. by listing geographic scopes which are not within the CA's own scope.

Once the Certificate is created, the CA returns it in a `CertificateResponse` structure.

```
    struct {
        Certificate       certificate_path<1 .. 2^32-1>;
```

```
        OrdinaryCRL        crl_path<1 .. 2^32-1>;
    } CertificateResponse;
```

The `certificate_path` contains the certificate path of the new certificate. This path is in order, with the most local certificate (the newly issued one) being first and each successive certificate signing the one before it. The path should be complete with the final certificate being a trust anchor. However, some implementations may choose to deliver less complete paths for space reasons.

The `crl_path` contains the CRLs necessary to validate the certificate. At minimum, it must contain the most recent version of the CRL series on which the issued certificate would appear if it were revoked. In addition, CAs should include CRLs corresponding to other CAs in the chain. These CRLs are not ordered.

5.4.2 OBUs Certificate Initialization

OBUs should be initialized by their manufacturers. This initialization must happen in such a way that no identifying information is stored linking any given OBU certificate to the identity (serial number, physical identity, etc. of the OBU).

The VSC team anticipates that the OBU CA and the OBU to be initialized will be physically collocated. When the operator of the CA authorizes the initialization of the OBU, the OBU generates a series of `CertificateSigningRequests` and provides them to the CA. The OBU also provides the encrypted h[i],B[i] pairs to the CA. Note that the escrow authority may not (and probably should not) be the same as the CA. The CA then signs the certificates and returns the `CertificateResponse` values. At this point the OBU is initialized.

5.5 Suggested Operating Procedures

This section provides identification of some of the security architecture operating requirements that will arise, and suggests a solution.

5.5.1 OBU Operating Requirements

Because OBUs are allowed to send so many different kinds of messages from so many different locations, the OBU must be designed to restrict the class of messages that can be sent.

The OBU signing keys must be embedded in a tamper- resistant Hardware Security Module (HSM). This HSM must be compliant with FIPS 140-2 level 3. The HSM must be designed not to release the OBU signing keys from the module. In addition, it must not be usable for signing arbitrary messages.

All messages signed by the HSM must be wrapped in a `SignedMessage` structure. The HSM must populate the `message_id`, `transmission_time`, and `transmission_location` fields. The `transmission_time` and `transmission_location` fields must be populated with data received respectively from a clock and GPS unit, which are housed within a FIPS 140-2 level 3 module. It is also recommended that the clock and GPS unit be housed within the same module as the signing module. However, if they are housed within a separate unit, then communications between the two modules must be authenticated with an algorithm that provides at least 100 bits of security and measures must be taken to ensure timing synchronization between the two modules.

The clock must be periodically updated from the GPS unit in order to correct for clock slip. However, because the GPS unit gets its input from radio signals outside the tamper boundary, mechanisms must be used to isolate the system from GPS spoofing. The clock must be calibrated

for maximum slip values and must not allow for corrections beyond those values. In addition, "backward" corrections must be performed by slow-ticking rather than by rolling time backward. In addition, the system should enforce physical plausibility rules, such as rejecting speeds in excess of the maximum speed of the vehicle, impossible altitudes, etc.

5.5.2 OBU CAs and Escrow Authorities

In order to preserve privacy, it is critical that no records be kept of the connection between any individual OBU and the certificates that it was issued. This requires certain procedures from CAs and escrow authorities.

5.5.3 CA's Procedures

For signature algorithms that are compatible with blind signatures, certificates should be signed using a blind signature protocol. However, not all algorithms are compatible with blind signatures. In particular, ECDSA-- which is the only currently defined algorithm--is not. An alternate mechanism is therefore described that should be used in such cases.

The actual CA signing unit should be embedded in a FIPS 140-2 level 4 tamperproof module. The OBU should be physically connected to the CA signing unit (e.g. via FireWire or USB) and should establish a cryptographically secure connection using TLS [6] (the CA's TLS certificate should be wired into the OBU at manufacture). All communications should take place over this channel. Once the certificates have been issued the CA should output the encrypted `h[i],B[i]` pairs and then delete all records of the transaction.

No OBU-specific identifying information should be passed over this channel. Instead, the authorization for this process should be performed by placing the CA in "active" mode. Once the CA is in active mode, it will sign certificates for some number of OBUs without knowing their identities. In order to protect the CA from theft and misuse, the ability to activate the CA should be controlled via conventional cryptographic token and secret sharing technology.

Escrow Authorities

As described in Section 5.3.1.5.1, the ability to link certificates from the same OBU is reserved to Escrow Authorities. In order to preserve privacy, Escrow Authorities should not be the same as the OBU CAs.

Escrow Authorities must keep linkage information under strict physical security and make best commercial efforts to retain confidentiality of said records. Access to the escrowed `h[i],B[i]` pairs should controlled by a FIPS 140-2 level 4 device. This device should restrict the number of linkage events to a limited number per day.

5.6 OBU Privacy Parameters

This section of the document addresses OBU privacy parameters.

5.6.1 Choice of Work Factor for OBU Blinding

Section 5.3.1.5.1 describes a mechanism for increasing the cost of de-escrowing OBU certificates. The rationale here is that OBU revocation will happen relatively rarely and therefore need not be inexpensive. Making the cost of linking OBU certificates relatively high reduces the probability that VSC can be used as a generic tracking system for a large number of OBUs. Thus, w should be chosen so that it is possible to de-escrow OBU certificates when necessary for revocation but sufficiently expensive to make it impractical to do so on a mass basis.

The correct metric for choosing w is cost. It should be sufficiently high that casual de-escrowing is expensive but sufficiently low that it is practical to de-escrow a key. In our constraints analysis,

we estimated that $5,000 would be the target investigative cost for incidents caused by a malicious OBU. Therefore, we recommend that w be chosen so that the cost of revoking an OBU once its certificate is identified be of the same order of magnitude, between $1,000 and $5,000. OBU manufacturers should periodically adjust the value of w upward to keep pace with the increasing speed and decreasing cost of hardware.

5.6.2 OBU Certificates

Giving each OBU a large number of certificates provides unlinkability against ordinary attackers. An attractive feature of the VSP protocol design is that the size of protocol messages is independent of the number of certificates per OBU. Thus, the only constraints on the number of certificates per OBU are the cost of initial OBU initialization and OBU memory.

We recommend that at minimum each OBU be issued 5,000 certificates. In order to minimize information leakage, signing keys should be randomly selected and used for a short time period and then discarded. Implementations may use the following algorithm, which produces a key half-life of h seconds or m miles, for key selection, with a uniform probability that a key will be discarded in any time period.

1. Select a random number r uniformly from the set [1,n]
2. Set the current key to K[r]. Set t0 to the current time in seconds.
3. As each second passes, with probability $[\log(2)]/h * e^{\log(.5/h)}$ discard the key and go to step 1.
4. As each mile passes, with probability $[\log(2)]/m * e^{\log(.5/m)}$ discard the key and go to step 1.

Because the probability that a key will be discarded is uniform, this leaks the minimal amount of information.

We recommend values of h=600, m=10. With these values, a vehicle moving at 60 mph will have a key half-life of 5 minutes. As a special case, we recommend not changing keys when the vehicle is not in motion. This prevents an attacker from observing large number of keys from parked running vehicles.

5.7 Opportunities for Optimization

Compactness of encoded protocol data units is an important consideration for VSC. VSP has, therefore, been designed to be fairly parsimonious with respect to PDU size. However, in the interest of maximizing protocol and design flexibility we have deliberately chosen not to make a number of small optimizations that would individually save a byte or two. It may be discovered that these optimizations pay off in the future as the protocol becomes more refined. Some such optimizations are listed here.

5.7.1 Combined Algorithm Identifiers

Currently VSP uses separate algorithms and parameters. Thus, ECDSA has a parameter specifying the group being used. This preserves the maximum amount of flexibility because it allows an arbitrary amount of information to be carried in algorithm parameters. However, it also consumes additional space and is unnecessary if there are only a small number of algorithm/parameter pairs. Identifying these pairs by a single integer would save a byte or two per certificate.

5.7.2 Length of Fields

VSP makes use of variable-length fields in a number of locations. These fields are denoted by use of the notation `<YYY - XXX>` where `XXX` is the maximum length of the field. When such fields are encoded, they are encoded by first encoding the length and then the value. The length is encoded as a fixed-width value of 1-byte multiples. Thus, in order to encode a field that might be 256 bytes long, we need a 2-byte length field – the same size length field as would be required for a value with a maximum length of 65535 bytes. Thus, whenever we wish to reserve a length larger than that which would fit in x bytes, we instead use the largest length that would fit in x+1 bytes. It is not expected that fields of that size will ever appear.

There are two potential optimizations here:

1. Restrict maximum lengths more tightly in the protocol. E.g., use opaque field `<1 .. 500>`.
2. Use smaller maximum length values, thus saving length bytes.

The first option only prevents programmers from using large data sizes, but doesn't provide an immediate savings. The second option provides a single byte saving for every field where the field is represented.

5.8 Summary of Syntax

This section provides a summary of the syntax discussed heretofore:

```
struct {
    uint8             certificate_version;
    SubjectType       subject_type;
    CertSpecificData  type_specific_data;
    Date              expiration;
    CRLSeries         crl_series;
    SignerID          signer_id;
    PublicKey         public_key;
} UnsignedCertificate.

opaque[8]     SignerID;
uint16        CRLSeries;

struct {
    select(subject_type){
      case ca:
        CAScope     scope;
      case rsu:
        RSUScope    scope;
      case psobu:
```

```
          PSOBUScope  scope;
        case obu:
          LinkageData linkage;
        case crlsigner:
          CRLSeries   responsible_series<2^16-1>;
      }
} CertSpecificData;

enum {ca(0), rsu(1), psobu(2), obu(3), crlsigner(4), (255)} SubjectType;

uint16 Date;

struct {
      SignatureAlgorithm algorithm;

      select(algorithm){
        case ecdsa:
          ECDSAKey key;
      }
} PublicKey;

struct {
      opaque point<1..2^8-1>;
} ECPoint;

enum { ecdsa(0), (255)} SignatureAlgorithm;

struct {
      uint16              length;
      UnsignedCertificate  unsigned_certificate;
      Signature           signature;
} VSPCertificate

opaque    Signature<1 .. 2^16-1>;

struct {
      NamedCurve        curve;
      ECPoint           point;
} ECDSAKey;

enum {
```

```
    K-163(1),
    B-163(2),
    K-233(3),
    B-233(4),
    reserved (5..239),
      private (240..255)
} NamedCurve;


struct {
     opaque point <1..2^8-1>;
} ECPoint;


struct {
       ApplicationID          applications<0 .. 2^16-1>;
       SubjectType            unit_types<1 .. 2^8-1>;
       GeographicRegion       region;
} CAscope.


struct {
      ApplicationType     type;
      ApplicationSubtype  subtype;
} ApplicationID;

enum  {cert_transmit(0), crl_transmit(1), (2^16-1)} ApplicationType;
opaque ApplicationSubtype<0 .. 255>;
enum  {fragment(0), (2048)} MessageFlags;


struct {
       RegionType   region_type;

       select(region_type){
         case polygon:
         PolygonalRegion    polygonal_region;
         case circle:
         CircularRegion     circular_region;
         case rectangle:
           RectangularRegion     rectangular_region<2^16-1>;
```

```
        }
}

enum {polygon(0), circle(1), rectangle(2), (255)} RegionType;


PolygonalRegion        2DLocation<2^16-1>;

struct {
      2DLocation   center;
      uint16       radius;
} CircularRegion;


struct {
    2DLocation     upper_left;
    2DLocation     lower_right;
} RectangularRegion;


struct {
       GeographicRegion        region;
       ApplicationID           applications<0 .. 2^16-1>;
} RSUScope;


struct {
       GeographicRegion        region;
       ApplicationID           applications<0 .. 2^16-1>;
} RSUScope;


struct {
       GeographicRegion        region;
       ApplicationID           applications<0 .. 2^16-1>;
} PSOBUScope;


struct {
      opaque        enc_w<2^8-1>;
      uint16       i_value;
```

```
} LinkageData;


struct {
    uint32          length;
    UnsignedCRL     unsignedCRL;
    Signature       signature;
} OrdinaryCRL;

struct {
    CRLSeries       crl_series;
    SignerID        certificate_type;
    SubjectType     entry_type;
    uint32          crl_serial;
    Date            last_crl;
    Date            this_crl;
    Date            next_crl;
    CRLEntry        entries<2^64-1>;

    SignerInfo      signer;
} UnsignedCRL;

struct {
    select(certificate_type){
        case ca:
        case psobu:
        case rsu:
            CertificateHash  cert_hash;
        case obu:
            OBUCRLLinkage    obu_link;
      }
} CRLEntry;


opaque CertificateHash[10];


opaque          OBUCRLLinkage <1 .. 2^8-1>;


enum { signed(0), (255)} MessageType;
```

```
struct {
    uint8              protocol_version;  /* 1 for this version */
    MessageType        type;
    opaque             message<2^16-1>;
} VSPMessage;


struct {
    ApplicationID     application;
    opaque            flags<0 .. 2^8-1>;
    opaque            application_data<1 .. 2^16-1>;
    opaque            message_id[2];
    Time              transmission_time;
    3DLocation        transmission_location;
    SignerInfo        signer;
} ToBeSigned;

struct {
    ToBeSigned        unsigned_message;
    Signature         signature;
} SignedMessage;

uint64            Time;


struct {
    opaque        latitude[5];
    opaque        longitude[5];
    uint16        altitude;
} 3DLocation


struct {
    opaque        latitude[5];
    opaque        longitude[5];
} 2DLocation


struct {
    SignerIdentifierType     id_type;
```

```
        select (id_type) {
          case certificate:
            VSPCertificate certificate;
          case certificate_digest:
            opaque        digest[20];
        }
} SignerInfo;

enum { certificate(0), certificate_digest(1), (255)} SignerIdentifierType.


struct {
      opaque[curve_order] r;
      opaque[curve_order] s;
} ECDSASignature;


struct {
        opaque              update_digest[20];
        uint32              required_symbols;
        uint8               fec_scheme;
        uint32              source_block;
        uint32              symbol_id;
        opaque              symbol<1 .. 2^16-1>;
} EncodedSymbol;


struct {
        uint8               csr_version;
        SubjectType         type;

        CertSpecificData type_specific_data<1 .. 2^16-1>.
        PublicKey           public_key;
} UnsignedCSR;

struct {
        UnsignedCSR         unsigned_csr;
        Signature           signature;
} CertificateSigningRequest;
```

```
struct {
    Certificate        certificate_path<1 .. 2^32-1>;
    OrdinaryCRL        crl_path<1 .. 2^32-1>;
} CertificateResponse;
```

6 References

1. CAMP VSC Consortium, *Vehicle Safety Communications Project, Task 3 Final Report* (May, 2004).
2. Housley, R., Polk, W., Ford, W., and Solo, D., "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," RFC 3280 (April 2002).
3. NIST, "Security Requirements for Cryptographic Modules," FIPS PUB 140-2 (2002).
4. Rescorla, E., Korver, B., and IAB, "Guidelines for Writing RFC Text on Security Considerations," RFC 3552 (May 2003).
5. Bellardo, J., and Savage, S., "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions," *Proceedings of the 12th USENIX Security Symposium* (August 2003).
6. Frederick, et al., "Cellular Telephone Fraud Anti-Fraud System," *US Patent 5,448,760* (September 5, 1995).
7. Chaum, D., and van Heijst, E., "Group Signatures," *EUROCRYPT 91*, pp. 256-265, Springer-Verlag (1991).
8. Tsudik, G., and Xu, S., *Accumulating Composites and Improved Group Signing*.
9. Viega, J., and McGraw, G., *Building Secure Software*, Addison-Wesley (2002).
10. Chesson, G., Personal communication.
11. Rescorla, E., “Security Holes... Who cares?,” *Proceedings of the 13th USENIX Security Conference* (2003).
12. Housley, R., Polk, W., Ford, W., and Solo, D., “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,” RFC 3280 (April 2002).
13. Housley, R., “Cryptographic Message Syntax,” RFC 3369 (August 2002).
14. Nagle, J., “Congestion Control in IP/TCP Internetworks,” RFC 0896 (Jan 1984).
15. Kent, S., Atkinson, R., and RFC 2406, *IP Encapsulating Security Payload (ESP)* (November 1998).
16. Myers, M., Ankney, R., Malpani, A., Galperin, S., and Adams, C., “ X.509 Internet Public Key Infrastructure Online Certificate Status Protocol—OCSP,” RFC 2560 (June 1999).
17. Scott, M., *Multiprecision Integer and Rational Arithmetic C/C++ Library*. http://indigo.ie/˜mscott/
18. Rivest, R.L., Shamir, A., and Adelman, L.M., “On Digital Signatures and Public Key Cryptosystems,” Technical Report, MIT/LCS/TR-212, MIT Laboratory for Computer Science (January 1979).
19. Boneh, D., Gentry, C., Lynn, B., and Shacham, H., “A Survey of Two Signature Aggregation Techniques,” *RSA CryptoBytes*, 6, 2 (2003).
20. Rivest, R., Shamir, A., and Adleman, L.M., “Cryptographic communications system and method,” US Patent 4405829 (September 1983).

21. National Institute of Standards and Technology (NIST), and Digital Signature Standard, FIPS PUB 186-2, U.S. Department of Commerce (2000).

22. Kravitz, D., "Digital signature algorithm," U.S. Patent 5,231,668 (July 1993).

23. Schnorr, K., "Method for Identifying Subscribers and for Generating and Verifying Electronic Signatures in a Data Exchange System," US Patent 4995082 (Feb 1991).

24. Certicom, *Possible patents pending Claim on ECDSA*. http://www.ietf.org/ietf/IPR/CERTICOM-ECDSA

25. Pintsov, L.A., and Vanstone, S.A., "Postal Revenue Collection in the Digital Age," *Lecture Notes in Computer Science*.

26. Boneh, D., Lynn, B., and Shacham, H., "Short Signatures from the Weil Pairing," *Proceedings of Asiacrypt 2001* (2001).

27. Naor, D., Naor, M., and Lotspiech, L., "Revocation and Tracing Schemes for Stateless Receivers," *Lecture Notes in Computer Science* (2001).

28. Postel, J., "Transmission Control Protocol," RFC 793 (September 1991).

29. Rizzo, L., "Effective Erasure Codes for Reliable Computer Communication Protocols," *ACM Computer Communication Review* (1997).

30. Sasson, Y., Cavin, D., and Schiper, A., "Probabilistic broadcast for flooding in wireless mobile ad hoc networks," *Proceedings of IEEE Wireless Communications and Networking Conference*.

31. Cartigny J., Simplot D., and Carle, J., *Stochastic flooding broadcast protocols in mobile wireless networks*.

32. Chaum, D., "Blind Signature Systems," *Advances in Cryptology, Crypto '83* (1983).

33. Camenisch, J.L., Piveteau, J., and Stadler, M.A., "Blind Signatures Based on the Discrete Logarithm Problem," *Lecture Notes in Computer Science* (1995).

34. Rabin, M.O., "Digital Signatures," *Foundations of Secure Communications* (1987).

35. Garay, J., Staddon, J., and Wool, A., "Long-Lived Broadcast Encryption," *Lecture Notes in Computer Science* (2000).

36. Jiang, D., "Security Consideration for Vehicle Safety Communications," *ASTM DSRC standardization meeting* (2002).

37. Chaum, D., and van Heyst, E., "Group Signatures," *Advances in Cryptology — EUROCRYPT 91* (1991).

38. Ateniese, G., Camenisch, J., Joye, M., and Tsudik, G., "A Practical and Provably Secure Coalition-Resistant Group Signature Scheme," *Lecture Notes in Computer Science* (2000).

39. Menezes, A., *Elliptic Curve Public Key Cryptosystems*, Kluwer (1993).

40. Lenstra, A.K., and Verheul, E.R., "Selecting Cryptographic Key Sizes," *Journal of Cryptology*, 14, 4, pp. 255-293.

41. Kohno, T,. Stubblefield, A., Rubin, A.D., Wallach, D.S. "Analysis of an Electronic Voting System", *IEEE Symposium on Security and Privacy 2004"*, May 2004.

42. Upton, J., "Gadget may wreak traffic havoc", The Detroit News, October 26, 2003.

Klein-Berndt, J. "NIST Summary of Simulation Results", September 30, 2004.

43. Dierks, T., and Allen, C., “The TLS Protocol Version 1.0,” RFC 2246 (January 1999)

44. Schaad, J., "Use of the Advanced Encryption Standard (AES) Encryption Algorithm in Cryptographic Message Syntax (CMS).," RFC 3565 (July 2003).

45. Cooper, D. A., "A More Efficient Use of Delta-CRLs, "Symposium on Security and Privacy, pp. 190-202.

46. ANSI, "Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)"," ANSI X9.62 (1998).

47. RFC 3825: Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information. J. Polk, J. Schnizlein, M. Linsner. July 2004. (Format: TXT=31715 bytes) (Status: PROPOSED STANDARD)

48. World Geodetic System 1984 (WGS 84), MIL-STD-2401, http://www.wgs84.com/

49. 3450 Asynchronous Layered Coding (ALC) Protocol Instantiation. M. Luby, J. Gemmell, L. Vicisano, L. Rizzo, J. Crowcroft. December 2002. (Format: TXT=86022 bytes) (Status: EXPERIMENTAL)

    3451 Layered Coding Transport (LCT) Building Block. M. Luby, J. Gemmell, L. Vicisano, L. Rizzo, M. Handley, J. Crowcroft. December 2002. (Format: TXT=72594 bytes) (Status: EXPERIMENTAL)

    3452 Forward Error Correction (FEC) Building Block. M. Luby, L. Vicisano, J. Gemmell, L. Rizzo, M. Handley, J. Crowcroft. December 2002. (Format: TXT=38368 bytes) (Status: EXPERIMENTAL)

    3453 The Use of Forward Error Correction (FEC) in Reliable Multicast. M. Luby, L. Vicisano, J. Gemmell, L. Rizzo, M. Handley, J. Crowcroft. December 2002. (Format: TXT=46853 bytes) (Status: INFORMATIONAL)

50. X9.63: American National Standard for Financial Services. ANSI X9.63-2001, Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport using Elliptic Curve Cryptography. November 2001.

7 Exhibit A: Analysis of ECDSA Performance

Only "even" elliptic curves (EC) will be considered here (i.e., EC over GF(2m)). "Odd" EC in general would be fairly comparable – but probably somewhat worse – in speed and size. The silicon industry in general has not seen many chips containing EC, so our estimates are somewhat theoretical in nature, as opposed to the modular math units discussed above for RSA and DSA, where many vendors have produced chips in recent years. However, our estimates here are quite encouraging.

The "straightforward" algorithms used to implement EC are explained in the book Elliptic Curve Public Key Cryptosystems by Alfred Menezes [39]. While it is generally believed possible to implement such EC functions without violating any patents, Certicom is almost guaranteed to disagree, and it may be prudent to obtain a license from Certicom, which fortunately is in the licensing business.

The basic step in an ECDSA signature is a point multiply, while the verify uses two such multiplies. Thus, verification is basically half the speed of signatures. All other operations involved are quite short, from a time perspective. Using the Menezes straightforward approach (page 22), each point doubling requires 1 field inversion, 4 field additions, 2 squares, and 3 multiplications. A point addition requires Over GF(2m), a field inversion can be performed in about *2m* clocks using Euclid's algorithm, and a square and a multiplication each take about *m/2* clocks, assuming we process two multiplier bits per clock. We use no normal bases, which would speed up the squares, since it slows down and complicates all the other steps rather significantly. If we assume that each field operation has an overhead of *H* clocks (where *H* is small, say 4), then a point doubling takes about

$$(2m + H) + 4H + 2(m/2 + H) + 3(m/2 + H) = 4.5m + 10H \text{ clocks}$$

and a point addition takes about

$$(2m + H) + 8H + (m/2 + H) + 2(m/2 + H) = 3.5m + 12H \text{ clocks}$$

For a point multiplication, assuming a random multiplier (i.e., with Hamming weight *m/2*), there are m point doublings and about *m/2* point additions, for a total of

$$6.25m^2 + 16Hm \text{ clocks}$$

Using $m = 163$, which is one of the NIST standard curves for ECDSA, and assuming a frequency of 200 MHz, we obtain a point multiplication time of about 0.8 msec, which easily achieves our signature and verification latency. By building two of these units, we can achieve a throughput of over 2000 ECDSA verifications/sec. The silicon area of each unit should be under 40 Kgates, so the whole core would occupy roughly 75 Kgates, with an incremental cost under $0.30 and a rough power consumption of under 0.2 Watts.

Observe that, if these EC numbers do not quite achieve the speed required (e.g.,if these theoretical estimates are slightly off), then there are several avenues available for optimization. First, the frequency of operation can probably be higher than 200 MHz fairly easily, as GF(2m) field operations never involve carry propagation. Second, it is possible to use somewhat more gates to increase the speed of squares and multiplies, by processing more multiplier bits per cycle. Third, standard windowing techniques for exponentiation could be used to minimize the number of point additions required. Finally, Certicom has some nice pending patents on optimizations that could be licensed to minimize the number of field operations required, basically by removing

the field inversions, without adding significantly to the silicon area. In any case, it seems quite clear that the performance goals for ECDSA can be met at a very reasonable silicon cost.

8 Exhibit B: Choice of Key Size

Although the protocols should be designed to work with a variety of key sizes, in this section we provide guidance for appropriate key sizes. Cryptographic key size is generally a choice between performance (both computation time and message size) and security. The following table (from [32]) shows the approximate strengths and sizes for a variety of ECDSA key sizes (all values in bits).

Key Size	Strength	Signature Size
130	70	130
148	75	148
165	80	165
185	85	185
205	90	205
222	95	222
240	100	240

Table 5: ECDSA Key Strengths and Sizes

We recommend that RSU and OBU keys be chosen at the 80-bit security level. Breaking such keys is well outside current capabilities and is surely far more expensive than simply violating the tamper seal on an OBU or RSU. Compromise of such keys can be dealt with by ordinary revocation mechanisms.

We recommend that OBU CA keys be chosen to be stronger, because failure of such a key is catastrophic. Such keys should be chosen at at least the 90-bit security level. The root RSU CA key should be chosen to be at an equivalent security level. Intermediate and local CA keys can be weaker, especially if they are of limited scope or the keys themselves are of limited lifetime.

9 Exhibit C: The Subset Difference Algorithm

Subset difference is an advanced broadcast encryption scheme with superior properties to the subset cover scheme. As with subset cover, we arrange the nodes in a binary tree. The notation we use is that for any node N_x, the left child is called $N_{x,l}$ and the right child is called $N_{x,r}$. A typical tree is shown in the figure below.

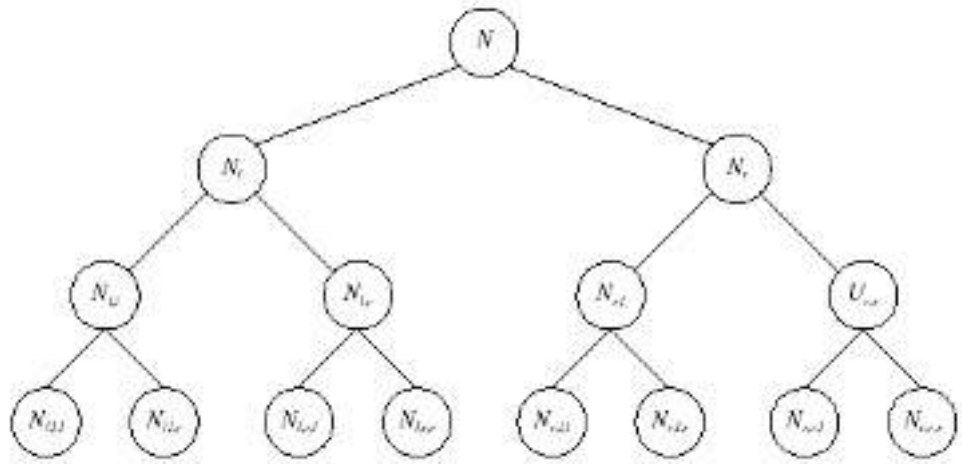


Figure 17: Subset Difference Broadcast Tree

Key assignment in subset difference is different from that of subset cover. In subset cover, a node gets the keys on the path from it to the root. In subset difference it gets the keys that are *off* the path to the root as well as for the children of those nodes. For instance, Figure 18 shows the nodes corresponding to the keys which node $N_{l,l,r}$ has as shaded. Thus, somewhat counter-intuitively, node $N_{l,l,r}$ receives the keys corresponding to nodes $N_{l,l,l}$, $N_{l,r}$ and N_r and their children, namely: $K_{l,l,l}$, $K_{l,r}$, $K_{l,r,l}$, $K_{l,r,r}$ K_r, $K_{r,l}$, $K_{r,l,l}$, $K_{r,l,r}$, $K_{r,r,l}$, and $K_{r,r,r}$.

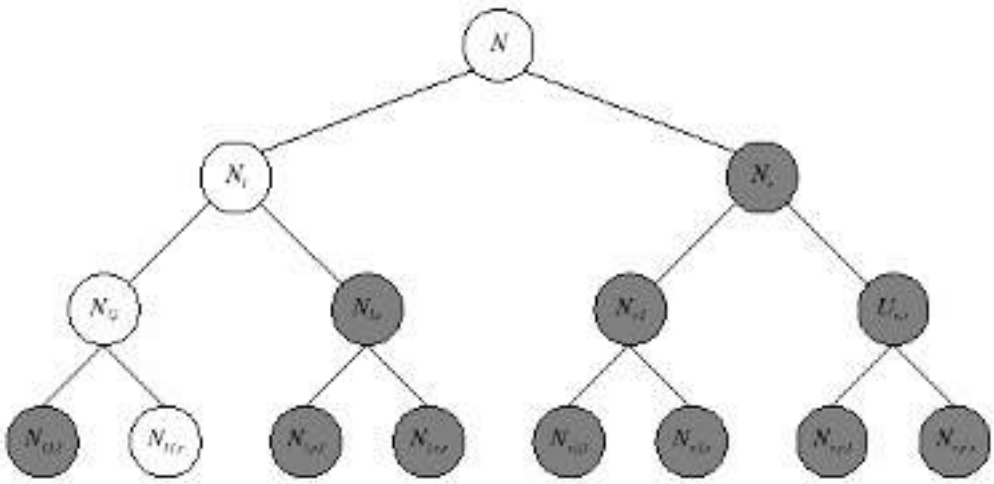


Figure 18: Keys Assigned to Node Nl,l,r

Encryption in subset difference is more complicated than in subset cover. The idea is to encrypt to subtrees with cutouts. So, for instance, we might encrypt to "every child of N_l except $N_{l,l,r}$". We call this subset $S(N_l, N_{l,l,r})$. Now, it should be clear that the only leaf node key that $N_{l,l,r}$ *doesn't* have is $K_{l,l,r}$. Moreover, it is the only node that doesn't have that key! So, if we want to encrypt to $S(N_l, N_{l,l,r})$, we counter-intuitively encrypt under key $K_{l,l,r}$. The nice thing about this scheme is that the ciphertext is much smaller. In order to revoke $N_{l,l,r}$ in the subset cover scheme we would have to encrypt under three keys (K_r, $K_{l,r}$, and $K_{l,l,r}$.). Here we need only encrypt under one key.

The problem here is that each leaf node is issued a ridiculous number of keys, eleven in this very simple system of eight users. However, this can be fixed with a little clever design. Instead of making each key independent, we use hashes to derive the keys for each child node from those of the parent node. Thus, instead of having the key for every other leaf node, each unit just has the keys of all the "off-nodes" in the path to the root and can derive the remaining keys by successive hashing. Thus, the number of keys stored at the end-node is commensurate with that required for subset cover.

10 Exhibit D: Table of Acronyms

ACJT	Ateniese, Camenisch, Joye, Tsudik (group signature algorithm)
BLS	Boneh Lynn Shacham (public key signature algorithm)
CA	Certificate Authority
CRL	Certificate Revocation List
DOT	Department of Transportation
DSRC	Dedicated Short Range Communications
DSA	Digital Signature Algorithm (public key signature algorithm)
ECDSA	Elliptic Curve Digital Signature Algorithm
FIPS	Federal Information PRocessing Standard
MAC	802.11 Media Access Control layer
	(also Message Authentication Code but not in this document--see MIC)
MIC	Message Integrity Check
OBU	On-Board Unit
OEM	Original Equipment Manufacturer
PHY	802.11 Physical layer
PKI	Public Key Infrastructure
PSOBU	Public Safety On-Board Unit
RSA	Rivest Shamir Adelman (public key cryptosystem)
RSU	Road-Side Unit
VIN	Vehicle Identification Number
VSC	Vehicle Safety Communications
VSCC	Vehicle Safety Communications Consortium

Appendix I:
Simulation Testing Results

TABLE OF CONTENTS

1 INTRODUCTION 1
1.1 Simulation Test Scenarios and Setup 1
1.1.1 Intersection Simulation Environment 2
1.1.2 Simulation Communication Settings 2
1.2 Cascading Emergency Message Protocol Design 3
1.2.1 Repetition-Based Cascading Protocol 4
1.2.2 Feedback-Based Cascading Protocol 6

2 SIMULATOR UPDATE 8
2.1 Traffic Trace Generator 8
2.2 Vehicle State and L3 Protocols 12
2.2.1 Vehicle Node IDs 12
2.2.2 Node Behavior Customization 12
2.3 RF Modeling 14
2.3.1 Motivation 14
2.3.2 RF Model Selection 14
2.3.3 RF Model Development 15
2.3.4 RF Model Implementation 17

3 SIMULATION TEST MATRIX 24
3.1 Batch 1, Routine and Emergency Safety Messaging in Saturated Channel 24
3.2 Batch 2, Routine and Emergency Safety Messaging in Less Stressful Channel 24
3.3 Batch 3, Intersection RSU Retransmission of Routine Safety Messages 26
3.4 Batch 4, Cascading Emergency Messages from Intersection 26
3.5 Batch 5, Additional Simulation Tests 27

4 ANALYSIS 28
4.1 Routine Safety Messages at Intersection 28
4.2 Emergency Safety Message at Intersection 33
4.2.1 Emergency Message from Intersection RSU 33
4.2.2 Emergency Message from Vehicle OBUs 34
4.3 Intersection RSU Rebroadcast of Vehicle OBU Messages 36
4.4 Cascading Emergency Messages 40

5 DETAILED SIMULATION TEST RESULTS 42
5.1 Batch 1, Routine and Emergency Safety Messaging in Saturated Channel 42
5.1.1 Scenario 1 42
5.1.2 Scenario 2 45
5.1.3 Scenario 3 47
5.1.4 Scenario 4 49
5.1.5 Scenario 5 51
5.1.6 Scenario 6 55
5.1.7 Scenario 7 59
5.1.8 Scenario 8 64

5.1.9 Scenario 9 ... 68
5.1.10 Scenario 10 ... 70
5.1.11 Scenario 11 ... 72
5.1.12 Scenario 12 ... 74
5.1.13 Scenario 13 ... 76
5.1.14 Scenario 14 ... 80
5.1.15 Scenario 15 ... 84
5.1.16 Scenario 16 ... 89
5.2 Batch 2, Routine and Emergency Safety Messaging in Less Stressful Channel 93
5.2.1 Scenario 17 ... 93
5.2.2 Scenario 18 ... 95
5.2.3 Scenario 19 ... 99
5.2.4 Scenario 20 ... 101
5.2.5 Scenario 21 ... 105
5.2.6 Scenario 22 ... 106
5.2.7 Scenario 23 ... 110
5.2.8 Scenario 24 ... 111
5.2.9 Scenario 25 ... 115
5.2.10 Scenario 26 ... 117
5.2.11 Scenario 27 ... 121
5.2.12 Scenario 28 ... 123
5.2.13 Scenario 29 ... 127
5.2.14 Scenario 30 ... 128
5.2.15 Scenario 31 ... 132
5.2.16 Scenario 32 ... 133
5.2.17 Scenario 33 ... 137
5.2.18 Scenario 34 ... 139
5.2.19 Scenario 35 ... 143
5.2.20 Scenario 36 ... 145
5.2.21 Scenario 37 ... 149
5.2.22 Scenario 38 ... 150
5.2.23 Scenario 39 ... 154
5.2.24 Scenario 40 ... 155
5.3 Batch 3, Intersection RSU Retransmission of Routine Safety Messages ... 159
5.3.1 Scenario 41 ... 159
5.3.2 Scenario 42 ... 163
5.4 Batch 4, Cascading Emergency Messages From Intersection ... 167
5.4.1 Scenario 43 ... 167
5.4.2 Scenario 44 ... 168
5.4.3 Scenario 45 ... 169
5.4.4 Scenario 46 ... 170
5.5 Batch 5, Additional Simulation Tests ... 171
5.5.1 Scenario 47 ... 171
5.5.2 Scenario 48 ... 172
5.5.3 Scenario 49 ... 173
5.5.4 Scenario 50 ... 174

6 FURTHER MESSAGING PERFORMANCE ANALYSIS 175
6.1 Routine Safety Messages 176
6.1.1 Scenario 9 176
6.1.2 Scenario 11 177
6.1.3 Scenario 17 178
6.1.4 Scenario 19 179
6.1.5 Scenario 25 180
6.1.6 Scenario 27 181
6.1.7 Scenario 33 182
6.1.8 Scenario 35 183
6.1.9 Scenario 49 184
6.1.10 Scenario 50 185
6.2 High Priority Emergency Messages 186
6.2.1 Scenario 9 186
6.2.2 Scenario 11 187
6.2.3 Scenario 13 188
6.2.4 Scenario 15 189
6.2.5 Scenario 17 190
6.2.6 Scenario 18 191
6.2.7 Scenario 19 192
6.2.8 Scenario 20 193
6.2.9 Scenario 21 194
6.2.10 Scenario 22 195
6.2.11 Scenario 23 196
6.2.12 Scenario 24 197
6.2.13 Scenario 25 198
6.2.14 Scenario 26 199
6.2.15 Scenario 27 200
6.2.16 Scenario 28 201
6.2.17 Scenario 29 202
6.2.18 Scenario 30 203
6.2.19 Scenario 31 204
6.2.20 Scenario 32 205
6.2.21 Scenario 33 206
6.2.22 Scenario 34 207
6.2.23 Scenario 35 208
6.2.24 Scenario 36 209
6.2.25 Scenario 37 210
6.2.26 Scenario 38 211
6.2.27 Scenario 39 212
6.2.28 Scenario 40 213
6.2.29 Scenario 49 214
6.2.30 Scenario 50 215

7 EFFECTS OF RSU REBROADCAST OF EMERGENCY MESSAGES..... 216

8 ADDITIONAL SIMULATIONS REGARDING ROUTINE SAFETY MESSAGE AT INTERSECTION, BASED ON SCENARIO 11 222

8.1 Routine Messages at 6 Hz, Routine Message Size – 200 byte 222
8.1.1 Reception Probability of Emergency Messages..... 223
8.1.2 Time Bound for Emergency Messages 224
8.1.3 Reception Probability of Routine Messages 225
8.1.4 Time Bound for Routine Messages..... 226
8.2 Routine Messages at 7 Hz, Routine Message Size – 200 byte 227
8.2.1 Reception Probability of Emergency Messages..... 227
8.2.2 Time Bound for Emergency Messages 228
8.2.3 Reception Probability of Routine Messages 229
8.2.4 Time Bound for Routine Messages..... 230
8.3 Routine Messages at 8 Hz, Routine Message Size – 200 byte 231
8.3.1 Reception Probability of Emergency Messages..... 231
8.3.2 Time Bound for Emergency Messages 232
8.3.3 Reception Probability of Routine Messages 233
8.3.4 Time Bound for Routine Messages..... 234
8.4 Routine Messages at 9 Hz, Routine Message Size – 200 byte 235
8.4.1 Reception Probability of Emergency Messages..... 235
8.4.2 Time Bound for Emergency Messages 236
8.4.3 Reception Probability of Routine Messages 237
8.4.4 Time Bound for Routine Messages..... 238
8.5 Routine Messages at 5 Hz, Routine Message Size – 250 byte 239
8.5.1 Reception Probability of Emergency Messages..... 239
8.5.2 Time Bound for Emergency Messages 240
8.5.3 Reception Probability of Routine Messages 241
8.5.4 Time Bound for Routine Messages..... 242
8.6 Routine Messages at 10 Hz, Routine Message Size – 250 byte 243
8.6.1 Reception Probability of Emergency Messages..... 243
8.6.2 Time Bound for Emergency Messages 244
8.6.3 Reception Probability of Routine Messages 245
8.6.4 Time Bound for Routine Messages..... 246
8.7 Routine Messages at 5 Hz, Routine Message Size – 300 byte 247
8.7.1 Reception Probability of Emergency Messages..... 247
8.7.2 Time Bound for Emergency Messages 248
8.7.3 Reception Probability of Routine Messages 249
8.7.4 Time Bound for Routine Messages..... 250
8.8 Routine Messages at 10 Hz, Routine Message Size – 300 byte 251
8.8.1 Reception Probability of Emergency Messages..... 251
8.8.2 Time Bound for Emergency Messages 252
8.8.3 Reception Probability of Routine Messages 253
8.8.4 Time Bound for Routine Messages..... 254

TABLE OF FIGURES

Figure 1-1: Intersection Simulation Environment 2
Figure 1-2: Pseudo Code of Repetition-Based Cascading Protocol 4
Figure 1-3: SDL Diagram of Repetition-Based Cascading Protocol 5
Figure 1-4: Pseudo Code of Feedback-Based Cascading Protocol 6
Figure 1-5: SDL Diagram of Feedback-Based Cascading Protocol 7
Figure 2-1: DSRC Simulator Architecture 8
Figure 2-2: General Intersection Scenario 9
Figure 2-3: Components of Intersection Scenario 10
Figure 2-4: Node Distribution and Movement on Highway 11
Figure 2-5: Node Distribution on Intersection Legs 11
Figure 2-6: RF Model Regions 14
Figure 2-7: City Intersection RF Model Data Collection Site 16
Figure 2-8: RF Model Selection Decision Table 17
Figure 2-9: Highway RF Model Nakagami Parameters 18
Figure 2-10: Signal Attenuation Over Distance, Highway RF Model 18
Figure 2-11: Simulation Setting, Single Sender on Freeway, Highway RF Model 19
Figure 2-12: Reception Probability on Freeway, Single Sender on Freeway, Highway RF model 19
Figure 2-13: City RF Model Nakagami Parameters 20
Figure 2-14: Signal Attenuation Over Distance, City RF Model 20
Figure 2-15: Simulation Setting, Single Sender in Intersection, City RF Model 21
Figure 2-16: Reception Probability Within Urban Canyon, Single Sender in Intersection, City RF model 21
Figure 2-17: Blocked RF Model Nakagami Parameters 22
Figure 2-18: Signal Attenuation Over Distance, Blocked RF Model 22
Figure 2-19: Simulation Setting, Single Sender around Corner, Blocked RF Model 23
Figure 2-20: Reception Probability around Corner, Single Sender, Blocked RF model 23
Figure 4-1: Reception Probability of Routine Messages, Sender on Road B, scenario 3 28
Figure 4-2: Reception Probability of Routine Messages, Sender on Road B, Scenario 11 28
Figure 4-3: Reception Probability of Routine at Intersection, Scenario 27 29
Figure 4-4: Time Bound for desired Confidence for Routine Messages Reception at Intersection, Scenario 27 29
Figure 4-5: Reception Probability of Routine Messages at Intersection, Scenario 19 30
Figure 4-6: Time Bound for Desired Confidence for Routine Messages Reception at Intersection, Scenario 19 30
Figure 4-7: Reception Probability of Routine Messages at Intersection, Scenario 35 30
Figure 4-8: Time Bound for desired Confidence for Routine Messages Reception at Intersection, Scenario 35 30
Figure 4-9: Reception Probability of Routine Messages at Intersection, Scenario 11 30
Figure 4-10: Time Bound for desired Confidence for Routine Messages Reception at Intersection, Scenario 11 30
Figure 4-11: Reception Probability of Routine Messages at Intersection, Based on Scenario 11, Routine Message Adjusted to 6 Hz 31
Figure 4-12: Time Bound for Desired Confidence for Routine Message Reception at Intersection, Based on Scenario 11, Routine Message Adjusted to 6 Hz 31
Figure 4-13: Reception Probability of Routine Messages at Intersection, Based on Scenario 11, Routine Message Adjusted to 7 Hz 31

Figure 4-14: Time Bound for Desired Confidence for Routine Message Reception at Intersection, Based on Scenario 11, Routine Message Adjusted to 7 Hz 31
Figure 4-16: Time Bound for Desired Confidence for Routine Message Reception at Intersection, Based on Scenario 11, Routine Message Adjusted to 8 Hz 32
Figure 4-18: Time Bound for Desired Confidence for Routine Message Reception at Intersection, Based on Scenario 11, Routine Message Adjusted to 9 Hz 32
Figure 4-19: Reception Probability of Emergency Messages-Scenario 11, Road B, Sender RSU 33
Figure 4-20: Reception Probability of Emergency Messages-Scenario11, Sender RSU 33
Figure 4-21: Reception Probability of Emergency Messages-Scenario 35, Road B, Sender RSU 33
Figure 4-22: Reception Probability of Emergency Messages-Scenario 35, Sender RSU 33
Figure 4-23: Reception Probability of Emergency Messages-Scenario19, Road B, Sender RSU 34
Figure 4-24: Reception Probability of Emergency Messages-Scenario19, Sender RSU 34
Figure 4-25: Reception Probability of Emergency Messages-Scenario 27, Road B, Sender RSU 34
Figure 4-26: Reception Probability of Emergency Messages-Scenario 27, Sender RSU 34
Figure 4-27: Reception Prob. of Emergency Messages - Scenario15, Rd. A, Sender on Rd. A1 35
Figure 4-28: Reception Prob. of Emergency Messages-Scenario 15, Sender on Rd. A1..... 35
Figure 4-29: Reception Prob. of Emergency Messages – Scenario 36, Rd. A, Sender on Rd. A1 36
Figure 4-30: Reception Prob. of Emergency Messages-Scenario 36, Sender on Rd. A1..... 36
Figure 4-31: Reception Prob. of Emergency Messages – Scenario 40, Rd. A, Sender on Rd. A1 36
Figure 4-32: Reception Prob. of Emergency Messages-Scenario 40, Sender on Rd. A1..... 36
Figure 4-33: Reception Prob. of Routine Message Scenario 41, Rd. B, Sender on Rd. A1..... 37
Figure 4-34: Reception Probability of Emergency Messages-Scenario 41, Sender on Rd. A1 ... 37
Figure 4-35: Reception Prob. of Routine Message Scenario 42, Rd. B, Sender on Rd. A1..... 37
Figure 4-36: Reception Probability of Emergency Messages-Scenario 42, Sender on Rd. A1 ... 37
Figure 4-37: Visualization of Emergency Messages Reception WITHOUT RSU Rebroadcast, Routine Message at 2Hz 39
Figure 4-38: Visualization of Emergency Messages Reception WITH RSU Rebroadcast, Routine Message at 2Hz 39
Figure 4-39: Visualization of Emergency Messages Reception WITHOUT RSU Rebroadcast, Routine Message at 5Hz 39
Figure 4-40: Visualization of Emergency Messages Reception WITH RSU Rebroadcast, Routine Message at 5Hz 39
Figure 4-41: Visualization of Emergency Messages Reception WITHOUT RSU Rebroadcast, Routine Message at 10Hz 39
Figure 4-42: Visualization of Emergency Messages Reception WITH RSU Rebroadcast, Routine Message at 10Hz 39
Figure 4-43: Message Cascading over Nodes, Scenario 43, Repetition 41
Figure 4-44: Message Cascading over Nodes, Scenario 44, Feedback 41
Figure 4-45: Message Cascading over Nodes, Scenario 45, Repetition 41
Figure 4-46: Message Cascading over Nodes, Scenario 46, Feedback 41
Figure 5-1: Reception Probability of Emergency Messages-Scenario1, Road A, Sender RSU ... 43
Figure 5-2: Reception Probability of Emergency Messages-Scenario 1, Road B, Sender RSU .. 43
Figure 5-3: Reception Probability of Emergency Messages-Scenario 1, HWY, Sender RSU..... 43
Figure 5-4: Reception Probability of Emergency Messages-Scenario 1, Sender RSU 43

Figure 5-5: Reception Probability of Routine Messages on Road A, Scenario 1 44
Figure 5-6: Reception Probability of Routine Messages on Road A, Scenario 1 44
Figure 5-7: Reception Probability of Routine Messages on Road B, Scenario 1 44
Figure 5-8: Reception Probability of Routine Messages on Road B, Scenario 1 44
Figure 5-9: Reception Probability of Routine Messages on HWY, Scenario 1 44
Figure 5-10: Reception Probability of Routine Messages on HWY, Scenario 1 44
Figure 5-11: Reception Probability of Emergency Messages-Scenario 2, Road A, Sender RSU 45
Figure 5-12: Reception Probability of Emergency Messages-Scenario 2, Road B, Sender RSU 45
Figure 5-13: Reception Probability of Emergency Messages-Scenario 2, HWY, Sender RSU 45
Figure 5-14: Reception Probability of Emergency Messages-Scenario 2, Sender RSU 45
Figure 5-15: Reception Probability of Routine Messages on Road A, Scenario 2 46
Figure 5-16: Reception Probability of Routine Messages on Road A, Scenario 2 46
Figure 5-17: Reception Probability of Routine Messages on Road B, Scenario 2 46
Figure 5-18: Reception Probability of Routine Messages on Road B, Scenario 2 46
Figure 5-19: Reception Probability of Routine Messages on HWY, Scenario 2 46
Figure 5-20: Reception Probability of Routine Messages on HWY, Scenario 2 46
Figure 5-21: Reception Probability of Emergency Messages-Scenario 3, Road A, Sender RSU 47
Figure 5-22: Reception Probability of Emergency Messages-Scenario 3, Road B, Sender RSU 47
Figure 5-23: Reception Probability of Emergency Messages-Scenario 3, HWY, Sender RSU 47
Figure 5-24: Reception Probability of Emergency Messages-Scenario 3, Sender RSU 47
Figure 5-25: Reception Probability of Routine Messages on Road A, Scenario 3 48
Figure 5-26: Reception Probability of Routine Messages on Road A, Scenario 3 48
Figure 5-27: Reception Probability of Routine Messages on Road B, Scenario 3 48
Figure 5-28: Reception Probability of Routine Messages on Road B, Scenario 3 48
Figure 5-29: Reception Probability of Routine Messages on HWY, Scenario 3 48
Figure 5-30: Reception Probability of Routine Messages on HWY, Scenario 3 48
Figure 5-31: Reception Probability of Emergency Messages-Scenario 4, Road A, Sender RSU 49
Figure 5-32: Reception Probability of Emergency Messages-Scenario 4, Road B, Sender RSU 49
Figure 5-33: Reception Probability of Emergency Messages-Scenario 4, HWY, Sender RSU 49
Figure 5-34: Reception Probability of Emergency Messages-Scenario 4, Sender RSU 49
Figure 5-35: Reception Probability of Routine Messages on Road A, Scenario 4 50
Figure 5-36: Reception Probability of Routine Messages on Road A, Scenario 4 50
Figure 5-37: Reception Probability of Routine Messages on Road B, Scenario 4 50
Figure 5-38: Reception Probability of Routine Messages on Road B, Scenario 4 50
Figure 5-39: Reception Probability of Routine Messages on HWY, Scenario 4 50
Figure 5-40: Reception Probability of Routine Messages on HWY, Scenario 4 50
Figure 5-41: Reception Prob. of Emergency Messages - Scenario5, Rd. A, Sender on Rd. A1 .. 51
Figure 5-42: Reception Prob. of Emergency Messages - Scenario5, Rd. B, Sender on Rd. A1 .. 51
Figure 5-43: Reception Prob. of Emergency Messages - Scenario5, HWY, Sender on Rd. A1 .. 51
Figure 5-44: Reception Prob. of Emergency Messages-Scenario 5, Sender on Rd. A1 51
Figure 5-45: Reception Prob. of Emergency Messages – Scenario 5, Rd. A, Sender on Rd. A2 52
Figure 5-46: Reception Prob. of Emergency Messages - Scenario 5, Rd. B, Sender on Rd. A2 . 53

Figure 5-47: Reception Prob. of Emergency Messages – Scenario 5, HWY, Sender on Rd. A2 52
Figure 5-48: Reception Prob. of Emergency Messages-Scenario 5, Sender on Rd. A2..... 52
Figure 5-49: Reception Prob. of Emergency Messages – Scenario 5, Rd. A, Sender on Rd. B... 53
Figure 5-50: Reception Prob. of Emergency Messages – Scenario 5, Rd. B, Sender on Rd. B... 53
Figure 5-51: Reception Prob. of Emergency Messages – Scenario 5, HWY, Sender on Rd. B... 53
Figure 5-52: Reception Prob. of Emergency Messages-Scenario 5, Sender on Rd. B..... 53
Figure 5-53: Reception Prob. of Emergency Messages – Scenario 5, Rd. A, Sender on HWY .. 54
Figure 5-54: Reception Prob. of Emergency Messages – Scenario 5, Rd. B, Sender on HWY... 54
Figure 5-55: Reception Prob. of Emergency Messages – Scenario 5, HWY, Sender on HWY .. 54
Figure 5-56: Reception Prob. of Emergency Messages-Scenario 5, Sender on HWY..... 54
Figure 5-57: Reception Prob. of Emergency Messages – Scenario 6, Rd. A, Sender on Rd. A1 55
Figure 5-58: Reception Prob. of Emergency Messages – Scenario 6, Rd. B, Sender on Rd. A1 55
Figure 5-59: Reception Prob. of Emergency Messages – Scenario 6, HWY, Sender on Rd. A1 55
Figure 5-60: Reception Prob. of Emergency Messages-Scenario 6, Sender on Rd. A1..... 55
Figure 5-61: Reception Prob. of Emergency Messages – Scenario 6, Rd. A, Sender on Rd. A2 56
Figure 5-62: Reception Prob. of Emergency Messages – Scenario 6, Rd. B, Sender on Rd. A2. 56
Figure 5-63: Reception Prob. of Emergency Messages – Scenario 6, HWY, Sender on Rd. A2 56
Figure 5-64: Reception Prob. of Emergency Messages-Scenario 6, Sender on Rd. A2..... 56
Figure 5-65: Reception Prob. of Emergency Messages – Scenario 6, Rd. A, Sender on Rd. B.. 57
Figure 5-66: Reception Prob. of Emergency Messages – Scenario 6, Rd. B, Sender on Rd. B.. 57
Figure 5-67: Reception Prob. of Emergency Messages – Scenario 6, HWY, Sender on Rd. B.. 57
Figure 5-68: Reception Prob. of Emergency Messages-Scenario 6, Sender on Rd. B..... 57
Figure 5-69: Reception Prob. of Emergency Messages – Scenario 6, Rd. A, Sender on HWY.. 58
Figure 5-70: Reception Prob. of Emergency Messages – Scenario 6, Rd. B, Sender on HWY.. 58
Figure 5-71: Reception Prob. of Emergency Messages – Scenario 6, HWY, Sender on HWY.. 58
Figure 5-72: Reception Prob. of Emergency Messages-Scenario 6, Sender on HWY..... 58
Figure 5-73: Reception Prob. of Emergency Messages – Scenario 7, Rd. A, Sender on Rd. A1 59
Figure 5-74: Reception Prob. of Emergency Messages – Scenario 7, Rd. B, Sender on Rd. A1. 59
Figure 5-75: Reception Prob. of Emergency Messages – Scenario 7, HWY, Sender on Rd. A1 59
Figure 5-76: Reception Prob. of Emergency Messages-Scenario 7, Sender on Rd. A1..... 59
Figure 5-77: Reception Prob. of Emergency Messages – Scenario 7, Rd. A, Sender on Rd. A2 60
Figure 5-78: Reception Prob. of Emergency Messages – Scenario 7, Rd. B, Sender on Rd. A2. 60
Figure 5-79: Reception Prob. of Emergency Messages – Scenario 7, HWY, Sender on Rd. A2 . 60
Figure 5-80: Reception Prob. of Emergency Messages-Scenario 7, Sender on Rd. A2..... 60
Figure 5-81: Reception Prob. of Emergency Messages – Scenario 7, Rd. A, Sender on Rd. B... 61
Figure 5-82: Reception Prob. of Emergency Messages – Scenario 7, Rd. B, Sender on Rd. B... 61
Figure 5-83: Reception Prob. of Emergency Messages – Scenario 7, HWY, Sender on Rd. B... 61
Figure 5-84: Reception Prob. of Emergency Messages-Scenario 7, Sender on Rd. B..... 61
Figure 5-85: Reception Prob. of Emergency Messages – Scenario 7, Rd. A, Sender on Rd. B... 62
Figure 5-86: Reception Prob. of Emergency Messages – Scenario 7, Rd. B, Sender on Rd. B... 62
Figure 5-87: Reception Prob. of Emergency Messages – Scenario 7, HWY, Sender on Rd. B... 62
Figure 5-88: Reception Prob. of Emergency Messages-Scenario 7, Sender on Rd. B..... 62
Figure 5-89: Reception Prob. of Emergency Messages – Scenario 7, Rd. A, Sender on HWY .. 63
Figure 5-90: Reception Prob. of Emergency Messages – Scenario 7, Rd. B, Sender on HWY... 63
Figure 5-91: Reception Prob. of Emergency Messages – Scenario 7, HWY, Sender on HWY .. 63
Figure 5-92: Reception Prob. of Emergency Messages-Scenario 7, Sender on HWY..... 63
Figure 5-93: Reception Prob. of Emergency Messages – Scenario 8, Rd. A, Sender on Rd. A1 64
Figure 5-94: Reception Prob. of Emergency Messages – Scenario 8, Rd. B, Sender on Rd. A1. 64
Figure 5-95: Reception Prob. of Emergency Messages – Scenario 8, HWY,
Sender on Rd. A1 64
Figure 5-96: Reception Prob. of Emergency Messages-Scenario 8, Sender on Rd. A1..... 64

Figure 5-97: Reception Prob. of Emergency Messages – Scenario 8, Rd. A, Sender on Rd. A2 65
Figure 5-98: Reception Prob. of Emergency Messages – Scenario 8, Rd. B, Sender on Rd. A2 65
Figure 5-99: Reception Prob. of Emergency Messages – Scenario 8, HWY, Sender on Rd. A2 65
Figure 5-100: Reception Prob. of Emergency Messages-Scenario 8, Sender on Rd. A2 65
Figure 5-101: Reception Prob. of Emergency Messages – Scenario 8, Rd. A, Sender on Rd. B 66
Figure 5-102: Reception Prob. of Emergency Messages – Scenario 8, Rd. B, Sender on Rd. B 66
Figure 5-103: Reception Prob. of Emergency Messages – Scenario 8, HWY, Sender on Rd. B 66
Figure 5-104: Reception Prob. of Emergency Messages-Scenario 8, Sender on Rd. B 66
Figure 5-105: Reception Prob. of Emergency Messages – Scenario 8, Rd. A, Sender on HWY 67
Figure 5-106: Reception Prob. of Emergency Messages – Scenario 8, Rd. B, Sender on HWY 67
Figure 5-107: Reception Prob. of Emergency Messages – Scenario 8, HWY, Sender on HWY 67
Figure 5-108: Reception Prob. of Emergency Messages-Scenario 8, Sender on HWY 67
Figure 5-109: Reception Probability of Emergency Messages-Scenario 9, Road A, Sender RSU 68
Figure 5-111: Reception Probability of Emergency Messages-Scenario 9, HWY, Sender RSU 68
Figure 5-112: Reception Probability of Emergency Messages-Scenario 9, Sender RSU 68
Figure 5-113: Reception Probability of Routine Messages on Road A, Scenario 9 69
Figure 5-114: Reception Probability of Routine Messages on Road A, Scenario 9 69
Figure 5-115: Reception Probability of Routine Messages on Road B, Scenario 9 69
Figure 5-116: Reception Probability of Routine Messages on Road B, Scenario 9 69
Figure 5-117: Reception Probability of Routine Messages on HWY, Scenario 9 69
Figure 5-118: Reception Probability of Routine Messages on HWY, Scenario 9 69
Figure 5-119: Reception Probability of Emergency Messages-Scenario 10, Road A, Sender RSU 70
Figure 5-120: Reception Probability of Emergency Messages-Scenario 10, Road B, Sender RSU 70
Figure 5-121: Reception Probability of Emergency Messages-Scenario 10, HWY, Sender RSU 70
Figure 5-122: Reception Probability of Emergency Messages-Scenario 10, Sender RSU 70
Figure 5-123: Reception Probability of Routine Messages on Road A, Scenario 10 71
Figure 5-124: Reception Probability of Routine Messages on Road A, Scenario 10 71
Figure 5-125: Reception Probability of Routine Messages on Road B, Scenario 10 71
Figure 5-126: Reception Probability of Routine Messages on Road B, Scenario 10 71
Figure 5-127: Reception Probability of Routine Messages on HWY, Scenario 10 71
Figure 5-128: Reception Probability of Routine Messages on HWY, Scenario 10 71
Figure 5-129: Reception Probability of Emergency Messages-Scenario 11, Road A, Sender RSU 72
Figure 5-130: Reception Probability of Emergency Messages-Scenario 11, Road B, Sender RSU 72
Figure 5-131: Reception Probability of Emergency Messages-Scenario 11, HWY, Sender RSU 72

Figure 5-132: Reception Probability of Emergency Messages-Scenario11, Sender RSU 72
Figure 5-133: Reception Probability of Routine Messages on Road A, Scenario 11..... 73
Figure 5-134: Reception Probability of Routine Messages on Road A, Scenario 11..... 73
Figure 5-135: Reception Probability of Routine Messages on Road B, Scenario 11..... 73
Figure 5-136: Reception Probability of Routine Messages on Road B, Scenario 11..... 73
Figure 5-137: Reception Probability of Routine Messages on HWY, Scenario 11 73
Figure 5-138: Reception Probability of Routine Messages on HWY, Scenario 11 73
Figure 5-139: Reception Probability of Emergency Messages-Scenario12, Road A, Sender RSU 74
Figure 5-140: Reception Probability of Emergency Messages-Scenario12, Road B, Sender RSU 74
Figure 5-141: Reception Probability of Emergency Messages-Scenario12, HWY, Sender RSU 74
Figure 5-142: Reception Probability of Emergency Messages-Scenario12, Sender RSU 74
Figure 5-143: Reception Probability of Routine Messages on Road A, Scenario 12..... 75
Figure 5-144: Reception Probability of Routine Messages on Road A, Scenario 12..... 75
Figure 5-145: Reception Probability of Routine Messages on Road B, Scenario 12..... 75
Figure 5-146: Reception Probability of Routine Messages on Road B, Scenario 12..... 75
Figure 5-147: Reception Probability of Routine Messages on HWY, Scenario 12 75
Figure 5-148: Reception Probability of Routine Messages on HWY, Scenario 12 75
Figure 5-149: Reception Prob. of Emergency Messages – Scenario 13, Rd. A, Sender on Rd. A1 76
Figure 5-150: Reception Prob. of Emergency Messages – Scenario 13, Rd. B, Sender on Rd. A1 76
Figure 5-151: Reception Prob. of Emergency Messages – Scenario 13, HWY, Sender on Rd. A1 76
Figure 5-152: Reception Prob. of Emergency Messages-Scenario 13, Sender on Rd. A1..... 76
Figure 5-153: Reception Prob. of Emergency Messages – Scenario 13, Rd. A, Sender on Rd. A2 77
Figure 5-154: Reception Prob. of Emergency Messages – Scenario 13, Rd. B, Sender on Rd. A2 77
Figure 5-155: Reception Prob. of Emergency Messages – Scenario 13, HWY, Sender on Rd. A2 77
Figure 5-156: Reception Prob. of Emergency Messages-Scenario 13, Sender on Rd. A2..... 77
Figure 5-157: Reception Prob. of Emergency Messages – Scenario 13, Rd. A, Sender on Rd. B 78
Figure 5-158: Reception Prob. of Emergency Messages – Scenario 13, Rd. B, Sender on Rd. B 78
Figure 5-159: Reception Prob. of Emergency Messages – Scenario 13, HWY, Sender on Rd. B 78
Figure 5-160: Reception Prob. of Emergency Messages-Scenario 13, Sender on Rd. B..... 78
Figure 5-161: Reception Prob. of Emergency Messages - Scenario 13, Rd. A, Sender on HWY 79
Figure 5-162: Reception Prob. of Emergency Messages - Scenario13, Rd. B, Sender on HWY 79
Figure 5-163: Reception Prob. of Emergency Messages - Scenario13, HWY, Sender on HWY 79
Figure 5-164: Reception Prob. of Emergency Messages-Scenario 13, Sender on HWY..... 79
Figure 5-165: Reception Prob. of Emergency Messages - Scenario14, Rd. A, Sender on Rd. A1 80

Figure 5-166: Reception Prob. of Emergency Messages - Scenario14, Rd. B, Sender on Rd. A1 80
Figure 5-167: Reception Prob. of Emergency Messages - Scenario14, HWY, Sender on Rd. A1 80
Figure 5-168: Reception Prob. of Emergency Messages-Scenario 14, Sender on Rd. A1 80
Figure 5-169: Reception Prob. of Emergency Messages - Scenario14, Rd. A, Sender on Rd. A2 81
Figure 5-170: Reception Prob. of Emergency Messages - Scenario14, Rd. B, Sender on Rd. A2 81
Figure 5-171: Reception Prob. of Emergency Messages - Scenario14, HWY, Sender on Rd. A2 81
Figure 5-172: Reception Prob. of Emergency Messages-Scenario 14, Sender on Rd. A2 81
Figure 5-173: Reception Prob. of Emergency Messages - Scenario14, Rd. A, Sender on Rd. B 82
Figure 5-174: Reception Prob. of Emergency Messages - Scenario14, Rd. B, Sender on Rd. B 82
Figure 5-175: Reception Prob. of Emergency Messages - Scenario14, HWY, Sender on Rd. B 82
Figure 5-176: Reception Prob. of Emergency Messages-Scenario 14, Sender on Rd. B 82
Figure 5-177: Reception Prob. of Emergency Messages - Scenario14, Rd. A, Sender on HWY 83
Figure 5-178: Reception Prob. of Emergency Messages - Scenario14, Rd. B, Sender on HWY 83
Figure 5-179: Reception Prob. of Emergency Messages - Scenario14, HWY, Sender on HWY 83
Figure 5-180: Reception Prob. of Emergency Messages-Scenario 14, Sender on HWY 83
Figure 5-181: Reception Prob. of Emergency Messages - Scenario15, Rd. A, Sender on Rd. A1 85
Figure 5-182: Reception Prob. of Emergency Messages - Scenario15, Rd. B, Sender on Rd. A1 85
Figure 5-183: Reception Prob. of Emergency Messages - Scenario15, HWY, Sender on Rd. A1 85
Figure 5-184: Reception Prob. of Emergency Messages-Scenario 15, Sender on Rd. A1 85
Figure 5-185: Reception Prob. of Emergency Messages - Scenario15, Rd. A, Sender on Rd. A2 86
Figure 5-186: Reception Prob. of Emergency Messages - Scenario15, Rd. B, Sender on Rd. A2 86
Figure 5-187: Reception Prob. of Emergency Messages - Scenario15, HWY, Sender on Rd. A2 86
Figure 5-188: Reception Prob. of Emergency Messages-Scenario 15, Sender on Rd. A2 86
Figure 5-189: Reception Prob. of Emergency Messages - Scenario15, Rd. A, Sender on Rd. B 87
Figure 5-190: Reception Prob. of Emergency Messages - Scenario15, Rd. B, Sender on Rd. B 87
Figure 5-191: Reception Prob. of Emergency Messages - Scenario15, HWY, Sender on Rd. B 87
Figure 5-192: Reception Prob. of Emergency Messages-Scenario 15, Sender on Rd. B 87
Figure 5-193: Reception Prob. of Emergency Messages - Scenario15, Rd. A, Sender on HWY 88
Figure 5-194: Reception Prob. of Emergency Messages - Scenario15, Rd. B, Sender on HWY 88

Figure 5-195: Reception Prob. of Emergency Messages - Scenario15, HWY, Sender on HWY 88
Figure 5-196: Reception Prob. of Emergency Messages-Scenario 15, Sender on HWY 88
Figure 5-197: Reception Prob. of Emergency Messages - Scenario16, Rd. A, Sender on Rd. A1 89
Figure 5-198: Reception Prob. of Emergency Messages - Scenario16, Rd. B, Sender on Rd. A1 89
Figure 5-199: Reception Prob. of Emergency Messages - Scenario16, HWY, Sender on Rd. A1 89
Figure 5-200: Reception Prob. of Emergency Messages-Scenario 16, Sender on Rd. A1 89
Figure 5-201: Reception Prob. of Emergency Messages - Scenario16, Rd. A, Sender on Rd. A2 90
Figure 5-202: Reception Prob. of Emergency Messages - Scenario16, Rd. B, Sender on Rd. A2 90
Figure 5-203: Reception Prob. of Emergency Messages - Scenario16, HWY, Sender on Rd. A2 90
Figure 5-204: Reception Prob. of Emergency Messages-Scenario 16, Sender on Rd. A2 90
Figure 5-205: Reception Prob. of Emergency Messages - Scenario16, Rd. A, Sender on Rd. B 91
Figure 5-206: Reception Prob. of Emergency Messages - Scenario16, Rd. B, Sender on Rd. B 91
Figure 5-207: Reception Prob. of Emergency Messages - Scenario16, HWY, Sender on Rd. B 91
Figure 5-208: Reception Prob. of Emergency Messages-Scenario 16, Sender on Rd. B 91
Figure 5-209: Reception Prob. of Emergency Messages - Scenario16, Rd. A, Sender on HWY 92
Figure 5-210: Reception Prob. of Emergency Messages - Scenario16, Rd. B, Sender on HWY 92
Figure 5-211: Reception Prob. of Emergency Messages - Scenario16, HWY, Sender on HWY 92
Figure 5-212: Reception Prob. of Emergency Messages-Scenario 16, Sender on HWY 92
Figure 5-213: Reception Probability of Emergency Messages-Scenario17, Road A, Sender RSU 93
Figure 5-214: Reception Probability of Emergency Messages-Scenario17, Road B, Sender RSU 93
Figure 5-215: Reception Probability of Emergency Messages-Scenario17, HWY, Sender RSU 93
Figure 5-216: Reception Probability of Emergency Messages-Scenario17, Sender RSU 93
Figure 5-217: Reception Probability of Routine Messages on Road A, Scenario17 94
Figure 5-218: Reception Probability of Routine Messages on Road A, Scenario 17 94
Figure 5-219: Reception Probability of Routine Messages on Road B, Scenario17 94
Figure 5-220: Reception Probability of Routine Messages on Road B, Scenario 17 94
Figure 5-221: Reception Probability of Routine Messages on HWY, Scenario17 94
Figure 5-222: Reception Probability of Routine Messages on HWY, Scenario 17 94
Figure 5-223: Reception Prob. of Emergency Messages - Scenario18, Rd. A, Sender on Rd. A1 95
Figure 5-224: Reception Prob. of Emergency Messages - Scenario18, Rd. B, Sender on Rd. A1 95
Figure 5-225: Reception Prob. of Emergency Messages - Scenario18, HWY, Sender on Rd. A1 95
Figure 5-226: Reception Prob. of Emergency Messages-Scenario 18, Sender on Rd. A1 95

Figure 5-227: Reception Prob. of Emergency Messages – Scenario 18, Rd. A, Sender on Rd. A2 96
Figure 5-228: Reception Prob. of Emergency Messages - Scenario18, Rd. B, Sender on Rd. A2 96
Figure 5-229: Reception Prob. of Emergency Messages – Scenario 18, HWY, Sender on Rd. A2 96
Figure 5-230: Reception Prob. of Emergency Messages-Scenario 18, Sender on Rd. A2 96
Figure 5-231: Reception Prob. of Emergency Messages - Scenario18, Rd. A, Sender on Rd. B 97
Figure 5-232: Reception Prob. of Emergency Messages - Scenario18, Rd. B, Sender on Rd. B 97
Figure 5-233: Reception Prob. of Emergency Messages - Scenario18, HWY, Sender on Rd. B 97
Figure 5-234: Reception Prob. of Emergency Messages-Scenario 18, Sender on Rd. B 97
Figure 5-235: Reception Prob. of Emergency Messages - Scenario18, Rd. A, Sender on HWY 98
Figure 5-236: Reception Prob. of Emergency Messages - Scenario18, Rd. B, Sender on HWY 98
Figure 5-237: Reception Prob. of Emergency Messages - Scenario18, HWY, Sender on HWY 98
Figure 5-238: Reception Prob. of Emergency Messages-Scenario 18, Sender on HWY 98
Figure 5-239: Reception Probability of Emergency Messages-Scenario19, Road A, Sender RSU 99
Figure 5-240: Reception Probability of Emergency Messages-Scenario19, Road B, Sender RSU 99
Figure 5-241: Reception Probability of Emergency Messages-Scenario19, HWY, Sender RSU 99
Figure 5-242: Reception Probability of Emergency Messages-Scenario 19, Sender RSU 99
Figure 5-243: Reception Probability of Routine Messages on Road A, Scenario 19 100
Figure 5-244: Reception Probability of Routine Messages on Road A, Scenario 19 100
Figure 5-245: Reception Probability of Routine Messages on Road B, Scenario 19 100
Figure 5-246: Reception Probability of Routine Messages on Road B, Scenario 19 100
Figure 5-247: Reception Probability of Routine Messages on HWY, Scenario 19 100
Figure 5-248: Reception Probability of Routine Messages on HWY, Scenario 19 100
Figure 5-249: Reception Prob. of Emergency Messages – Scenario 20, Rd. A, Sender on Rd. A1 101
Figure 5-250: Reception Prob. of Emergency Messages – Scenario 20, Rd. B, Sender on Rd. A1 101
Figure 5-251: Reception Prob. of Emergency Messages – Scenario 20, HWY, Sender on Rd. A1 101
Figure 5-252: Reception Prob. of Emergency Messages-Scenario 20, Sender on Rd. A1 101
Figure 5-253: Reception Prob. of Emergency Messages – Scenario 20, Rd. A, Sender on Rd. A2 102
Figure 5-254: Reception Prob. of Emergency Messages – Scenario 20, Rd. B, Sender on Rd. A2 102
Figure 5-255: Reception Prob. of Emergency Messages – Scenario 20, HWY, Sender on Rd. A2 102
Figure 5-256: Reception Prob. of Emergency Messages-Scenario 20, Sender on Rd. A2 102
Figure 5-257: Reception Prob. of Emergency Messages – Scenario 20, Rd. A, Sender on Rd. B 103

Figure 5-258: Reception Prob. of Emergency Messages – Scenario 20, Rd. B, Sender on Rd. B 103
Figure 5-259: Reception Prob. of Emergency Messages – Scenario 20, HWY, Sender on Rd. B 103
Figure 5-260: Reception Prob. of Emergency Messages - Scenario 20, Sender on Rd. B 103
Figure 5-261: Reception Prob. of Emergency Messages – Scenario 20, Rd. A, Sender on HWY 104
Figure 5-262: Reception Prob. of Emergency Messages – Scenario 20, Rd. B, Sender on HWY 104
Figure 5-263: Reception Prob. of Emergency Messages – Scenario 20, HWY, Sender on HWY 104
Figure 5-264: Reception Prob. of Emergency Messages-Scenario 20, Sender on HWY 104
Figure 5-265: Reception Probability of Emergency Messages-Scenario 21, Road A, Sender RSU 105
Figure 5-266: Reception Probability of Emergency Messages-Scenario 21, Road B, Sender RSU 105
Figure 5-267: Reception Probability of Emergency Messages-Scenario 21, HWY, Sender RSU 105
Figure 5-268: Reception Probability of Emergency Messages-Scenario 21, Sender RSU 105
Figure 5-269: Reception Prob. of Emergency Messages – Scenario 22, Rd. A, Sender on Rd. A1 106
Figure 5-270: Reception Prob. of Emergency Messages – Scenario 22, Rd. B, Sender on Rd. A1 106
Figure 5-271: Reception Prob. of Emergency Messages – Scenario 22, HWY, Sender on Rd. A1 106
Figure 5-272: Reception Prob. of Emergency Messages-Scenario 22, Sender on Rd. A1 106
Figure 5-273: Reception Prob. of Emergency Messages – Scenario 22, Rd. A, Sender on Rd. A2 107
Figure 5-274: Reception Prob. of Emergency Messages – Scenario 22, Rd. B, Sender on Rd. A2 107
Figure 5-275: Reception Prob. of Emergency Messages – Scenario 22, HWY, Sender on Rd. A2 107
Figure 5-276: Reception Prob. of Emergency Messages-Scenario 22, Sender on Rd. A2 107
Figure 5-277: Reception Prob. of Emergency Messages – Scenario 22, Rd. A, Sender on Rd. B 108
Figure 5-278: Reception Prob. of Emergency Messages – Scenario 22, Rd. B, Sender on Rd. B 108
Figure 5-279: Reception Prob. of Emergency Messages – Scenario 22, HWY, Sender on Rd. B 108
Figure 5-280: Reception Prob. of Emergency Messages-Scenario 22, Sender on Rd. B 108
Figure 5-281: Reception Prob. of Emergency Messages – Scenario 22, Rd. A, Sender on HWY 109
Figure 5-282: Reception Prob. of Emergency Messages – Scenario 22, Rd. B, Sender on HWY 109
Figure 5-283: Reception Prob. of Emergency Messages – Scenario 22, HWY, Sender on HWY 109
Figure 5-284: Reception Prob. of Emergency Messages - Scenario 22, Sender on HWY 109
Figure 5-285: Reception Probability of Emergency Messages-Scenario 23, Road A, Sender RSU 110
Figure 5-286: Reception Probability of Emergency Messages-Scenario 23, Road B, Sender RSU 110

Figure 5-287: Reception Probability of Emergency Messages-Scenario 23, HWY, Sender RSU 110
Figure 5-288: Reception Probability of Emergency Messages-Scenario 23, Sender RSU 110
Figure 5-289: Reception Prob. of Emergency Messages – Scenario 24, Rd. A, Sender on Rd. A1 111
Figure 5-290: Reception Prob. of Emergency Messages – Scenario 24, Rd. B, Sender on Rd. A1 111
Figure 5-291: Reception Prob. of Emergency Messages – Scenario 24, HWY, Sender on Rd. A1 111
Figure 5-292: Reception Prob. of Emergency Messages-Scenario 24, Sender on Rd. A1..... 111
Figure 5-293: Reception Prob. of Emergency Messages – Scenario 24, Rd. A, Sender on Rd. A2 112
Figure 5-294: Reception Prob. of Emergency Messages – Scenario 24, Rd. B, Sender on Rd. A2 112
Figure 5-295: Reception Prob. of Emergency Messages – Scenario 24, HWY, Sender on Rd. A2 112
Figure 5-296: Reception Prob. of Emergency Messages-Scenario 24, Sender on Rd. A2..... 112
Figure 5-297: Reception Prob. of Emergency Messages – Scenario 24, Rd. A, Sender on Rd. B 113
Figure 5-298: Reception Prob. of Emergency Messages – Scenario 24, Rd. B, Sender on Rd. B 113
Figure 5-299: Reception Prob. of Emergency Messages – Scenario 24, HWY, Sender on Rd. B 113
Figure 5-300: Reception Prob. of Emergency Messages-Scenario 24, Sender on Rd. B..... 113
Figure 5-301: Reception Prob. of Emergency Messages – Scenario 24, Rd. A, Sender on HWY 114
Figure 5-302: Reception Prob. of Emergency Messages – Scenario 24, Rd. B, Sender on HWY 114
Figure 5-303: Reception Prob. of Emergency Messages – Scenario 24, HWY, Sender on HWY 114
Figure 5-304: Reception Prob. of Emergency Messages-Scenario 24, Sender on HWY..... 114
Figure 5-305: Reception Probability of Emergency Messages-Scenario 25, Road A, Sender RSU 115
Figure 5-306: Reception Probability of Emergency Messages-Scenario 25, Road B, Sender RSU 115
Figure 5-307: Reception Probability of Emergency Messages-Scenario 25, HWY, Sender RSU 115
Figure 5-308: Reception Probability of Emergency Messages-Scenario 25, Sender RSU 115
Figure 5-309: Reception Probability of Routine Messages on Road A Scenario 25..... 116
Figure 5-310: Reception Probability of Routine Messages on Road A Scenario 25..... 116
Figure 5-311: Reception Probability of Routine Messages on Road B Scenario 25..... 116
Figure 5-312: Reception Probability of Routine Messages on Road B Scenario 25..... 116
Figure 5-313: Reception Probability of Routine Messages on HWY Scenario 25 116
Figure 5-314: Reception Probability of Routine Messages on HWY Scenario 25 116
Figure 5-315: Reception Prob. of Emergency Messages – Scenario 26, Rd. A, Sender on Rd. A1 117
Figure 5-316: Reception Prob. of Emergency Messages – Scenario 26, Rd. B, Sender on Rd. A1 117
Figure 5-317: Reception Prob. of Emergency Messages – Scenario 26, HWY, Sender on Rd. A1 117
Figure 5-318: Reception Prob. of Emergency Messages-Scenario 26, Sender on Rd. A1..... 117

Figure 5-319: Reception Prob. of Emergency Messages – Scenario 26, Rd. A, Sender on Rd. A2 118
Figure 5-320: Reception Prob. of Emergency Messages – Scenario 26, Rd. B, Sender on Rd. A2 118
Figure 5-321: Reception Prob. of Emergency Messages – Scenario 26, HWY, Sender on Rd. A2 118
Figure 5-322: Reception Prob. of Emergency Messages-Scenario 26, Sender on Rd. A2 118
Figure 5-323: Reception Prob. of Emergency Messages – Scenario 26, Rd. A, Sender on Rd. B 119
Figure 5-324: Reception Prob. of Emergency Messages – Scenario 26, Rd. B, Sender on Rd. B 119
Figure 5-325: Reception Prob. of Emergency Messages – Scenario 26, HWY, Sender on Rd. B 119
Figure 5-326: Reception Prob. of Emergency Messages-Scenario 26, Sender on Rd. B 119
Figure 5-327: Reception Prob. of Emergency Messages – Scenario 26, Rd. A, Sender on HWY 120
Figure 5-328: Reception Prob. of Emergency Messages – Scenario 26, Rd. B, Sender on HWY 120
Figure 5-329: Reception Prob. of Emergency Messages – Scenario 26, HWY, Sender on HWY 120
Figure 5-330: Reception Prob. of Emergency Messages-Scenario 26, Sender on HWY 120
Figure 5-331: Reception Probability of Emergency Messages-Scenario 27, Road A, Sender RSU 121
Figure 5-332: Reception Probability of Emergency Messages-Scenario 27, Road B, Sender RSU 121
Figure 5-333: Reception Probability of Emergency Messages-Scenario 27, HWY, Sender RSU 121
Figure 5-334: Reception Probability of Emergency Messages-Scenario 27, Sender RSU 121
Figure 5-335: Reception Probability of Routine Messages on Road A, Scenario 27 122
Figure 5-336: Reception Probability of Routine Messages on Road A, Scenario 27 122
Figure 5-337: Reception Probability of Routine Messages on Road B, Scenario 27 122
Figure 5-338: Reception Probability of Routine Messages on Road B, Scenario 27 122
Figure 5-339: Reception Probability of Routine Messages on HWY, Scenario 27 122
Figure 5-340: Reception Probability of Routine Messages on HWY, Scenario 27 122
Figure 5-341: Reception Prob. of Emergency Messages – Scenario 28, Rd. A, Sender on Rd. A1 123
Figure 5-342: Reception Prob. of Emergency Messages – Scenario 28, Rd. B, Sender on Rd. A1 123
Figure 5-343: Reception Prob. of Emergency Messages – Scenario 28, HWY, Sender on Rd. A1 123
Figure 5-344: Reception Prob. of Emergency Messages-Scenario 28, Sender on Rd. A1 123
Figure 5-345: Reception Prob. of Emergency Messages – Scenario 28, Rd. A, Sender on Rd. A2 124
Figure 5-346: Reception Prob. of Emergency Messages – Scenario 28, Rd. B, Sender on Rd. A2 124
Figure 5-347: Reception Prob. of Emergency Messages – Scenario 28, HWY, Sender on Rd. A2 124
Figure 5-348: Reception Prob. of Emergency Messages – Scenario 28, Sender on Rd. A2 124
Figure 5-349: Reception Prob. of Emergency Messages – Scenario 28, Rd. A, Sender on Rd. B 125

Figure 5-350: Reception Prob. of Emergency Messages – Scenario 28, Rd. B, Sender on Rd. B 125
Figure 5-351: Reception Prob. of Emergency Messages – Scenario 28, HWY, Sender on Rd. B 125
Figure 5-352: Reception Prob. of Emergency Messages-Scenario 28, Sender on Rd. B 125
Figure 5-353: Reception Prob. of Emergency Messages – Scenario 28, Rd. A, Sender on HWY 126
Figure 5-354: Reception Prob. of Emergency Messages – Scenario 28, Rd. B, Sender on HWY 126
Figure 5-355: Reception Prob. of Emergency Messages – Scenario 28, HWY, Sender on HWY 126
Figure 5-356: Reception Prob. of Emergency Messages-Scenario 28, Sender on HWY 126
Figure 5-357: Reception Probability of Emergency Messages-Scenario 29, Road A, Sender RSU 127
Figure 5-358: Reception Probability of Emergency Messages-Scenario 29, Road B, Sender RSU 127
Figure 5-359: Reception Probability of Emergency Messages-Scenario 29, HWY, Sender RSU 127
Figure 5-360: Reception Probability of Emergency Messages-Scenario 29, Sender RSU 127
Figure 5-361: Reception Prob. of Emergency Messages – Scenario 30, Rd. A, Sender on Rd. A1 128
Figure 5-362: Reception Prob. of Emergency Messages – Scenario 30, Rd. B, Sender on Rd. A1 128
Figure 5-363: Reception Prob. of Emergency Messages – Scenario 30, HWY, Sender on Rd. A1 128
Figure 5-364: Reception Prob. of Emergency Messages-Scenario 30, Sender on Rd. A1 128
Figure 5-365: Reception Prob. of Emergency Messages – Scenario 30, Rd. A, Sender on Rd. A2 129
Figure 5-366: Reception Prob. of Emergency Messages – Scenario 30, Rd. B, Sender on Rd. A2 129
Figure 5-367: Reception Prob. of Emergency Messages – Scenario 30, HWY, Sender on Rd. A2 129
Figure 5-368: Reception Prob. of Emergency Messages-Scenario 30, Sender on Rd. A2 129
Figure 5-369: Reception Prob. of Emergency Messages – Scenario 30, Rd. A, Sender on Rd. B 130
Figure 5-370: Reception Prob. of Emergency Messages – Scenario 30, Rd. B, Sender on Rd. B 130
Figure 5-371: Reception Prob. of Emergency Messages – Scenario 30, HWY, Sender on Rd. B 130
Figure 5-372: Reception Prob. of Emergency Messages-Scenario 30, Sender on Rd. B 130
Figure 5-373: Reception Prob. of Emergency Messages – Scenario 30, Rd. A, Sender on HWY 131
Figure 5-374: Reception Prob. of Emergency Messages – Scenario 30, Rd. B, Sender on HWY 131
Figure 5-375: Reception Prob. of Emergency Messages – Scenario 30, HWY, Sender on HWY 131
Figure 5-376: Reception Prob. of Emergency Messages-Scenario 30, Sender on HWY 131
Figure 5-377: Reception Probability of Emergency Messages-Scenario 31, Road A, Sender RSU 132
Figure 5-378: Reception Probability of Emergency Messages-Scenario 31, Road B, Sender RSU 132

Figure 5-379: Reception Probability of Emergency Messages-Scenario 31, HWY, Sender RSU 132
Figure 5-380: Reception Probability of Emergency Messages-Scenario 31, Sender RSU 132
Figure 5-381: Reception Prob. of Emergency Messages – Scenario 32, Rd. A, Sender on Rd. A1 133
Figure 5-382: Reception Prob. of Emergency Messages – Scenario 32, Rd. B, Sender on Rd. A1 133
Figure 5-383: Reception Prob. of Emergency Messages – Scenario 32, HWY, Sender on Rd. A1 133
Figure 5-384: Reception Prob. of Emergency Messages-Scenario 32, Sender on Rd. A1..... 133
Figure 5-385: Reception Prob. of Emergency Messages – Scenario 32, Rd. A, Sender on Rd. A2 134
Figure 5-386: Reception Prob. of Emergency Messages – Scenario 32, Rd. B, Sender on Rd. A2 134
Figure 5-387: Reception Prob. of Emergency Messages – Scenario 32, HWY, Sender on Rd. A2 134
Figure 5-388: Reception Prob. of Emergency Messages-Scenario 32, Sender on Rd. A2..... 134
Figure 5-389: Reception Prob. of Emergency Messages – Scenario 32, Rd. A, Sender on Rd. B 135
Figure 5-390: Reception Prob. of Emergency Messages – Scenario 32, Rd. B, Sender on Rd. B 135
Figure 5-391: Reception Prob. of Emergency Messages – Scenario 32, HWY, Sender on Rd. B 135
Figure 5-392: Reception Prob. of Emergency Messages-Scenario 32, Sender on Rd. B..... 135
Figure 5-393: Reception Prob. of Emergency Messages – Scenario 32, Rd. A, Sender on HWY 136
Figure 5-394: Reception Prob. of Emergency Messages – Scenario 32, Rd. B, Sender on HWY 136
Figure 5-395: Reception Prob. of Emergency Messages – Scenario 32, HWY, Sender on HWY 136
Figure 5-396: Reception Prob. of Emergency Messages-Scenario 32, Sender on HWY..... 136
Figure 5-397: Reception Probability of Emergency Messages-Scenario 33, Road A, Sender RSU 137
Figure 5-398: Reception Probability of Emergency Messages-Scenario 33, Road B, Sender RSU 137
Figure 5-399: Reception Probability of Emergency Messages-Scenario 33, HWY, Sender RSU 137
Figure 5-400: Reception Probability of Emergency Messages-Scenario 33, Sender RSU 137
Figure 5-401: Reception Probability of Routine Messages on Road A, Scenario 33..... 138
Figure 5-402: Reception Probability of Routine Messages on Road A, Scenario 33..... 138
Figure 5-403: Reception Probability of Routine Messages on Road B, Scenario 33..... 138
Figure 5-404: Reception Probability of Routine Messages on Road B, Scenario 33..... 138
Figure 5-405: Reception Probability of Routine Messages on HWY, Scenario 33 138
Figure 5-406: Reception Probability of Routine Messages on HWY, Scenario 33 138
Figure 5-407: Reception Prob. of Emergency Messages – Scenario 34, Rd. A, Sender on Rd. A1 139
Figure 5-408: Reception Prob. of Emergency Messages – Scenario 34, Rd. B, Sender on Rd. A1 139
Figure 5-409: Reception Prob. of Emergency Messages – Scenario 34, HWY, Sender on Rd. A1 139
Figure 5-410: Reception Prob. of Emergency Messages-Scenario 34, Sender on Rd. A1..... 139

Figure 5-411: Reception Prob. of Emergency Messages – Scenario 34, Rd. A, Sender on Rd. A2 140
Figure 5-412: Reception Prob. of Emergency Messages – Scenario 34, Rd. B, Sender on Rd. A2 140
Figure 5-413: Reception Prob. of Emergency Messages – Scenario 34, HWY, Sender on Rd. A2 140
Figure 5-414: Reception Prob. of Emergency Messages-Scenario 34, Sender on Rd. A2 140
Figure 5-415: Reception Prob. of Emergency Messages – Scenario 34, Rd. A, Sender on Rd. B 141
Figure 5-416: Reception Prob. of Emergency Messages – Scenario 34, Rd. B, Sender on Rd. B 141
Figure 5-417: Reception Prob. of Emergency Messages – Scenario 34, HWY, Sender on Rd. B 141
Figure 5-418: Reception Prob. of Emergency Messages-Scenario 34, Sender on Rd. B 141
Figure 5-419: Reception Prob. of Emergency Messages – Scenario 34, Rd. A, Sender on HWY 142
Figure 5-420: Reception Prob. of Emergency Messages – Scenario 34, Rd. B, Sender on HWY 142
Figure 5-421: Reception Prob. of Emergency Messages – Scenario 34, HWY, Sender on HWY 142
Figure 5-422: Reception Prob. of Emergency Messages-Scenario 34, Sender on HWY 142
Figure 5-423: Reception Probability of Emergency Messages-Scenario 35, Road A, Sender RSU 143
Figure 5-424: Reception Probability of Emergency Messages-Scenario 35, Road B, Sender RSU 143
Figure 5-425: Reception Probability of Emergency Messages-Scenario 35, HWY, Sender RSU 143
Figure 5-426: Reception Probability of Emergency Messages-Scenario 35, Sender RSU 143
Figure 5-427: Reception Probability of Routine Messages on Road A Scenario 35 144
Figure 5-428: Reception Probability of Routine Messages on Road A Scenario 35 144
Figure 5-429: Reception Probability of Routine Messages on Road B Scenario 35 144
Figure 5-430: Reception Probability of Routine Messages on Road B Scenario 35 144
Figure 5-431: Reception Probability of Routine Messages on HWY Scenario 35 144
Figure 5-432: Reception Probability of Routine Messages on HWY Scenario 35 144
Figure 5-433: Reception Prob. of Emergency Messages – Scenario 36, Rd. A, Sender on Rd. A1 145
Figure 5-434: Reception Prob. of Emergency Messages – Scenario 36, Rd. B, Sender on Rd. A1 145
Figure 5-435: Reception Prob. of Emergency Messages – Scenario 36, HWY, Sender on Rd. A1 145
Figure 5-436: Reception Prob. of Emergency Messages-Scenario 36, Sender on Rd. A1 145
Figure 5-437: Reception Prob. of Emergency Messages – Scenario 36, Rd. A, Sender on Rd. A2 146
Figure 5-438: Reception Prob. of Emergency Messages – Scenario 36, Rd. B, Sender on Rd. A2 146
Figure 5-439: Reception Prob. of Emergency Messages – Scenario 36, HWY, Sender on Rd. A2 146
Figure 5-440: Reception Prob. of Emergency Messages-Scenario 36, Sender on Rd. A2 146
Figure 5-441: Reception Prob. of Emergency Messages – Scenario 36, Rd. A, Sender on Rd. B 147

Figure 5-442: Reception Prob. of Emergency Messages – Scenario 36, Rd. B, Sender on Rd. B 147
Figure 5-443: Reception Prob. of Emergency Messages – Scenario 36, HWY, Sender on Rd. B 147
Figure 5-444: Reception Prob. of Emergency Messages-Scenario 36, Sender on Rd. B 147
Figure 5-445: Reception Prob. of Emergency Messages – Scenario 36, Rd. A, Sender on HWY 148
Figure 5-446: Reception Prob. of Emergency Messages – Scenario 36, Rd. B, Sender on HWY 148
Figure 5-447: Reception Prob. of Emergency Messages – Scenario 36, HWY, Sender on HWY 148
Figure 5-448: Reception Prob. of Emergency Messages-Scenario 36, Sender on HWY 148
Figure 5-449: Reception Probability of Emergency Messages-Scenario 37, Road A, Sender RSU 149
Figure 5-450: Reception Probability of Emergency Messages-Scenario 37, Road B, Sender RSU 149
Figure 5-451: Reception Probability of Emergency Messages-Scenario 37, HWY, Sender RSU 149
Figure 5-452: Reception Probability of Emergency Messages-Scenario 37, Sender RSU 149
Figure 5-453: Reception Prob. of Emergency Messages – Scenario 38, Rd. A, Sender on Rd. A1 150
Figure 5-454: Reception Prob. of Emergency Messages – Scenario 38, Rd. B, Sender on Rd. A1 150
Figure 5-455: Reception Prob. of Emergency Messages – Scenario 38, HWY, Sender on Rd. A1 150
Figure 5-456: Reception Prob. of Emergency Messages-Scenario 38, Sender on Rd. A1 150
Figure 5-457: Reception Prob. of Emergency Messages – Scenario 38, Rd. A, Sender on Rd. A2 151
Figure 5-458: Reception Prob. of Emergency Messages – Scenario 38, Rd. B, Sender on Rd. A2 151
Figure 5-459: Reception Prob. of Emergency Messages – Scenario 38, HWY, Sender on Rd. A2 151
Figure 5-460: Reception Prob. of Emergency Messages-Scenario 38, Sender on Rd. A2 151
Figure 5-461: Reception Prob. of Emergency Messages – Scenario 38, Rd. A, Sender on Rd. B 152
Figure 5-462: Reception Prob. of Emergency Messages – Scenario 38, Rd. B, Sender on Rd. B 152
Figure 5-463: Reception Prob. of Emergency Messages – Scenario 38, HWY, Sender on Rd. B 152
Figure 5-464: Reception Prob. of Emergency Messages-Scenario 38, Sender on Rd. B 152
Figure 5-465: Reception Prob. of Emergency Messages – Scenario 38, Rd. A, Sender on HWY 153
Figure 5-466: Reception Prob. of Emergency Messages – Scenario 38, Rd. B, Sender on HWY 153
Figure 5-467: Reception Prob. of Emergency Messages – Scenario 38, HWY, Sender on HWY 153
Figure 5-468: Reception Prob. of Emergency Messages-Scenario 38, Sender on HWY 153
Figure 5-469: Reception Probability of Emergency Messages-Scenario 39, Road A, Sender RSU 154
Figure 5-470: Reception Probability of Emergency Messages-Scenario 39, Road B, Sender RSU 154

Figure 5-471: Reception Probability of Emergency Messages-Scenario 39, HWY, Sender RSU 154
Figure 5-472: Reception Probability of Emergency Messages-Scenario 39, Sender RSU 154
Figure 5-473: Reception Prob. of Emergency Messages – Scenario 40, Rd. A, Sender on Rd. A1 155
Figure 5-474: Reception Prob. of Emergency Messages – Scenario 40, Rd. B, Sender on Rd. A1 155
Figure 5-475: Reception Prob. of Emergency Messages – Scenario 40, HWY, Sender on Rd. A1 155
Figure 5-476: Reception Prob. of Emergency Messages-Scenario 40, Sender on Rd. A1..... 155
Figure 5-477: Reception Prob. of Emergency Messages – Scenario 40, Rd. A, Sender on Rd. A2 156
Figure 5-478: Reception Prob. of Emergency Messages – Scenario 40, Rd. B, Sender on Rd. A2 156
Figure 5-479: Reception Prob. of Emergency Messages – Scenario 40, HWY, " Sender on Rd. A2 156
Figure 5-480: Reception Prob. of Emergency Messages-Scenario 40, Sender on Rd. A2..... 156
Figure 5-481: Reception Prob. of Emergency Messages – Scenario 40, Rd. A, Sender on Rd. B 157
Figure 5-482: Reception Prob. of Emergency Messages – Scenario 40, Rd. B, Sender on Rd. B 157
Figure 5-483: Reception Prob. of Emergency Messages – Scenario 40, HWY, Sender on Rd. B 157
Figure 5-484: Reception Prob. of Emergency Messages-Scenario 40, Sender on Rd. B..... 157
Figure 5-485: Reception Prob. of Emergency Messages – Scenario 40, Rd. A, Sender on HWY 158
Figure 5-486: Reception Prob. of Emergency Messages – Scenario 40, Rd. B, Sender on HWY 158
Figure 5-487: Reception Prob. of Emergency Messages – Scenario 40, HWY, Sender on HWY 158
Figure 5-488: Reception Prob. of Emergency Messages-Scenario 40, Sender on HWY..... 158
Figure 5-489: Reception Prob. of Routine Message Scenario 41, Rd. A, Sender on Rd. A1 159
Figure 5-490: Reception Prob. of Routine Message Scenario 41, Rd. B, Sender on Rd. A1 159
Figure 5-491: Reception Prob. of Routine Message Scenario 41, HWY, Sender on Rd. A1 159
Figure 5-492: Reception Prob. of Routine Message Scenario 41, RSU, Sender on Rd. A1 159
Figure 5-493: Reception Probability of Emergency Messages-Scenario 41, Sender on Rd. A1 160
Figure 5-494: Reception Prob. of Routine Message Scenario 41, Rd. A, Sender on Rd. A2..... 161
Figure 5-495: Reception Prob. of Routine Message Scenario 41, Rd. B, Sender on Rd. A2..... 161
Figure 5-496: Reception Prob. of Routine Message Scenario 41, HWY, Sender on Rd. A2..... 161
Figure 5-497: Reception Prob. of Routine Message Scenario 41, RSU, Sender on Rd. A2 161
Figure 5-498: Reception Probability of Emergency Messages-Scenario41, Sender on Rd. A2 161
Figure 5-499: Reception Prob. of Routine Message Scenario 41, Rd. A, Sender on HWY..... 162
Figure 5-500: Reception Prob. of Routine Message Scenario 41, Rd. B, Sender on HWY..... 162
Figure 5-501: Reception Prob. of Routine Message Scenario 41, HWY, Sender on HWY..... 162
Figure 5-502: Reception Prob. of Routine Message Scenario 41, RSU, Sender on HWY 162

Figure 5-503: Reception Probability of Emergency Messages-Scenario 41, Sender on HWY . 162
Figure 5-504: Reception Prob. of Routine Message Scenario 42, Rd. A, Sender on Rd. A1..... 164
Figure 5-505: Reception Prob. of Routine Message Scenario 42, Rd. B, Sender on Rd. A1..... 164
Figure 5-506: Reception Prob. of Routine Message Scenario 42, HWY, Sender on Rd. A1..... 164
Figure 5-507: Reception Prob. of Routine Message Scenario 42, RSU, Sender on Rd. A1 164
Figure 5-508: Reception Probability of Emergency Messages-Scenario 42, Sender on Rd. A1 164
Figure 5-509: Reception Prob. of Routine Message Scenario 42, Rd. A, Sender on Rd. A2..... 165
Figure 5-510: Reception Prob. of Routine Message Scenario 42, Rd. B, Sender on Rd. A2..... 165
Figure 5-511: Reception Prob. of Routine Message Scenario 42, HWY, Sender on Rd. A2..... 165
Figure 5-512: Reception Prob. of Routine Message Scenario 42, RSU, Sender on Rd. A2 165
Figure 5-513: Reception Probability of Emergency Messages-Scenario42, Sender on Rd. A1 165
Figure 5-514: Reception Prob. of Routine Message Scenario 42, Rd. A, Sender on HWY..... 166
Figure 5-515: Reception Prob. of Routine Message Scenario 42, Rd. B, Sender on HWY..... 166
Figure 5-516: Reception Prob. of Routine Message Scenario 42, HWY, Sender on HWY..... 166
Figure 5-517: Reception Prob. of Routine Message Scenario 42, RSU, Sender on HWY 166
Figure 5-518: Reception Probability of Emergency Messages-Scenario 42, Sender on HWY 166
Figure 5-519: Propagation Time Over Nodes, Cascading Protocol 1 167
Figure 5-520: Propagation Time Over Nodes, Cascading Protocol 2 168
Figure 5-521: Propagation Time Over Nodes, Cascading Protocol 1 169
Figure 5-522: Propagation Time Over Nodes, Cascading Protocol 2 170
Figure 5-523: Reception Probability of Emergency Messages-Scenario 47, Road A, Sender RSU 171
Figure 5-524: Reception Probability of Emergency Messages-Scenario 47, Road B, Sender RSU 171
Figure 5-525: Reception Probability of Emergency Messages-Scenario 47, HWY, Sender RSU 171
Figure 5-526: Reception Probability of Emergency Messages-Scenario 47, Sender RSU 171
Figure 5-527: Reception Probability of Emergency Messages-Scenario 48, Road A, Sender RSU 172
Figure 5-528: Reception Probability of Emergency Messages-Scenario 48, Road B, Sender RSU 172
Figure 5-529: Reception Probability of Emergency Messages-Scenario 48, HWY, Sender RSU 172
Figure 5-530: Reception Probability of Emergency Messages-Scenario 48, Sender RSU 172
Figure 5-531: Reception Probability of Emergency Messages-Scenario 49, Road A, Sender RSU 173
Figure 5-532: Reception Probability of Emergency Messages-Scenario 49, Road B, Sender RSU 173
Figure 5-533: Reception Probability of Emergency Messages-Scenario 49, HWY, Sender RSU 173
Figure 5-534: Reception Probability of Emergency Messages-Scenario 49, Sender RSU 173
Figure 5-535: Reception Probability of Emergency Messages-Scenario 50, Road A, Sender RSU 174
Figure 5-536: Reception Probability of Emergency Messages-Scenario 50, Road B, Sender RSU 174
Figure 5-537: Reception Probability of Emergency Messages-Scenario 50, HWY, Sender RSU 174
Figure 5-538: Reception Probability of Emergency Messages-Scenario 50, Sender RSU 174

Figure 6-1: Reception Probability of Routine Messages – Scenario 9, Road A..... 176
Figure 6-2: Reception Probability of Routine Messages – Scenario 9, Road A..... 176
Figure 6-3: Time Bound for Desired Confidence, Routine Messages - Scenario 9, Road A..... 176
Figure 6-4: Time Bound for Desired Confidence, Routine Messages - Scenario 9, Road B..... 176
Figure 6-5: Reception Probability of Routine Messages on Road A, Scenario 11..... 177
Figure 6-6: Reception Probability of Routine Messages on Road B, Scenario 11..... 177
Figure 6-7: Time Bound for Desired Confidence, Routine Messages - Scenario 11, Road A... 177
Figure 6-8: Time Bound for Desired Confidence, Routine Messages - Scenario 11, Road B... 177
Figure 6-9: Reception Probability of Routine Messages on Road A, Scenario 17..... 178
Figure 6-10: Reception Probability of Routine Messages on Road B, Scenario 17..... 178
Figure 6-11: Time Bound for Desired Confidence, Routine Messages - Scenario 17, Road A. 178
Figure 6-12: Time Bound for Desired Confidence, Routine Messages - Scenario 17, Road B. 178
Figure 6-13: Reception Probability of Routine Messages on Road A, Scenario 19..... 179
Figure 6-14: Reception Probability of Routine Messages on Road B, Scenario 19..... 179
Figure 6-15: Time Bound for Desired Confidence, Routine Messages -Scenario 19, Road A.. 179
Figure 6-16: Time Bound for Desired Confidence, Routine Messages - Scenario 19, Road B. 179
Figure 6-17: Reception Probability of Routine Messages on Road A Scenario 25..... 180
Figure 6-18: Reception Probability of Routine Messages on Road B Scenario 25..... 180
Figure 6-19: Time Bound for Desired Confidence, Routine Messages - Scenario 25, Road A. 180
Figure 6-20: Time Bound for Desired Confidence, Routine Messages - Scenario 25, Road B. 180
Figure 6-21: Reception Probability of Routine Messages on Road A, Scenario 27..... 181
Figure 6-22: Reception Probability of Routine Messages on Road B, Scenario 27..... 181
Figure 6-23: Time Bound for Desired Confidence, Routine Messages - Scenario 27, Road A. 181
Figure 6-24: Time Bound for Desired Confidence, Routine Messages - Scenario 27, Road B. 181
Figure 6-25: Reception Probability of Routine Messages on Road A, Scenario 33..... 182
Figure 6-26: Reception Probability of Routine Messages on Road B, Scenario 33..... 182
Figure 6-27: Time Bound for Desired Confidence, Routine Messages - Scenario 33, Road A. 182
Figure 6-28: Time Bound for Desired Confidence, Routine Messages - Scenario 33, Road B. 182
Figure 6-29: Reception Probability of Routine Messages on Road A Scenario 35..... 183
Figure 6-30: Reception Probability of Routine Messages on Road B Scenario 35..... 183
Figure 6-31: Time Bound for Desired Confidence, Routine Messages - Scenario 35, Road A. 183
Figure 6-32: Time Bound for Desired Confidence, Routine Messages - Scenario 35, Road B. 183
Figure 6-33: Reception Probability of Routine Messages on Road A, Scenario 49..... 184
Figure 6-34: Reception Probability of Routine Messages on Road B, Scenario 49..... 184
Figure 6-35: Time Bound for Desired Confidence, Routine Messages - Scenario 49, Road A. 184
Figure 6-36: Time Bound for Desired Confidence, Routine Messages - Scenario 49, Road B. 184
Figure 6-37: Reception Probability of Routine Messages on Road A, Scenario 50..... 185
Figure 6-38: Reception Probability of Routine Messages on Road B, Scenario 50..... 185
Figure 6-39: Time Bound for Desired Confidence, Routine Messages - Scenario 50, Road A. 185
Figure 6-40: Time Bound for Desired Confidence, Routine Messages - Scenario 50, Road B. 185
Figure 6-41: Reception Probability of Emergency Messages-Scenario 9, Road A, Sender RSU..... 186
Figure 6-42: Reception Probability of Emergency Messages-Scenario 9, Road B, Sender RSU..... 186
Figure 6-43: Time Bound for Desired Confidence, Emergency Messages - Scenario 9, Road A, Sender RSU..... 186
Figure 6-44: Time Bound for Desired Confidence, Emergency Messages - Scenario 9, Road B, Sender RSU..... 186
Figure 6-45: Reception Probability of Emergency Messages-Scenario 11, Road A, Sender RSU..... 187

Figure 6-46: Reception Probability of Emergency Messages-Scenario 11, Road B, Sender RSU 187
Figure 6-47: Time Bound for Desired Confidence, Emergency Messages - Scenario 11, Road A, Sender RSU 187
Figure 6-48: Time Bound for Desired Confidence, Emergency Messages - Scenario 11, Road B, Sender RSU 187
Figure 6-49: Reception Prob. of Emergency Messages – Scenario 13, Rd. A, Sender on Rd. A2 188
Figure 6-50: Reception Prob. of Emergency Messages – Scenario 13, Rd. B, Sender on Rd. A2 188
Figure 6-51: Time Bound for Desired Confidence, Emergency Messages – Scenario 13, Road A, Sender on Road A2 188
Figure 6-52: Time Bound for Desired Confidence, Emergency Messages - Scenario 13, Road B, Sender on Road A2 188
Figure 6-53: Reception Prob. of Emergency Messages – Scenario 15, Rd. A, Sender on Rd. A2 189
Figure 6-54: Reception Prob. of Emergency Messages – Scenario 15, Rd. B, Sender on Rd. A2 189
Figure 6-55: Time Bound for Desired Confidence, Emergency Messages - Scenario 15, Road A, Sender on Road A2 189
Figure 6-56: Time Bound for Desired Confidence, Emergency Messages - Scenario 15, Road B, Sender on Road A2 189
Figure 6-57: Reception Probability of Emergency Messages-Scenario17, Road A, Sender RSU 190
Figure 6-58: Reception Probability of Emergency Messages-Scenario 17, Road B, Sender RSU 190
Figure 6-59: Time Bound for Desired Confidence, Emergency Messages – Scenario 17, Road A, Sender RSU 190
Figure 6-60: Time Bound for Desired Confidence, Emergency Messages – Scenario 17, Road B, Sender RSU 190
Figure 6-61: Reception Prob. of Emergency Messages – Scenario 18, Rd. A, Sender on Rd. A2 191
Figure 6-62: Reception Prob. of Emergency Messages – Scenario 18, Rd. B, Sender on Rd. A2 191
Figure 6-63: Time Bound for Desired Confidence, Emergency Messages - Scenario 18, Road A, Sender on Road A2 191
Figure 6-64: Time Bound for Desired Confidence, Emergency Messages - Scenario 18, Road B, Sender on Road A2 191
Figure 6-65: Reception Probability of Emergency Messages-Scenario 19, Road A, Sender RSU 192
Figure 6-66: Reception Probability of Emergency Messages-Scenario 19, Road B, Sender RSU 192
Figure 6-67: Time Bound for Desired Confidence, Emergency Messages - Scenario 19, Road A, Sender RSU 192
Figure 6-68: Time Bound for Desired Confidence, Emergency Messages - Scenario 19, Road B, Sender RSU 192
Figure 6-69: Reception Prob. of Emergency Messages – Scenario 20, Rd. A, Sender on Rd. A2 193
Figure 6-70: Reception Prob. of Emergency Messages – Scenario 20, Rd. B, Sender on Rd. A2 193

Figure 6-71: Time Bound for Desired Confidence, Emergency Messages - Scenario 20, Road A, Sender on Road A2 193
Figure 6-72: Time Bound for Desired Confidence, Emergency Messages - Scenario 20, Road B, Sender on Road A2..... 193
Figure 6-73: Reception Probability of Emergency Messages-Scenario 21, Road A, Sender RSU 194
Figure 6-74: Reception Probability of Emergency Messages-Scenario 21, Road B, Sender RSU 194
Figure 6-75: Time Bound for Desired Confidence, Emergency Messages - Scenario 21, Road A, Sender RSU..... 194
Figure 6-76: Time Bound for Desired Confidence, Emergency Messages - Scenario 21, Road B, Sender RSU 194
Figure 6-77: Reception Prob. of Emergency Messages – Scenario 22, Rd. A, Sender on Rd. A2 195
Figure 6-78: Reception Prob. of Emergency Messages – Scenario 22, Rd. B, Sender on Rd. A2 195
Figure 6-79: Time Bound for Desired Confidence, Emergency Messages - Scenario 22, Road A, Sender on Road A2 195
Figure 6-80: Time Bound for Desired Confidence, Emergency Messages - Scenario 22, Road B, Sender on Road A2..... 195
Figure 6-81: Reception Probability of Emergency Messages-Scenario 23, Road A, Sender RSU..... 196
Figure 6-82: Reception Probability of Emergency Messages-Scenario 23, Road B, Sender RSU 196
Figure 6-83: Time Bound for Desired Confidence, Emergency Messages - Scenario 23, Road A, Sender RSU..... 196
Figure 6-84: Time Bound for Desired Confidence, Emergency Messages - Scenario 23, Road B, Sender RSU 196
Figure 6-85: Reception Prob. of Emergency Messages – Scenario 24, Rd. A, Sender on Rd. A2 197
Figure 6-86: Reception Prob. Of Emergency Messages –Scenario 24, Rd. B, Sender on Rd. A2 197
Figure 6-87: Time Bound for Desired Confidence, Emergency Messages - Scenario 24, Road A, Sender on Road A2 197
Figure 6-88: Time Bound for Desired Confidence, Emergency Messages - Scenario 24, Road B, Sender on Road A2..... 197
Figure 6-89: Reception Probability of Emergency Messages-Scenario 25, Road A, Sender RSU..... 198
Figure 6-90: Reception Probability of Emergency Messages-Scenario 25, Road B, Sender RSU 198
Figure 6-91: Time Bound for Desired Confidence, Emergency Messages - Scenario 25, Road A, Sender RSU..... 198
Figure 6-92: Time Bound for Desired Confidence, Emergency Messages - Scenario 25, Road B, Sender RSU 198
Figure 6-93: Reception Prob. of Emergency Messages – Scenario 26, Rd. A, Sender on Rd. A2 199
Figure 6-94: Reception Prob. of Emergency Messages – Scenario 26, Rd. B, Sender on Rd. A2 199
Figure 6-95: Time Bound for Desired Confidence, Emergency Messages - Scenario 26, Road A, Sender on Road A2 199

Figure 6-96: Time Bound for Desired Confidence, Emergency Messages - Scenario 26, Road B, Sender on Road A2 199
Figure 6-97: Reception Probability of Emergency Messages-Scenario 27, Road A, Sender RSU 200
Figure 6-98: Reception Probability of Emergency Messages-Scenario 27, Road B, Sender RSU 200
Figure 6-99: Time Bound for Desired Confidence, Emergency Messages - Scenario 27, Road A, Sender RSU 200
Figure 6-100: Time Bound for Desired Confidence, Emergency Messages – Scenario 27, Road B, Sender RSU 200
Figure 6-101: Reception Prob. of Emergency Messages – Scenario 28, Rd. A, Sender on Rd. A2 201
Figure 6-102: Reception Prob. of Emergency Messages – Scenario 28, Rd. B, Sender on Rd. A2 201
Figure 6-103: Time Bound for Desired Confidence, Emergency Messages - Scenario 28, Road A, Sender on Road A2 201
Figure 6-104: Time Bound for Desired Confidence, Emergency Messages - Scenario 28, Road B, Sender on Road A2 201
Figure 6-105: Reception Probability of Emergency Messages-Scenario 29, Road A, Sender RSU 202
Figure 6-106: Reception Probability of Emergency Messages-Scenario 29, Road B, Sender RSU 202
Figure 6-107: Time Bound for Desired Confidence, Emergency Messages - Scenario 29, Road A, Sender RSU 202
Figure 6-108: Time Bound for Desired Confidence, Emergency Messages - Scenario 29, Road B, Sender RSU 202
Figure 6-109: Reception Prob. of Emergency Messages – Scenario 30, Rd. A, Sender on Rd. A2 203
Figure 6-110: Reception Prob. of Emergency Messages – Scenario 30, Rd. B, Sender on Rd A2 203
Figure 6-111: Time Bound for Desired Confidence, Emergency Messages - Scenario 30, Road A, Sender on Road A2 203
Figure 6-112: Time Bound for Desired Confidence, Emergency Messages - Scenario 30, Road B, Sender on Road A2 203
Figure 6-113: Reception Probability of Emergency Messages-Scenario 31, Road A, Sender RSU 204
Figure 6-114: Reception Probability of Emergency Messages-Scenario 31, Road B, Sender RSU 204
Figure 6-115: Time Bound for Desired Confidence, Emergency Messages - Scenario 31, Road A, Sender RSU 204
Figure 6-116: Time Bound for Desired Confidence, Emergency Messages - Scenario 31, Road B, Sender RSU 204
Figure 6-117: Reception Prob. of Emergency Messages – Scenario 32, Rd. A, Sender on Rd. A2 205
Figure 6-118: Reception Prob. of Emergency Messages – Scenario 32, Rd. B, Sender on Rd A2 205
Figure 6-119: Time Bound for Desired Confidence, Emergency Messages - Scenario 32, Road A, Sender on Road A2 205
Figure 6-120: Time Bound for Desired Confidence, Emergency Messages – Scenario 32, Road B, Sender on Road A2 205

Figure 6-121: Reception Probability of Emergency Messages-Scenario 33, Road A, Sender RSU 206
Figure 6-122: Reception Probability of Emergency Messages-Scenario 33, Road B, Sender RSU 206
Figure 6-123: Time Bound for Desired Confidence, Emergency Messages - Scenario 33, Road A, Sender RSU 206
Figure 6-124: Time Bound for Desired Confidence, Emergency Messages – Scenario 33, Road B, Sender RSU 206
Figure 6-125: Reception Prob. of Emergency Messages – Scenario 34, Rd. A, Sender on Rd. A2 207
Figure 6-126: Reception Prob. of Emergency Messages – Scenario 34, Rd. B, Sender on Rd. A2 207
Figure 6-127: Time Bound for Desired Confidence, Emergency Messages - Scenario 34, Road A, Sender on Road A2 207
Figure 6-128: Time Bound for Desired Confidence, Emergency Messages - Scenario 34, Road B, Sender on Road A2 207
Figure 6-129: Reception Probability of Emergency Messages-Scenario 35, Road A, Sender RSU 208
Figure 6-130: Reception Probability of Emergency Messages-Scenario 35, Road B, Sender RSU 208
Figure 6-131: Time Bound for Desired Confidence, Emergency Messages - Scenario 35, Road A, Sender RSU 208
Figure 6-132: Time Bound for Desired Confidence, Emergency Messages – Scenario 35, Road B, Sender RSU 208
Figure 6-133: Reception Prob. of Emergency Messages – Scenario 36, Rd. A, Sender on Rd. A2 209
Figure 6-134: Reception Prob. of Emergency Messages – Scenario 36, Rd. B, Sender on Rd. A2 209
Figure 6-135: Time Bound for Desired Confidence, Emergency Messages - Scenario 36, Road A, Sender on Road A2 209
Figure 6-136: Time Bound for Desired Confidence, Emergency Messages - Scenario 36, Road B, Sender on Road A2 209
Figure 6-137: Reception Probability of Emergency Messages-Scenario 37, Road A, Sender RSU 210
Figure 6-138: Reception Probability of Emergency Messages-Scenario 37, Road B, Sender RSU 210
Figure 6-139: Time Bound for Desired Confidence, Emergency Messages - Scenario 37, Road A, Sender RSU 210
Figure 6-140: Time Bound for Desired Confidence, Emergency Messages - Scenario 37, Road B, Sender RSU 210
Figure 6-141: Reception Prob. of Emergency Messages – Scenario 38, Rd. A, Sender on Rd. A2 211
Figure 6-142: Reception Prob. of Emergency Messages –Scenario 38, Rd. B, Sender on Rd. A2 211
Figure 6-143: Time Bound for Desired Confidence, Emergency Messages - Scenario 38, Road A, Sender on Road A2 211
Figure 6-144: Time Bound for Desired Confidence, Emergency Messages - Scenario 38, Road B, Sender on Road A2 211
Figure 6-145: Reception Probability of Emergency Messages-Scenario 39, Road A, Sender RSU 212

Figure 6-146: Reception Probability of Emergency Messages-Scenario 39, Road B, Sender RSU 212
Figure 6-147: Time Bound for Desired Confidence, Emergency Messages - Scenario 39, Road A, Sender RSU 212
Figure 6-148: Time Bound for Desired Confidence, Emergency Messages - Scenario 39, Road B, Sender RSU 212
Figure 6-149: Reception Prob. of Emergency Messages – Scenario 40, Rd. A, Sender on Rd. A2 213
Figure 6-150: Reception Prob. of Emergency Messages –Scenario 40, Rd. B, Sender on Rd. A2 213
Figure 6-151: Time Bound for Desired Confidence, Emergency Messages - Scenario 40, Road A, Sender on Road A2 213
Figure 6-152: Time Bound for Desired Confidence, Emergency Messages - Scenario 40, Road B, Sender on Road A2 213
Figure 6-153: Reception Probability of Emergency Messages-Scenario 49, Road A, Sender RSU 214
Figure 6-154: Reception Probability of Emergency Messages-Scenario 49, Road B, Sender RSU 214
Figure 6-155: Time Bound for Desired Confidence, Emergency Messages - Scenario 49, Road A, Sender RSU 214
Figure 6-156: Time Bound for Desired Confidence, Emergency Messages – Scenario 49, Road B, Sender RSU 214
Figure 6-157: Reception Probability of Emergency Messages-Scenario 50, Road A, Sender RSU 215
Figure 6-158: Reception Probability of Emergency Messages-Scenario 50, Road B, Sender RSU 215
Figure 6-159: Time Bound for Desired Confidence, Emergency Messages - Scenario 50, Road A, Sender RSU 215
Figure 6-160: Time Bound for Desired Confidence, Emergency Messages – Scenario 50, Road B, Sender RSU 215
Figure 7-1: Reception Probability of Emergency Messages without RSU Retransmission, Road A, Sender on Road A1 216
Figure 7-2: Reception Probability of Emergency Messages with RSU Retransmission, Road A, Sender on Road A1 216
Figure 7-3: Reception Probability of Emergency Messages without RSU Retransmission, Road B, Sender on Road A1 216
Figure 7-4: Reception Probability of Emergency Messages with RSU Retransmission, Road B, Sender on Road A1 216
Figure 7-5: Visualization of the Reception Probability of Emergency Messages without RSU Retransmission, Sender on Road A1 217
Figure 7-6: Visualization of the Reception Probability of Emergency Messages with RSU Retransmission, Sender on Road A1 217
Figure 7-7: Reception Probability of Emergency Messages without RSU Retransmission, Road A, Sender on Road A1 218
Figure 7-8: Reception Probability of Emergency Messages with RSU Retransmission, Road A, Sender on Road A1 218
Figure 7-9: Reception Probability of Emergency Messages without RSU Retransmission, Road B, Sender on Road A1 218
Figure 7-10: Reception Probability of Emergency Messages with RSU Retransmission, Road B, Sender on Road A1 218

Figure 7-11: Visualization of the Reception Probability of Emergency Messages Without RSU Retransmission, Sender on Road A1 219
Figure 7-12: Visualization of the Reception Probability of Emergency Messages With RSU Retransmission, Sender on Road A1 219
Figure 7-13: Reception Probability of Emergency Messages Without RSU Retransmission, Road A, Sender on Road A1..... 220
Figure 7-14: Reception Probability of Emergency Messages With RSU Retransmission, Road A, Sender on Road A1..... 220
Figure 7-15: Reception Probability of Emergency MessagesWwithout RSU Retransmission, Road B, Sender on Road A1..... 220
Figure 7-16: Reception Probability of Emergency Messages With RSU Retransmission, Road B, Sender on Road A1..... 220
Figure 7-17: Visualization of the Reception Probability of Emergency Messages Without RSU Retransmission, Sender on Road A1 221
Figure 7-18: Visualization of the Reception Probability of Emergency Messages With RSU Retransmission, Sender on Road A1 221
Figure 8-1: Reception Probability of Emergency Messages-Scenario 11, Road A, Sender RSU..... 223
Figure 8-2: Reception Probability of Emergency Messages-Scenario 11, Road B, Sender RSU..... 223
Figure 8-3: Reception Probability of Emergency Messages-Scenario 11, HWY, Sender RSU 223
Figure 8-4: Reception Probability of Emergency Messages-Scenario11, Sender RSU 223
Figure 8-5: Reception Probability of Emergency Messages-Scenario 11, Road A, Sender RSU..... 224
Figure 8-6: Reception Probability of Emergency Messages-Scenario 11, Road B, Sender RSU..... 224
Figure 8-7: Time Bound for Desired Confidence, Emergency Messages - Scenario 11, Road A, Sender RSU..... 224
Figure 8-8: Time Bound for Desired Confidence, Emergency Messages – Scenario 11, Road B, Sender RSU..... 224
Figure 8-9: Reception Probability of Routine Messages on Road A, Scenario 11..... 225
Figure 8-10: Reception Probability of Routine Messages on Road A, Scenario 11..... 225
Figure 8-11: Reception Probability of Routine Messages on Road B, Scenario 11..... 225
Figure 8-12: Reception Probability of Routine Messages on Road B, Scenario 11..... 225
Figure 8-13: Reception Probability of Routine Messages on HWY, Scenario 11 225
Figure 8-14: Reception Probability of Routine Messages on HWY, Scenario 11 225
Figure 8-15: Reception Probability of Routine Messages on Road A, Scenario 11..... 226
Figure 8-16: Reception Probability of Routine Messages on Road B, Scenario 11..... 226
Figure 8-17: Time Bound for Desired Confidence, Routine Messages - Scenario 11, Road A..... 226
Figure 8-18: Time Bound for Desired Confidence, Routine Messages - Scenario 11, Road B..... 226
Figure 8-19: Reception Probability of Emergency Messages-Scenario 11, Road A, Sender RSU..... 227
Figure 8-20: Reception Probability of Emergency Messages-Scenario 11, Road B, Sender RSU..... 227
Figure 8-21: Reception Probability of Emergency Messages-Scenario 11, HWY, Sender RSU..... 227
Figure 8-22: Reception Probability of Emergency Messages-Scenario 11, Sender RSU 227

Figure 8-23: Reception Probability of Emergency Messages-Scenario 11, Road A, Sender RSU 228
Figure 8-24: Reception Probability of Emergency Messages-Scenario 11, Road B, Sender RSU 228
Figure 8-25: Time Bound for desired Confidence, Emergency Messages - Scenario 11, Road A, Sender RSU 228
Figure 8-26: Time Bound for Desired Confidence, Emergency Messages - Scenario 11, Road B, Sender RSU 228
Figure 8-27: Reception Probability of Routine Messages on Road A Scenario 11 229
Figure 8-28: Reception Probability of Routine Messages on Road A, Scenario 11 229
Figure 8-29: Reception Probability of Routine Messages on Road B, Scenario 11 229
Figure 8-30: Reception Probability of Routine Messages on Road B, Scenario 11 229
Figure 8-31: Reception Probability of Routine Messages on HWY, Scenario 11 229
Figure 8-32: Reception Probability of Routine Messages on HWY, Scenario 11 229
Figure 8-33: Reception Probability of Routine Messages on Road A, Scenario 11 230
Figure 8-34: Reception Probability of Routine Messages on Road B, Scenario 11 230
Figure 8-35: Time Bound for Desired Confidence, Routine Messages – Scenario 11, Road A 230
Figure 8-36: Time Bound for Desired Confidence, Routine Messages - Scenario 11, Road B 230
Figure 8-37: Reception Probability of Emergency Messages-Scenario 11, Road A, Sender RSU 231
Figure 8-38: Reception Probability of Emergency Messages-Scenario 11, Road B, Sender RSU 231
Figure 8-39: Reception Probability of Emergency Messages-Scenario 11, HWY, Sender RSU 231
Figure 8-40: Reception Probability of Emergency Messages-Scenario 11, Sender RSU 231
Figure 8-41: Reception Probability of Emergency Messages-Scenario 11, Road A, Sender RSU 232
Figure 8-42: Reception Probability of Emergency Messages-Scenario 11, Road B, Sender RSU 232
Figure 8-43: Time Bound for Desired Confidence, Emergency Messages - Scenario 11, Road A, Sender RSU 232
Figure 8-44: Time Bound for Desired Confidence, Emergency Messages - Scenario 11, Road B, Sender RSU 232
Figure 8-45: Reception Probability of Routine Messages on Road A, Scenario 11 233
Figure 8-46: Reception Probability of Routine Messages on Road A, Scenario 11 233
Figure 8-47: Reception Probability of Routine Messages on Road B, Scenario 11 233
Figure 8-48: Reception Probability of Routine Messages on Road B, Scenario 11 233
Figure 8-49: Reception Probability of Routine Messages on HWY, Scenario 11 233
Figure 8-50: Reception Probability of Routine Messages on HWY, Scenario 11 233
Figure 8-51: Reception Probability of Routine Messages on Road A, Scenario 11 234
Figure 8-52: Reception Probability of Routine Messages on Road B, Scenario 11 234
Figure 8-53: Time Bound for Desired Confidence, Routine Messages - Scenario 11, Road A 234
Figure 8-54: Time Bound for Desired Confidence, Routine Messages - Scenario 11, Road B 234
Figure 8-55: Reception Probability of Emergency Messages-Scenario 11, Road A, Sender RSU 235
Figure 8-56: Reception Probability of Emergency Messages-Scenario 11, Road B, Sender RSU 235

Figure 8-57: Reception Probability of Emergency Messages-Scenario 11, HWY, Sender RSU 235
Figure 8-58: Reception Probability of Emergency Messages-Scenario11, Sender RSU 235
Figure 8-59: Reception Probability of Emergency Messages-Scenario 11, Road A, Sender RSU 236
Figure 8-60: Reception Probability of Emergency Messages-Scenario 11, Road B, Sender RSU 236
Figure 8-61: Time Bound for Desired Confidence, Emergency Messages - Scenario 11, Road A, Sender RSU 236
Figure 8-62: Time Bound for Desired Confidence, Emergency Messages – Scenario 11, Road B, Sender RSU 236
Figure 8-63: Reception Probability of Routine Messages on Road A, Scenario 11 237
Figure 8-64: Reception Probability of Routine Messages on Road A, Scenario 11 237
Figure 8-65: Reception Probability of Routine Messages on Road B, Scenario 11 237
Figure 8-66: Reception Probability of Routine Messages on Road B, Scenario 11 237
Figure 8-67: Reception Probability of Routine Messages on HWY, Scenario 11 237
Figure 8-68: Reception Probability of Routine Messages on HWY, Scenario 11 237
Figure 8-69: Reception Probability of Routine Messages on Road A, Scenario 11 238
Figure 8-70: Reception Probability of Routine Messages on Road B, Scenario 11 238
Figure 8-71: Time Bound for Desired Confidence, Routine Messages - Scenario 11, Road A 238
Figure 8-72: Time Bound for Desired Confidence, Routine Messages - Scenario 11, Road B 238
Figure 8-73: Reception Probability of Emergency Messages-Scenario 11, Road A, Sender RSU 239
Figure 8-74: Reception Probability of Emergency Messages-Scenario 11, Road B, Sender RSU 239
Figure 8-75: Reception Probability of Emergency Messages-Scenario 11, HWY, Sender RSU 239
Figure 8-76: Reception Probability of Emergency Messages-Scenario11, Sender RSU 239
Figure 8-77: Reception Probability of Emergency Messages-Scenario 11, Road A, Sender RSU 240
Figure 8-78: Reception Probability of Emergency Messages-Scenario 11, Road B, Sender RSU 240
Figure 8-79: Time Bound for Desired Confidence, Emergency Messages - Scenario 11, Road A, Sender RSU 240
Figure 8-80: Time Bound for Desired Confidence, Emergency Messages - Scenario 11, Road B, Sender RSU 240
Figure 8-81: Reception Probability of Routine Messages on Road A, Scenario 11 241
Figure 8-82: Reception Probability of Routine Messages on Road A, Scenario 11 241
Figure 8-83: Reception Probability of Routine Messages on Road B, Scenario 11 241
Figure 8-84: Reception Probability of Routine Messages on Road B, Scenario 11 241
Figure 8-85: Reception Probability of Routine Messages on HWY, Scenario 11 241
Figure 8-86: Reception Probability of Routine Messages on HWY, Scenario 11 241
Figure 8-87: Reception Probability of Routine Messages on Road A, Scenario 11 242
Figure 8-88: Reception Probability of Routine Messages on Road B, Scenario 11 242
Figure 8-89: Time Bound for Desired Confidence, Routine Messages - Scenario 11, Road A 242
Figure 8-90: Time Bound for Desired Confidence, Routine Messages - Scenario 11, Road B 242

Figure 8-91: Reception Probability of Emergency Messages-Scenario 11, Road A, Sender RSU 243
Figure 8-92: Reception Probability of Emergency Messages-Scenario 11, Road B, Sender RSU 243
Figure 8-93: Reception Probability of Emergency Messages-Scenario 11, HWY, Sender RSU 243
Figure 8-94: Reception Probability of Emergency Messages-Scenario 11, Sender RSU 243
Figure 8-95: Reception Probability of Emergency Messages-Scenario 11, Road A, Sender RSU 244
Figure 8-96: Reception Probability of Emergency Messages-Scenario 11, Road B, Sender RSU 244
Figure 8-97: Time Bound for Desired Confidence, Emergency Messages - Scenario 11, Road A, Sender RSU 244
Figure 8-98: Time Bound for Desired Confidence, Emergency Messages - Scenario 11, Road B, Sender RSU 244
Figure 8-99: Reception Probability of Routine Messages on Road A, Scenario 11 245
Figure 8-100: Reception Probability of Routine Messages on Road A, Scenario 11 245
Figure 8-101: Reception Probability of Routine Messages on Road B, Scenario 11 245
Figure 8-102: Reception Probability of Routine Messages on Road B, Scenario 11 245
Figure 8-103: Reception Probability of Routine Messages on HWY, Scenario 11 245
Figure 8-104: Reception Probability of Routine Messages on HWY, Scenario 11 245
Figure 8-105: Reception Probability of Routine Messages on Road A, Scenario 11 246
Figure 8-106: Reception Probability of Routine Messages on Road B, Scenario 11 246
Figure 8-107: Time Bound for Desired Confidence, Routine Messages - Scenario 11, Road A 246
Figure 8-108: Time Bound for Desired Confidence, Routine Messages - Scenario 11, Road B 246
Figure 8-109: Reception Probability of Emergency Messages-Scenario 11, Road A, Sender RSU 247
Figure 8-110: Reception Probability of Emergency Messages-Scenario 11, Road B, Sender RSU 247
Figure 8-111: Reception Probability of Emergency Messages-Scenario 11, HWY, Sender RSU 247
Figure 8-112: Reception Probability of Emergency Messages-Scenario 11, Sender RSU 247
Figure 8-113: Reception Probability of Emergency Messages-Scenario 11, Road A, Sender RSU 248
Figure 8-114: Reception Probability of Emergency Messages-Scenario 11, Road B, Sender RSU 248
Figure 8-115: Time Bound for Desired Confidence, Emergency Messages - Scenario 11, Road A, Sender RSU 248
Figure 8-116: Time Bound for Desired Confidence, Emergency Messages – Scenario 11, Road B, Sender RSU 248
Figure 8-117: Reception Probability of Routine Messages on Road A, Scenario 11 249
Figure 8-118: Reception Probability of Routine Messages on Road A, Scenario 11 249
Figure 8-119: Reception Probability of Routine Messages on Road B, Scenario 11 249
Figure 8-120: Reception Probability of Routine Messages on Road B, Scenario 11 249
Figure 8-121: Reception Probability of Routine Messages on HWY, Scenario 11 249
Figure 8-122: Reception Probability of Routine Messages on HWY, Scenario 11 249
Figure 8-123: Reception Probability of Routine Messages on Road A, Scenario 11 250
Figure 8-124: Reception Probability of Routine Messages on Road B, Scenario 11 250

Figure 8-125: Time Bound for Desired Confidence, Routine Messages – Scenario 11, Road A 250
Figure 8-126: Time Bound for Desired Confidence, Routine Messages - Scenario 11, Road B 250
Figure 8-127: Reception Probability of Emergency Messages-Scenario 11, Road A, Sender RSU 251
Figure 8-128: Reception Probability of Emergency Messages-Scenario 11, Road B, Sender RSU 251
Figure 8-129: Reception Probability of Emergency Messages-Scenario 11, HWY, Sender RSU 251
Figure 8-130: Reception Probability of Emergency Messages-Scenario 11, Sender RSU 251
Figure 8-131: Reception Probability of Emergency Messages-Scenario 11, Road A, Sender RSU 252
Figure 8-132: Reception Probability of Emergency Messages-Scenario 11, Road B, Sender RSU 252
Figure 8-133: Time Bound for Desired Confidence, Emergency Messages - Scenario 11, Road A, Sender RSU 252
Figure 8-134: Time Bound for Desired Confidence, Emergency Messages - Scenario 11, Road B, Sender RSU 252
Figure 8-135: Reception Probability of Routine Messages on Road A, Scenario 11 253
Figure 8-136: Reception Probability of Routine Messages on Road A, Scenario 11 253
Figure 8-137: Reception Probability of Routine Messages on Road B, Scenario 11 253
Figure 8-138: Reception Probability of Routine Messages on Road B, Scenario 11 253
Figure 8-139: Reception Probability of Routine Messages on HWY, Scenario 11 253
Figure 8-140: Reception Probability of Routine Messages on HWY, Scenario 11 253
Figure 8-141: Reception Probability of Routine Messages on Road A, Scenario 11 254
Figure 8-142: Reception Probability of Routine Messages on Road B, Scenario 11 254
Figure 8-143: Time Bound for desired Confidence, Routine Messages - Scenario 11, Road A 254
Figure 8-144: Time Bound for desired Confidence, Routine Messages - Scenario 11, Road B 254

TABLE OF TABLES

Table 2.1. Node ID Prefixes 12
Table 2.2. Example Initial Script Node Configuration 13

1 Introduction

This appendix summarizes the progress and findings of Task 12, the follow-on effort to VSC Task 6A. In this task, the focus is on evaluating simulated DSRC performance in an urban intersection environment densely populated with DSRC-equipped vehicles. This environment includes a nearby highway for compounding nearby message traffic effects.

In order to accomplish this goal, several modifications were made to the DSRC simulator, originally developed under task 4 and enhanced under task 6A. The most significant change was the addition of an intersection traffic and roadway environment to the simulator. This involved the addition of buildings to the simulation environment, which necessitated the creation of new radio frequency (RF) models to accommodate multi-path, dominant effects due to radio signal reflections off the buildings. The team conducted road tests at a representative city intersection with buildings at all four corners to develop these empirical RF models for the simulator. For comparison, DSRC performance was also evaluated without buildings present in the intersection setting. This was done using empirically derived highway RF models for open road conditions.

Once the RF models and intersection models were constructed, a number of simulation cases were defined in order to closely examine communication channel performance under varying conditions in the urban setting. Each simulation case required at least one complete simulation test run. These results were then analyzed using additional mathematical tools, often several analyses were run per simulation case, in order to produce presentable results contained in this appendix.

1.1 Simulation Test Scenarios and Setup

The simulation scenarios described in this appendix were focused upon high-volume, signalized intersections. For potential future field testing of cooperative intersection crash countermeasures built upon DSRC technology, it is important to determine if DSRC is likely to support this class of applications in such dense traffic situations.

Accordingly, simulation test scenarios were designed to focus on a high-volume intersection environment. The following sections discuss the overall simulation test scenarios and setup.

1.1.1 Intersection Simulation Environment

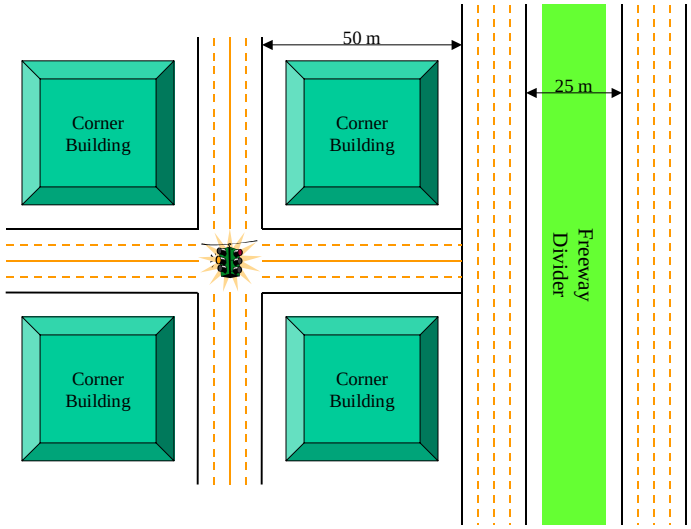


Figure 1-1: Intersection Simulation Environment

As shown in Figure 1-1: Intersection Simulation Environment, an intersection with four lanes of traffic in each leg is defined. Each lane is four meters wide. There are buildings at each corner spaced 8m from the edges of the roads so that there is a shadowing effect for communications around the corner. One freeway with four lanes in each direction is placed near the intersection. There is a 25-meter open gap between the two directions of travel with no barrier in between. The freeway runs parallel to one of the roads forming the intersection. The distance between the freeway edge and this road is 50m. The close presence of the freeway in this setup is meant to feed in a large amount of external interference. This combination of roadways creates an environment with potentially very high vehicle count in an intersection environment in a believable manner.

One RSU node is placed at a 5-meter height in the middle of the intersection. Four commercial RSUs are to be placed along the four legs of the intersection. These commercial RSUs will inject additional non-safety messages into the channel.

Vehicle flows for both the intersection roads and the freeway are configured in dense but believable manners. The vehicle density is 80 cars per lane mile on the freeway. One road of the intersection has 134 cars per lane mile, assuming the traffic is flowing, while the other road has a stopped-traffic density of 230 cars per lane mile.

1.1.2 Simulation Communication Settings

Four types of messages are configured to compete for channel access in the simulation test scenarios.

- **Routine Safety Messages**. Some applications specified in task 3 call for routine safety messages transmitted at 10Hz. This is the base setting for all vehicles in the simulation. Some other communication load parameter values are also evaluated through the course of this project. In some scenarios, these messages are also retransmitted by the intersection RSU to help them reach around the corner.
- **Emergency Messages**. In each simulation test scenario, some vehicles or the intersection RSU are configured to transmit high priority emergency messages.
- **Commercial RSU Messages**. These four commercial RSUs are configured to periodically transmit beacon messages into the control channel advertising their services to all nearby vehicles.
- **Cascading Emergency Messages**. This is a pattern of emergency messages among some selected vehicles. This pattern is meant to emulate communication behaviors of intersection safety applications in a general manner. Please see the following section for more details.

All transmissions are sent at a power intended for a range of 200m, unless specifically reconfigured in some simulation test scenarios. All routine safety messages are 200 Bytes long. Emergency messages for both the RSU and vehicles on the intersection roads are 500 bytes long.

1.2 Cascading Emergency Message Protocol Design

As described in the above section, most of the communications in each simulation test scenarios are messages on their own, whether they are routine safety messages or emergency ones. They would also be evaluated on their own, which means each message is examined to see how well it individually is received by nearby receivers. Although these results would provide understanding regarding how effective DSRC broadcast communications would be in certain settings, they do not show how well a particular safety application would fare.

A cascading emergency message pattern is designed to emulate the behaviors of some safety applications in a more direct manner in order to gain better insight of the safety applications' performance from the communication angle.

There are many ways for an emergency to happen at an intersection. A car could run the red light or some aggressive lane change maneuvers could cause a close call. Assuming such a situation is detected, either by a vehicle or the infrastructure, and made aware to a car approaching the intersection in some manner, it could trigger cascading events and associated communications through the traffic. For example, the lead vehicle may have to brake hard, causing the next car in the lane to brake as well, and so on and so forth.

Cascading messages of this type have a dependency among them. The following rule defines one such class of cascading events and communications.

For all vehicles in an affected lane and for each cascading flow, each car immediately starts its turn of transmitting high priority emergency messages if and only if it receives one such message from the car immediately ahead.

The team designed and implemented two cascading protocols to model these emergency message patterns in simulation test scenarios. They are described in detail in the following subsections.

1.2.1 Repetition based Cascading Protocol

The simplest method is the tried-and-true repetition technique. Each vehicle, at its turn of transmission, repeats its message N times. The N parameter needs to be set sufficiently high to ensure successful propagation of the event and emergency messages through the traffic, yet low enough to prevent vicious competition among these vehicles for the channel access. The figures below show the pseudo-code and SDL diagram of this protocol.

```
Repetition based Cascading Protocol:
VSCAgent:
when a packet is received
if packet is emergency message {

              if the sender is from the car in front
              {
                     if it is a new emergency message
                     {
record the message ID
(stop the old retransmission if it is still active)
                            start retransmitting, for N times
                     }
              }
if the sender is from the car behind it
{
       do nothing
}

}
```

Figure 1-2: Pseudo Code of Repetition-Based Cascading Protocol

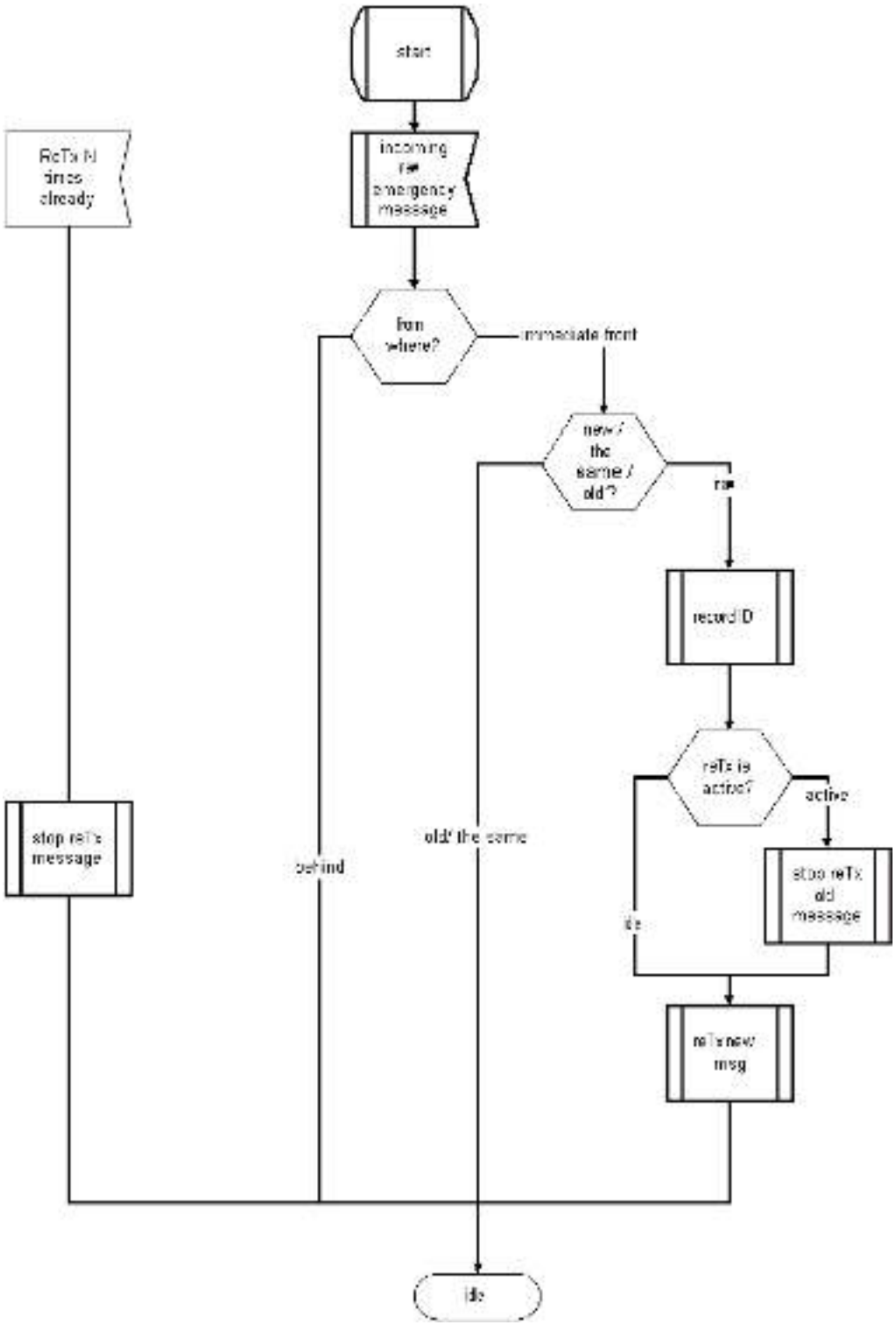


Figure 1-3: SDL Diagram of Repetition-Based Cascading Protocol

1.2.2 Feedback-Based Cascading Protocol

The repetition-based cascading protocol, although simple, is neither efficient nor reliable in ensuring message propagation. Therefore another feedback-based protocol is designed by adding one more rule.

> *Each vehicle, while at its turn of transmission, repeats until it receives one such message from any vehicle behind*[1]*. At this point it stops transmission.*

This protocol is designed so a vehicle would transmit enough times to ensure message propagation, but no more. The figures below show the pseudo-code and SDL diagram of this protocol.

```
Feedback based Cascading Protocol:
VSCAgent:
when a packet is received
if packet is emergency message {

              if the sender is from the car in front of it
              {
                     if it is a new emergency message
                     {
record the message ID
(stop the old retransmission if it is still active)
                            start retransmitting
                     }
              }
if the sender is from the cars behind it
{

       if the message ID is the same as current ID,
              stop retransmitting

}

}
```

Figure 1-4: Pseudo Code of Feedback-Based Cascading Protocol

[1] Assuming all vehicles involved would transmit emergency messages containing the same cascading event id, then a car could, upon reception of an emergency message containing the same id from behind, infer that its own transmission has been properly cascaded through.

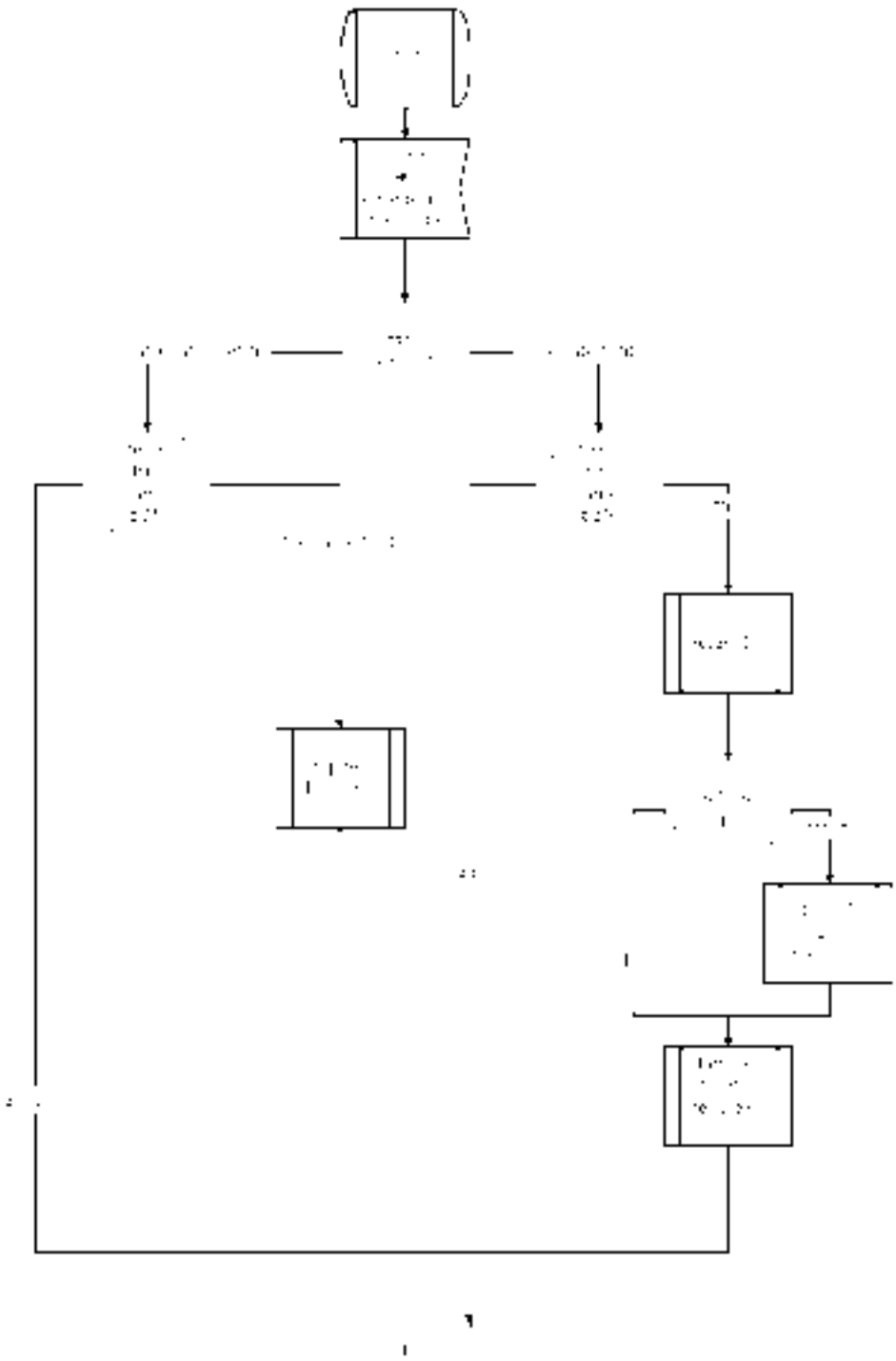


Figure 1-5: SDL Diagram of Feedback-Based Cascading Protocol

2 Simulator Update

The DSRC simulator underwent significant changes in order to configure and run intersection-based simulation test cases. These areas of change are indicated in the simulator architecture figure below. Major updates are described further in the following sections.

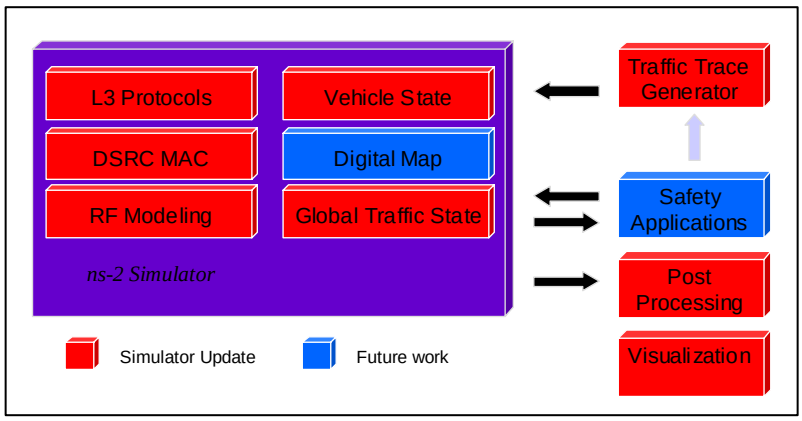


Figure 2-1: DSRC Simulator Architecture

2.1 Traffic Trace Generator

Mobile (cars, OBU) and fixed (roadside units, RSU) nodes were distributed in an intersection environment (Figure 2) that also included a nearby highway. This scenario was generated in response to a Department of Transportation request for simulation testing in a highly congested intersection environment. A new traffic generator was developed to create a specific traffic input file for this scenario.

Since the scenario involved road segments with different traffic patterns, the traffic generator had to incorporate a method of defining and controlling traffic flow based on road segment and travel direction. It also had to contain road shapes, lengths, widths, relative positions, allowable speed ranges, and the presence or absence of buildings.

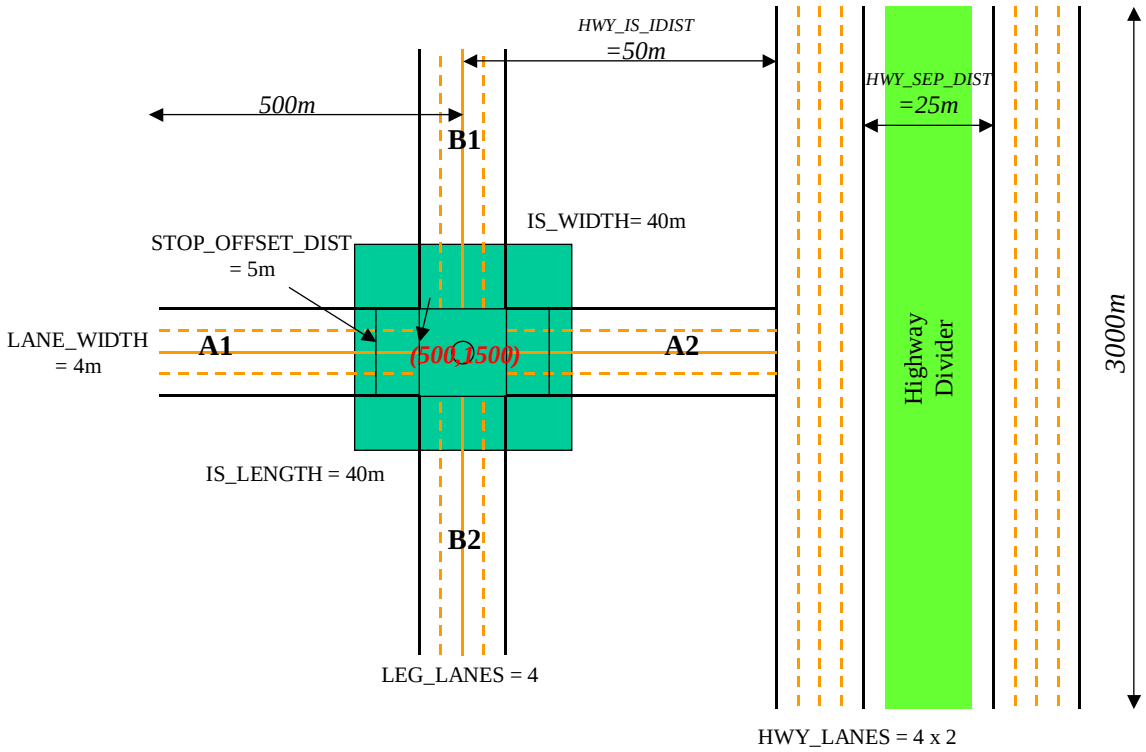


Figure 2-2: General Intersection Scenario

The traffic generator divides the scenario into several components (Figure 3):

1. Divided highway
2. Intersecting roads A and B and their sub-segments (A1, A2, B1, and B2)
3. Intersection (shown in teal in Figure 2)
4. Commercial RSU locations (shown in royal blue in Figure 3)

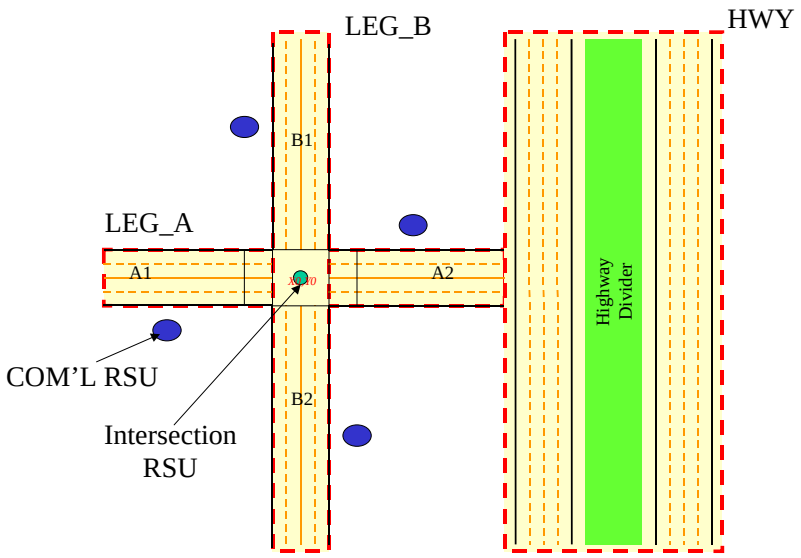


Figure 2-3: Components of Intersection Scenario

The traffic generator can create a traffic input file for each of the components or a combination of selected components. While unrealistic, in order to create the best chance for a high density of communications, all roadways including road segment A2 and the highway are at the same elevation. As such, communications on the intersecting roads A and B may be received on the highway and vice versa, but vehicles from the highway do not intersect nor commingle with vehicles on A or B.

The highway is composed of four lanes in each direction. The vehicles (or nodes) on each lane have fixed speeds that vary (between 60 and 120 km/h) by lane assignment and the vehicle density is fixed at 80 cars per lane mile. A representative node distribution is shown in Figure 4. The number of nodes and the length of each lane are calculated so that a consistent number of nodes remain within the borders of the simulation area.

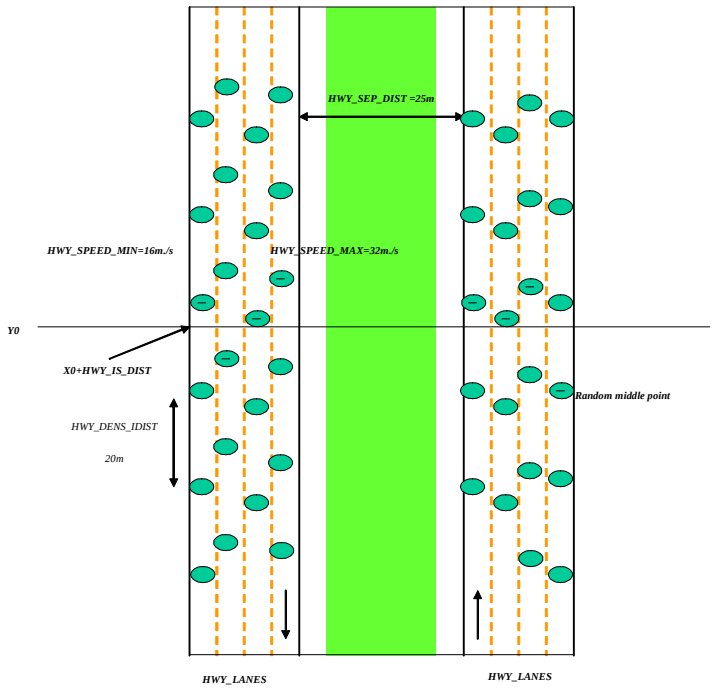


Figure 2-4: Node Distribution and Movement on Highway

Nodes are distributed on the intersecting roads as shown in Figure 5. As depicted, road B traffic has a green light at the intersection and road A has a red light.

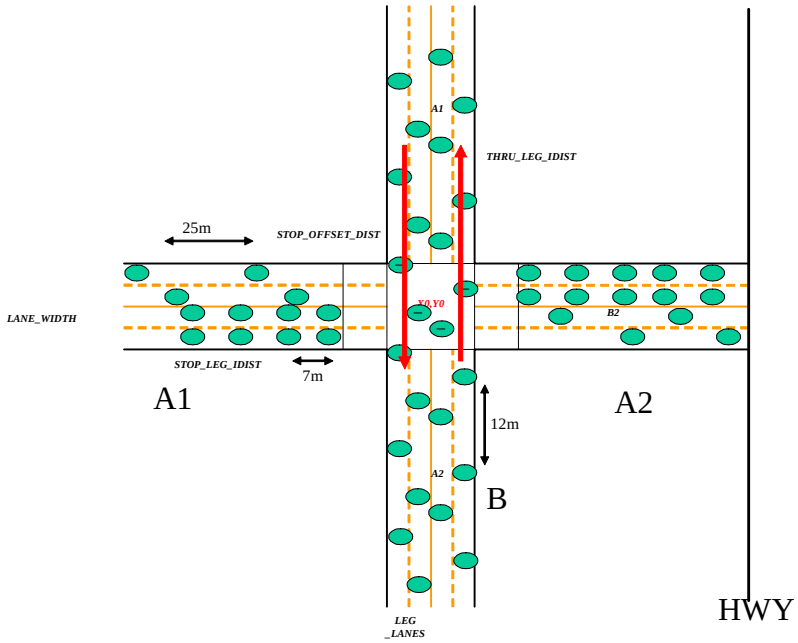


Figure 2-5: Node Distribution on Intersection Legs

Road A nodes approaching the intersection are stopped at the red light and are tightly spaced at 230 cars per lane mile (7m between nodes), which is significantly higher than the road B node density of 134 cars per lane mile (12m between nodes). Road A nodes traveling away from the intersection are spaced at 64 cars per lane mile (25m between nodes). The nodes on road B move similarly to nodes on the highway, but at lower speeds. The minimal speed is ~29 km/h and maximum is ~58 km/h.

Adding all vehicle on-board unit (OBU) nodes and the few RSU nodes in the simulation environment yields roughly 1900 separate communication nodes.

2.2 Vehicle State and L3 Protocols

2.2.1 Vehicle Node IDs

Each node is assigned an ID. These are used to differentiate between nodes in different road segments. The first digit of the ID indicates the node's road segment.

Scenario component	ID range	Prefix	Node type
Highway	1-999	0	1
Road A	1001-1999	1	2
Road B	2001-2999	2	2
Intersection RSU	0		3
Commercial RSU	3001-3999	3	4

Table 2.1. Node ID prefixes

2.2.2 Node Behavior Customization

Previous versions of the simulator had only limited support for customizing a node's behavior. Every node was identical in the protocol stack and protocol parameters. The only difference is their location and priority level. However, task 12 requires much more control on each node. Based on location, there are four types of nodes: Highway, Intersecting Road, Intersection RSU, and Commercial RSU. Each type of node is expected to have unique VSC application settings. Furthermore, each node has unique event-driven communications. Therefore, the nodes need to be customized, as delineated below.

2.2.2.1 Methods of Node Customization

With the nodes' IDs, it is possible to customize the node in two ways:

A. Define several vehicle types. Each type has certain protocol settings and routine communication patterns. Each node is assigned a vehicle type in the scenario input file. The node is configured while the scenario input file as being parsed.

B. Use a plug-in script in which all transmit events of each node are defined. Solution A groups the nodes' behavior. It has the advantage that when the scenario requires changing the behavior of one vehicle type, it only needs to be changed in the definition for that vehicle type. All nodes belonging to that vehicle type will be configured accordingly when the scenario file is parsed.

Solution B makes each node unique. It allows each node's behavior to be totally different than the others. So unique event-driven messages are possible with this solution.

2.2.2.2 Implementation of Node Configuration

A combination of the above two solutions was implemented. Vehicle type is defined in an initial script. Each node is configured according to its vehicle type and routine transmissions are defined. After the configuration, a communication file for event-driven transmissions of each node is loaded.

	Type	Routine transmit	Set-interval	Set-priority	Size
Nodes on HWY	0	ON_ASYN	0.1	1	500
Nodes in intersection	1	ON_ASYN	0.1	1	200
Intersection RSU	2	ON_ASYN/OFF	0.1	1	500
Commercial RSU	3	ON_ASYN/OFF	1.0	0	500

Table 2.2. Example Initial Script Node Configuration

Event driven communication

A TCL script (communication file) is used to describe all event-driven communications. The simulator loads this script.

Command syntax:

$ns at *time* "*agent_name* send"

Example Scripts:

```
$ns at 1.6 "$agent_1 send"
$ns at 1.64 "$agent_29 send"
```

2.3 RF Modeling

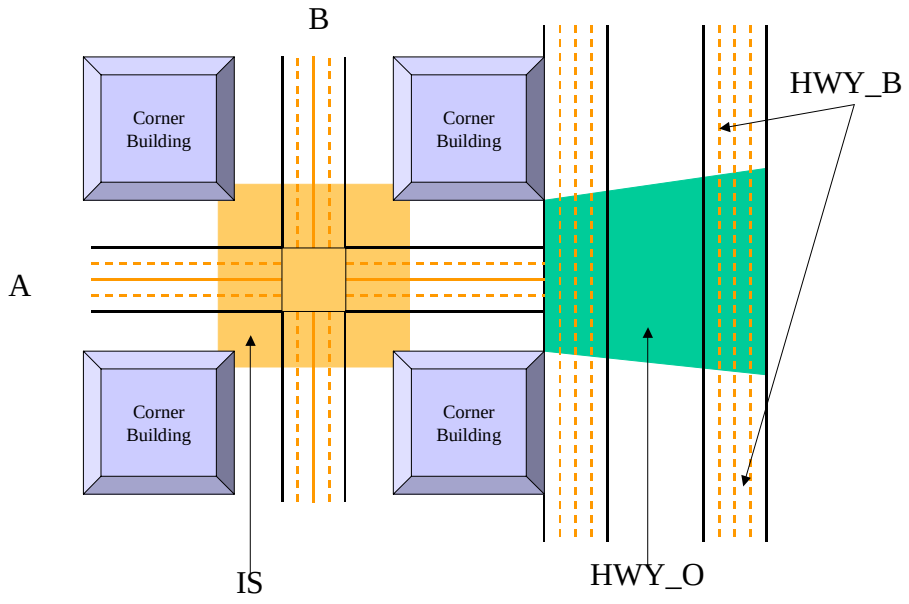


Figure 2-6: RF Model Regions

2.3.1 Motivation

Because of the complexity of the urban environment with buildings, the computation of reception power not only depends on the mutual distance between the sender and receiver, but also on the radio frequency (RF) characteristics in the space between them (e.g., multipath effects, obstructions). For simulation tests in the mixed urban/highway environment, multiple RF models are required. A decision function was implemented in the simulated DSRC physical (PHY) layer to choose the proper model for computation. In the scenarios without buildings, a single RF model was used for all communications in all regions for the intersection and highway environments.

2.3.2 RF Model Selection

There are two methods of deciding which model to choose when buildings are present in the simulation environment.

A. Query a Map. If there is a common map available for all nodes, the PHY layer can query the map, which checks the sender and receiver's location and uses the appropriate model.

B. Use the location information in the node ID. By checking the sender's ID, the simulator knows whether a receiver and sender are in the same region. This information is used to make the decision on which RF model to use.

The common map solution is a complete solution. A map can tell precisely what is in-between the sender and receiver and determine the real radio path. However, such a solution is very complex and requires a great deal of computation. In addition, this is general purpose research, so it is not meaningful to use a very specific map. The second solution is only a partial solution; with only this information, it is hard to choose the correct model precisely.

So the final implementation is a hybrid solution: the ID determines whether the sender and receiver are on the same road. Two special regions are also defined: IS (intersection) and HWY_O (highway open). The IS region represents the real intersection area, in which there are no buildings. HWY_O represents the region on the highway where the nodes can influence communications at the intersection.

Further regions are denoted as intersecting roads A and B, and HWY_B (highway blocked), which does not have a clear line of sight (LOS) to the intersection when buildings are present. Note that commercial RSUs are contained within roads A or B and, as such, do not constitute a region.

2.3.3 RF Model Development

Since a highway RF model had already been developed for task 6A, most efforts were focused on creating an RF model for the newly defined urban environment. This was done by finding a real-world intersection similar to the one defined in the simulator and collecting extensive empirical RF measurements. The intersection used for data collection is pictured below and is indicated by the blue dot. Many tests were conducted at and around this intersection in order to collect statistically significant amounts of data at appropriate ranges. The primary range of interest is 200m and below. This was selected since it generally included most intersection safety applications envisioned in the VSC Task 3 report.

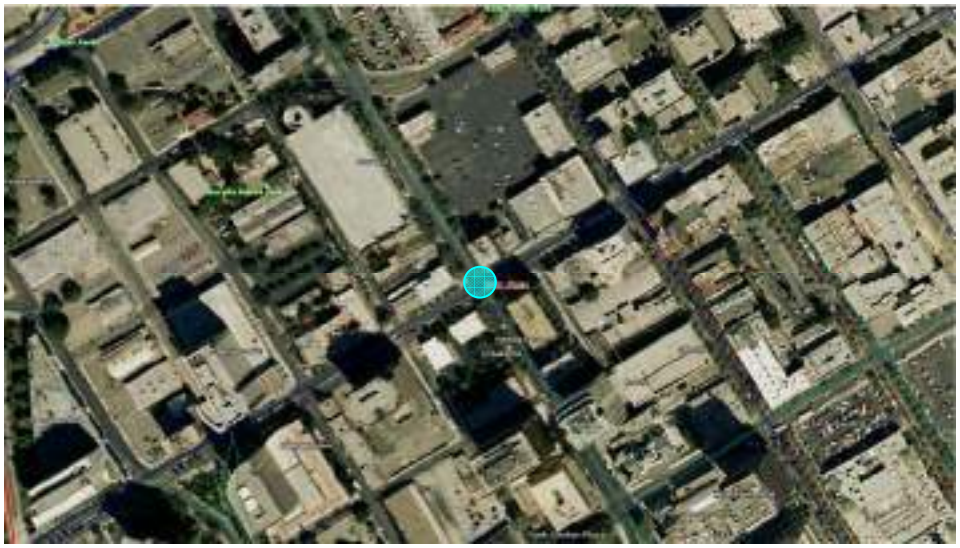


Figure 2-7: City Intersection RF Model Data Collection Site

Data was collected using multiple test vehicles, a single intersection RSU test stand, DSRC communications test kits (CTK) as developed in Tasks 4 and 6A, and DSRC-tuned antennas developed in Task 6C. New WAVE radio modules (WRM) from Task 6D were not yet available at the time of data collection.

Based on the data collected at this intersection and previously on the highway, three different types of RF models were derived[2]:

Highway: Model for highway and for all roads when no buildings are present
City: Model for nodes within LOS on city roads with buildings present
Blocked: Model for nodes with buildings blocking the LOS path

[2] It is important to note that RF modeling for intersections is an enormously complex task. There are many factors that impact the RF behaviors, including intersection landscape, street geometry, corner building shape, position, material, etc. Due to the resource and timing restrictions, the models implemented in this task are derived from measurements obtained at one particular urban intersection. These are not meant to generalize all intersections. On the other hand, this intersection was selected carefully to match the one agreed within VSCC and with DOT for the simulation scenarios. Accordingly, the RF models are meaningful for this simulation study.

These three models were implemented in the simulator and applied to reception power calculations based on the following decision table.

Node location	A	B	IS	HWY_O	HWY_B
A	City	Blocked	City	City	Blocked
B	-	City	City	Blocked	Blocked[3]
IS	-	-	City	City	Blocked
HWY-O	-	-	-	Highway	Highway
HWY-B	-	-	-	-	Highway

Figure 2-8: RF Model Selection Decision Table

2.3.4 RF Model Implementation

By analyzing the data collected from road tests, empirical Nakagami parameters were derived for each RF model. Each model has a different set of Nakagami parameters, which give the models their characteristic traits and accurately portrays performance based on statistical analysis of applicable RF data collection.

Additionally, two variants of each model were used in the simulations. For each distance measured between test vehicles, many transmitted packets were collected, but received signal strength that always varied significantly. For simplicity, 80 percent of the most likely reception signal strengths at each distance were used to develop a distributed RF model. The blue upper and lower boundary lines in the following charts represent this distributed range of most likely signal strengths. The deterministic model further simplifies this distribution by representing the average value (in red) over the distributed range of signal strengths. Details of each model are listed below together with simulation results showing the reception probability with no interference.

It is interesting to observe that signal attenuation within one urban canyon is less severe than on highways. The reason is that buildings on both side of the street are able to contain and channel the signal through multi-path effects, which is less available on the open highways. The implication is that, for the same transmission power and assuming same interference level, the reception of a packet is likely better than that on a highway. Of course, reception around a corner in an urban setting is much less than within the same street, as expected.

[3] Please note that transmission between B and HWY_B is a special case. The sender and the receiver are placed on opposite sides of a building block. Assuming no RF signal penetration through the building, the signal attenuation is calculated according to two, around-corner propagations using the blocked model. There is a further 15 dB signal loss to account for additional reflections.

2.3.4.1 Highway RF Model

Nakagami Parameters	Highway Model Values
gamma0	1.9
gamma1	3.8
d0_gamma	200
d1_gamma	600
m0	1.5
m1	0.75
m2	0.75
d0_m	80

Figure 2-9: Highway RF Model Nakagami Parameters

The above table shows the Nakagami parameters for the highway RF model, while the figure below shows the signal attenuation over distance for this model.

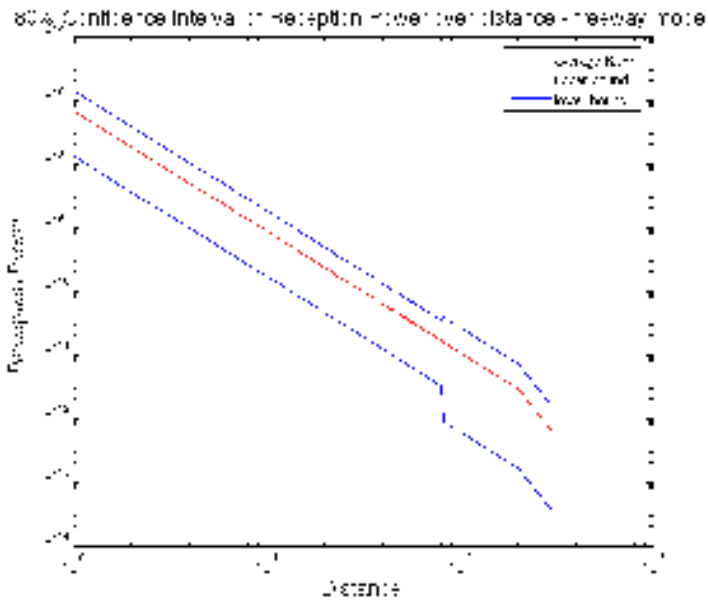


Figure 2-10: Signal Attenuation Over Distance, Highway RF Model

2.3.4.1.1 Ideal Performance With Highway RF Model

The following simulation result shows the impact by the highway RF model on message reception in an ideal (interference free) environment.

Sender location	Middle of the freeway
Receiver location	All nodes on freeway
Communication Activities	Single sender sends message periodically with no interference
Transmission Range	200m

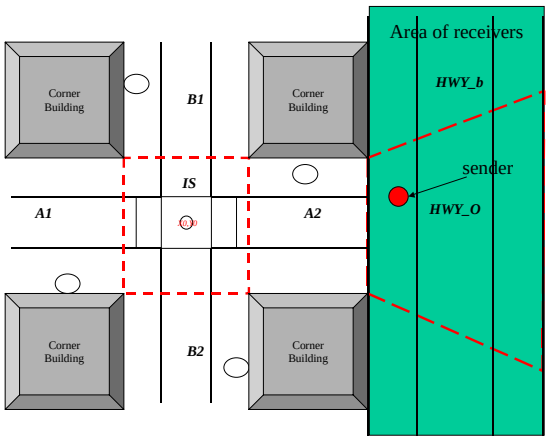


Figure 2-11: Simulation Setting, Single Sender on Freeway, Highway RF Model

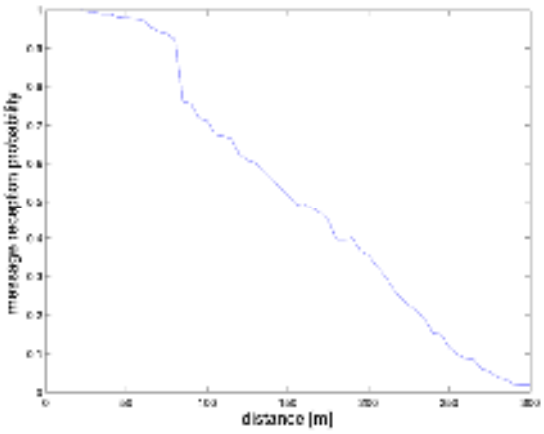


Figure 2-12: Reception Probability on Freeway, Single Sender on Freeway, Highway RF model

2.3.4.2 City RF Model

Nakagami Parameters	City Model Values
gamma0	1.5
gamma1	4
d0_gamma	125
m0	0.75
m1	0.5
d0_m	125

Figure 2-13: City RF Model Nakagami Parameters

The above table shows the Nakagami parameters for the city RF model, while the figure below shows the signal attenuation over distance for this model.

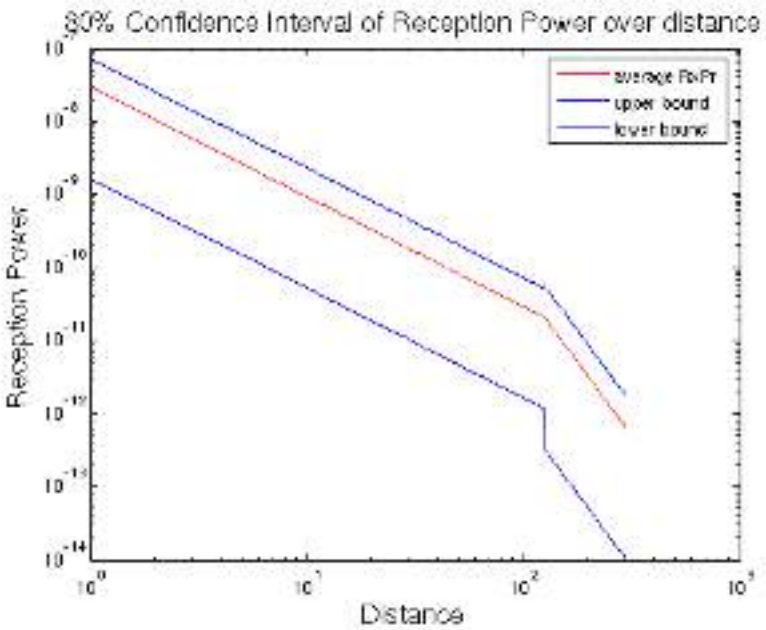


Figure 2-14: Signal Attenuation over Distance, City RF Model

2.3.4.2.1 Ideal Performance with City RF model

The following simulation result shows the impact by the city RF model on message reception in an ideal (interference free) environment.

Sender location	Middle of the intersection
Receiver location	Road B (the through road)
Communication Activities	Single sender sends message periodically with no interference
Transmission Range	200m

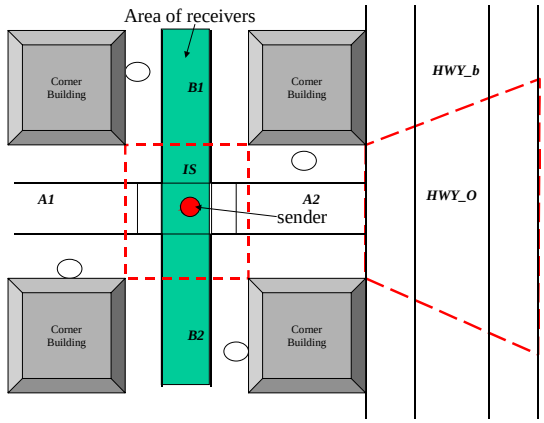


Figure 2-15: Simulation Setting, Single Sender in Intersection, City RF Model

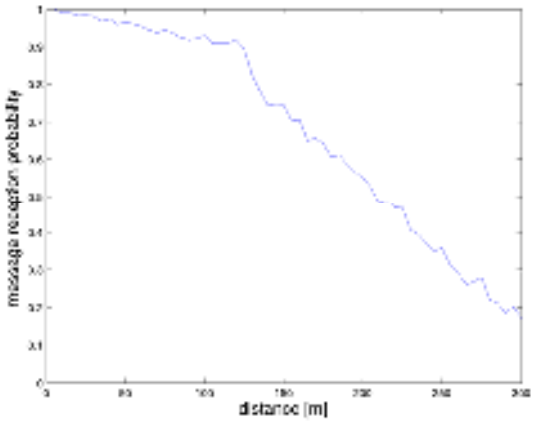


Figure 2-16: Reception Probability within Urban Canyon, Single Sender in Intersection, City RF Model

2.3.4.3 Blocked RF Model

Nakagami Parameters	Blocked Model Values
Gamma0	2
Gamma1	10
d0_gamma	125
m0	0.5
m1	0. 5
d0_m	125

Figure 2-17: Blocked RF Model Nakagami Parameters

The above table shows the Nakagami parameters for the blocked RF model, while the figure below shows the signal attenuation over distance for this model.

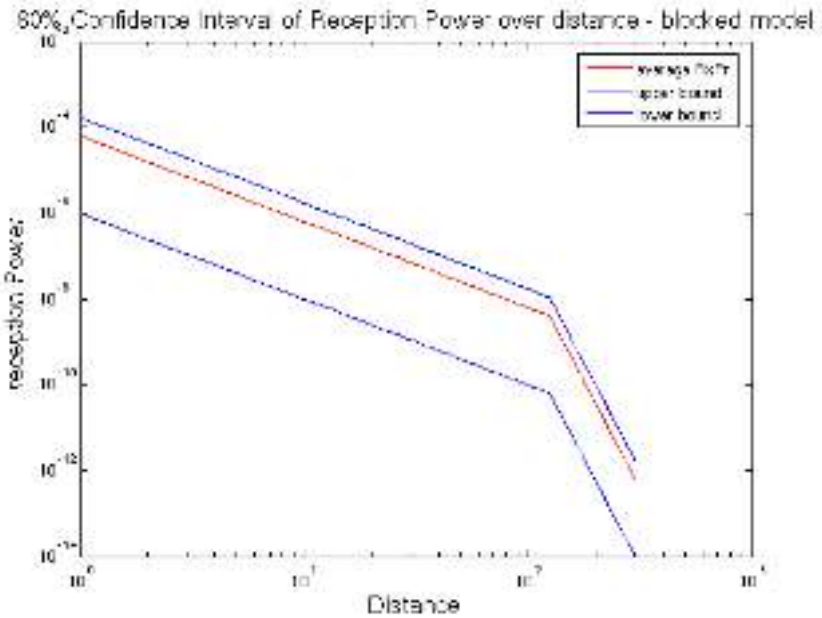


Figure 2-18: Signal Attenuation over Distance, Blocked RF Model

2.3.4.3.1 Ideal Performance with Blocked RF model

The following simulation results show the impact by the blocked RF model on message reception in an ideal (interference free) environment.

Sender location	A node on Road A close to the intersection
Receiver location	Road B (outside of the IS area)
Communication Activities	Single sender sends message periodically with no interference
Transmission Range	200m

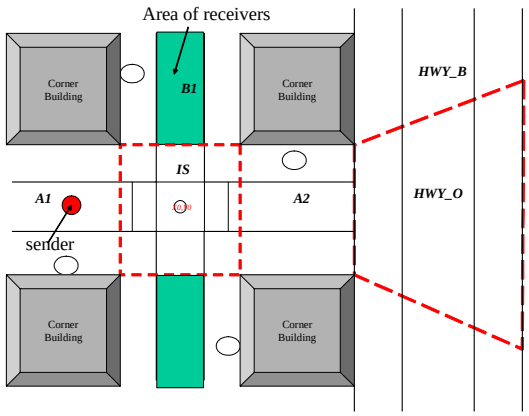


Figure 2-19: Simulation Setting, Single Sender Around Corner, Blocked RF Model

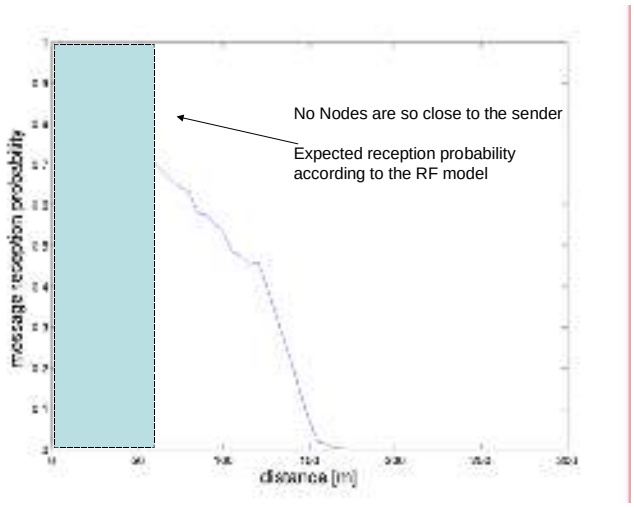


Figure 2-20: Reception Probability Around Corner, Single Sender, Blocked RF model

3 Simulation Test Matrix

The following sections describe the parameter settings for all simulation tests conducted for this task. Please refer to the later chapters for the full results of all the simulation tests.

3.1 Batch 1, Routine and Emergency Safety Messaging in Saturated Channel

As shown in the table below, this batch of simulation tests places the emphasis on stressing the channel. All OBUs are arranged to transmit routine safety messages at 10Hz with an intended range of 200m. Four commercial RSUs placed at roadside all inject messages into the channel as well in some of the scenarios.

Number.	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
	Deterministic or Distributed	Buildings in corners or not	RSU or OBU	200m or 300m	ON or OFF	1/2/5/10 Hz	200m or 100m	Repetition or feedback
1	Deterministic	Open	RSU	200m	ON	10Hz	200m	
2	Deterministic	Open	RSU	200m	OFF	10Hz	200m	
3	Deterministic	Building	RSU	200m	ON	10Hz	200m	
4	Deterministic	Building	RSU	200m	OFF	10Hz	200m	
5	Deterministic	Open	OBU	200m	ON	10Hz	200m	
6	Deterministic	Open	OBU	200m	OFF	10Hz	200m	
7	Deterministic	Building	OBU	200m	ON	10Hz	200m	
8	Deterministic	Building	OBU	200m	OFF	10Hz	200m	
9	Distributed	Open	RSU	200m	ON	10Hz	200m	
10	Distributed	Open	RSU	200m	OFF	10Hz	200m	
11	Distributed	Building	RSU	200m	ON	10Hz	200m	
12	Distributed	Building	RSU	200m	OFF	10Hz	200m	
13	Distributed	Open	OBU	200m	ON	10Hz	200m	
14	Distributed	Open	OBU	200m	OFF	10Hz	200m	
15	Distributed	Building	OBU	200m	ON	10Hz	200m	
16	Distributed	Building	OBU	200m	OFF	10Hz	200m	

3.2 Batch 2, Routine and Emergency Safety Messaging in Less Stressful Channel

This second batch of simulation tests is configured in reaction to the results from the first batch. Given the large number of vehicles present around intersections and on the freeway, it is clear that transmitting routine safety messages from all of them at 10Hz creates a saturated channel. Routine safety messages have collapsed performances across the board. Therefore, it is necessary to adjust the channel load and re-evaluate the routine safety message performance. Instead of reducing the vehicle density, which is set at a

level quite plausible in reality, the team decided to reduce the routine message transmission frequency since it is a communication design option.

Number.	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
	Deterministic or Distributed	Buildings in corners or not	RSU or OBU	200m or 300m	ON or OFF	1/2/5/10 Hz	200m or 100m	Repetition or feedback
17	Distributed	Open	RSU	200m	ON	2Hz	200m	
18	Distributed	Open	OBU	200m	ON	2Hz	200m	
19	Distributed	Building	RSU	200m	ON	2Hz	200m	
20	Distributed	Building	OBU	200m	ON	2Hz	200m	
21	Distributed	Open	RSU	300m	ON	2Hz	200m	
22	Distributed	Open	OBU	300m	ON	2Hz	200m	
23	Distributed	Building	RSU	300m	ON	2Hz	200m	
24	Distributed	Building	OBU	300m	ON	2Hz	200m	
25	Distributed	Open	RSU	200m	ON	1Hz	200m	
26	Distributed	Open	OBU	200m	ON	1Hz	200m	
27	Distributed	Building	RSU	200m	ON	1Hz	200m	
28	Distributed	Building	OBU	200m	ON	1Hz	200m	
29	Distributed	Open	RSU	300m	ON	1Hz	200m	
30	Distributed	Open	OBU	300m	ON	1Hz	200m	
31	Distributed	Building	RSU	300m	ON	1Hz	200m	
32	Distributed	Building	OBU	300m	ON	1Hz	200m	
33	Distributed	Open	RSU	200m	ON	5Hz	200m	
34	Distributed	Open	OBU	200m	ON	5Hz	200m	
35	Distributed	Building	RSU	200m	ON	5Hz	200m	
36	Distributed	Building	OBU	200m	ON	5Hz	200m	
37	Distributed	Open	RSU	300m	ON	5Hz	200m	
38	Distributed	Open	OBU	300m	ON	5Hz	200m	
39	Distributed	Building	RSU	300m	ON	5Hz	200m	
40	Distributed	Building	OBU	300m	ON	5Hz	200m	

After analyzing the results of the aforementioned tests, the presence of commercial RSU messages on the channel has evidently no effect whatsoever. This is expected since their communication load pales in comparison with the number of other vehicles and their transmissions. Accordingly, this parameter is no longer varied in this batch.

3.3 Batch 3, Intersection RSU Retransmission of Routine Safety Messages

Given the challenge caused by the RF model for messaging performance around the corner, there is interest from the vehicle safety community to use intersection RSU retransmission techniques to improve the situation. This batch of simulation tests is designed to evaluate this concept.

Two levels of channel load are evaluated. One is saturated, with all vehicles transmitting routine safety messages at 10Hz. Another is more moderate at 2Hz since the earlier results showed comparatively better overall communication performance at this stress level.

Number.	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
	Deterministic or Distributed	Buildings in corners or not	RSU or OBU	200m or 300m	ON or OFF	1/2/5/10 Hz	200m or 100m	Repetition or feedback
41	Distributed	Building	NA	200m	ON	2Hz	200m	
42	Distributed	Building	NA	200m	ON	10Hz	200m	

3.4 Batch 4, Cascading Emergency Messages from Intersection

This batch of simulation tests evaluates the performance of emergency message cascading within one lane from the intersection. The cascading emergency message pattern is used to emulate intersection safety application communication behaviours as a dangerous situation is discovered at the intersection.

Two emergency message cascading protocols are evaluated. One uses the tried-and-true repetition method. The other uses a more intelligent feedback based method, which means a car will stop repeating emergency messages if it detects subsequent transmissions by its intended audience behind.

Number.	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
	Deterministic or Distributed	Buildings in corners or not	RSU or OBU	200m or 300m	ON or OFF	1/2/5/10 Hz	200m or 100m	Repetition or feedback
43	Distributed	Building	OBU Cascading in one lane	200m	ON	5Hz	200m	Repetition
44	Distributed	Building		200m	ON	5Hz	200m	Smart protocol2
45	Distributed	Building		200m	ON	10Hz	200m	Repetition
46	Distributed	Building		200m	ON	10Hz	200m	Smart protocol2

3.5 Batch 5, Additional Simulation Tests

This batch of simulation tests contains additional configurations as requested by other VSCC members.

Number.	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
	Deterministic or Distributed	Buildings in corners or not	RSU or OBU	200m or 300m	ON or OFF	1/2/5/10 Hz	200m or 100m	Repetition or feedback
47	Distributed	Open	RSU	200m	ON	NA	NA	
48	Distributed	Building	RSU	200m	ON	NA	NA	
49	Deterministic	Open	RSU	200m	ON	10Hz	100m	
50	Deterministic	Building	RSU	200m	ON	10Hz	100m	

4 Analysis

In this section, the team analyzes the simulation results and makes observations of the implications for both the underlining communication design as well as its usage by safety applications.

4.1 Routine Safety Messages at Intersection

This task was initiated with the desire to find out how well DSRC would work in a high volume intersection with plenty of external interference sources. It is not unexpected that impact from a highly loaded channel on the routine safety messages among vehicles is severe.

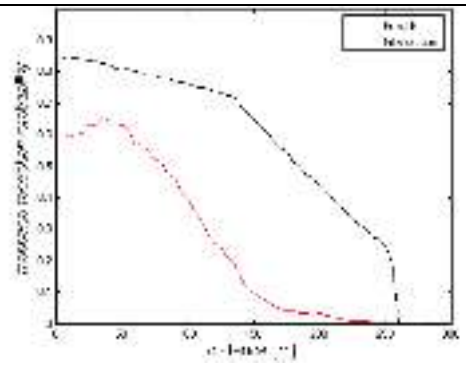


Figure 4-1: Reception Probability of Routine Messages, Sender on Road B, scenario 3

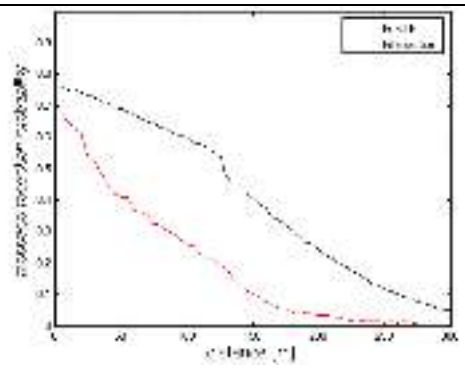


Figure 4-2: Reception Probability of Routine Messages, Sender on Road B, Scenario 11

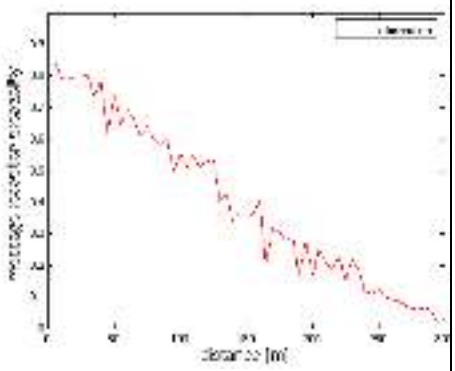
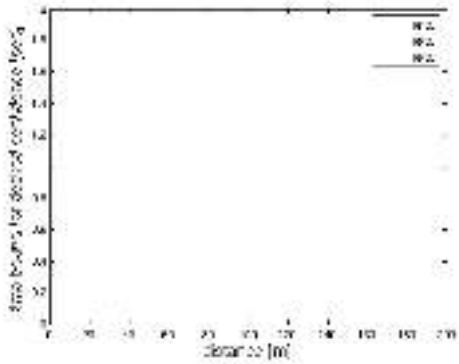
The first batch of simulation tests is designed to stress the channel to the limit. All vehicle OBUs, which numbers about 2000, are configured to transmit a 200 Byte message at 10 Hz to the intended range of 200 Meter. The results demonstrate a collapsed channel weighted down by these routine safety messages for receivers at the intersection as shown by the red lines in the figures above for scenario 3 and 11.

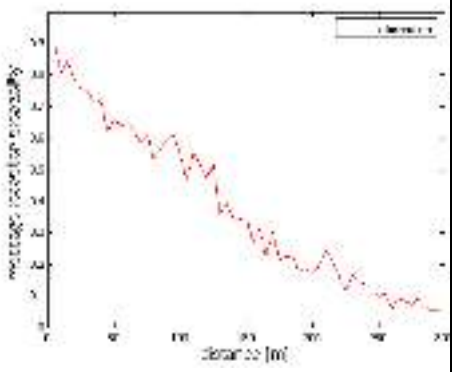
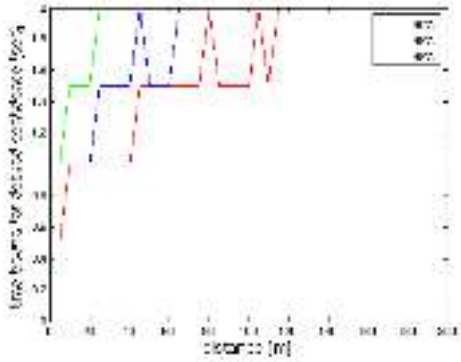
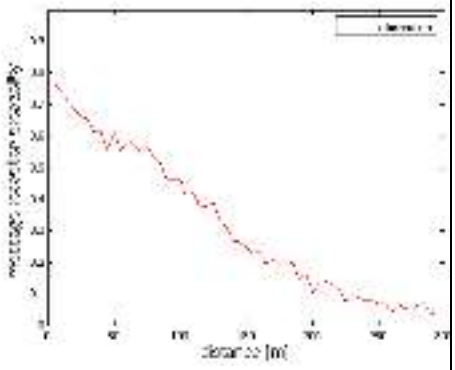
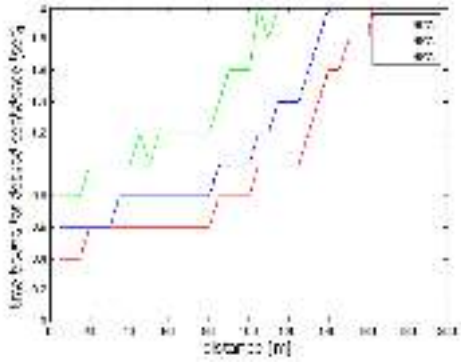
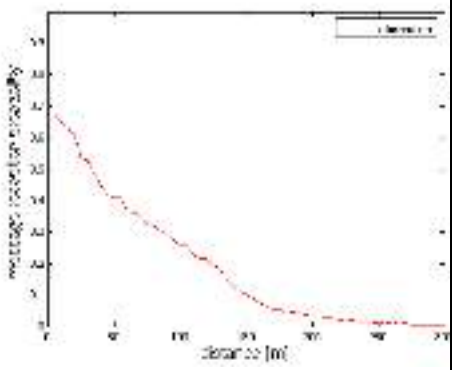
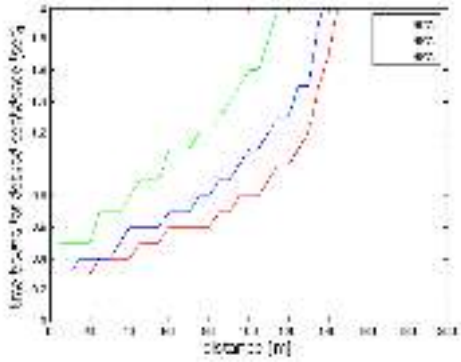
The only difference between these two scenarios is the usage of the RF model. Scenario 3 uses the RF model deterministically while scenario 11 uses it in a distributed manner. Using the RF model in a distributed manner causes further degradation of the messaging performance[4]. However, the dominating outcome is the saturated channel and the collapsed messaging performance for all routine safety messages at the intersection. This

[4] Using the RF model deterministically is equivalent to drawing circles around a sender. A receiver is either able to receive (or be interfered by) the message or not simply by its position in or outside of the circles. This view is simplistic and clean, but not realistic. Using the RF model in a distributed manner means there is an average for the received signal strength at a particular distance, but the actual value for each instance of transmission is the result of a distribution function. This is **Messages** more realistic but also implies less communication performance in comparable settings for two reasons. First, even within the so-called reception range, some messages still would not be receivable by some nodes due to the possible lower than receivable signal strength value. Second, more nodes are possible interferers.

is true for all other simulation tests in the first batch. Please check the figures presented in the later chapters for scenario 1-4 and 9-12 for further details.

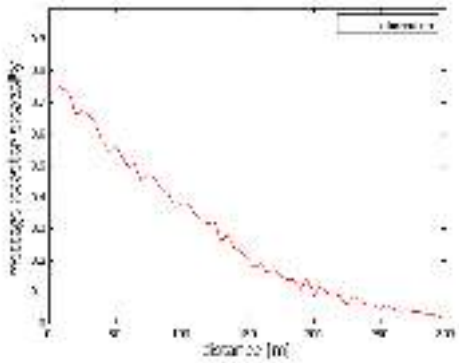
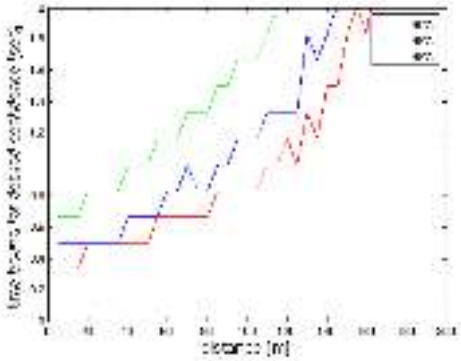
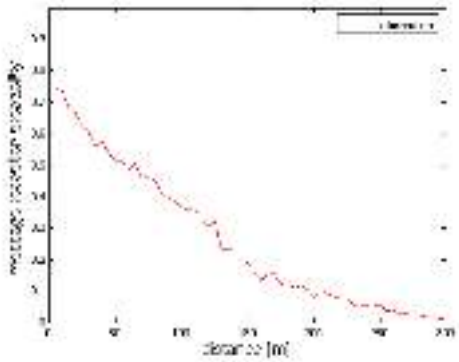
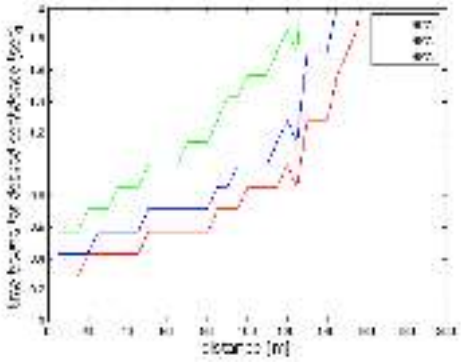
The results in the first batch of simulation tests clearly indicate a general saturation of the channel. Accordingly, the second batch is configured to reduce the overall channel loading. The results show improvements in message reception probability. However, it is important to note that it takes more than just a reception probability over distance figure for one to understand the implication of such communication performance for safety applications. For example, it could be better for a safety application to transmit five messages each at 50 percent reception probability than to deliver one message reliably in the same time frame. The following figures show both the routine message reception rate at the intersection as well as the time period necessary for a sender to be confident to 90 percent, 95 percent and 99 percent that at least one message would be received for scenarios 27, 19, 35 and 11. These four scenarios are otherwise configured in the same way, but with communication load defined by routine safety message rate of 1Hz, 2Hz, 5Hz, and 10Hz respectively. Please see the later chapters for similar figures of some other scenarios.

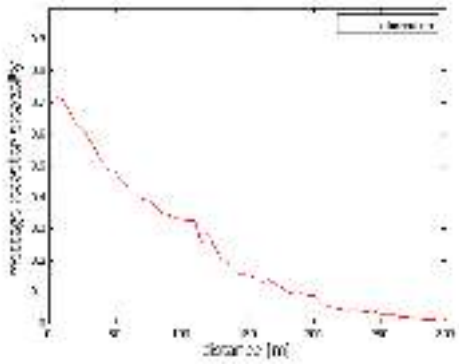
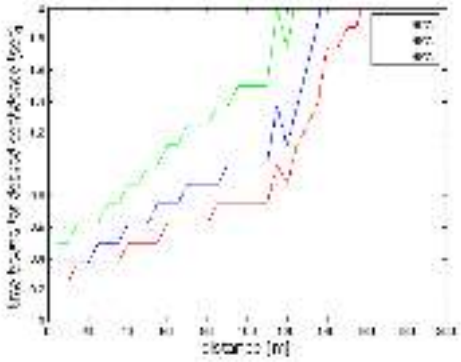
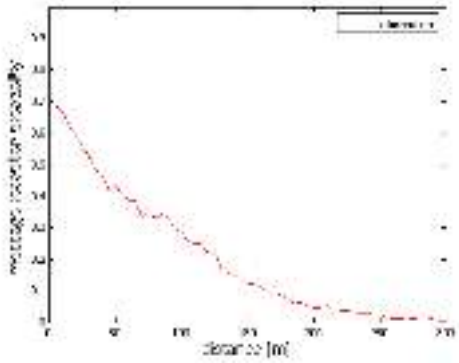
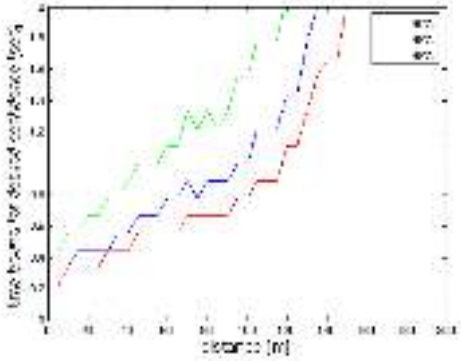
	Reception probability	Time Bound
1 Hz	 **Figure 4-3: Reception Probability of Routine at Intersection, scenario 27**	 **Figure 4-4: Time Bound for desired Confidence for Routine Messages Reception at Intersection, Scenario 27**

2 Hz	 **Figure 4-5: Reception Probability of Routine Messages at Intersection, Scenario 19**	 **Figure 4-6: Time Bound for Desired Confidence for Routine Messages Reception at Intersection, Scenario 19**
5 Hz	 **Figure 4-7: Reception Probability of Routine Messages at Intersection, Scenario 35**	 **Figure 4-8: Time Bound for Desired Confidence for Routine Messages Reception at Intersection, Scenario 35**
10 Hz	 **Figure 4-9: Reception Probability of Routine Messages at Intersection, Scenario 11**	 **Figure 4-10: Time Bound for Desired Confidence for Routine Messages Reception at Intersection, Scenario 11**

It is interesting to see that message reception latency at certain confidence level figures for scenario 11 and 35 are similar even though the later has only half of the routine

message transmission rate of the former. This is due to the improved message reception rate in the less stressful case. Additional simulation test runs are configured to further examine the implication of reduced routine message transmission rate. Please see Chapter 8 for further details.

	Reception probability	Time Bound
6 Hz	 **Figure 4-11: Reception Probability of Routine Messages at Intersection, Based on Scenario 11, Routine Message Adjusted to 6 Hz**	 **Figure 4-12: Time Bound for Desired Confidence for Routine Message Reception at Intersection, Based on Scenario 11, Routine Message Adjusted to 6 Hz**
7 Hz	 **Figure 4-13: Reception Probability of Routine Messages at Intersection, Based on Scenario 11, Routine Message Adjusted to 7 Hz**	 **Figure 4-14: Time Bound for Desired Confidence for Routine Message Reception at Intersection, Based on Scenario 11, Routine Message Adjusted to 7 Hz**

8 Hz	 **Figure 4-15: Reception Probability of Routine Messages at Intersection, Based on Scenario 11, Routine Message Adjusted to 8 Hz**	 **Figure 4-16: Time Bound for Desired Confidence for Routine Message Reception at Intersection, Based on scenario 11, Routine Message Adjusted to 8 Hz**
9 Hz	 **Figure 4-17: Reception Probability of Routine Messages at Intersection, Based on Scenario 11, Routine Message Adjusted to 9 Hz**	 **Figure 4-18: Time Bound for Desired Confidence for Routine Message Reception at Intersection, Based on Scenario 11, Routine Message Adjusted to 9 Hz**

The figures above show the results of additional simulation test runs based on scenario 11 but with routine message transmission rate set at 6Hz, 7Hz, 8Hz, and 9Hz. Although there is a shift in message reception rate according to the channel loading, message reception latency at certain confidence level figures do not seem to differ much.

Taken together, routine safety messaging reception is sensitive to the channel loading, but more careful evaluation is necessary before the implication for safety applications are understood. The routine safety message reception latency at certain confidence level analysis shows similar results for a range of channel load (i.e. from 6Hz to 10Hz). Accordingly, it may not be necessary for all cars to transmit routine messages at 10Hz to 200 meter in congested environments as called for in the preliminary communications requirements in the Task 3 document. In the context of simulation test scenarios discussed above, transmitting less may be just as effective as sending more frequently.

It is also important to point out that none of the above cases would be able to satisfy the preliminary communication requirements listed in Task 3. Task 3 asks for 100 ms communication latency without specifying distance. This is equivalent to drawing a

horizontal line at 100 ms line in all the figures above. The simulation environment is configured to represent a high-volume intersection environment with high external interference levels in a believable manner. Within this context, the simulation results show that it is not feasible to have everyone transmitting messages at 10 Hz to 200 meters as described in Task 3 and achieving perfect performance. The implication is that the DSRC community may have to reevaluate how safety applications use DSRC communications in highly congested environments as a follow up to Task 3 and provide updated guidance in judging the results obtained here.

4.2 Emergency Safety Message at Intersection

4.2.1 Emergency Message from Intersection RSU

In comparison with the routine safety messages, emergency messages consistently have better reception at any distance. The figures below show the reception rates of emergency messages from the intersection RSU for scenario 11, 35, 19, and 27. These four scenarios are the same as the last four analyzed in the previous section on routine safety message performance.

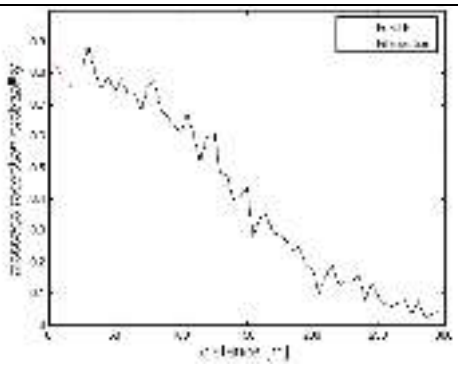


Figure 4-19: Reception Probability of Emergency Messages-Scenario 11, Road B, Sender RSU

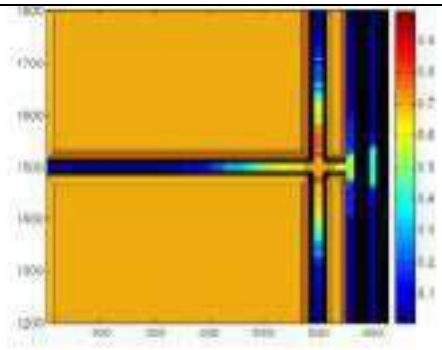


Figure 4-20: Reception Probability of Emergency Messages-Scenario 11, Sender RSU

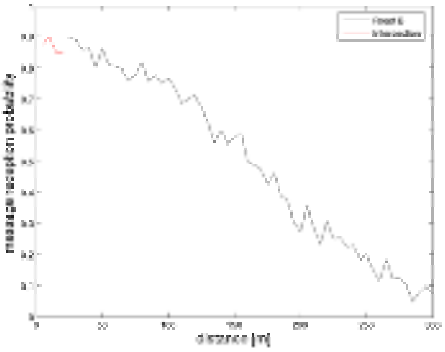


Figure 4-21: Reception Probability of Emergency Messages-Scenario 35, Road B, Sender RSU

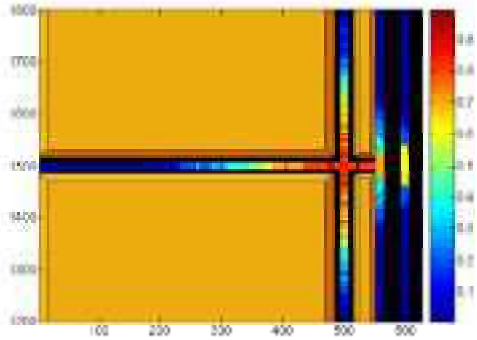


Figure 4-22: Reception Probability of Emergency Messages-Scenario 35, Sender RSU

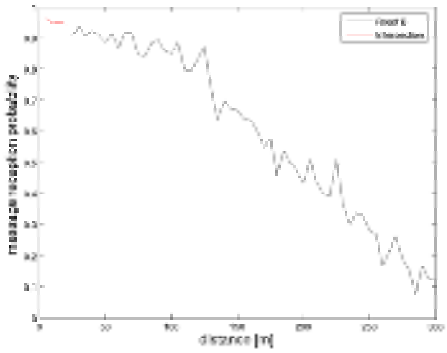


Figure 4-23: Reception Probability of Emergency Messages-Scenario19, Road B, Sender RSU

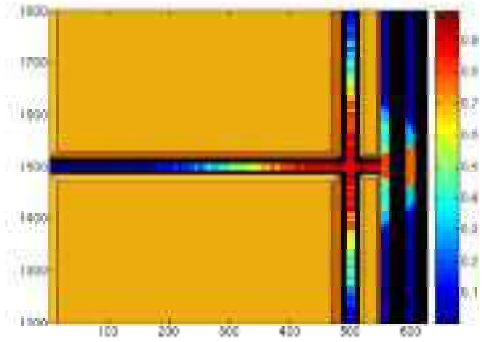


Figure 4-24: Reception Probability of Emergency Messages-Scenario19, Sender RSU

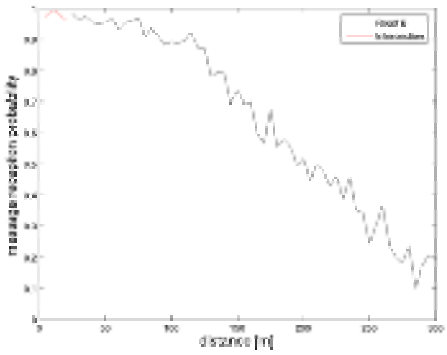


Figure 4-25: Reception Probability of Emergency Messages-Scenario 27, Road B, Sender RSU

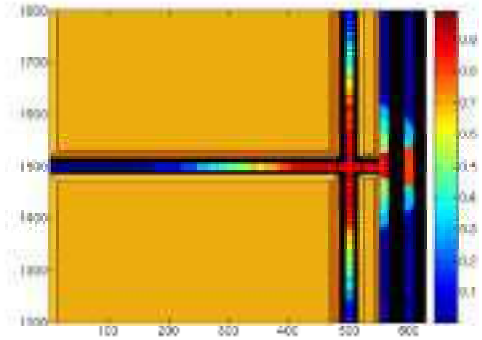


Figure 4-26: Reception Probability of Emergency Messages-Scenario 27, Sender RSU

With a less stressful channel, emergency messages from the intersection RSU perform even better. This is demonstrated in the figures above, which are the results for scenario 35, 19, and 27. As the routine safety message rate is reduced to 5Hz, 2Hz and 1Hz, the emergency message reception is quickly improved to almost matching the ideal performance permitted by the RF models. As a quick note, scenario 47 and 48 are configured with no routine safety messages. As expected, the emergency message reception in these two scenarios matches the upper bound set by the RF models.

4.2.2 Emergency Message from Vehicle OBUs

The performance of emergency messages from vehicle OBUs also follows the same pattern as the ones for RSU messages. Figure 4-27 and Figure 4-28 below show the results for scenario 15, which is comparable with scenario 11 and with the only difference being the source of emergency messages.

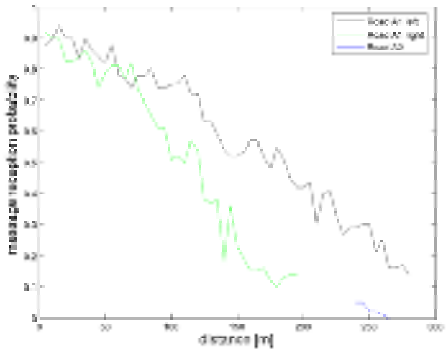


Figure 4-27: Reception Prob. of Emergency Messages - Scenario15, Rd. A, Sender on Rd. A1

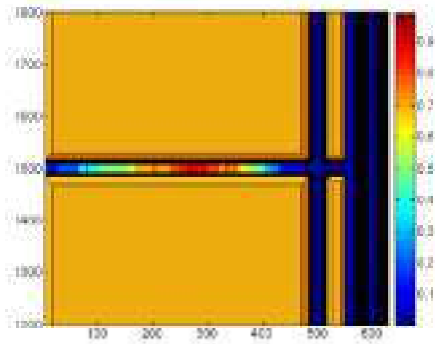


Figure 4-28: Reception Prob. of Emergency Messages-Scenario 15, Sender on Rd. A1

In batch 2, the team also evaluated the impact of increased transmission power for emergency messages. The figures below show the results for scenarios 36 and 40. The channel loading for both scenarios is defined by a routine safety message rate of 5Hz. Emergency messages in scenario 36 are transmitted at the same power as routine safety messages and the intended range is 200 meters. In scenario 40, this power is raised to a level intended for 300-meter range.

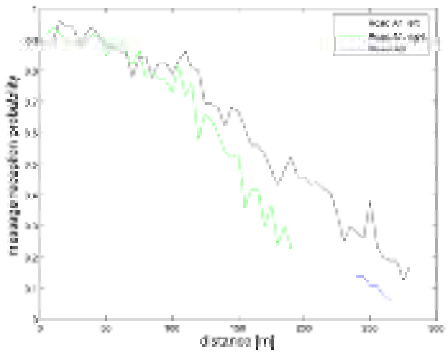


Figure 4-29: Reception Prob. of Emergency Messages – Scenario 36, Rd. A, Sender on Rd. A1

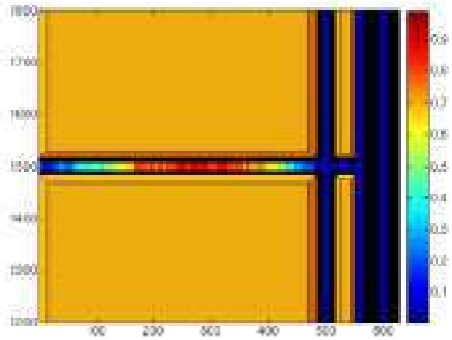


Figure 4-30: Reception Prob. of Emergency Messages-Scenario 36, Sender on Rd. A1

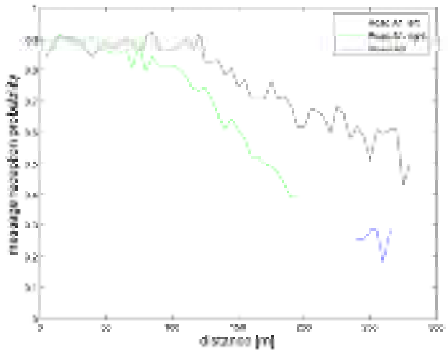


Figure 4-31: Reception prob. of Emergency Messages – Scenario 40, Rd. A, Sender on Rd. A1

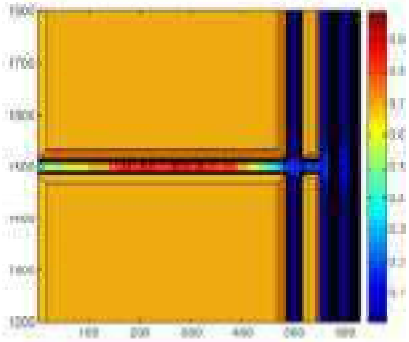


Figure 4-32: Reception Prob. of Emergency Messages-Scenario 40, Sender on Rd. A1

The results show substantial improvement for emergency messages with increased transmission power.

4.3 Intersection RSU Rebroadcast of Vehicle OBU Messages

There was a general acknowledgement within the vehicle safety community that broadcast around the corner is unlikely to have a satisfactory performance in intersection settings. This is certainly true for the measurement as well as for the simulation test results. Consequently, there is a desire to find ways to compensate for this problem. One of the ideas is to have the intersection RSU rebroadcast vehicle OBU messages.

Obviously, RSU retransmission of OBU messages will increase the load on the channel and may be counter-productive when there is already a stressful channel. On the other hand, this idea certainly appears to show promise when the channel loading is moderately low. One subtle advantage of this vehicle-to-infrastructure-to-vehicle approach is the benefit of an RSU's antenna placement. Because the intersection RSU's antenna is expected to be placed in line of sight with most vehicles around the intersection, the

reception probability should be relatively higher for both the vehicle to RSU link as well as the RSU to vehicle link. Taken together, it is thought that RSU retransmission of OBU messages could dramatically improve the message reception around the corner, if the channel is not overly stressed as a consequence.

The figures below show the broadcast performance from road section A1 around the corner to road B. Scenario 41 has a channel load defined by a routine safety message rate of 2Hz while scenario 42 has the rate set at 10Hz.

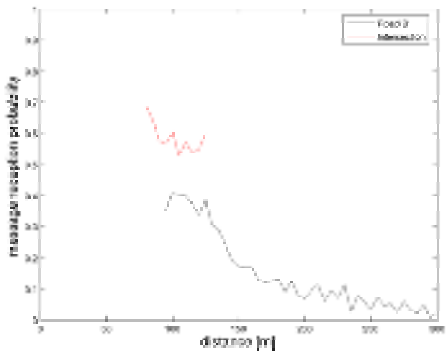


Figure 4-33: Reception Prob. of Routine Message Scenario 41, Rd. B, Sender on Rd. A1

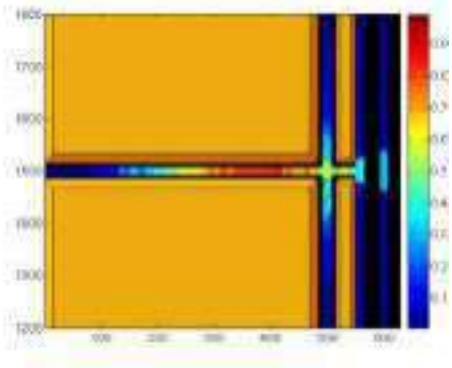


Figure 4-34: Reception Probability of Emergency Messages-Scenario 41, Sender on Rd. A1

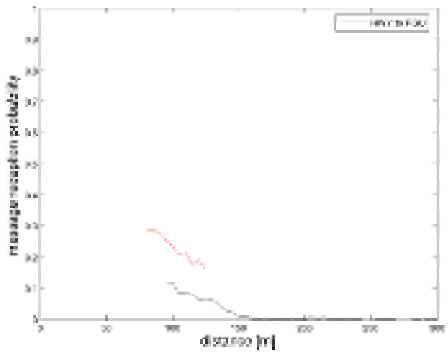


Figure 4-35: Reception prob. of Routine Message Scenario 42, Rd. B, Sender on Rd. A1

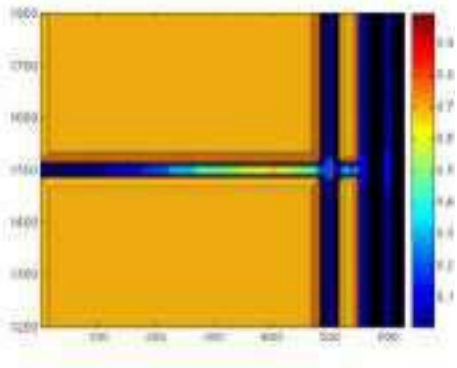
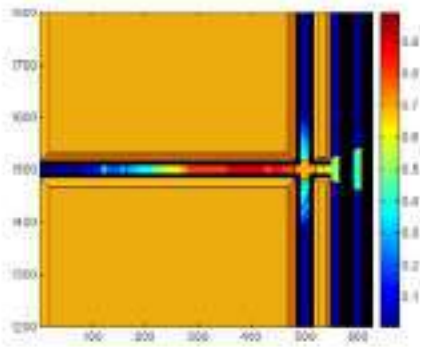
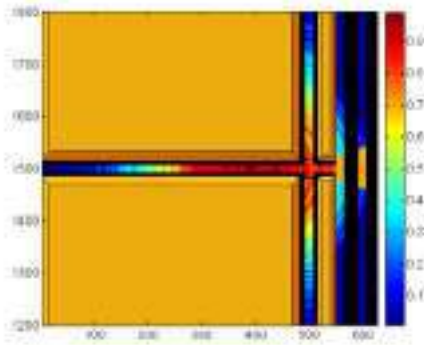
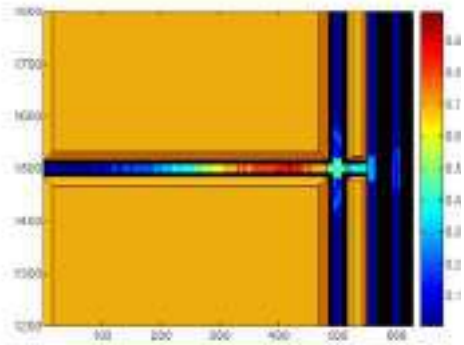
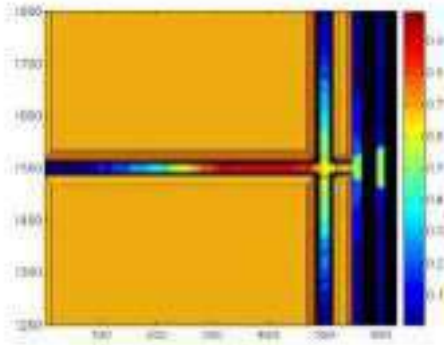
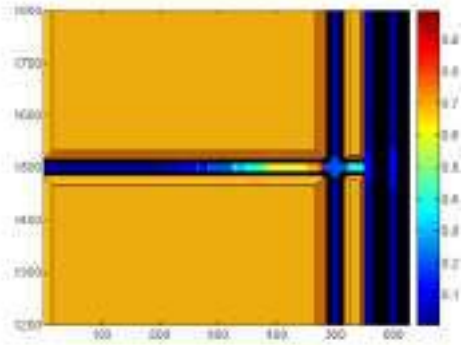
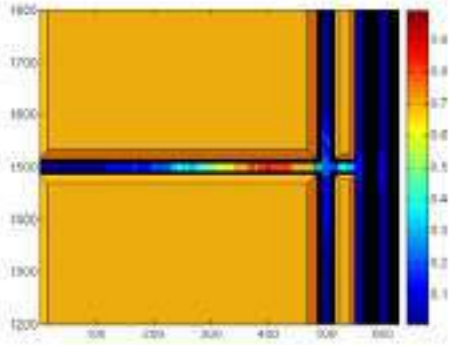


Figure 4-36: Reception Probability of Emergency Messages-Scenario 42, Sender on Rd. A1

Around the corner message reception in a saturated channel, as shown in Figure 4-35 and Figure 4-36, is very low as expected. The results in a much less stressful channel as shown in Figure 4-33 and Figure 4-34, however, do not match expectation. The starting assumption is that even if RSU retransmission doubles the amount of messages in the channel, the overall load is still lower than the scenarios with a routine safety message rate set at 5Hz. But the results look as if coming from a saturated channel.

The problem turns out to be how an RSU competes with other OBUs for channel access. The IEEE 802.11 MAC is meant to be fair. The RSU is competing with a very large number of nearby OBUs for transmission opportunities. If it has roughly the same number of messages to be sent as all other OBUs, then everyone would have roughly the same messaging performance. This is no longer true when the RSU is configured to

retransmit other OBUs' routine safety messages. For each message successfully transmitted into the channel by the RSU, several other OBUs would be competing at the same time and would have injected their share of the messages into the channel as well. Many of these messages would be received by the RSU and added into its queue for rebroadcast. Now another round of competition begins anew between the RSU and a number of other OBUs. In this manner, the number of messages waiting in the RSU's queue quickly increases until a point at which the RSU has to drop messages before transmitting them. Indeed, the RSU's queue drop rate in scenario 41 is found to be 67 percent!

	Without RSU Rebroadcast	With RSU Rebroadcast
Routine message transmission at 2Hz	 **Figure 4-37: Visualization of Emergency Messages Reception WITHOUT RSU Rebroadcast, Routine Message at 2Hz**	 **Figure 4-38: Visualization of Emergency Messages Reception WITH RSU Rebroadcast, Routine Message at 2Hz**
Routine message transmission at 5Hz	 **Figure 4-39: Visualization of Emergency Messages Reception WITHOUT RSU Rebroadcast, Routine Message at 5Hz**	 **Figure 4-40: Visualization of Emergency Messages Reception WITH RSU Rebroadcast, Routine Message at 5Hz**
Routine message transmission at 10Hz	 **Figure 4-41: Visualization of Emergency Messages Reception WITHOUT RSU Rebroadcast, Routine Message at 10Hz**	 **Figure 4-42: Visualization of Emergency Messages Reception WITH RSU Rebroadcast, Routine Message at 10Hz**

In short, RSU rebroadcast of routine OBU messages would not be productive unless there is a very low channel load to begin with. On the other hand, RSU rebroadcast of OBU

emergency messages shows improvement in both low and moderately stressed channels, as shown in the figures above[5]. This is because OBU emergency messages are not sent from all cars at all times. Consequently, the RSU is able to keep up with these messages so long as the channel is not saturated.

4.4 Cascading Emergency Messages

The scenarios in the batch 4 of the simulations are designed to emulate the communication patterns of intersection vehicle safety applications in emergency time. The following figures show the results for scenarios 43 to 46. The top two are for scenarios with a channel load defined by a routine safety message rate of 5Hz while the lower two are with the rate of 10Hz. The left column shows results of cascading emergency message through the simple repetition method, while the right column uses a more controlled feedback oriented method. Please see the earlier section on simulation scenarios and setup for details.

Each figure shows the time it takes for the cascading message to reach each car within a single lane from the intersection. The Y-axis shows time in seconds while the X-axis shows the number of cars from the starting point. The X-axis goes up to 70 cars, which is about 500 meters from the starting point.

The blue line shows the time at which each vehicle starts its turn of transmissions; while the red line shows the time at which each car first hears one of such emergency messages from ahead. Because of the arbitrarily strict rule that allows each vehicle to start its emergency transmission only if it hears from the car immediately ahead, the blue line is progressing significantly slower than the red line initially. In this way, the red line could be read as the lower bound for emergency messages to cascade through a lane of traffic.

[5] Please see Appendix C for further details.

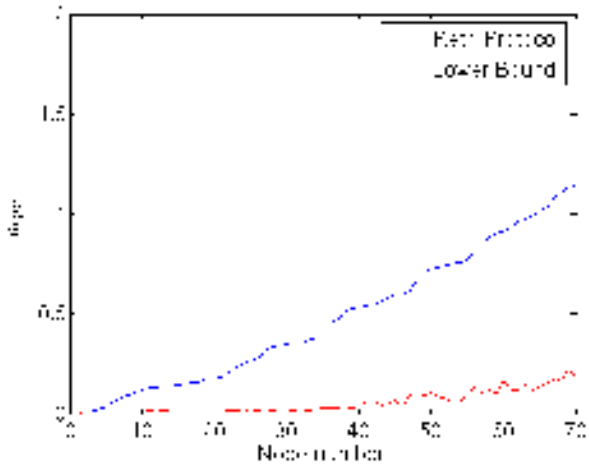


Figure 4-43: Message Cascading Over Nodes, Scenario 43, Repetition

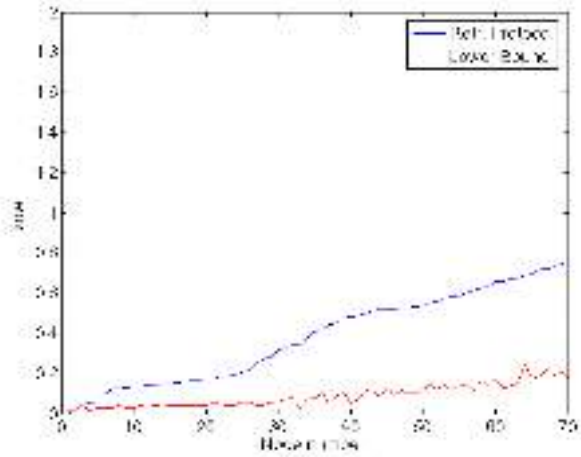


Figure 4-44: Message Cascading Over Nodes, Scenario 44, Feedback

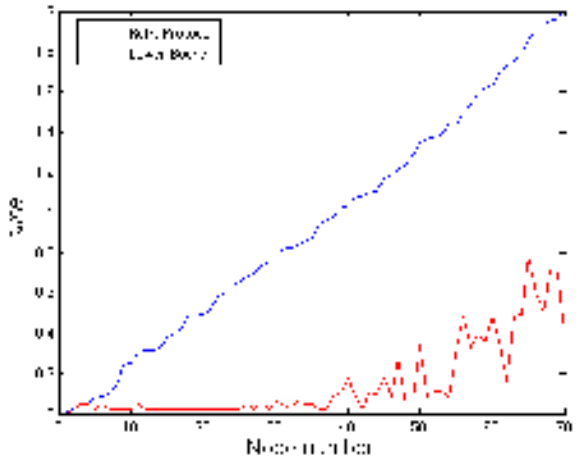


Figure 4-45: Message Cascading Over Nodes, Scenario 45, Repetition

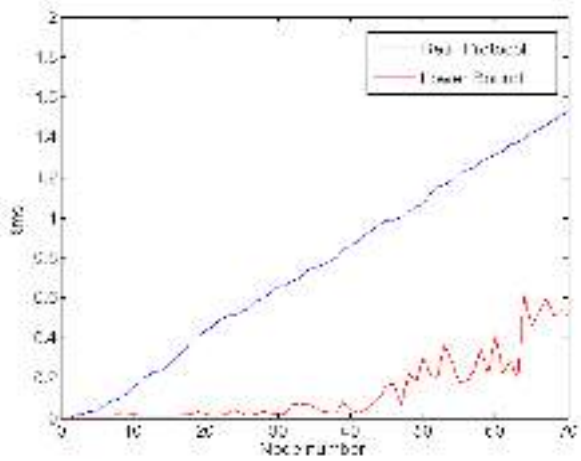


Figure 4-46: Message Cascading Over Nodes, Scenario 46, Feedback

Overall, emergency messages seem to cascade consistently even in a very saturated channel. Please note that all scenarios are configured so that a node would wait 20 ms before its next transmission (if necessary). The result in Figure 4-46 shows it takes slightly more than 20 ms on average for the emergency message to cascade from car to car. This means each hop is taking about 1 retransmission each. Therefore, there is certainly potential for this performance to be improved upon via tuning the parameters

5 Detailed Simulation Test Results

In this appendix section, detailed results are provided for the entire simulation test scenarios described in the five batches of simulation matrixes.

5.1 Batch 1, Routine and Emergency Safety Messaging in Saturated Channel

5.1.1 Scenario 1

Simulation Scenario Settings:

RF Model	Deterministic
Emergency Message Sender	RSU, 500 bytes/ 10Hz/200m
Corner Model	No buildings
Commercial RSU	On, 500 bytes/ 2Hz/ 200m
Routine Messages	200 bytes /10Hz /200m

5.1.1.1 Reception Probability of Emergency Messages

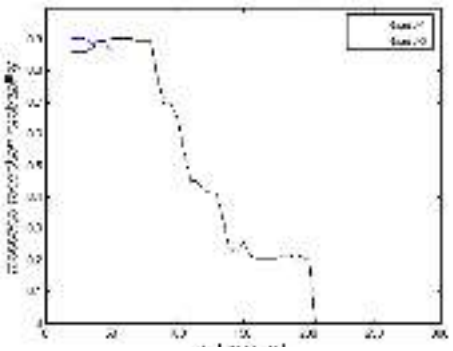


Figure 5-1: Reception Probability of Emergency Messages-Scenario1, Road A, Sender RSU

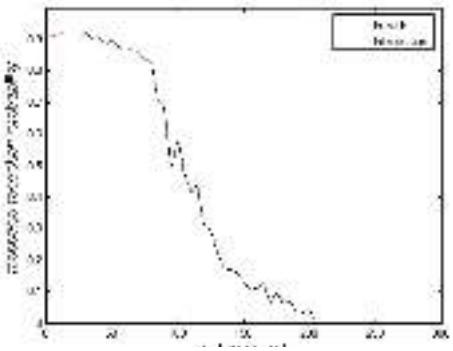


Figure 5-2: Reception Probability of Emergency Messages-Scenario 1, Road B, Sender RSU

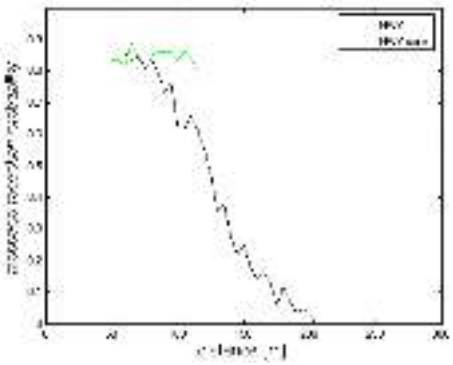


Figure 5-3: Reception Probability of Emergency Messages-Scenario 1, HWY, Sender RSU

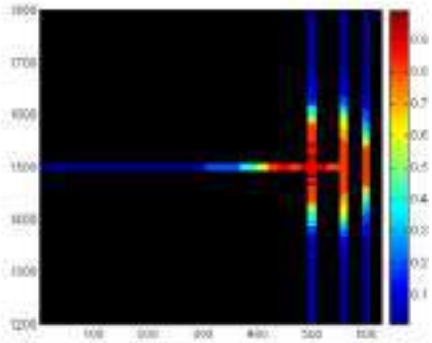


Figure 5-4: Reception Probability of Emergency Messages-Scenario 1, Sender RSU

5.1.1.2 Reception Probability of Routine Messages

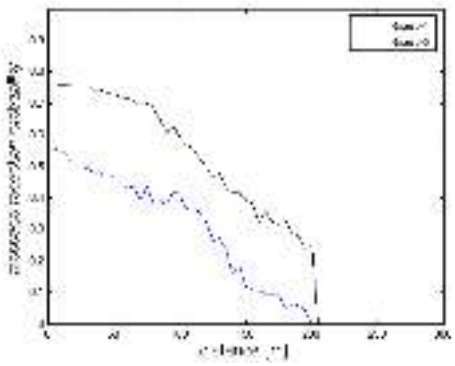


Figure 5-5: Reception Probability of Routine Messages on Road A, Scenario 1

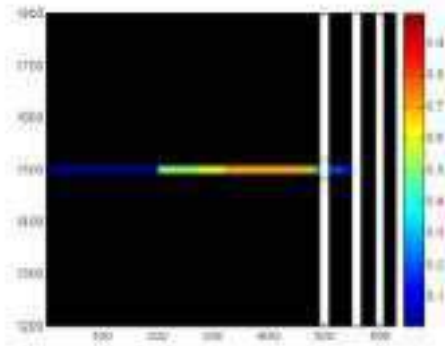


Figure 5-6: Reception Probability of Routine Messages on Road A, Scenario 1

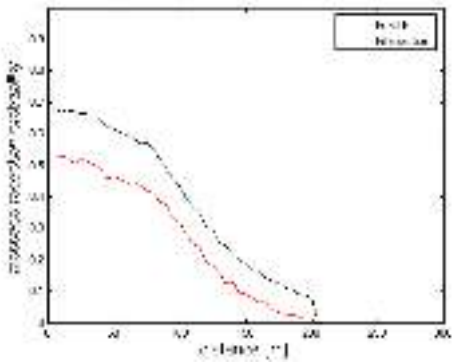


Figure 5-7: Reception Probability of Routine Messages on Road B, Scenario 1

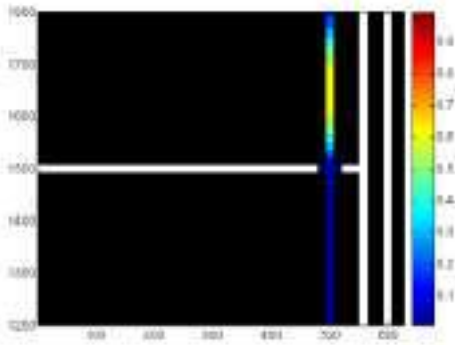


Figure 5-8: Reception Probability of Routine Messages on Road B, Scenario 1

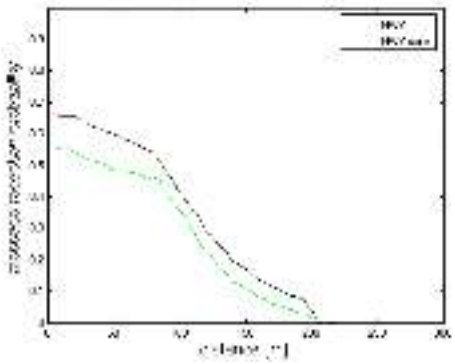


Figure 5-9: Reception Probability of Routine Messages on HWY, Scenario 1

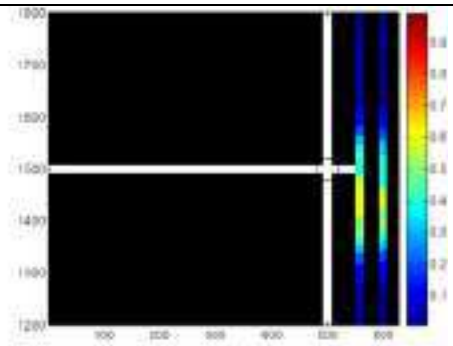


Figure 5-10: Reception Probability of Routine Messages on HWY, Scenario 1

5.1.2 Scenario 2

Simulation Scenario Settings:

RF Model	Deterministic
Emergency Message Sender	RSU, 500 bytes/ 10Hz/200m
Corner Model	No buildings
Commercial RSU	OFF
Routine Messages	200byte /10Hz /200m

5.1.2.1 Reception Probability of Emergency Messages

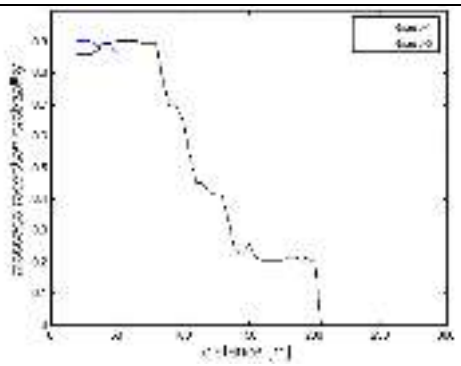


Figure 5-11: Reception Probability of Emergency Messages-Scenario 2, Road A, Sender RSU

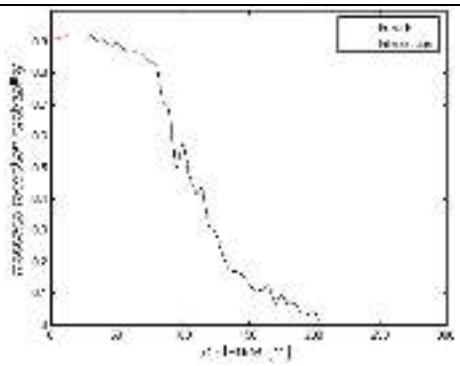


Figure 5-12: Reception Probability of Emergency Messages-Scenario 2, Road B, Sender RSU

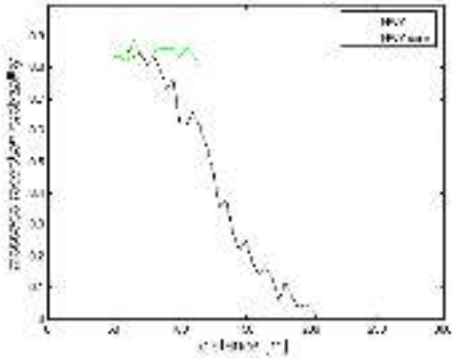


Figure 5-13: Reception Probability of Emergency Messages-Scenario 2, HWY, Sender RSU

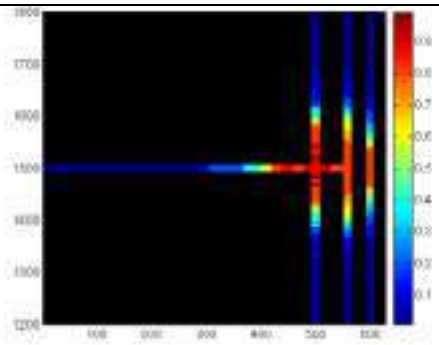


Figure 5-14: Reception Probability of Emergency Messages-Scenario 2, Sender RSU

5.1.2.2 Reception Probability of Routine Messages

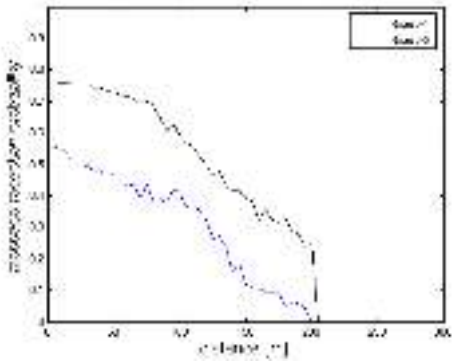


Figure 5-15: Reception Probability of Routine Messages on Road A, Scenario 2

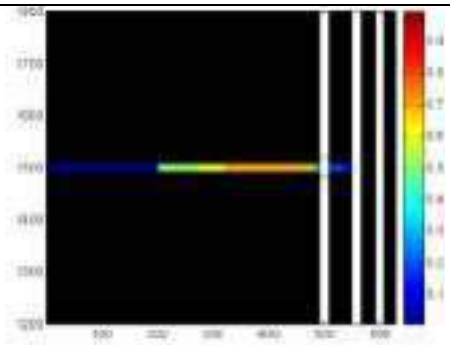


Figure 5-16: Reception Probability of Routine Messages on Road A, Scenario 2

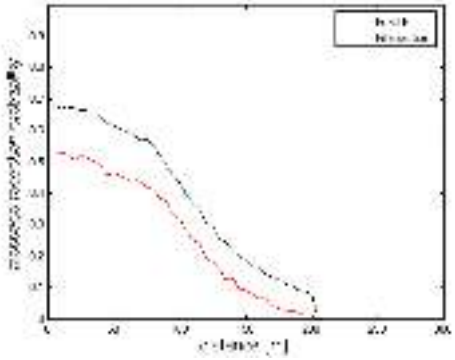


Figure 5-17: Reception Probability of Routine Messages on Road B, Scenario 2

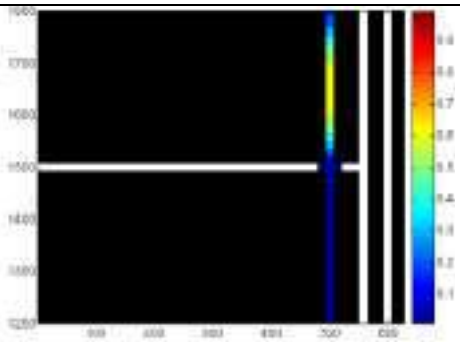


Figure 5-18: Reception Probability of Routine Messages on Road B, Scenario 2

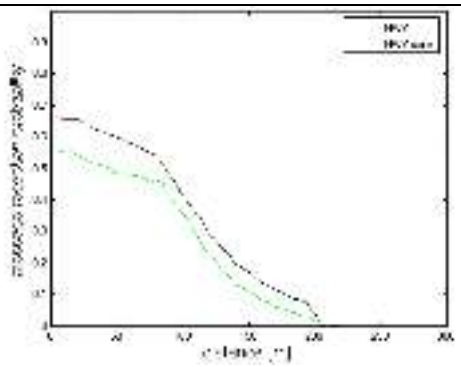


Figure 5-19: Reception Probability of Routine Messages on HWY, Scenario 2

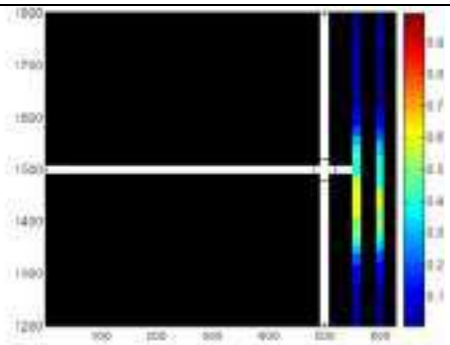


Figure 5-20: Reception Probability of Routine Messages on HWY, Scenario 2

5.1.3 Scenario 3

Simulation Scenario Settings:

RF Model	Deterministic
Emergency Message Sender	RSU, 500 bytes/ 10Hz/200m
Corner Model	Tall buildings
Commercial RSU	On, 500bytes/2Hz/200m
Routine Messages	200byte /10Hz /200m

5.1.3.1 Reception Probability of Emergency Messages

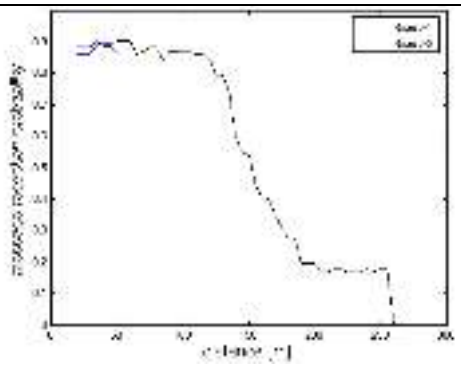


Figure 5-21: Reception Probability of Emergency Messages-Scenario 3, Road A, Sender RSU

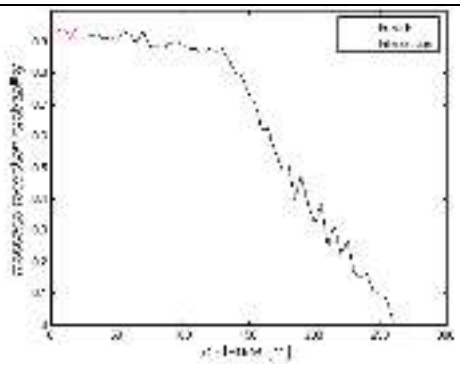


Figure 5-22: Reception Probability of Emergency Messages-Scenario 3, Road B, Sender RSU

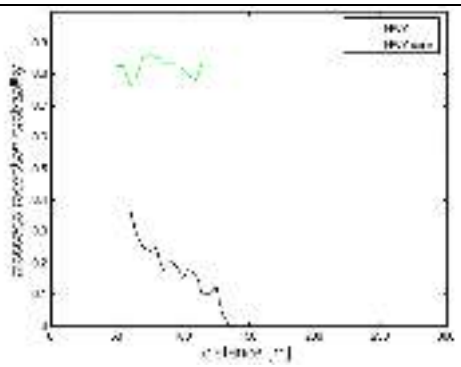


Figure 5-23: Reception Probability of Emergency Messages-Scenario 3, HWY, Sender RSU

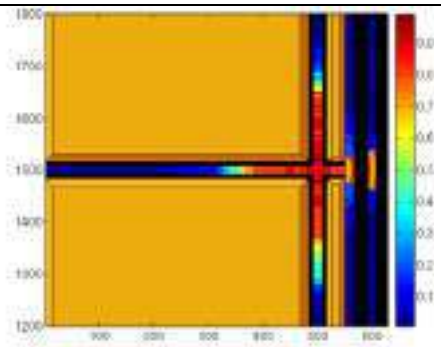


Figure 5-24: Reception Probability of Emergency Messages-Scenario 3, Sender RSU

5.1.3.2 Reception Probability of Routine Messages

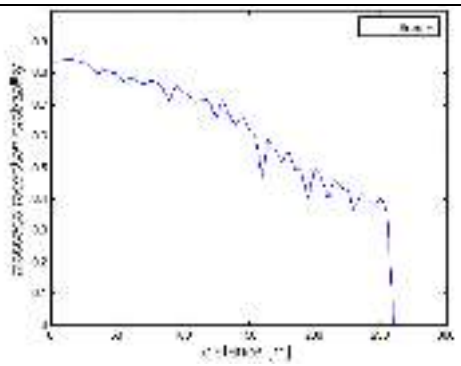


Figure 5-25: Reception Probability of Routine Messages on Road A, Scenario 3

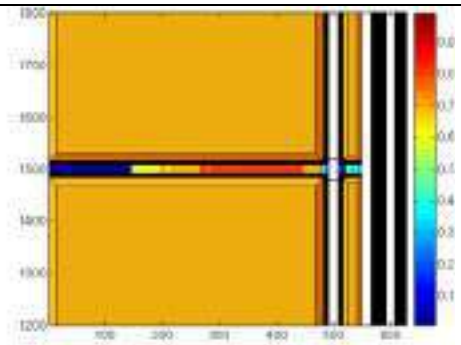


Figure 5-26: Reception Probability of Routine Messages on Road A, Scenario 3

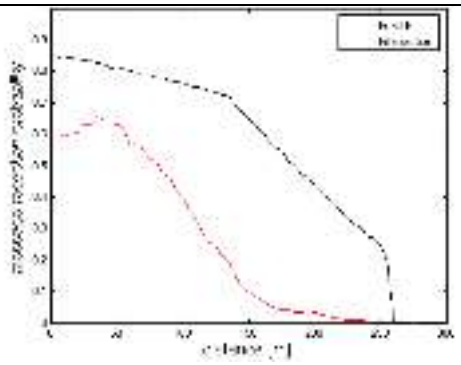


Figure 5-27: Reception Probability of Routine Messages on Road B, Scenario 3

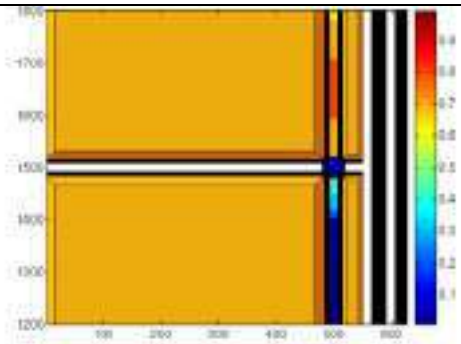


Figure 5-28: Reception Probability of Routine Messages on Road B, Scenario 3

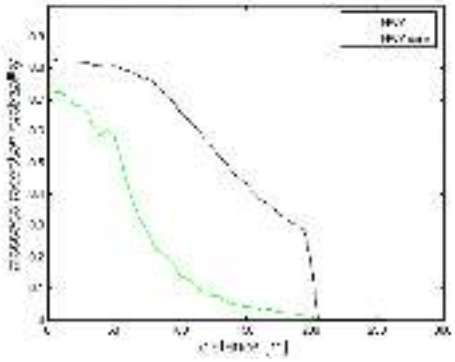


Figure 5-29: Reception Probability of Routine Messages on HWY, Scenario 3

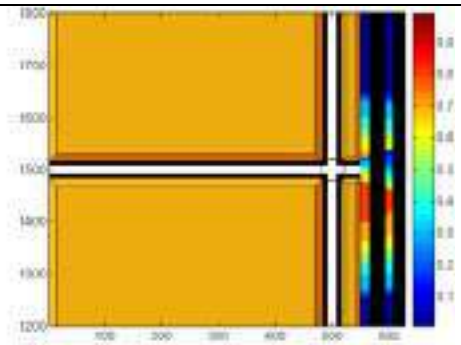


Figure 5-30: Reception Probability of Routine Messages on HWY, Scenario 3

5.1.4 Scenario 4

Simulation Scenario Settings:

RF Model	Deterministic
Emergency Message Sender	RSU, 500 bytes/ 10Hz/200m
Corner Model	Tall buildings
Commercial RSU	OFF
Routine Messages	200byte /10Hz /200m

5.1.4.1 Reception Probability of Emergency Messages

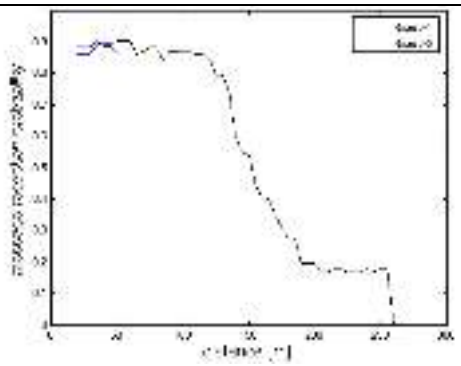


Figure 5-31: Reception Probability of Emergency Messages-Scenario 4, Road A, Sender RSU

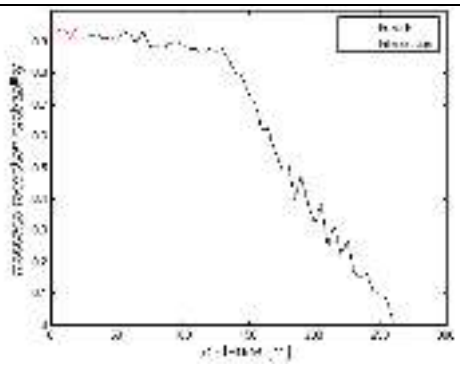


Figure 5-32: Reception Probability of Emergency Messages-Scenario 4, Road B, Sender RSU

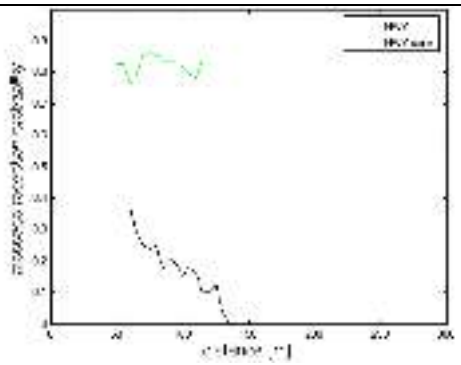


Figure 5-33: Reception Probability of Emergency Messages-Scenario 4, HWY, Sender RSU

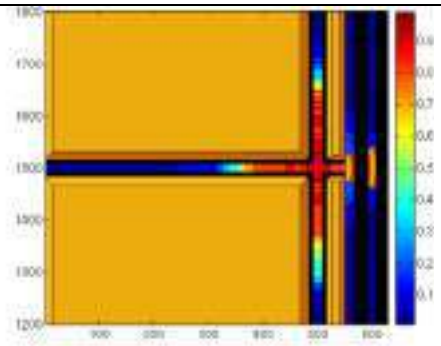


Figure 5-34: Reception Probability of Emergency Messages-Scenario 4, Sender RSU

5.1.4.2 Reception Probability of Routine Messages

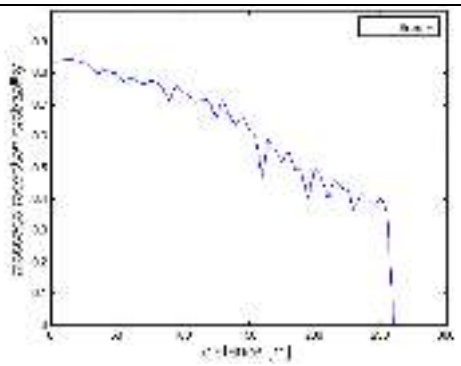


Figure 5-35: Reception Probability of Routine Messages on Road A, Scenario 4

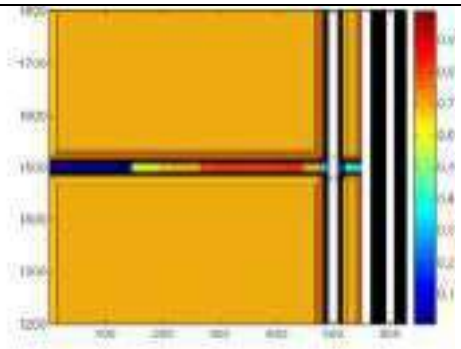


Figure 5-36: Reception Probability of Routine Messages on Road A, Scenario 4

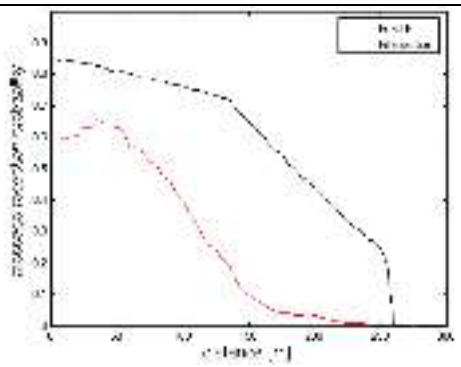


Figure 5-37: Reception Probability of Routine Messages on Road B, Scenario 4

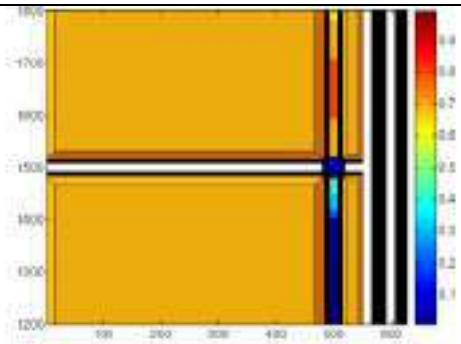


Figure 5-38: Reception Probability of Routine Messages on Road B, Scenario 4

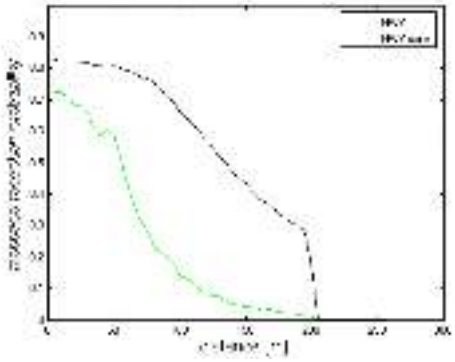


Figure 5-39: Reception Probability of Routine Messages on HWY, Scenario 4

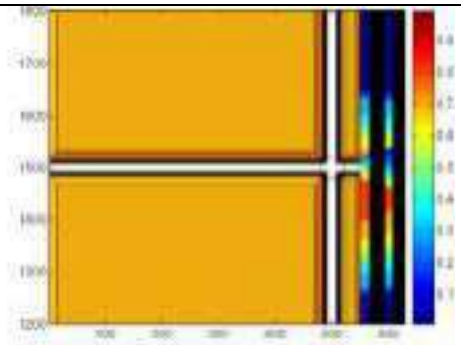


Figure 5-40: Reception Probability of Routine Messages on HWY, Scenario 4

5.1.5 Scenario 5

Simulation Scenario Setting:

RF Model	Deterministic
Emergency Message Sender	OBUs on Road A1, A2, B 500 bytes/ 10Hz/200m on HWY 200 bytes/ 50Hz/200m
Corner Model	No building
Commercial RSU	On, 500bytes/ 2Hz/ 200m
Routine Messages	200byte /10Hz /200m

5.1.5.1 Reception Probability of Emergency Messages from OBU on A1

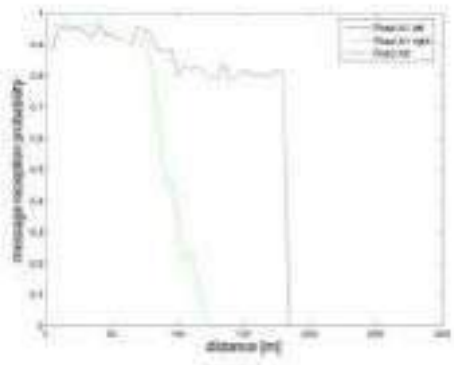


Figure 5-41: Reception Prob. of Emergency Messages - Scenario5, Rd. A, Sender on Rd. A1

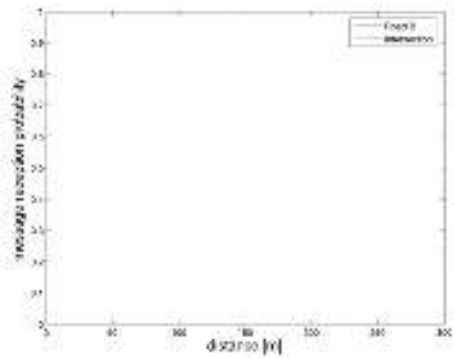


Figure 5-42: Reception Prob. of Emergency Messages - Scenario5, Rd. B, Sender on Rd. A1

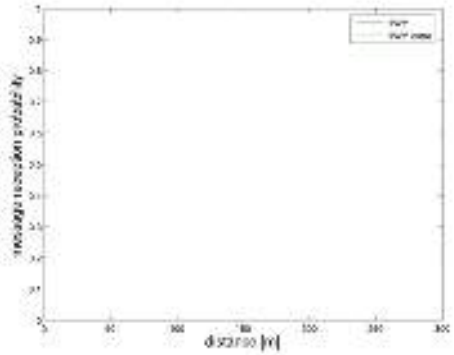


Figure 5-43: Reception Prob. of Emergency Messages - Scenario5, HWY, Sender on Rd. A1

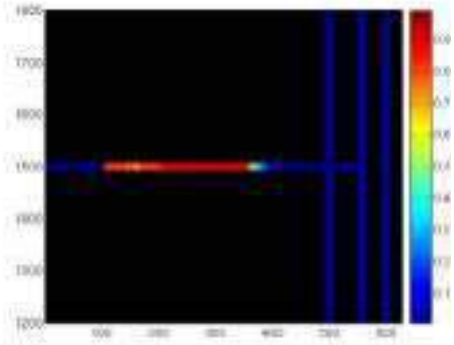


Figure 5-44: Reception Prob. of Emergency Messages-Scenario 5, Sender on Rd. A1

5.1.5.2 Reception Probability of Emergency Messages from OBU on A2

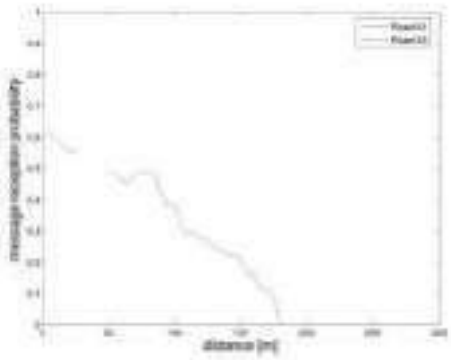


Figure 5-45: Reception Prob. of Emergency Messages – Scenario 5, Rd. A, Sender on Rd. A2

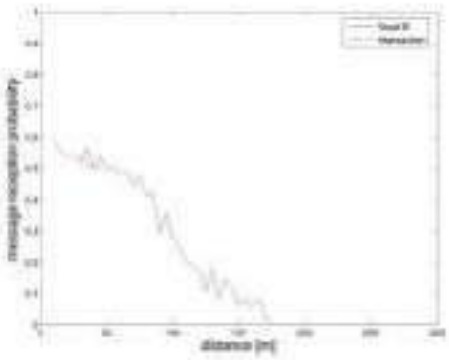


Figure 5-46: Reception Prob. of Emergency Messages – Scenario 5, Rd. B, Sender on Rd. A2

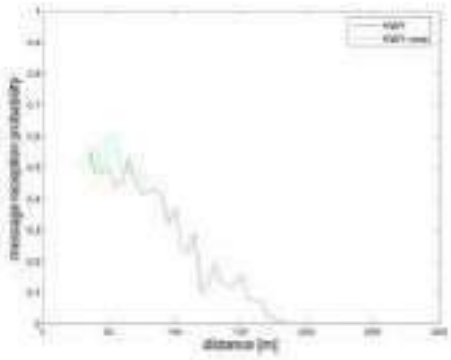


Figure 5-47: Reception Prob. of Emergency Messages – Scenario 5, HWY, Sender on Rd. A2

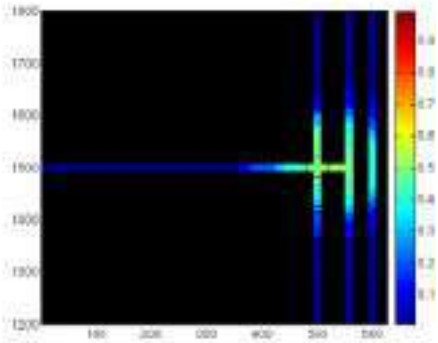


Figure 5-48: Reception Prob. of Emergency Messages-Scenario 5, Sender on Rd. A2

5.1.5.3 Reception Probability of Emergency Messages from OBU on B

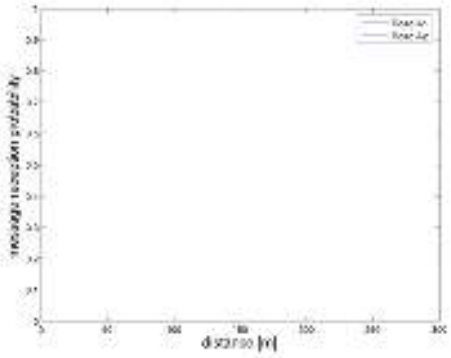


Figure 5-49: Reception Prob. of Emergency Messages – Scenario 5, Rd. A, Sender on Rd. B

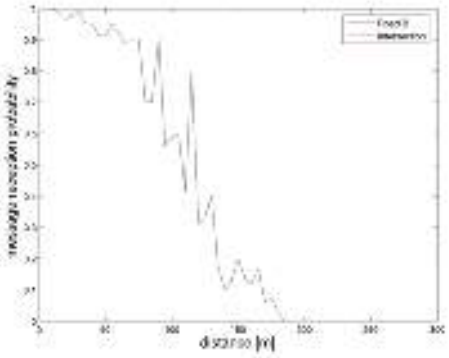


Figure 5-50: Reception Prob. of Emergency Messages – Scenario 5, Rd. B, Sender on Rd. B

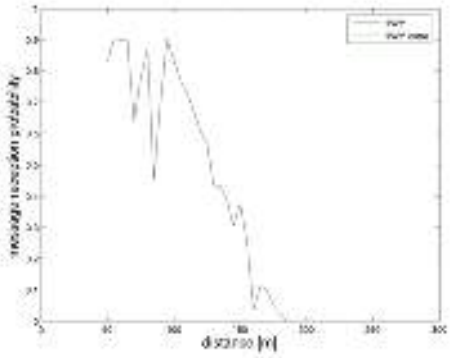


Figure 5-51: Reception Prob. of Emergency Messages – Scenario 5, HWY, Sender on Rd. B

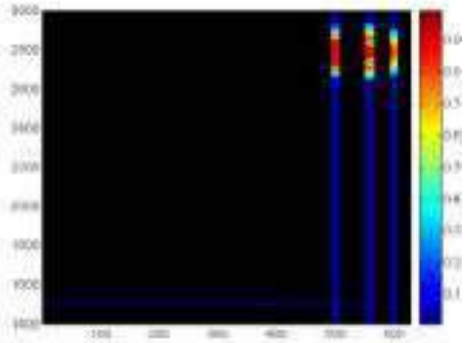


Figure 5-52: Reception Prob. of Emergency Messages-Scenario 5, Sender on Rd. B

5.1.5.4 Reception Probability of Emergency Messages from OBU on HWY

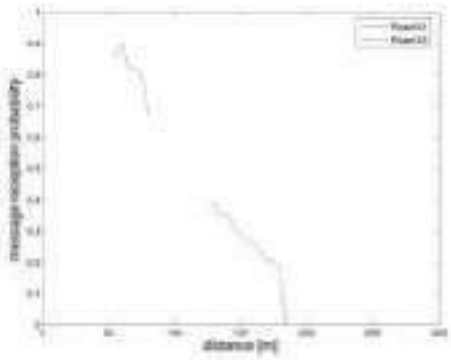


Figure 5-53: Reception Prob. of Emergency Messages – Scenario 5, Rd. A, Sender on HWY

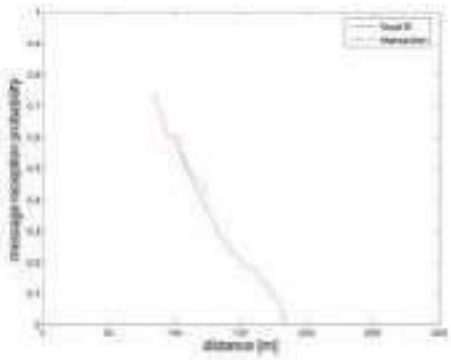


Figure 5-54: Reception Prob. of Emergency Messages – Scenario 5, Rd. B, Sender on HWY

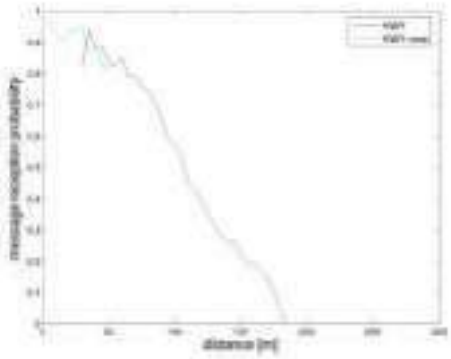


Figure 5-55: Reception Prob. of Emergency Messages – Scenario 5, HWY, Sender on HWY

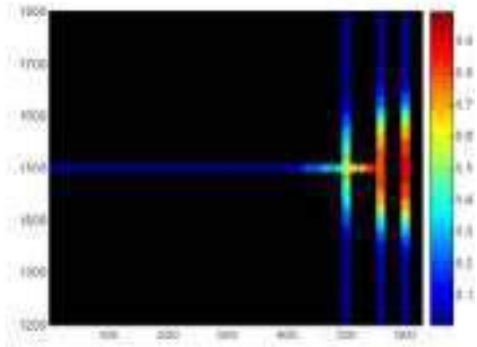


Figure 5-56: Reception Prob. of Emergency Messages-Scenario 5, Sender on HWY

5.1.6 Scenario 6

Simulation Scenario Setting:

RF Model	Deterministic
Emergency Message Sender	OBUs on Road A1, A2, B 500 bytes/ 10Hz/200m on HWY 200 bytes/ 50Hz/200m
Corner Model	No building
Commercial RSU	OFF
Routine Messages	200byte /10Hz /200m

5.1.6.1 Reception Probability of Emergency Messages from OBU on A1

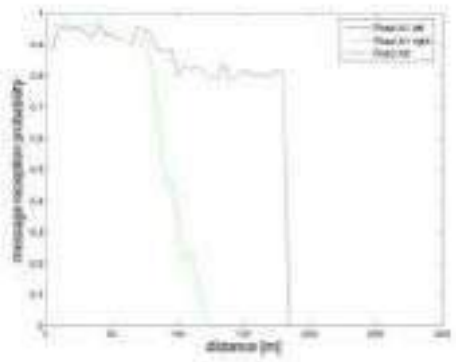


Figure 5-57: Reception Prob. of Emergency Messages – Scenario 6, Rd. A, Sender on Rd. A1

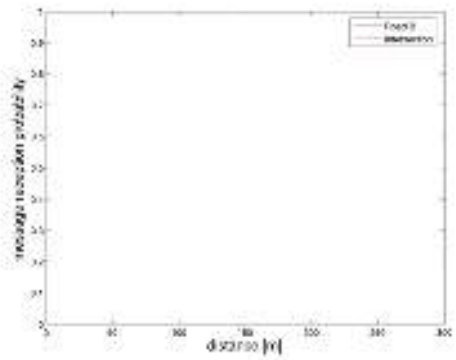


Figure 5-58: Reception Prob. of Emergency Messages – Scenario 6, Rd. B, Sender on Rd. A1

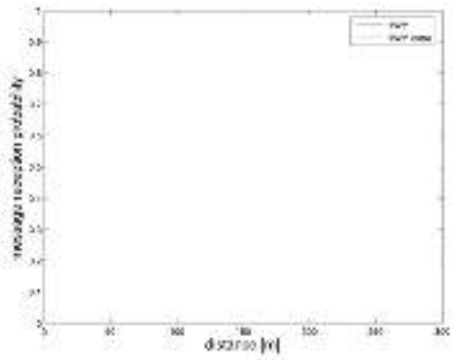


Figure 5-59: Reception Prob. of Emergency Messages – Scenario 6, HWY, Sender on Rd. A1

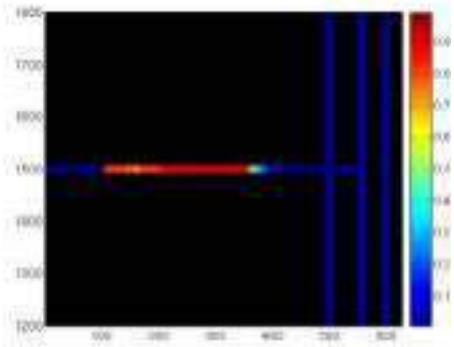


Figure 5-60: Reception Prob. of Emergency Messages-Scenario 6, Sender on Rd. A1

5.1.6.2 Reception Probability of Emergency Messages from OBU on A2

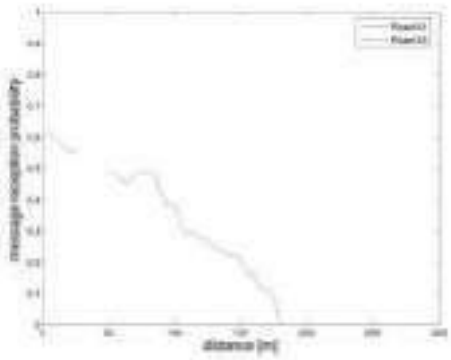


Figure 5-61: Reception Prob. of Emergency Messages – Scenario 6, Rd. A, Sender on Rd. A2

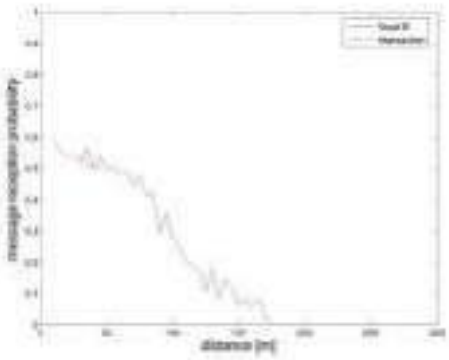


Figure 5-62: Reception Prob. of Emergency Messages – Scenario 6, Rd. B, Sender on Rd. A2

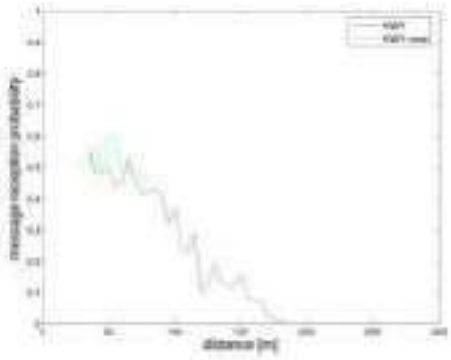


Figure 5-63: Reception Prob. of Emergency Messages – Scenario 6, HWY, Sender on Rd. A2

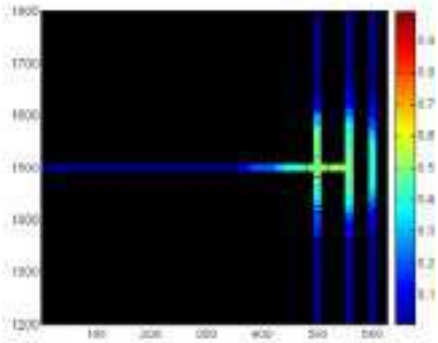


Figure 5-64: Reception Prob. of Emergency Messages-Scenario 6, Sender on Rd. A2

5.1.6.3 Reception Probability of Emergency Messages from OBU on B

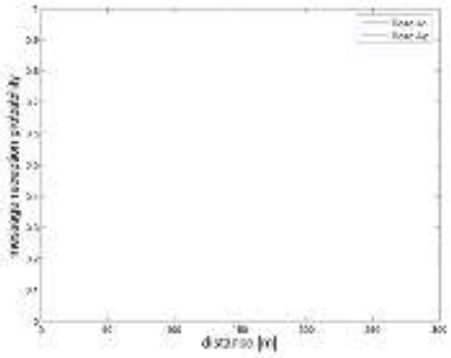


Figure 5-65: Reception Prob. of Emergency Messages – Scenario 6, Rd. A, Sender on Rd. B

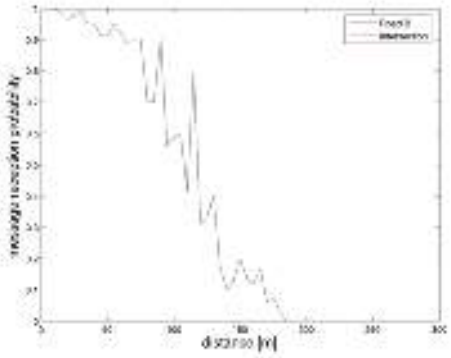


Figure 5-66: Reception Prob. of Emergency Messages – Scenario 6, Rd. B, Sender on Rd. B

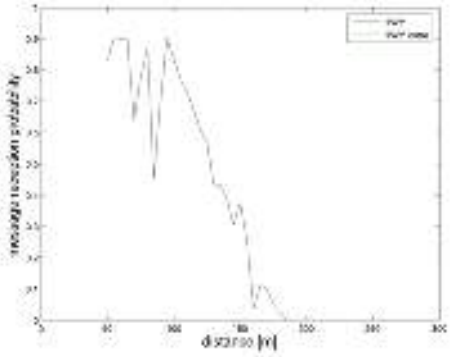


Figure 5-67: Reception Prob. of Emergency Messages – Scenario 6, HWY, Sender on Rd. B

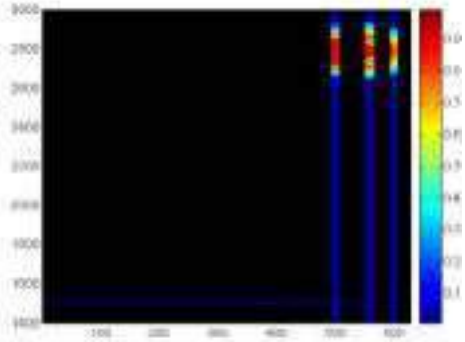


Figure 5-68: Reception Prob. of Emergency Messages-Scenario 6, Sender on Rd. B

5.1.6.4 Reception Probability of Emergency Messages from OBU on HWY

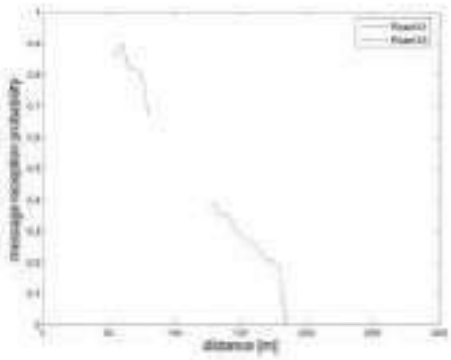


Figure 5-69: Reception Prob. of Emergency Messages – Scenario 6, Rd. A, Sender on HWY

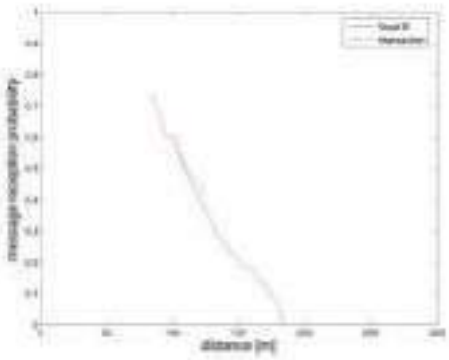


Figure 5-70: Reception Prob. of Emergency Messages – Scenario 6, Rd. B, Sender on HWY

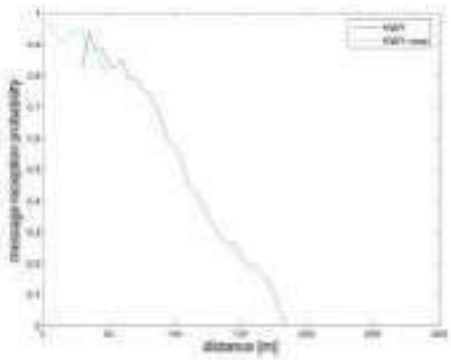


Figure 5-71: Reception Prob. of Emergency Messages – Scenario 6, HWY, Sender on HWY

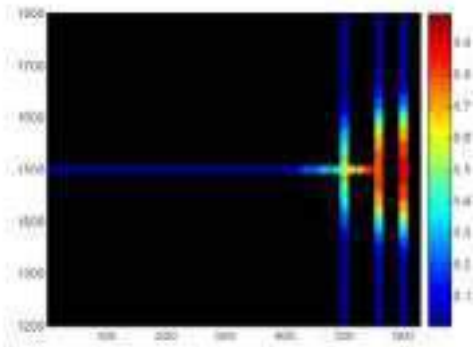


Figure 5-72: Reception Prob. of Emergency Messages-Scenario 6, Sender on HWY

5.1.7 Scenario 7

Simulation Scenario Setting:

RF Model	Deterministic
Emergency Message Sender	OBUs on Road A1, A2, B 500 bytes/ 10Hz/200m on HWY 200 bytes/ 50Hz/200m
Corner Model	Tall building
Commercial RSU	On, 500bytes/ 2Hz/ 200m
Routine Messages	200byte /10Hz /200m

5.1.7.1 Reception Probability of Emergency Messages from OBU on A1

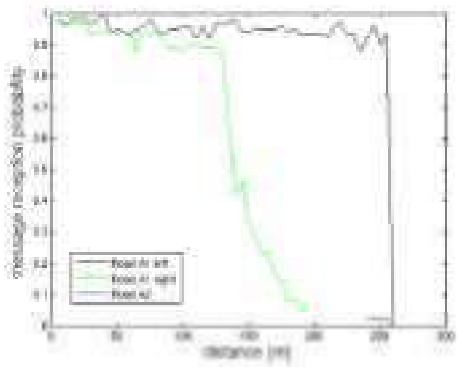


Figure 5-73: Reception Prob. of Emergency Messages – Scenario 7, Rd. A, Sender on Rd. A1

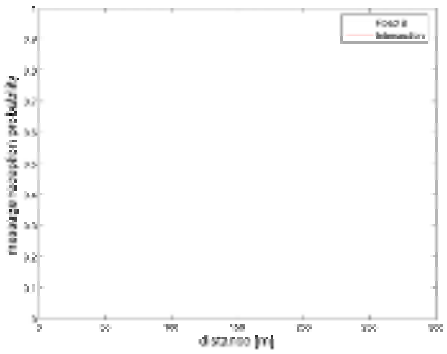


Figure 5-74: Reception Prob. of Emergency Messages – Scenario 7, Rd. B, Sender on Rd. A1

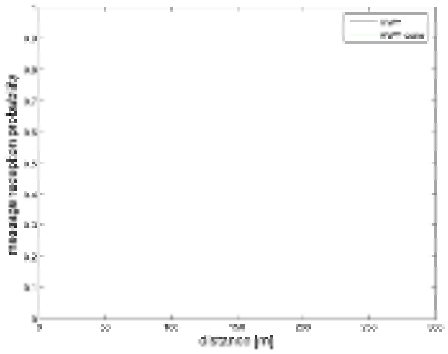


Figure 5-75: Reception Prob. of Emergency Messages – Scenario 7, HWY, Sender on Rd. A1

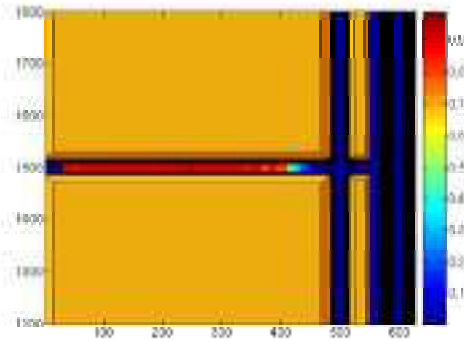


Figure 5-76: Reception Prob. of Emergency Messages-Scenario 7, Sender on Rd. A1

5.1.7.2 Reception Probability of Emergency Messages from OBU on A2

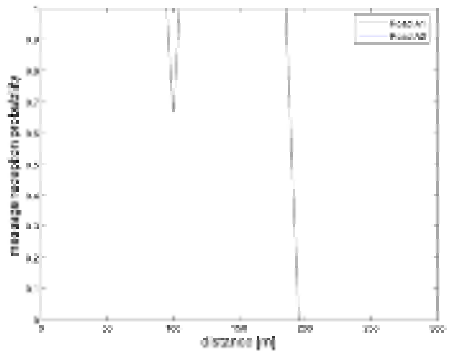


Figure 5-77: Reception Prob. of Emergency Messages – Scenario 7, Rd. A, Sender on Rd. A2

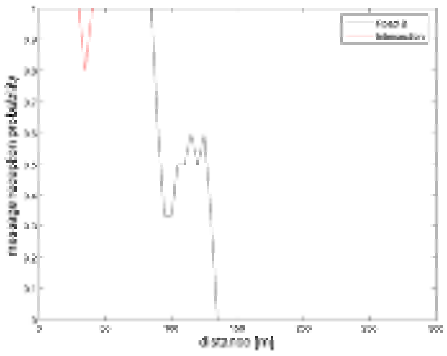


Figure 5-78: Reception Prob. of Emergency Messages – Scenario 7, Rd. B, Sender on Rd. A2

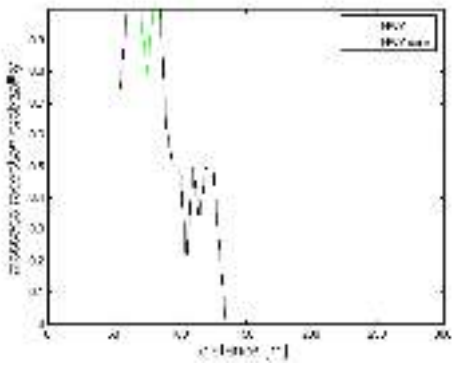


Figure 5-79: Reception Prob. of Emergency Messages – Scenario 7, HWY, Sender on Rd. A2

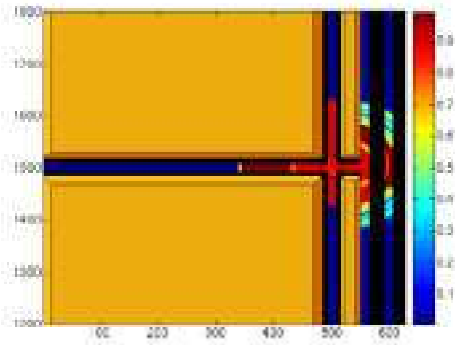


Figure 5-80: Reception Prob. of Emergency Messages-Scenario 7, Sender on Rd. A2

5.1.7.3 Reception Probability of Emergency Messages from OBU on B

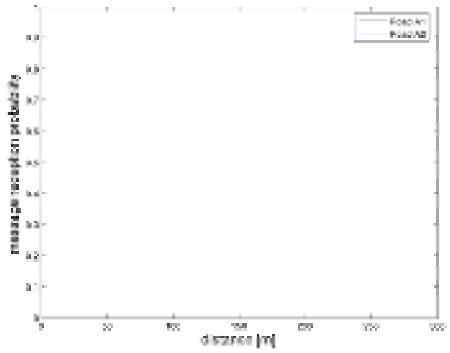


Figure 5-81: Reception Prob. of Emergency Messages – Scenario 7, Rd. A, Sender on Rd. B

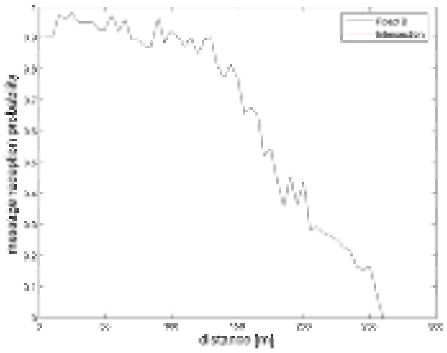


Figure 5-82: Reception Prob. of Emergency Messages – Scenario 7, Rd. B, Sender on Rd. B

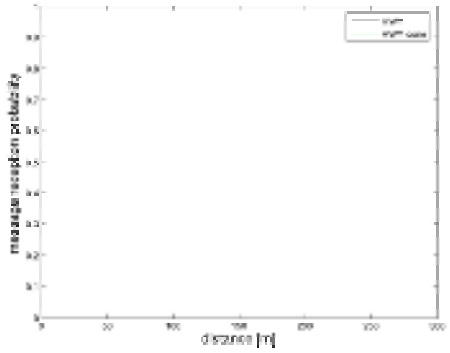


Figure 5-83: Reception Prob. of Emergency Messages – Scenario 7, HWY, Sender on Rd. B

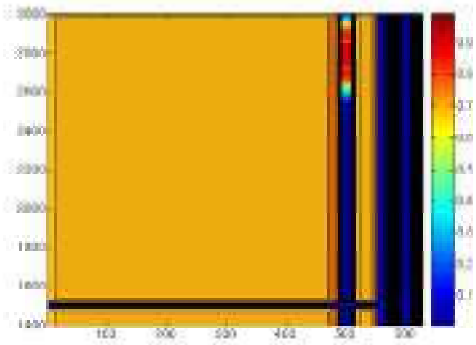


Figure 5-84: Reception Prob. of Emergency Messages-Scenario 7, Sender on Rd. B

5.1.7.4 Reception Probability of Emergency Messages from OBU on B

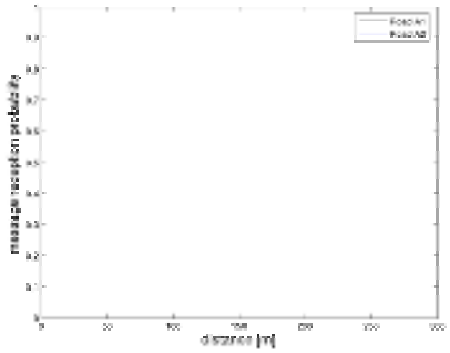


Figure 5-85: Reception Prob. of Emergency Messages – Scenario 7, Rd. A, Sender on Rd. B

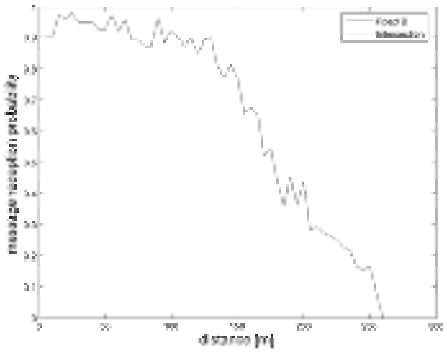


Figure 5-86: Reception Prob. of Emergency Messages – Scenario 7, Rd. B, Sender on Rd. B

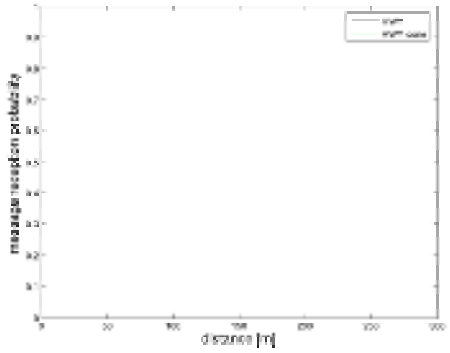


Figure 5-87: Reception Prob. of Emergency Messages – Scenario 7, HWY, Sender on Rd. B

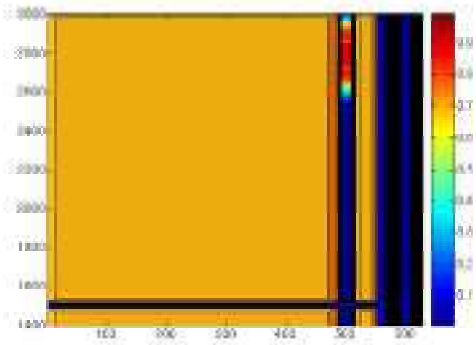


Figure 5-88: Reception Prob. of Emergency Messages-Scenario 7, Sender on Rd. B

5.1.7.5 Reception Probability of Emergency Messages from OBU on HWY

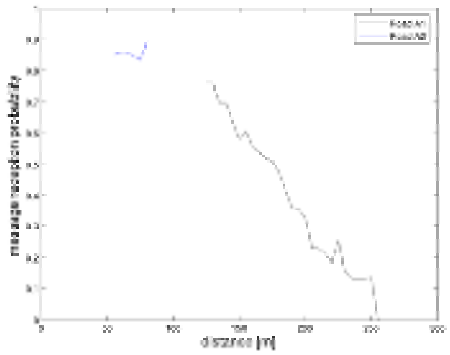


Figure 5-89: Reception Prob. of Emergency Messages – Scenario 7, Rd. A, Sender on HWY

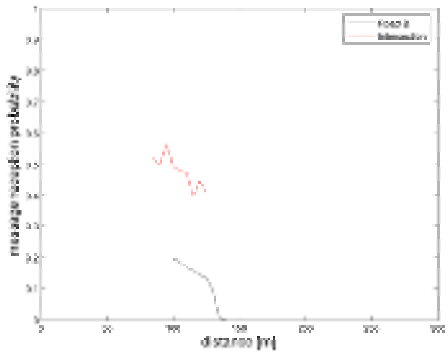


Figure 5-90: Reception Prob. of Emergency Messages – Scenario 7, Rd. B, Sender on HWY

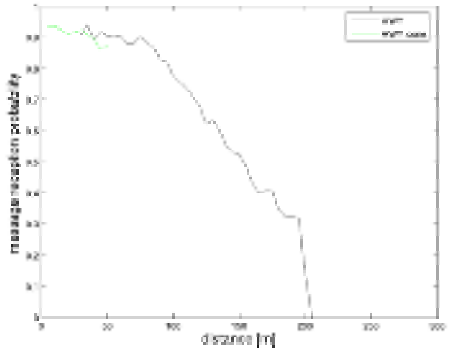


Figure 5-91: Reception Prob. of Emergency Messages – Scenario 7, HWY, Sender on HWY

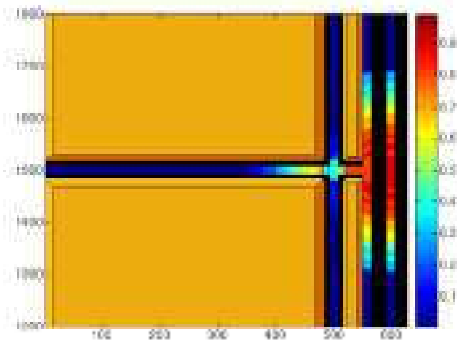


Figure 5-92: Reception Prob. of Emergency Messages-Scenario 7, Sender on HWY

5.1.8 Scenario 8

Simulation Scenario Setting:

RF Model	Deterministic
Emergency Message Sender	OBUs on Road A1, A2, B 500 bytes/ 10Hz/200m on HWY 200 bytes/ 50Hz/200m
Corner Model	Tall building
Commercial RSU	OFF
Routine Messages	200byte /10Hz /200m

5.1.8.1 Reception Probability of Emergency Messages from OBU on A1

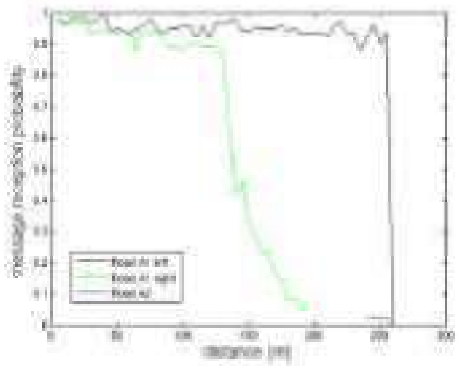


Figure 5-93: Reception Prob. of Emergency Messages – Scenario 8, Rd. A, Sender on Rd. A1

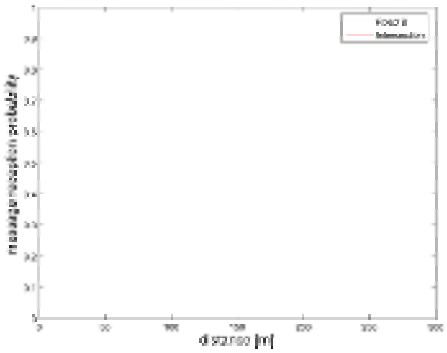


Figure 5-94: Reception Prob. of Emergency Messages – Scenario 8, Rd. B, Sender on Rd. A1

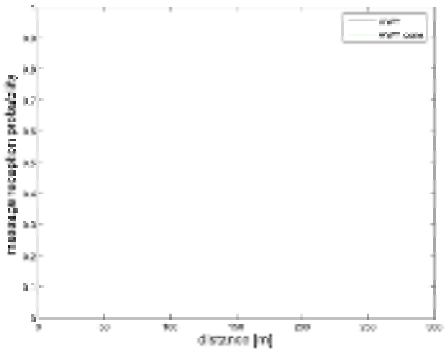


Figure 5-95: Reception Prob. of Emergency Messages – Scenario 8, HWY, Sender on Rd. A1

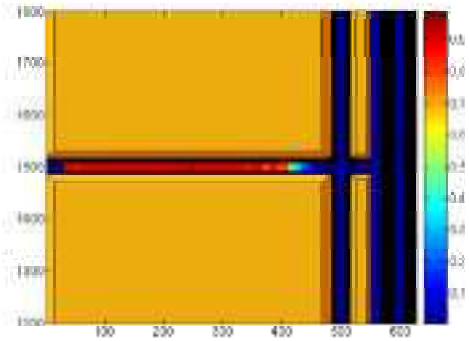


Figure 5-96: Reception Prob. of Emergency Messages-Scenario 8, Sender on Rd. A1

5.1.8.2 Reception Probability of Emergency Messages from OBU on A2

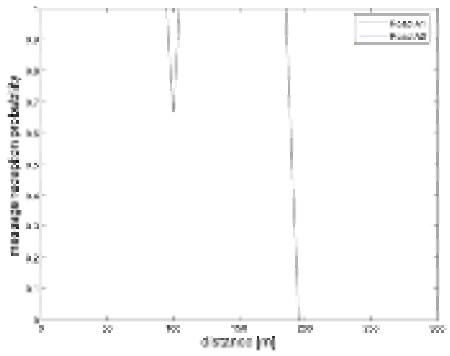


Figure 5-97: Reception Prob. of Emergency Messages – Scenario 8, Rd. A, Sender on Rd. A2

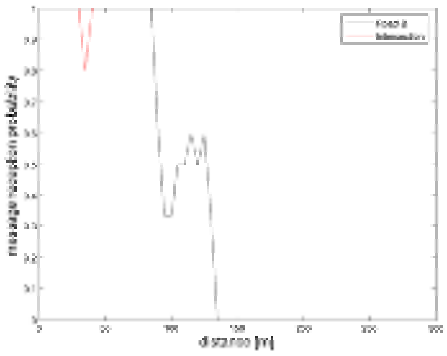


Figure 5-98: Reception Prob. of Emergency Messages – Scenario 8, Rd. B, Sender on Rd. A2

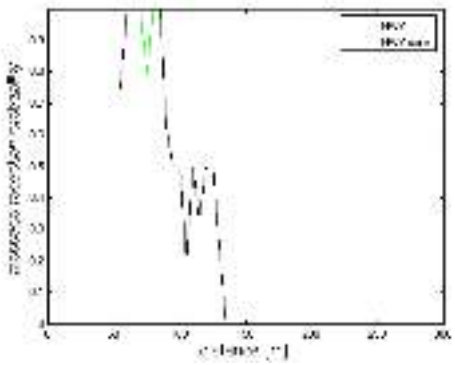


Figure 5-99: Reception Prob. of Emergency Messages – Scenario 8, HWY, Sender on Rd. A2

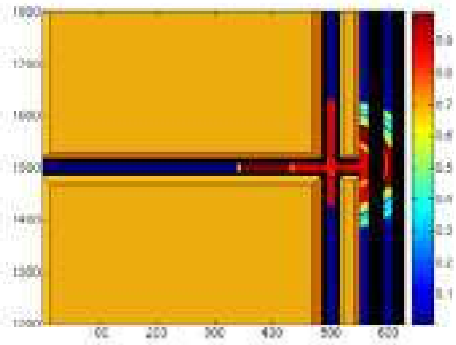


Figure 5-100: Reception Prob. of Emergency Messages-Scenario 8, Sender on Rd. A2

5.1.8.3 Reception Probability of Emergency Messages from OBU on B

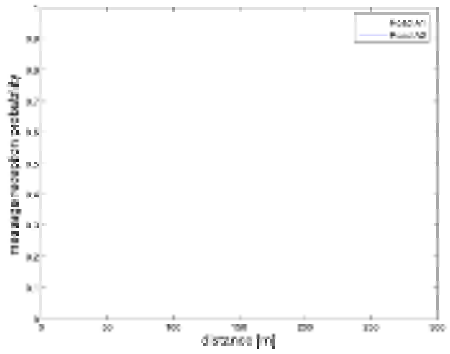


Figure 5-101: Reception Prob. of Emergency Messages – Scenario 8, Rd. A, Sender on Rd. B

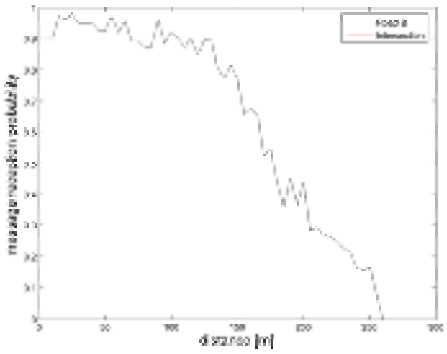


Figure 5-102: Reception Prob. of Emergency Messages – Scenario 8, Rd. B, Sender on Rd. B

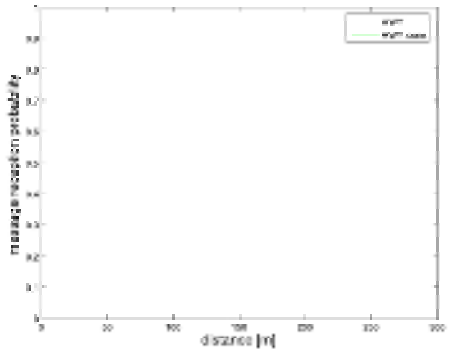


Figure 5-103: Reception Prob. of Emergency Messages – Scenario 8, HWY, Sender on Rd. B

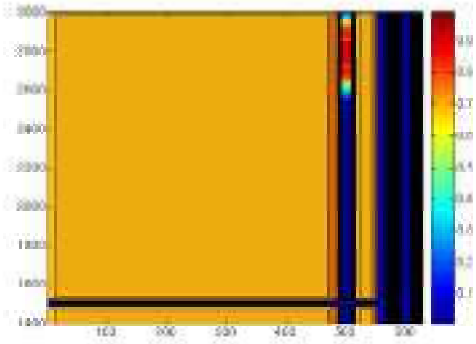


Figure 5-104: Reception Prob. of Emergency Messages-Scenario 8, Sender on Rd. B

5.1.8.4 Reception Probability of Emergency Messages from OBU on HWY

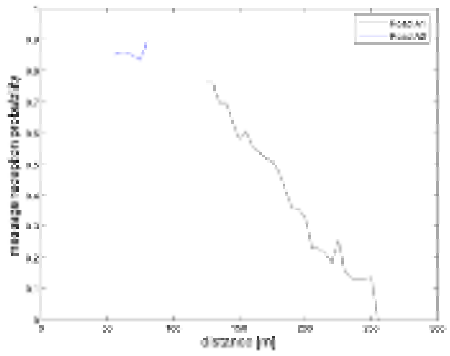


Figure 5-105: Reception Prob. of Emergency Messages – Scenario 8, Rd. A, Sender on HWY

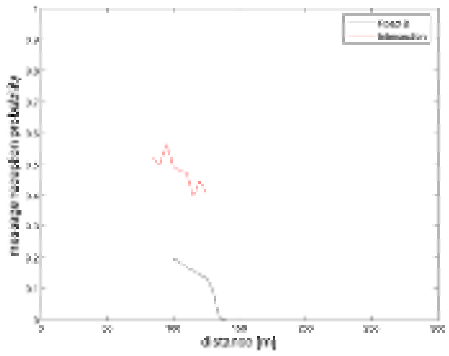


Figure 5-106: Reception Prob. of Emergency Messages – Scenario 8, Rd. B, Sender on HWY

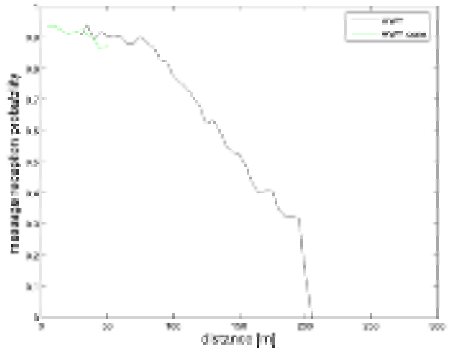


Figure 5-107: Reception Prob. of Emergency Messages – Scenario 8, HWY, Sender on HWY

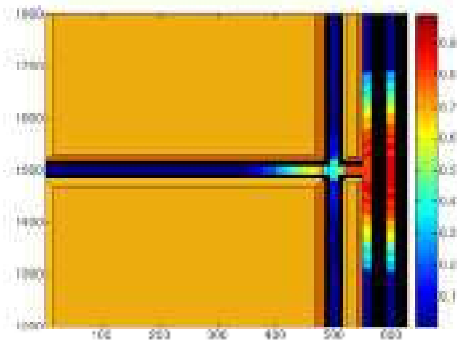


Figure 5-108: Reception Prob. of Emergency Messages-Scenario 8, Sender on HWY

5.1.9 Scenario 9

Simulation Scenario Settings:

RF Model	Distributed
Emergency Message Sender	RSU, 500 bytes/ 10Hz/200m
Corner Model	No buildings
Commercial RSU	On, 500 bytes/ 2Hz/ 200m
Routine Messages	200 bytes /10Hz /200m

5.1.9.1 Reception Probability of Emergency Messages

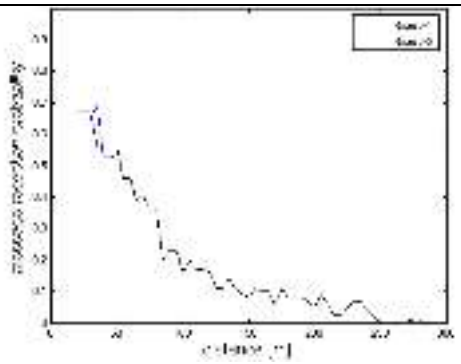


Figure 5-109: Reception Probability of Emergency Messages-Scenario 9, Road A, Sender RSU

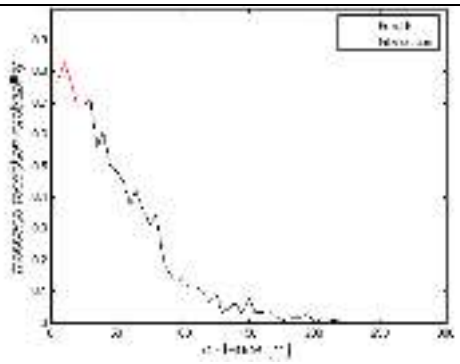


Figure 5-110: Reception Probability of Emergency Messages-Scenario 9, Road B, Sender RSU

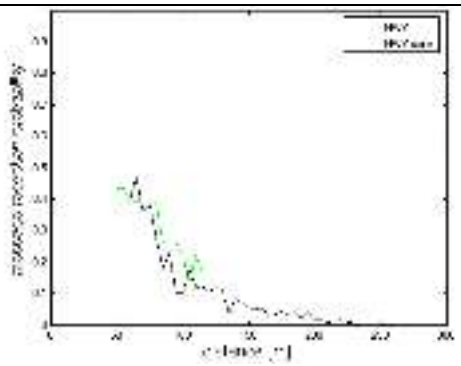


Figure 5-111: Reception Probability of Emergency Messages-Scenario 9, HWY, Sender RSU

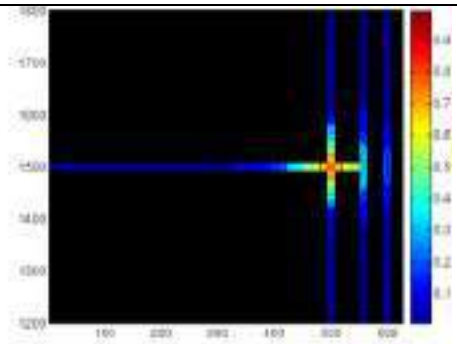


Figure 5-112: Reception Probability of Emergency Messages-Scenario 9, Sender RSU

5.1.9.2 Reception Probability of Routine Messages

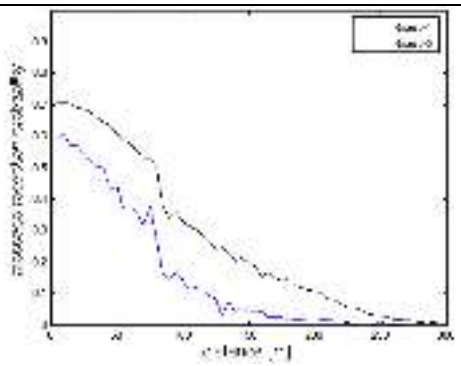


Figure 5-113: Reception Probability of Routine Messages on Road A, Scenario 9

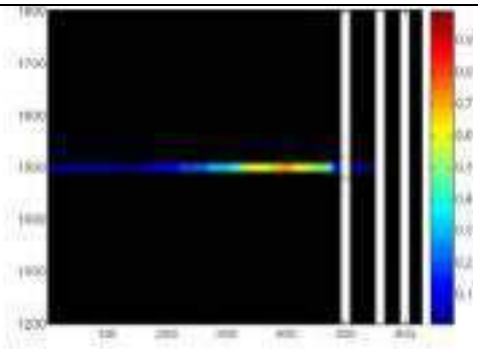


Figure 5-114: Reception Probability of Routine Messages on Road A, Scenario 9

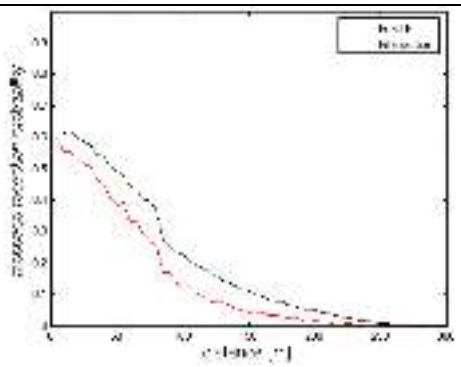


Figure 5-115: Reception Probability of Routine Messages on Road B, Scenario 9

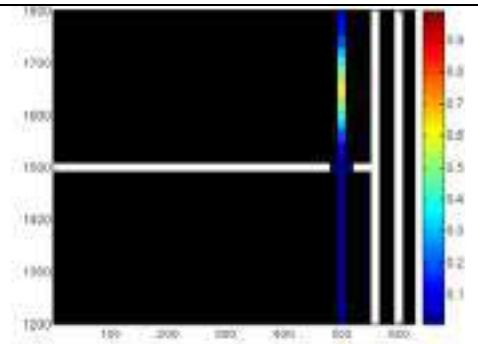


Figure 5-116: Reception Probability of Routine Messages on Road B, Scenario 9

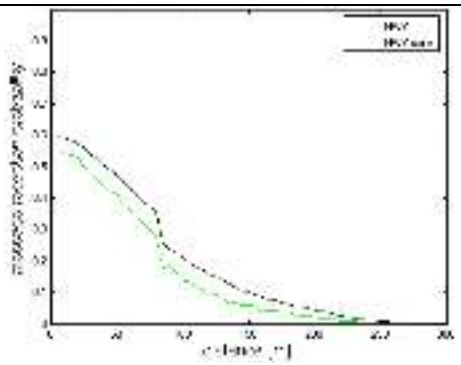


Figure 5-117: Reception Probability of Routine Messages on HWY, Scenario 9

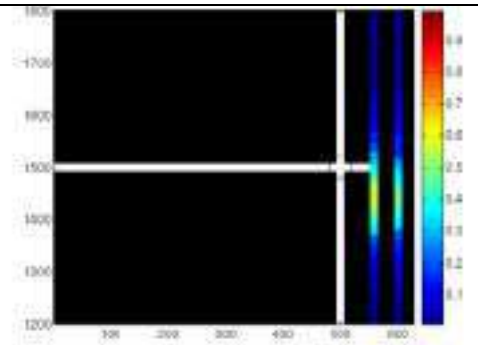


Figure 5-118: Reception Probability of Routine Messages on HWY, Scenario 9

5.1.10 Scenario 10

Simulation Scenario Settings:

RF Model	Distributed
Emergency Message Sender	RSU, 500 bytes/ 10Hz/200m
Corner Model	No buildings
Commercial RSU	OFF
Routine Messages	200byte /10Hz /200m

5.1.10.1 Reception Probability of Emergency Messages

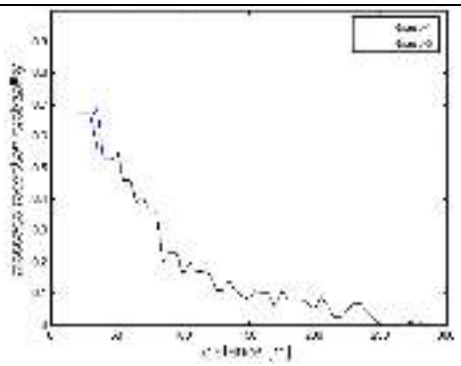


Figure 5-119: Reception Probability of Emergency Messages-Scenario 10, Road A, Sender RSU

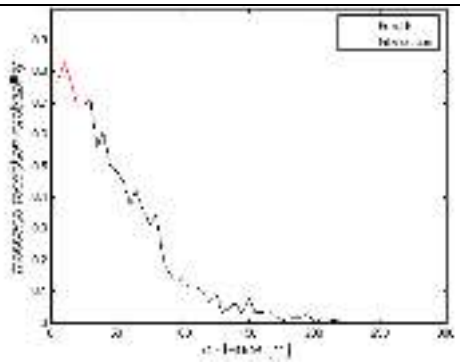


Figure 5-120: Reception Probability of Emergency Messages-Scenario 10, Road B, Sender RSU

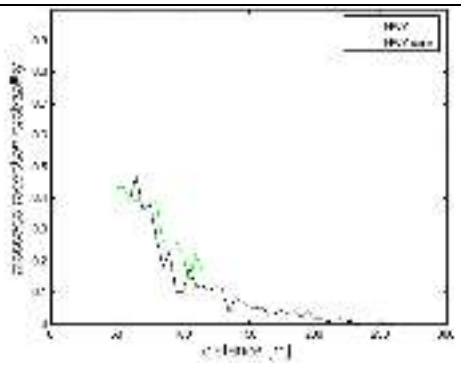


Figure 5-121: Reception Probability of Emergency Messages-Scenario 10, HWY, Sender RSU

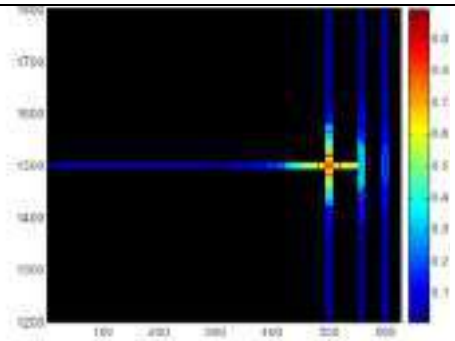


Figure 5-122: Reception Probability of Emergency Messages-Scenario 10, Sender RSU

5.1.10.2 Reception Probability of Routine Messages

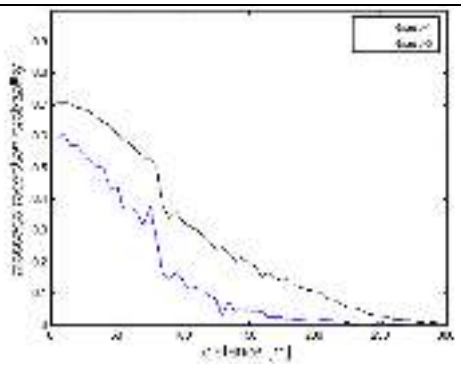


Figure 5-123: Reception Probability of Routine Messages on Road A, Scenario 10

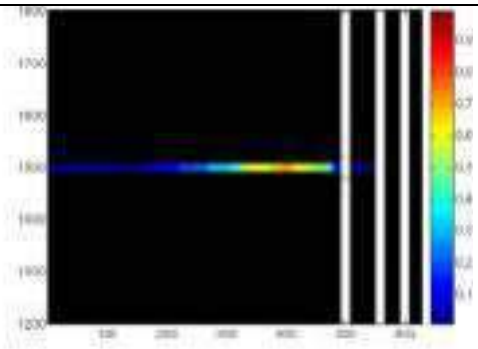


Figure 5-124: Reception Probability of Routine Messages on Road A, Scenario 10

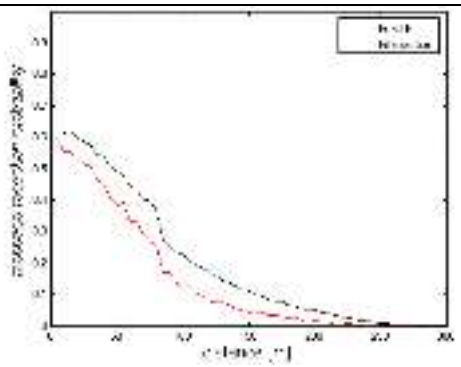


Figure 5-125: Reception Probability of Routine Messages on Road B, scenario 10

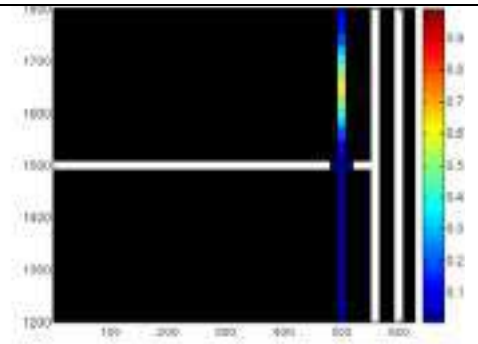


Figure 5-126: Reception Probability of Routine Messages on Road B, scenario 10

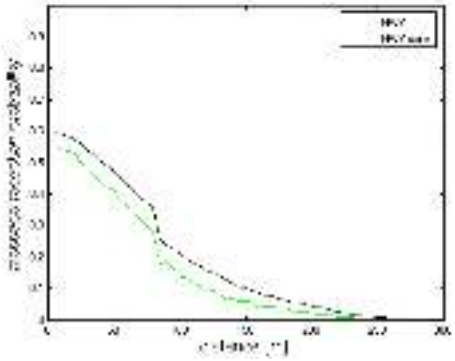


Figure 5-127: Reception Probability of Routine Messages on HWY, scenario 10

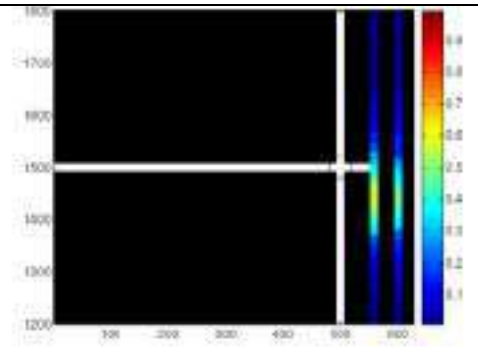


Figure 5-128: Reception Probability of Routine Messages on HWY, scenario 10

5.1.11 Scenario 11

Simulation Scenario Settings:

RF Model	Distributed
Emergency Message Sender	RSU, 500 bytes/ 10Hz/200m
Corner Model	Tall buildings
Commercial RSU	On, 500bytes/2Hz/200m
Routine Messages	200byte /10Hz /200m

5.1.11.1 Reception Probability of Emergency Messages

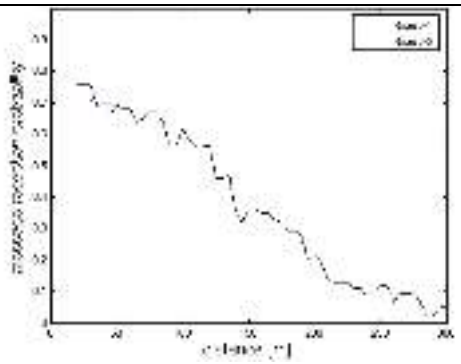


Figure 5-129: Reception Probability of Emergency Messages-Scenario 11, Road A, Sender RSU

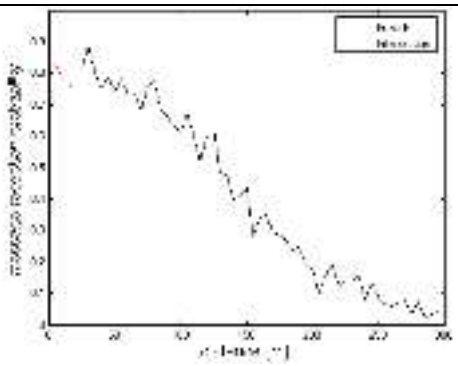


Figure 5-130: Reception Probability of Emergency Messages-Scenario 11, Road B, Sender RSU

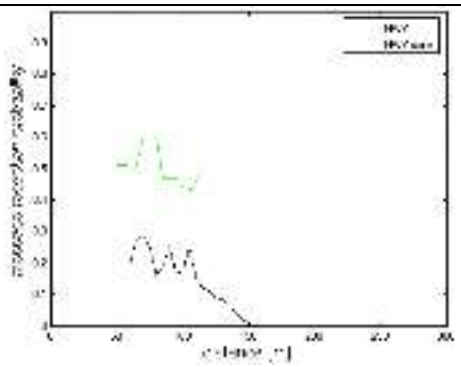


Figure 5-131: Reception Probability of Emergency Messages-Scenario 11, HWY, Sender RSU

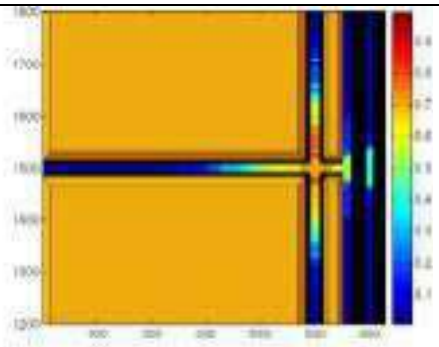


Figure 5-132: Reception Probability of Emergency Messages-Scenario11, Sender RSU

5.1.11.2 Reception Probability of Routine Messages

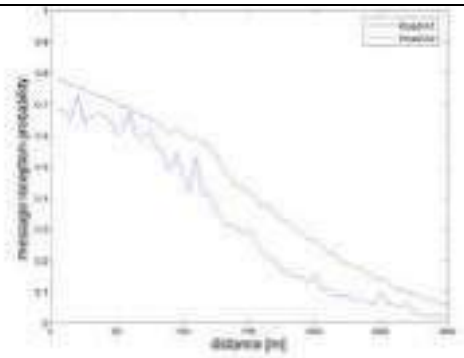


Figure 5-133: Reception Probability of Routine Messages on Road A, Scenario 11

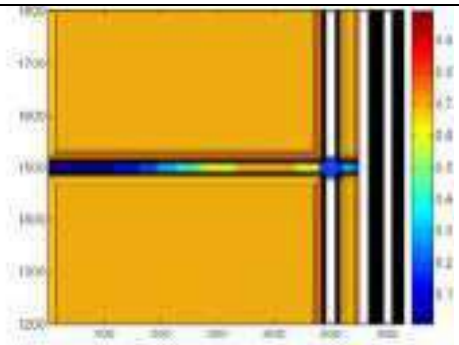


Figure 5-134: Reception Probability of Routine Messages on Road A, Scenario 11

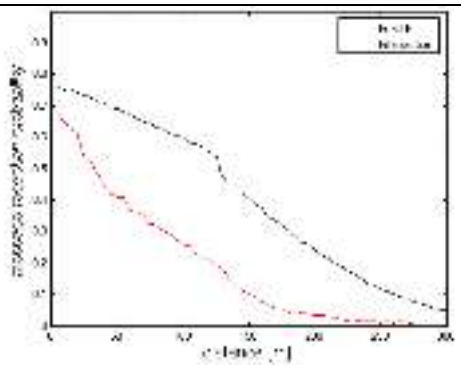


Figure 5-135: Reception Probability of Routine Messages on Road B, Scenario 11

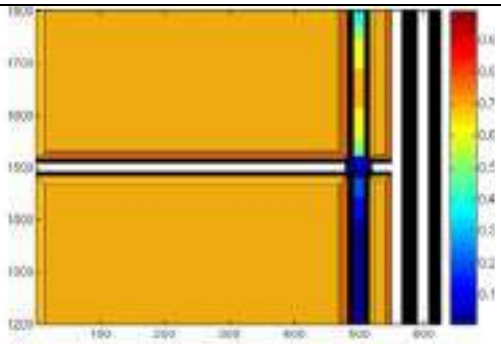


Figure 5-136: Reception Probability of Routine Messages on Road B, Scenario 11

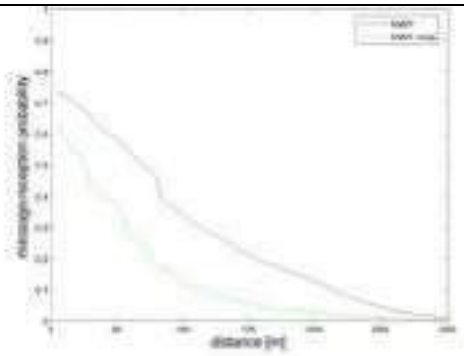


Figure 5-137: Reception Probability of Routine Messages on HWY, Scenario 11

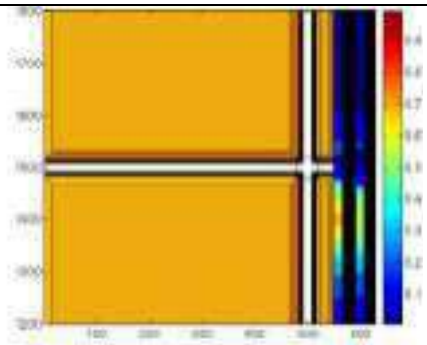


Figure 5-138: Reception Probability of Routine Messages on HWY, Scenario 11

5.1.12 Scenario 12

Simulation Scenario Settings:

RF Model	Distributed
Emergency Message Sender	RSU, 500 bytes/ 10Hz/200m
Corner Model	Tall buildings
Commercial RSU	OFF
Routine Messages	200byte /10Hz /200m

5.1.12.1 Reception Probability of Emergency Messages

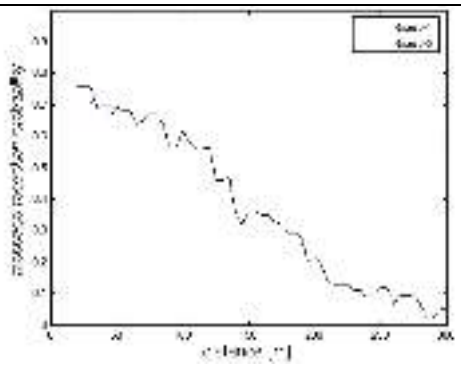


Figure 5-139: Reception Probability of Emergency Messages-Scenario12, Road A, Sender RSU

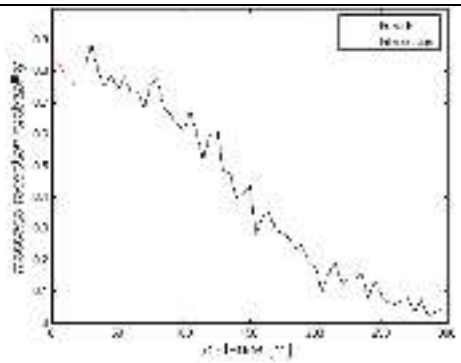


Figure 5-140: Reception Probability of Emergency Messages-Scenario12, Road B, Sender RSU

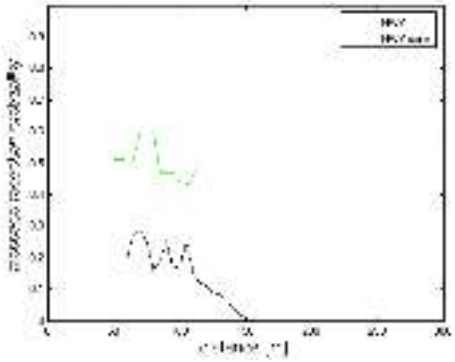


Figure 5-141: Reception Probability of Emergency Messages-Scenario12, HWY, Sender RSU

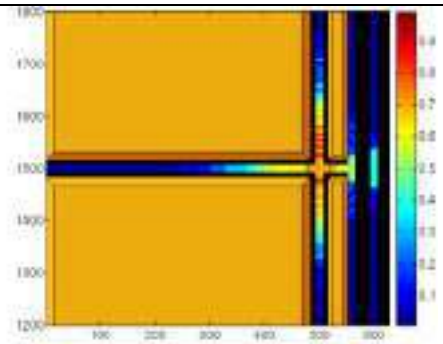


Figure 5-142: Reception Probability of Emergency Messages-Scenario12, Sender RSU

5.1.12.2 Reception Probability of Routine Messages

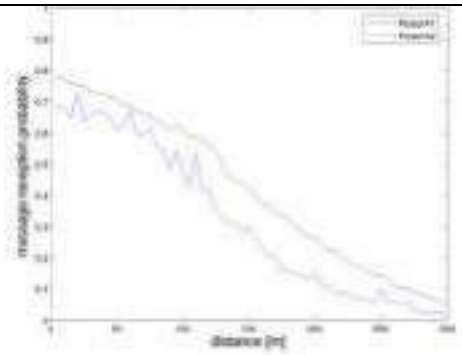


Figure 5-143: Reception Probability of Routine Messages on Road A, Scenario 12

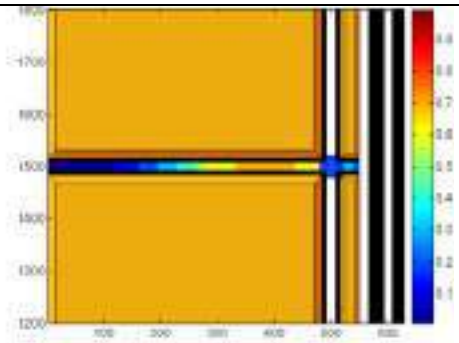


Figure 5-144: Reception Probability of Routine Messages on Road A, Scenario 12

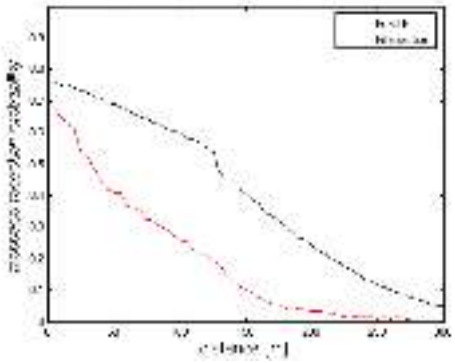


Figure 5-145: Reception Probability of Routine Messages on Road B, Scenario 12

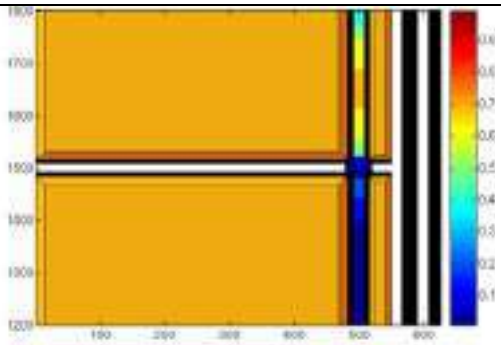


Figure 5-146: Reception Probability of Routine Messages on Road B, Scenario 12

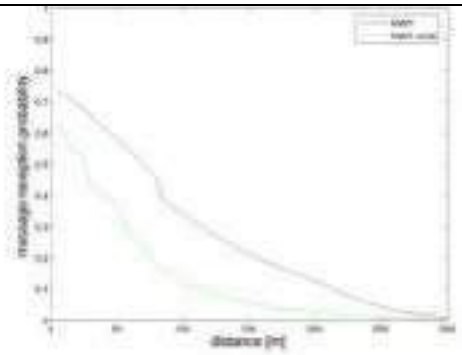


Figure 5-147: Reception Probability of Routine Messages on HWY, Scenario 12

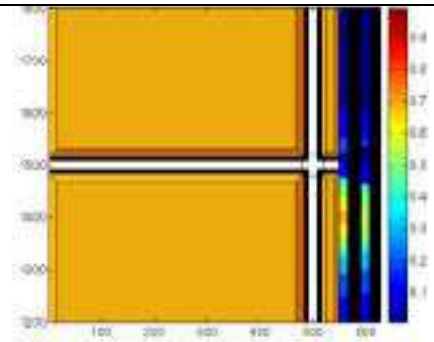


Figure 5-148: Reception Probability of Routine Messages on HWY, Scenario 12

5.1.13 Scenario 13

Simulation Scenario Setting:

RF Model	Distributed
Emergency Message Sender	OBUs on Road A1, A2, B 500 bytes/ 10Hz/200m on HWY 200 bytes/ 50Hz/200m
Corner Model	No building
Commercial RSU	On, 500bytes/ 2Hz/ 200m
Routine Messages	200byte /10Hz /200m

5.1.13.1 Reception Probability of Emergency Messages From OBU on A1

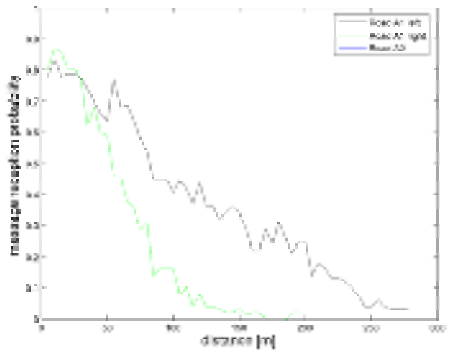


Figure 5-149: Reception Prob. of Emergency Messages – Scenario 13, Rd. A, Sender on Rd. A1

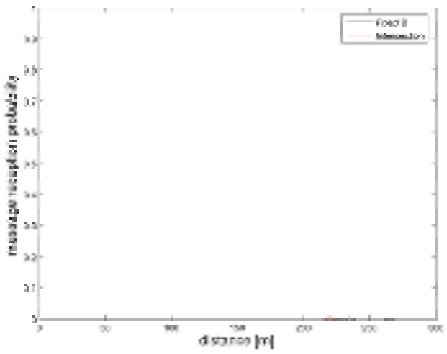


Figure 5-150: Reception Prob. of Emergency Messages – Scenario 13, Rd. B, Sender on Rd. A1

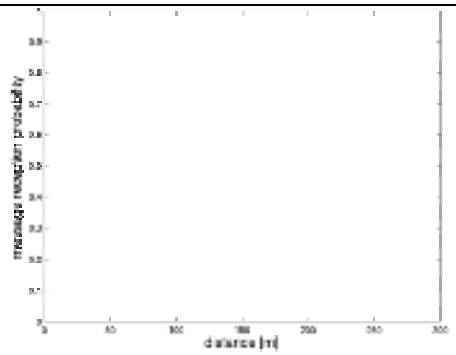


Figure 5-151: Reception Prob. of Emergency Messages – Scenario 13, HWY, Sender on Rd. A1

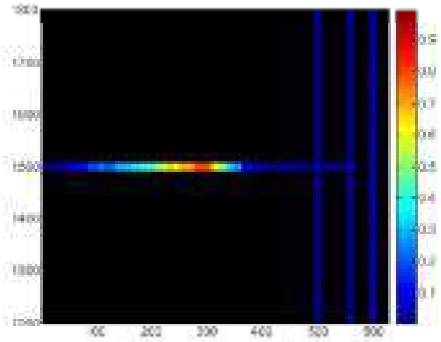


Figure 5-152: Reception Prob. of Emergency Messages-Scenario 13, Sender on Rd. A1

5.1.13.2 Reception Probability of Emergency Messages From OBU on A2

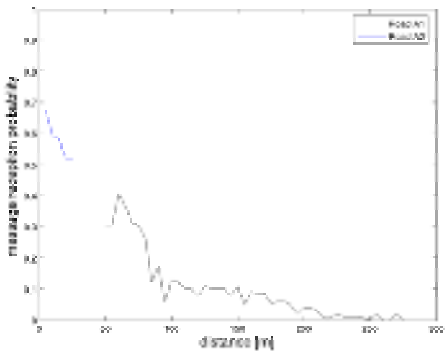


Figure 5-153: Reception Prob. of Emergency Messages – Scenario 13, Rd. A, Sender on Rd. A2

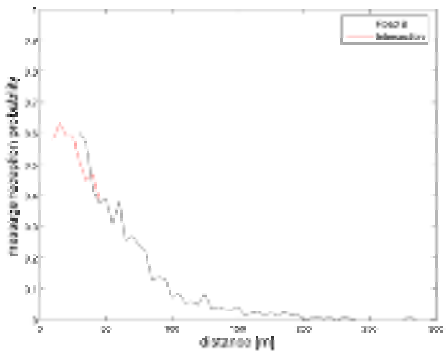


Figure 5-154: Reception Prob. of Emergency Messages – Scenario 13, Rd. B, Sender on Rd. A2

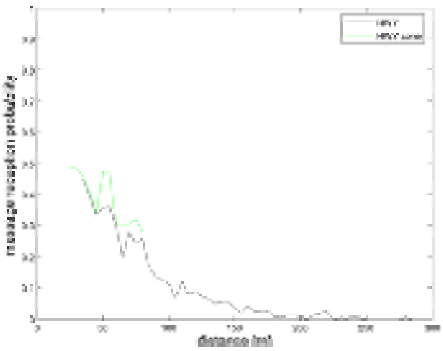


Figure 5-155: Reception Prob. of Emergency Messages – Scenario 13, HWY, Sender on Rd. A2

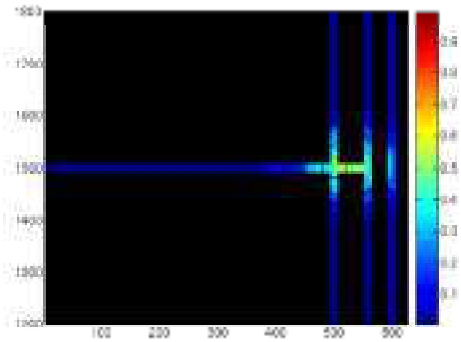


Figure 5-156: Reception Prob. of Emergency Messages-Scenario 13, Sender on Rd. A2

5.1.13.3 Reception Probability of Emergency MessagesFrom OBU on B

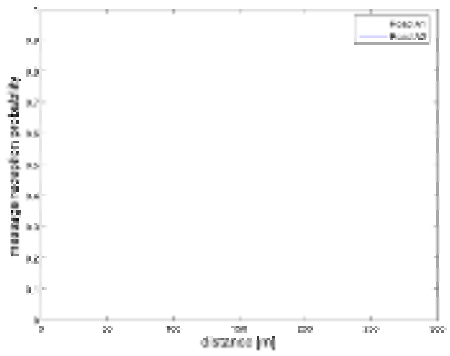


Figure 5-157: Reception Prob. of Emergency Messages – Scenario 13, Rd. A, Sender on Rd. B

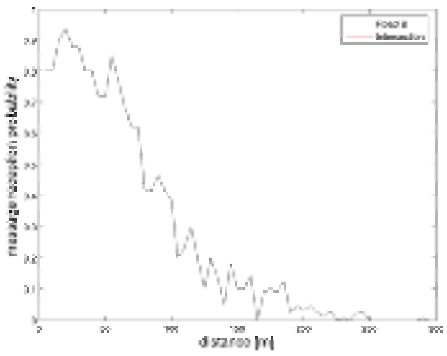


Figure 5-158: Reception Prob. of Emergency Messages – Scenario 13, Rd. B, Sender on Rd. B

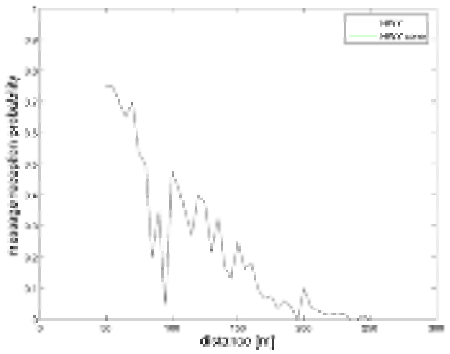


Figure 5-159: Reception Prob. of Emergency Messages – Scenario 13, HWY, Sender on Rd. B

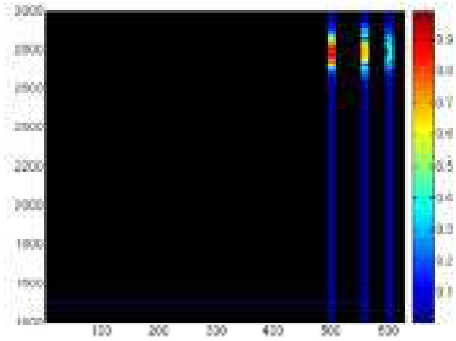


Figure 5-160: Reception Prob. of Emergency Messages-Scenario 13, Sender on Rd. B

5.1.13.4 Reception Probability of Emergency Messages From OBU on HWY

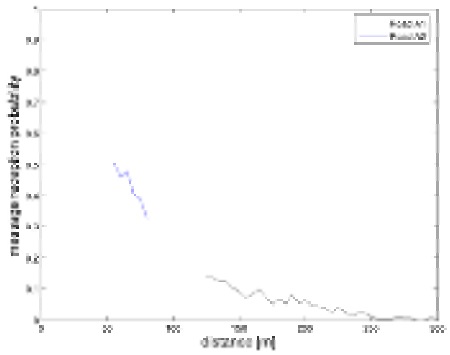


Figure 5-161: Reception Prob. of Emergency Messages - Scenario 13, Rd. A, Sender on HWY

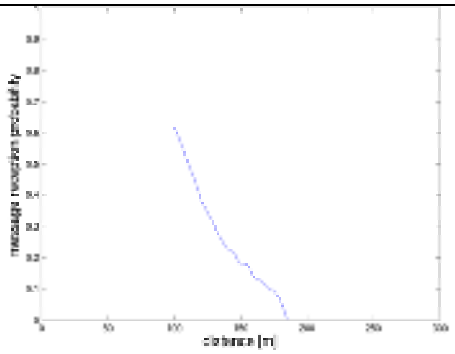


Figure 5-162: Reception Prob. of Emergency Messages - Scenario13, Rd. B, Sender on HWY

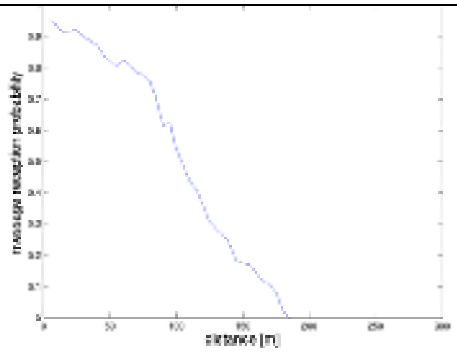


Figure 5-163: Reception Prob. of Emergency Messages - Scenario13, HWY, Sender on HWY

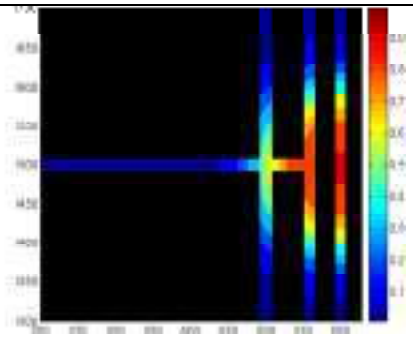


Figure 5-164: Reception Prob. of Emergency Messages-Scenario 13, Sender on HWY

5.1.14 Scenario 14

Simulation Scenario Setting:

RF Model	Distributed
Emergency Message Sender	OBUs on Road A1, A2, B 500 bytes/ 10Hz/200m on HWY 200 bytes/ 50Hz/200m
Corner Model	No building
Commercial RSU	OFF
Routine Messages	200byte /10Hz /200m

5.1.14.1 Reception Probability of Emergency Messages From OBU on A1

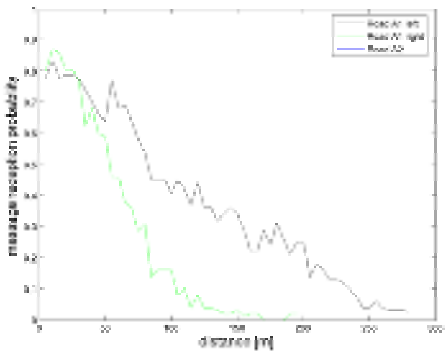


Figure 5-165: Reception Prob. of Emergency Messages - Scenario14, Rd. A, Sender on Rd. A1

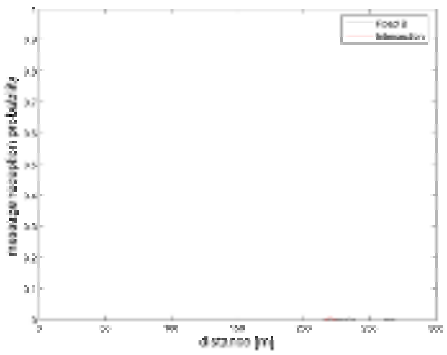


Figure 5-166: Reception Prob. of Emergency Messages - Scenario14, Rd. B, Sender on Rd. A1

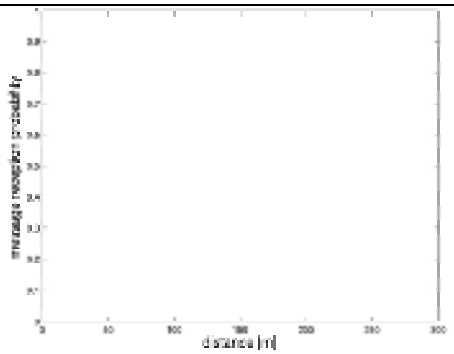


Figure 5-167: Reception Prob. of Emergency Messages - Scenario14, HWY, Sender on Rd. A1

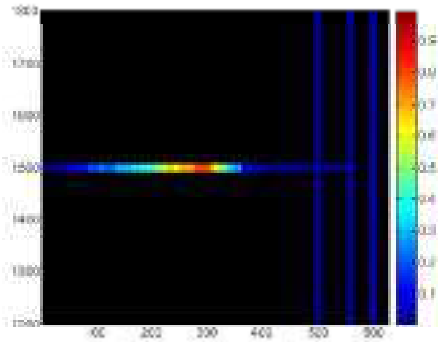


Figure 5-168: Reception Prob. of Emergency Messages-Scenario 14, Sender on Rd. A1

5.1.14.2 Reception Probability of Emergency Messages From OBU on A2

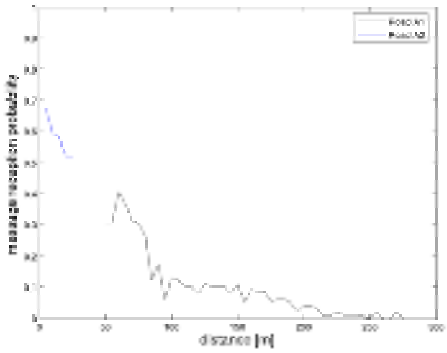


Figure 5-169: Reception Prob. of Emergency Messages - Scenario14, Rd. A, Sender on Rd. A2

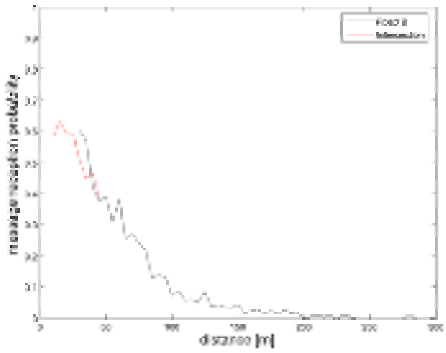


Figure 5-170: Reception Prob. of Emergency Messages - Scenario14, Rd. B, Sender on Rd. A2

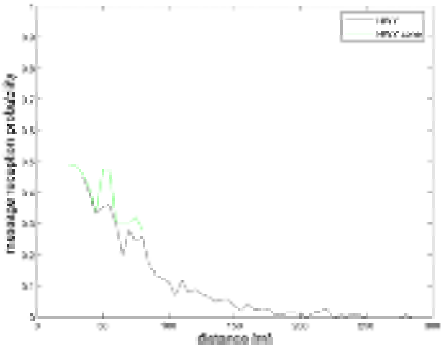


Figure 5-171: Reception Prob. of Emergency Messages - Scenario14, HWY, Sender on Rd. A2

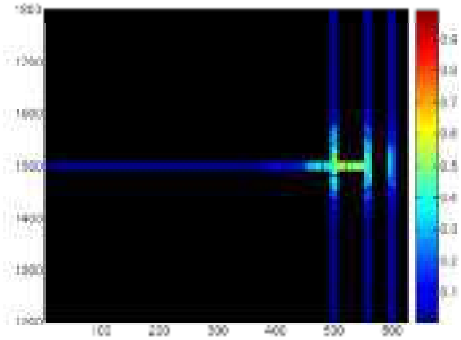


Figure 5-172: Reception Prob. of Emergency Messages-Scenario 14, Sender on Rd. A2

5.1.14.3 Reception Probability of Emergency Messages from OBU on B

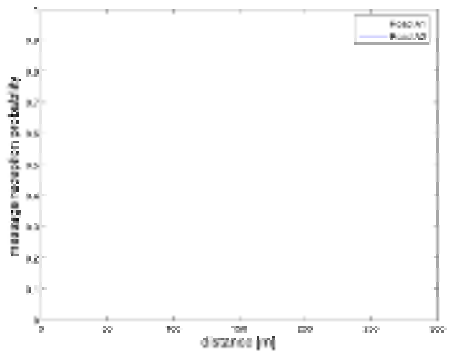


Figure 5-173: Reception Prob. of Emergency Messages - Scenario14, Rd. A, Sender on Rd. B

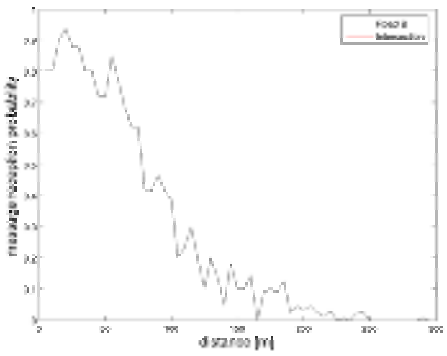


Figure 5-174: Reception Prob. of Emergency Messages - Scenario14, Rd. B, Sender on Rd. B

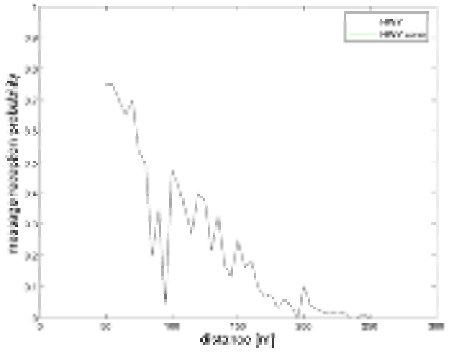


Figure 5-175: Reception Prob. of Emergency Messages - Scenario14, HWY, Sender on Rd. B

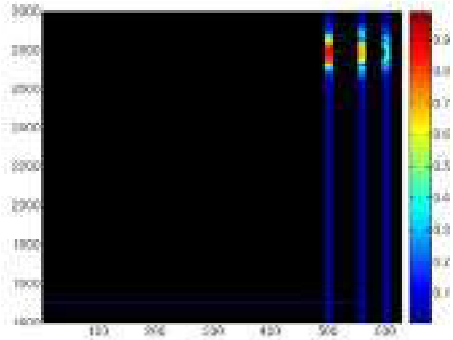


Figure 5-176: Reception Prob. of Emergency Messages-Scenario 14, Sender on Rd. B

5.1.14.4 Reception Probability of Emergency Messages From OBU on HWY

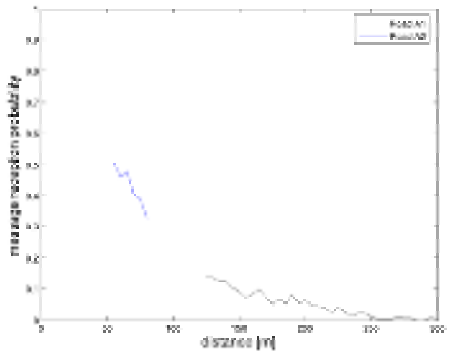


Figure 5-177: Reception Prob. of Emergency Messages - Scenario14, Rd. A, Sender on HWY

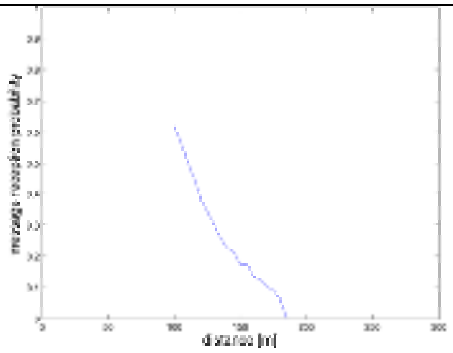


Figure 5-178: Reception Prob. of Emergency Messages - Scenario14, Rd. B, Sender on HWY

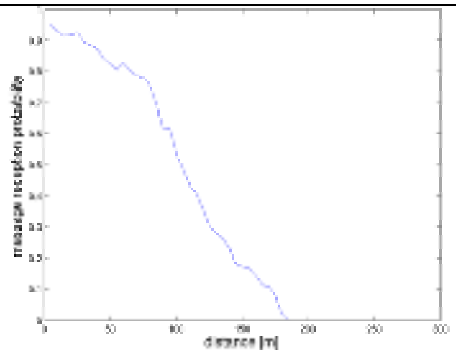


Figure 5-179: Reception Prob. of Emergency Messages - Scenario14, HWY, Sender on HWY

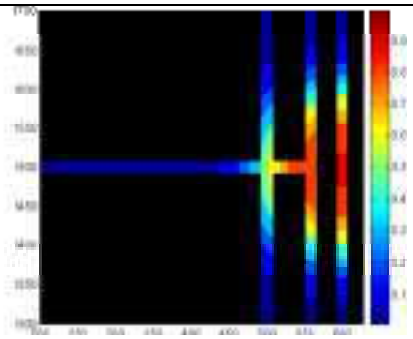


Figure 5-180: Reception Prob. of Emergency Messages-Scenario 14, Sender on HWY

5.1.15 Scenario 15

Simulation Scenario Setting:

RF Model	Distributed
Emergency Message Sender	OBUs on Road A1, A2, B 500 bytes/ 10Hz/200m on HWY 200 bytes/ 50Hz/200m
Corner Model	Tall building
Commercial RSU	On, 500bytes/ 2Hz/ 200m
Routine Messages	200byte /10Hz /200m

5.1.15.1 Reception Probability of Emergency Msgs From OBU on A1

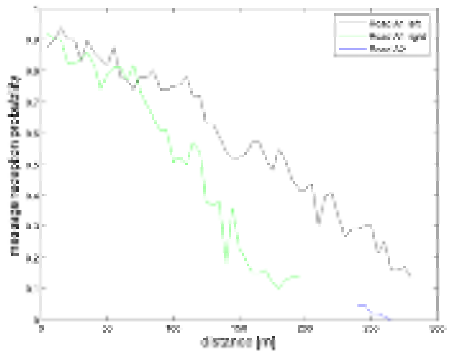


Figure 5-181: Reception Prob. of Emergency Messages - Scenario15, Rd. A, Sender on Rd. A1

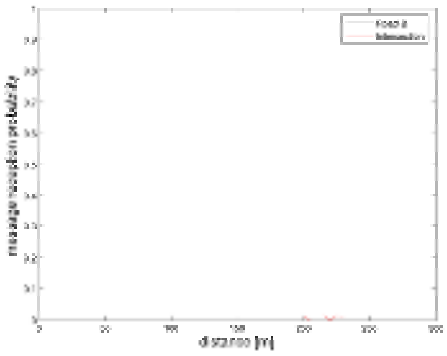


Figure 5-182: Reception Prob. of Emergency Messages - Scenario15, Rd. B, Sender on Rd. A1

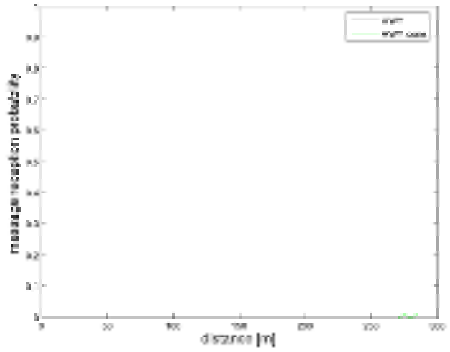


Figure 5-183: Reception Prob. of Emergency Messages - Scenario15, HWY, Sender on Rd. A1

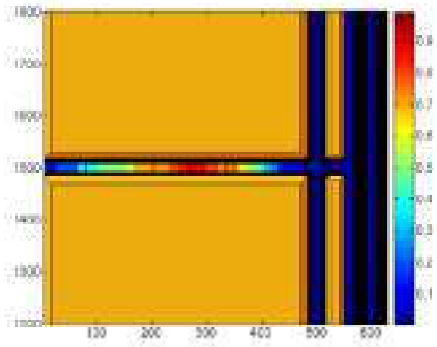


Figure 5-184: Reception Prob. of Emergency Messages-Scenario 15, Sender on Rd. A1

5.1.15.2 Reception Probability of Emergency Messages From OBU on A2

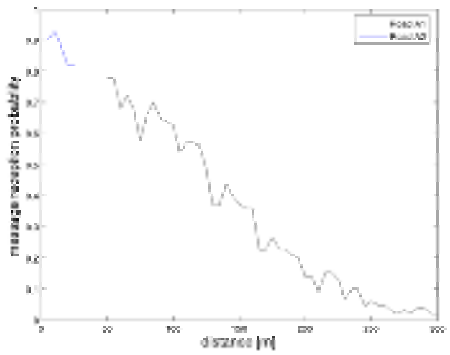


Figure 5-185: Reception Prob. of Emergency Messages - Scenario15, Rd. A, Sender on Rd. A2

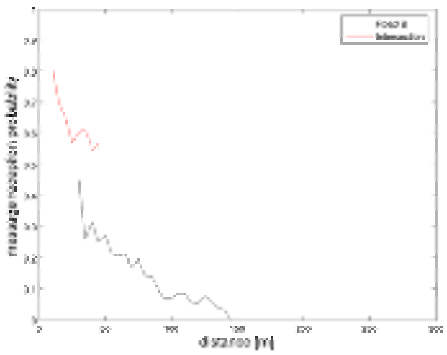


Figure 5-186: Reception Prob. of Emergency Messages - Scenario15, Rd. B, Sender on Rd. A2

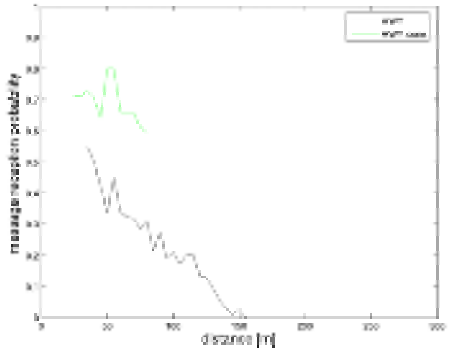


Figure 5-187: Reception Prob. of Emergency Messages - Scenario15, HWY, Sender on Rd. A2

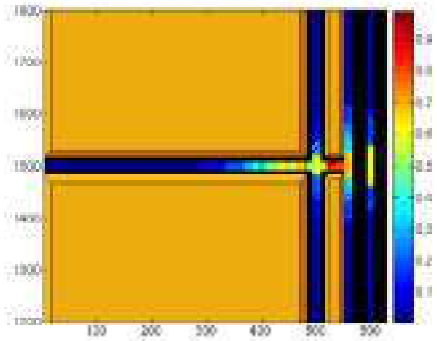


Figure 5-188: Reception Prob. of Emergency Messages-Scenario 15, Sender on Rd. A2

5.1.15.3 Reception Probability of Emergency Messages From OBU on B

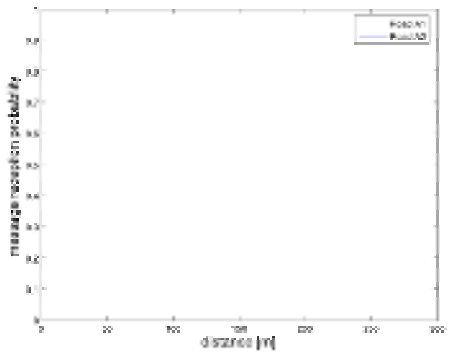


Figure 5-189: Reception Prob. of Emergency Messages - Scenario15, Rd. A, Sender on Rd. B

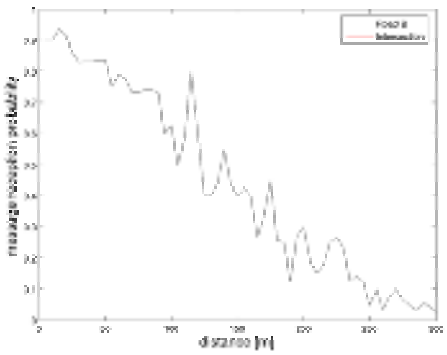


Figure 5-190: Reception Prob. of Emergency Messages - Scenario15, Rd. B, Sender on Rd. B

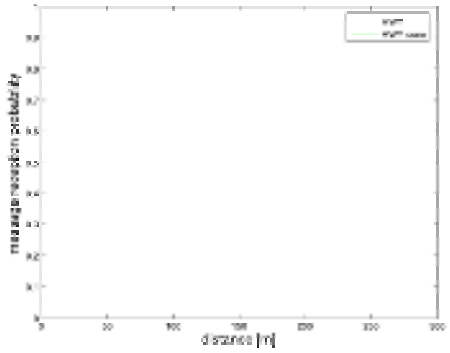


Figure 5-191: Reception Prob. of Emergency Messages - Scenario15, HWY, Sender on Rd. B

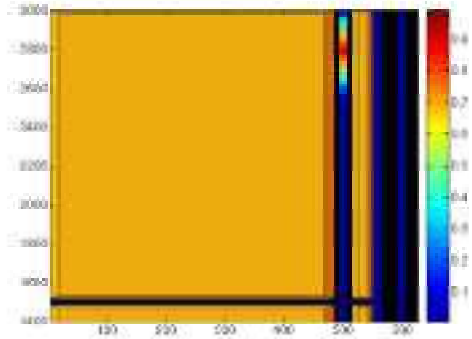


Figure 5-192: Reception Prob. of Emergency Messages-Scenario 15, Sender on Rd. B

5.1.15.4 Reception Probability of Emergency Messages From OBU on HWY

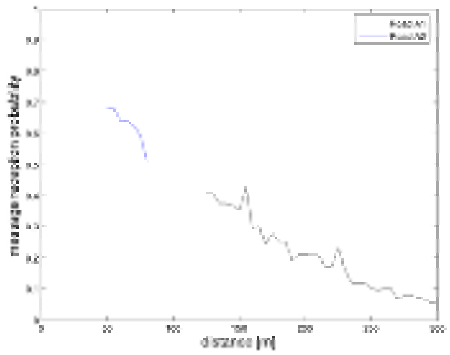


Figure 5-193: Reception Prob. of Emergency Messages - Scenario15, Rd. A, Sender on HWY

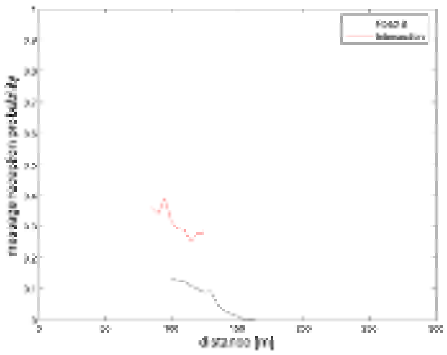


Figure 5-194: Reception Prob. of Emergency Messages - Scenario15, Rd. B, Sender on HWY

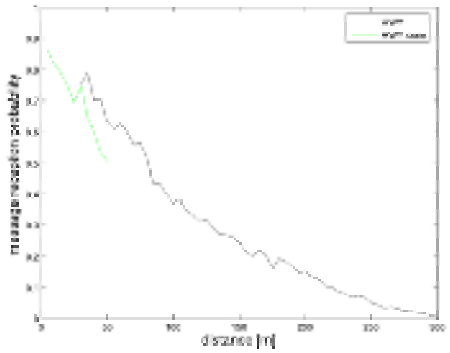


Figure 5-195: Reception Prob. of Emergency Messages - Scenario15, HWY, Sender on HWY

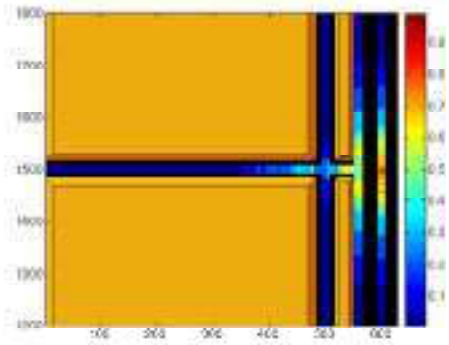


Figure 5-196: Reception Prob. of Emergency Messages-Scenario 15, Sender on HWY

5.1.16 Scenario 16

Simulation Scenario Setting:

RF Model	Distributed
Emergency Message Sender	OBUs on Road A1, A2, B 500 bytes/ 10Hz/200m on HWY 200 bytes/ 50Hz/200m
Corner Model	Tall building
Commercial RSU	OFF
Routine Messages	200byte /10Hz /200m

5.1.16.1 Reception Probability of Emergency Messages From OBU on A1

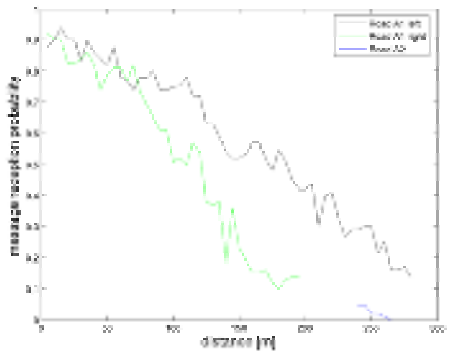


Figure 5-197: Reception Prob. of Emergency Messages - Scenario16, Rd. A, Sender on Rd. A1

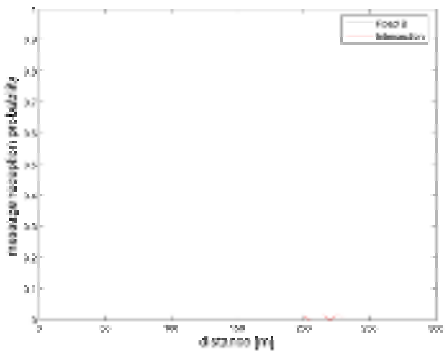


Figure 5-198: Reception Prob. of Emergency Messages - Scenario16, Rd. B, Sender on Rd. A1

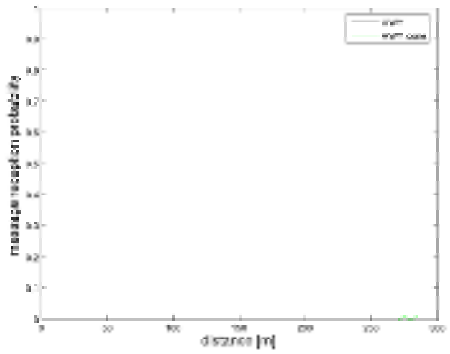


Figure 5-199: Reception Prob. of Emergency Messages - Scenario16, HWY, Sender on Rd. A1

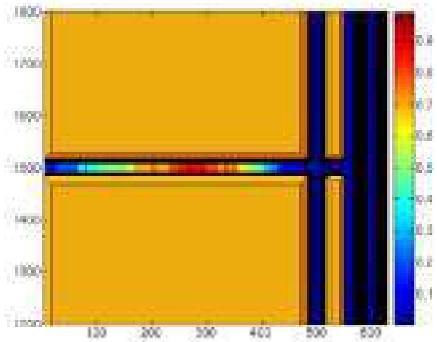


Figure 5-200: Reception Prob. of Emergency Messages-Scenario 16, Sender on Rd. A1

5.1.16.2 Reception Probability of Emergency Messages From OBU on A2

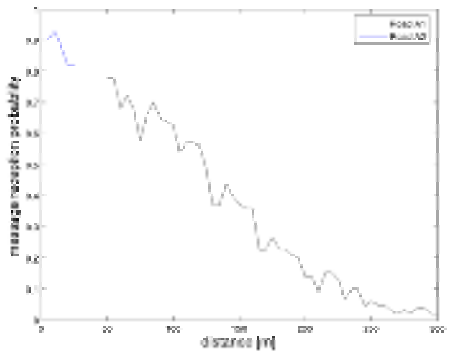


Figure 5-201: Reception Prob. of Emergency Messages - Scenario16, Rd. A, Sender on Rd. A2

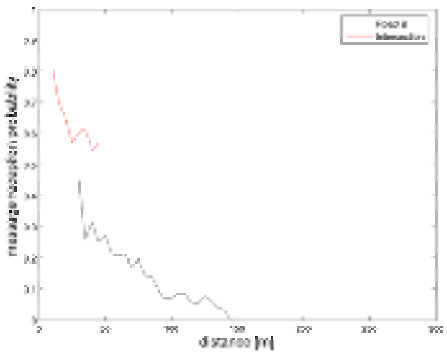


Figure 5-202: Reception Prob. of Emergency Messages - Scenario16, Rd. B, Sender on Rd. A2

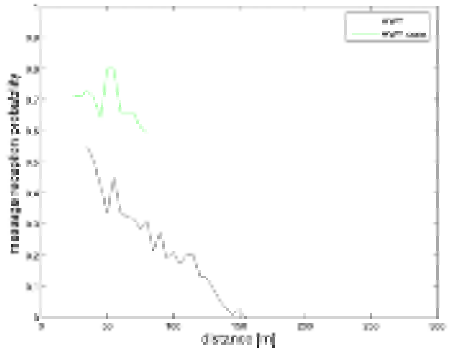


Figure 5-203: Reception Prob. of Emergency Messages - Scenario16, HWY, Sender on Rd. A2

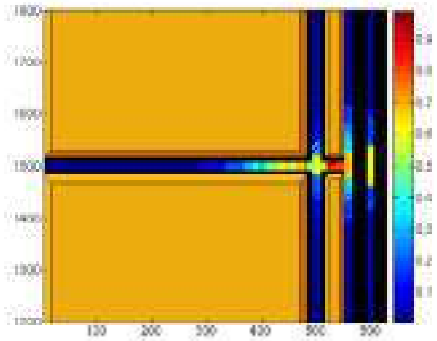


Figure 5-204: Reception Prob. of Emergency Messages-Scenario 16, Sender on Rd. A2

5.1.16.3 Reception Probability of Emergency Messages From OBU on B

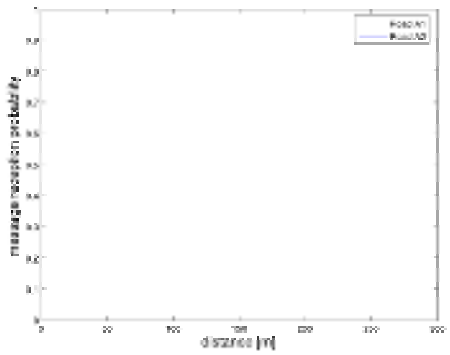


Figure 5-205: Reception Prob. of Emergency Messages - Scenario16, Rd. A, Sender on Rd. B

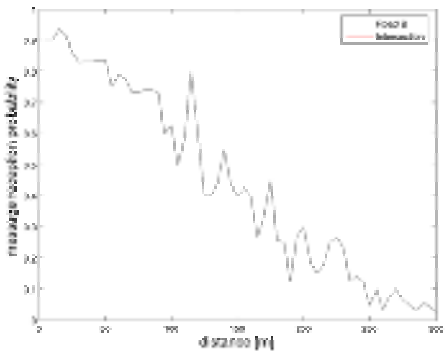


Figure 5-206: Reception Prob. of Emergency Messages - Scenario16, Rd. B, Sender on Rd. B

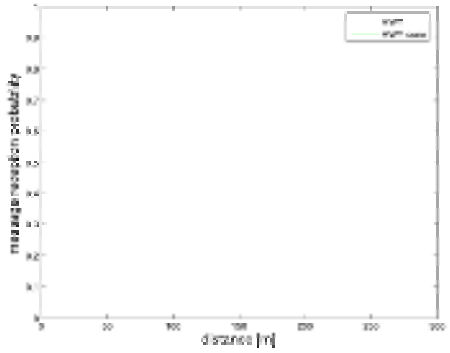


Figure 5-207: Reception Prob. of Emergency Messages - Scenario16, HWY, Sender on Rd. B

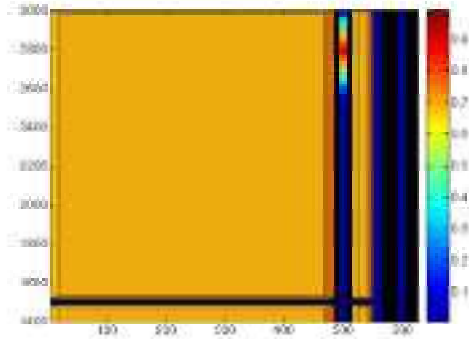


Figure 5-208: Reception Prob. of Emergency Messages-Scenario 16, Sender on Rd. B

5.1.16.4 Reception Probability of Emergency Messages From OBU on HWY

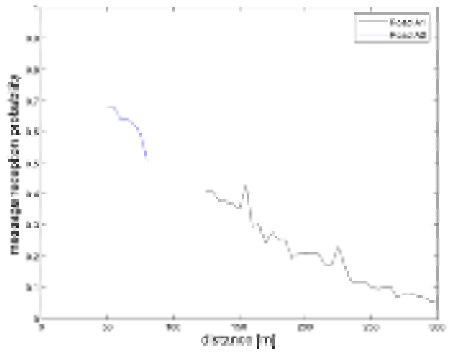


Figure 5-209: Reception Prob. of Emergency Messages - Scenario16, Rd. A, Sender on HWY

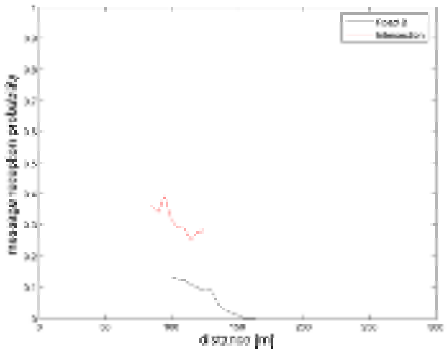


Figure 5-210: Reception Prob. of Emergency Messages - Scenario16, Rd. B, Sender on HWY

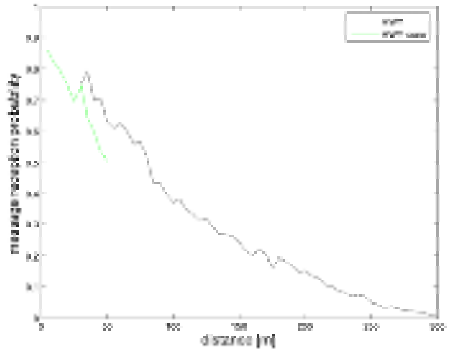


Figure 5-211: Reception Prob. of Emergency Messages - Scenario16, HWY, Sender on HWY

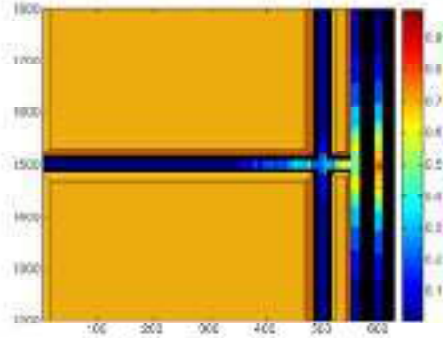


Figure 5-212: Reception Prob. of Emergency Messages-Scenario 16, Sender on HWY

5.2 Batch 2, Routine and Emergency Safety Messaging in Less Stressful Channel

5.2.1 Scenario 17

Simulation Scenario Setting:

RF Model	Distributed
Emergency Message Sender	RSU, 10Hz/ 500 bytes/ 200m
Corner Model	no buildings
Pt	200m coverage
Routine Message Frequency	2Hz

5.2.1.1 Reception Probability of Emergency Messages

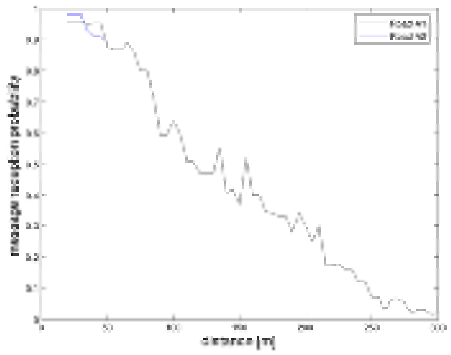


Figure 5-213: Reception Probability of Emergency Messages-Scenario17, Road A, Sender RSU

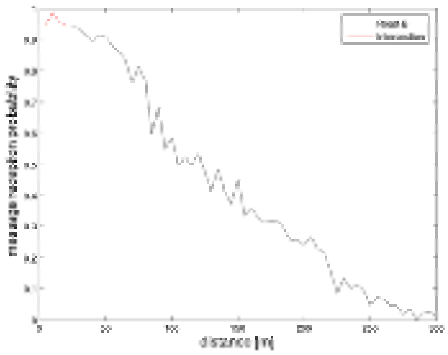


Figure 5-214: Reception Probability of Emergency Messages-Scenario17, Road B, Sender RSU

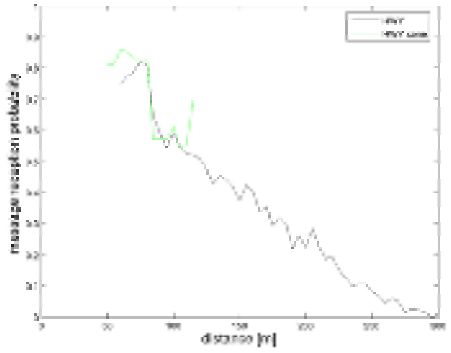


Figure 5-215: Reception Probability of Emergency Messages-Scenario17, HWY, Sender RSU

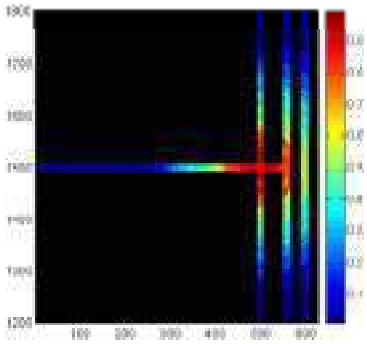


Figure 5-216: Reception Probability of Emergency Messages-Scenario17, Sender RSU

5.2.1.2 Reception Probability of Routine Messages

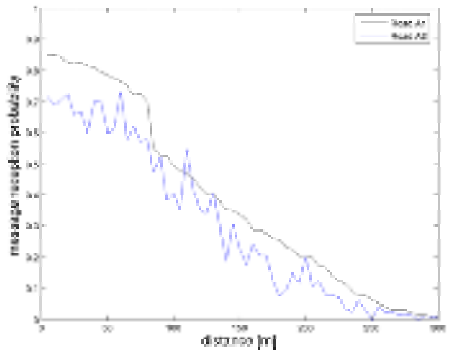


Figure 5-217: Reception Probability of Routine Messages on Road A, Scenario17

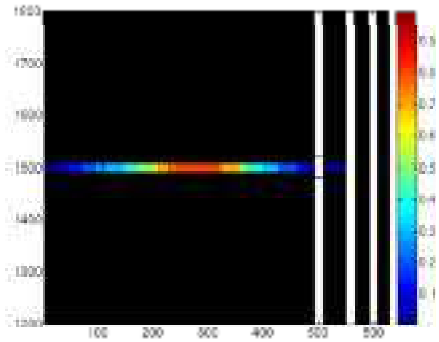


Figure 5-218: Reception Probability of Routine Messages on Road A, Scenario 17

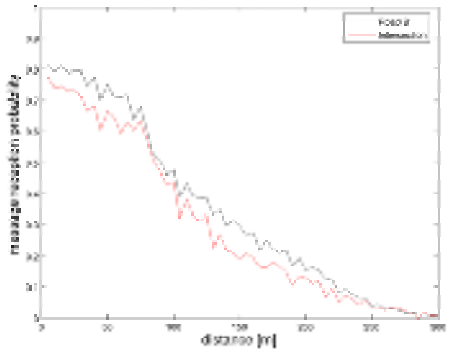


Figure 5-219: Reception Probability of Routine Messages on Road B, Scenario17

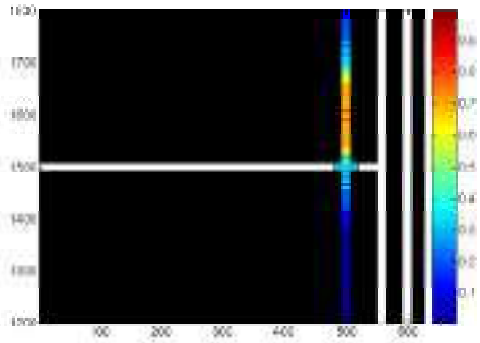


Figure 5-220: Reception Probability of Routine Messages on Road B, Scenario 17

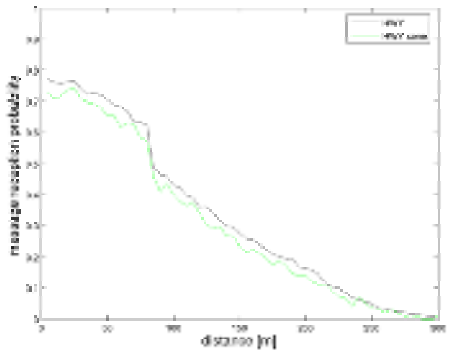


Figure 5-221: Reception Probability of Routine Messages on HWY, Scenario17

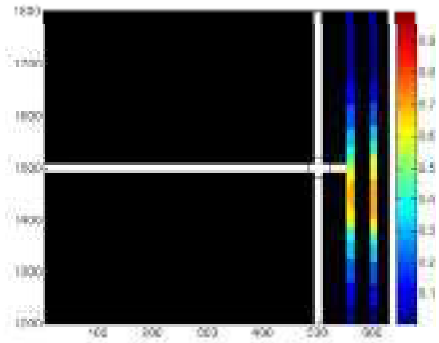


Figure 5-222: Reception Probability of Routine Messages on HWY, Scenario 17

5.2.2 Scenario 18

Simulation Scenario Setting:

RF Model	Distributed
Emergency Message Sender	OBUs on Road A1, A2, B and HWY
Corner Model	no building
Pt	200m coverage
Routine Message Frequency	2Hz

5.2.2.1 Reception Probability of Emergency Messages From OBU on A1

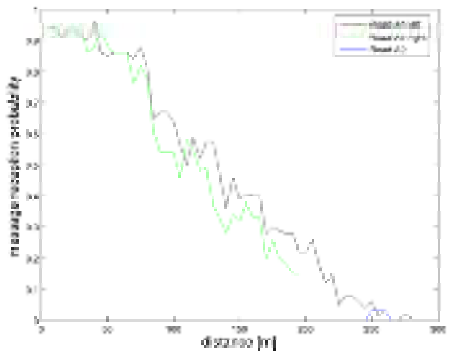


Figure 5-223: Reception Prob. of Emergency Messages - Scenario18, Rd. A, Sender on Rd. A1

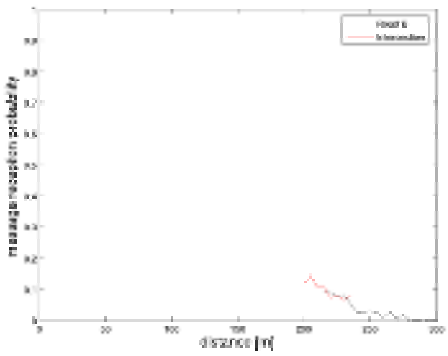


Figure 5-224: Reception Prob. of Emergency Messages - Scenario18, Rd. B, Sender on Rd. A1

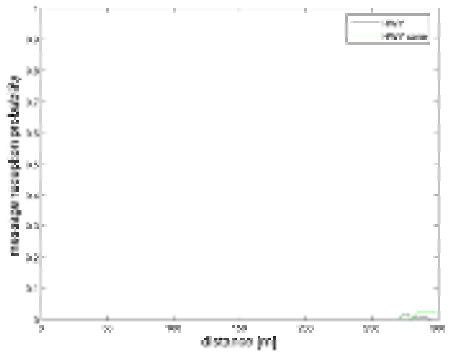


Figure 5-225: Reception Prob. of Emergency Messages - Scenario18, HWY, Sender on Rd. A1

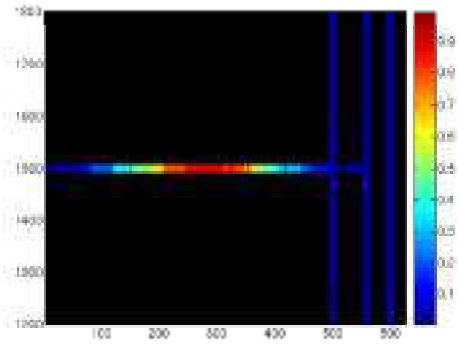


Figure 5-226: Reception Prob. of Emergency Messages-Scenario 18, Sender on Rd. A1

5.2.2.2 Reception Probability of Emergency Messages From OBU on A2

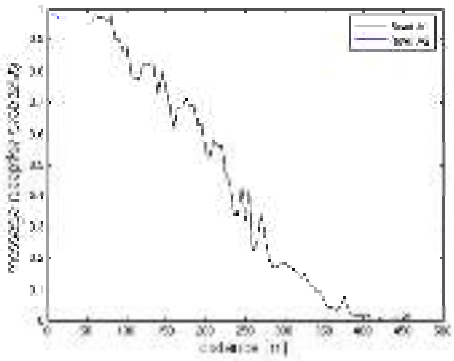


Figure 5-227: Reception Prob. of Emergency Messages – Scenario 18, Rd. A, Sender on Rd. A2

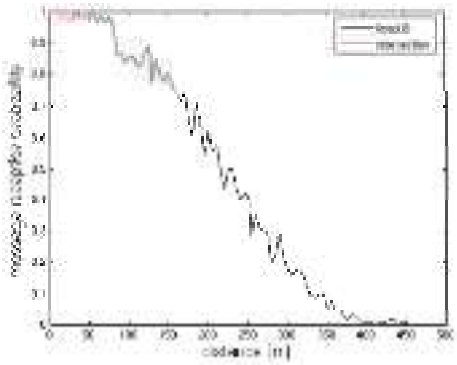


Figure 5-228: Reception Prob. of Emergency Messages - Scenario18, Rd. B, Sender on Rd. A2

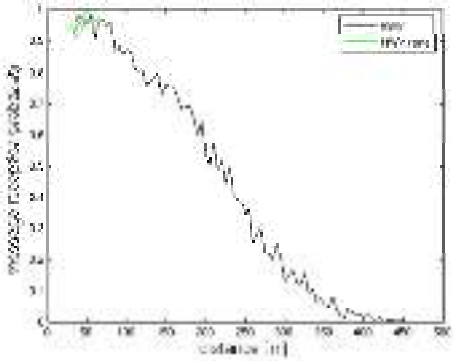


Figure 5-229: Reception Prob. of Emergency Messages – Scenario 18, HWY, Sender on Rd. A2

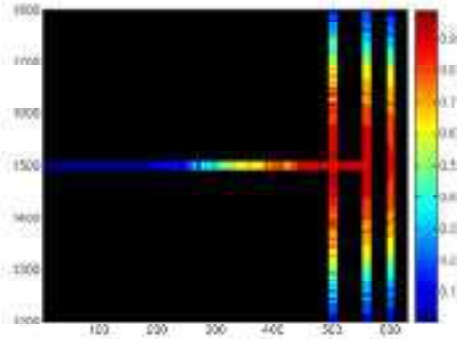


Figure 5-230: Reception Prob. of Emergency Messages-Scenario 18, Sender on Rd. A2

5.2.2.3 Reception Probability of Emergency Messages From OBU on B

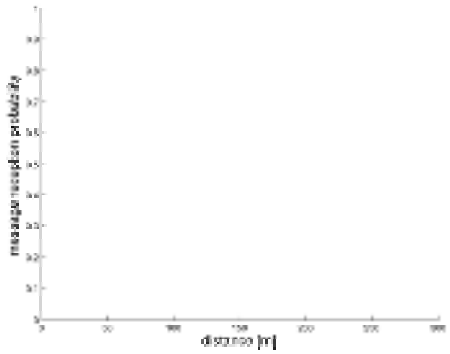


Figure 5-231: Reception Prob. of Emergency Messages - Scenario18, Rd. A, Sender on Rd. B

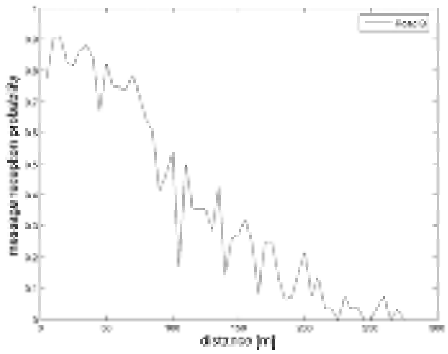


Figure 5-232: Reception Prob. of Emergency Messages - Scenario18, Rd. B, Sender on Rd. B

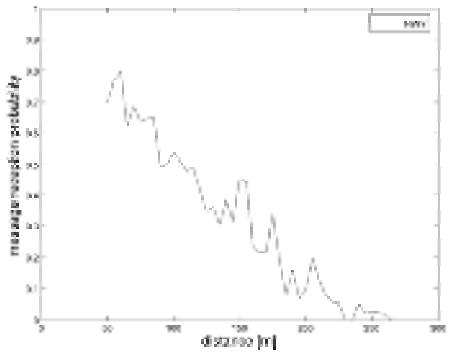


Figure 5-233: Reception Prob. of Emergency Messages - Scenario18, HWY, Sender on Rd. B

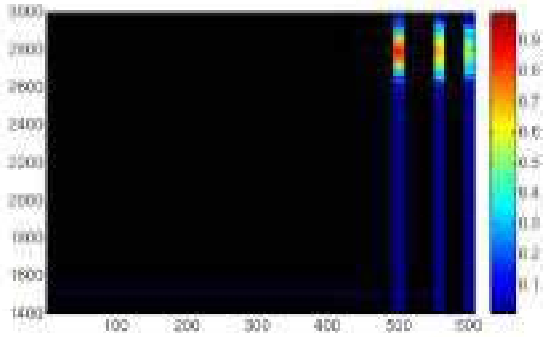


Figure 5-234: Reception Prob. of Emergency Messages-Scenario 18, Sender on Rd. B

5.2.2.4 Reception Probability of Emergency Messages From OBU on HWY

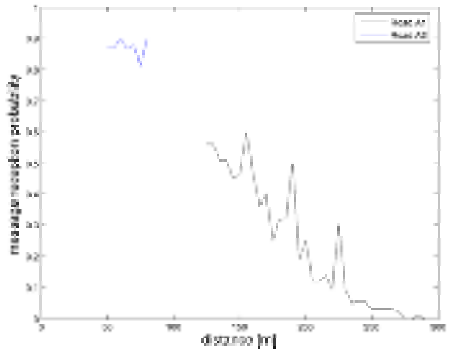


Figure 5-235: Reception Prob. of Emergency Messages - Scenario18, Rd. A, Sender on HWY

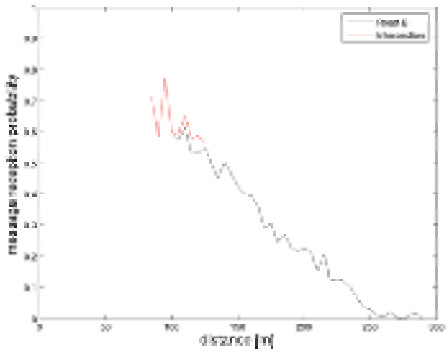


Figure 5-236: Reception Prob. of Emergency Messages - Scenario18, Rd. B, Sender on HWY

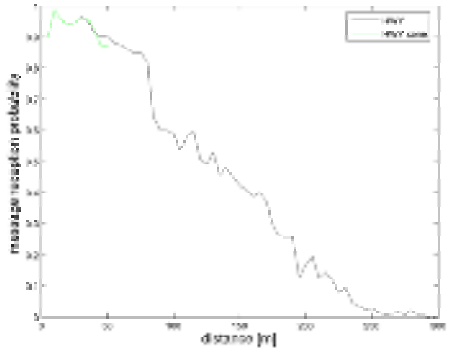


Figure 5-237: Reception Prob. of Emergency Messages - Scenario18, HWY, Sender on HWY

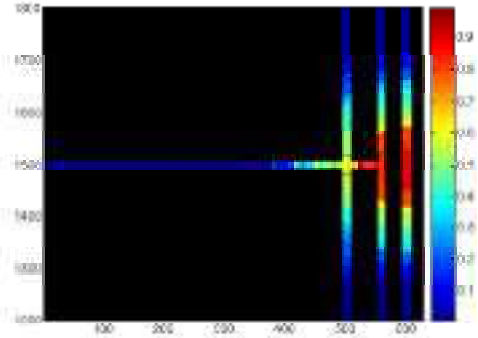


Figure 5-238: Reception Prob. of Emergency Messages-Scenario 18, Sender on HWY

5.2.3 Scenario 19

Simulation Scenario Setting:

RF Model	Distributed
Emergency Message Sender	RSU, 10Hz/ 500 bytes/ 200m
Corner Model	tall buildings
Pt	200m coverage
Routine Message Frequency	2Hz

5.2.3.1 Reception Probability of Emergency Messages

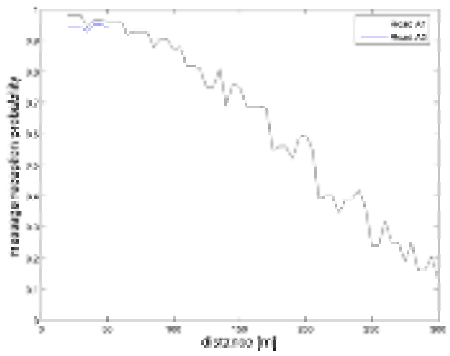


Figure 5-239: Reception Probability of Emergency Messages-Scenario19, Road A, Sender RSU

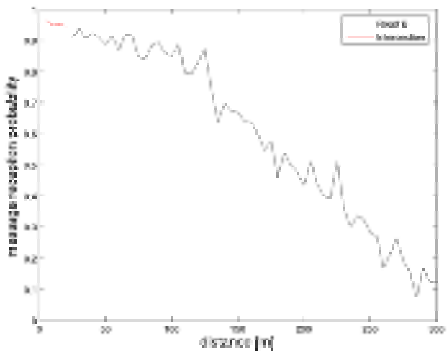


Figure 5-240: Reception Probability of Emergency Messages-Scenario19, Road B, Sender RSU

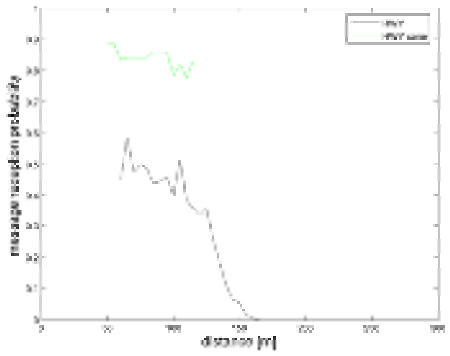


Figure 5-241: Reception Probability of Emergency Messages-Scenario19, HWY, Sender RSU

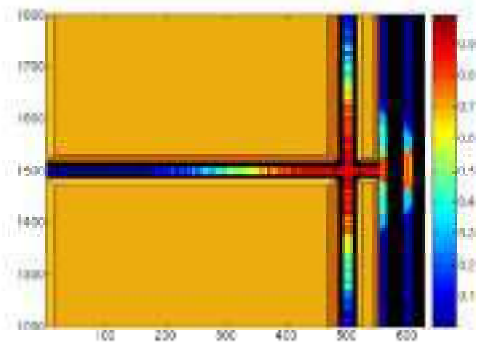


Figure 5-242: Reception Probability of Emergency Messages-Scenario19, Sender RSU

5.2.3.2 Reception Probability of Routine Messages

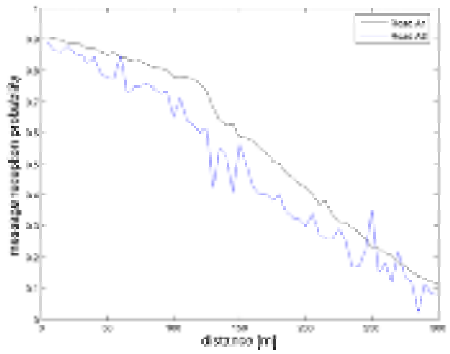


Figure 5-243: Reception Probability of Routine Messages on Road A, Scenario 19

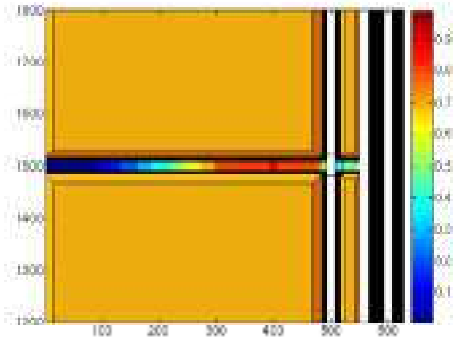


Figure 5-244: Reception Probability of Routine Messages on Road A, Scenario 19

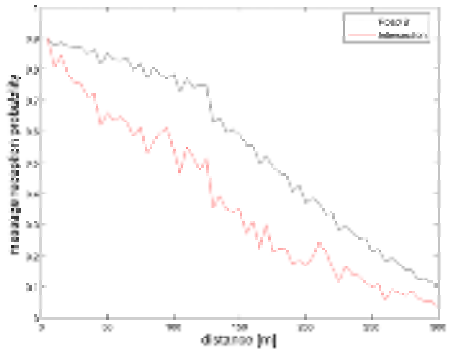


Figure 5-245: Reception Probability of Routine Messages on Road B, Scenario 19

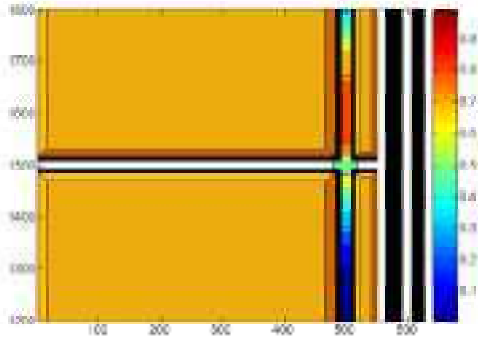


Figure 5-246: Reception Probability of Routine Messages on Road B, Scenario 19

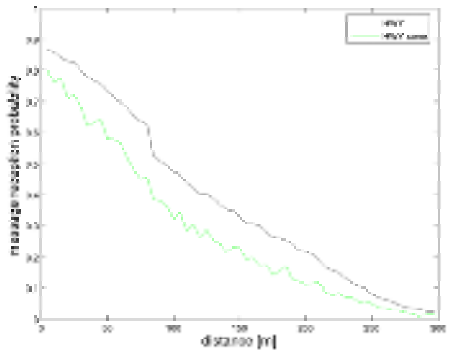


Figure 5-247: Reception Probability of Routine Messages on HWY, Scenario 19

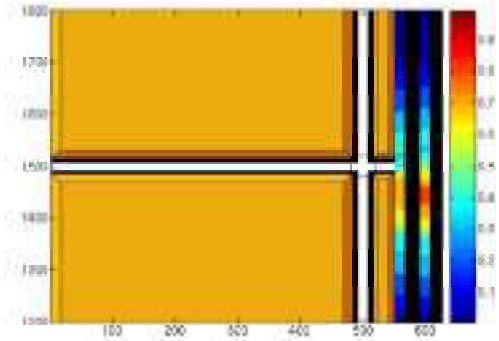


Figure 5-248: Reception Probability of Routine Messages on HWY, Scenario 19

5.2.4 Scenario 20

Simulation Scenario Setting:

RF Model	Distributed
Emergency Message Sender	OBUs on Road A1, A2, B and HWY
Corner Model	tall building
Pt	200m coverage
Routine Message Frequency	2Hz

5.2.4.1 Reception Probability of Emergency Messages From OBU on A1

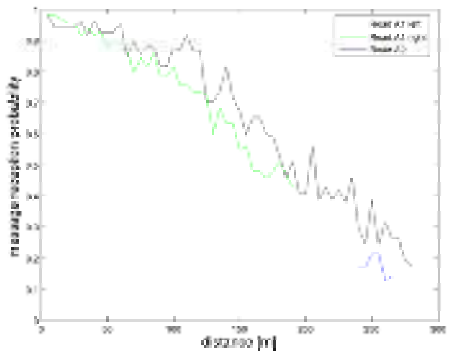


Figure 5-249: Reception Prob. of Emergency Messages - Scenario20, Rd. A, Sender on Rd. A1

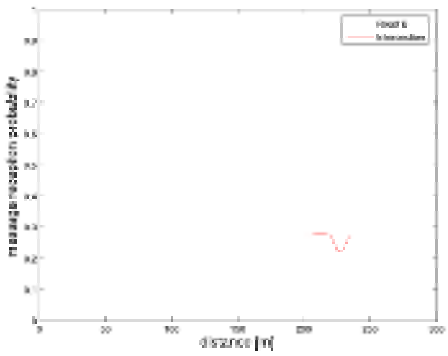


Figure 5-250: Reception Prob. of Emergency Messages - Scenario20, Rd. B, Sender on Rd. A1

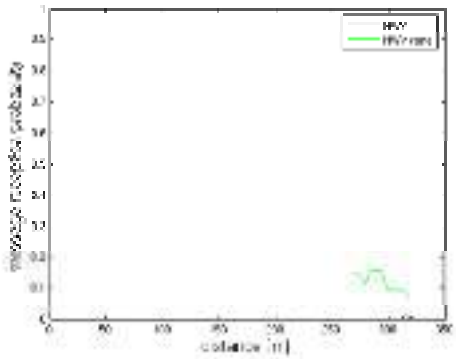


Figure 5-251: Reception Prob. of Emergency Messages - Scenario20, HWY, Sender on Rd. A1

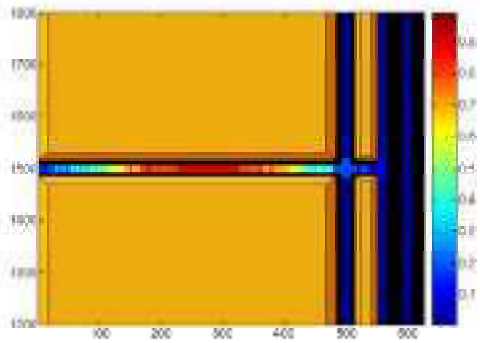


Figure 5-252: Reception Prob. of Emergency Messages-Scenario 20, Sender on Rd. A1

5.2.4.2 Reception Probability of Emergency Messages From OBU on A2

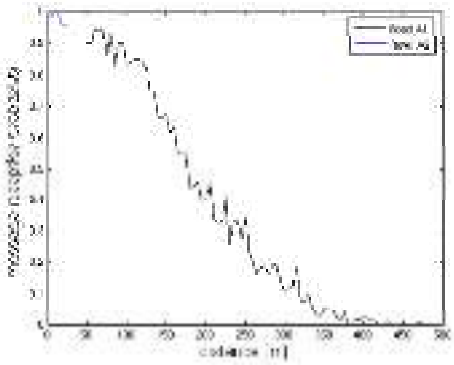


Figure 5-253: Reception Prob. of Emergency Messages - Scenario20, Rd. A, Sender on Rd. A2

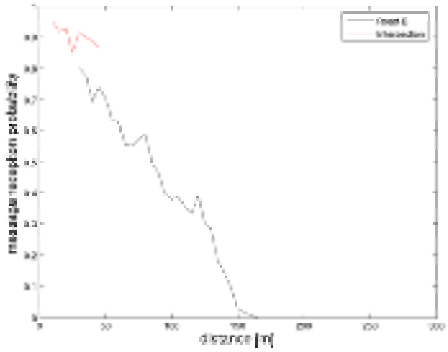


Figure 5-254: Reception Prob. of Emergency Messages - Scenario20, Rd. B, Sender on Rd. A2

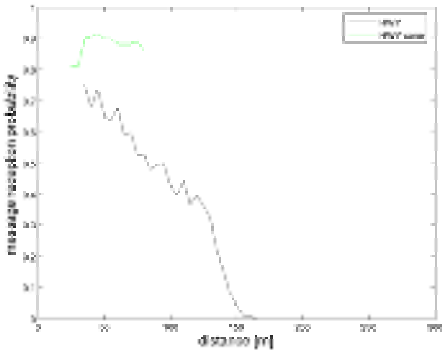


Figure 5-255: Reception Prob. of Emergency Messages - Scenario20, HWY, Sender on Rd. A2

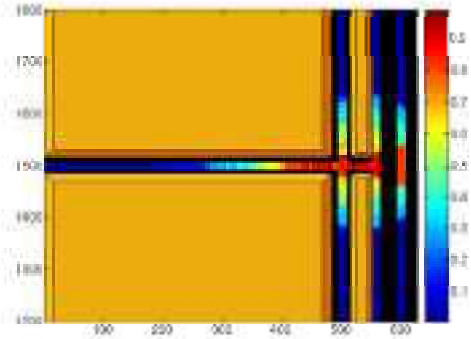


Figure 5-256: Reception Prob. of Emergency Messages-Scenario 20, Sender on Rd. A2

5.2.4.3 Reception Probability of Emergency Messages From OBU on B

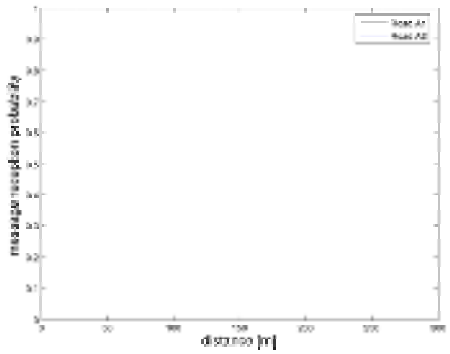


Figure 5-257: Reception Prob. of Emergency Messages - Scenario20, Rd. A, Sender on Rd. B

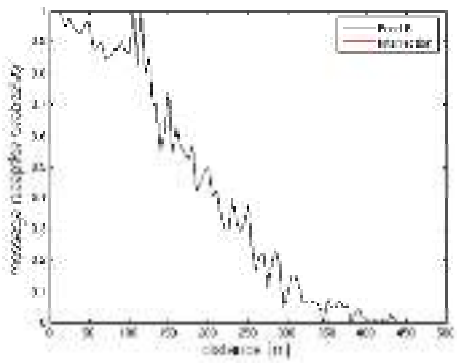


Figure 5-258: Reception Prob. of Emergency Messages - Scenario20, Rd. B, Sender on Rd. B

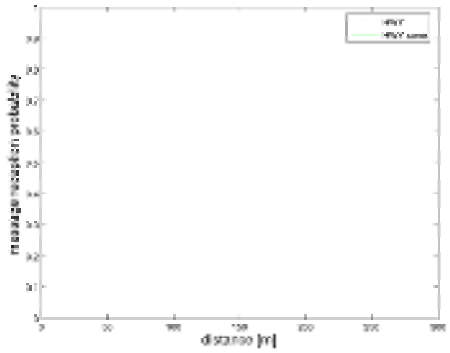


Figure 5-259: Reception Prob. of Emergency Messages - Scenario20, HWY, Sender on Rd. B

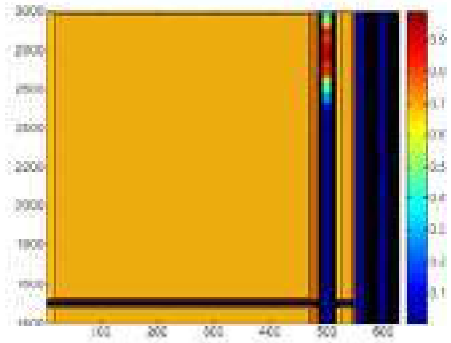


Figure 5-260: Reception Prob. of Emergency Messages - Scenario 20, Sender on Rd. B

5.2.4.4 Reception Probability of Emergency Messages From OBU on HWY

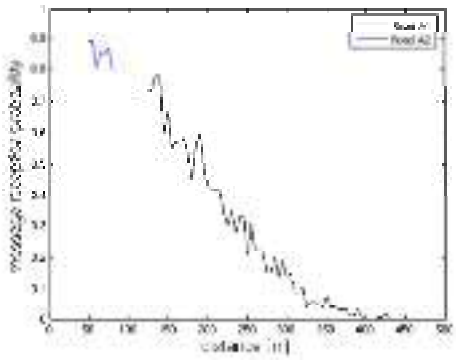


Figure 5-261: Reception Prob. of Emergency Messages - Scenario20, Rd. A, Sender on HWY

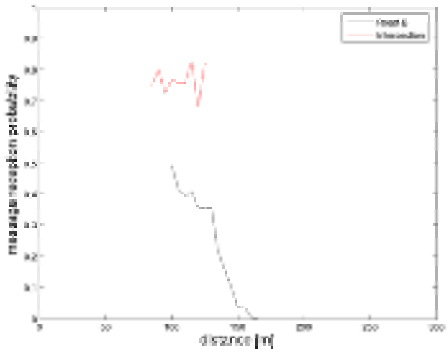


Figure 5-262: Reception Prob. of Emergency Messages - Scenario20, Rd. B, Sender on HWY

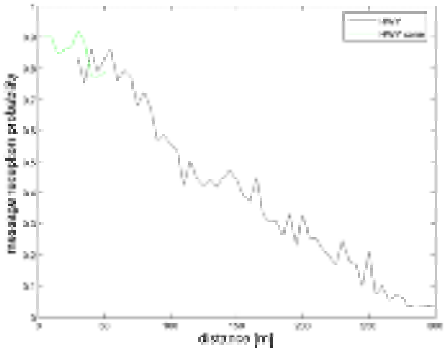


Figure 5-263: Reception Prob. of Emergency Messages - Scenario20, HWY, Sender on HWY

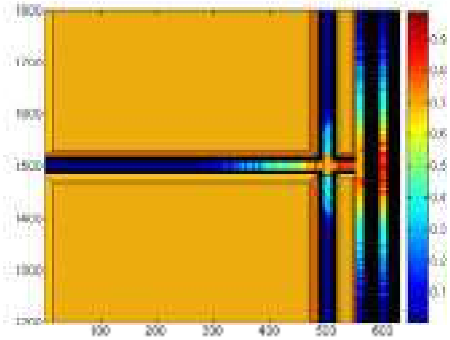


Figure 5-264: Reception Prob. of Emergency Messages-Scenario 20, Sender on HWY

5.2.5 Scenario 21

Simulation Scenario Setting:

RF Model	Distributed
Emergency Message Sender	RSU, 10Hz/ 500 bytes/ 200m
Corner Model	no buildings
Pt	300m coverage
Routine Message Frequency	2Hz

5.2.5.1 Reception Probability of Emergency Messages

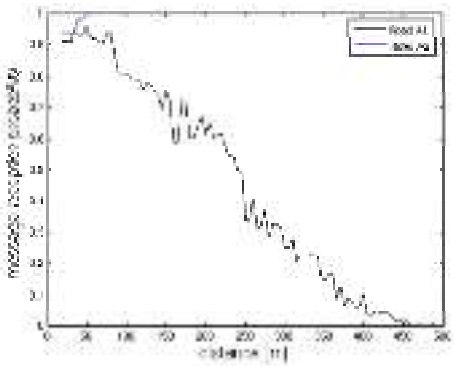


Figure 5-265: Reception Probability of Emergency Messages-Scenario21, Road A, Sender RSU

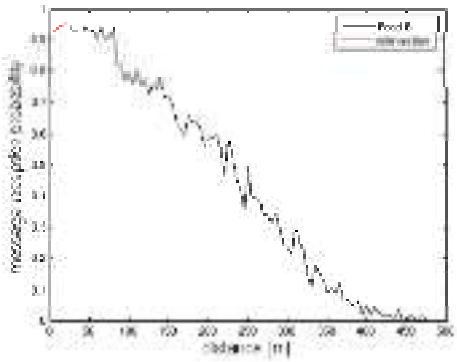


Figure 5-266: Reception Probability of Emergency Messages-Scenario21, Road B, Sender RSU

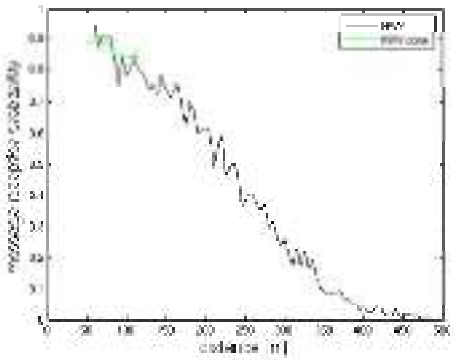


Figure 5-267: Reception Probability of Emergency Messages-Scenario21, HWY, Sender RSU

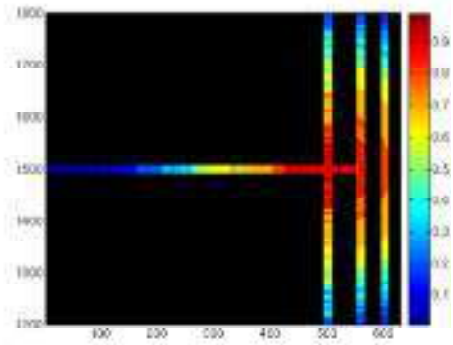


Figure 5-268: Reception Probability of Emergency Messages-Scenario21, Sender RSU

5.2.6 Scenario 22

Simulation Scenario Setting:

RF Model	Distributed
Emergency Message Sender	OBUs on Road A1, A2, B and HWY
Corner Model	no building
Pt	300m coverage
Routine Message Frequency	2Hz

5.2.6.1 Reception Probability of Emergency Messages From OBU on A1

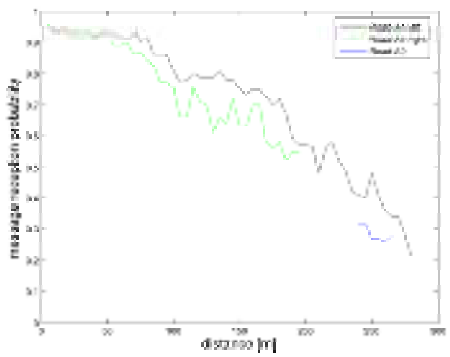


Figure 5-269: Reception Prob. of Emergency Messages - Scenario22, Rd. A, Sender on Rd. A1

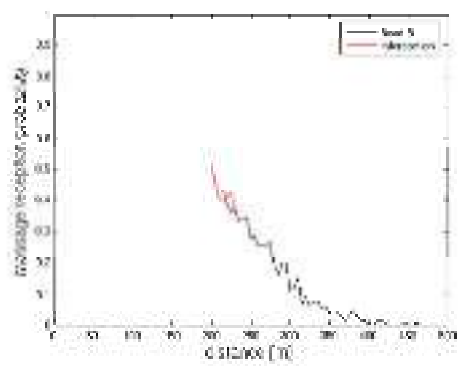


Figure 5-270: Reception Prob. of Emergency Messages - Scenario22, Rd. B, Sender on Rd. A1

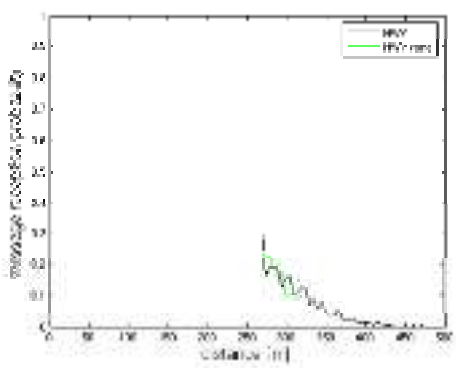


Figure 5-271: Reception Prob. of Emergency Messages - Scenario22, HWY, Sender on Rd. A1

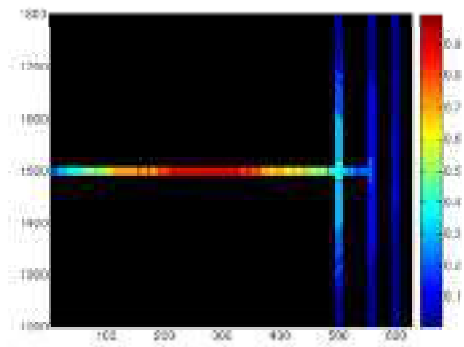


Figure 5-272: Reception Prob. of Emergency Messages-Scenario 22, Sender on Rd. A1

5.2.6.2 Reception Probability of Emergency Messages From OBU on A2

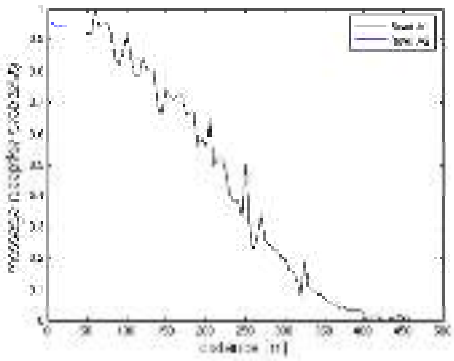


Figure 5-273: Reception Prob. of Emergency Messages - Scenario22, Rd. A, Sender on Rd. A2

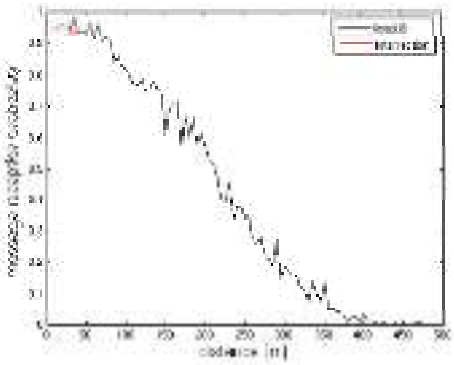


Figure 5-274: Reception Prob. of Emergency Messages - Scenario22, Rd. B, Sender on Rd. A2

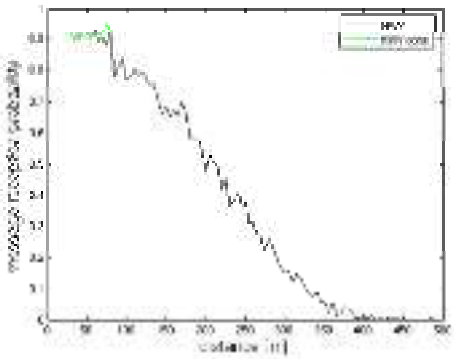


Figure 5-275: Reception Prob. of Emergency Messages - Scenario22, HWY, Sender on Rd. A2

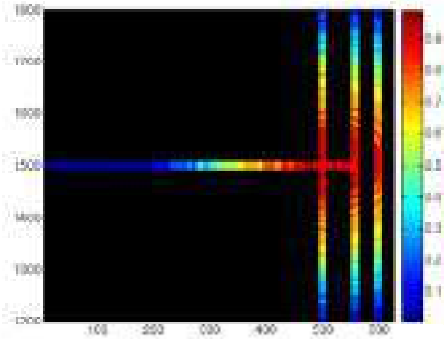


Figure 5-276: Reception Prob. of Emergency Messages-Scenario 22, Sender on Rd. A2

5.2.6.3 Reception Probability of Emergency Messages From OBU on B

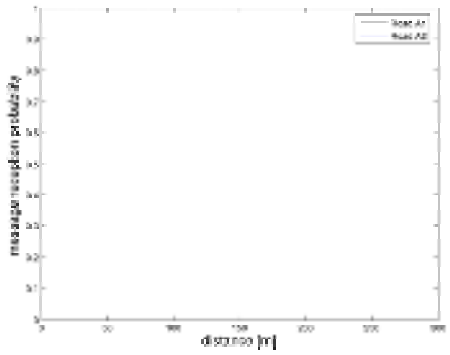


Figure 5-277: Reception Prob. of Emergency Messages - Scenario22, Rd. A, Sender on Rd. B

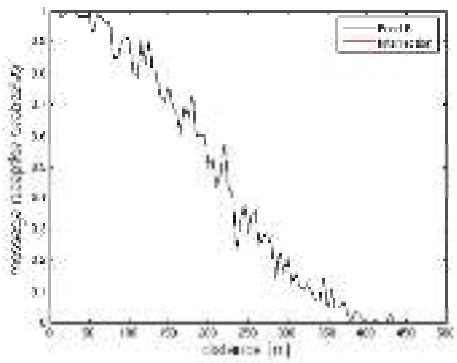


Figure 5-278: Reception Prob. of Emergency Messages - Scenario22, Rd. B, Sender on Rd. B

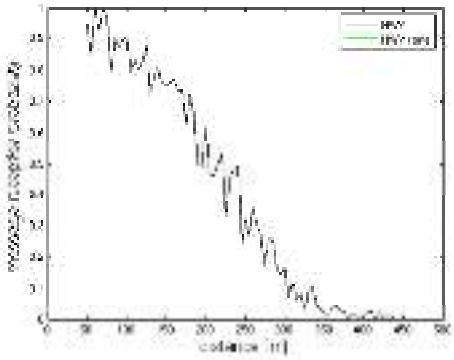


Figure 5-279: Reception Prob. of Emergency Messages - Scenario22, HWY, Sender on Rd. B

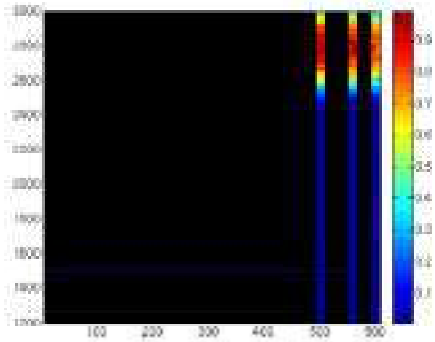


Figure 5-280: Reception Prob. of Emergency Messages-Scenario 22, Sender on Rd. B

5.2.6.4 Reception Probability of Emergency Messages From OBU on HWY

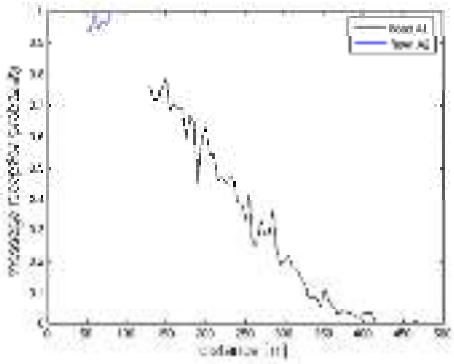


Figure 5-281: Reception Prob. of Emergency Messages - Scenario22, Rd. A, Sender on HWY

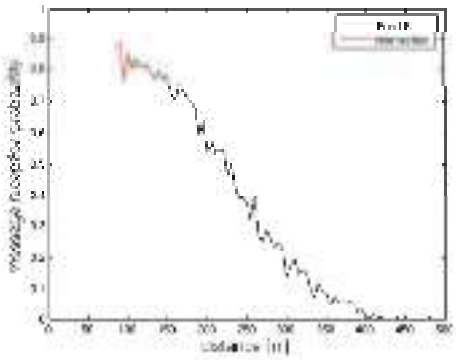


Figure 5-282: Reception Prob. of Emergency Messages - Scenario22, Rd. B, Sender on HWY

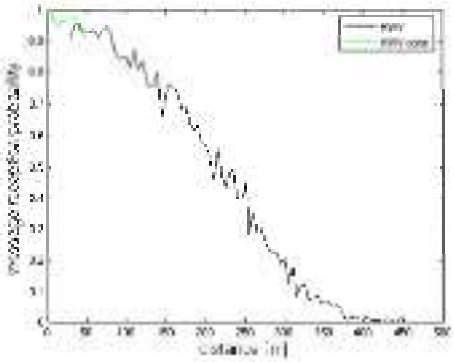


Figure 5-283: Reception Prob. of Emergency Messages - Scenario22, HWY, Sender on HWY

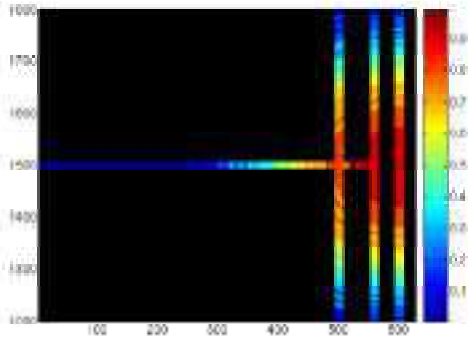


Figure 5-284: Reception Prob. of Emergency Messages - Scenario 22, Sender on HWY

5.2.7 Scenario 23

Simulation Scenario Setting:

RF Model	Distributed
Emergency Message Sender	RSU, 10Hz/ 500 bytes/ 200m
Corner Model	Tall building
Pt	300m coverage
Routine Message Frequency	2Hz

5.2.7.1 Reception Probability of Emergency Messages

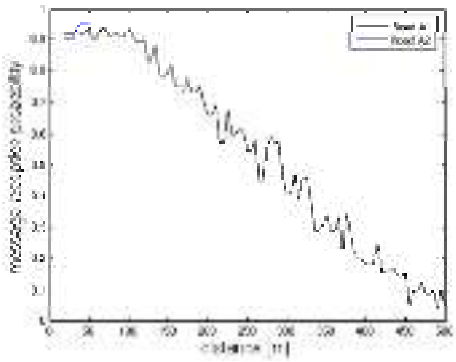


Figure 5-285: Reception Probability of Emergency Messages-Scenario 23, Road A, Sender RSU

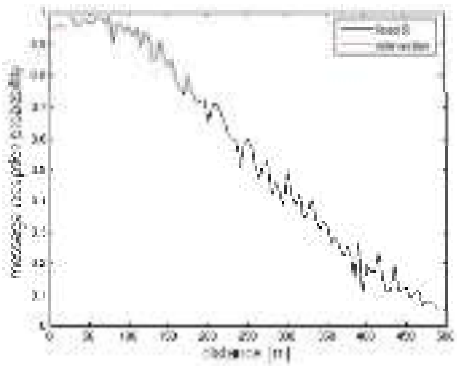


Figure 5-286: Reception Probability of Emergency Messages-Scenario 23, Road B, Sender RSU

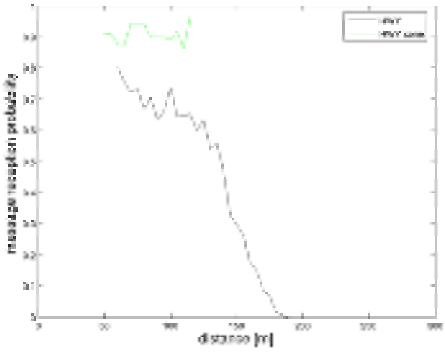


Figure 5-287: Reception Probability of Emergency Messages-Scenario 23, HWY, Sender RSU

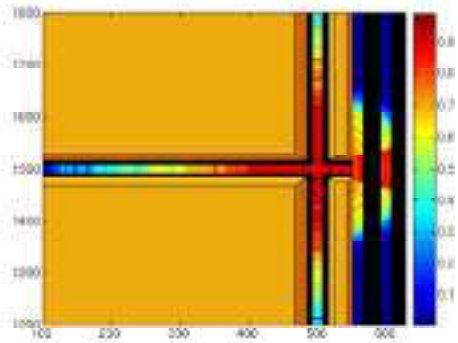


Figure 5-288: Reception Probability of Emergency Messages-Scenario 23, Sender RSU

5.2.8 Scenario 24

Simulation Scenario Setting:

RF Model	Distributed
Emergency Message Sender	OBUs on Road A1, A2, B and HWY
Corner Model	tall building
Pt	300m coverage
Routine Message Frequency	2Hz

5.2.8.1 Reception Probability of Emergency Messages from OBU on A1

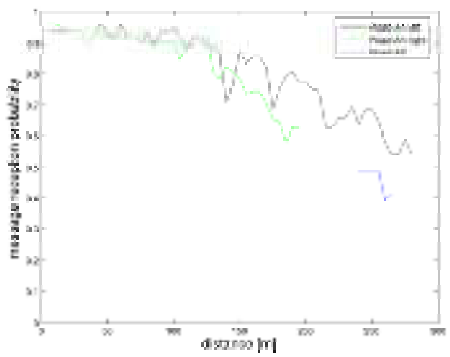


Figure 5-289: Reception Prob. of Emergency Messages – Scenario 24, Rd. A, Sender on Rd. A1

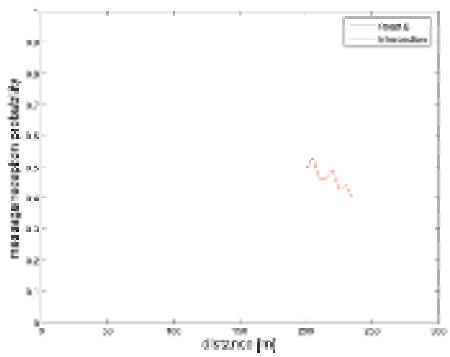


Figure 5-290: Reception Prob. of Emergency Messages – Scenario 24, Rd. B, Sender on Rd. A1

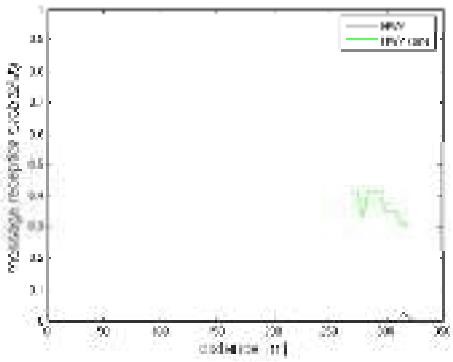


Figure 5-291: Reception Prob. of Emergency Messages – Scenario 24, HWY, Sender on Rd. A1

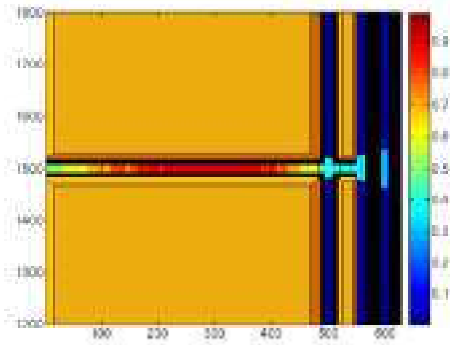


Figure 5-292: Reception Prob. of Emergency Messages-Scenario 24, Sender on Rd. A1

5.2.8.2 Reception Probability of Emergency Messages From OBU on A2

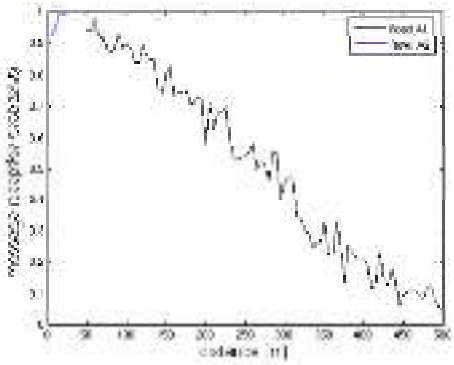


Figure 5-293: Reception Prob. of Emergency Messages – Scenario 24, Rd. A, Sender on Rd. A2

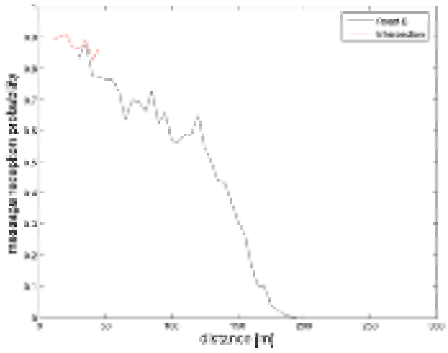


Figure 5-294: Reception Prob. of Emergency Messages – Scenario 24, Rd. B, Sender on Rd. A2

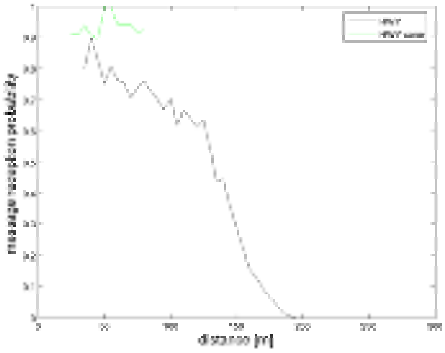


Figure 5-295: Reception Prob. of Emergency Messages – Scenario 24, HWY, Sender on Rd. A2

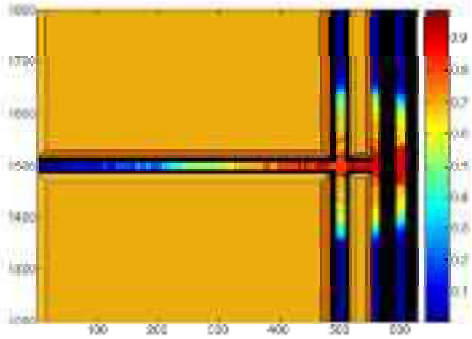


Figure 5-296: Reception Prob. of Emergency Messages-Scenario 24, Sender on Rd. A2

5.2.8.3 Reception Probability of Emergency Messages From OBU on B

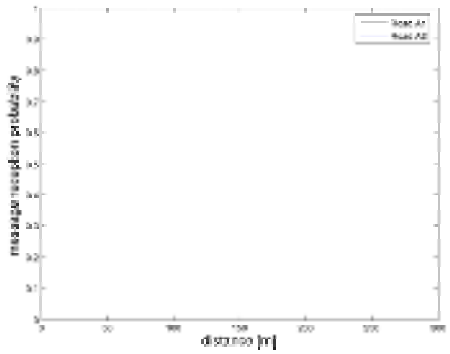


Figure 5-297: Reception Prob. of Emergency Messages - Scenario24, Rd. A, Sender on Rd. B

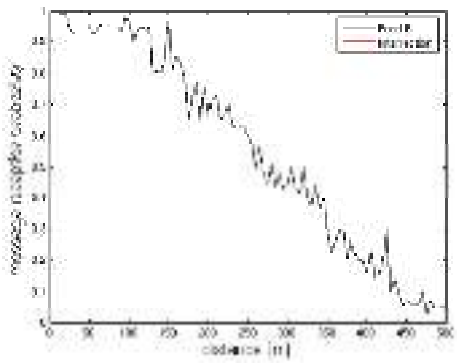


Figure 5-298: Reception Prob. of Emergency Messages - Scenario24, Rd. B, Sender on Rd. B

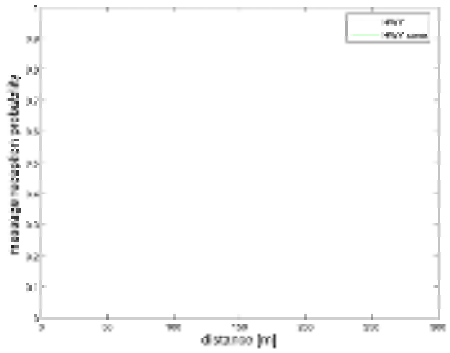


Figure 5-299: Reception Prob. of Emergency Messages - Scenario24, HWY, Sender on Rd. B

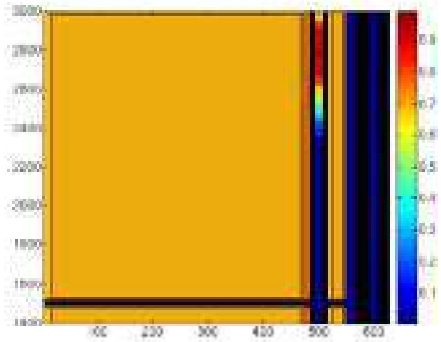


Figure 5-300: Reception Prob. of Emergency Messages-Scenario 24, Sender on Rd. B

5.2.8.4 Reception Probability of Emergency Messages From OBU on HWY

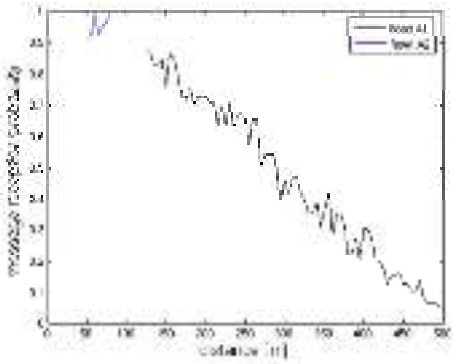


Figure 5-301: Reception Prob. of Emergency Messages - Scenario24, Rd. A, Sender on HWY

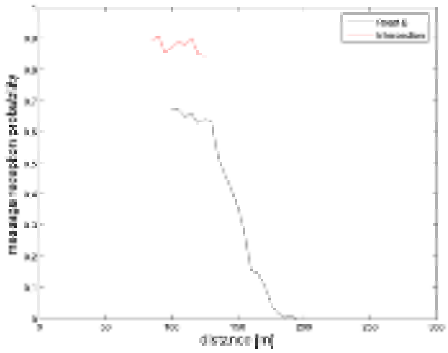


Figure 5-302: Reception Prob. of Emergency Messages - Scenario24, Rd. B, Sender on HWY

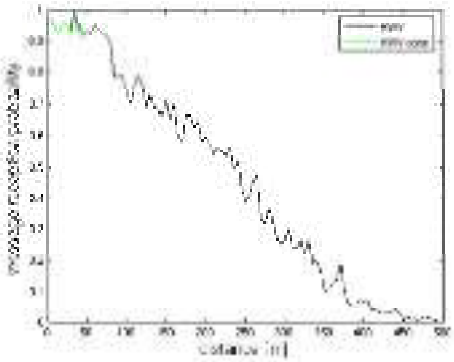


Figure 5-303: Reception Prob. of Emergency Messages - Scenario24, HWY, Sender on HWY

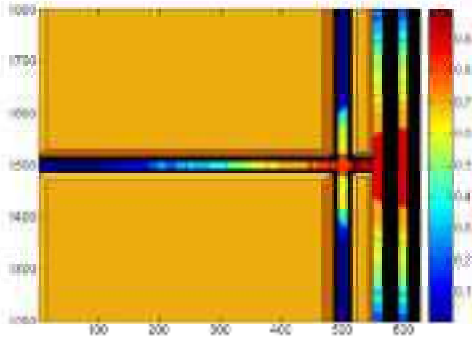


Figure 5-304: Reception Prob. of Emergency Messages-Scenario 24, Sender on HWY

5.2.9 Scenario 25

Simulation Scenario Setting:

RF Model	Distributed
Emergency Message Sender	RSU, 10Hz/ 500 bytes/ 200m
Corner Model	no buildings
Pt	200m coverage
Routine Message Frequency	1 Hz

5.2.9.1 Reception Probability of Emergency Messages

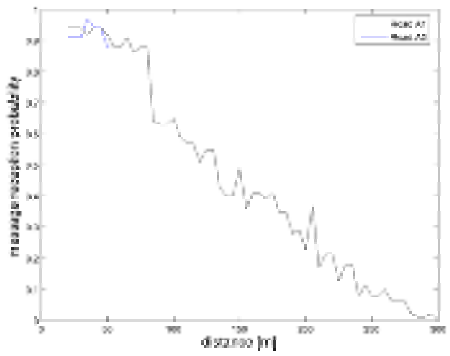


Figure 5-305: Reception Probability of Emergency Messages-Scenario 25, Road A, Sender RSU

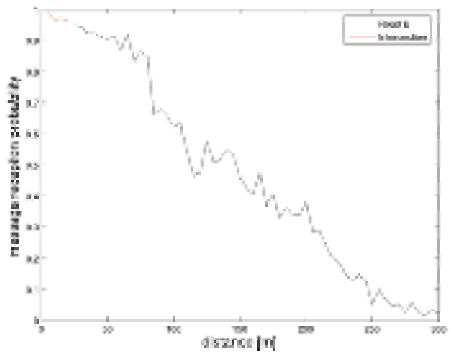


Figure 5-306: Reception Probability of Emergency Messages-Scenario 25, Road B, Sender RSU

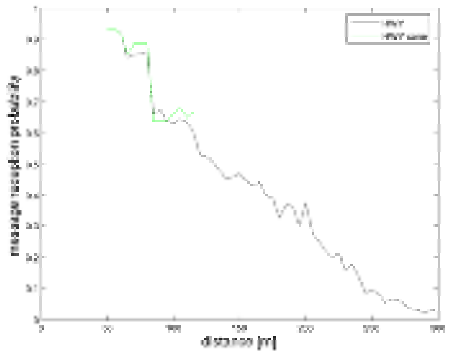


Figure 5-307: Reception Probability of Emergency Messages-Scenario 25, HWY, Sender RSU

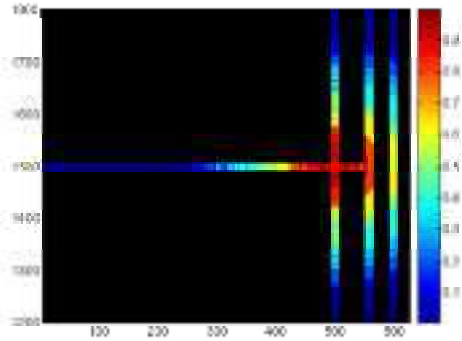


Figure 5-308: Reception Probability of Emergency Messages-Scenario 25, Sender RSU

5.2.9.2 Routine Message Reception Probability

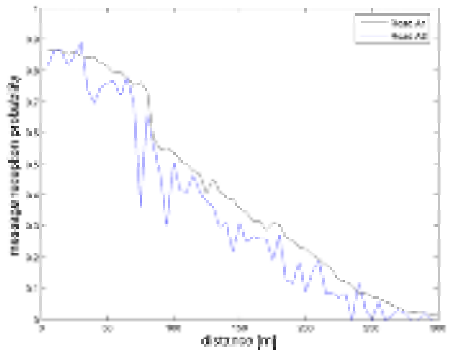


Figure 5-309: Reception Probability of Routine Messages on Road A Scenario 25

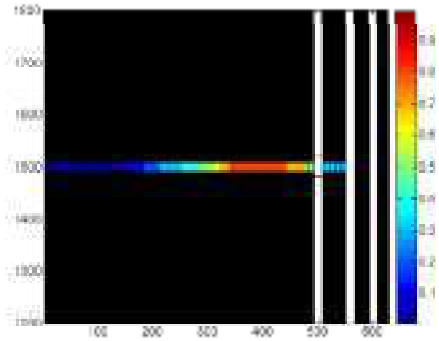


Figure 5-310: Reception Probability of Routine Messages on Road A Scenario 25

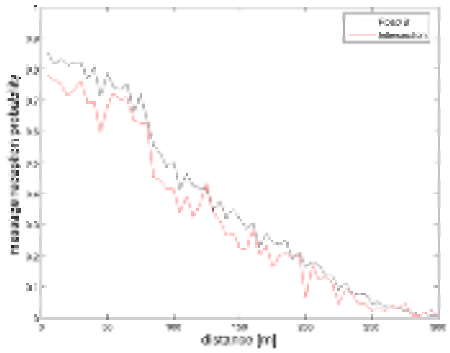


Figure 5-311: Reception Probability of Routine Messages on Road B Scenario 25

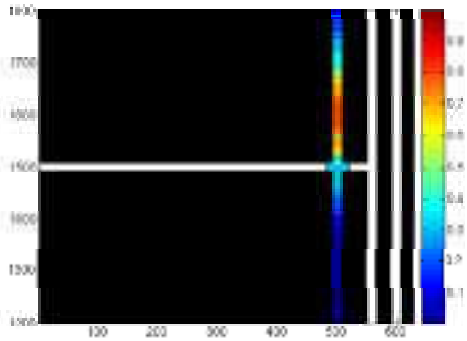


Figure 5-312: Reception Probability of Routine Messages on Road B Scenario 25

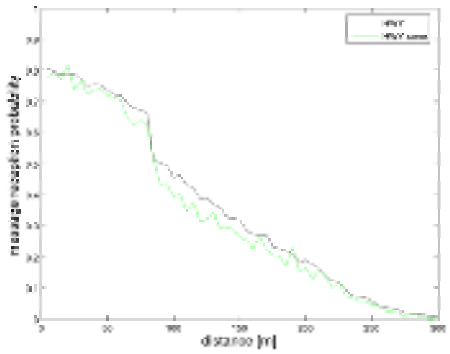


Figure 5-313: Reception Probability of Routine Messages on HWY Scenario 25

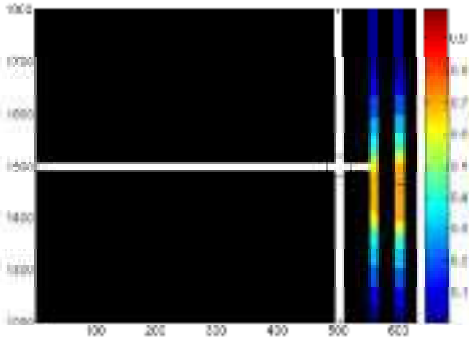


Figure 5-314: Reception Probability of Routine Messages on HWY Scenario 25

5.2.10 Scenario 26

Simulation Scenario Setting:

RF Model	Distributed
Emergency Message Sender	OBUs on Road A1, A2, B and HWY
Corner Model	no building
Pt	200m coverage
Routine Message Frequency	1Hz

5.2.10.1 Reception Probability of Emergency Messages From OBU on A1

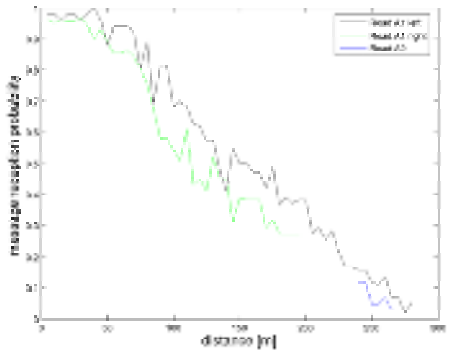


Figure 5-315: Reception Prob. of Emergency Messages – Scenario 26, Rd. A, Sender on Rd. A1

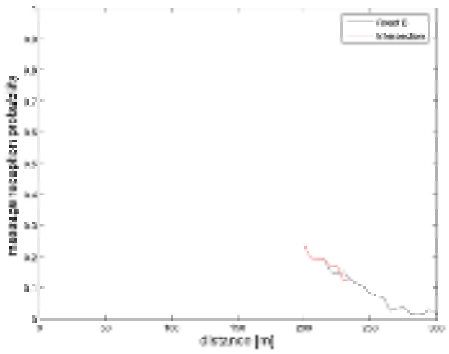


Figure 5-316: Reception Prob. of Emergency Messages – Scenario 26, Rd. B, Sender on Rd. A1

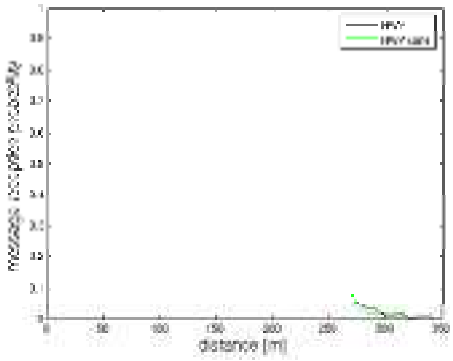


Figure 5-317: Reception Prob. of Emergency Messages – Scenario 26, HWY, Sender on Rd. A1

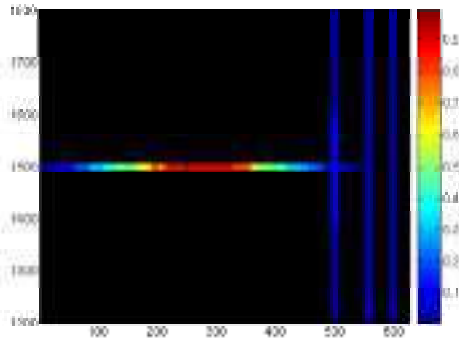


Figure 5-318: Reception Prob. of Emergency Messages-Scenario 26, Sender on Rd. A1

5.2.10.2 Reception Probability of Emergency Messages From OBU on A2

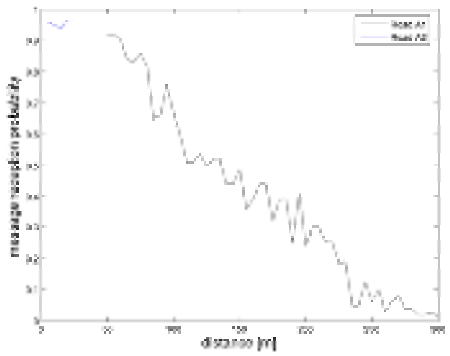


Figure 5-319: Reception Prob. of Emergency Messages - Scenario26, Rd. A, Sender on Rd. A2

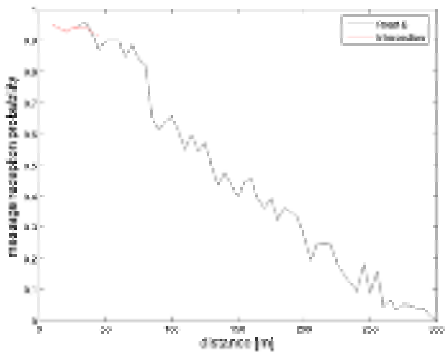


Figure 5-320: Reception Prob. of Emergency Messages - Scenario26, Rd. B, Sender on Rd. A2

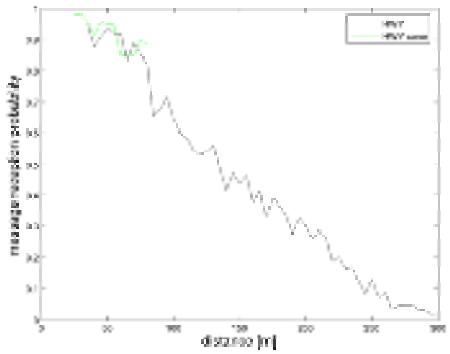


Figure 5-321: Reception Prob. of Emergency Messages - Scenario26, HWY, Sender on Rd. A2

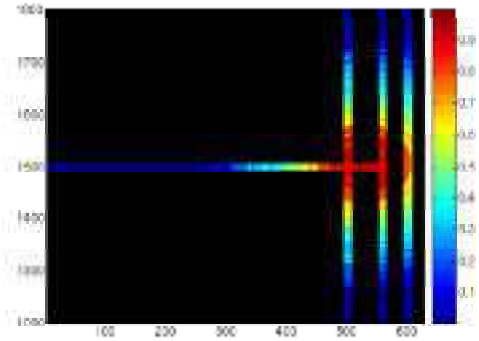


Figure 5-322: Reception Prob. of Emergency Messages-Scenario 26, Sender on Rd. A2

5.2.10.3 Reception Probability of Emergency Messages From OBU on B

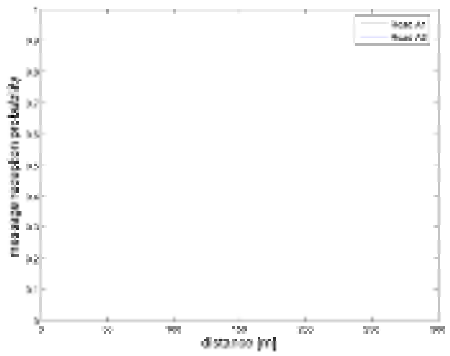


Figure 5-323: Reception Prob. of Emergency Messages – Scenario 26, Rd. A, Sender on Rd. B

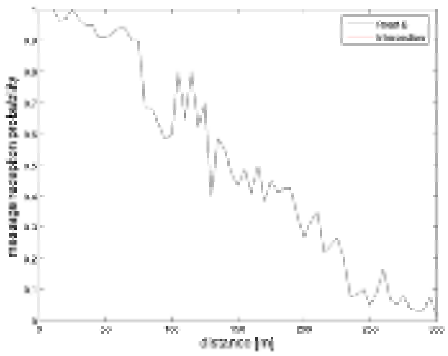


Figure 5-324: Reception Prob. of Emergency Messages – Scenario 26, Rd. B, Sender on Rd. B

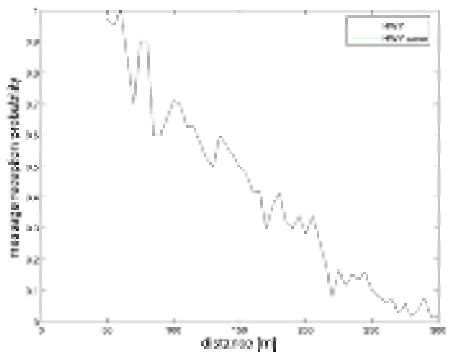


Figure 5-325: Reception Prob. of Emergency Messages – Scenario 26, HWY, Sender on Rd. B

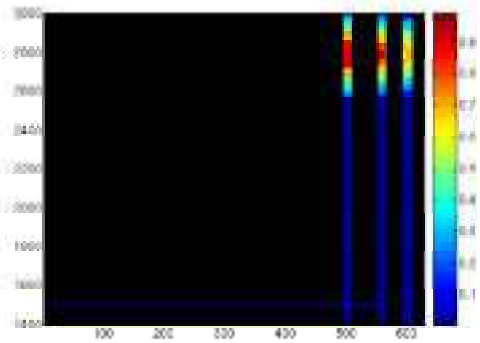


Figure 5-326: Reception Prob. of Emergency Messages-Scenario 26, Sender on Rd. B

5.2.10.4 Reception Probability of Emergency Messages From OBU on HWY

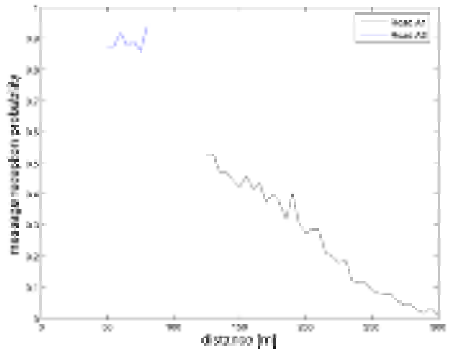


Figure 5-327: Reception Prob. of Emergency Messages – Scenario 26, Rd. A, Sender on HWY

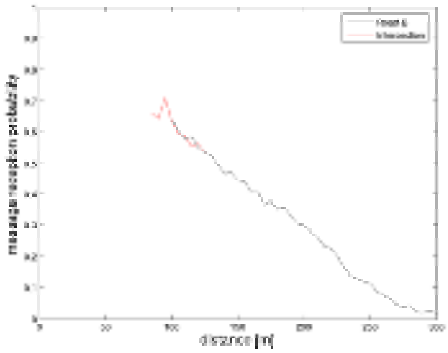


Figure 5-328: Reception Prob. of Emergency Messages – Scenario 26, Rd. B, Sender on HWY

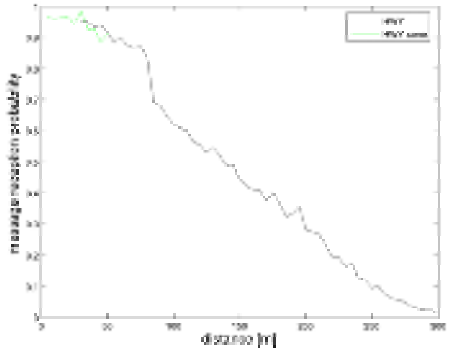


Figure 5-329: Reception Prob. of Emergency Messages – Scenario 26, HWY, Sender on HWY

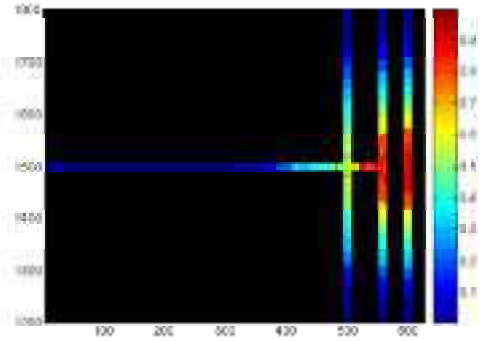


Figure 5-330: Reception Prob. of Emergency Messages-Scenario 26, Sender on HWY

5.2.11 Scenario 27

Simulation Scenario Setting:

RF Model	Distributed
Emergency Message Sender	RSU, 10Hz/ 500 bytes/ 200m
Corner Model	no buildings
Pt	200m coverage
Routine Message Frequency	1 Hz

5.2.11.1 Reception Probability of Emergency Messages

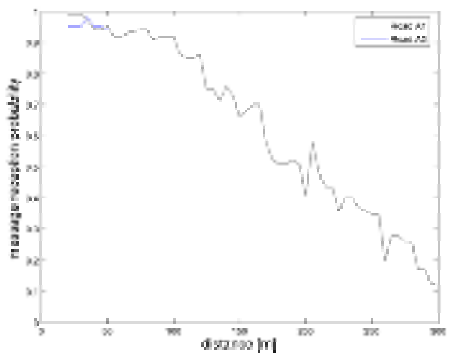


Figure 5-331: Reception Probability of Emergency Messages-Scenario 27, Road A, Sender RSU

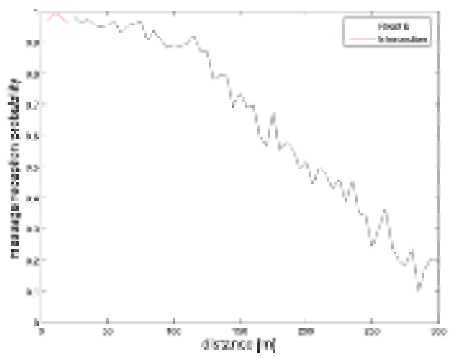


Figure 5-332: Reception Probability of Emergency Messages-Scenario 27, Road B, Sender RSU

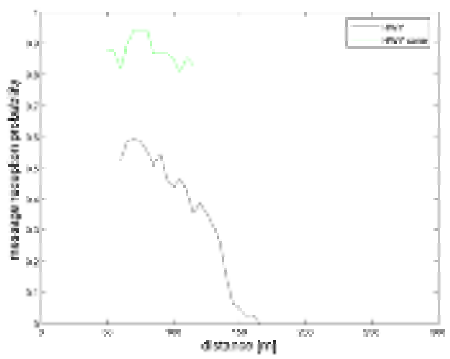


Figure 5-333: Reception Probability of Emergency Messages-Scenario 27, HWY, Sender RSU

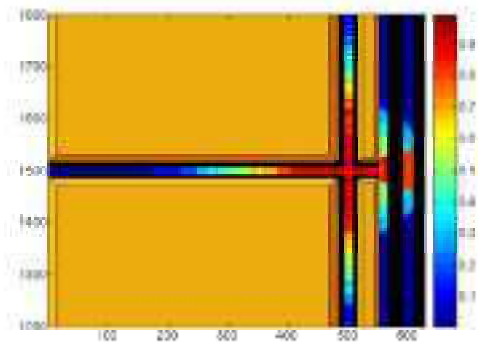


Figure 5-334: Reception Probability of Emergency Messages-Scenario 27, Sender RSU

5.2.11.2 Reception Probability of Routine Messages

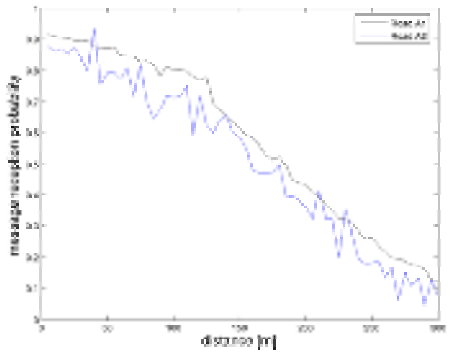


Figure 5-335: Reception Probability of Routine Messages on Road A, Scenario 27

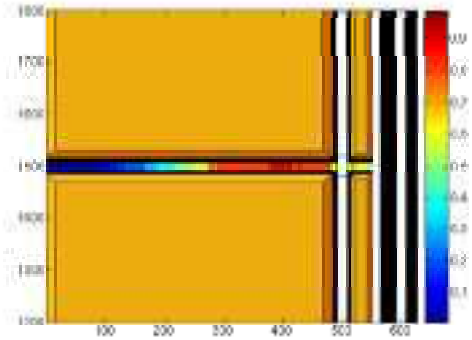


Figure 5-336: Reception Probability of Routine Messages on Road A, Scenario 27

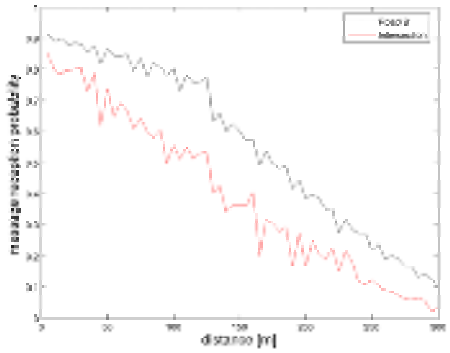


Figure 5-337: Reception Probability of Routine Messages on Road B, Scenario 27

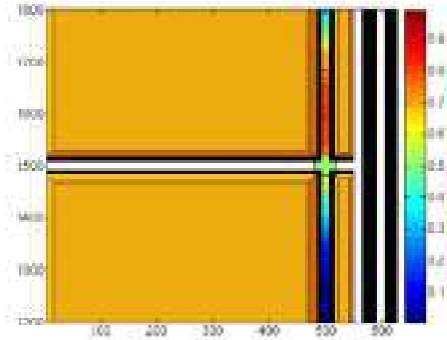


Figure 5-338: Reception Probability of Routine Messages on Road B, Scenario 27

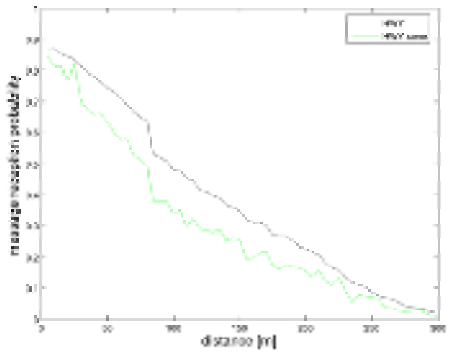


Figure 5-339: Reception Probability of Routine Messages on HWY, Scenario 27

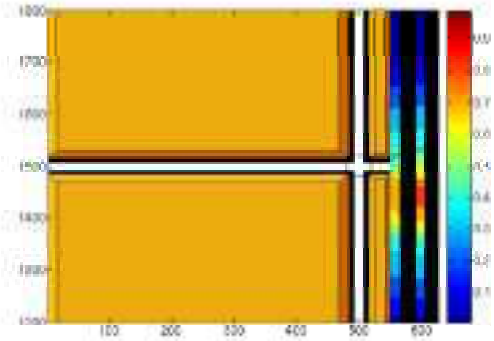


Figure 5-340: Reception Probability of Routine Messages on HWY, Scenario 27

5.2.12 Scenario 28

Simulation Scenario Setting:

RF Model	Distributed
Emergency Message Sender	OBUs on Road A1, A2, B and HWY
Corner Model	tall building
Pt	200m coverage
Routine Message Frequency	1Hz

5.2.12.1 Reception Probability of Emergency Messages from OBU on A1

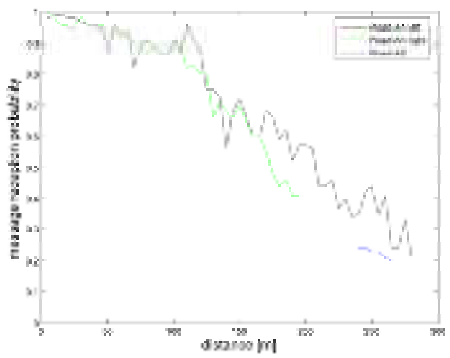


Figure 5-341: Reception Prob. of Emergency Messages – Scenario 28, Rd. A, Sender on Rd. A1

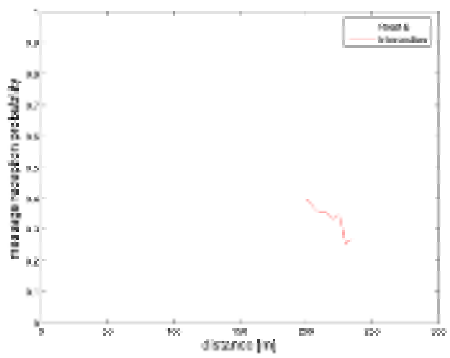


Figure 5-342: Reception Prob. of Emergency Messages – Scenario 28, Rd. B, Sender on Rd. A1

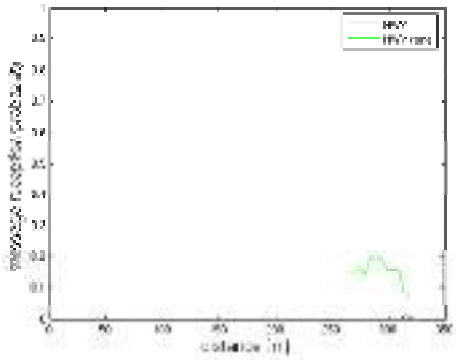


Figure 5-343: Reception Prob. of Emergency Messages – Scenario 28, HWY, Sender on Rd. A1

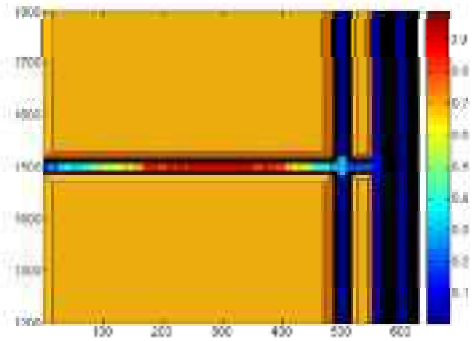


Figure 5-344: Reception Prob. of Emergency Messages-Scenario 28, Sender on Rd. A1

5.2.12.2 Reception Probability of Emergency Messages from OBU on A2

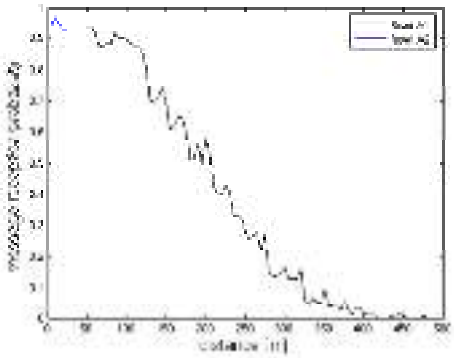


Figure 5-345: Reception Prob. of Emergency Messages – Scenario 28, Rd. A, Sender on Rd. A2

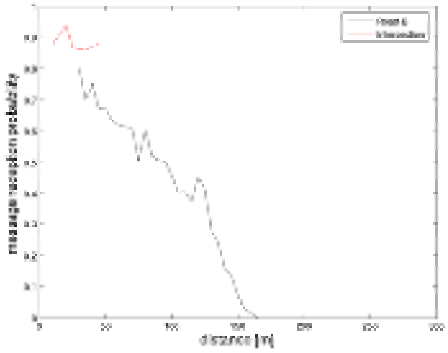


Figure 5-346: Reception Prob. of Emergency Messages – Scenario 28, Rd. B, Sender on Rd. A2

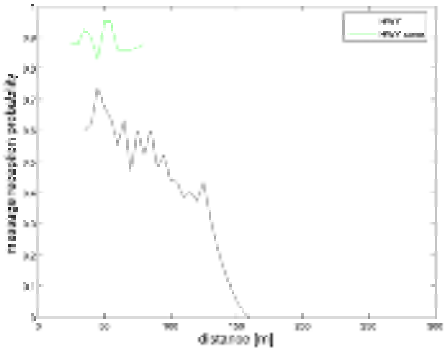


Figure 5-347: Reception Prob. of Emergency Messages – Scenario 28, HWY, Sender on Rd. A2

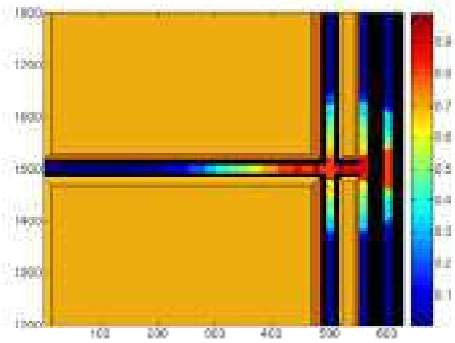


Figure 5-348: Reception Prob. of Emergency Messages – Scenario 28, Sender on Rd. A2

5.2.12.3 Reception Probability of Emergency Messages From OBU on B

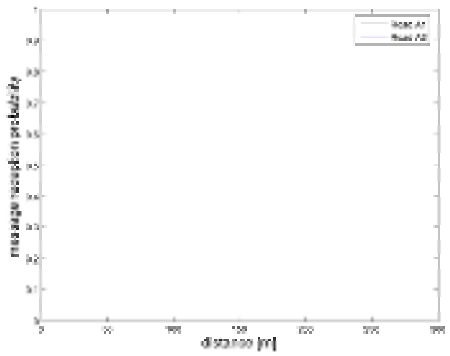


Figure 5-349: Reception Prob. of Emergency Messages – Scenario 28, Rd. A, Sender on Rd. B

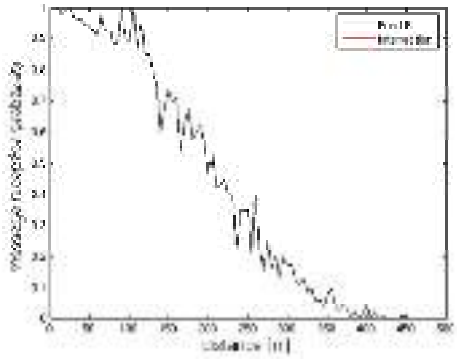


Figure 5-350: Reception Prob. of Emergency Messages – Scenario 28, Rd. B, Sender on Rd. B

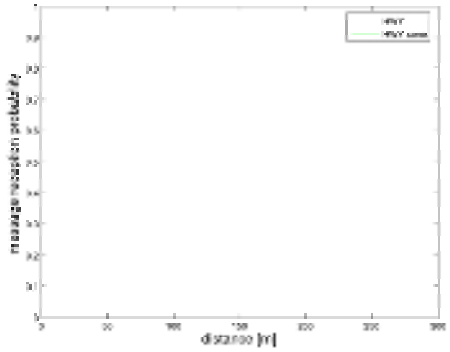


Figure 5-351: Reception Prob. of Emergency Messages – Scenario 28, HWY, Sender on Rd. B

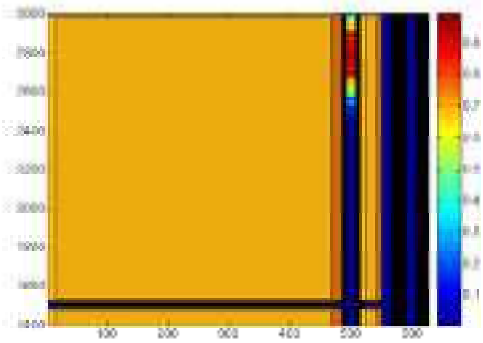


Figure 5-352: Reception Prob. of Emergency Messages-Scenario 28, Sender on Rd. B

5.2.12.4 Reception Probability of Emergency Messages From OBU on HWY

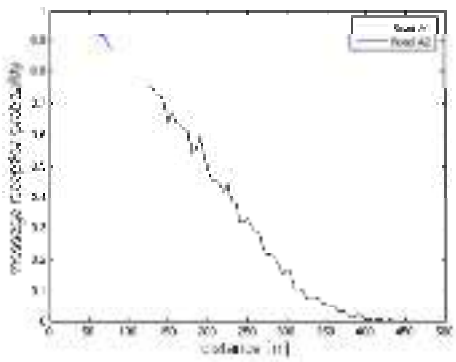


Figure 5-353: Reception Prob. of Emergency Messages – Scenario 28, Rd. A, Sender on HWY

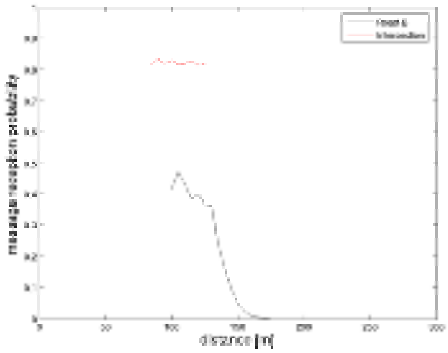


Figure 5-354: Reception Prob. of Emergency Messages – Scenario 28, Rd. B, Sender on HWY

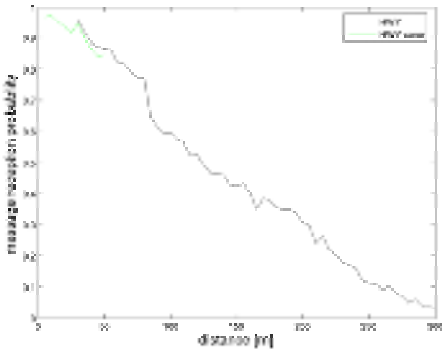


Figure 5-355: Reception Prob. of Emergency Messages – Scenario 28, HWY, Sender on HWY

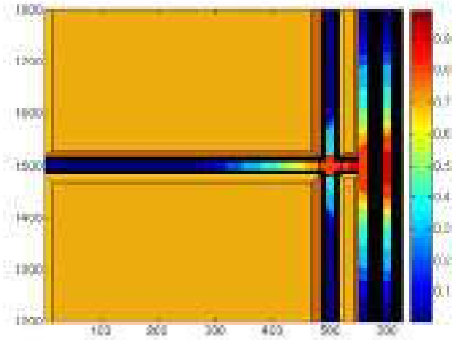


Figure 5-356: Reception Prob. of Emergency Messages-Scenario 28, Sender on HWY

5.2.13 Scenario 29

Simulation Scenario Setting:

RF Model	Distributed
Emergency Message Sender	RSU, 10Hz/ 500 bytes/ 200m
Corner Model	no buildings
Pt	300m coverage
Routine Message Frequency	1Hz

5.2.13.1 Reception Probability of Emergency Messages

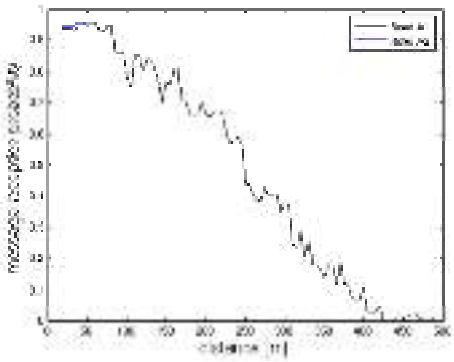


Figure 5-357: Reception Probability of Emergency Messages-Scenario 29, Road A, Sender RSU

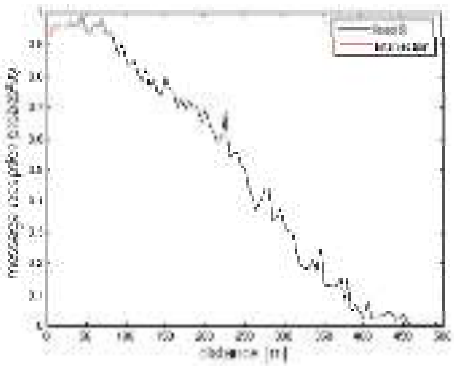


Figure 5-358: Reception Probability of Emergency Messages-Scenario 29, Road B, Sender RSU

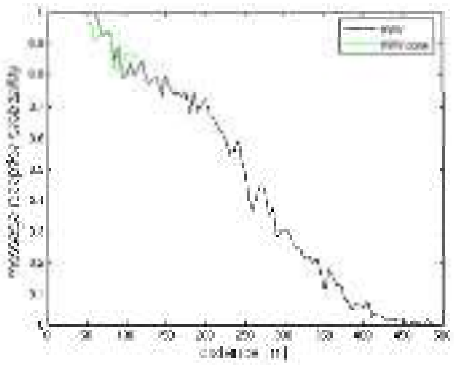


Figure 5-359: Reception Probability of Emergency Messages-Scenario 29, HWY, Sender RSU

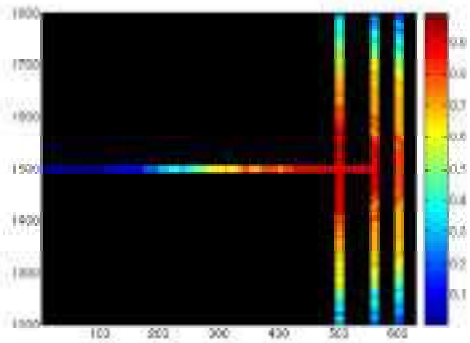


Figure 5-360: Reception Probability of Emergency Messages-Scenario 29, Sender RSU

5.2.14 Scenario 30

Simulation Scenario Setting:

RF Model	Distributed
Emergency Message Sender	OBUs on Road A1, A2, B and HWY
Corner Model	no building
Pt	300m coverage
Routine Message Frequency	1Hz

5.2.14.1 Reception Probability of Emergency Messages From OBU on A1

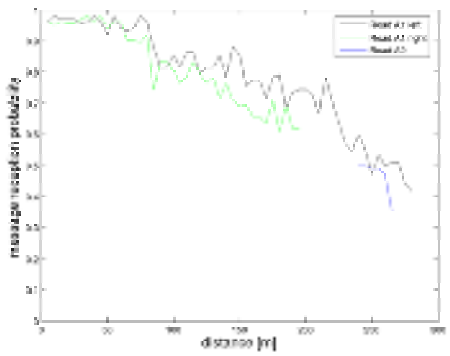


Figure 5-361: Reception Prob. of Emergency Messages – Scenario 30, Rd. A, Sender on Rd. A1

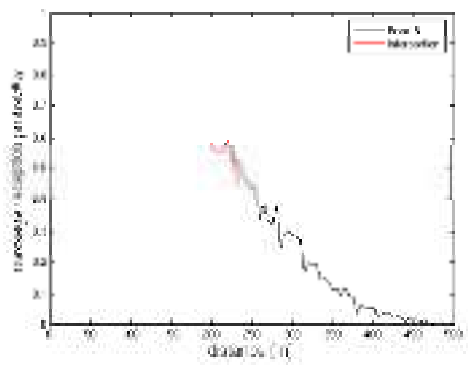


Figure 5-362: Reception Prob. of Emergency Messages – Scenario 30, Rd. B, Sender on Rd. A1

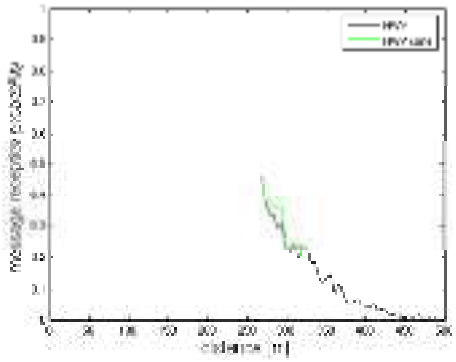


Figure 5-363: Reception Prob. of Emergency Messages – Scenario 30, HWY, Sender on Rd. A1

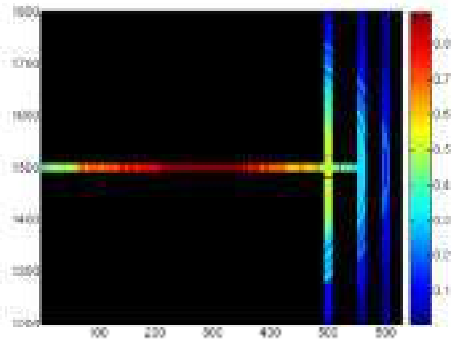


Figure 5-364: Reception Prob. of Emergency Messages-Scenario 30, Sender on Rd. A1

5.2.14.2 Reception Probability of Emergency Messages From OBU on A2

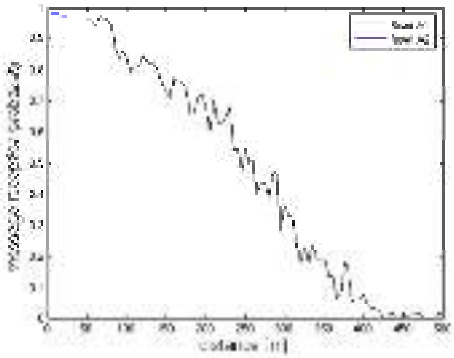


Figure 5-365: Reception Prob. of Emergency Messages – Scenario 30, Rd. A, Sender on Rd. A2

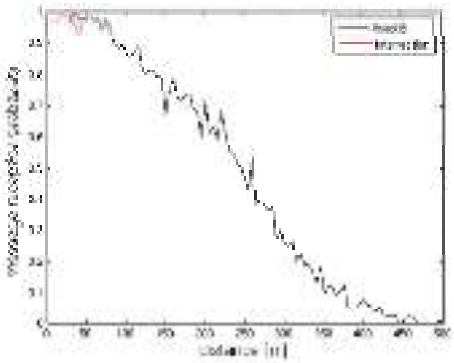


Figure 5-366: Reception Prob. of Emergency Messages – Scenario 30, Rd. B, Sender on Rd. A2

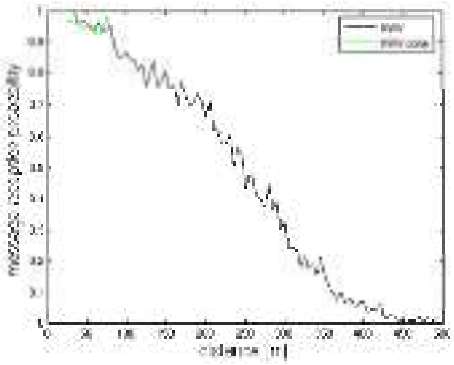


Figure 5-367: Reception Prob. of Emergency Messages – Scenario 30, HWY, Sender on Rd. A2

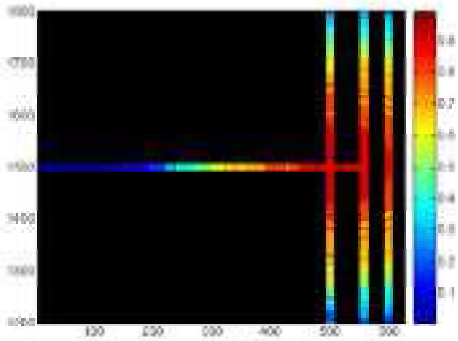


Figure 5-368: Reception Prob. of Emergency Messages-Scenario 30, Sender on Rd. A2

5.2.14.3 Reception Probability of Emergency Messages From OBU on B

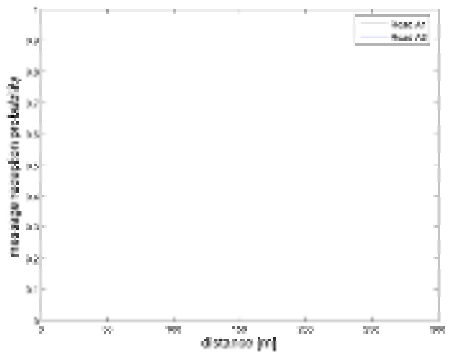


Figure 5-369: Reception Prob. of Emergency Messages – Scenario 30, Rd. A, Sender on Rd. B

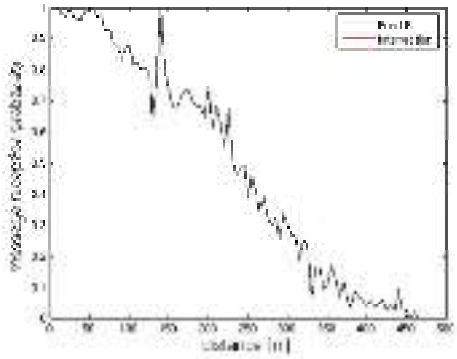


Figure 5-370: Reception Prob. of Emergency Messages – Scenario 30, Rd. B, Sender on Rd. B

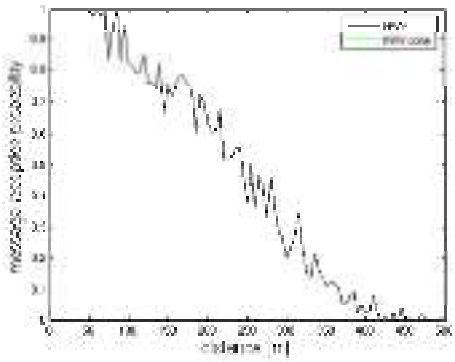


Figure 5-371: Reception Prob. of Emergency Messages – Scenario 30, HWY, Sender on Rd. B

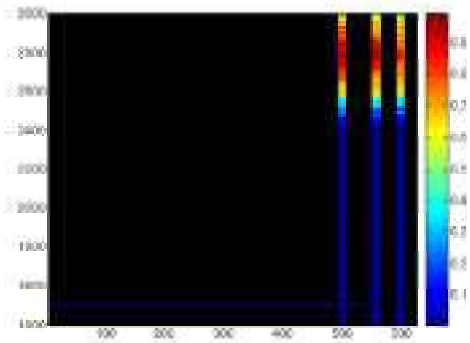


Figure 5-372: Reception Prob. of Emergency Messages-Scenario 30, Sender on Rd. B

5.2.14.4 Reception Probability of Emergency Messages From OBU on HWY

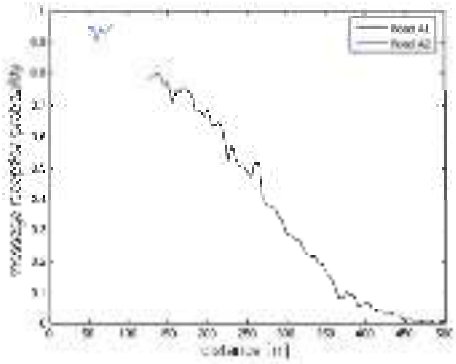


Figure 5-373: Reception Prob. of Emergency Messages – Scenario 30, Rd. A, Sender on HWY

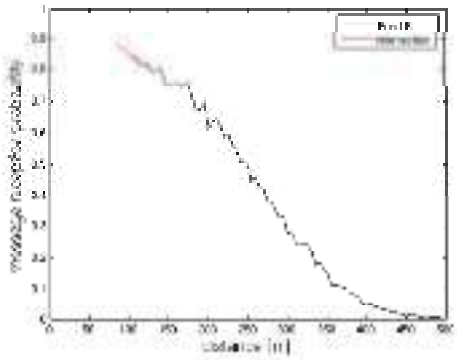


Figure 5-374: Reception Prob. of Emergency Messages – Scenario 30, Rd. B, Sender on HWY

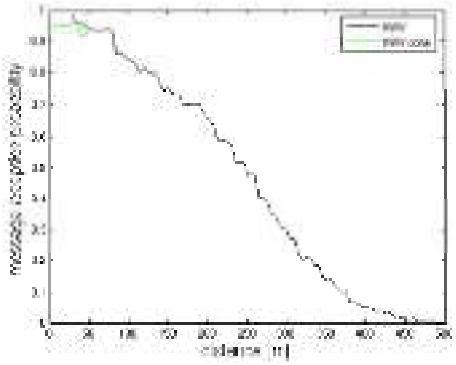


Figure 5-375: Reception Prob. of Emergency Messages – Scenario 30, HWY, Sender on HWY

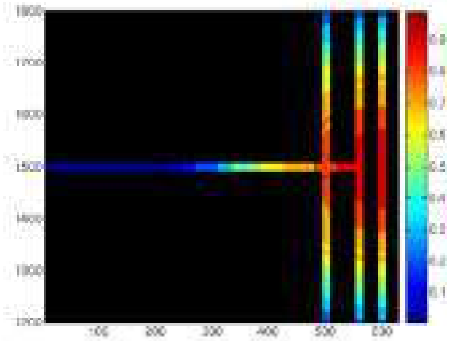


Figure 5-376: Reception Prob. of Emergency Messages-Scenario 30, Sender on HWY

5.2.15 Scenario 31

Simulation Scenario Setting:

RF Model	Distributed
Emergency Message Sender	RSU, 10Hz/ 500 bytes/ 200m
Corner Model	Tall building
Pt	300m coverage
Routine Message Frequency	1Hz

5.2.15.1 Reception Probability of Emergency Messages

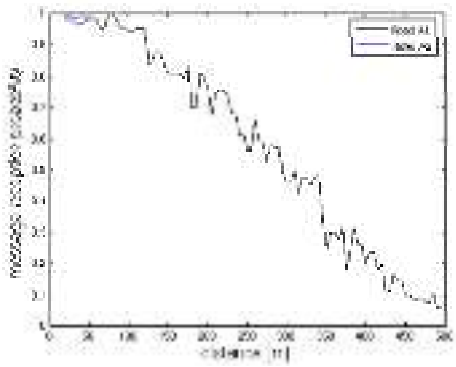


Figure 5-377: Reception Probability of Emergency Messages-Scenario 31, Road A, Sender RSU

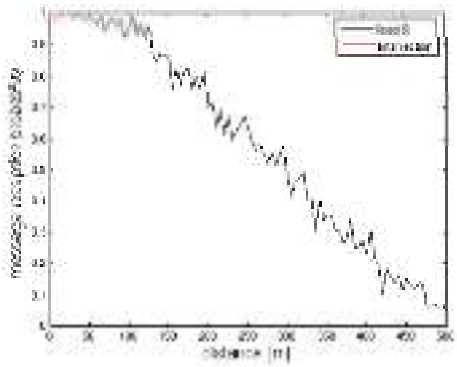


Figure 5-378: Reception Probability of Emergency Messages-Scenario 31, Road B, Sender RSU

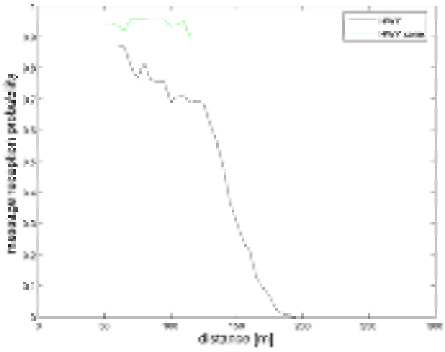


Figure 5-379: Reception Probability of Emergency Messages-Scenario 31, HWY, Sender RSU

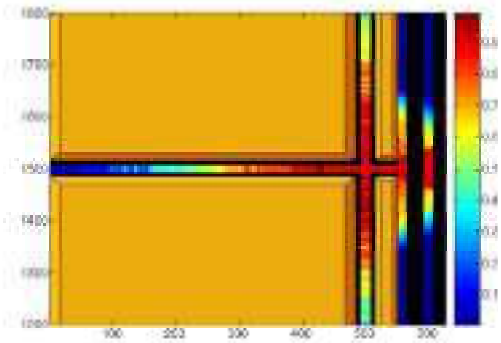


Figure 5-380: Reception Probability of Emergency Messages-Scenario 31, Sender RSU

5.2.16 Scenario 32

Simulation Scenario Setting:

RF Model	Distributed
Emergency Message Sender	OBUs on Road A1, A2, B and HWY
Corner Model	tall building
Pt	300m coverage
Routine Message Frequency	1Hz

5.2.16.1 Reception Probability of Emergency Messages From OBU on A1

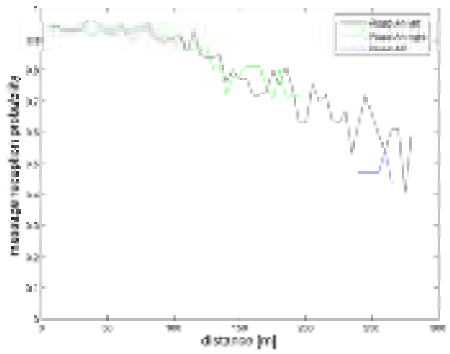


Figure 5-381: Reception Prob. of Emergency Messages – Scenario 32, Rd. A, Sender on Rd. A1

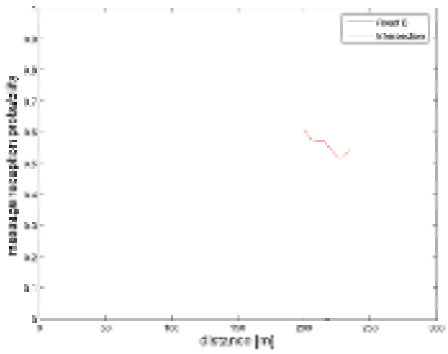


Figure 5-382: Reception Prob. of Emergency Messages – Scenario 32, Rd. B, Sender on Rd. A1

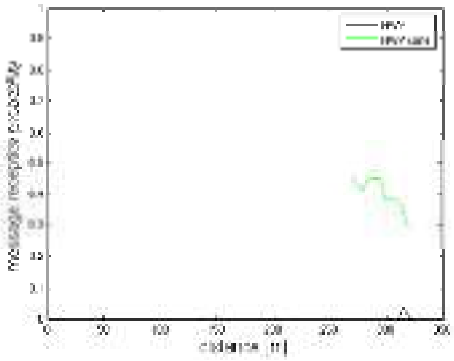


Figure 5-383: Reception Prob. of Emergency Messages – Scenario 32, HWY, Sender on Rd. A1

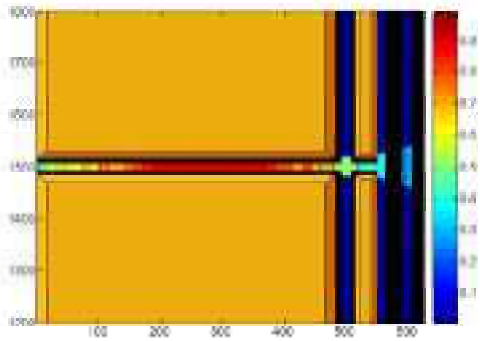


Figure 5-384: Reception Prob. of Emergency Messages-Scenario 32, Sender on Rd. A1

5.2.16.2 Reception Probability of Emergency Messages From OBU on A2

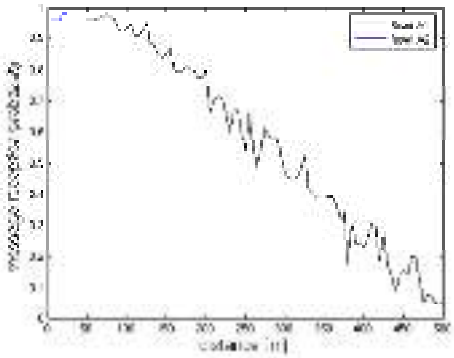


Figure 5-385: Reception Prob. of Emergency Messages – Scenario 32, Rd. A, Sender on Rd. A2

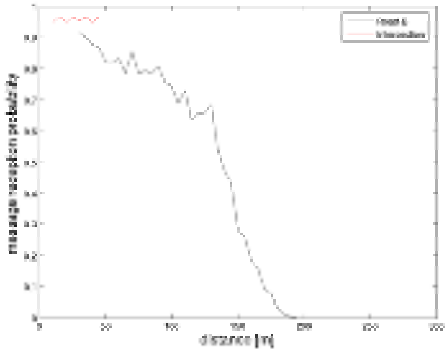


Figure 5-386: Reception Prob. of Emergency Messages – Scenario 32, Rd. B, Sender on Rd. A2

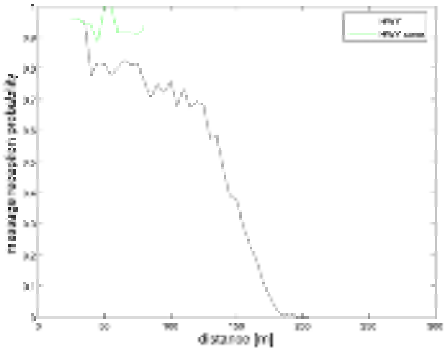


Figure 5-387: Reception Prob. of Emergency Messages – Scenario 32, HWY, Sender on Rd. A2

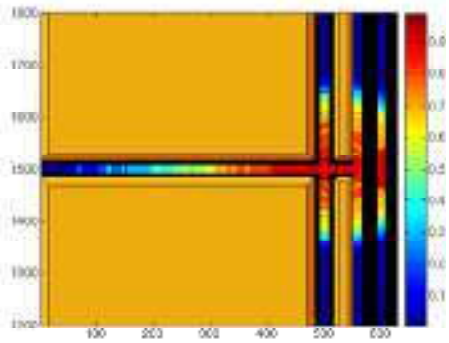


Figure 5-388: Reception Prob. of Emergency Messages-Scenario 32, Sender on Rd. A2

5.2.16.3 Reception Probability of Emergency Messages From OBU on B

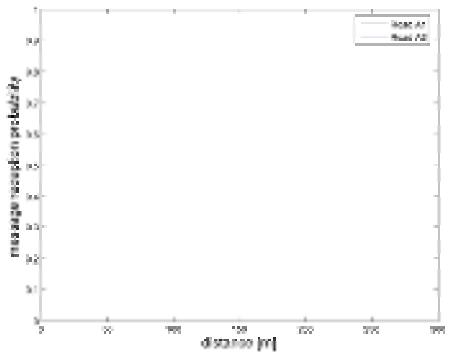


Figure 5-389: Reception Prob. of Emergency Messages – Scenario 32, Rd. A, Sender on Rd. B

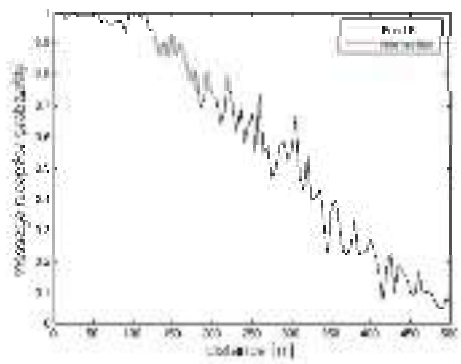


Figure 5-390: Reception Prob. of Emergency Messages – Scenario 32, Rd. B, Sender on Rd. B

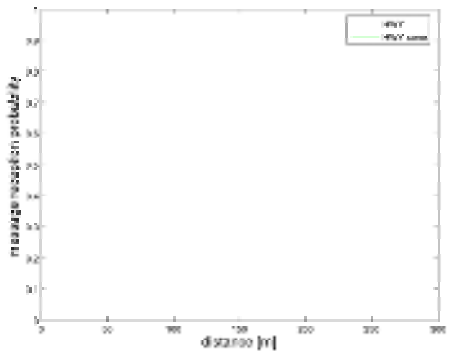


Figure 5-391: Reception Prob. of Emergency Messages – Scenario 32, HWY, Sender on Rd. B

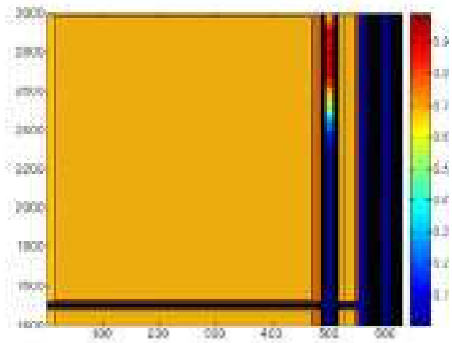


Figure 5-392: Reception Prob. of Emergency Messages-Scenario 32, Sender on Rd. B

5.2.16.4 Reception Probability of Emergency Messages From OBU on HWY

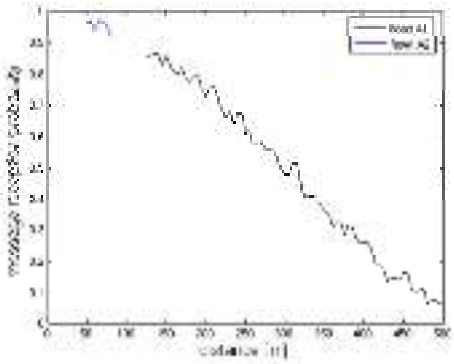


Figure 5-393: Reception Prob. of Emergency Messages – Scenario 32, Rd. A, Sender on HWY

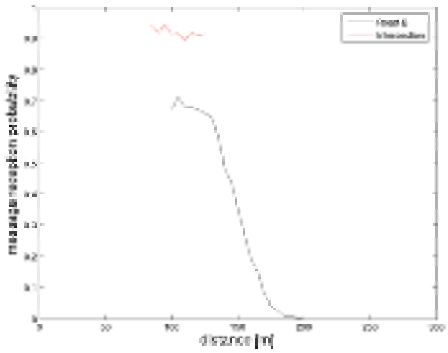


Figure 5-394: Reception Prob. of Emergency Messages – Scenario 32, Rd. B, Sender on HWY

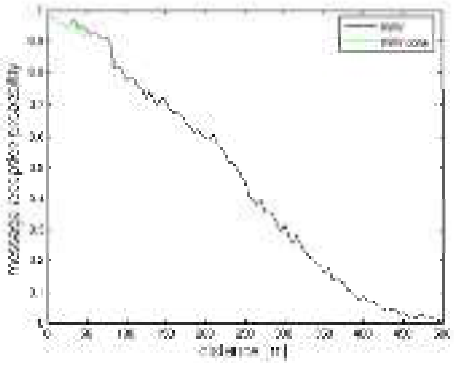


Figure 5-395: Reception Prob. of Emergency Messages – Scenario 32, HWY, Sender on HWY

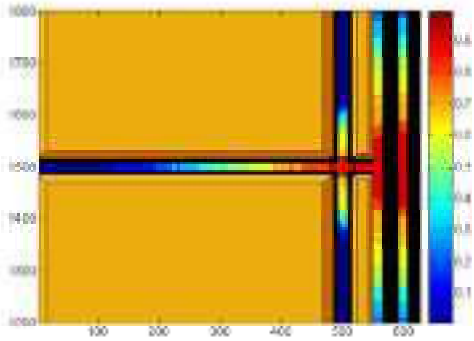


Figure 5-396: Reception Prob. of Emergency Messages-Scenario 32, Sender on HWY

5.2.17 Scenario 33

Simulation Scenario Setting:

RF Model	Distributed
Emergency Message Sender	RSU, 10Hz/ 500 bytes/ 200m
Corner Model	no buildings
Pt	200m coverage
Routine Message Frequency	5Hz

5.2.17.1 Reception Probability of Emergency Messages

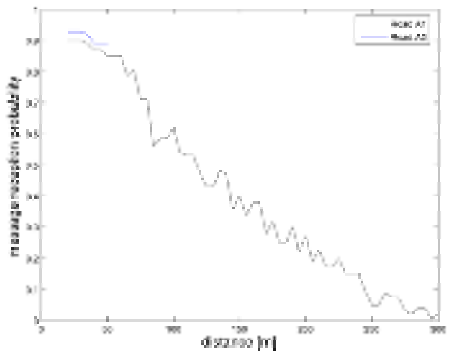


Figure 5-397: Reception Probability of Emergency Messages-Scenario 33, Road A, Sender RSU

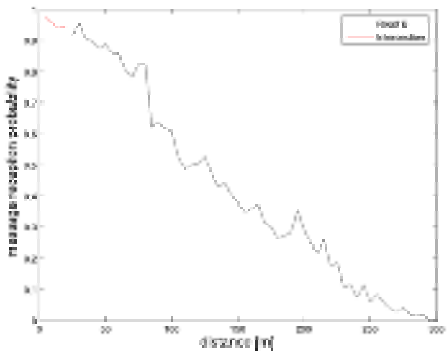


Figure 5-398: Reception Probability of Emergency Messages-Scenario 33, Road B, Sender RSU

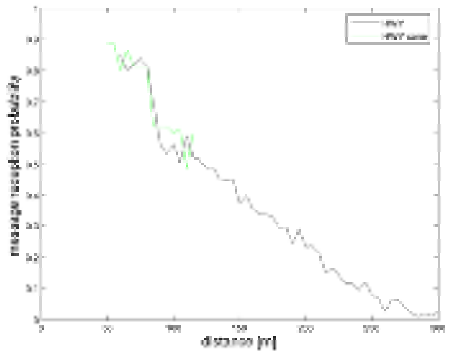


Figure 5-399: Reception Probability of Emergency Messages-Scenario 33, HWY, Sender RSU

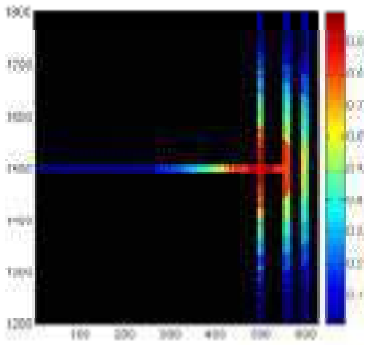


Figure 5-400: Reception Probability of Emergency Messages-Scenario 33, Sender RSU

5.2.17.2 Reception Probability of Routine Messages

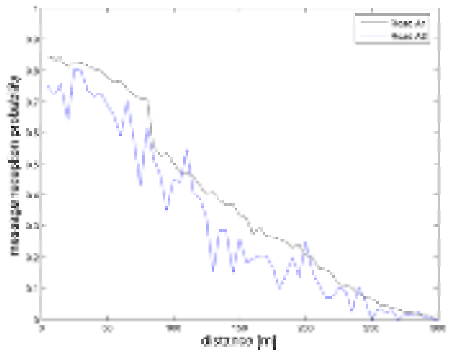


Figure 5-401: Reception Probability of Routine Messages on Road A, Scenario 33

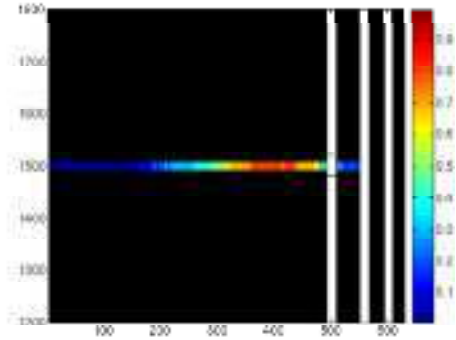


Figure 5-402: Reception Probability of Routine Messages on Road A, Scenario 33

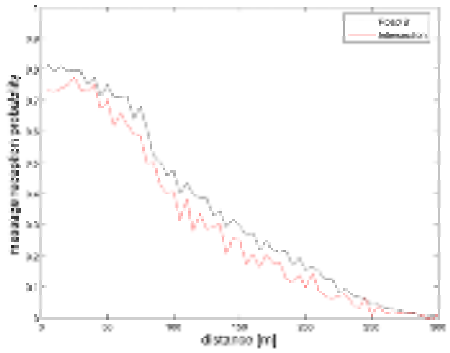


Figure 5-403: Reception Probability of Routine Messages on Road B, Scenario 33

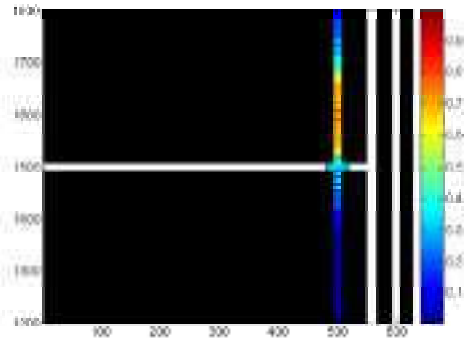


Figure 5-404: Reception Probability of Routine Messages on Road B, Scenario 33

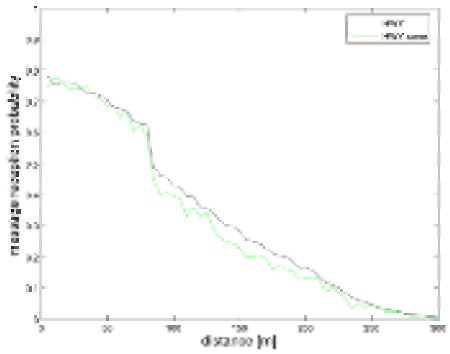


Figure 5-405: Reception Probability of Routine Messages on HWY, Scenario 33

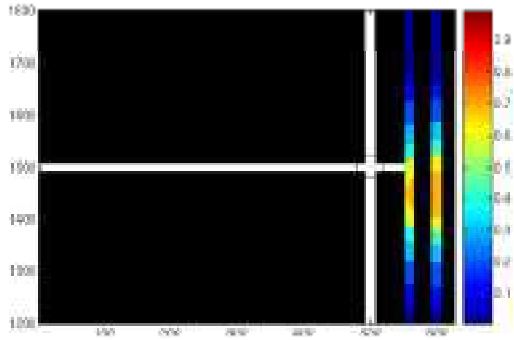


Figure 5-406: Reception Probability of Routine Messages on HWY, Scenario 33

5.2.18 Scenario 34

Simulation Scenario Setting:

RF Model	Distributed
Emergency Message Sender	OBUs on Road A1, A2, B and HWY
Corner Model	no building
Pt	200m coverage
Routine Message Frequency	5Hz

5.2.18.1 Reception Probability of Emergency Messages From OBU on A1

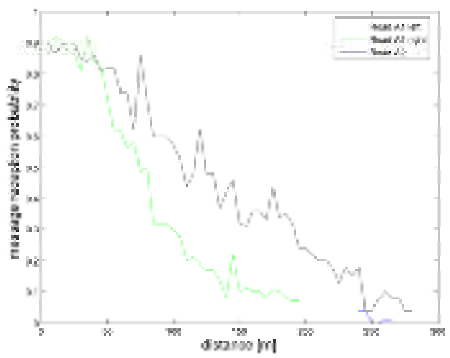


Figure 5-407: Reception Prob. of Emergency Messages – Scenario 34, Rd. A, Sender on Rd. A1

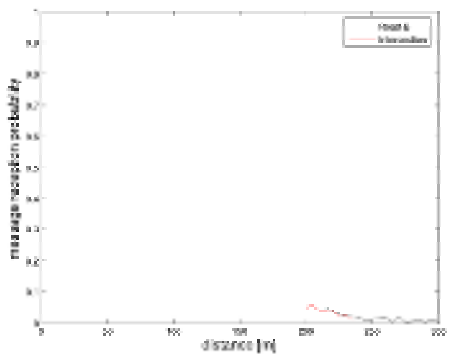


Figure 5-408: Reception Prob. of Emergency Messages – Scenario 34, Rd. B, Sender on Rd. A1

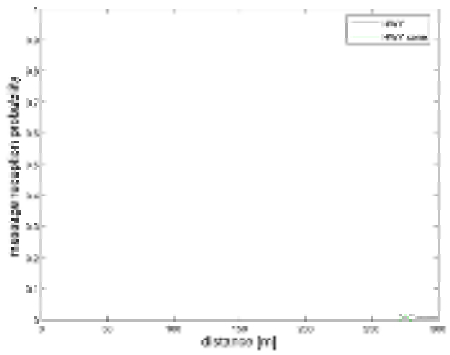


Figure 5-409: Reception Prob. of Emergency Messages – Scenario 34, HWY, Sender on Rd. A1

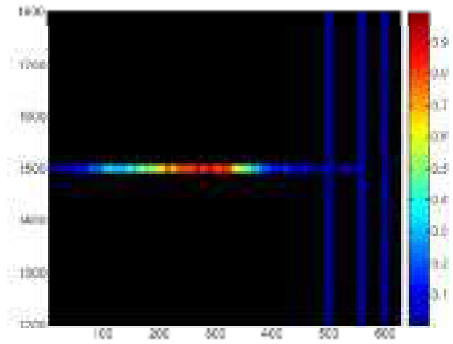


Figure 5-410: Reception Prob. of Emergency Messages-Scenario 34, Sender on Rd. A1

5.2.18.2 Reception Probability of Emergency Messages From OBU on A2

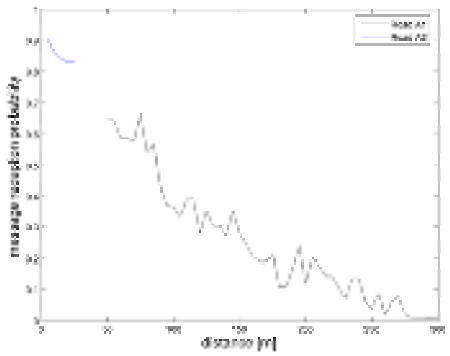


Figure 5-411: Reception Prob. of Emergency Messages – Scenario 34, Rd. A, Sender on Rd. A2

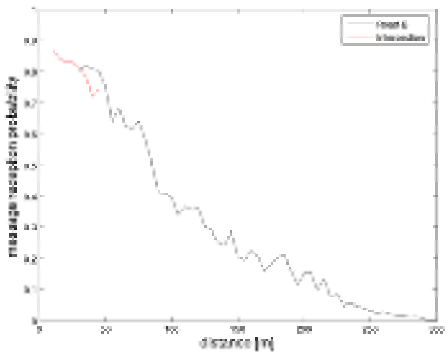


Figure 5-412: Reception Prob. of Emergency Messages – Scenario 34, Rd. B, Sender on Rd. A2

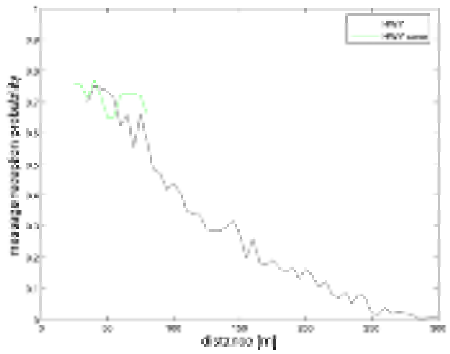


Figure 5-413: Reception Prob. of Emergency Messages – Scenario 34, HWY, Sender on Rd. A2

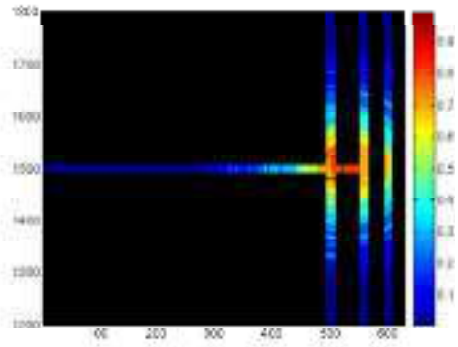


Figure 5-414: Reception Prob. of Emergency Messages-Scenario 34, Sender on Rd. A2

5.2.18.3 Reception Probability of Emergency Messages From OBU on B

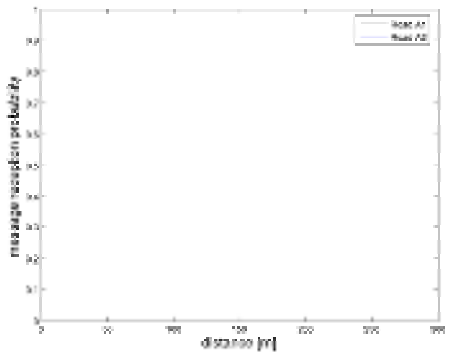


Figure 5-415: Reception Prob. of Emergency Messages – Scenario 34, Rd. A, Sender on Rd. B

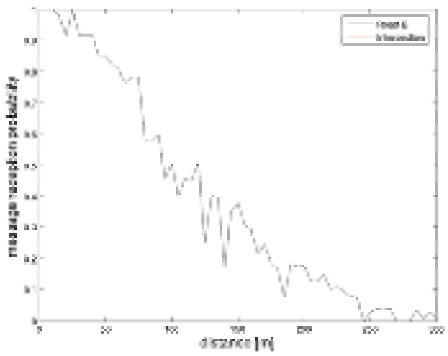


Figure 5-416: Reception Prob. of Emergency Messages – Scenario 34, Rd. B, Sender on Rd. B

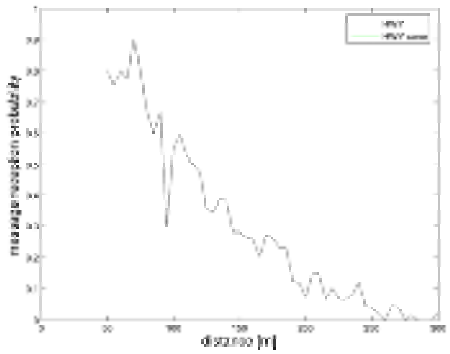


Figure 5-417: Reception Prob. of Emergency Messages – Scenario 34, HWY, Sender on Rd. B

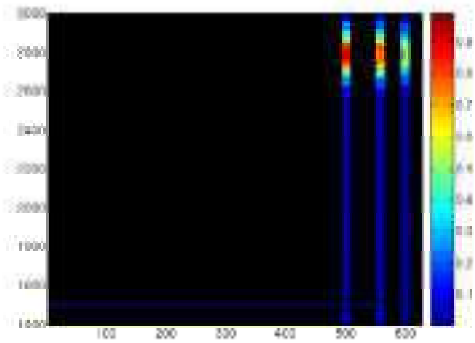


Figure 5-418: Reception Prob. of Emergency Messages-Scenario 34, Sender on Rd. B

5.2.18.4 Reception Probability of Emergency Messages From OBU on HWY

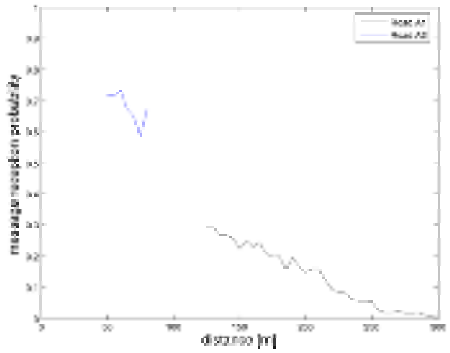


Figure 5-419: Reception Prob. of Emergency Messages – Scenario 34, Rd. A, Sender on HWY

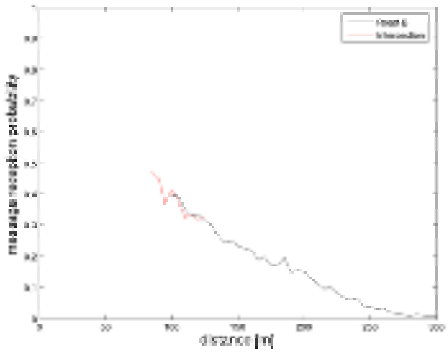


Figure 5-420: Reception Prob. of Emergency Messages – Scenario 34, Rd. B, Sender on HWY

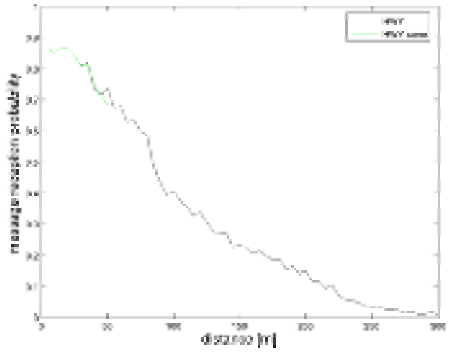


Figure 5-421: Reception Prob. of Emergency Messages – Scenario 34, HWY, Sender on HWY

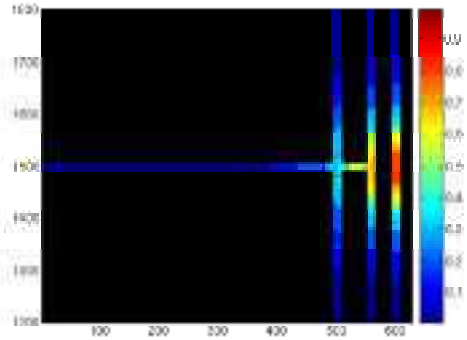


Figure 5-422: Reception Prob. of Emergency Messages-Scenario 34, Sender on HWY

5.2.19 Scenario 35

Simulation Scenario Setting:

RF Model	Distributed
Emergency Message Sender	RSU, 10Hz/ 500 bytes/ 200m
Corner Model	Tall building
Pt	200m coverage
Routine Message Frequency	5Hz

5.2.19.1 Reception Probability of Emergency Messages

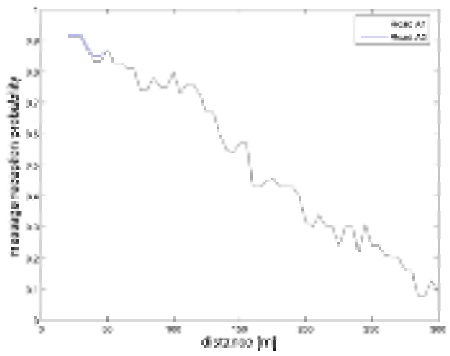


Figure 5-423: Reception Probability of Emergency Messages-Scenario 35, Road A, Sender RSU

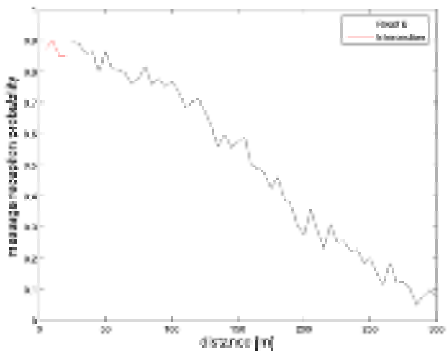


Figure 5-424: Reception Probability of Emergency Messages-Scenario 35, Road B, Sender RSU

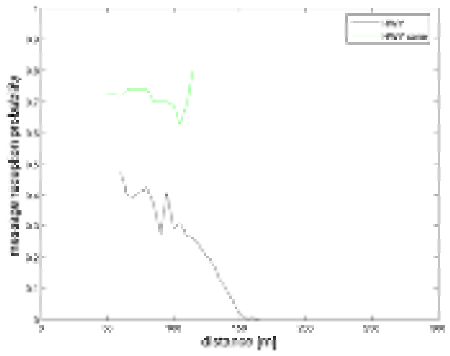


Figure 5-425: Reception Probability of Emergency Messages-Scenario 35, HWY, Sender RSU

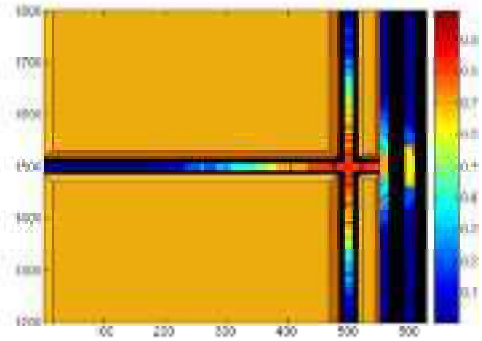


Figure 5-426: Reception Probability of Emergency Messages-Scenario 35, Sender RSU

5.2.19.2 Routine Message Reception Probability

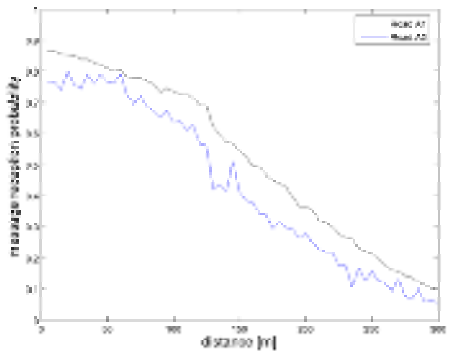


Figure 5-427: Reception Probability of Routine Messages on Road A Scenario 35

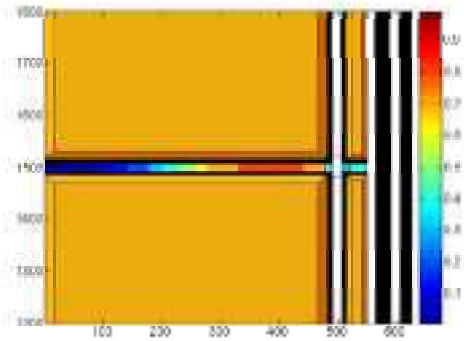


Figure 5-428: Reception Probability of Routine Messages on Road A Scenario 35

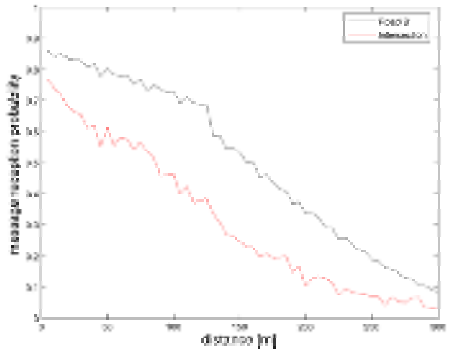


Figure 5-429: Reception Probability of Routine Messages on Road B Scenario 35

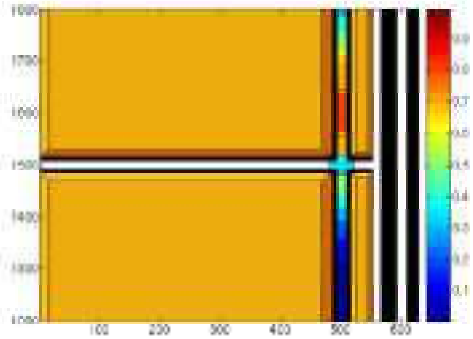


Figure 5-430: Reception Probability of Routine Messages on Road B Scenario 35

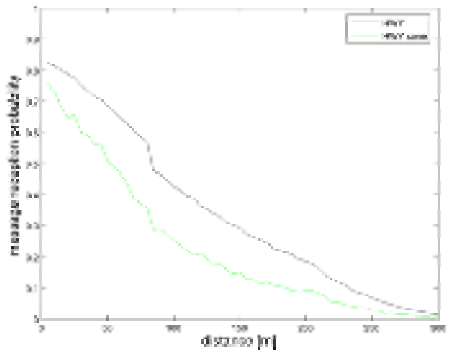


Figure 5-431: Reception Probability of Routine Messages on HWY Scenario 35

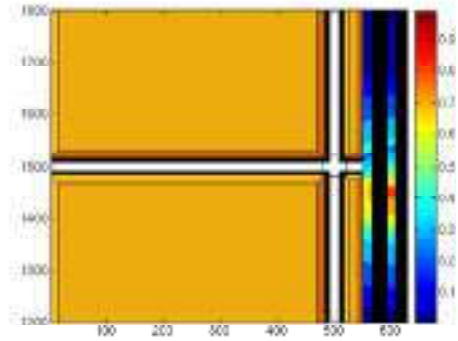


Figure 5-432: Reception Probability of Routine Messages on HWY Scenario 35

5.2.20 Scenario 36

Simulation Scenario Setting:

RF Model	Distributed
Emergency Message Sender	OBUs on Road A1, A2, B and HWY
Corner Model	tall building
Pt	200m coverage
Routine Message Frequency	5Hz

5.2.20.1 Reception Probability of Emergency Messages From OBU on A1

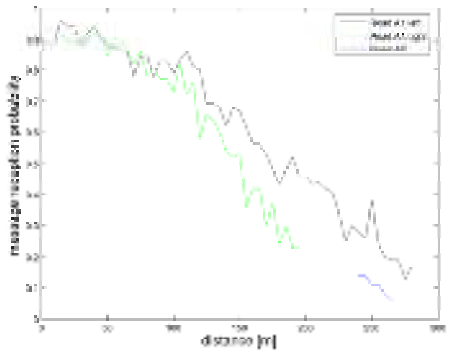


Figure 5-433: Reception Prob. of Emergency Messages – Scenario 36, Rd. A, Sender on Rd. A1

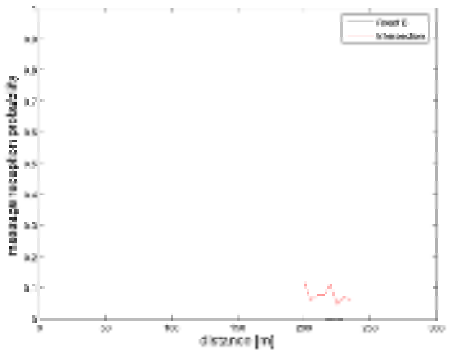


Figure 5-434: Reception Prob. of Emergency Messages – Scenario 36, Rd. B, Sender on Rd. A1

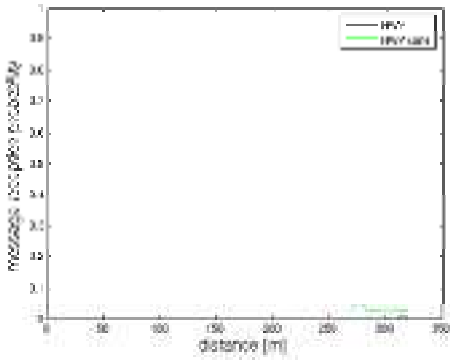


Figure 5-435: Reception Prob. of Emergency Messages – Scenario 36, HWY, Sender on Rd. A1

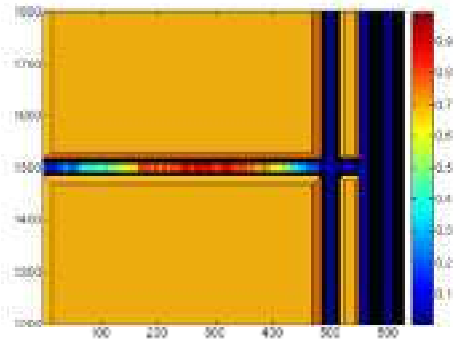


Figure 5-436: Reception Prob. of Emergency Messages-Scenario 36, Sender on Rd. A1

5.2.20.2 Reception Probability of Emergency Messages From OBU on A2

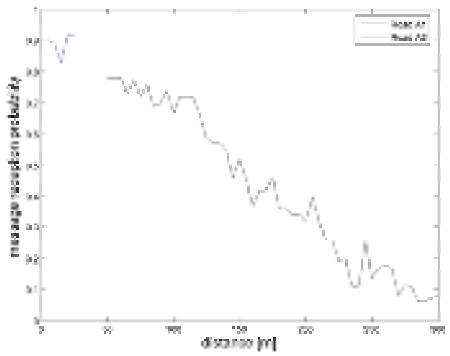


Figure 5-437: Reception Prob. of Emergency Messages – Scenario 36, Rd. A, Sender on Rd. A2

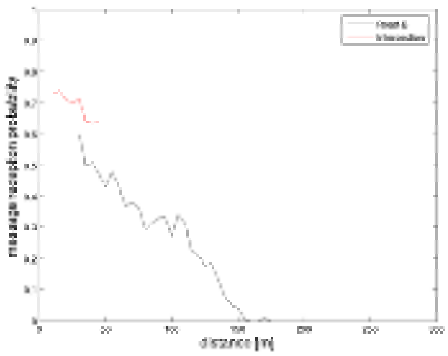


Figure 5-438: Reception Prob. of Emergency Messages – Scenario 36, Rd. B, Sender on Rd. A2

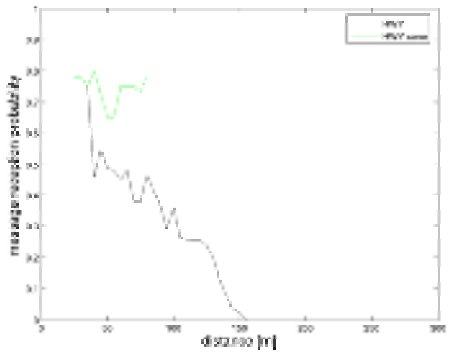


Figure 5-439: Reception Prob. of Emergency Messages – Scenario 36, HWY, Sender on Rd. A2

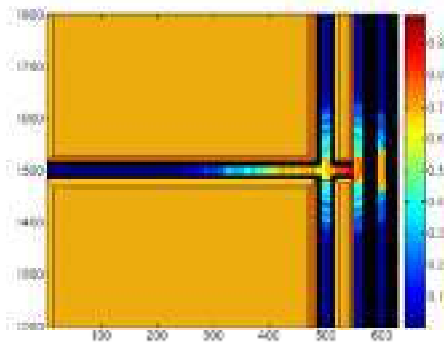


Figure 5-440: Reception Prob. of Emergency Messages-Scenario 36, Sender on Rd. A2

5.2.20.3 Reception Probability of Emergency Messages From OBU on B

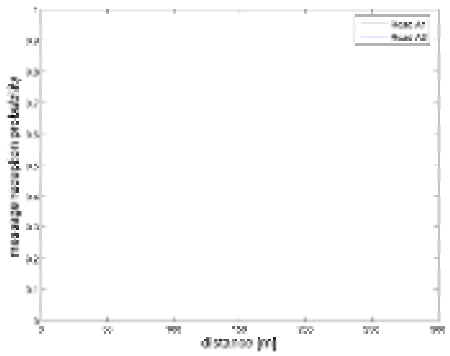


Figure 5-441: Reception Prob. of Emergency Messages – Scenario 36, Rd. A, Sender on Rd. B

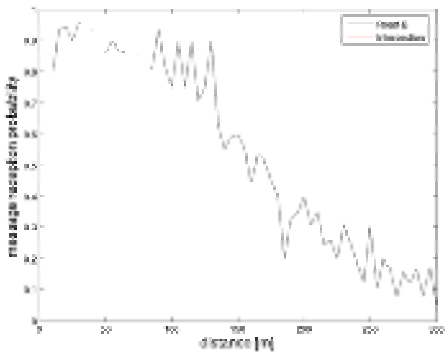


Figure 5-442: Reception Prob. of Emergency Messages – Scenario 36, Rd. B, Sender on Rd. B

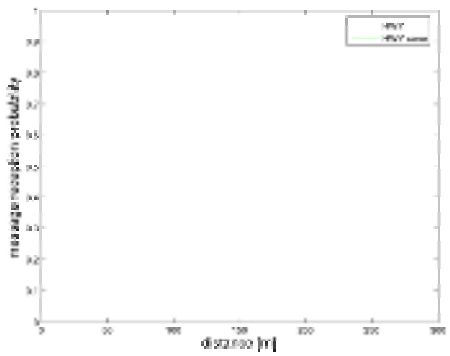


Figure 5-443: Reception Prob. of Emergency Messages – Scenario 36, HWY, Sender on Rd. B

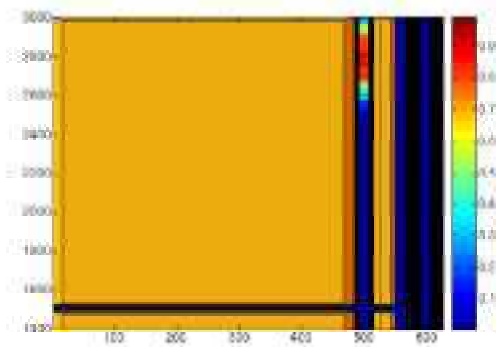


Figure 5-444: Reception Prob. of Emergency Messages-Scenario 36, Sender on Rd. B

5.2.20.4 Reception Probability of Emergency Messages From OBU on HWY

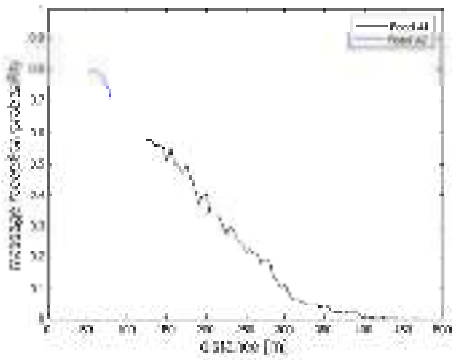


Figure 5-445: Reception Prob. of Emergency Messages – Scenario 36, Rd. A, Sender on HWY

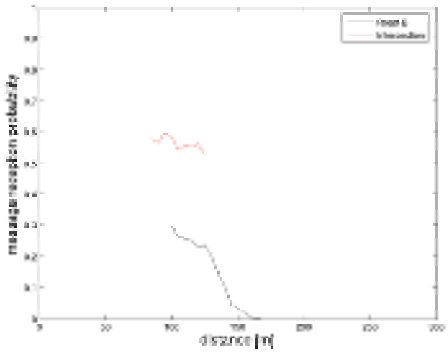


Figure 5-446: Reception Prob. of Emergency Messages – Scenario 36, Rd. B, Sender on HWY

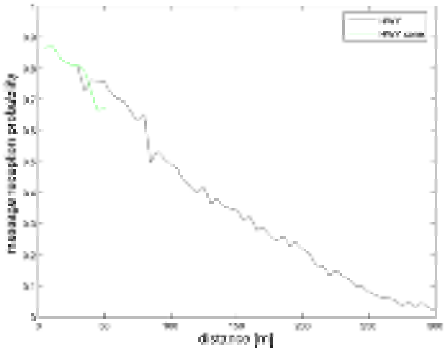


Figure 5-447: Reception Prob. of Emergency Messages – Scenario 36, HWY, Sender on HWY

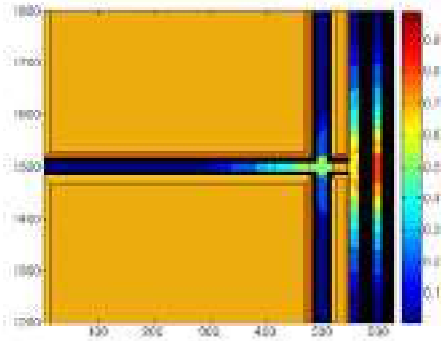


Figure 5-448: Reception Prob. of Emergency Messages-Scenario 36, Sender on HWY

5.2.21 Scenario 37

Simulation Scenario Setting:

RF Model	Distributed
Emergency Message Sender	RSU, 10Hz/ 500 bytes/ 200m
Corner Model	no buildings
Pt	300m coverage
Routine Message Frequency	5Hz

5.2.21.1 Reception Probability of Emergency Messages

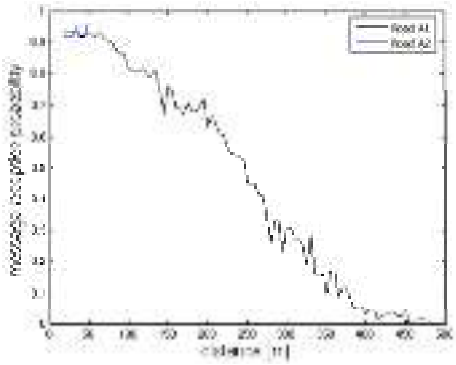


Figure 5-449: Reception Probability of Emergency Messages-Scenario 37, Road A, Sender RSU

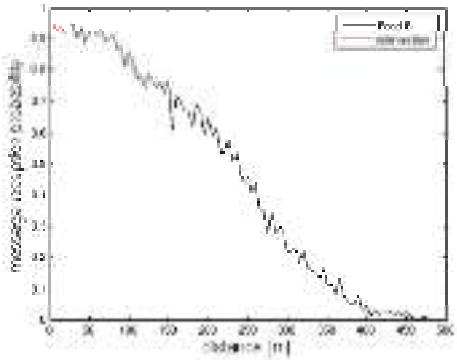


Figure 5-450: Reception Probability of Emergency Messages-Scenario 37, Road B, Sender RSU

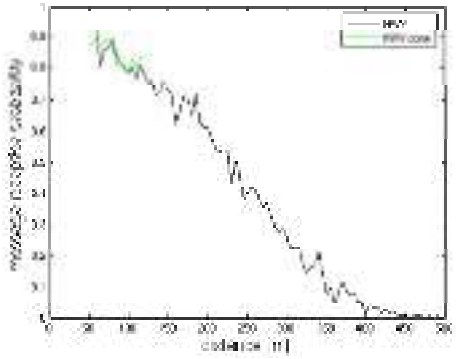


Figure 5-451: Reception Probability of Emergency Messages-Scenario 37, HWY, Sender RSU

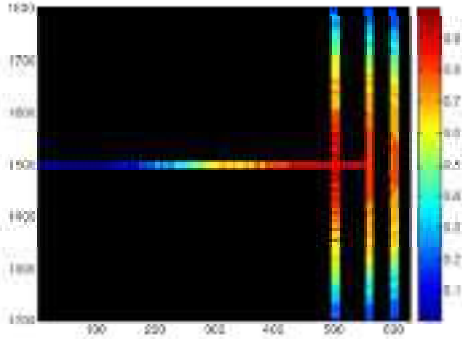


Figure 5-452: Reception Probability of Emergency Messages-Scenario 37, Sender RSU

5.2.22 Scenario 38

Simulation Scenario Setting:

RF Model	Distributed
Emergency Message Sender	OBUs on Road A1, A2, B and HWY
Corner Model	no building
Pt	300m coverage
Routine Message Frequency	5Hz

5.2.22.1 Reception Probability of Emergency Messages From OBU on A1

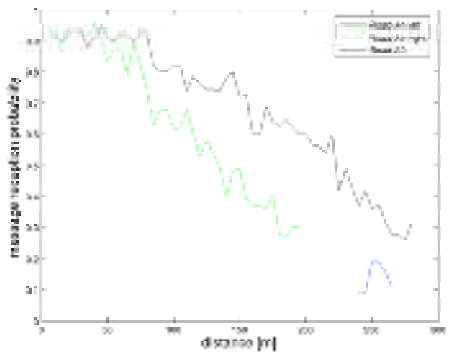


Figure 5-453: Reception Prob. of Emergency Messages – Scenario 38, Rd. A, Sender on Rd. A1

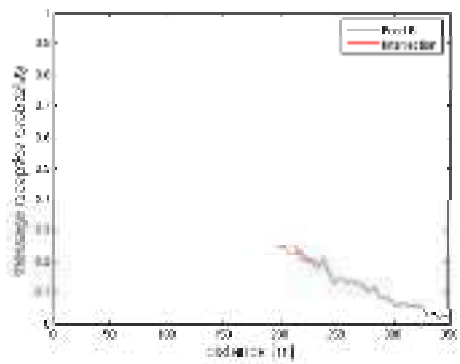


Figure 5-454: Reception Prob. of Emergency Messages – Scenario 38, Rd. B, Sender on Rd. A1

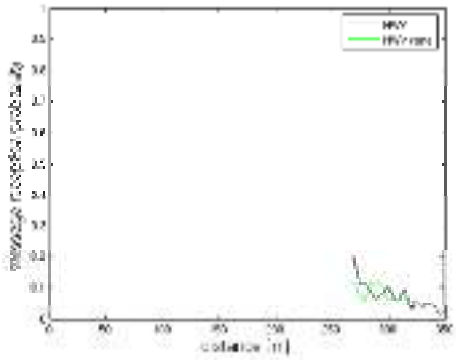


Figure 5-455: Reception Prob. of Emergency Messages – Scenario 38, HWY, Sender on Rd. A1

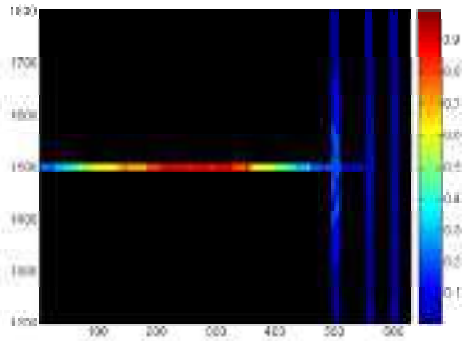


Figure 5-456: Reception Prob. of Emergency Messages-Scenario 38, Sender on Rd. A1

5.2.22.2 Reception Probability of Emergency Messages From OBU on A2

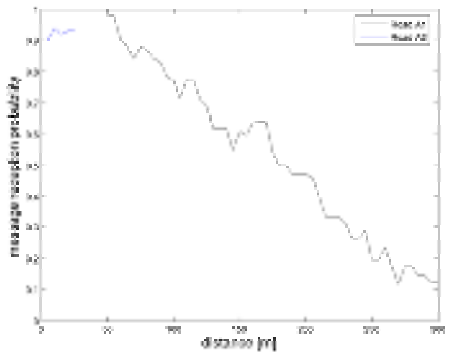


Figure 5-457: Reception Prob. of Emergency Messages – Scenario 38, Rd. A, Sender on Rd. A2

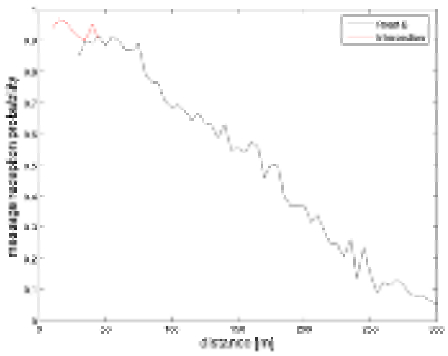


Figure 5-458: Reception Prob. of Emergency Messages – Scenario 38, Rd. B, Sender on Rd. A2

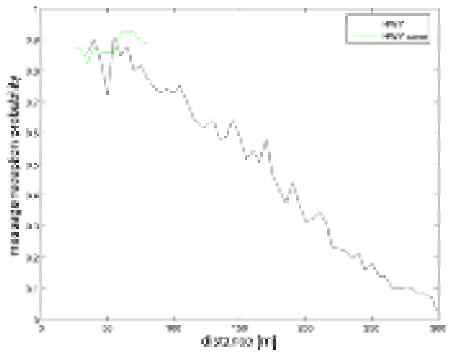


Figure 5-459: Reception Prob. of Emergency Messages – Scenario 38, HWY, Sender on Rd. A2

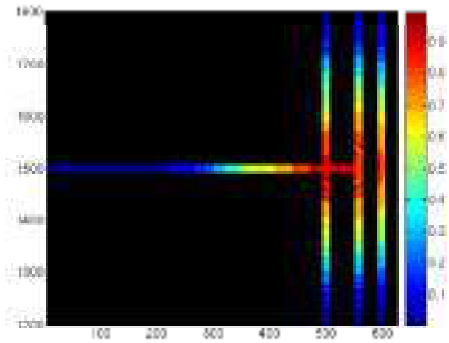


Figure 5-460: Reception Prob. of Emergency Messages-Scenario 38, Sender on Rd. A2

5.2.22.3 Reception Probability of Emergency Messages From OBU on B

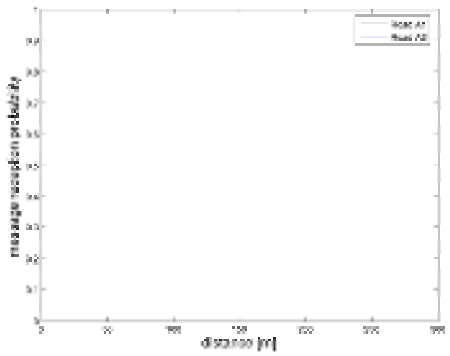


Figure 5-461: Reception Prob. of Emergency Messages – Scenario 38, Rd. A, Sender on Rd. B

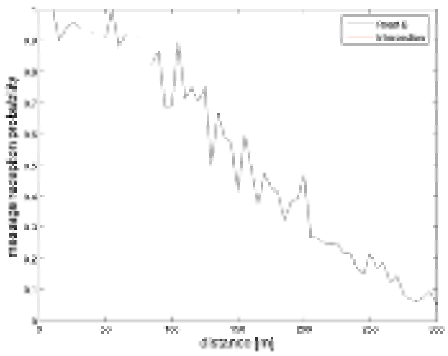


Figure 5-462: Reception Prob. of Emergency Messages – Scenario 38, Rd. B, Sender on Rd. B

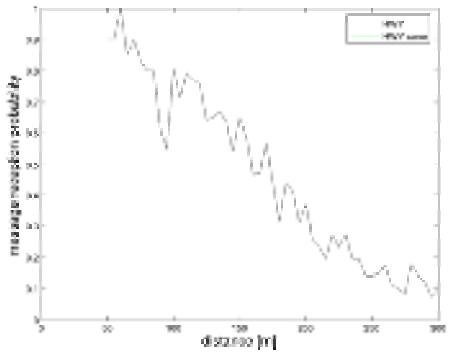


Figure 5-463: Reception Prob. of Emergency Messages – Scenario 38, HWY, Sender on Rd. B

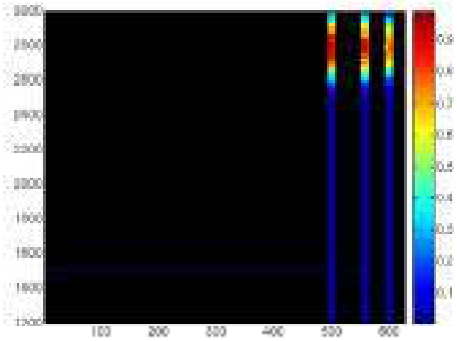


Figure 5-464: Reception Prob. of Emergency Messages-Scenario 38, Sender on Rd. B

5.2.22.4 Reception Probability of Emergency Messages From OBU on HWY

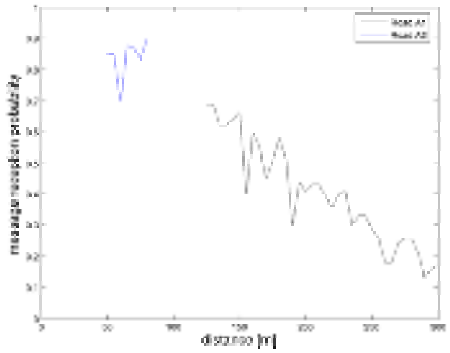


Figure 5-465: Reception Prob. of Emergency Messages – Scenario 38, Rd. A, Sender on HWY

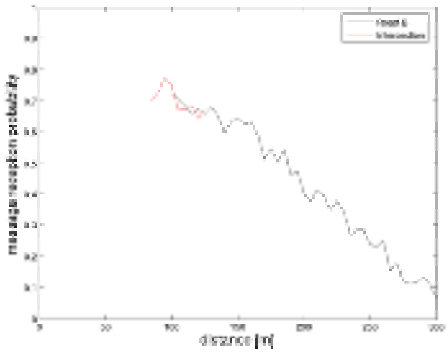


Figure 5-466: Reception Prob. of Emergency Messages – Scenario 38, Rd. B, Sender on HWY

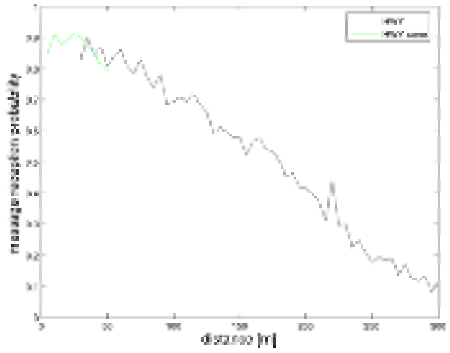


Figure 5-467: Reception Prob. of Emergency Messages – Scenario 38, HWY, Sender on HWY

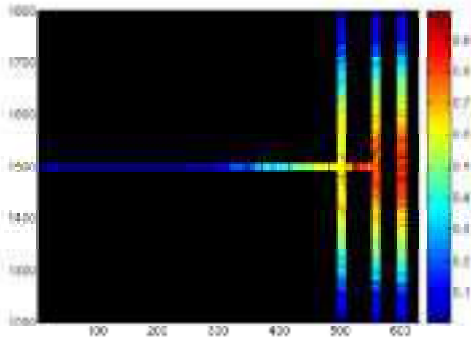


Figure 5-468: Reception Prob. of Emergency Messages-Scenario 38, Sender on HWY

5.2.23 Scenario 39

Simulation Scenario Setting:

RF Model	Distributed
Emergency Message Sender	RSU, 10Hz/ 500 bytes/ 200m
Corner Model	Tall building
Pt	300m coverage
Routine Message Frequency	5Hz

5.2.23.1 Reception Probability of Emergency Messages

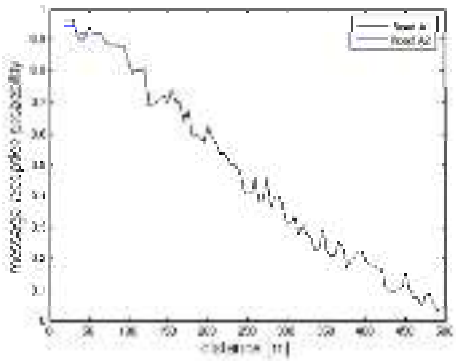


Figure 5-469: Reception Probability of Emergency Messages-Scenario 39, Road A, Sender RSU

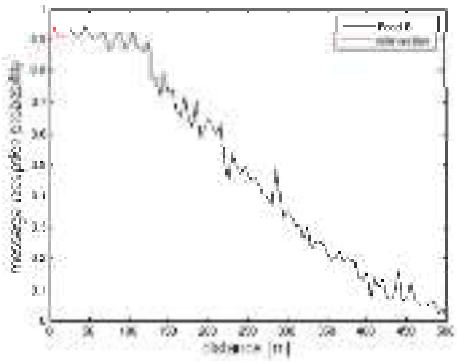


Figure 5-470: Reception Probability of Emergency Messages-Scenario 39, Road B, Sender RSU

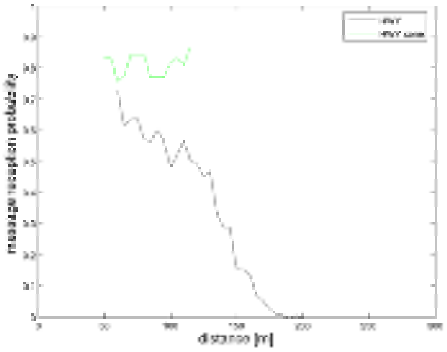


Figure 5-471: Reception Probability of Emergency Messages-Scenario 39, HWY, Sender RSU

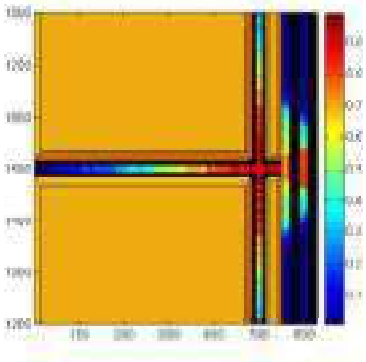


Figure 5-472: Reception Probability of Emergency Messages-Scenario 39, Sender RSU

5.2.24 Scenario 40

Simulation Scenario Setting:

RF Model	Distributed
Emergency Message Sender	OBUs on Road A1, A2, B and HWY
Corner Model	tall building
Pt	300m coverage
Routine Message Frequency	5Hz

5.2.24.1 Reception Probability of Emergency Messages From OBU on A1

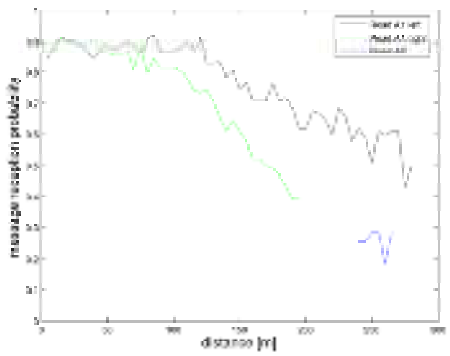


Figure 5-473: Reception Prob. of Emergency Messages – Scenario 40, Rd. A, Sender on Rd. A1

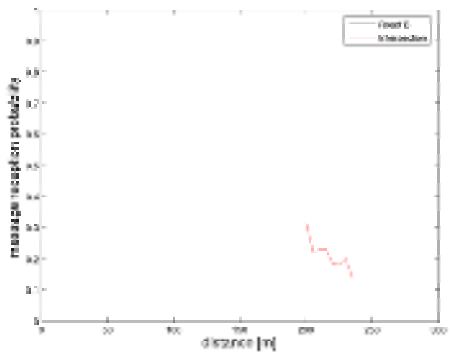


Figure 5-474: Reception Prob. of Emergency Messages – Scenario 40, Rd. B, Sender on Rd. A1

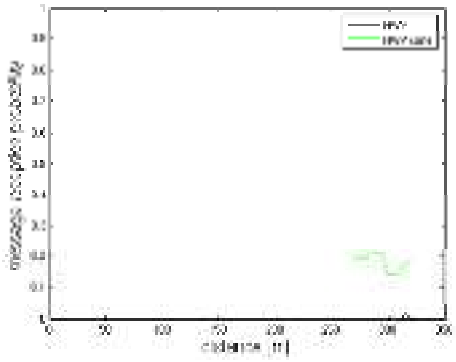


Figure 5-475: Reception Prob. of Emergency Messages – Scenario 40, HWY, Sender on Rd. A1

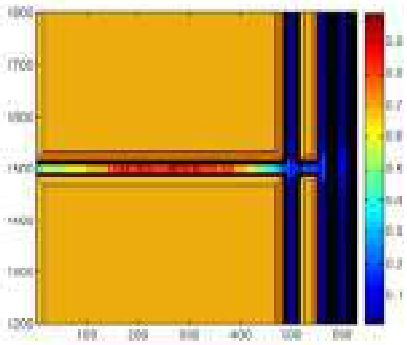


Figure 5-476: Reception Prob. of Emergency Messages-Scenario 40, Sender on Rd. A1

5.2.24.2 Reception Probability of Emergency Messages From OBU on A2

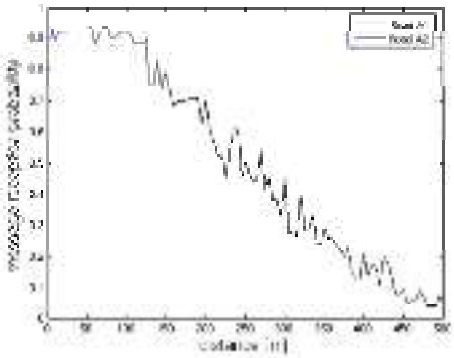


Figure 5-477: Reception Prob. of Emergency Messages – Scenario 40, Rd. A, Sender on Rd. A2

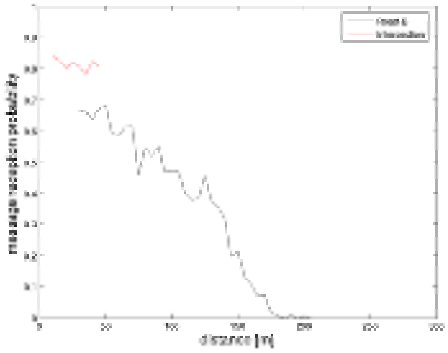


Figure 5-478: Reception Prob. of Emergency Messages – Scenario 40, Rd. B, Sender on Rd. A2

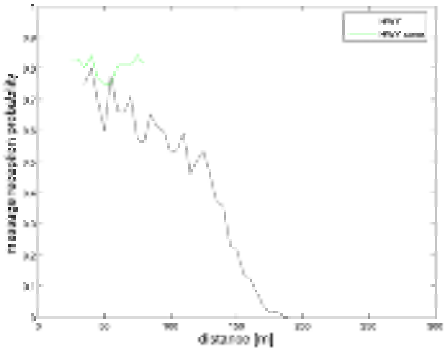


Figure 5-479: Reception Prob. of Emergency Messages – Scenario 40, HWY, Sender on Rd. A2

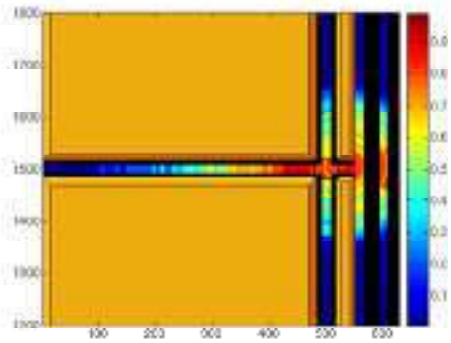


Figure 5-480: Reception Prob. of Emergency Messages-Scenario 40, Sender on Rd. A2

5.2.24.3 Reception Probability of Emergency Messages From OBU on B

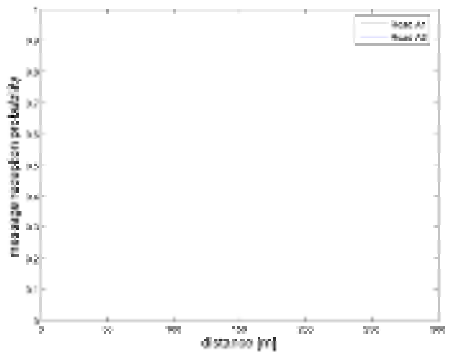


Figure 5-481: Reception Prob. of Emergency Messages – Scenario 40, Rd. A, Sender on Rd. B

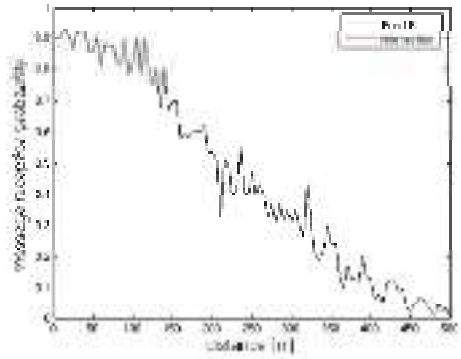


Figure 5-482: Reception Prob. of Emergency Messages – Scenario 40, Rd. B, Sender on Rd. B

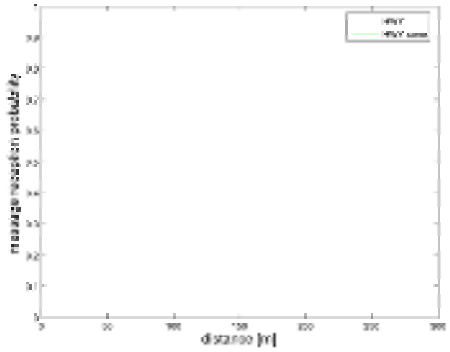


Figure 5-483: Reception Prob. of Emergency Messages – Scenario 40, HWY, Sender on Rd. B

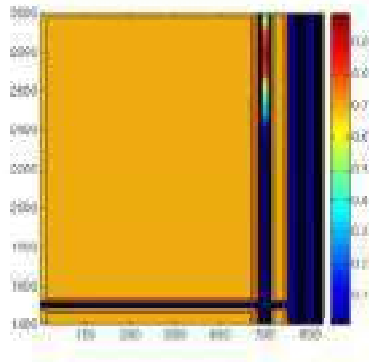


Figure 5-484: Reception Prob. of Emergency Messages-Scenario 40, Sender on Rd. B

5.2.24.4 Reception Probability of Emergency Messages From OBU on HWY

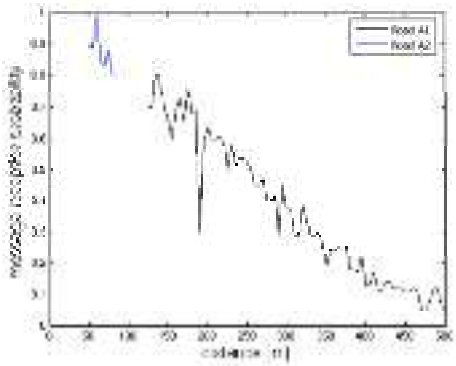


Figure 5-485: Reception Prob. of Emergency Messages – Scenario 40, Rd. A, Sender on HWY

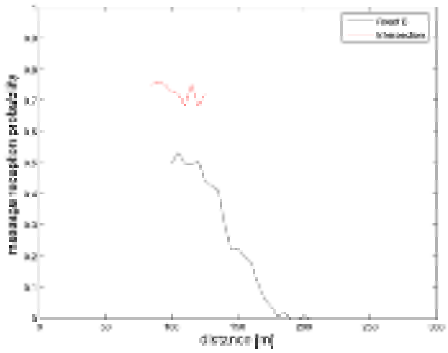


Figure 5-486: Reception Prob. of Emergency Messages – Scenario 40, Rd. B, Sender on HWY

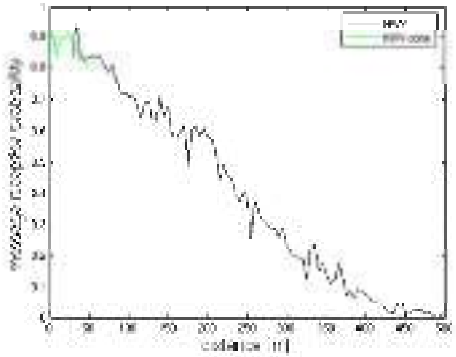


Figure 5-487: Reception Prob. of Emergency Messages – Scenario 40, HWY, Sender on HWY

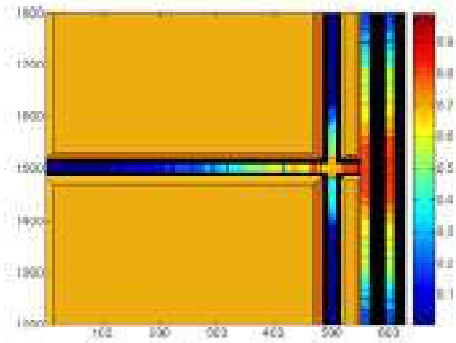


Figure 5-488: Reception Prob. of Emergency Messages-Scenario 40, Sender on HWY

5.3 Batch 3, Intersection RSU Retransmission of Routine Safety Messages

5.3.1 Scenario 41

Routine messages	2Hz 200byte 200m
RF Model	Distributed
Corner Model	tall building
Emergency Message	None, RSU forwarding routine message

Sender on A1

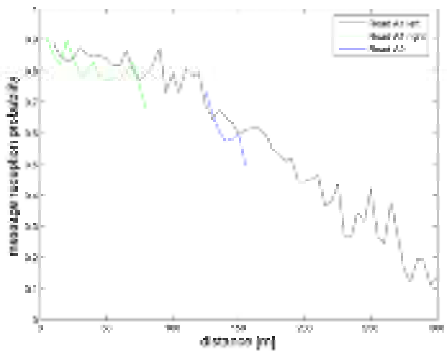


Figure 5-489: Reception Prob. of Routine Message Scenario 41, Rd. A, Sender on Rd. A1

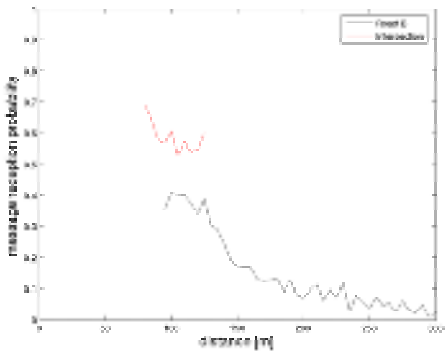


Figure 5-490: Reception Prob. of Routine Message Scenario 41, Rd. B, Sender on Rd. A1

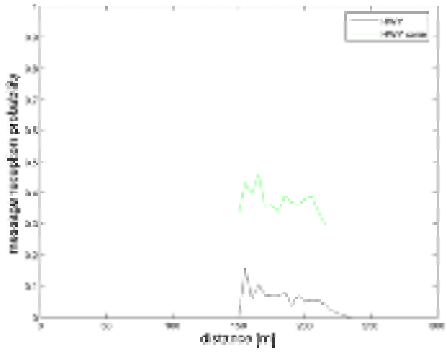


Figure 5-491: Reception Prob. of Routine Message Scenario 41, HWY, Sender on Rd. A1

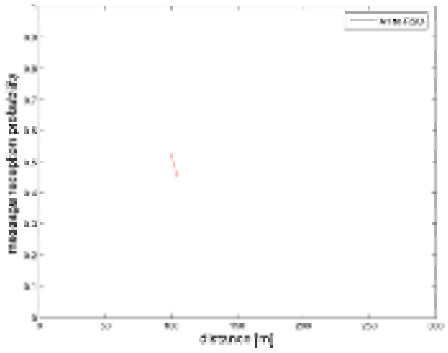
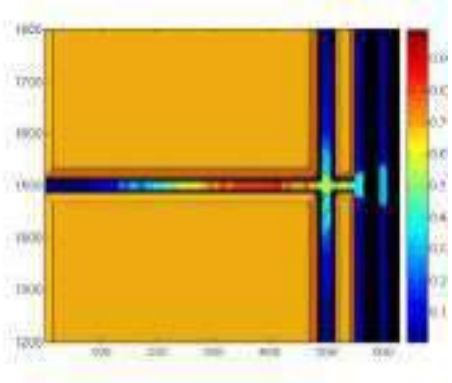


Figure 5-492: Reception Prob. of Routine Message Scenario 41, RSU, Sender on Rd. A1

 **Figure 5-493: Reception Probability of Emergency Messages-Scenario 41, Sender on Rd. A1**	

Sender on Road A2

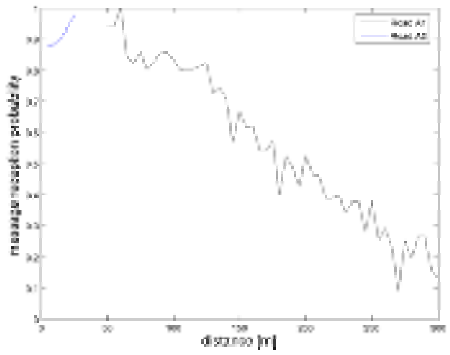


Figure 5-494: Reception Prob. of Routine Message Scenario 41, Rd. A, Sender on Rd. A2

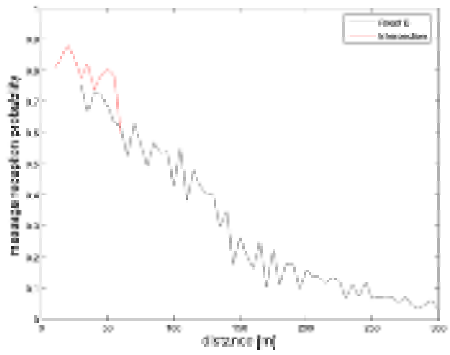


Figure 5-495: Reception Prob. of Routine Message Scenario 41, Rd. B, Sender on Rd. A2

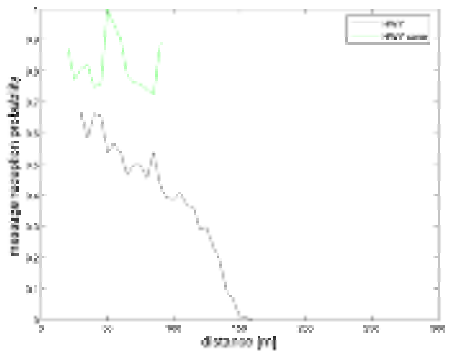


Figure 5-496: Reception Prob. of Routine Message Scenario 41, HWY, Sender on Rd. A2

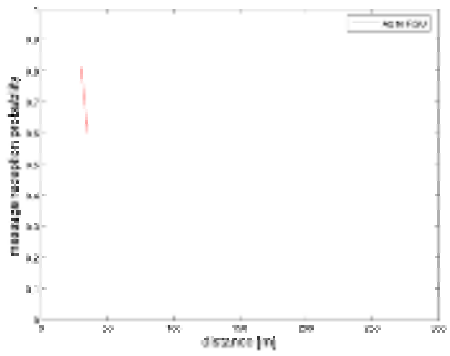


Figure 5-497: Reception Prob. of Routine Message Scenario 41, RSU, Sender on Rd. A2

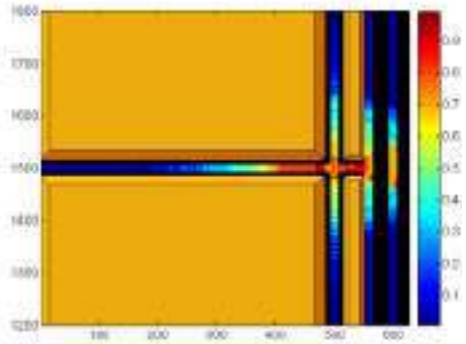


Figure 5-498: Reception Probability of Emergency Messages-Scenario41, Sender on Rd. A2

Sender on HWY

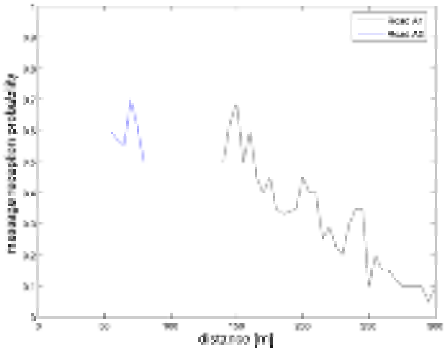


Figure 5-499: Reception Prob. of Routine Message Scenario 41, Rd. A, Sender on HWY

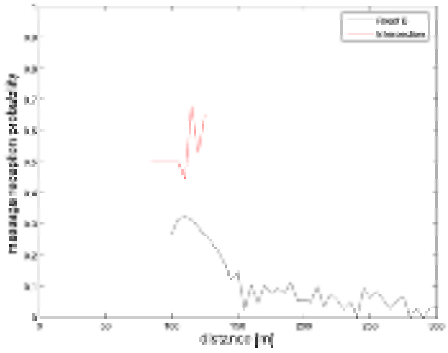


Figure 5-500: Reception Prob. of Routine Message Scenario 41, Rd. B, Sender on HWY

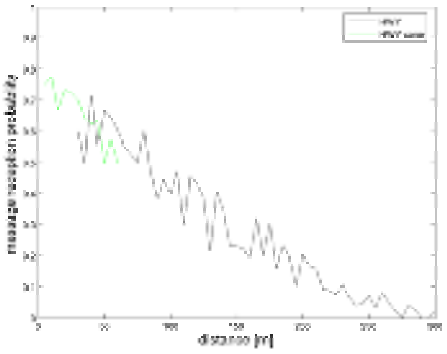


Figure 5-501: Reception Prob. of Routine Message Scenario 41, HWY, Sender on HWY

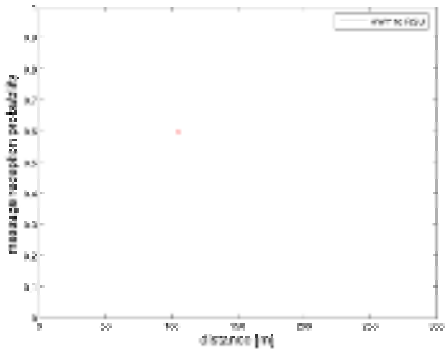


Figure 5-502: Reception Prob. of Routine Message Scenario 41, RSU, Sender on HWY

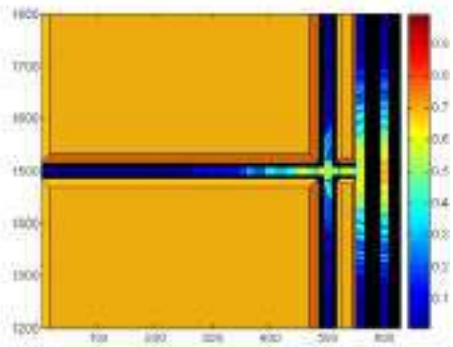


Figure 5-503: Reception Probability of Emergency Messages-Scenario 41, Sender on HWY

5.3.2 Scenario 42

Routine messages	10Hz 200byte 200m
RF Model	Distributed
Corner Model	tall building
Emergency Message	None , RSU forwarding routine messages

Sender on A1

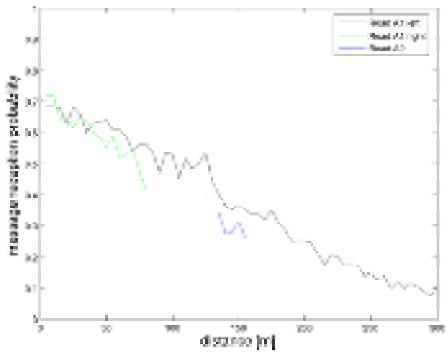


Figure 5-504: Reception Prob. of Routine Message Scenario 42, Rd. A, Sender on Rd. A1

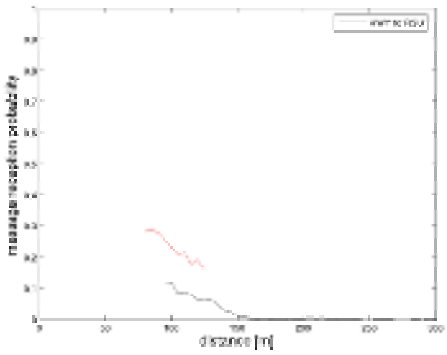


Figure 5-505: Reception Prob. of Routine Message Scenario 42, Rd. B, Sender on Rd. A1

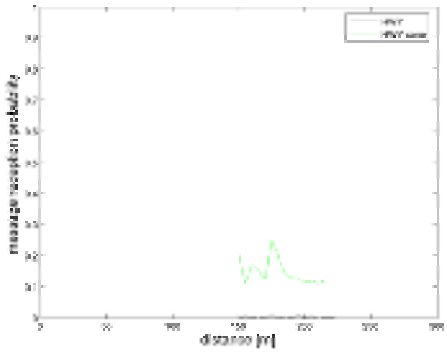


Figure 5-506: Reception Prob. of Routine Message Scenario 42, HWY, Sender on Rd. A1

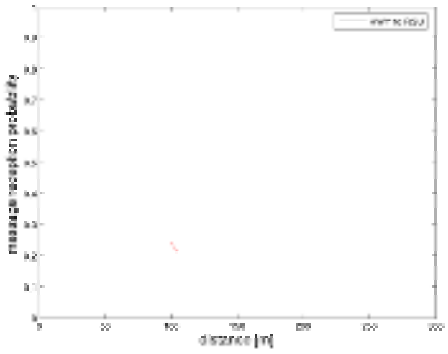


Figure 5-507: Reception Prob. of Routine Message Scenario 42, RSU, Sender on Rd. A1

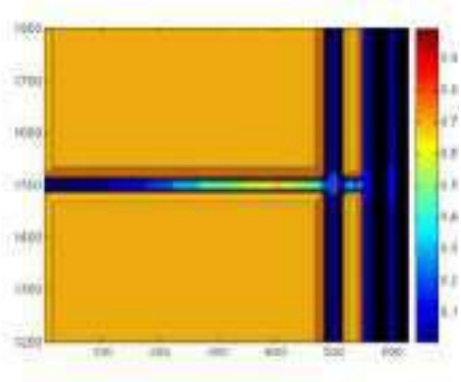


Figure 5-508: Reception Probability of Emergency Messages-Scenario 42, Sender on Rd. A1

Sender on Road A2

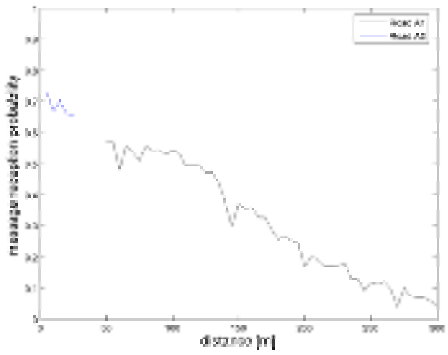


Figure 5-509: Reception Prob. of Routine Message Scenario 42, Rd. A, Sender on Rd. A2

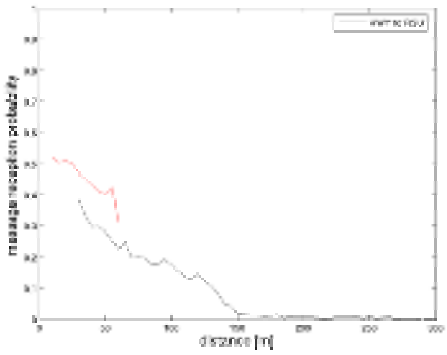


Figure 5-510: Reception Prob. of Routine Message Scenario 42, Rd. B, Sender on Rd. A2

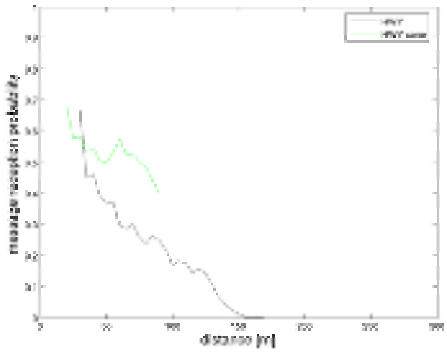


Figure 5-511: Reception Prob. of Routine Message Scenario 42, HWY, Sender on Rd. A2

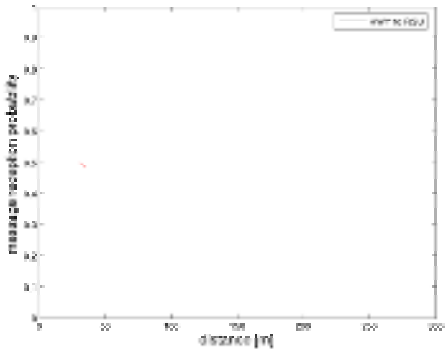


Figure 5-512: Reception Prob. of Routine Message Scenario 42, RSU, Sender on Rd. A2

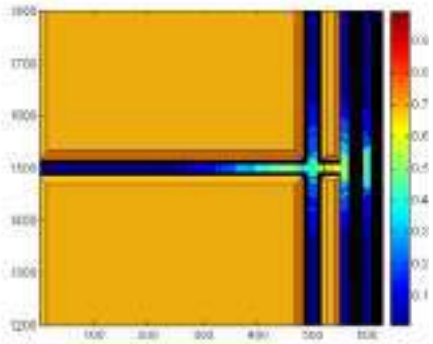


Figure 5-513: Reception Probability of Emergency Messages-Scenario42, Sender on Rd. A1

Sender on HWY

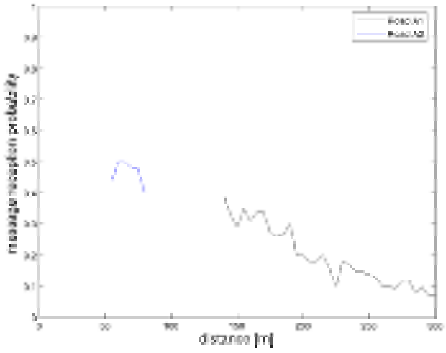


Figure 5-514: Reception Prob. of Routine Message Scenario 42, Rd. A, Sender on HWY

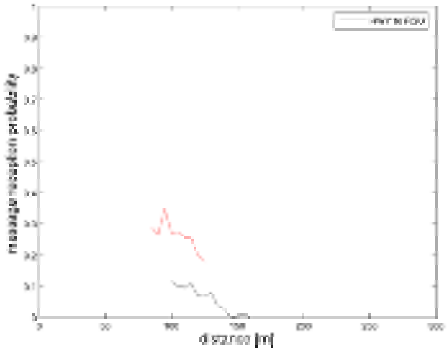


Figure 5-515: Reception Prob. of Routine Message Scenario 42, Rd. B, Sender on HWY

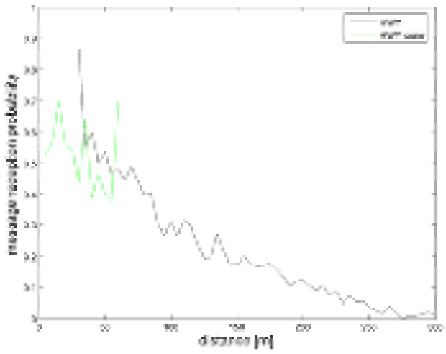


Figure 5-516: Reception Prob. of Routine Message Scenario 42, HWY, Sender on HWY

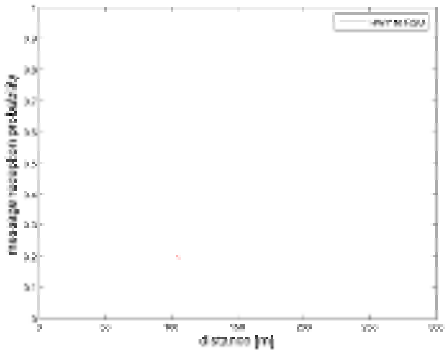


Figure 5-517: Reception Prob. of Routine Message Scenario 42, RSU, Sender on HWY

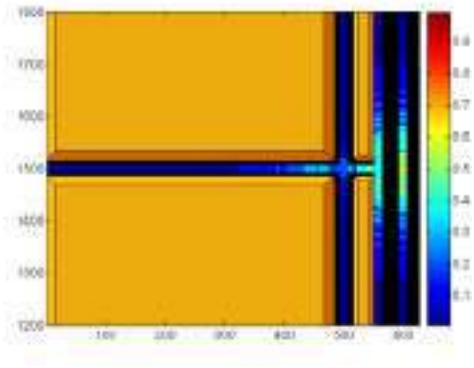


Figure 5-518: Reception Probability of Emergency Messages-Scenario 42, Sender on HWY

5.4 Batch 4, Cascading Emergency Messages From Intersection

5.4.1 Scenario 43

Cascading message on Road A1, based on Cascading protocol 1, repetition

Routine messages	5Hz 200byte 200m
RF Model	Distributed
Corner Model	Tall building

Retransmission interval T=0.02s;

Triggering Event happens at the intersection, cascading to the end of road A1, node density on Rd. A1 is 7m/car

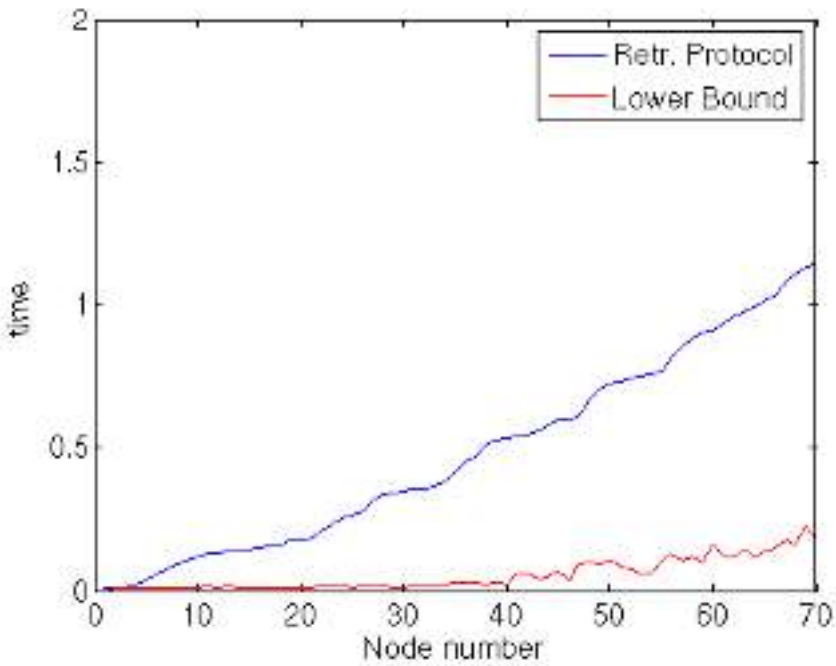


Figure 5-519: Propagation time over nodes, cascading protocol 1

5.4.2 Scenario 44

Cascading message on Road A1, based on Cascading protocol 2, feedback

Routine messages	5Hz 200byte 200m
RF Model	Distributed
Corner Model	Tall building

Retransmission interval T=0.02s;
Triggering Event happens at the intersection, cascading to the end of road A1, node density on Rd. A1 is 7m/car

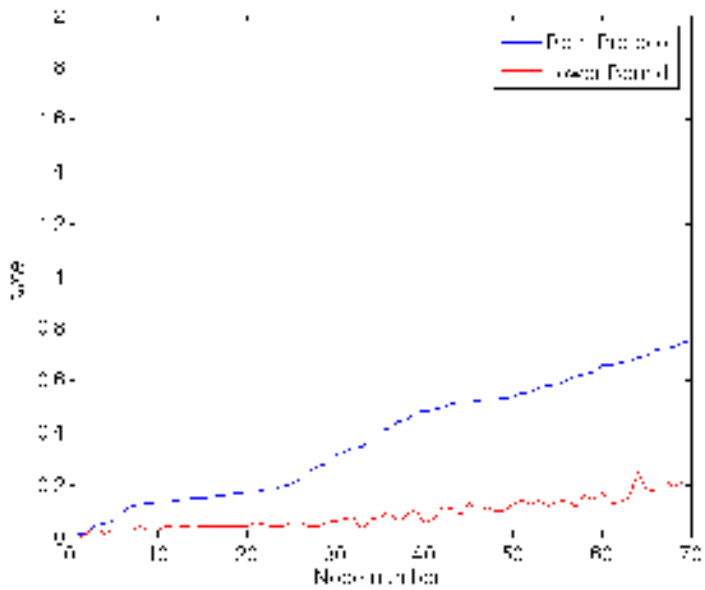


Figure 5-520: Propagation Time Over Nodes, Cascading Protocol 2

5.4.3 Scenario 45

Cascading message on Road A1, based on Cascading protocol 1, repetition

Routine messages	10Hz 200byte 200m
RF Model	Distributed
Corner Model	Tall building

Retransmission interval T=0.02s;
Triggering Event happens at the intersection, cascading to the end of road A1, node density on Rd. A1 is 7m/car

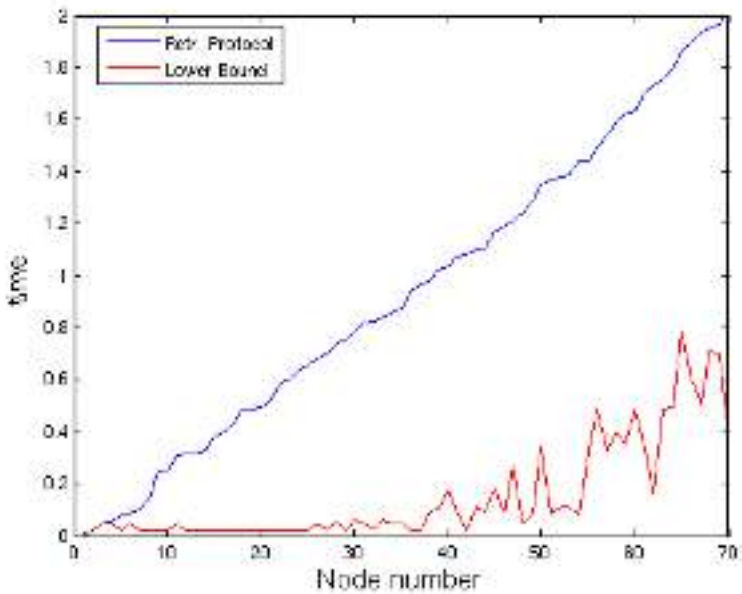


Figure 5-521: Propagation Time Over Nodes, Cascading Protocol 1

5.4.4 Scenario 46

Cascading message on Road A1, based on Cascading protocol 2, feedback

Routine messages	10Hz 200byte 200m
RF Model	Distributed
Corner Model	Tall building

Retransmission interval T=0.02s;
Triggering Event happens at the intersection, cascading to the end of road A1, node density on Rd. A1 is 7m/car

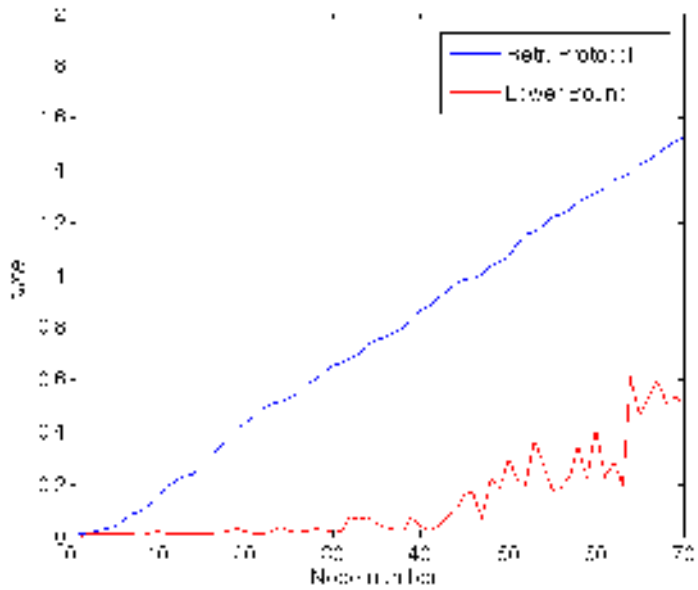


Figure 5-522: Propagation Time Over Nodes, Cascading Protocol 2

5.5 Batch 5, Additional Simulation Tests

5.5.1 Scenario 47

Simulation Scenario Setting:

Emergency Message Sender	RSU, 10Hz/ 500 bytes/ 200m
Corner Model	no buildings
Routine Message Frequency	none

5.5.1.1 Reception Probability of Emergency Messages

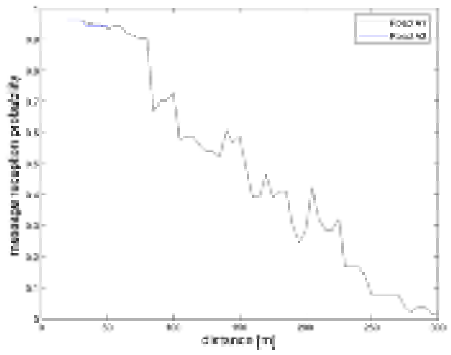


Figure 5-523: Reception Probability of Emergency Messages-Scenario 47, Road A, Sender RSU

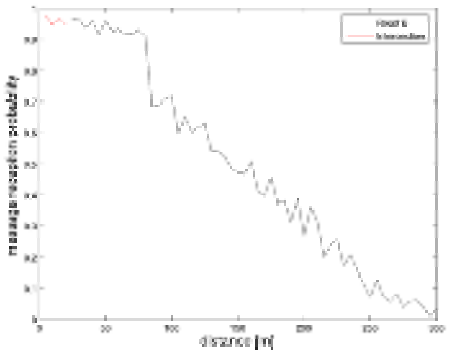


Figure 5-524: Reception Probability of Emergency Messages-Scenario 47, Road B, Sender RSU

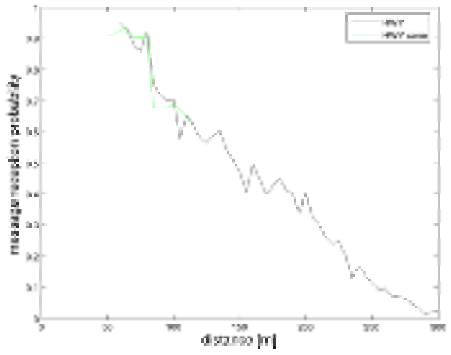


Figure 5-525: Reception Probability of Emergency Messages-Scenario 47, HWY, Sender RSU

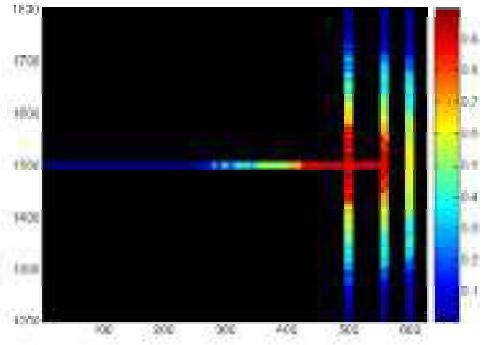


Figure 5-526: Reception Probability of Emergency Messages-Scenario 47, Sender RSU

5.5.2 Scenario 48

Simulation Scenario Setting:

Emergency Message Sender	RSU, 10Hz/ 500 bytes/ 200m
Corner Model	tall building
Routine Message Frequency	none

5.5.2.1 Reception Probability of Emergency Messages

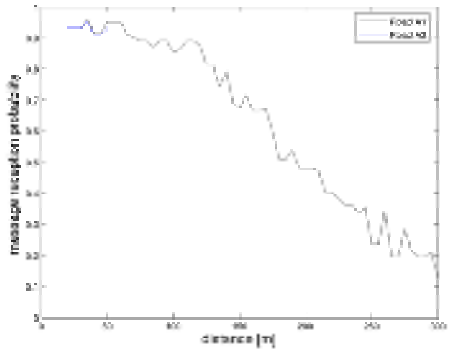


Figure 5-527: Reception Probability of Emergency Messages-Scenario 48, Road A, Sender RSU

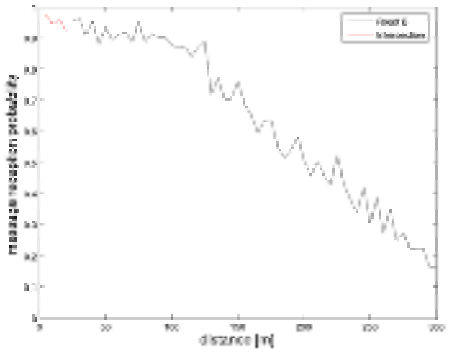


Figure 5-528: Reception Probability of Emergency Messages-Scenario 48, Road B, Sender RSU

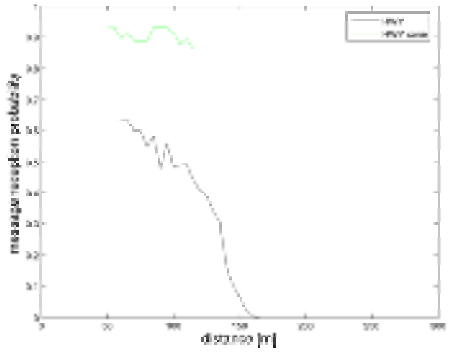


Figure 5-529: Reception Probability of Emergency Messages-Scenario 48, HWY, Sender RSU

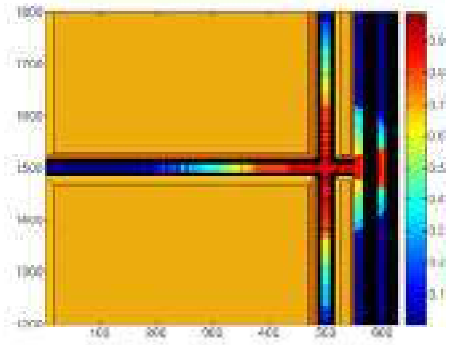


Figure 5-530: Reception Probability of Emergency Messages-Scenario 48, Sender RSU

5.5.3 Scenario 49

Simulation Scenario Setting:

Emergency Message Sender	RSU, 10Hz/ 500 bytes/ 200m
Corner Model	no buildings
Routine Message Frequency	2Hz

5.5.3.1 Reception Probability of Emergency Messages

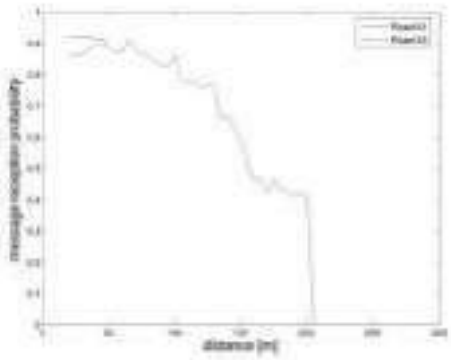


Figure 5-531: Reception Probability of Emergency Messages-Scenario 49, Road A, Sender RSU

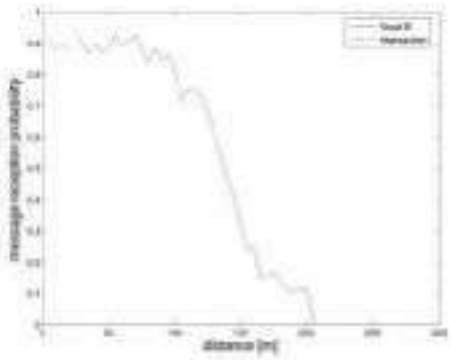


Figure 5-532: Reception Probability of Emergency Messages-Scenario 49, Road B, Sender RSU

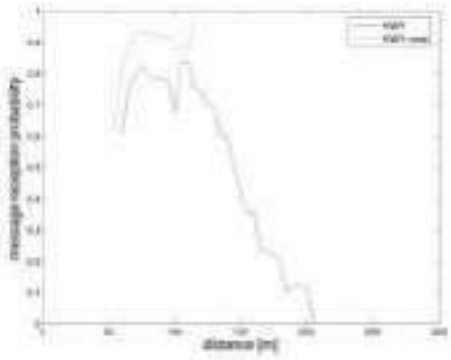


Figure 5-533: Reception Probability of Emergency Messages-Scenario 49, HWY, Sender RSU

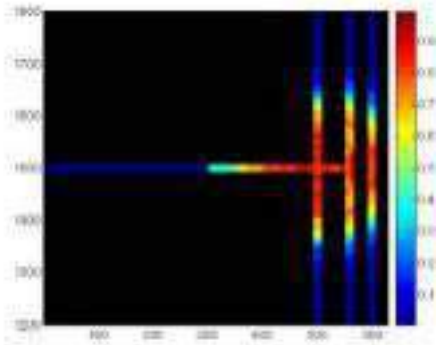


Figure 5-534: Reception Probability of Emergency Messages-Scenario 49, Sender RSU

5.5.4 Scenario 50

Simulation Scenario Setting:

Emergency Message Sender	RSU, 10Hz/ 500 bytes/ 200m
Corner Model	Tall buildings
Pt for emergency message	200m coverage
Pt for routine message	100m coverage
Routine Message Frequency	10Hz

5.5.4.1 Reception Probability of Emergency Messages

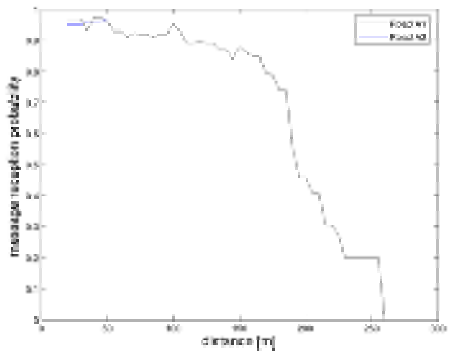


Figure 5-535: Reception Probability of Emergency Messages-Scenario 50, Road A, Sender RSU

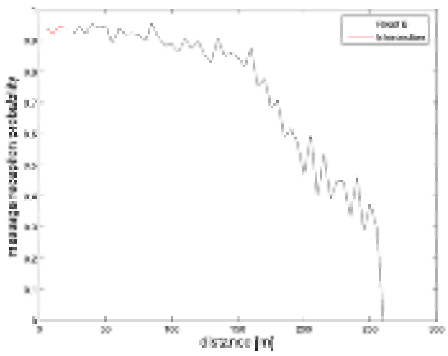


Figure 5-536: Reception Probability of Emergency Messages-Scenario 50, Road B, Sender RSU

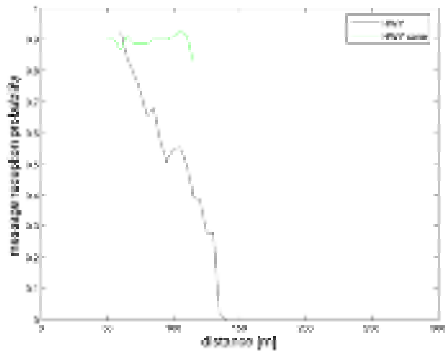


Figure 5-537: Reception Probability of Emergency Messages-Scenario 50, HWY, Sender RSU

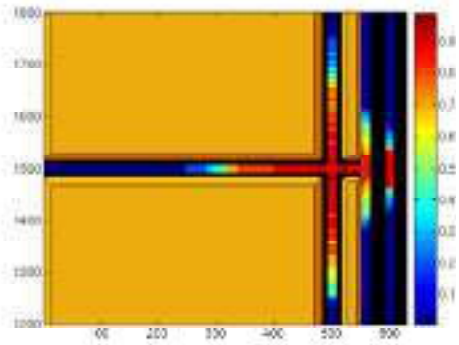


Figure 5-538: Reception Probability of Emergency Messages-Scenario 50, Sender RSU

6 Further Messaging Performance Analysis

The simulations results listed in the previous chapter provide figures of DSRC communication performance in various scenarios. However, it takes more than just a reception probability over distance figure for one to understand the implication of such communication performance for safety applications. For example, it could be better for a safety application to transmit 5 messages each at 50 percent reception probability than to deliver 1 message reliably in the same time frame.

This chapter provides further analysis figures based on the communication performance results of some selected scenarios. The new figures show the time period necessary for a sender to be confident to a certain degree that at least one message would be received by a receiver at a particular distance. All such figures have the X-axis set at 200 meters, and the Y-axis set at 2 seconds. Three confidence levels are shown, at 90 percent, 95 percent, and 99 percent.

The figures are produced in the following manner: Let p be the reception probability at distance d. Now find the number N so that after N transmission, the probability of receiving at least one of the messages should be greater than a given confidence level α.

$$p(at\ least\ 1\ success\ in\ N\ tries) = 1 - p(all\ \ failures\ in\ N\ tries) = 1 - (1-p)^N \geq \alpha$$

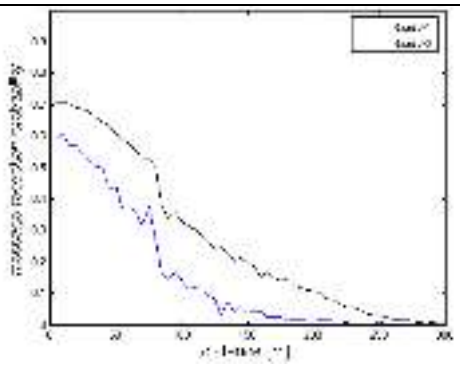
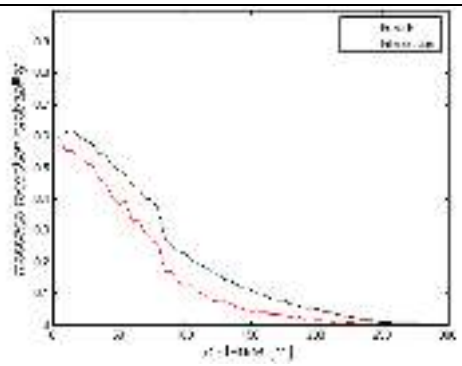
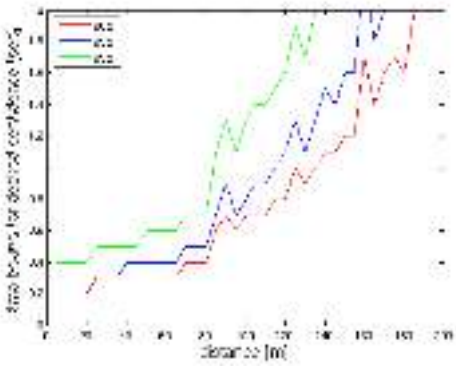
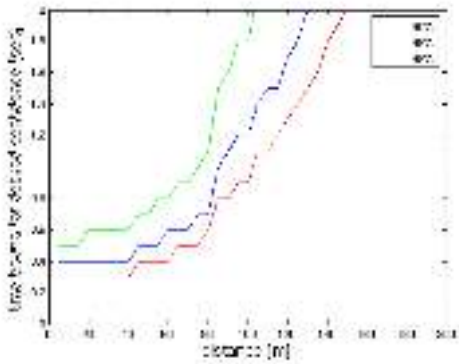
$$\longrightarrow (1-p)^N \leq 1 - \alpha$$

$$\longrightarrow N \geq \frac{\log(1-\alpha)}{\log(1-p)}$$

Therefore the time bound for a given confidence α is *N*Transmission Interval.*

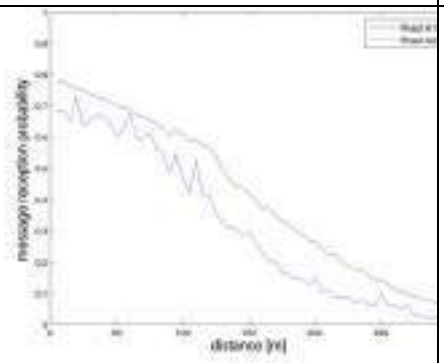
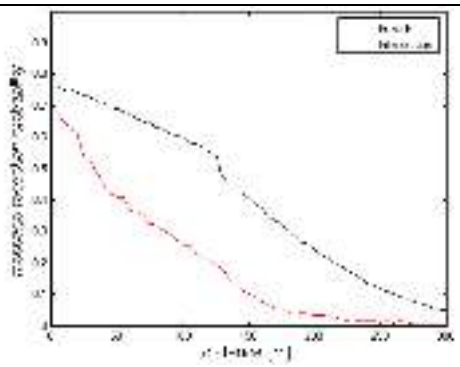
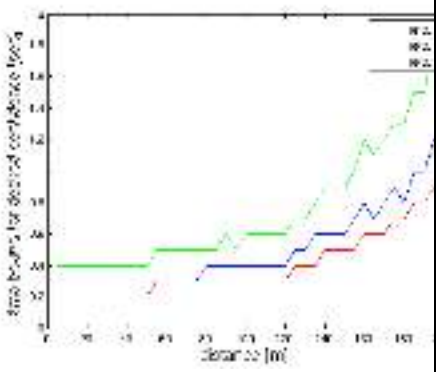
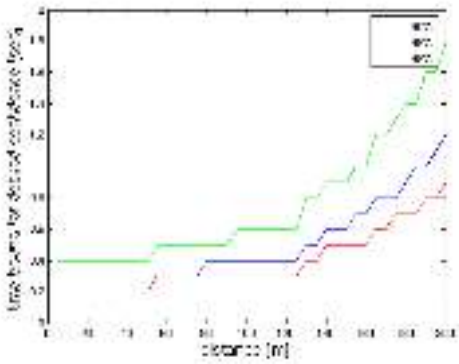
6.1 Routine Safety Messages

6.1.1 Scenario 9

Number	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
	Distributed	Open	RSU	200m	ON	10Hz	200m	
	Routine Messages							
	Road A				Road B			
Reception probability	 **Figure 6-1: Reception Probability of Routine Messages – Scenario 9, Road A**				 **Figure 6-2: Reception Probability of Routine Messages – Scenario 9, Road A**			
Time bound for needed confidence	 **Figure 6-3: Time Bound for desired Confidence, Routine Messages - Scenario 9, Road A**				 **Figure 6-4: Time Bound for desired Confidence, Routine Messages - Scenario 9, Road B**			

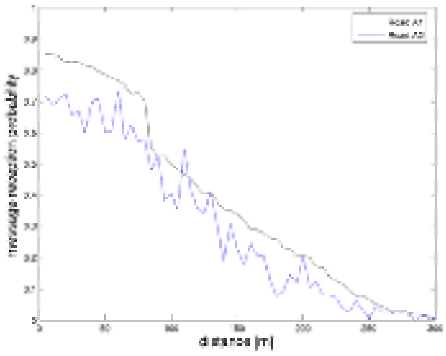
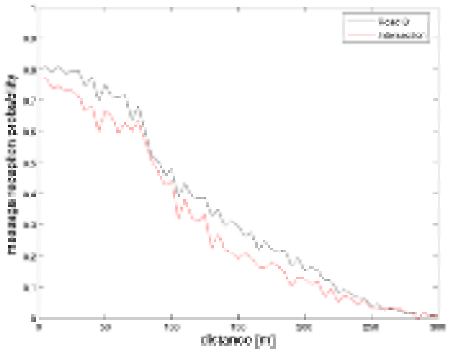
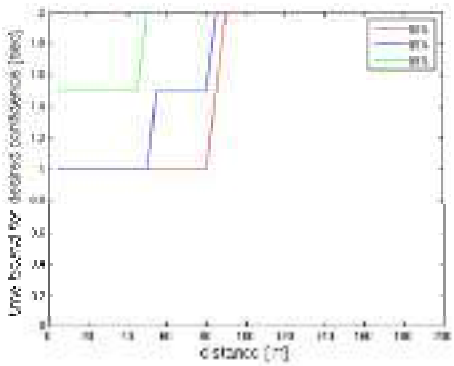
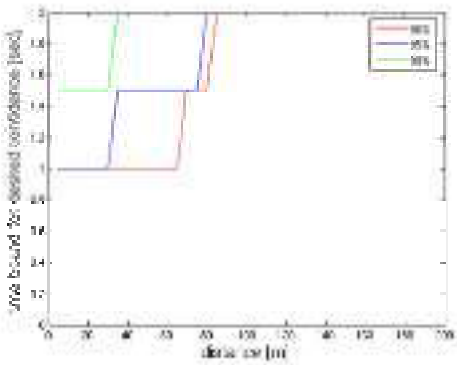
6.1.2 Scenario 11

Number	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
11	Distributed	Building	RSU	200m	ON	10Hz	200m	

	Routine Messages	
	Road A	Road B
Reception probability	 **Figure 6-5: Reception Probability of Routine Messages on Road A, Scenario 11**	 **Figure 6-6: Reception Probability of Routine Messages on Road B, Scenario 11**
Time bound for needed confidence	 **Figure 6-7: Time Bound for desired Confidence, Routine Messages - Scenario 11, Road A**	 **Figure 6-8: Time Bound for desired Confidence, Routine Messages - Scenario 11, Road B**

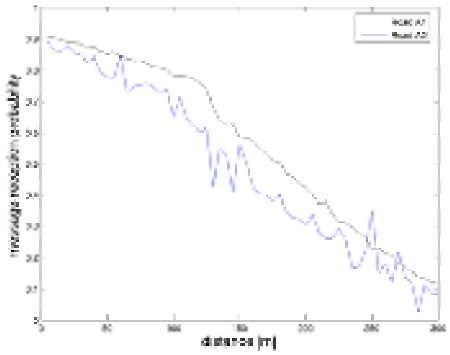
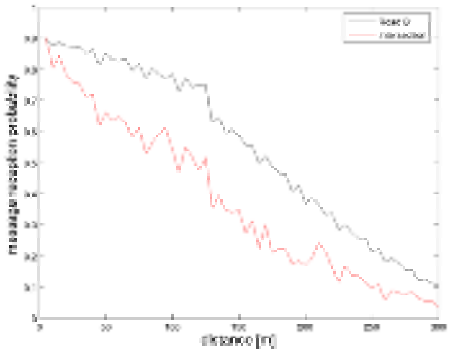
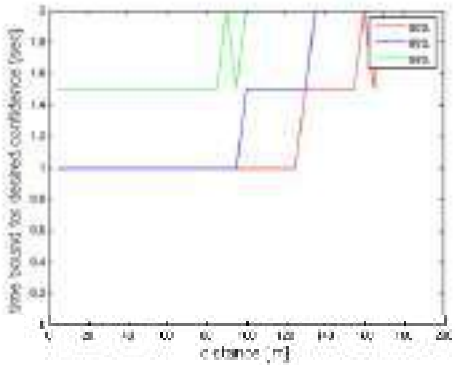
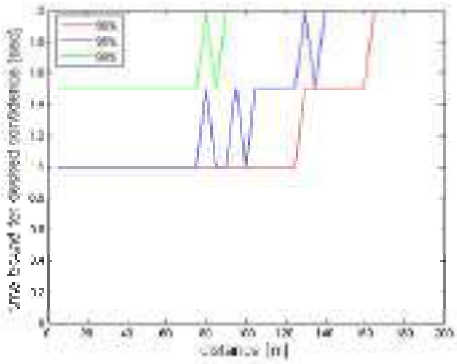
6.1.3 Scenario 17

Number	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
17	Distributed	Open	RSU	200m	ON	2Hz	200m	

	Routine Messages	
	Road A	Road B
Reception probability	 **Figure 6-9: Reception Probability of Routine Messages on Road A, Scenario 17**	 **Figure 6-10: Reception Probability of Routine Messages on Road B, Scenario 17**
Time bound for needed confidence	 **Figure 6-11: Time Bound for desired Confidence, Routine Messages - Scenario 17, Road A**	 **Figure 6-12: Time Bound for desired Confidence, Routine Messages - Scenario 17, Road B**

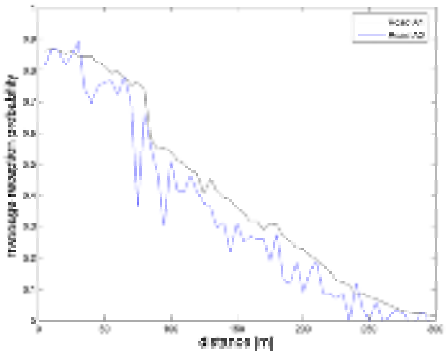
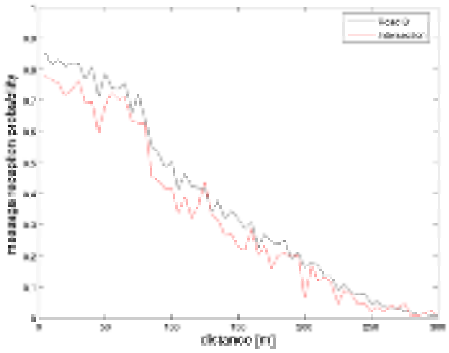
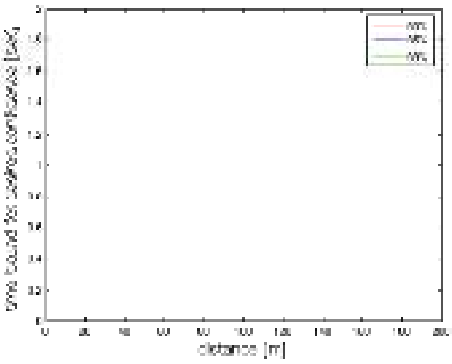
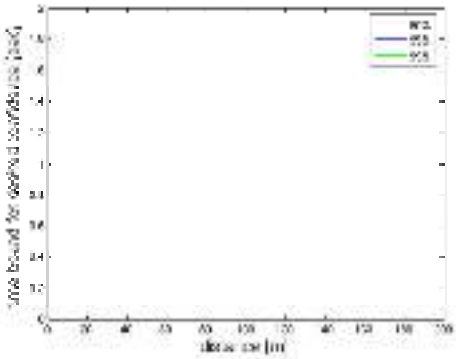
6.1.4 Scenario 19

Number	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
19	Distributed	Building	RSU	200m	ON	2Hz	200m	

	Routine Messages	
	Road A	Road B
Reception probability	 **Figure 6-13: Reception Probability of Routine Messages on Road A, Scenario 19**	 **Figure 6-14: Reception Probability of Routine Messages on Road B, Scenario 19**
Time bound for needed confidence	 **Figure 6-15: Time Bound for desired Confidence, Routine Messages - Scenario 19, Road A**	 **Figure 6-16: Time Bound for desired Confidence, Routine Messages - Scenario 19, Road B**

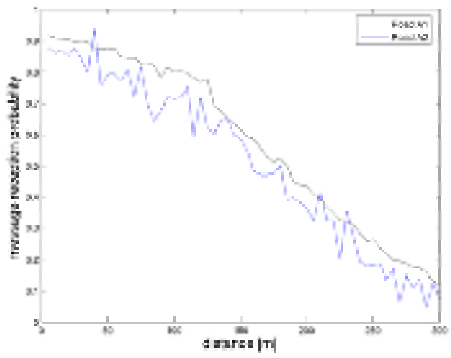
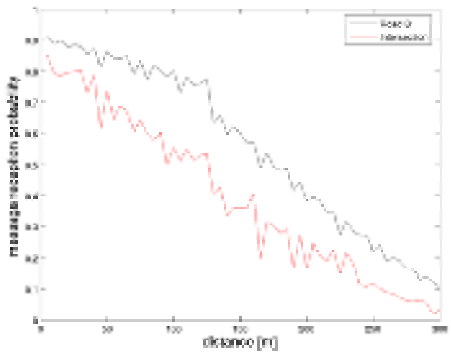
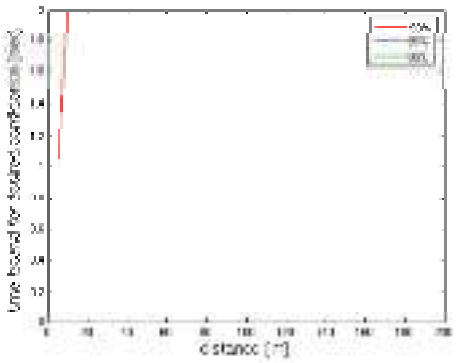
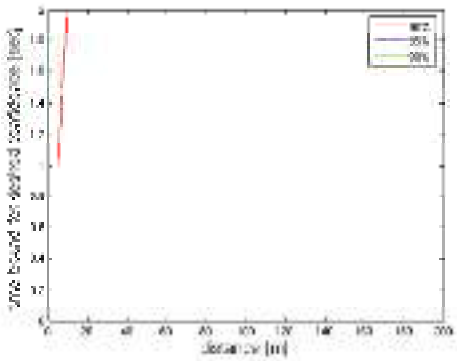
6.1.5 Scenario 25

Number	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
25	Distributed	Open	RSU	200m	ON	1Hz	200m	

	Routine Messages	
	Road A	Road B
Reception probability	 **Figure 6-17: Reception Probability of Routine Messages on Road A Scenario 25**	 **Figure 6-18: Reception Probability of Routine Messages on Road B Scenario 25**
Time bound for needed confidence	 **Figure 6-19: Time Bound for desired Confidence, Routine Messages - Scenario 25, Road A**	 **Figure 6-20: Time Bound for desired Confidence, Routine Messages - Scenario 25, Road B**

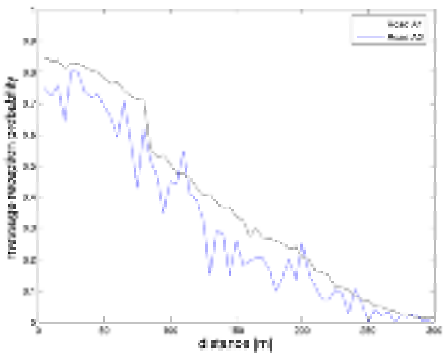
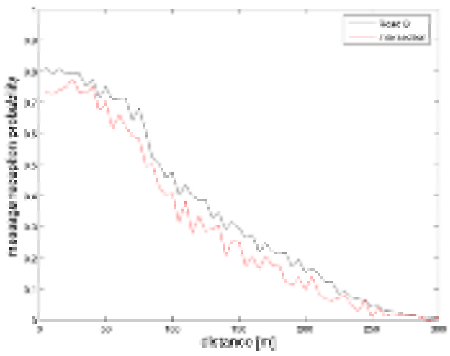
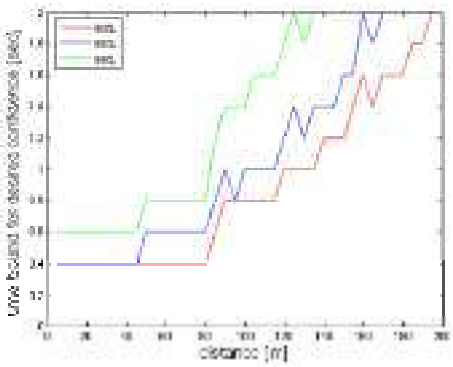
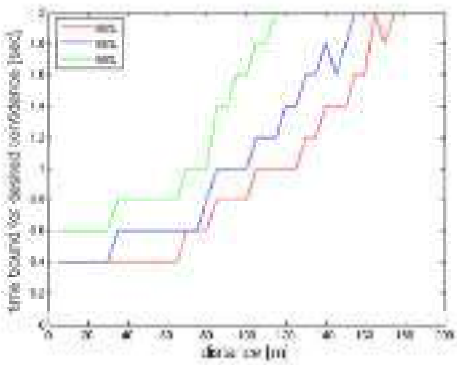
6.1.6 Scenario 27

Number	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
27	Distributed	Building	RSU	200m	ON	1Hz	200m	

	Routine Messages	
	Road A	Road B
Reception probability	 **Figure 6-21: Reception Probability of Routine Messages on Road A, Scenario 27**	 **Figure 6-22: Reception Probability of Routine Messages on Road B, Scenario 27**
Time bound for needed confidence	 **Figure 6-23: Time Bound for desired Confidence, Routine Messages - Scenario 27, Road A**	 **Figure 6-24: Time Bound for desired Confidence, Routine Messages - Scenario 27, Road B**

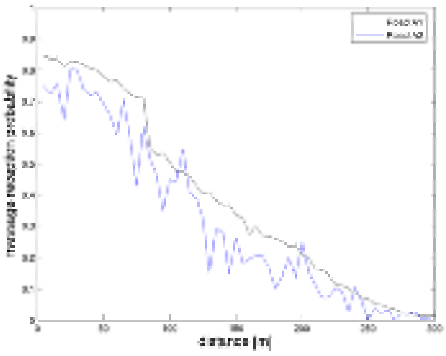
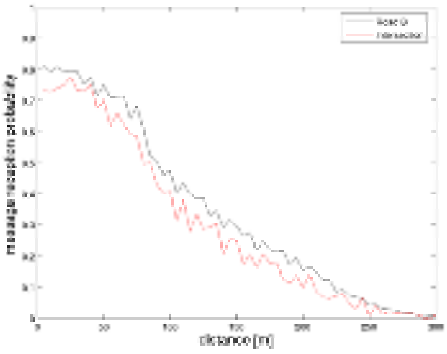
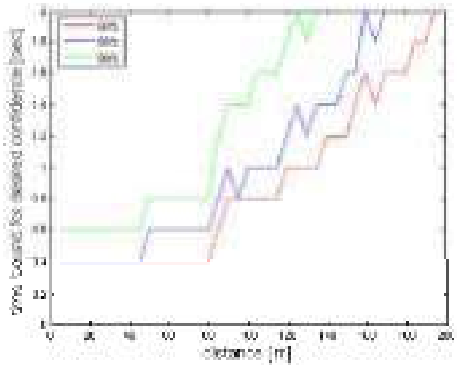
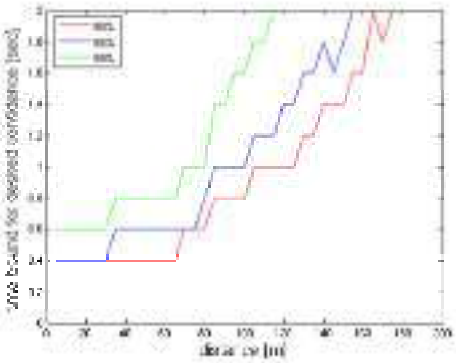
6.1.7 Scenario 33

Number	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
33	Distributed	Open	RSU	200m	ON	5Hz	200m	

	Routine Messages	
	Road A	Road B
Reception probability	 **Figure 6-25: Reception Probability of Routine Messages on Road A, Scenario 33**	 **Figure 6-26: Reception Probability of Routine Messages on Road B, Scenario 33**
Time bound for needed confidence	 **Figure 6-27: Time Bound for desired Confidence, Routine Messages - Scenario 33, Road A**	 **Figure 6-28: Time Bound for desired Confidence, Routine Messages - Scenario 33, Road B**

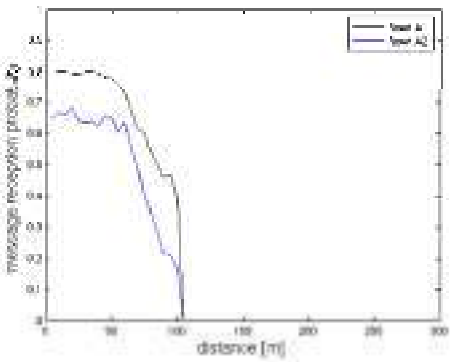
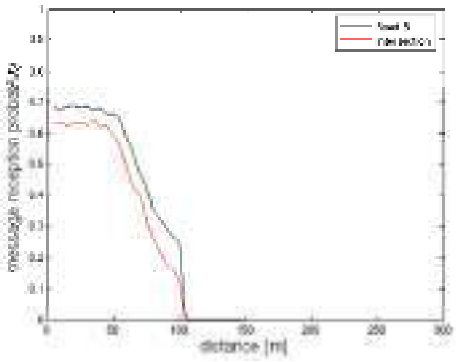
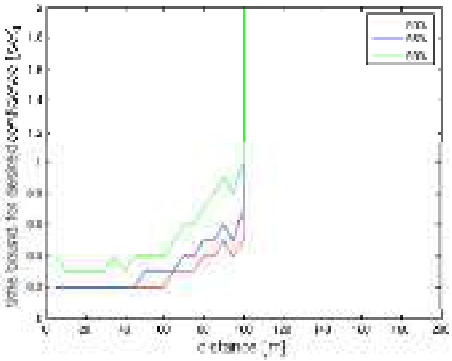
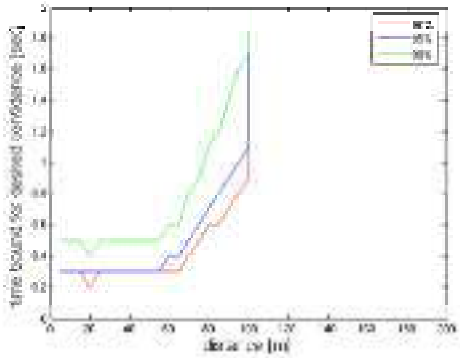
6.1.8 Scenario 35

Number	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
35	Distributed	Building	RSU	200m	ON	5Hz	200m	

	Routine Messages	
	Road A	Road B
Reception probability	 **Figure 6-29: Reception Probability of Routine Messages on Road A Scenario 35**	 **Figure 6-30: Reception Probability of Routine Messages on Road B Scenario 35**
Time bound for needed confidence	 **Figure 6-31: Time Bound for desired Confidence, Routine Messages - Scenario 35, Road A**	 **Figure 6-32: Time Bound for desired Confidence, Routine Messages - Scenario 35, Road B**

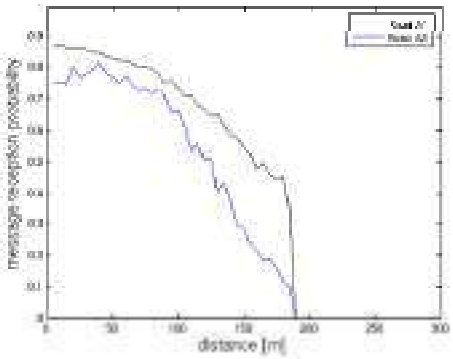
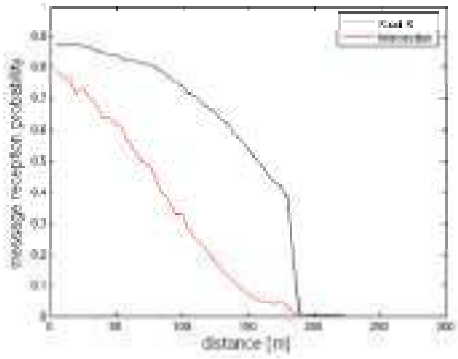
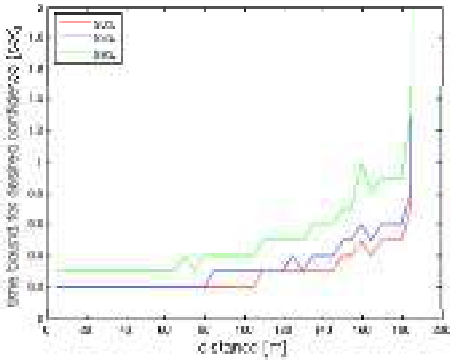
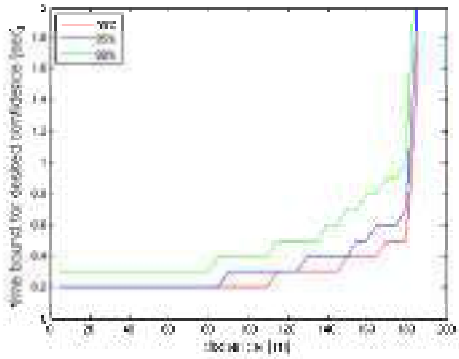
6.1.9 Scenario 49

Number	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
35	Deterministic	Open Building	RSU	200m	ON	10Hz	100m	

	Routine Messages	
	Road A	Road B
Reception probability	 **Figure 6-33: Reception Probability of Routine Messages on Road A, Scenario 49**	 **Figure 6-34: Reception Probability of Routine Messages on Road B, Scenario 49**
Time bound for needed confidence	 **Figure 6-35: Time Bound for desired Confidence, Routine Messages - Scenario 49, Road A**	 **Figure 6-36: Time Bound for desired Confidence, Routine Messages - Scenario 49, Road B**

6.1.10 Scenario 50

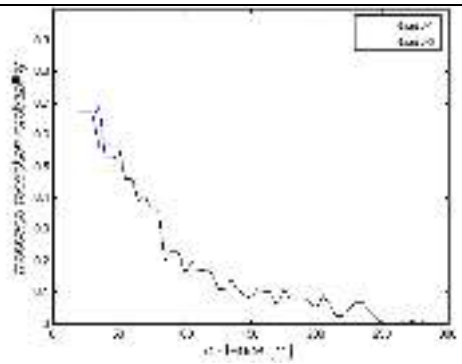
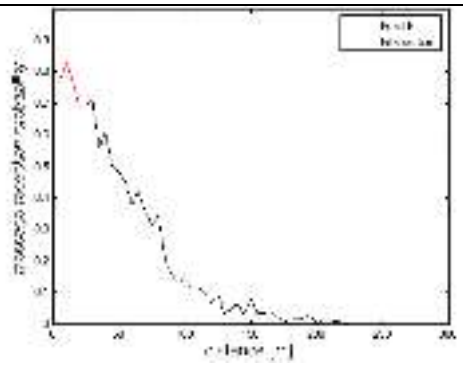
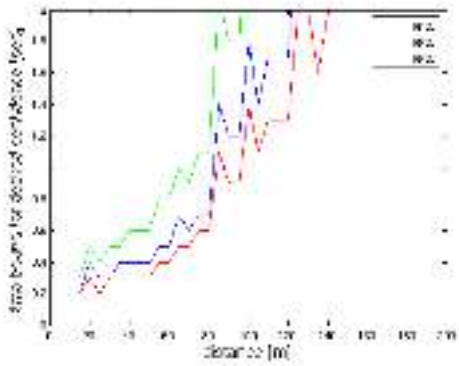
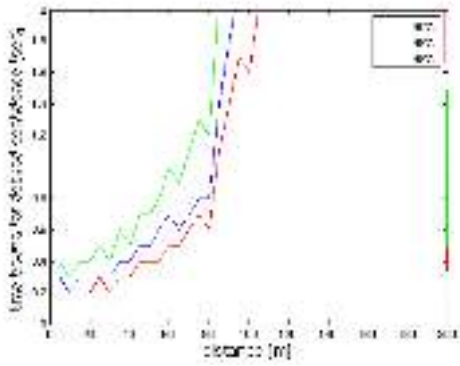
Number	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
35	Deterministic	Building	RSU	200m	ON	10Hz	100m	

	Routine Messages	
	Road A	Road B
Reception probability	 **Figure 6-37: Reception Probability of Routine Messages on Road A, Scenario 50**	 **Figure 6-38: Reception Probability of Routine Messages on Road B, Scenario 50**
Time bound for needed confidence	 **Figure 6-39: Time Bound for desired Confidence, Routine Messages - Scenario 50, Road A**	 **Figure 6-40: Time Bound for desired Confidence, Routine Messages - Scenario 50, Road B**

6.2 High Priority Emergency Messages

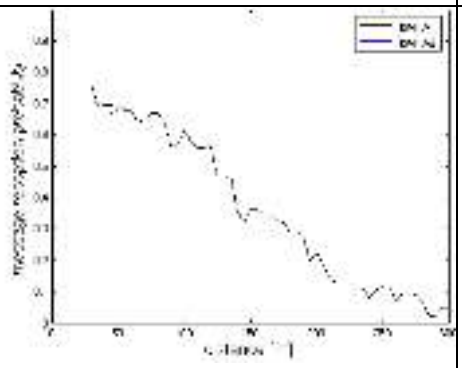
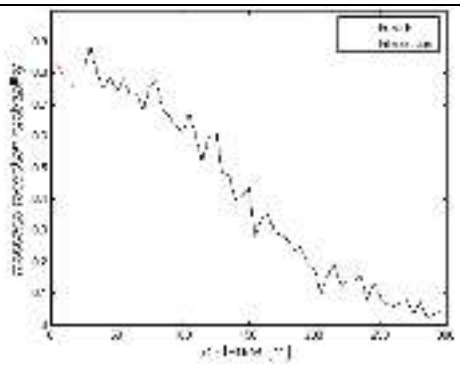
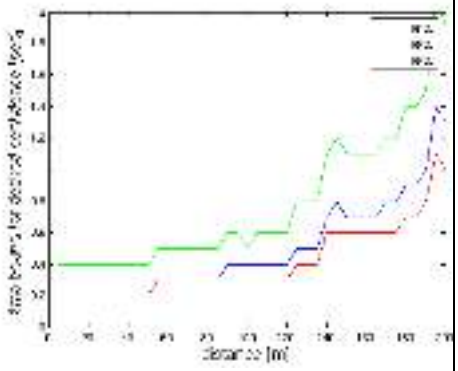
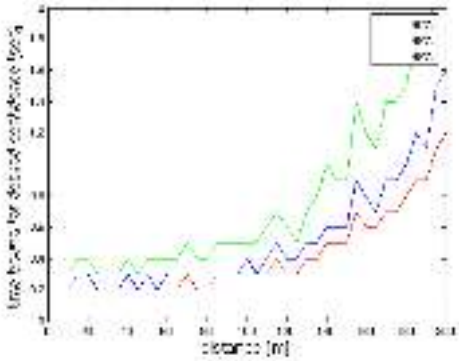
6.2.1 Scenario 9

Number	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
9	Distributed	Open	RSU	200m	ON	10Hz	200m	

	Emergency messages	
	Road A	Road B
Reception probability	 **Figure 6-41: Reception Probability of Emergency Messages-Scenario 9, Road A, Sender RSU**	 **Figure 6-42: Reception Probability of Emergency Messages-Scenario 9, Road B, Sender RSU**
Time bound for needed confidence	 **Figure 6-43: Time Bound for desired Confidence, Emergency Messages - Scenario 9, Road A, Sender RSU**	 **Figure 6-44: Time Bound for desired Confidence, Emergency Messages - Scenario 9, Road B, Sender RSU**

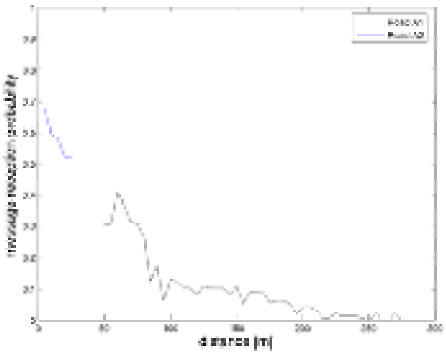
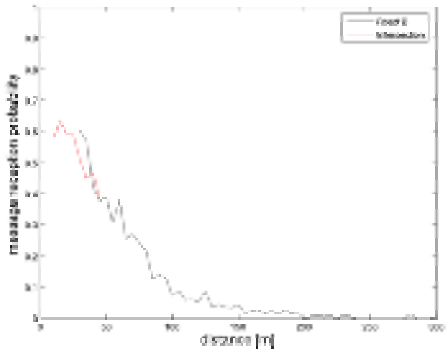
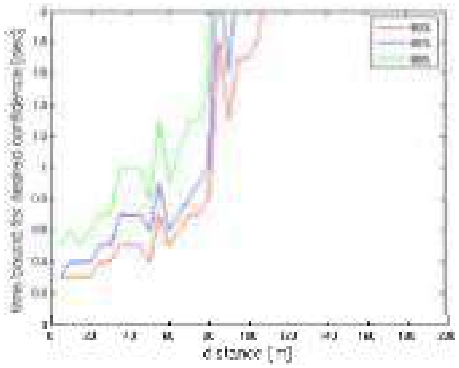
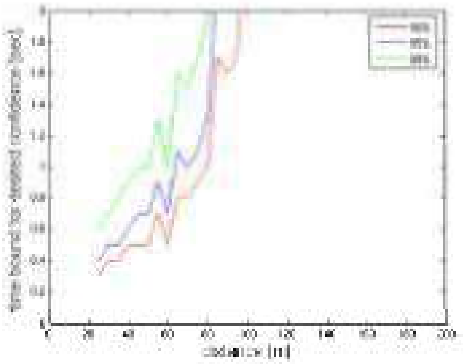
6.2.2 Scenario 11

Number	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
11	Distributed	Building	RSU	200m	ON	10Hz	200m	

	Emergency messages	
	Road A	Road B
Reception probability	 **Figure 6-45: Reception Probability of Emergency Messages-Scenario 11, Road A, Sender RSU**	 **Figure 6-46: Reception Probability of Emergency Messages-Scenario 11, Road B, Sender RSU**
Time bound for needed confidence	 **Figure 6-47: Time Bound for desired Confidence, Emergency Messages - Scenario 11, Road A, Sender RSU**	 **Figure 6-48: Time Bound for desired Confidence, Emergency Messages - Scenario 11, Road B, Sender RSU**

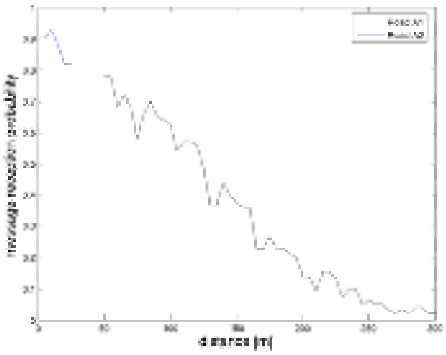
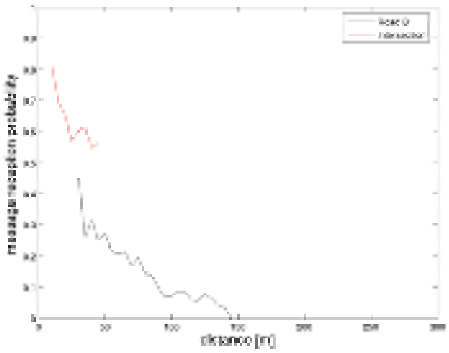
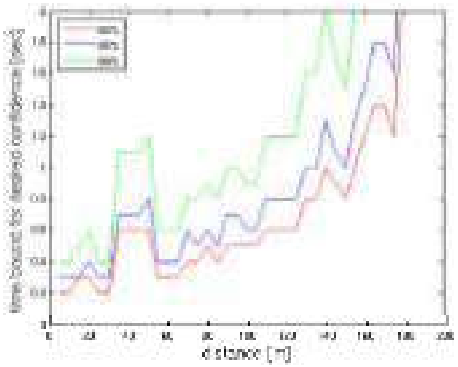
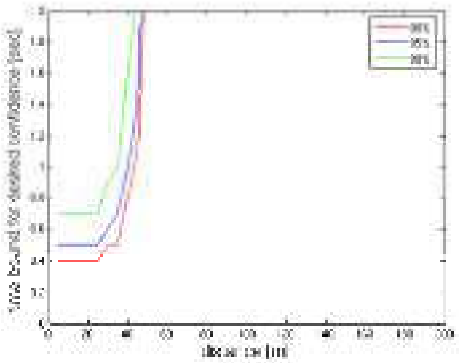
6.2.3 Scenario 13

Number	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
13	Distributed	Open	OBU	200m	ON	10Hz	200m	

	Emergency Messages	
	OBU at A2 Reception on Road A	OBU at A2 Reception on Road B
Reception probability	 **Figure 6-49: Reception Prob. of Emergency Messages – Scenario 13, Rd. A, Sender on Rd. A2**	 **Figure 6-50: Reception Prob. of Emergency Messages – Scenario 13, Rd. B, Sender on Rd. A2**
Time bound for needed confidence	 **Figure 6-51: Time Bound for desired Confidence, Emergency Messages – Scenario 13, Road A, Sender on Road A2**	 **Figure 6-52: Time Bound for desired Confidence, Emergency Messages - Scenario 13, Road B, Sender on Road A2**

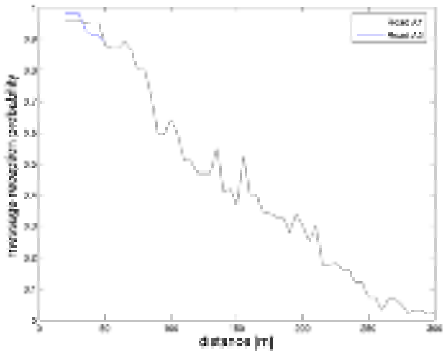
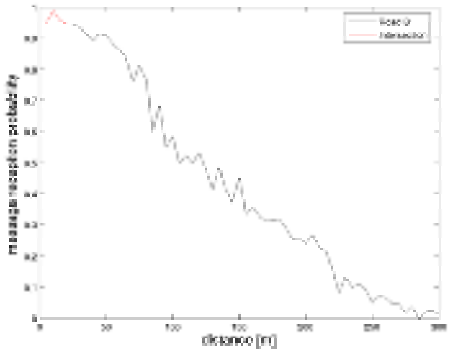
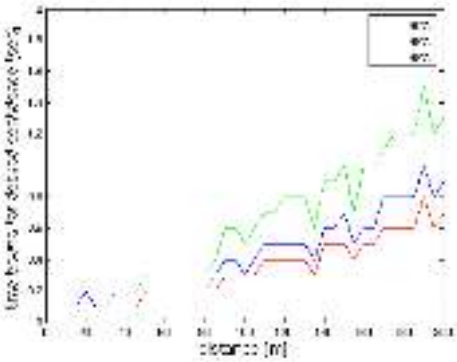
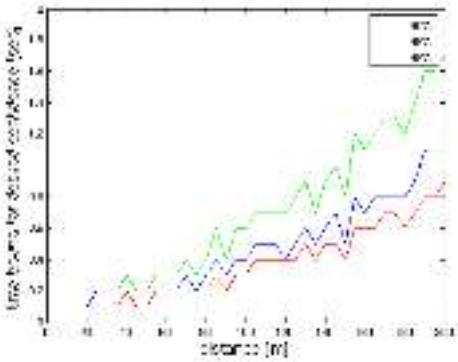
6.2.4 Scenario 15

Number	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
15	Distributed	Building	OBU	200m	ON	10Hz	200m	

	Emergency Messages	
	Road A2	Road B
Reception probability	 **Figure 6-53: Reception Prob. of Emergency Messages – Scenario 15, Rd. A, Sender on Rd. A2**	 **Figure 6-54: Reception Prob. of Emergency Messages – Scenario 15, Rd. B, Sender on Rd. A2**
Time bound for needed confidence	 **Figure 6-55: Time Bound for desired Confidence, Emergency Messages - Scenario 15, Road A, Sender on Road A2**	 **Figure 6-56: Time Bound for desired Confidence, Emergency Messages - Scenario 15, Road B, Sender on Road A2**

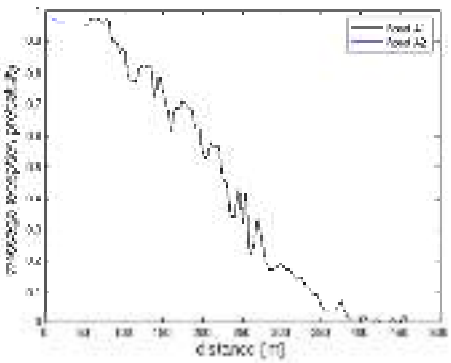
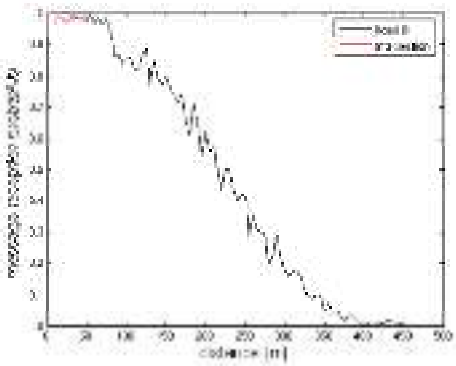
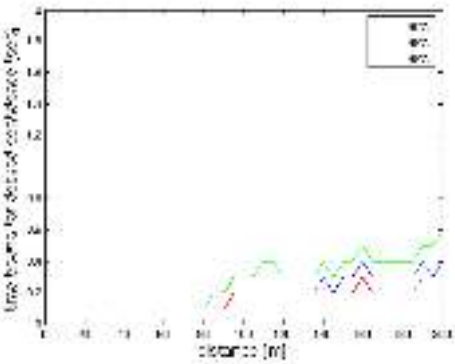
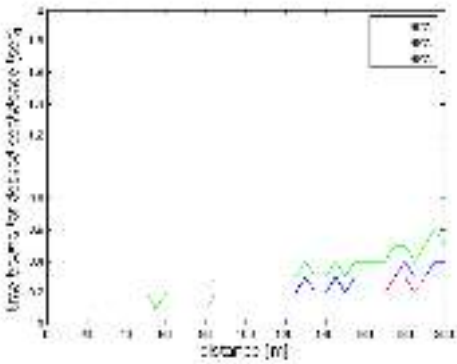
6.2.5 Scenario 17

Number	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
17	Distributed	Open	RSU	200m	ON	2Hz	200m	

	Emergency Messages	
	Road A	Road B
Reception probability	 **Figure 6-57: Reception Probability of Emergency Messages-Scenario17, Road A, Sender RSU**	 **Figure 6-58: Reception Probability of Emergency Messages-Scenario 17, Road B, Sender RSU**
Time bound for needed confidence	 **Figure 6-59: Time Bound for desired Confidence, Emergency Messages – Scenario 17, Road A, Sender RSU**	 **Figure 6-60: Time Bound for desired Confidence, Emergency Messages – Scenario 17, Road B, Sender RSU**

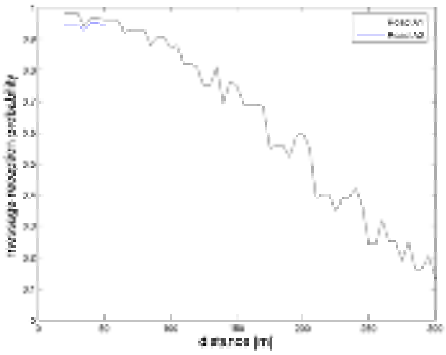
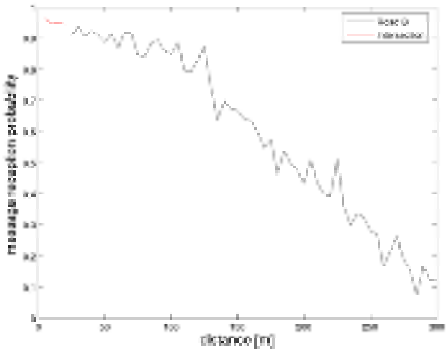
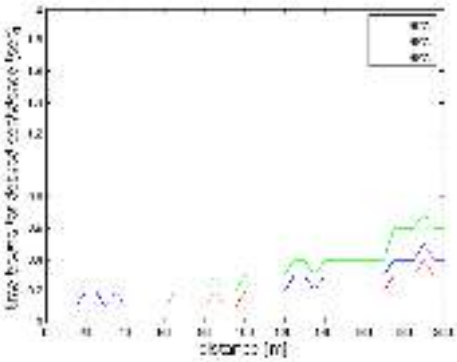
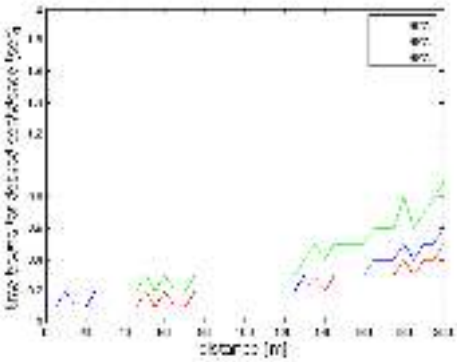
6.2.6 Scenario 18

Number	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
18	Distributed	Open	OBU	200m	ON	2Hz	200m	

	Emergency Messages	
	Road A2	Road B
Reception probability	 **Figure 6-61: Reception Prob. of Emergency Messages – Scenario 18, Rd. A, Sender on Rd. A2**	 **Figure 6-62: Reception Prob. of Emergency Messages – Scenario 18, Rd. B, Sender on Rd. A2**
Time bound for needed confidence	 **Figure 6-63: Time Bound for desired Confidence, Emergency Messages - Scenario 18, Road A, Sender on Road A2**	 **Figure 6-64: Time Bound for desired Confidence, Emergency Messages - Scenario 18, Road B, Sender on Road A2**

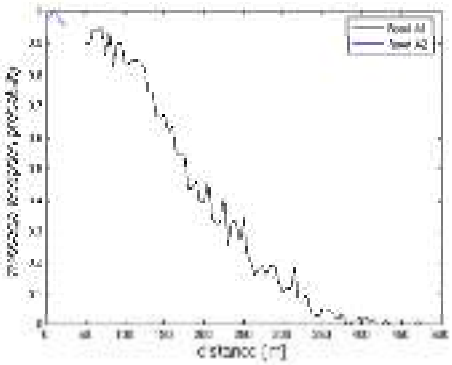
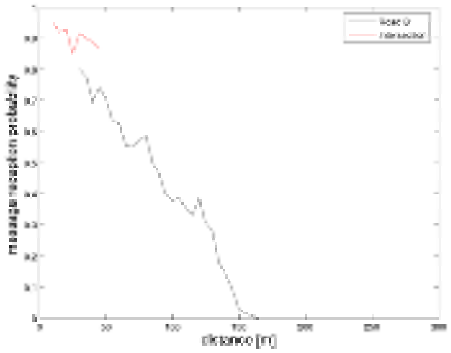
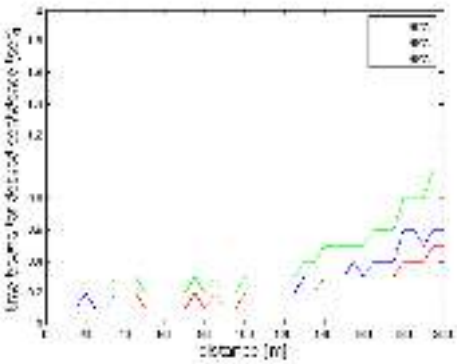
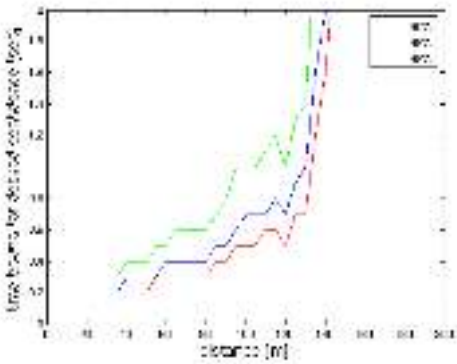
6.2.7 Scenario 19

Number	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
19	Distributed	Building	RSU	200m	ON	2Hz	200m	

	Emergency Messages	
	Road A	Road B
Reception probability	 **Figure 6-65: Reception Probability of Emergency Messages-Scenario19, Road A, Sender RSU**	 **Figure 6-66: Reception Probability of Emergency Messages-Scenario19, Road B, Sender RSU**
Time bound for needed confidence	 **Figure 6-67: Time Bound for desired Confidence, Emergency Messages - Scenario 19, Road A, Sender RSU**	 **Figure 6-68: Time Bound for desired Confidence, Emergency Messages - Scenario 19, Road B, Sender RSU**

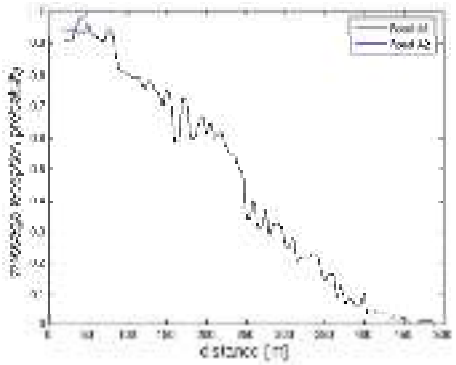
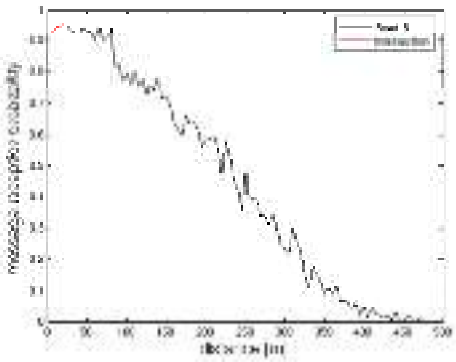
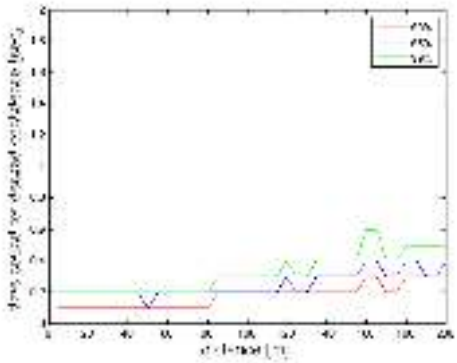
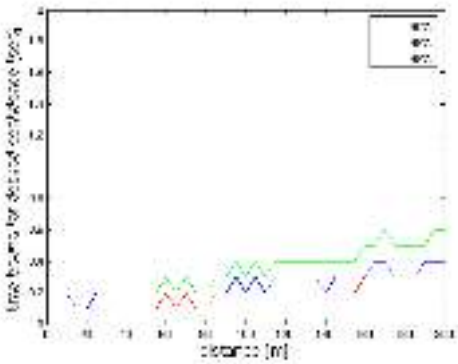
6.2.8 Scenario 20

Number	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
20	Distributed	Building	OBU	200m	ON	2Hz	200m	

	Emergency Messages	
	Road A2	Road B
Reception probability	 **Figure 6-69: Reception Prob. of Emergency Messages – Scenario 20, Rd. A, Sender on Rd. A2**	 **Figure 6-70: Reception Prob. of Emergency Messages – Scenario 20, Rd. B, Sender on Rd. A2**
Time bound for needed confidence	 **Figure 6-71: Time Bound for desired Confidence, Emergency Messages - Scenario 20, Road A, Sender on Road A2**	 **Figure 6-72: Time Bound for desired Confidence, Emergency Messages - Scenario 20, Road B, Sender on Road A2**

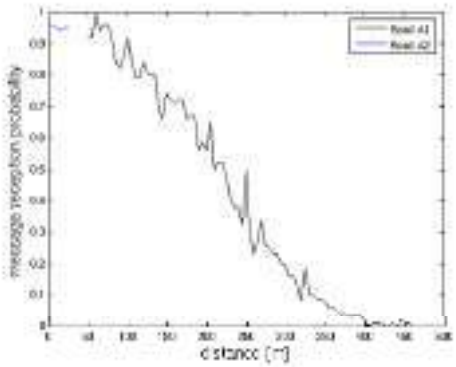
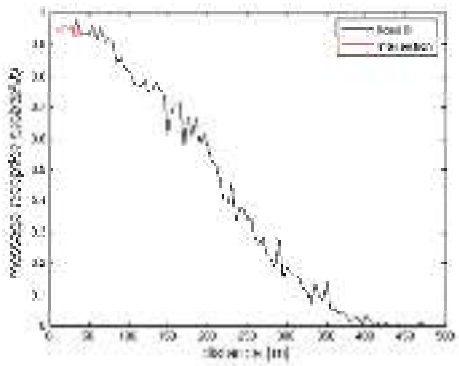
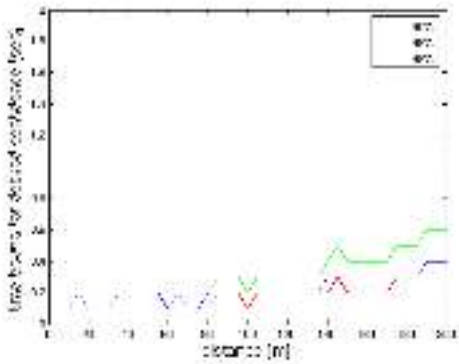
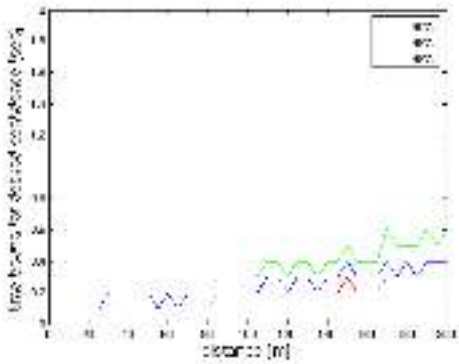
6.2.9 Scenario 21

Number	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
21	Distributed	Open	RSU	300m	ON	2Hz	200m	

	Emergency Messages	
	Road A	Road B
Reception probability	 **Figure 6-73: Reception Probability of Emergency Messages-Scenario 21, Road A, Sender RSU**	 **Figure 6-74: Reception Probability of Emergency Messages-Scenario 21, Road B, Sender RSU**
Time bound for needed confidence	 **Figure 6-75: Time Bound for desired Confidence, Emergency Messages - Scenario 21, Road A, Sender RSU**	 **Figure 6-76: Time Bound for desired Confidence, Emergency Messages - Scenario 21, Road B, Sender RSU**

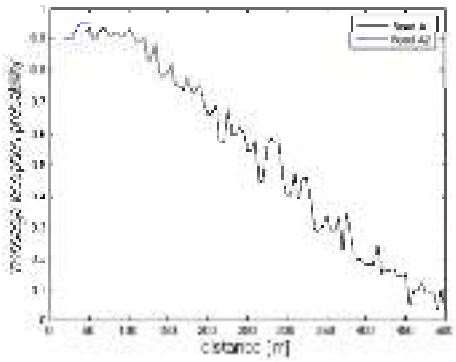
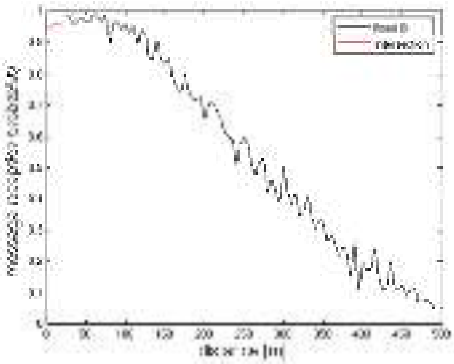
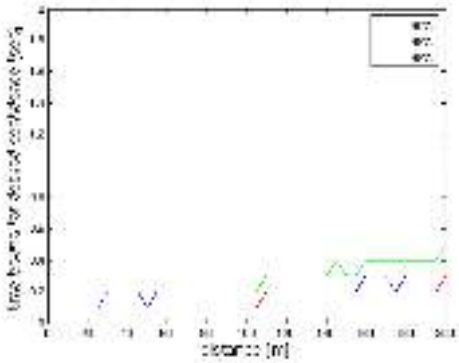
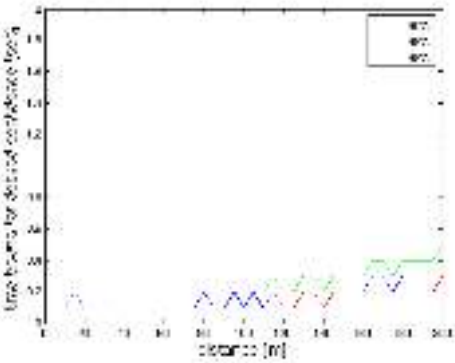
6.2.10 Scenario 22

Number	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
22	Distributed	Open	OBU	300m	ON	2Hz	200m	

	Emergency Messages	
	Road A2	Road B
Reception probability	 **Figure 6-77: Reception Prob. of Emergency Messages – Scenario 22, Rd. A, Sender on Rd. A2**	 **Figure 6-78: Reception Prob. of Emergency Messages – Scenario 22, Rd. B, Sender on Rd. A2**
Time bound for needed confidence	 **Figure 6-79: Time Bound for desired Confidence, Emergency Messages - Scenario 22, Road A, Sender on Road A2**	 **Figure 6-80: Time Bound for desired Confidence, Emergency Messages - Scenario 22, Road B, Sender on Road A2**

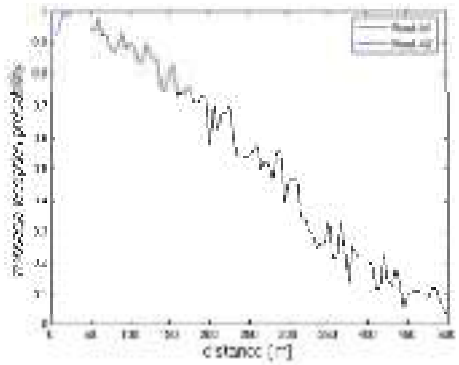
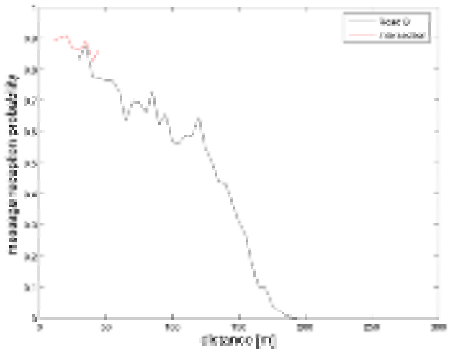
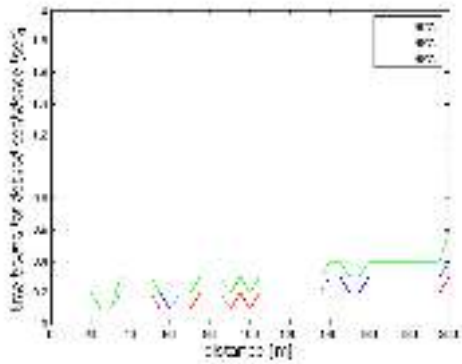
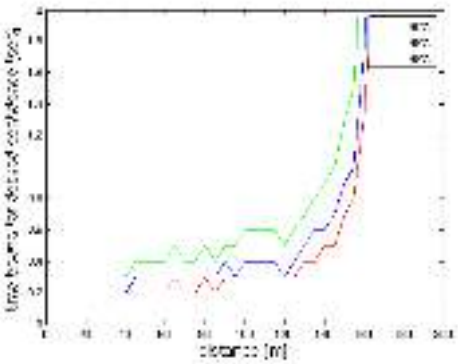
6.2.11 Scenario 23

Number	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
23	Distributed	Building	RSU	300m	ON	2Hz	200m	

	Emergency Messages	
	Road A	Road B
Reception probability	 **Figure 6-81: Reception Probability of Emergency Messages-Scenario 23, Road A, Sender RSU**	 **Figure 6-82: Reception Probability of Emergency Messages-Scenario 23, Road B, Sender RSU**
Time bound for needed confidence	 **Figure 6-83: Time Bound for desired Confidence, Emergency Messages - Scenario 23, Road A, Sender RSU**	 **Figure 6-84: Time Bound for desired Confidence, Emergency Messages - Scenario 23, Road B, Sender RSU**

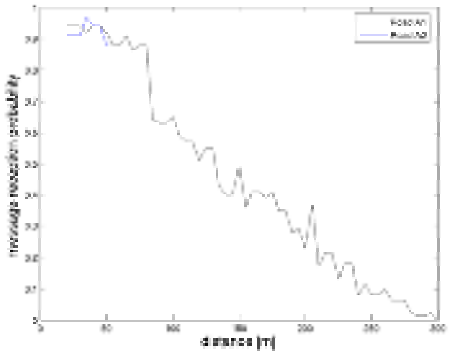
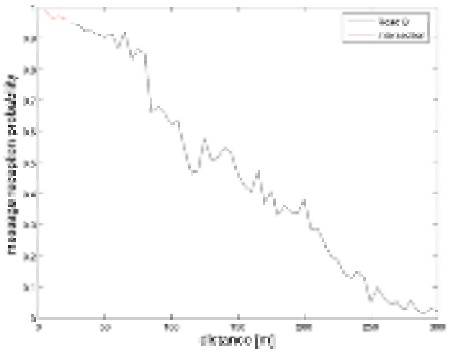
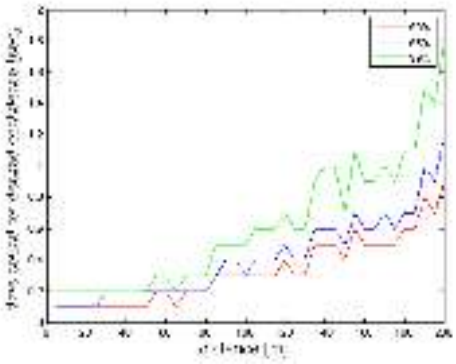
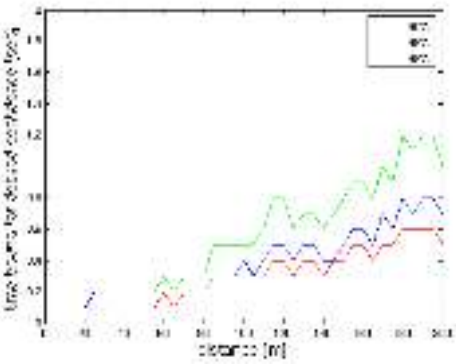
6.2.12 Scenario 24

Number	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
24	Distributed	Building	OBU	300m	ON	2Hz	200m	

	Emergency Messages	
	Road A2	Road B
Reception probability	 **Figure 6-85: Reception Prob. of Emergency Messages – Scenario 24, Rd. A, Sender on Rd. A2**	 **Figure 6-86: Reception Prob. Of Emergency Messages –Scenario 24, Rd. B, Sender on Rd. A2**
Time bound for needed confidence	 **Figure 6-87: Time Bound for desired Confidence, Emergency Messages - Scenario 24, Road A, Sender on Road A2**	 **Figure 6-88: Time Bound for desired Confidence, Emergency Messages - Scenario 24, Road B, Sender on Road A2**

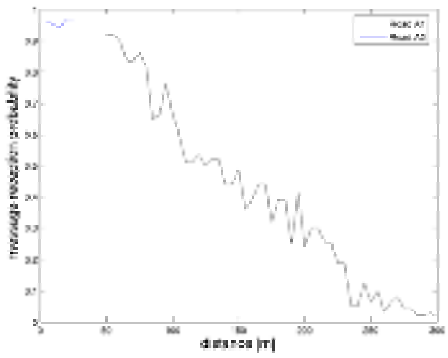
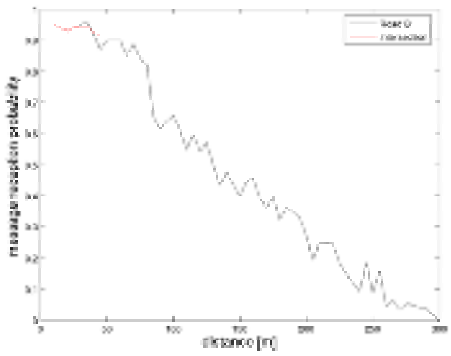
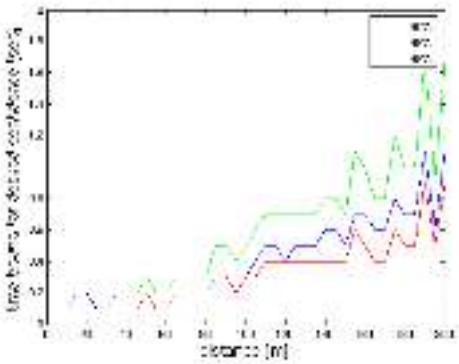
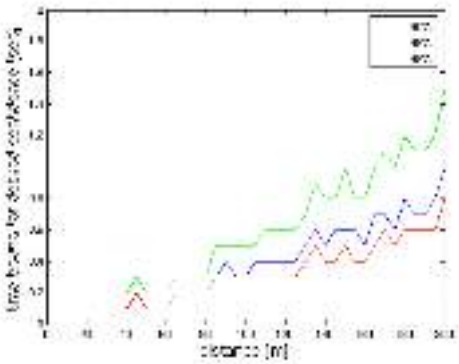
6.2.13 Scenario 25

Number	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
25	Distributed	Open	RSU	200m	ON	1Hz	200m	

	Emergency Messages	
	Road A	Road B
Reception probability	 **Figure 6-89: Reception Probability of Emergency Messages-Scenario 25, Road A, Sender RSU**	 **Figure 6-90: Reception Probability of Emergency Messages-Scenario 25, Road B, Sender RSU**
Time bound for needed confidence	 **Figure 6-91: Time Bound for desired Confidence, Emergency Messages - Scenario 25, Road A, Sender RSU**	 **Figure 6-92: Time Bound for desired Confidence, Emergency Messages - Scenario 25, Road B, Sender RSU**

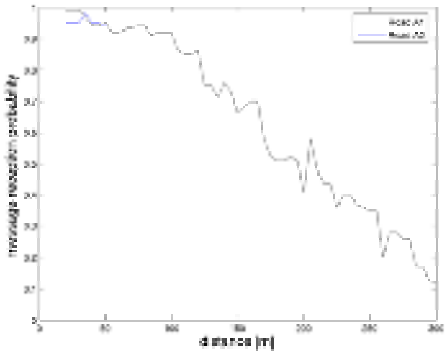
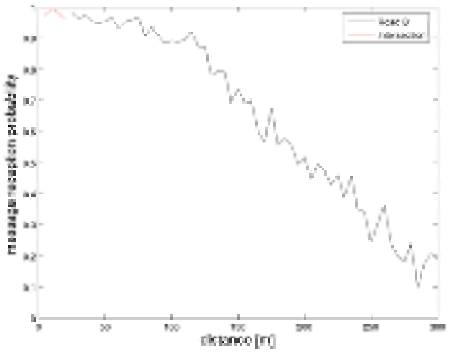
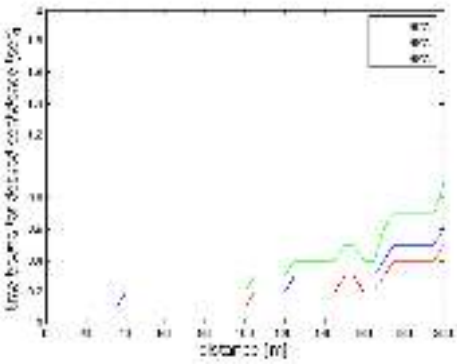
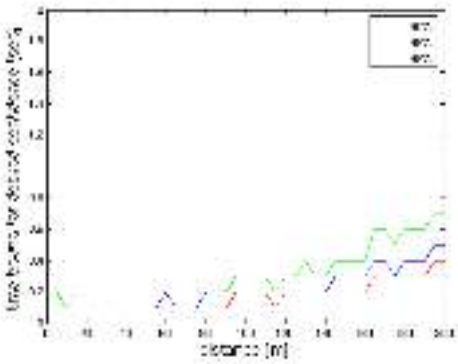
6.2.14 Scenario 26

Number	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
26	Distributed	Open	OBU	200m	ON	1Hz	200m	

	Emergency Messages	
	Road A2	Road B
Reception probability	 **Figure 6-93: Reception Prob. of Emergency Messages – Scenario 26, Rd. A, Sender on Rd. A2**	 **Figure 6-94: Reception Prob. of Emergency Messages – Scenario 26, Rd. B, Sender on Rd. A2**
Time bound for needed confidence	 **Figure 6-95: Time Bound for desired Confidence, Emergency Messages - Scenario 26, Road A, Sender on Road A2**	 **Figure 6-96: Time Bound for desired Confidence, Emergency Messages - Scenario 26, Road B, Sender on Road A2**

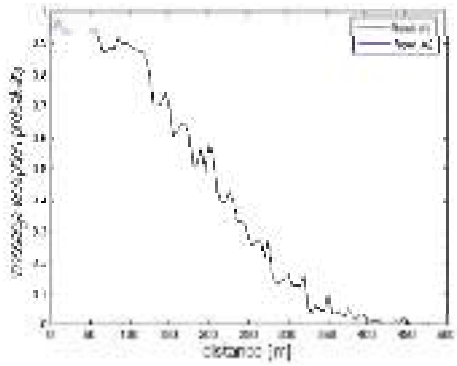
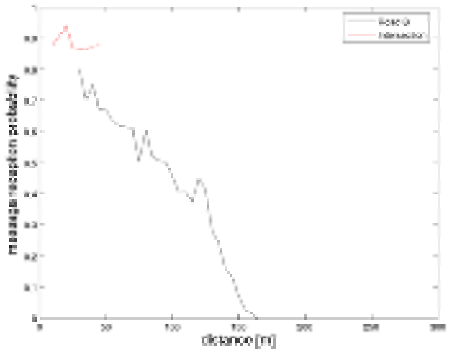
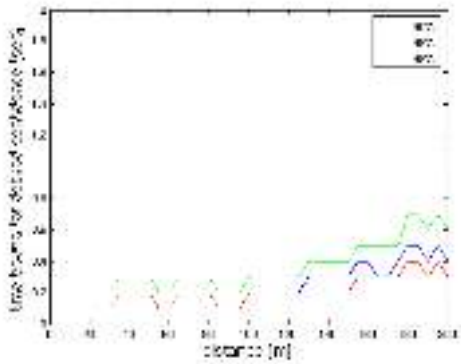
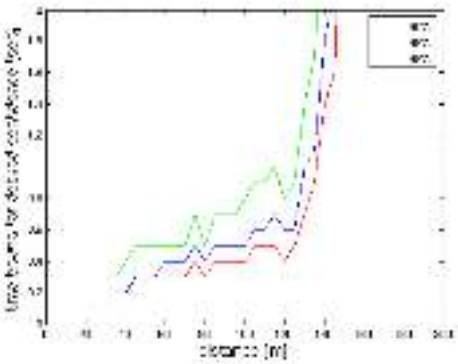
6.2.15 Scenario 27

Number	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
27	Distributed	Building	RSU	200m	ON	1Hz	200m	

	Emergency Messages	
	Road A	Road B
Reception probability	 **Figure 6-97: Reception Probability of Emergency Messages-Scenario 27, Road A, Sender RSU**	 **Figure 6-98: Reception Probability of Emergency Messages-Scenario 27, Road B, Sender RSU**
Time bound for needed confidence	 **Figure 6-99: Time Bound for desired Confidence, Emergency Messages - Scenario 27, Road A, Sender RSU**	 **Figure 6-100: Time Bound for desired Confidence, Emergency Messages – Scenario 27, Road B, Sender RSU**

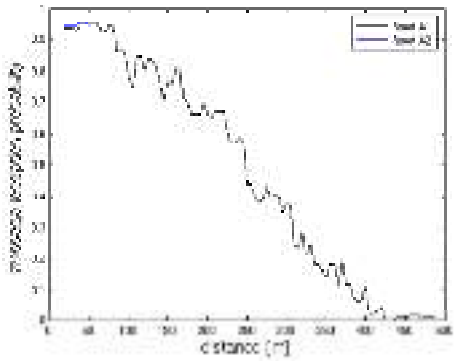
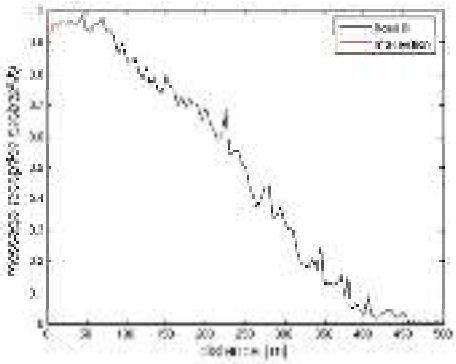
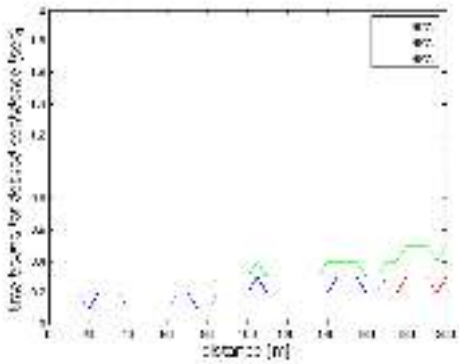
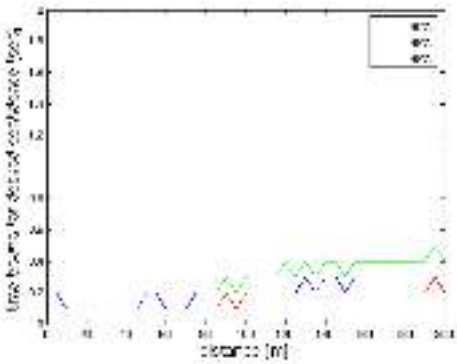
6.2.16 Scenario 28

Number	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
28	Distributed	Building	OBU	200m	ON	1Hz	200m	

	Emergency Messages	
	Road A2	Road B
Reception probability	 **Figure 6-101: Reception Prob. of Emergency Messages – Scenario 28, Rd. A, Sender on Rd. A2**	 **Figure 6-102: Reception Prob. of Emergency Messages – Scenario 28, Rd. B, Sender on Rd. A2**
Time bound for needed confidence	 **Figure 6-103: Time Bound for desired Confidence, Emergency Messages - Scenario 28, Road A, Sender on Road A2**	 **Figure 6-104: Time Bound for desired Confidence, Emergency Messages - Scenario 28, Road B, Sender on Road A2**

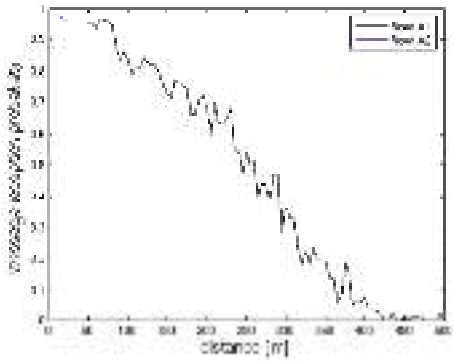
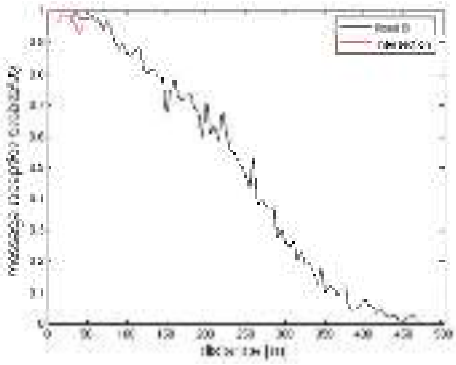
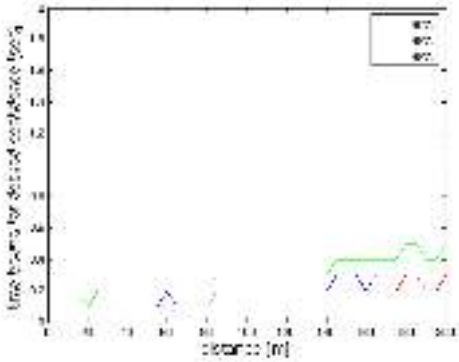
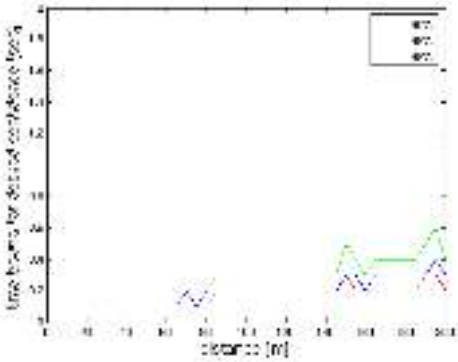
6.2.17 Scenario 29

Number	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
29	Distributed	Open	RSU	300m	ON	1Hz	200m	

	Emergency Messages	
	Road A	Road B
Reception probability	 **Figure 6-105: Reception Probability of Emergency Messages-Scenario 29, Road A, Sender RSU**	 **Figure 6-106: Reception Probability of Emergency Messages-Scenario 29, Road B, Sender RSU**
Time bound for needed confidence	 **Figure 6-107: Time Bound for desired Confidence, Emergency Messages - Scenario 29, Road A, Sender RSU**	 **Figure 6-108: Time Bound for desired Confidence, Emergency Messages - Scenario 29, Road B, Sender RSU**

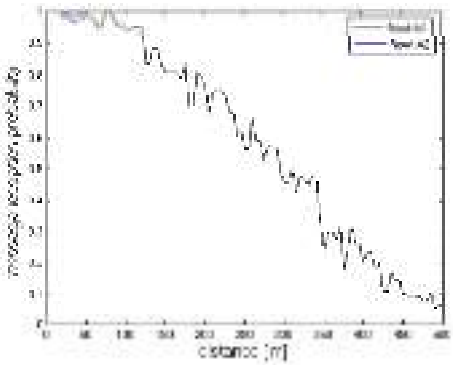
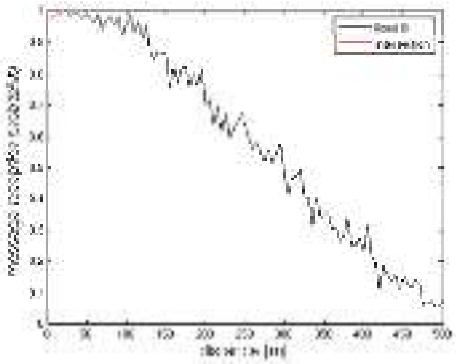
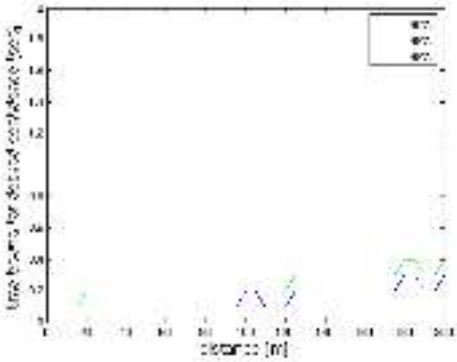
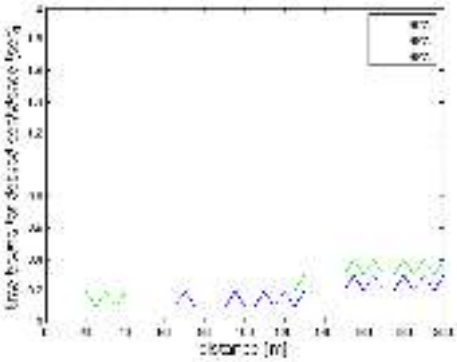
6.2.18 Scenario 30

Number	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
30	Distributed	Open	OBU	300m	ON	1Hz	200m	

	Emergency Messages	
	Road A2	Road B
Reception probability	 **Figure 6-109: Reception Prob. of Emergency Messages – Scenario 30, Rd. A, Sender on Rd. A2**	 **Figure 6-110: Reception Prob. of Emergency Messages – Scenario 30, Rd. B, Sender on Rd A2**
Time bound for needed confidence	 **Figure 6-111: Time Bound for desired Confidence, Emergency Messages - Scenario 30, Road A, Sender on Road A2**	 **Figure 6-112: Time Bound for desired Confidence, Emergency Messages - Scenario 30, Road B, Sender on Road A2**

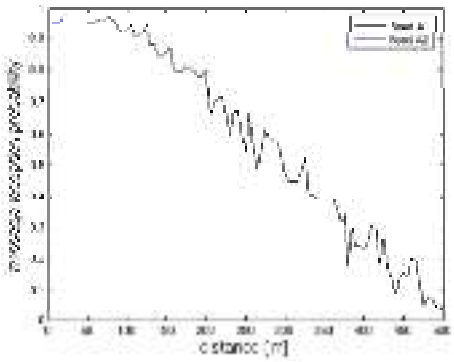
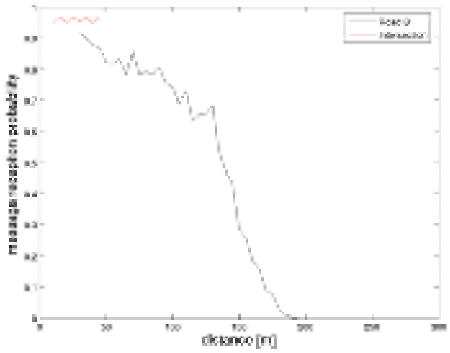
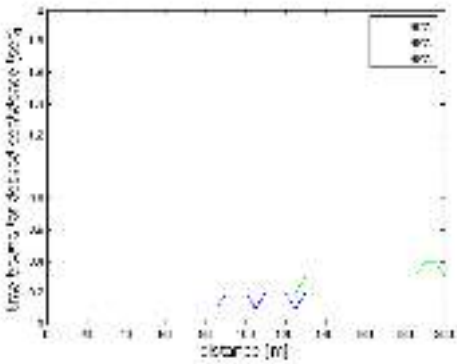
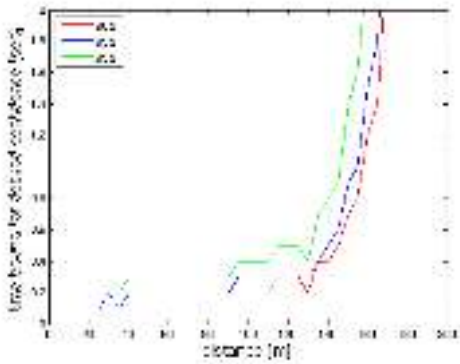
6.2.19 Scenario 31

Number	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
31	Distributed	Building	RSU	300m	ON	1Hz	200m	

	Emergency Messages	
	Road A	Road B
Reception probability	 **Figure 6-113: Reception Probability of Emergency Messages-Scenario 31, Road A, Sender RSU**	 **Figure 6-114: Reception Probability of Emergency Messages-Scenario 31, Road B, Sender RSU**
Time bound for needed confidence	 **Figure 6-115: Time Bound for desired Confidence, Emergency Messages - Scenario 31, Road A, Sender RSU**	 **Figure 6-116: Time Bound for desired Confidence, Emergency Messages - Scenario 31, Road B, Sender RSU**

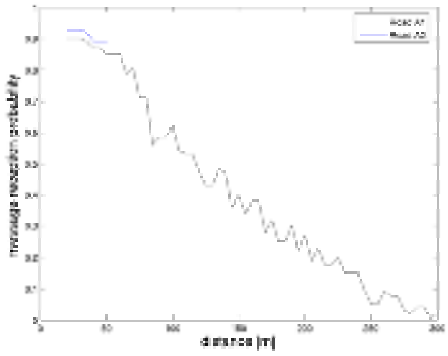
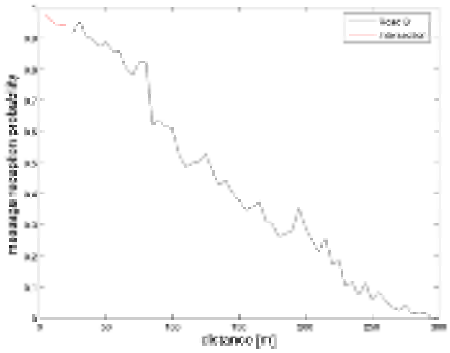
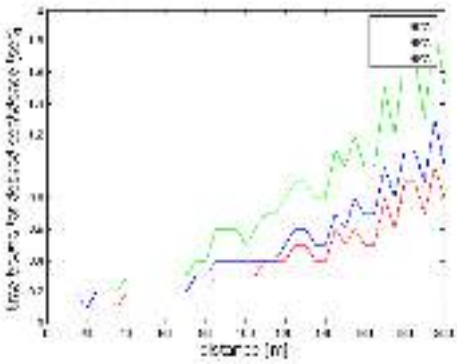
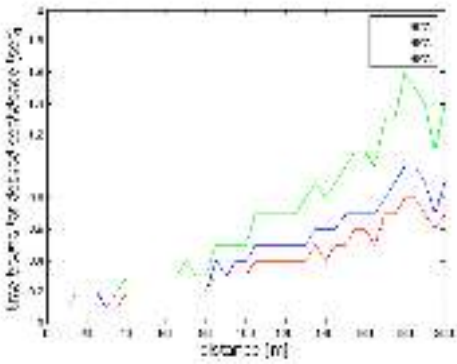
6.2.20 Scenario 32

Number	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
32	Distributed	Building	OBU	300m	ON	1Hz	200m	

	Emergency Messages	
	Road A2	Road B
Reception probability	 **Figure 6-117: Reception Prob. of Emergency Messages – Scenario 32, Rd. A, Sender on Rd. A2**	 **Figure 6-118: Reception Prob. of Emergency Messages – Scenario 32, Rd. B, Sender on Rd A2**
Time bound for needed confidence	 **Figure 6-119: Time Bound for desired Confidence, Emergency Messages - Scenario 32, Road A, Sender on Road A2**	 **Figure 6-120: Time Bound for desired Confidence, Emergency Messages – Scenario 32, Road B, Sender on Road A2**

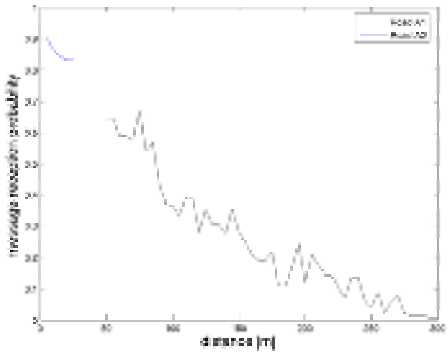
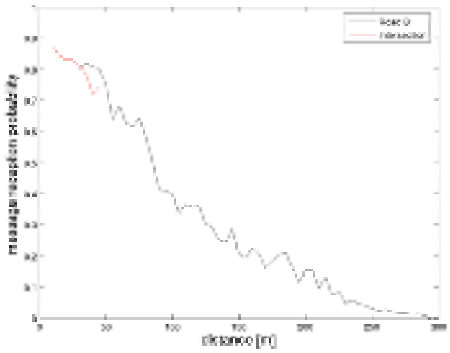
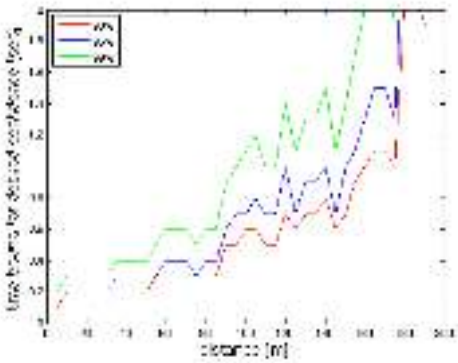
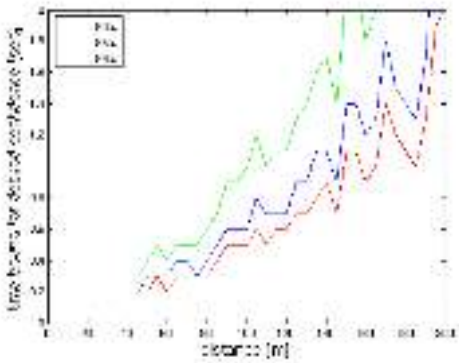
6.2.21 Scenario 33

Number	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
33	Distributed	Open	RSU	200m	ON	5Hz	200m	

	Emergency Messages	
	Road A	Road B
Reception probability	 **Figure 6-121: Reception Probability of Emergency Messages-Scenario 33, Road A, Sender RSU**	 **Figure 6-122: Reception Probability of Emergency Messages-Scenario 33, Road B, Sender RSU**
Time bound for needed confidence	 **Figure 6-123: Time Bound for desired Confidence, Emergency Messages - Scenario 33, Road A, Sender RSU**	 **Figure 6-124: Time Bound for desired Confidence, Emergency Messages – Scenario 33, Road B, Sender RSU**

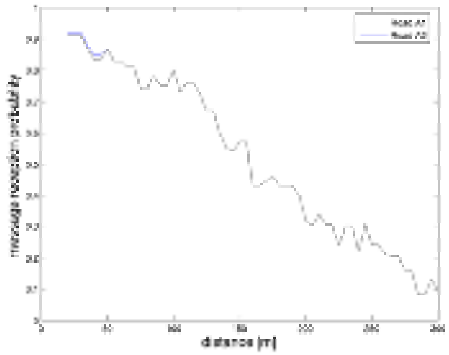
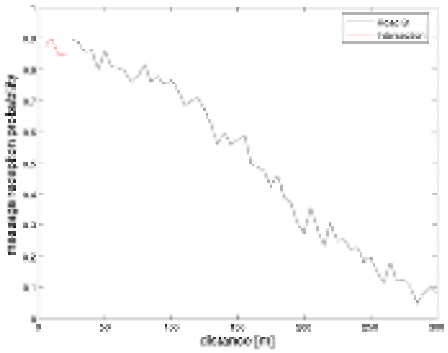
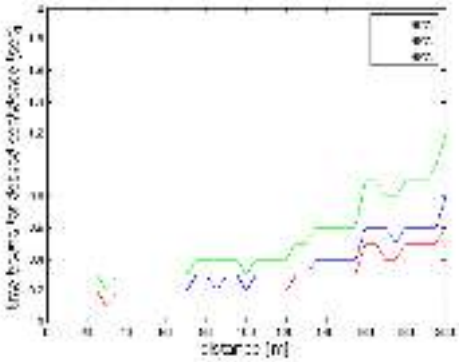
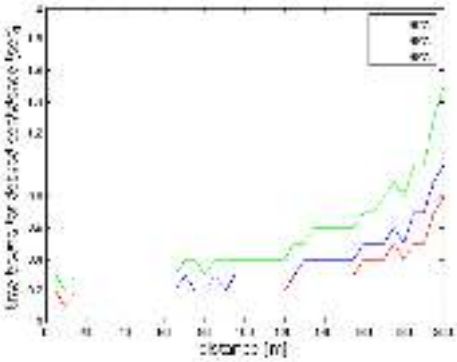
6.2.22 Scenario 34

Number	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
34	Distributed	Open	OBU	200m	ON	5Hz	200m	

	Emergency Messages	
	Road A2	Road B
Reception probability	 **Figure 6-125: Reception Prob. of Emergency Messages – Scenario 34, Rd. A, Sender on Rd. A2**	 **Figure 6-126: Reception Prob. of Emergency Messages – Scenario 34, Rd. B, Sender on Rd. A2**
Time bound for needed confidence	 **Figure 6-127: Time Bound for desired Confidence, Emergency Messages - Scenario 34, Road A, Sender on Road A2**	 **Figure 6-128: Time Bound for desired Confidence, Emergency Messages - Scenario 34, Road B, Sender on Road A2**

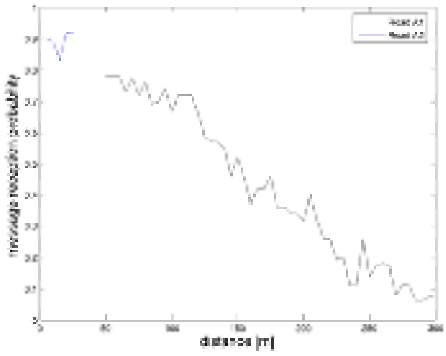
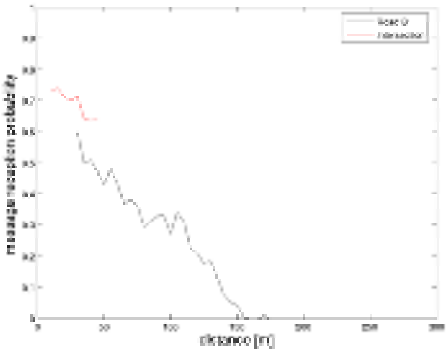
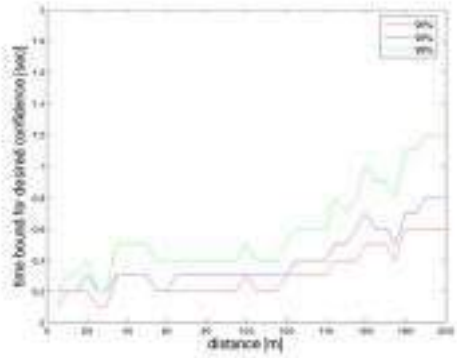
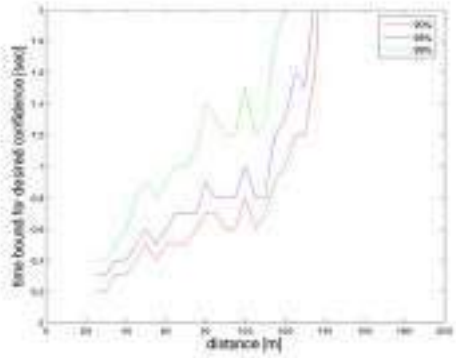
6.2.23 Scenario 35

Number	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
35	Distributed	Building	RSU	200m	ON	5Hz	200m	

	Emergency Messages	
	Road A	Road B
Reception probability	 **Figure 6-129: Reception Probability of Emergency Messages-Scenario 35, Road A, Sender RSU**	 **Figure 6-130: Reception Probability of Emergency Messages-Scenario 35, Road B, Sender RSU**
Time bound for needed confidence	 **Figure 6-131: Time Bound for desired Confidence, Emergency Messages - Scenario 35, Road A, Sender RSU**	 **Figure 6-132: Time Bound for desired Confidence, Emergency Messages – Scenario 35, Road B, Sender RSU**

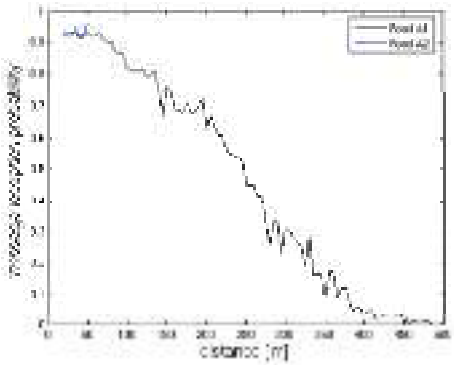
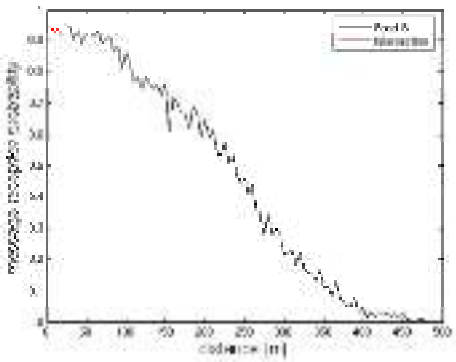
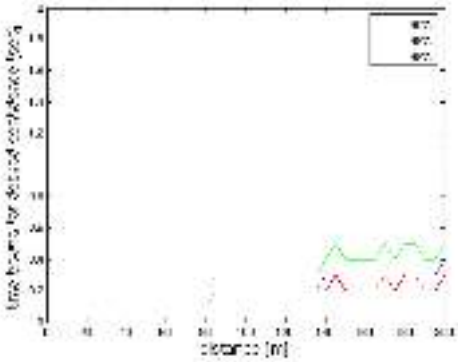
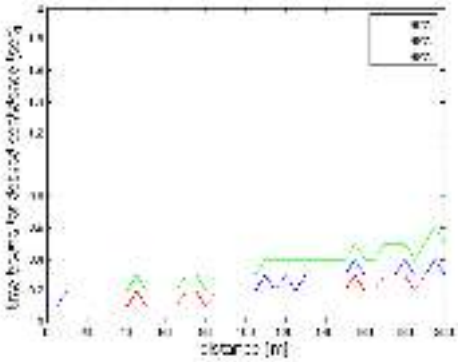
6.2.24 Scenario 36

Number	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
36	Distributed	Building	OBU	200m	ON	5Hz	200m	

	Emergency Messages	
	Road A2	Road B
Reception probability	 **Figure 6-133: Reception Prob. of Emergency Messages – Scenario 36, Rd. A, Sender on Rd. A2**	 **Figure 6-134: Reception Prob. of Emergency Messages – Scenario 36, Rd. B, Sender on Rd. A2**
Time bound for needed confidence	 **Figure 6-135: Time Bound for desired Confidence, Emergency Messages - Scenario 36, Road A, Sender on Road A2**	 **Figure 6-136: Time Bound for desired Confidence, Emergency Messages - Scenario 36, Road B, Sender on Road A2**

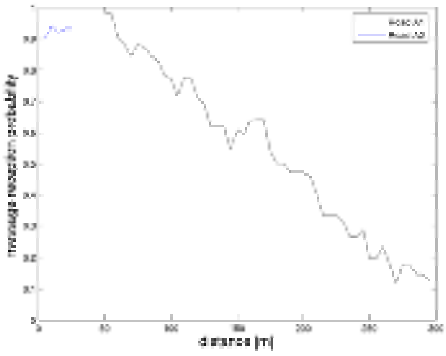
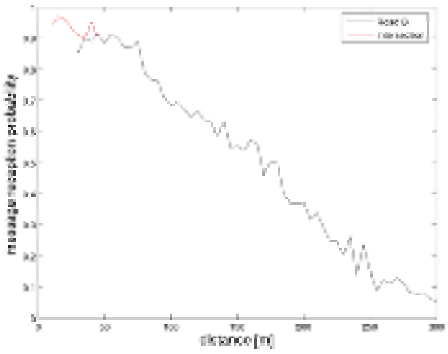
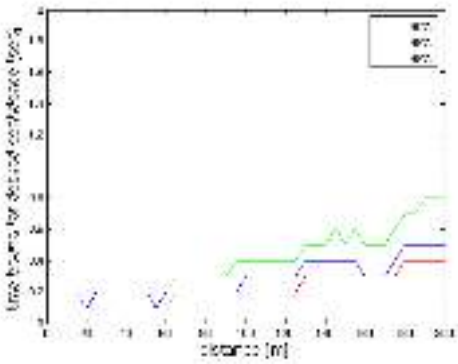
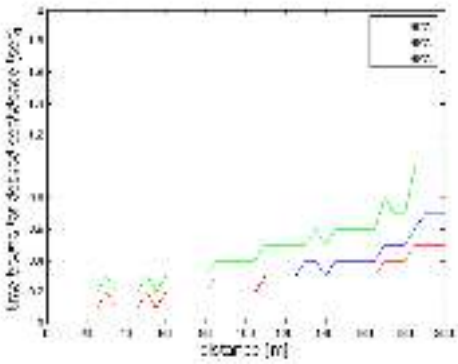
6.2.25 Scenario 37

Number	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
37	Distributed	Open	RSU	300m	ON	5Hz	200m	

	Emergency Messages	
	Road A	Road B
Reception probability	 **Figure 6-137: Reception Probability of Emergency Messages-Scenario 37, Road A, Sender RSU**	 **Figure 6-138: Reception Probability of Emergency Messages-Scenario 37, Road B, Sender RSU**
Time bound for needed confidence	 **Figure 6-139: Time Bound for desired Confidence, Emergency Messages - Scenario 37, Road A, Sender RSU**	 **Figure 6-140: Time Bound for desired Confidence, Emergency Messages - Scenario 37, Road B, Sender RSU**

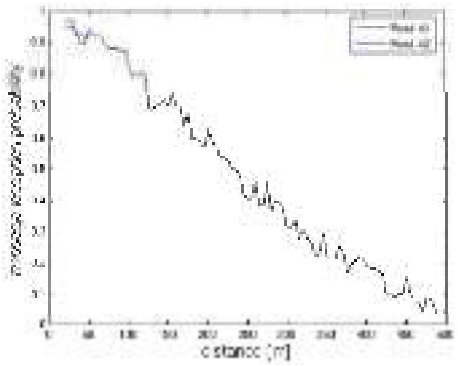
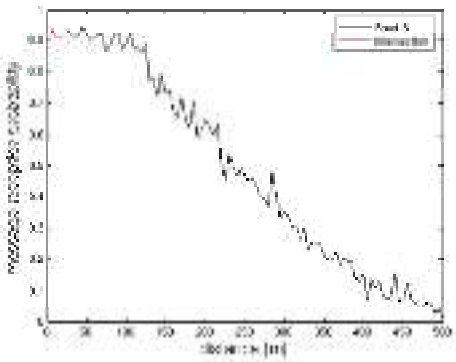
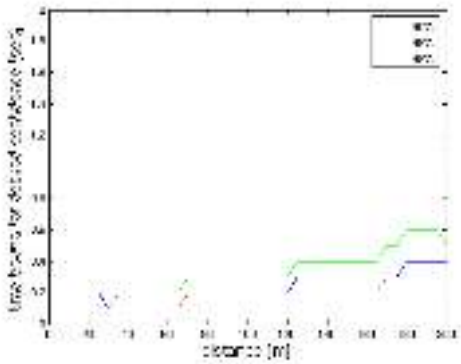
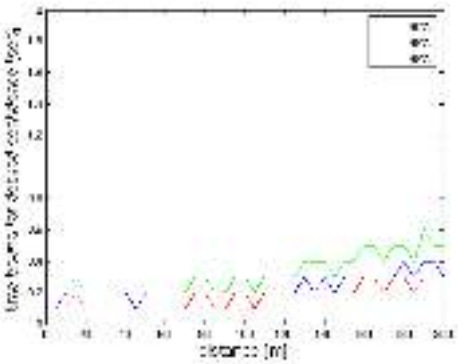
6.2.26 Scenario 38

Number	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
38	Distributed	Open	OBU	300m	ON	5Hz	200m	

	Emergency Messages	
	Road A2	Road B
Reception probability	 **Figure 6-141: Reception Prob. of Emergency Messages – Scenario 38, Rd. A, Sender on Rd. A2**	 **Figure 6-142: Reception Prob. of Emergency Messages –Scenario 38, Rd. B, Sender on Rd. A2**
Time bound for needed confidence	 **Figure 6-143: Time Bound for desired Confidence, Emergency Messages - Scenario 38, Road A, Sender on Road A2**	 **Figure 6-144: Time Bound for desired Confidence, Emergency Messages - Scenario 38, Road B, Sender on Road A2**

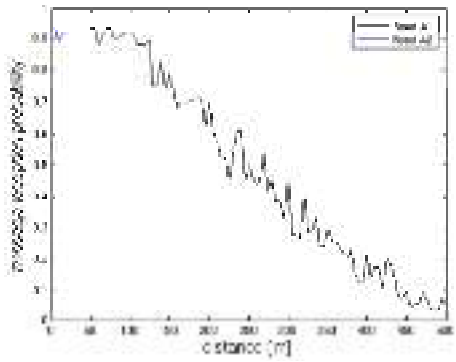
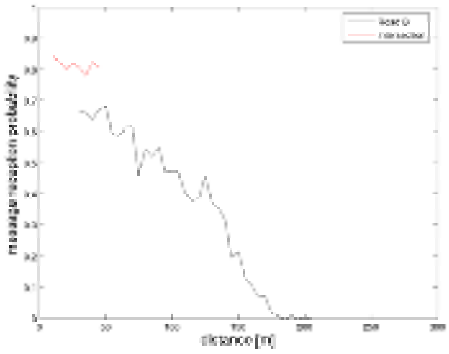
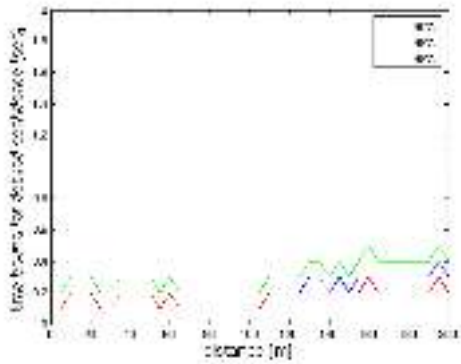
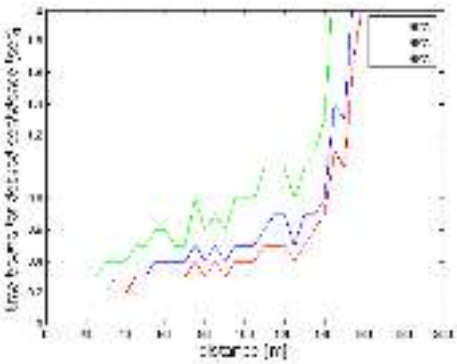
6.2.27 Scenario 39

Number	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
39	Distributed	Building	RSU	300m	ON	5Hz	200m	

	Emergency Messages	
	Road A	Road B
Reception probability	 **Figure 6-145: Reception Probability of Emergency Messages-Scenario 39, Road A, Sender RSU**	 **Figure 6-146: Reception Probability of Emergency Messages-Scenario 39, Road B, Sender RSU**
Time bound for needed confidence	 **Figure 6-147: Time Bound for desired Confidence, Emergency Messages - Scenario 39, Road A, Sender RSU**	 **Figure 6-148: Time Bound for desired Confidence, Emergency Messages - Scenario 39, Road B, Sender RSU**

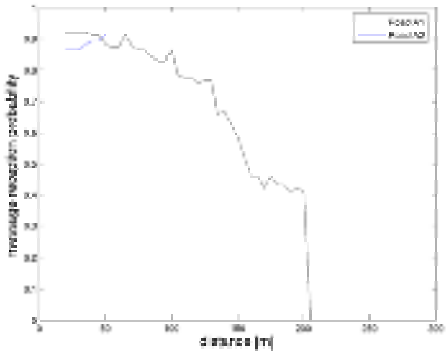
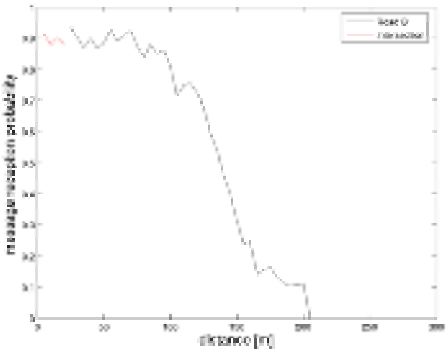
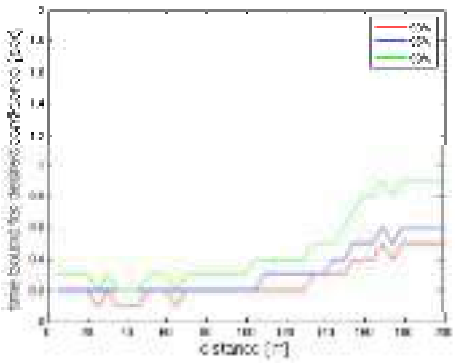
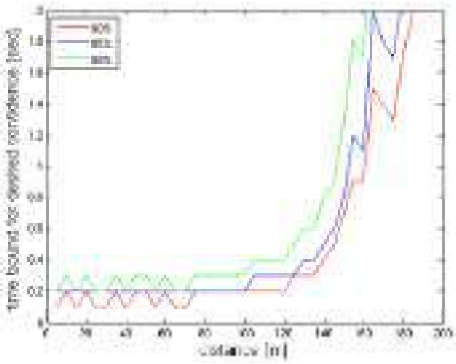
6.2.28 Scenario 40

Number	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
40	Distributed	Building	OBU	300m	ON	5Hz	200m	

	Emergency Messages	
	Road A2	Road B
Reception probability	 **Figure 6-149: Reception Prob. of Emergency Messages – Scenario 40, Rd. A, Sender on Rd. A2**	 **Figure 6-150: Reception Prob. of Emergency Messages –Scenario 40, Rd. B, Sender on Rd. A2**
Time bound for needed confidence	 **Figure 6-151: Time Bound for desired Confidence, Emergency Messages - Scenario 40, Road A, Sender on Road A2**	 **Figure 6-152: Time Bound for desired Confidence, Emergency Messages - Scenario 40, Road B, Sender on Road A2**

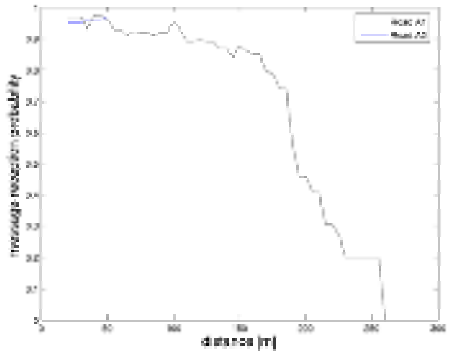
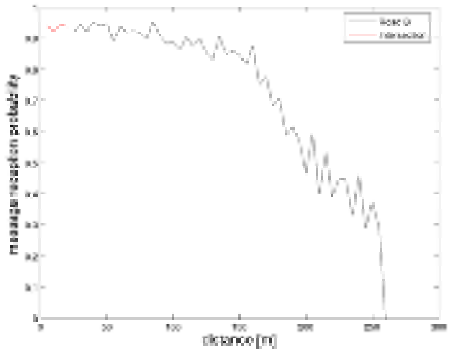
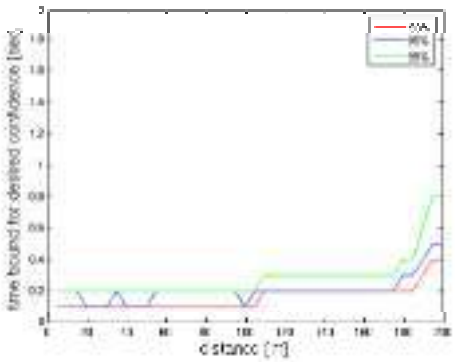
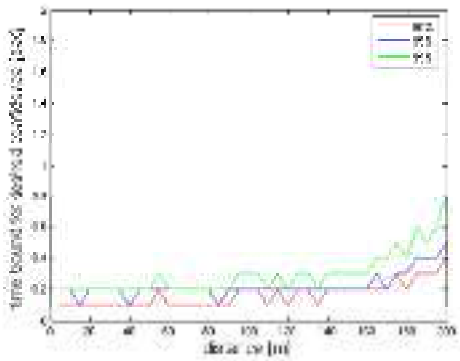
6.2.29 Scenario 49

Number	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
49	Deterministic	Open	RSU	200m	ON	10Hz	100m	

	Emergency Messages	
	Road A	Road B
Reception probability	 **Figure 6-153: Reception Probability of Emergency Messages-Scenario 49, Road A, Sender RSU**	 **Figure 6-154: Reception Probability of Emergency Messages-Scenario 49, Road B, Sender RSU**
Time bound for needed confidence	 **Figure 6-155: Time Bound for desired Confidence, Emergency Messages - Scenario 49, Road A, Sender RSU**	 **Figure 6-156: Time Bound for desired Confidence, Emergency Messages – Scenario 49, Road B, Sender RSU**

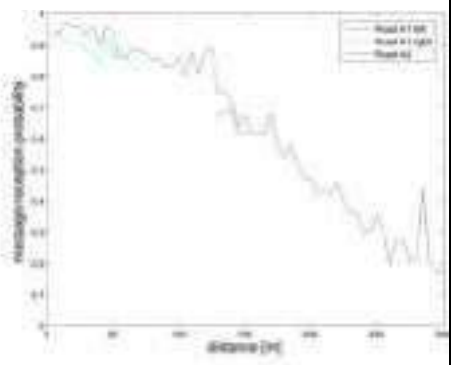
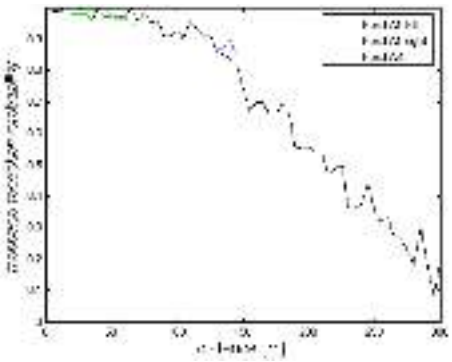
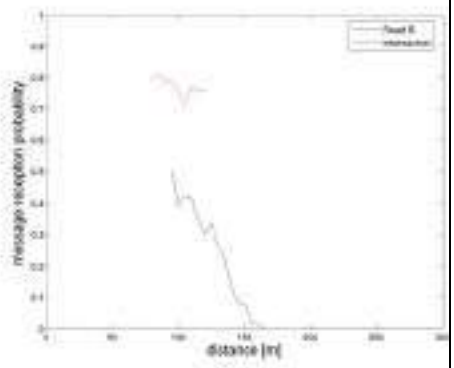
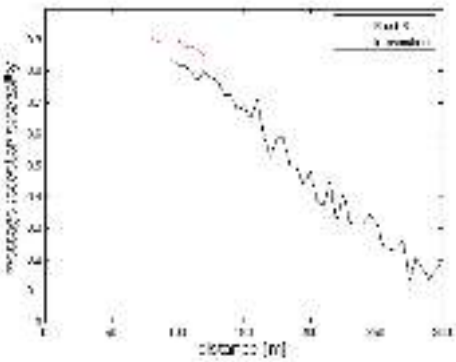
6.2.30 Scenario 50

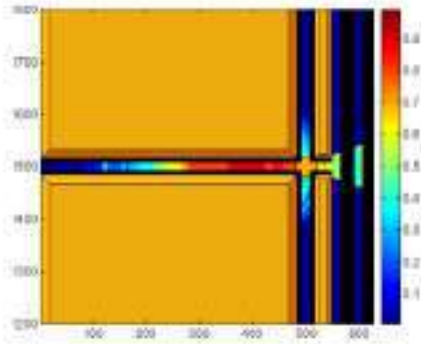
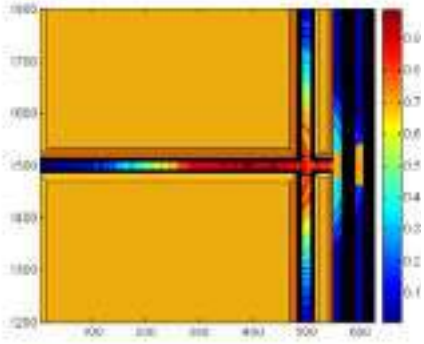
Number	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
50	Deterministic	Building	RSU	200m	ON	10Hz	100m	

	Emergency Messages	
	Road A	Road B
Reception probability	 **Figure 6-157: Reception Probability of Emergency Messages-Scenario 50, Road A, Sender RSU**	 **Figure 6-158: Reception Probability of Emergency Messages-Scenario 50, Road B, Sender RSU**
Time bound for needed confidence	 **Figure 6-159: Time Bound for desired Confidence, Emergency Messages - Scenario 50, Road A, Sender RSU**	 **Figure 6-160: Time Bound for desired Confidence, Emergency Messages – Scenario 50, Road B, Sender RSU**

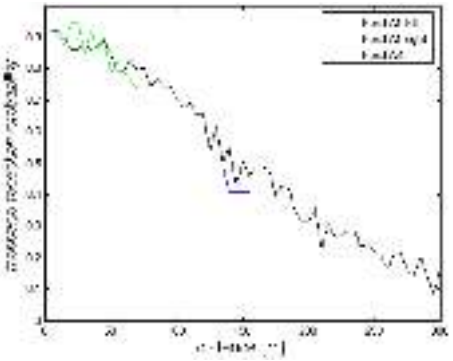
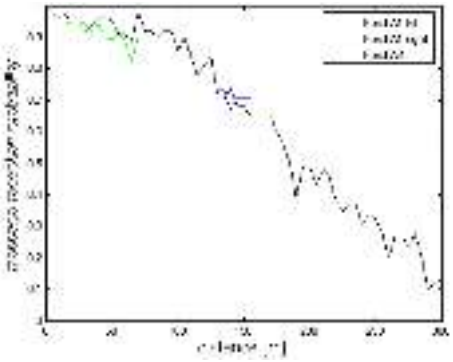
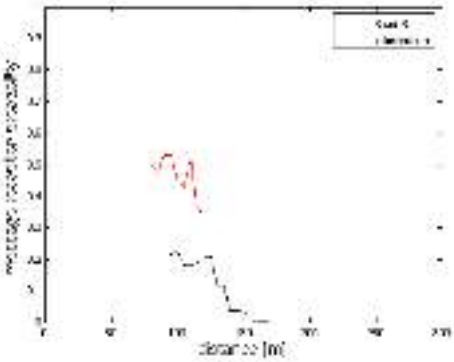
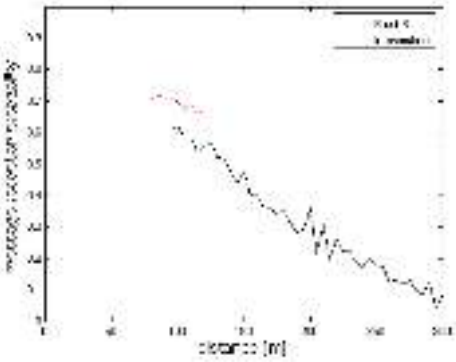
7 Effects of RSU Rebroadcast of Emergency Messages

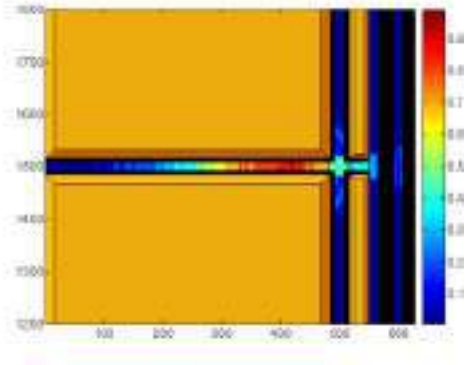
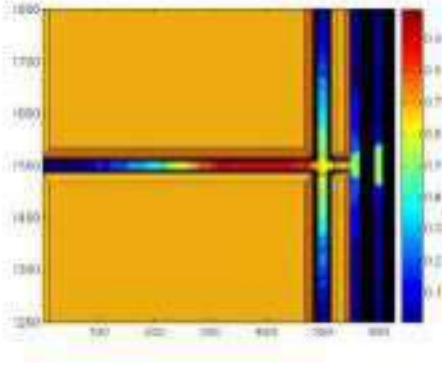
Number	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
Additional 1	Distributed	Building	OBU	200m	ON	2Hz	200m	

	Emergency Messages **Without** ReTx	Emergency Messages **With** ReTx
Road A	 **Figure 7-1: Reception Probability of Emergency Messages** Without **RSU Retransmission, Road A, Sender on Road A1**	 **Figure 7-2: Reception Probability of Emergency Messages** With **RSU Retransmission, Road A, Sender on Road A1**
Road B	 **Figure 7-3: Reception Probability of Emergency Messages** Without **RSU Retransmission, Road B, Sender on Road A1**	 **Figure 7-4: Reception Probability of Emergency Messages** With **RSU Retransmission, Road B, Sender on Road A1**

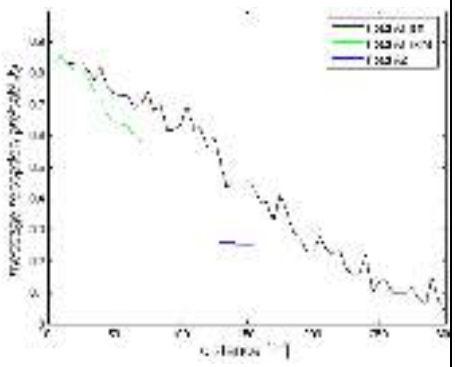
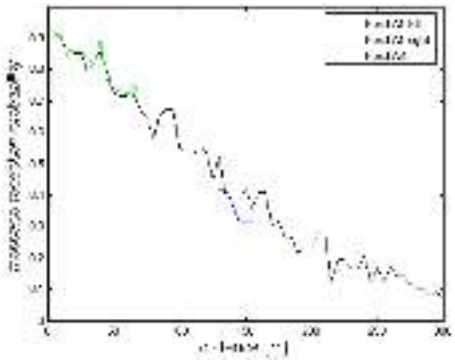
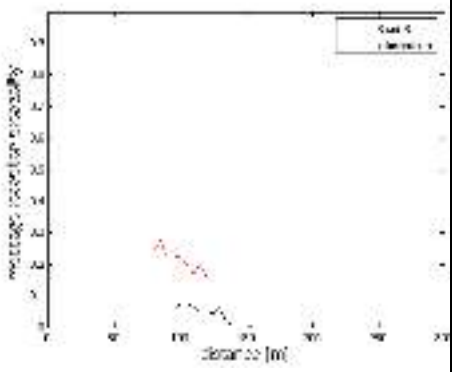
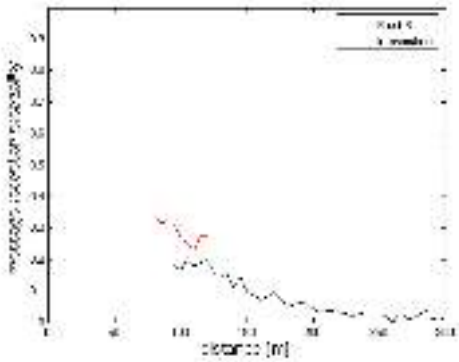
Number	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
Visualization	 **Figure 7-5: Visualization of the Reception Probability of Emergency Messages** Without **RSU Retransmission, Sender on Road A1**				 **Figure 7-6: Visualization of the Reception Probability of Emergency Messages** With **RSU Retransmission, Sender on Road A1**			

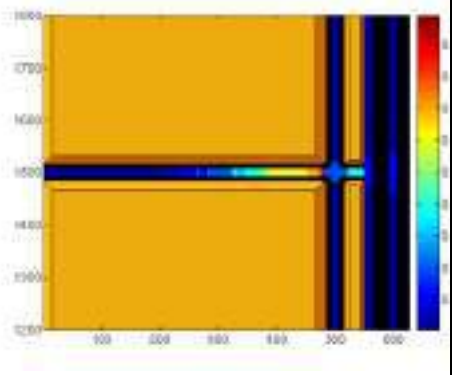
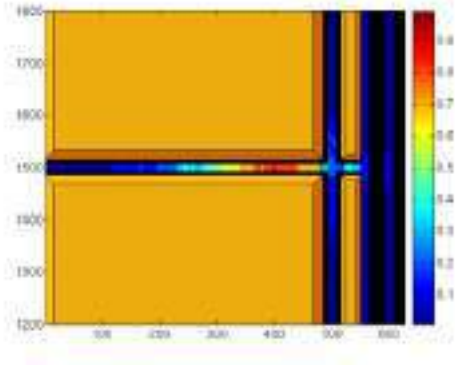
Number.	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
Additional 2	Distributed	Building	OBU	200m	ON	5Hz	200m	

	Emergency Messages **Without** ReTx	Emergency Messages **With** ReTx
Road A	 **Figure 7-7: Reception Probability of Emergency Messages** Without **RSU Retransmission, Road A, Sender on Road A1**	 **Figure 7-8: Reception Probability of Emergency Messages** With **RSU Retransmission, Road A, Sender on Road A1**
Road B	 **Figure 7-9: Reception Probability of Emergency Messages** Without **RSU Retransmission, Road B, Sender on Road A1**	 **Figure 7-10: Reception Probability of Emergency Messages** With **RSU Retransmission, Road B, Sender on Road A1**

Number.	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
Visualization	 **Figure 7-11: Visualization of the Reception Probability of Emergency Messages** Without **RSU Retransmission, Sender on Road A1**				 **Figure 7-12: Visualization of the Reception Probability of Emergency Messages** With **RSU Retransmission, Sender on Road A1**			

Number.	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
Additional 2	Distributed	Building	OBU	200m	ON	10Hz	200m	

	Emergency Messages **Without** ReTx	Emergency Messages **With** ReTx
Road A	 **Figure 7-13: Reception Probability of Emergency Messages** Without **RSU Retransmission, Road A, Sender on Road A1**	 **Figure 7-14: Reception Probability of Emergency Messages** With **RSU Retransmission, Road A, Sender on Road A1**
Road B	 **Figure 7-15: Reception Probability of Emergency Messages** Without **RSU Retransmission, Road B, Sender on Road A1**	 **Figure 7-16: Reception Probability of Emergency Messages** With **RSU Retransmission, Road B, Sender on Road A1**

Number.	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
Visualization	 **Figure 7-17: Visualization of the Reception Probability of Emergency Messages** Without **RSU Retransmission, Sender on Road A1**				 **Figure 7-18: Visualization of the Reception Probability of Emergency Messages** With **RSU Retransmission, Sender on Road A1**			

8 Additional Simulations Regarding Routine Safety Message at Intersection, Based on Scenario 11

8.1 Routine Messages at 6 Hz, Routine Message Size – 200 byte

Simulation Scenario Settings:

RF Model	Distributed
Emergency Message Sender	RSU, 500 bytes/ 10Hz/200m
Corner Model	Tall buildings
Commercial RSU	On, 500bytes/2Hz/200m
Routine Messages	200byte /6Hz /200m

8.1.1 Reception Probability of Emergency Messages

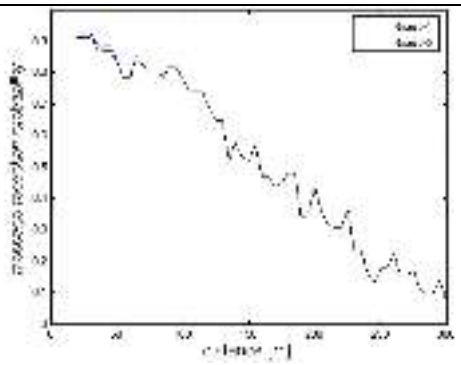


Figure 8-1: Reception Probability of Emergency Messages-Scenario 11, Road A, Sender RSU

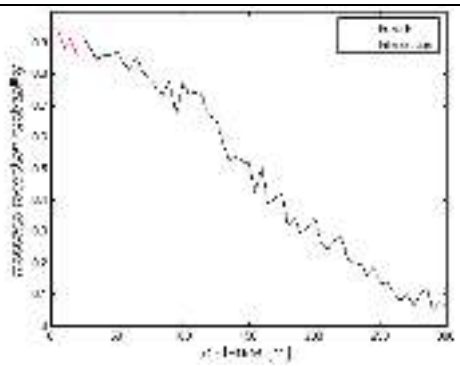


Figure 8-2: Reception Probability of Emergency Messages-Scenario 11, Road B, Sender RSU

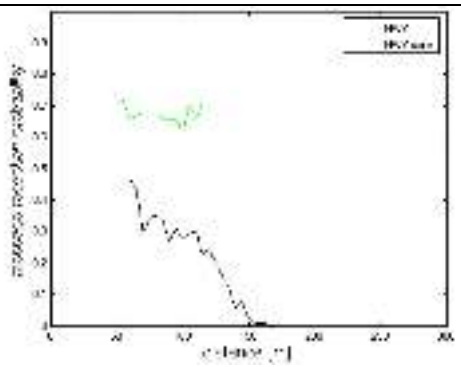


Figure 8-3: Reception Probability of Emergency Messages-Scenario 11, HWY, Sender RSU

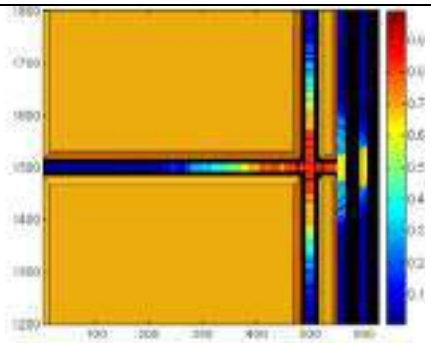
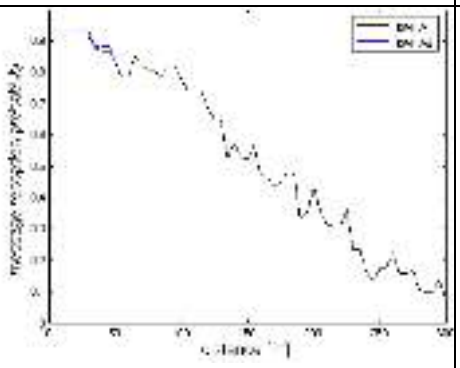
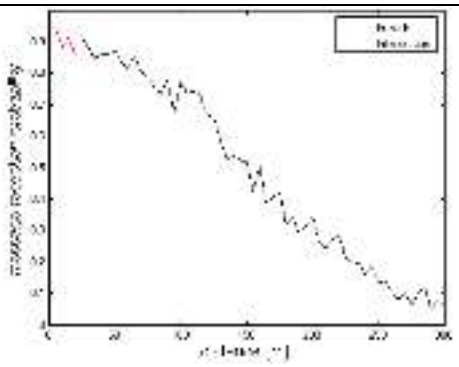
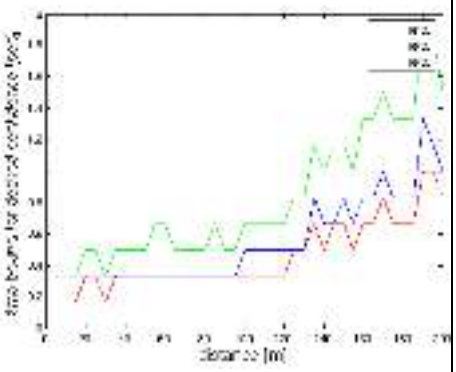
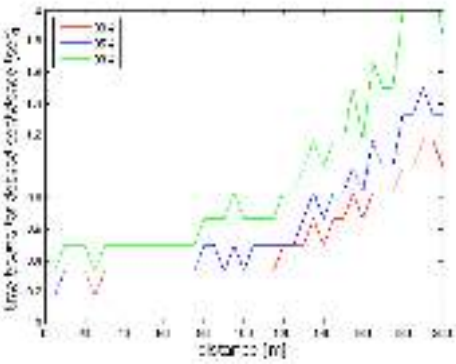


Figure 8-4: Reception Probability of Emergency Messages-Scenario11, Sender RSU

8.1.2 Time Bound for Emergency Messages

Number	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
11	Distributed	Building	RSU	200m	ON	6Hz	200m	

	Emergency Messages	
	Road A	Road B
Reception probability	 **Figure 8-5: Reception Probability of Emergency Messages-Scenario 11, Road A, Sender RSU**	 **Figure 8-6: Reception Probability of Emergency Messages-Scenario 11, Road B, Sender RSU**
Time bound for needed confidence	 **Figure 8-7: Time Bound for desired Confidence, Emergency Messages - Scenario 11, Road A, Sender RSU**	 **Figure 8-8: Time Bound for desired Confidence, Emergency Messages – Scenario 11, Road B, Sender RSU**

8.1.3 Reception Probability of Routine Messages

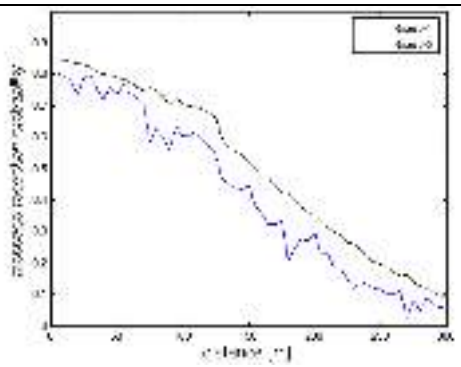


Figure 8-9: Reception Probability of Routine Messages on Road A, Scenario 11

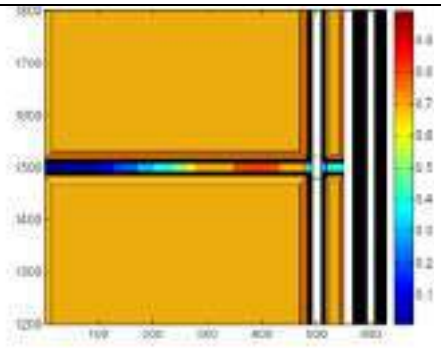


Figure 8-10: Reception Probability of Routine Messages on Road A, Scenario 11

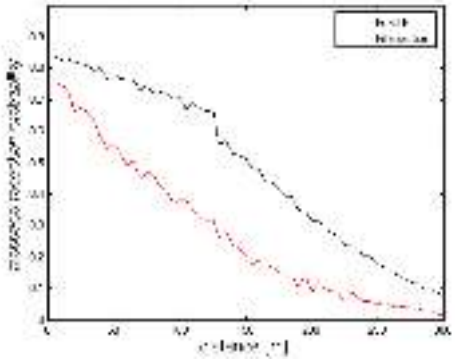


Figure 8-11: Reception Probability of Routine Messages on Road B, Scenario 11

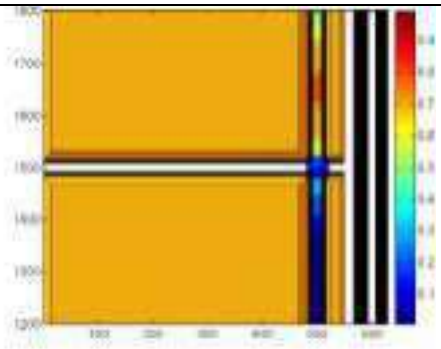


Figure 8-12: Reception Probability of Routine Messages on Road B, Scenario 11

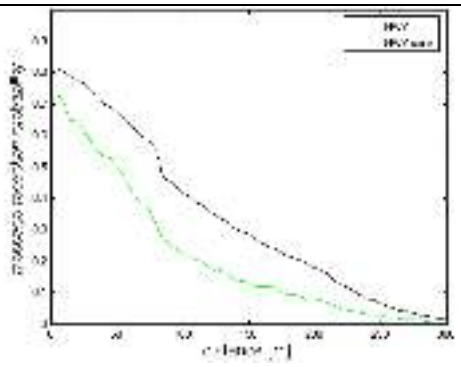


Figure 8-13: Reception Probability of Routine Messages on HWY, Scenario 11

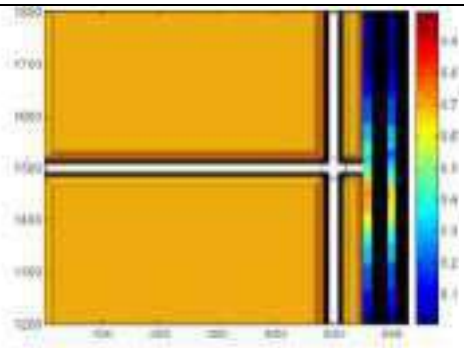
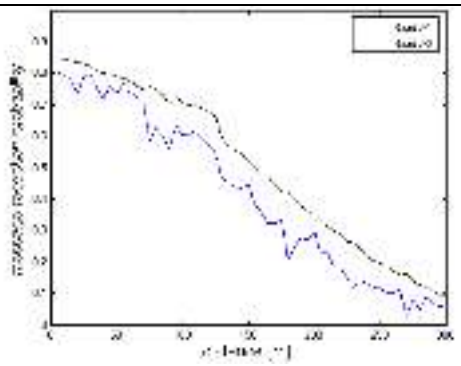
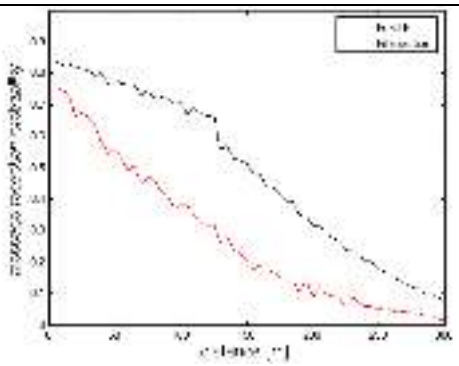
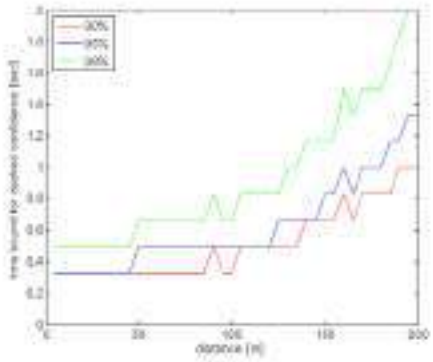
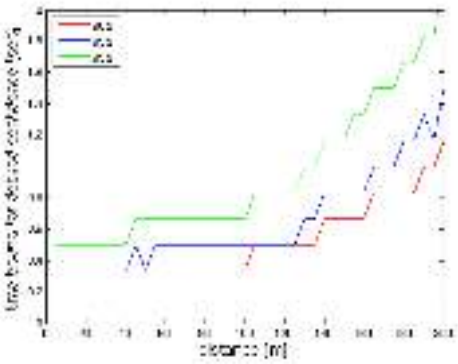


Figure 8-14: Reception Probability of Routine Messages on HWY, Scenario 11

8.1.4 Time Bound for Routine Messages

Number	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
11	Distributed	Building	RSU	200m	ON	6Hz	200m	

	Routine Messages	
	Road A	Road B
Reception probability	 **Figure 8-15: Reception Probability of Routine Messages on Road A, Scenario 11**	 **Figure 8-16: Reception Probability of Routine Messages on Road B, Scenario 11**
Time bound for needed confidence	 **Figure 8-17: Time Bound for Desired Confidence, Routine Messages - Scenario 11, Road A**	 **Figure 8-18: Time Bound for Desired Confidence, Routine Messages - Scenario 11, Road B**

8.2 Routine Messages at 7 Hz, Routine Message Size – 200 byte

Simulation Scenario Settings:

RF Model	Distributed
Emergency Message Sender	RSU, 500 bytes/ 10Hz/200m
Corner Model	Tall buildings
Commercial RSU	On, 500bytes/2Hz/200m
Routine Messages	200byte /7Hz /200m

8.2.1 Reception Probability of Emergency Messages

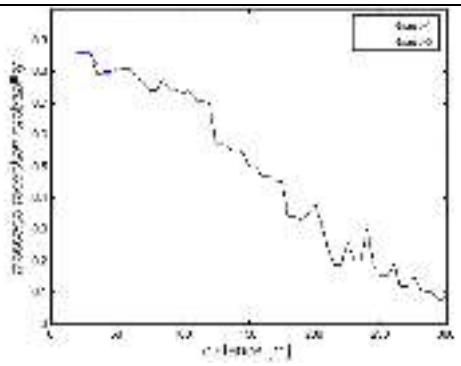


Figure 8-19: Reception Probability of Emergency Messages-Scenario 11, Road A, Sender RSU

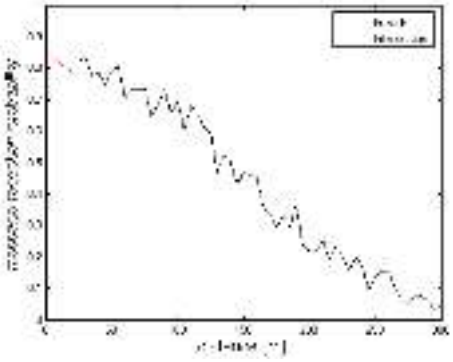


Figure 8-20: Reception Probability of Emergency Messages-Scenario 11, Road B, Sender RSU

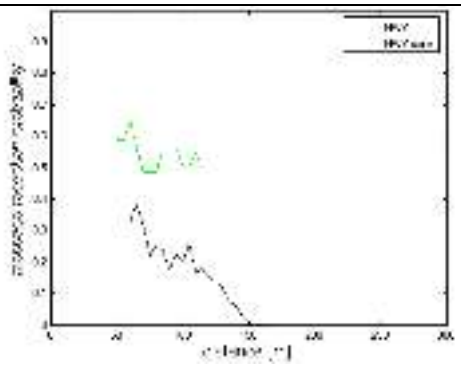


Figure 8-21: Reception Probability of Emergency Messages-Scenario 11, HWY, Sender RSU

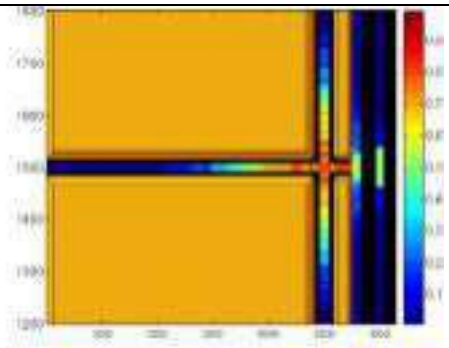
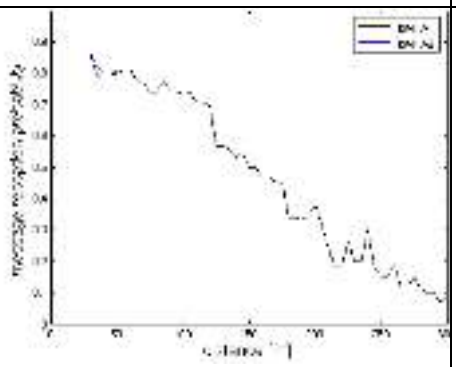
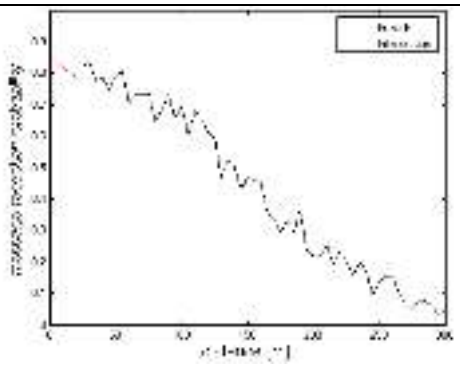
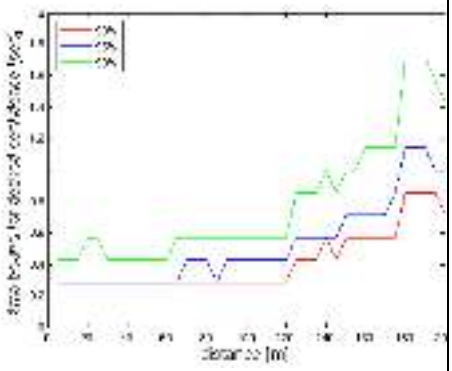
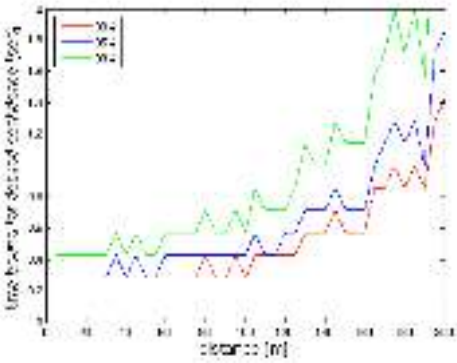


Figure 8-22: Reception Probability of Emergency Messages-Scenario 11, Sender RSU

8.2.2 Time Bound for Emergency Messages

Number.	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
11	Distributed	Building	RSU	200m	ON	7Hz	200m	

	Emergency Messages	
	Road A	Road B
Reception probability	 **Figure 8-23: Reception Probability of Emergency Messages-Scenario 11, Road A, Sender RSU**	 **Figure 8-24: Reception Probability of Emergency Messages-Scenario 11, Road B, Sender RSU**
Time bound for needed confidence	 **Figure 8-25: Time Bound for desired Confidence, Emergency Messages - Scenario 11, Road A, Sender RSU**	 **Figure 8-26: Time Bound for desired Confidence, Emergency Messages - Scenario 11, Road B, Sender RSU**

8.2.3 Reception Probability of Routine Messages

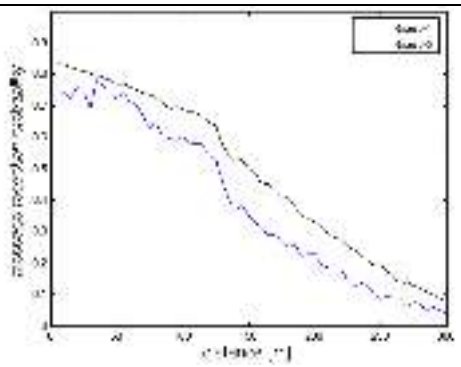


Figure 8-27: Reception Probability of Routine Messages on Road A, Scenario 11

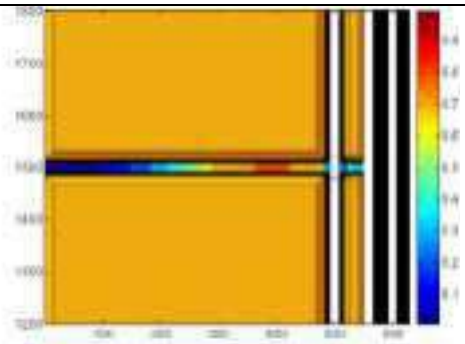


Figure 8-28: Reception Probability of Routine Messages on Road A, Scenario 11

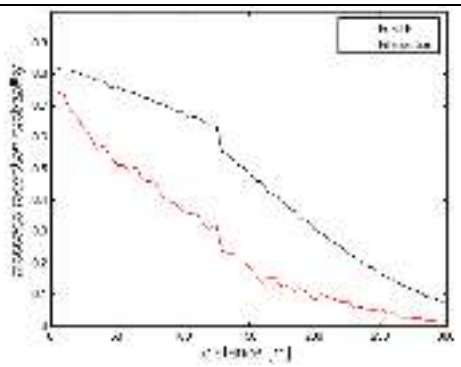


Figure 8-29: Reception Probability of Routine Messages on Road B, Scenario 11

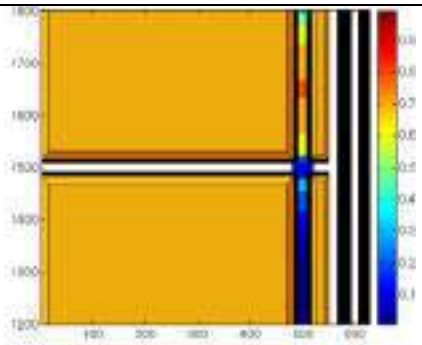


Figure 8-30: Reception Probability of Routine Messages on Road B, Scenario 11

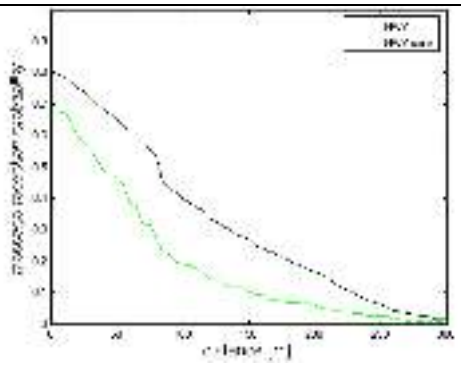


Figure 8-31: Reception Probability of Routine Messages on HWY, Scenario 11

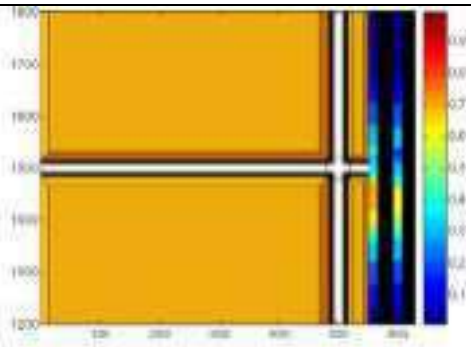
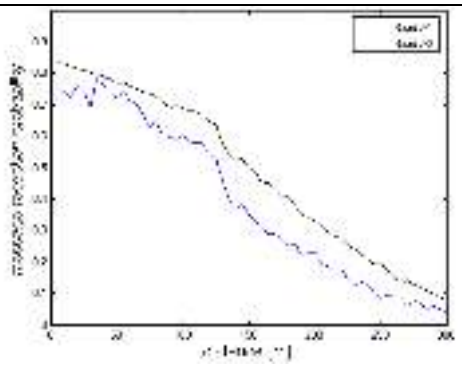
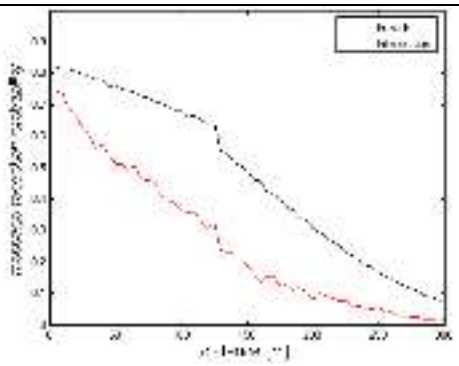
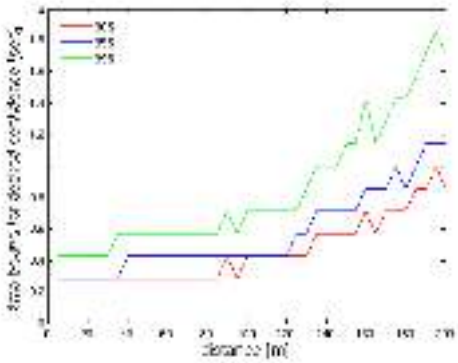
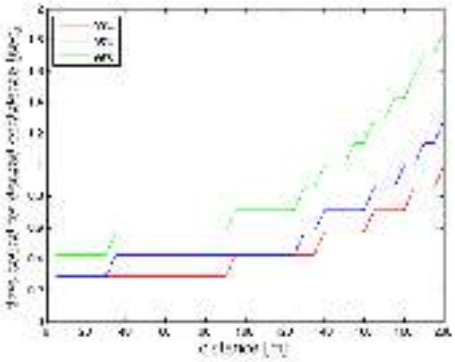


Figure 8-32: Reception Probability of Routine Messages on HWY, Scenario 11

8.2.4 Time Bound for Routine Messages

Number	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
11	Distributed	Building	RSU	200m	ON	7Hz	200m	

	Routine Messages	
	Road A	Road B
Reception probability	 **Figure 8-33: Reception Probability of Routine Messages on Road A, Scenario 11**	 **Figure 8-34: Reception Probability of Routine Messages on Road B, Scenario 11**
Time bound for needed confidence	 **Figure 8-35: Time Bound for Desired Confidence, Routine Messages – Scenario 11, Road A**	 **Figure 8-36: Time Bound for Desired Confidence, Routine Messages - Scenario 11, Road B**

8.3 Routine Messages at 8 Hz, Routine Message Size – 200 byte

Simulation Scenario Settings:

RF Model	Distributed
Emergency Message Sender	RSU, 500 bytes/ 10Hz/200m
Corner Model	Tall buildings
Commercial RSU	On, 500bytes/2Hz/200m
Routine Messages	200byte /8Hz /200m

8.3.1 Reception Probability of Emergency Messages

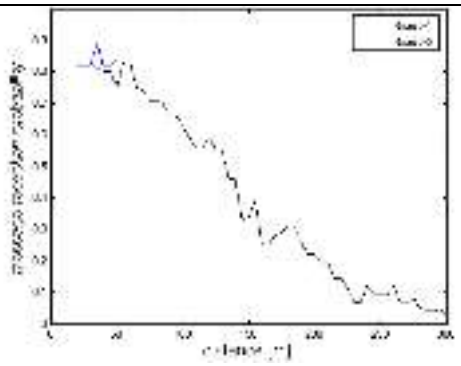


Figure 8-37: Reception Probability of Emergency Messages-Scenario 11, Road A, Sender RSU

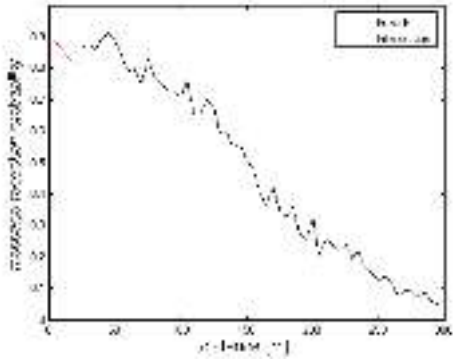


Figure 8-38: Reception Probability of Emergency Messages-Scenario 11, Road B, Sender RSU

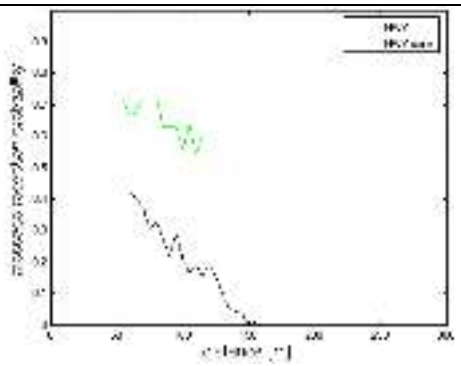


Figure 8-39: Reception Probability of Emergency Messages-Scenario 11, HWY, Sender RSU

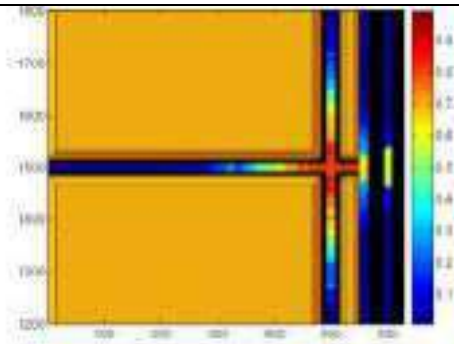
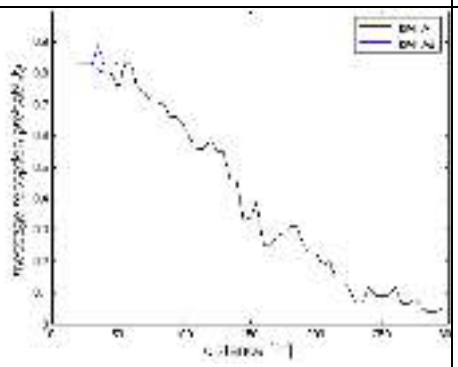
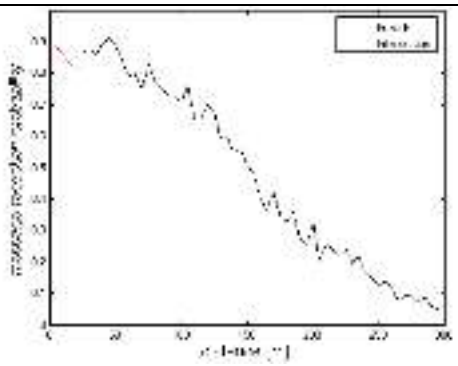
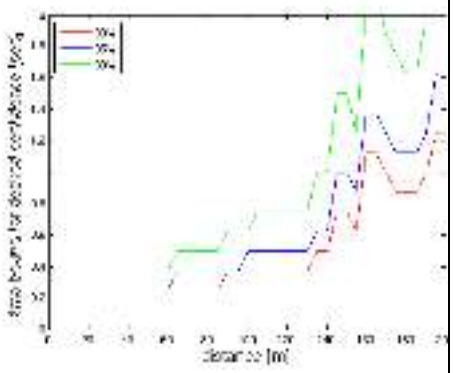
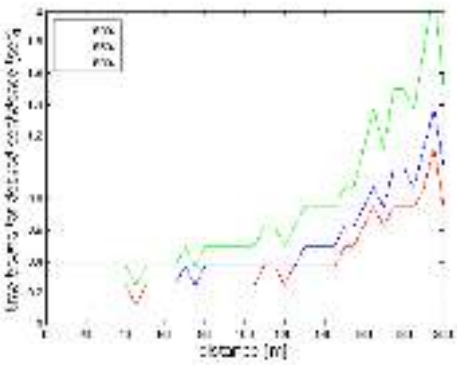


Figure 8-40: Reception Probability of Emergency Messages-Scenario 11, Sender RSU

8.3.2 Time Bound for Emergency Messages

Number	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
11	Distributed	Building	RSU	200m	ON	8Hz	200m	

	Emergency Messages	
	Road A	Road B
Reception probability	 **Figure 8-41: Reception Probability of Emergency Messages-Scenario 11, Road A, Sender RSU**	 **Figure 8-42: Reception Probability of Emergency Messages-Scenario 11, Road B, Sender RSU**
Time bound for needed confidence	 **Figure 8-43: Time Bound for Desired Confidence, Emergency Messages - Scenario 11, Road A, Sender RSU**	 **Figure 8-44: Time Bound for Desired Confidence, Emergency Messages - Scenario 11, Road B, Sender RSU**

8.3.3 Reception Probability of Routine Messages

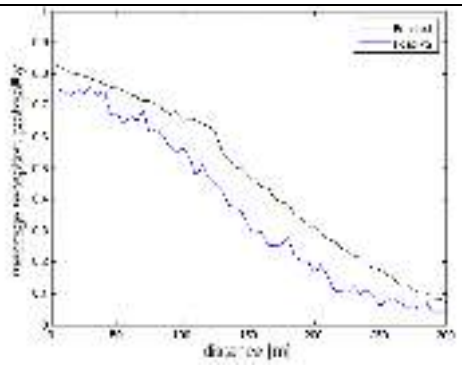


Figure 8-45: Reception Probability of Routine Messages on Road A, Scenario 11

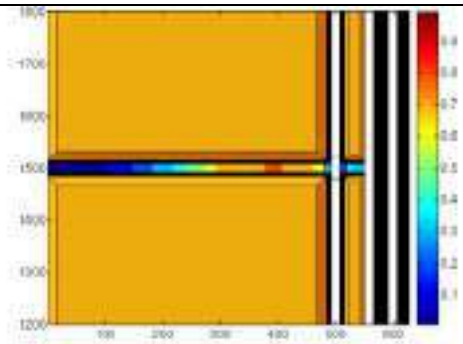


Figure 8-46: Reception Probability of Routine Messages on Road A, Scenario 11

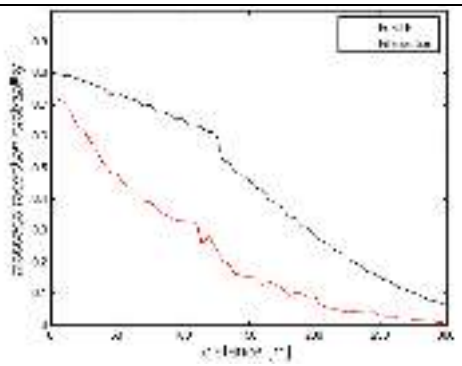


Figure 8-47: Reception Probability of Routine Messages on Road B, Scenario 11

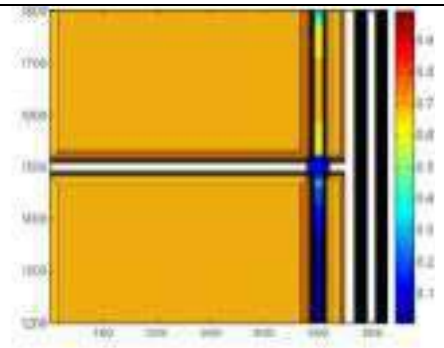


Figure 8-48: Reception Probability of Routine Messages on Road B, Scenario 11

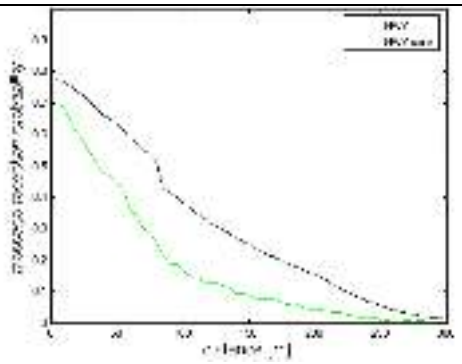


Figure 8-49: Reception Probability of Routine Messages on HWY, Scenario 11

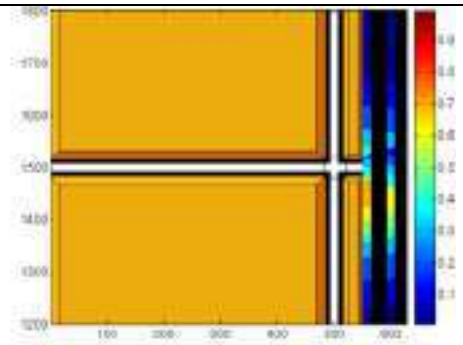
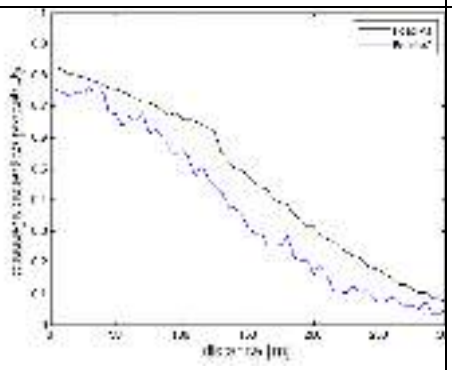
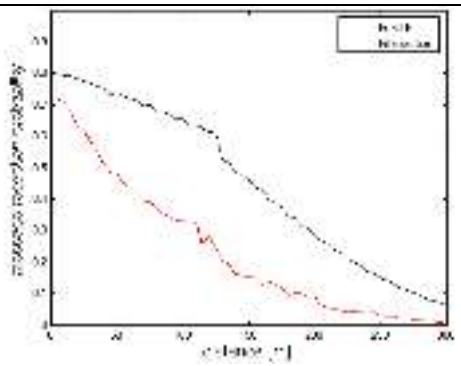
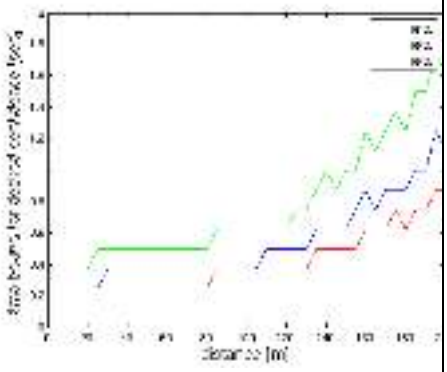
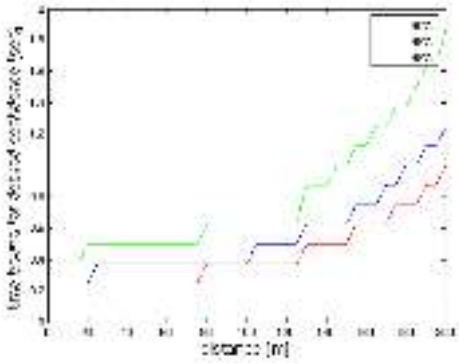


Figure 8-50: Reception Probability of Routine Messages on HWY, Scenario 11

8.3.4 Time Bound for Routine Messages

Number	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
11	Distributed	Building	RSU	200m	ON	8Hz	200m	

	Routine Messages	
	Road A	Road B
Reception probability	 **Figure 8-51: Reception Probability of Routine Messages on Road A, Scenario 11**	 **Figure 8-52: Reception Probability of Routine Messages on Road B, Scenario 11**
Time bound for needed confidence	 **Figure 8-53: Time Bound for Desired Confidence, Routine Messages - Scenario 11, Road A**	 **Figure 8-54: Time Bound for Desired Confidence, Routine Messages - Scenario 11, Road B**

8.4 Routine Messages at 9 Hz, Routine Message Size – 200 byte

Simulation Scenario Settings:

RF Model	Distributed
Emergency Message Sender	RSU, 500 bytes/ 10Hz/200m
Corner Model	Tall buildings
Commercial RSU	On, 500bytes/2Hz/200m
Routine Messages	200byte /9Hz /200m

8.4.1 Reception Probability of Emergency Messages

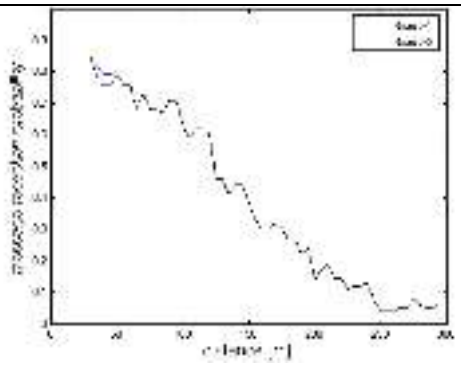


Figure 8-55: Reception Probability of Emergency Messages-Scenario 11, Road A, Sender RSU

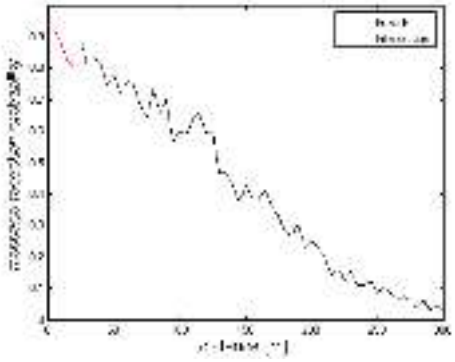


Figure 8-56: Reception Probability of Emergency Messages-Scenario 11, Road B, Sender RSU

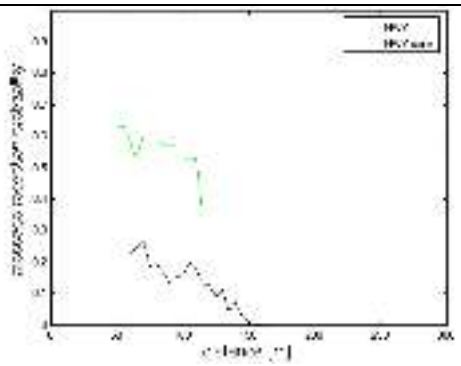


Figure 8-57: Reception Probability of Emergency Messages-Scenario 11, HWY, Sender RSU

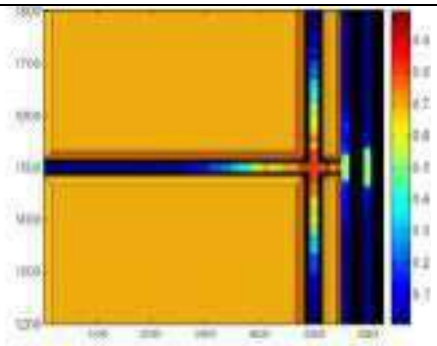
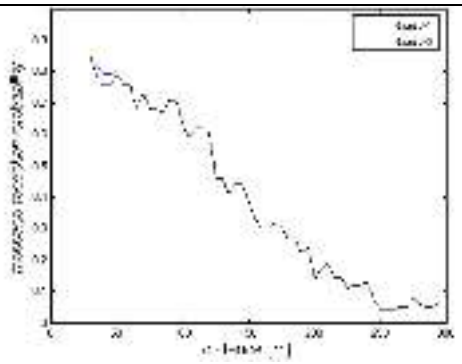
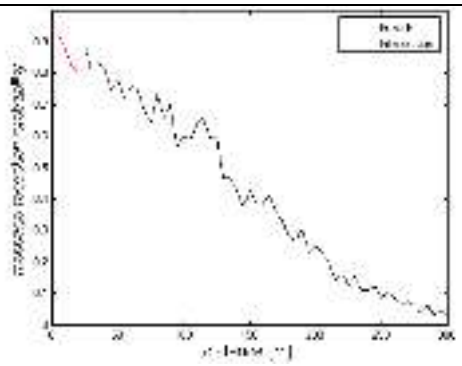
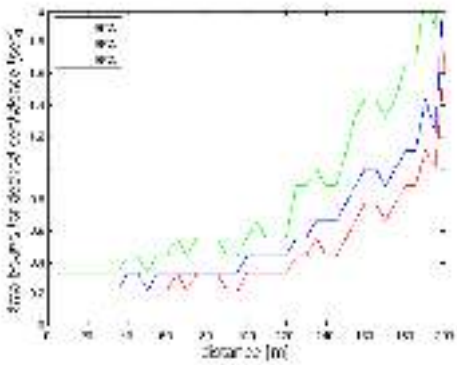
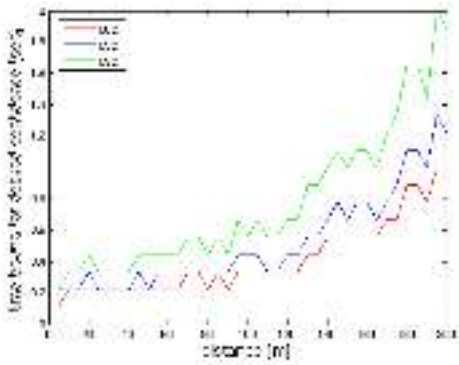


Figure 8-58: Reception Probability of Emergency Messages-Scenario11, Sender RSU

8.4.2 Time Bound for Emergency Messages

Number.	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
11	Distributed	Building	RSU	200m	ON	9Hz	200m	

	Emergency Messages	
	Road A	Road B
Reception probability	 **Figure 8-59: Reception Probability of Emergency Messages-Scenario 11, Road A, Sender RSU**	 **Figure 8-60: Reception Probability of Emergency Messages-Scenario 11, Road B, Sender RSU**
Time bound for needed confidence	 **Figure 8-61: Time Bound for Desired Confidence, Emergency Messages - Scenario 11, Road A, Sender RSU**	 **Figure 8-62: Time Bound for Desired Confidence, Emergency Messages – Scenario 11, Road B, Sender RSU**

8.4.3 Reception Probability of Routine Messages

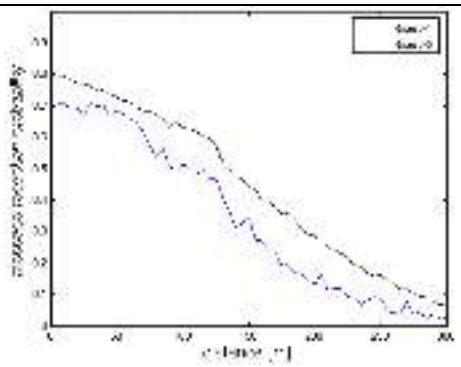


Figure 8-63: Reception Probability of Routine Messages on Road A, Scenario 11

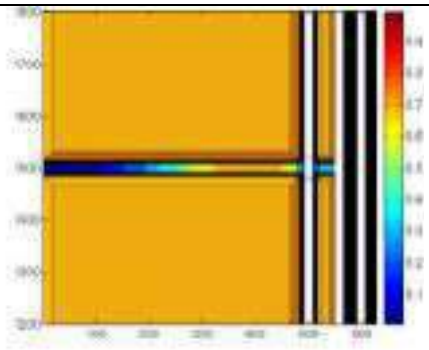


Figure 8-64: Reception Probability of Routine Messages on Road A, Scenario 11

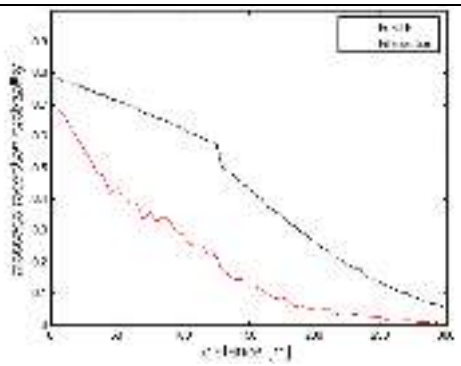


Figure 8-65: Reception Probability of Routine Messages on Road B, Scenario 11

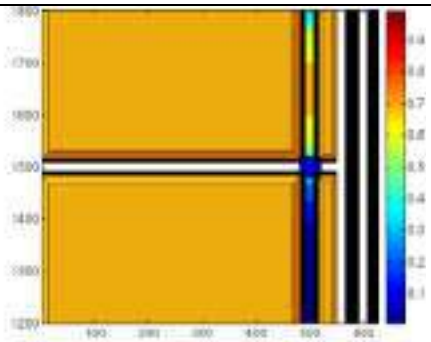


Figure 8-66: Reception Probability of Routine Messages on Road B, Scenario 11

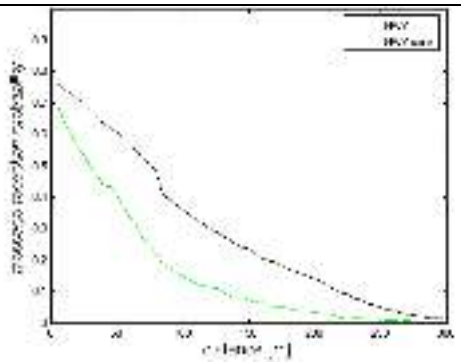


Figure 8-67: Reception Probability of Routine Messages on HWY, Scenario 11

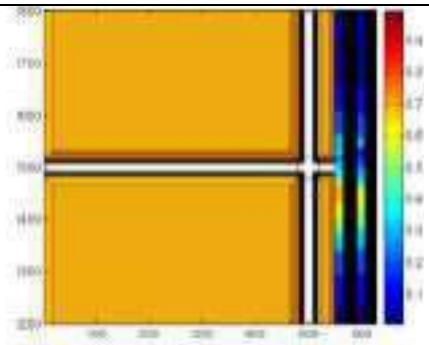
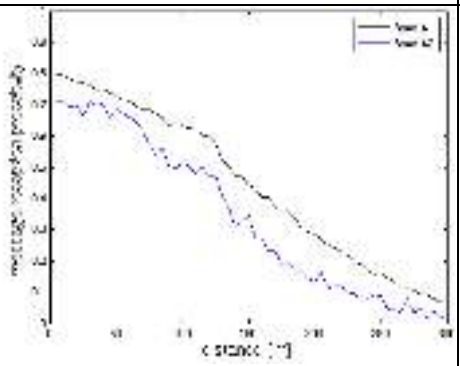
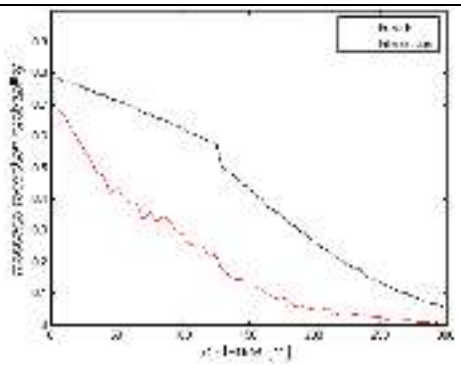
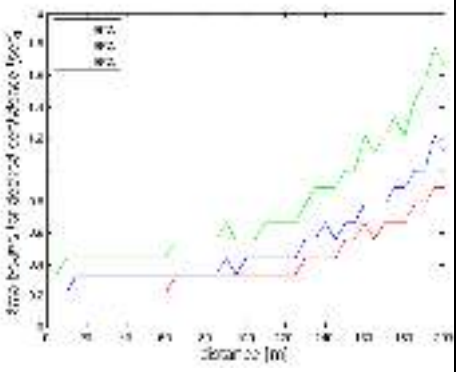
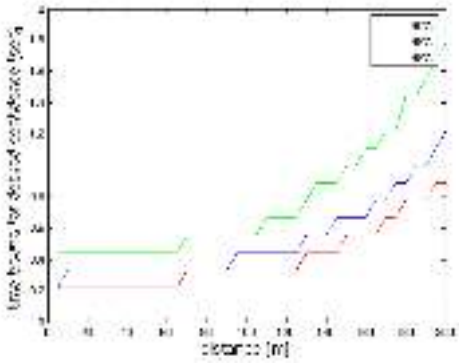


Figure 8-68: Reception Probability of Routine Messages on HWY, Scenario 11

8.4.4 Time Bound for Routine Messages

Number	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
11	Distributed	Building	RSU	200m	ON	9Hz	200m	

	Routine Messages	
	Road A	Road B
Reception probability	 **Figure 8-69: Reception Probability of Routine Messages on Road A, Scenario 11**	 **Figure 8-70: Reception Probability of Routine Messages on Road B, Scenario 11**
Time bound for needed confidence	 **Figure 8-71: Time Bound for Desired Confidence, Routine Messages - Scenario 11, Road A**	 **Figure 8-72: Time Bound for Desired Confidence, Routine Messages - Scenario 11, Road B**

8.5 Routine Messages at 5 Hz, Routine Message Size – 250 byte

Simulation Scenario Settings:

RF Model	Distributed
Emergency Message Sender	RSU, 500 bytes/ 10Hz/200m
Corner Model	Tall buildings
Commercial RSU	On, 500bytes/2Hz/200m
Routine Messages	250byte /5Hz /200m

8.5.1 Reception Probability of Emergency Messages

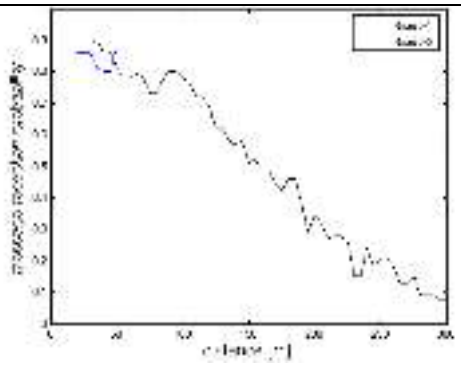


Figure 8-73: Reception Probability of Emergency Messages-Scenario 11, Road A, Sender RSU

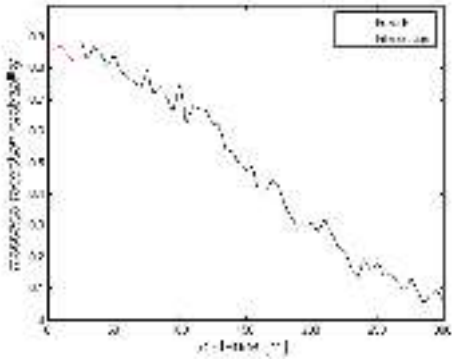


Figure 8-74: Reception Probability of Emergency Messages-Scenario 11, Road B, Sender RSU

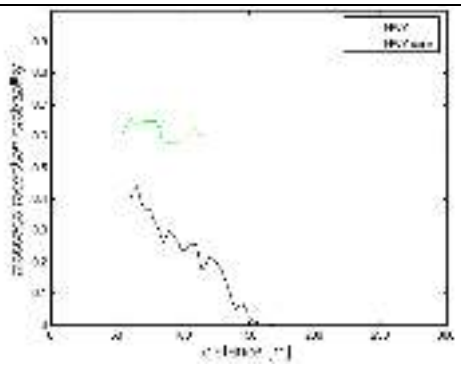


Figure 8-75: Reception Probability of Emergency Messages-Scenario 11, HWY, Sender RSU

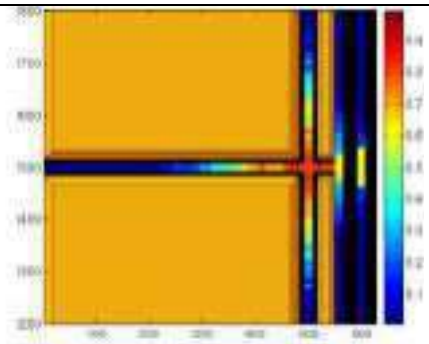
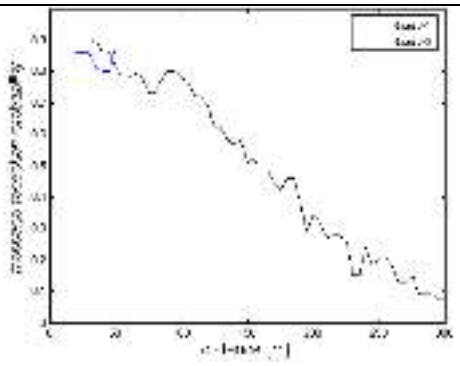
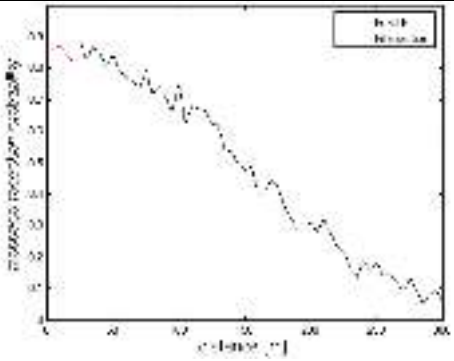
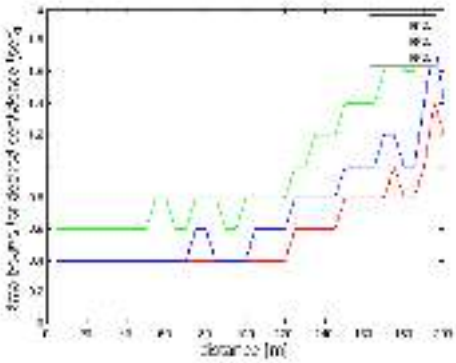
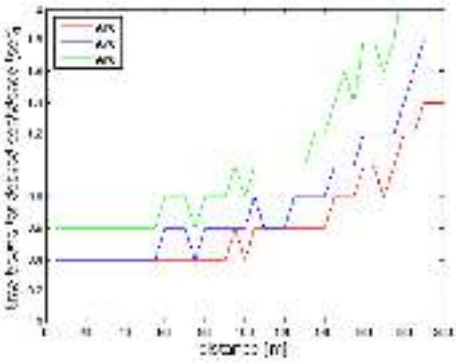


Figure 8-76: Reception Probability of Emergency Messages-Scenario11, Sender RSU

8.5.2 Time Bound for Emergency Messages

Number	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
11	Distributed	Building	RSU	200m	ON	5Hz, 250 byte	200m	

	Emergency Messages	
	Road A	Road B
Reception probability	 **Figure 8-77: Reception Probability of Emergency Messages-Scenario 11, Road A, Sender RSU**	 **Figure 8-78: Reception Probability of Emergency Messages-Scenario 11, Road B, Sender RSU**
Time bound for needed confidence	 **Figure 8-79: Time Bound for Desired Confidence, Emergency Messages - Scenario 11, Road A, Sender RSU**	 **Figure 8-80: Time Bound for Desired Confidence, Emergency Messages - Scenario 11, Road B, Sender RSU**

8.5.3 Reception Probability of Routine Messages

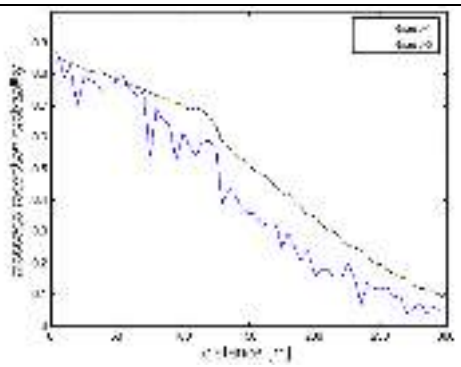


Figure 8-81: Reception Probability of Routine Messages on Road A, Scenario 11

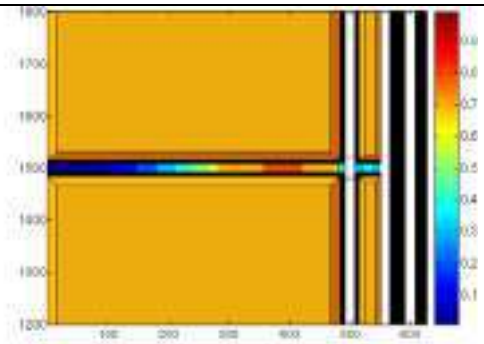


Figure 8-82: Reception Probability of Routine Messages on Road A, Scenario 11

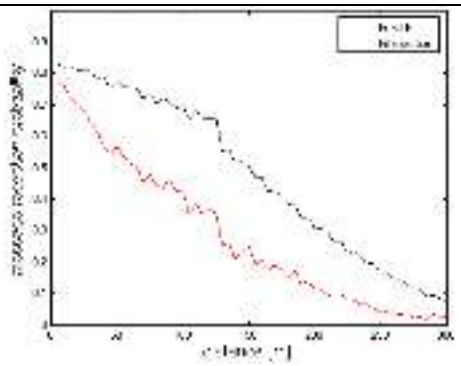


Figure 8-83: Reception Probability of Routine Messages on Road B, Scenario 11

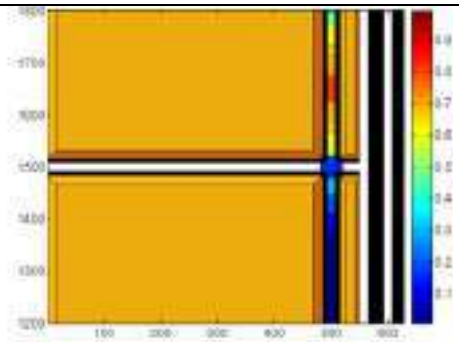


Figure 8-84: Reception Probability of Routine Messages on Road B, Scenario 11

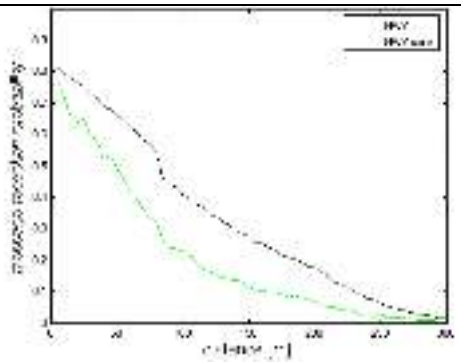


Figure 8-85: Reception Probability of Routine Messages on HWY, Scenario 11

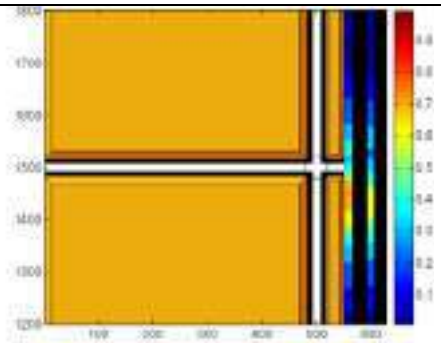
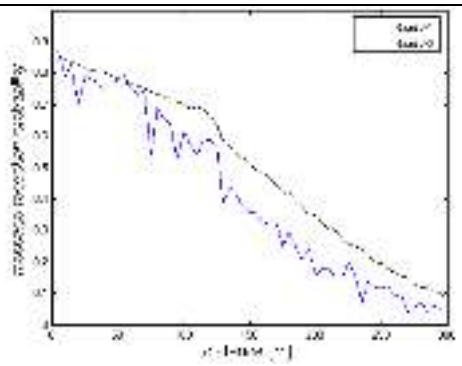
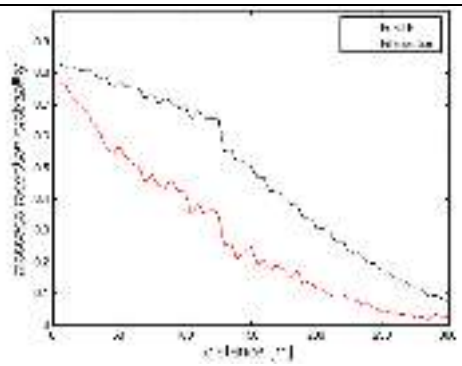
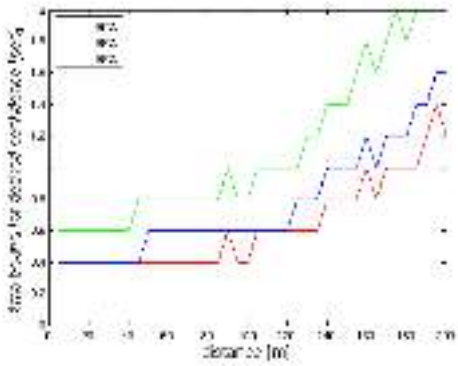
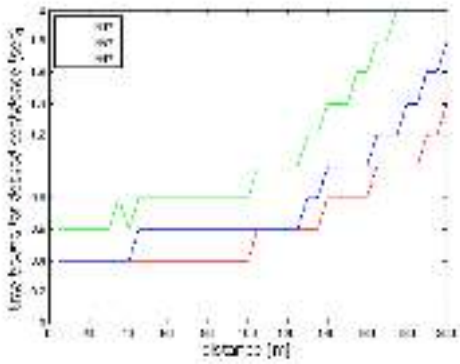


Figure 8-86: Reception Probability of Routine Messages on HWY, Scenario 11

8.5.4 Time Bound for Routine Messages

Number	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
11	Distributed	Building	RSU	200m	ON	5Hz, 250 byte	200m	

	Routine Messages	
	Road A	Road B
Reception probability	 **Figure 8-87: Reception Probability of Routine Messages on Road A, Scenario 11**	 **Figure 8-88: Reception Probability of Routine Messages on Road B, Scenario 11**
Time bound for needed confidence	 **Figure 8-89: Time Bound for Desired Confidence, Routine Messages - Scenario 11, Road A**	 **Figure 8-90: Time Bound for Desired Confidence, Routine Messages - Scenario 11, Road B**

8.6 Routine Messages at 10 Hz, Routine Message Size – 250 byte

Simulation Scenario Settings:

RF Model	Distributed
Emergency Message Sender	RSU, 500 bytes/ 10Hz/200m
Corner Model	Tall buildings
Commercial RSU	On, 500bytes/2Hz/200m
Routine Messages	250byte /10Hz /200m

8.6.1 Reception Probability of Emergency Messages

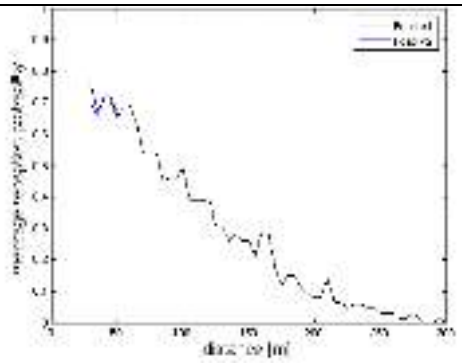


Figure 8-91: Reception Probability of Emergency Messages-Scenario 11, Road A, Sender RSU

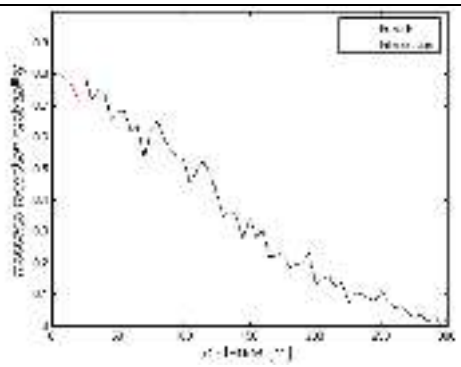


Figure 8-92: Reception Probability of Emergency Messages-Scenario 11, Road B, Sender RSU

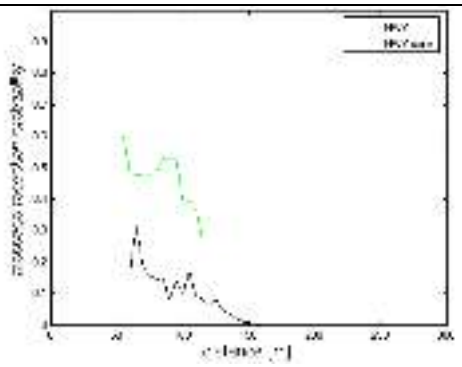


Figure 8-93: Reception Probability of Emergency Messages-Scenario 11, HWY, Sender RSU

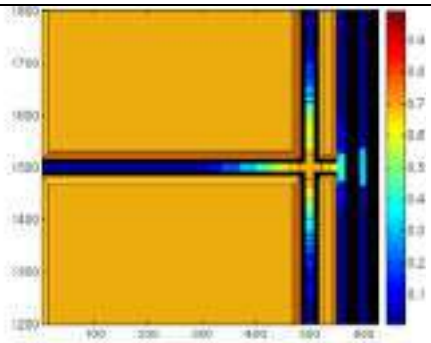
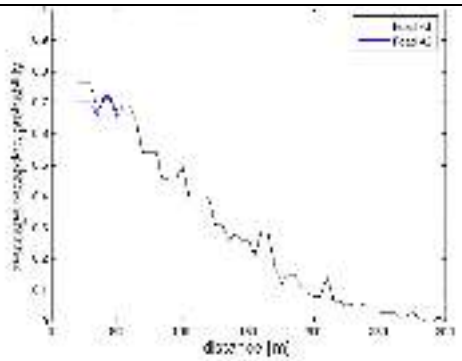
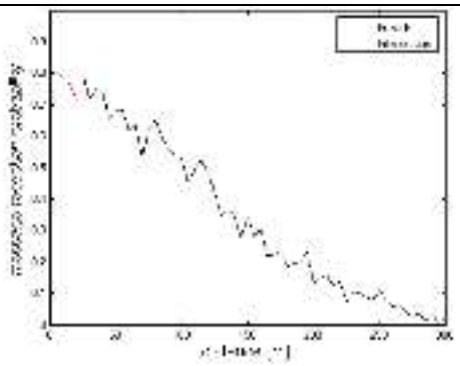
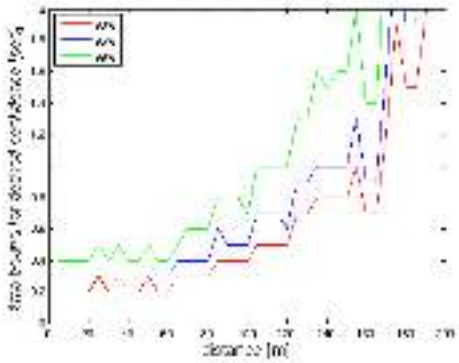
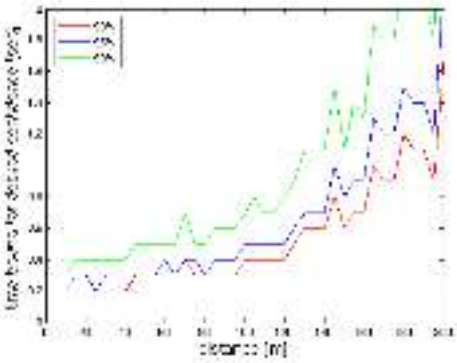


Figure 8-94: Reception Probability of Emergency Messages-Scenario 11, Sender RSU

8.6.2 Time Bound for Emergency Messages

Number	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
11	Distributed	Building	RSU	200m	ON	10Hz, 250 byte	200m	

	Emergency Messages	
	Road A	Road B
Reception probability	 **Figure 8-95: Reception Probability of Emergency Messages-Scenario 11, Road A, Sender RSU**	 **Figure 8-96: Reception Probability of Emergency Messages-Scenario 11, Road B, Sender RSU**
Time bound for needed confidence	 **Figure 8-97: Time Bound for Desired Confidence, Emergency Messages - Scenario 11, Road A, Sender RSU**	 **Figure 8-98: Time Bound for Desired Confidence, Emergency Messages - Scenario 11, Road B, Sender RSU**

8.6.3 Reception Probability of Routine Messages

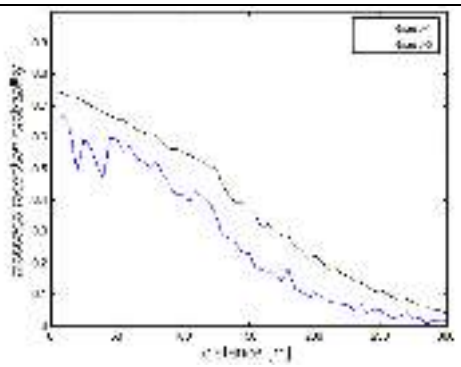


Figure 8-99: Reception Probability of Routine Messages on Road A, Scenario 11

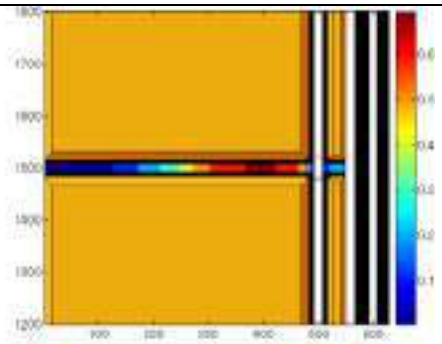


Figure 8-100: Reception Probability of Routine Messages on Road A, Scenario 11

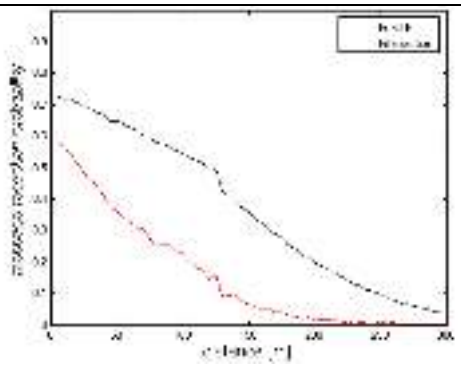


Figure 8-101: Reception Probability of Routine Messages on Road B, Scenario 11

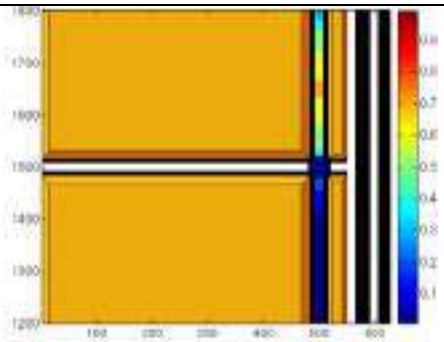


Figure 8-102: Reception Probability of Routine Messages on Road B, Scenario 11

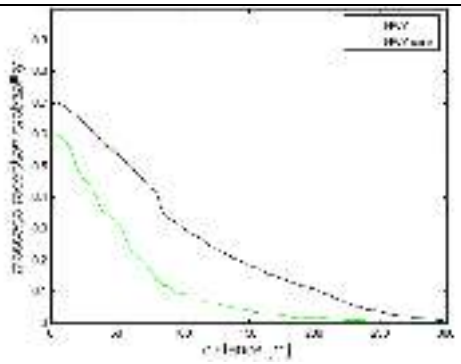


Figure 8-103: Reception Probability of Routine Messages on HWY, Scenario 11

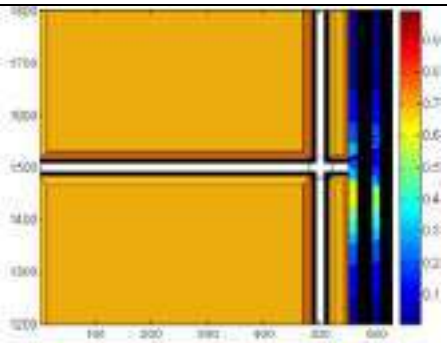
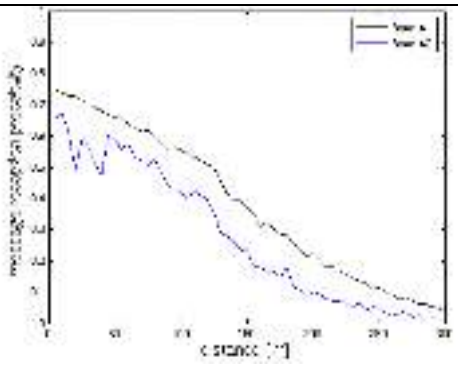
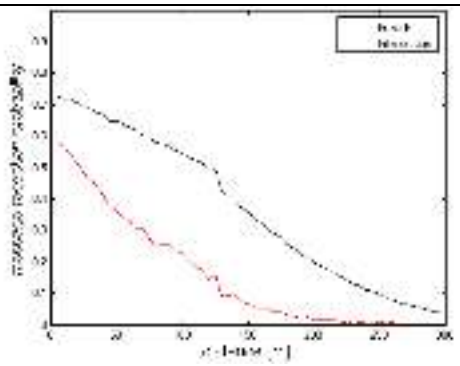
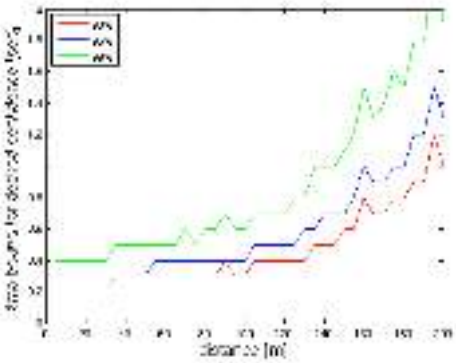
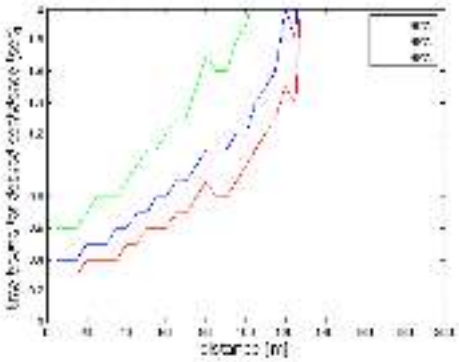


Figure 8-104: Reception Probability of Routine Messages on HWY, Scenario 11

8.6.4 Time Bound for Routine Messages

Number.	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
11	Distributed	Building	RSU	200m	ON	10Hz, 250 byte	200m	

	Routine Messages	
	Road A	Road B
Reception probability	 **Figure 8-105: Reception Probability of Routine Messages on Road A, Scenario 11**	 **Figure 8-106: Reception Probability of Routine Messages on Road B, Scenario 11**
Time bound for needed confidence	 **Figure 8-107: Time Bound for Desired Confidence, Routine Messages - Scenario 11, Road A**	 **Figure 8-108: Time Bound for Desired Confidence, Routine Messages - Scenario 11, Road B**

8.7 Routine Messages at 5 Hz, Routine Message Size – 300 byte

Simulation Scenario Settings:

RF Model	Distributed
Emergency Message Sender	RSU, 500 bytes/ 10Hz/200m
Corner Model	Tall buildings
Commercial RSU	On, 500 bytes/2Hz/200m
Routine Messages	300 byte /5Hz /200m

8.7.1 Reception Probability of Emergency Messages

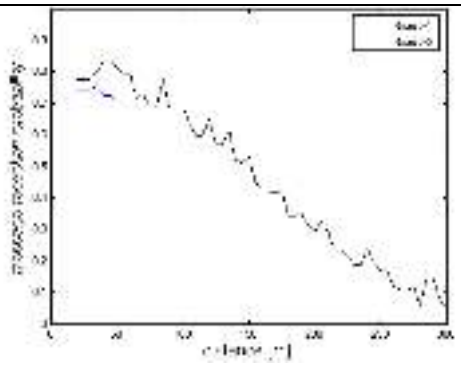


Figure 8-109: Reception Probability of Emergency Messages-Scenario 11, Road A, Sender RSU

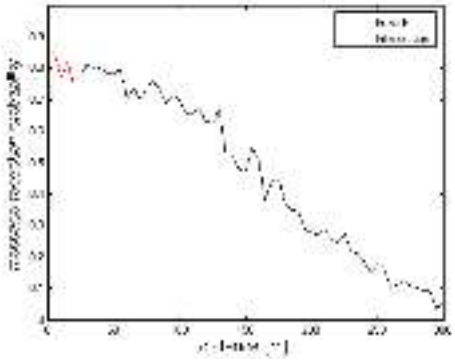


Figure 8-110: Reception Probability of Emergency Messages-Scenario 11, Road B, Sender RSU

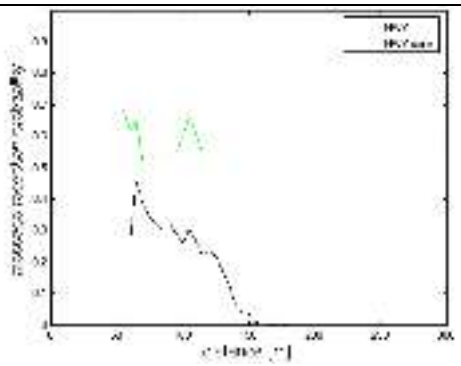


Figure 8-111: Reception Probability of Emergency Messages-Scenario 11, HWY, Sender RSU

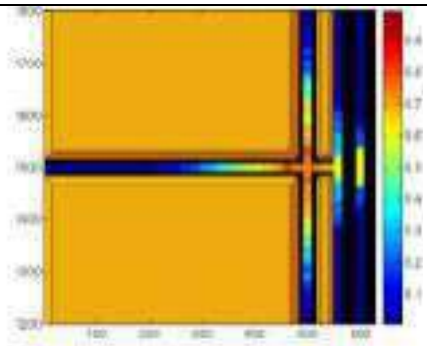
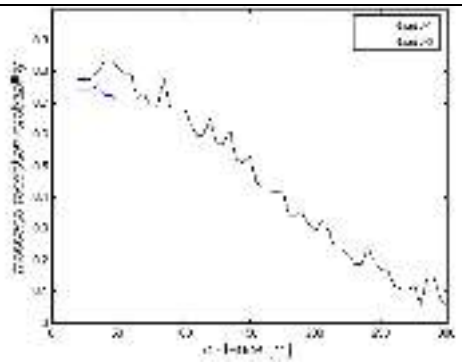
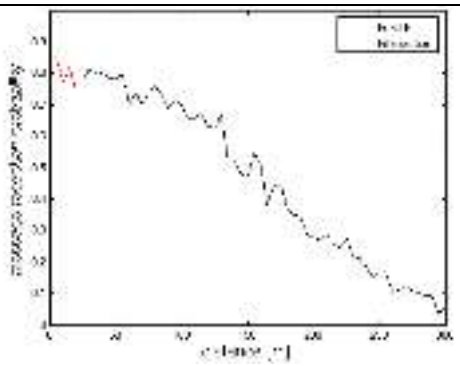
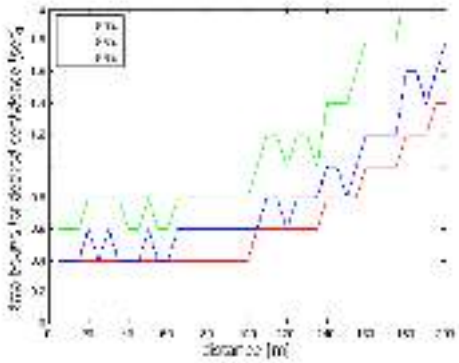
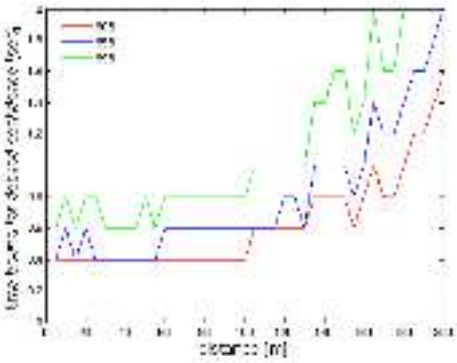


Figure 8-112: Reception Probability of Emergency Messages-Scenario 11, Sender RSU

8.7.2 Time Bound for Emergency Messages

Number.	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
11	Distributed	Building	RSU	200m	ON	5Hz, 300 byte	200m	

	Emergency Messages	
	Road A	Road B
Reception probability	 **Figure 8-113: Reception Probability of Emergency Messages-Scenario 11, Road A, Sender RSU**	 **Figure 8-114: Reception Probability of Emergency Messages-Scenario 11, Road B, Sender RSU**
Time bound for needed confidence	 **Figure 8-115: Time Bound for Desired Confidence, Emergency Messages - Scenario 11, Road A, Sender RSU**	 **Figure 8-116: Time Bound for Desired Confidence, Emergency Messages – Scenario 11, Road B, Sender RSU**

8.7.3 Reception Probability of Routine Messages

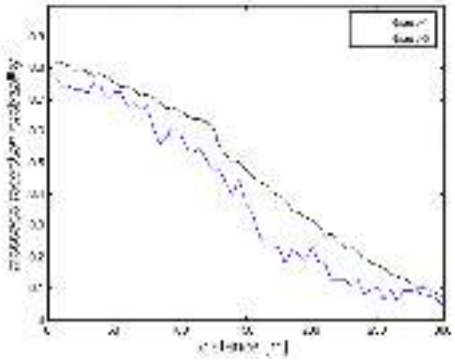


Figure 8-117: Reception Probability of Routine Messages on Road A, Scenario 11

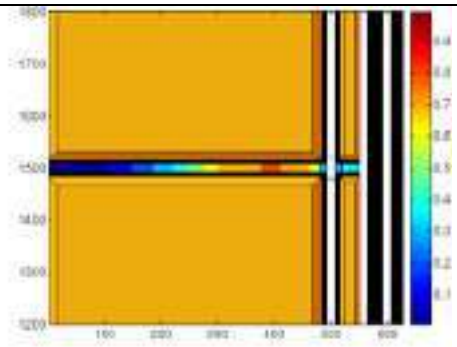


Figure 8-118: Reception Probability of Routine Messages on Road A, Scenario 11

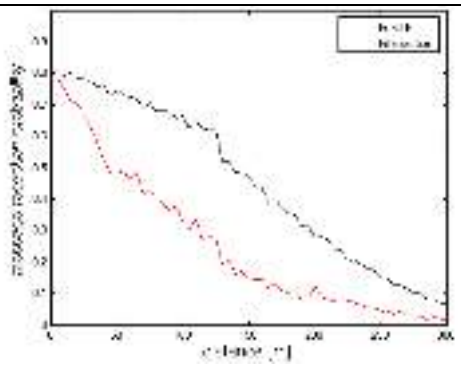


Figure 8-119: Reception Probability of Routine Messages on Road B, Scenario 11

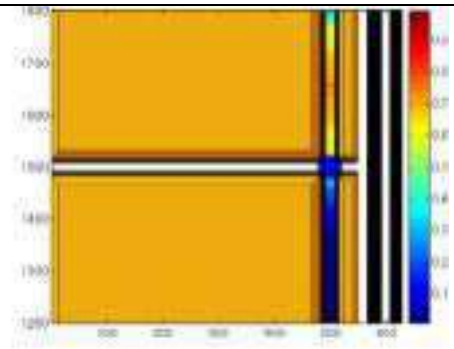


Figure 8-120: Reception Probability of Routine Messages on Road B, Scenario 11

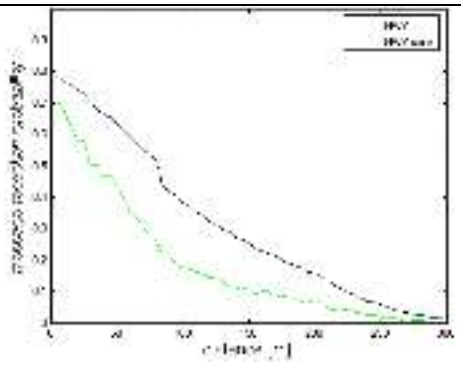


Figure 8-121: Reception Probability of Routine Messages on HWY, Scenario 11

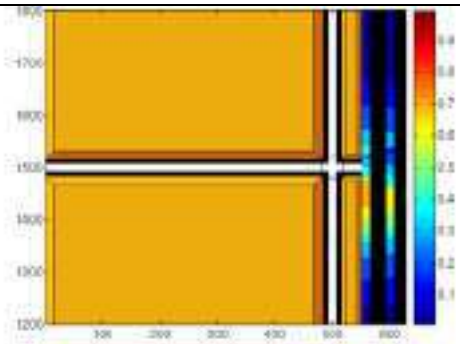
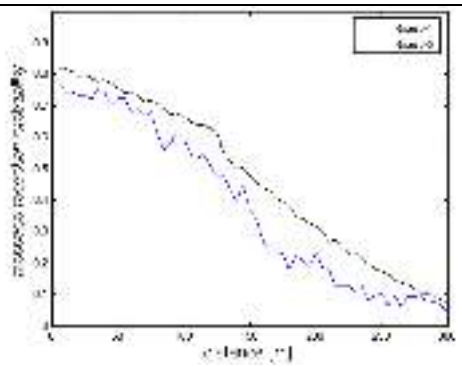
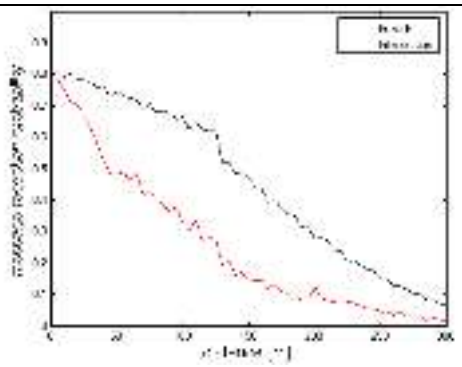
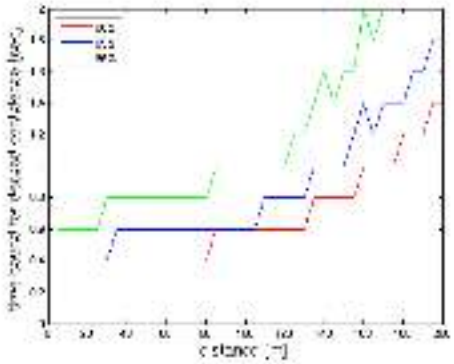
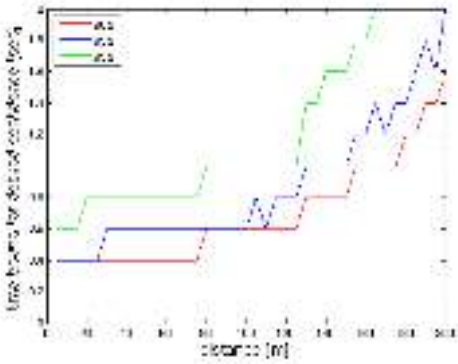


Figure 8-122: Reception Probability of Routine Messages on HWY, Scenario 11

8.7.4 Time Bound for Routine Messages

Number.	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
11	Distributed	Building	RSU	200m	ON	5Hz, 300 byte	200m	

	Routine Messages	
	Road A	Road B
Reception probability	 **Figure 8-123: Reception Probability of Routine Messages on Road A, Scenario 11**	 **Figure 8-124: Reception Probability of Routine Messages on Road B, Scenario 11**
Time bound for needed confidence	 **Figure 8-125: Time Bound for desired Confidence, Routine Messages – Scenario 11, Road A**	 **Figure 8-126: Time Bound for desired Confidence, Routine Messages - Scenario 11, Road B**

8.8 Routine Messages at 10 Hz, Routine Message Size – 300 byte

Simulation Scenario Settings:

RF Model	Distributed
Emergency Message Sender	RSU, 500 bytes/ 10Hz/200m
Corner Model	Tall buildings
Commercial RSU	On, 500bytes/2Hz/200m
Routine Messages	300byte /10Hz /200m

8.8.1 Reception Probability of Emergency Messages

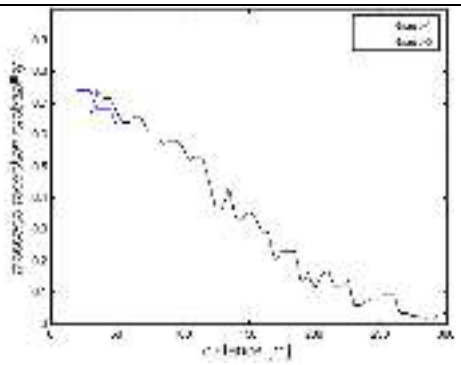


Figure 8-127: Reception Probability of Emergency Messages-Scenario 11, Road A, Sender RSU

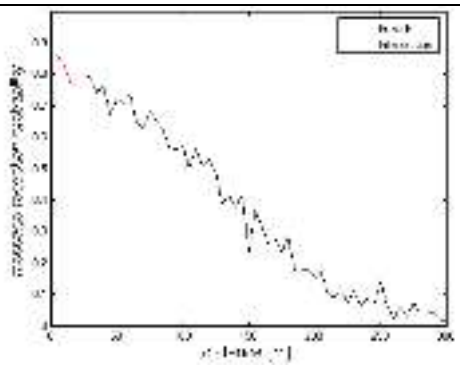


Figure 8-128: Reception Probability of Emergency Messages-Scenario 11, Road B, Sender RSU

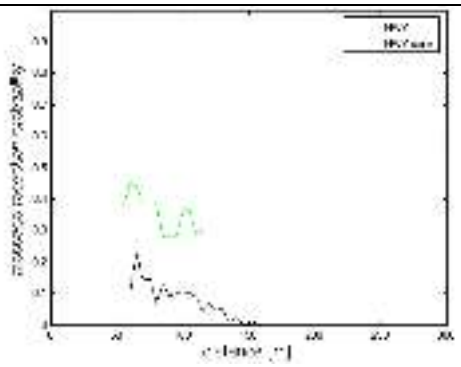


Figure 8-129: Reception Probability of Emergency Messages-Scenario 11, HWY, Sender RSU

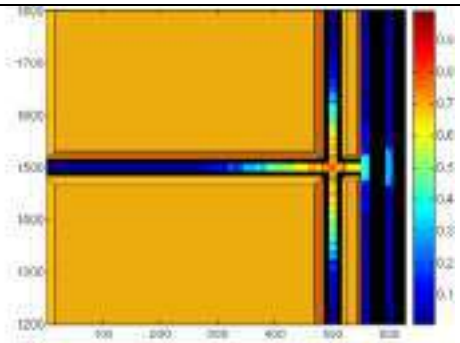
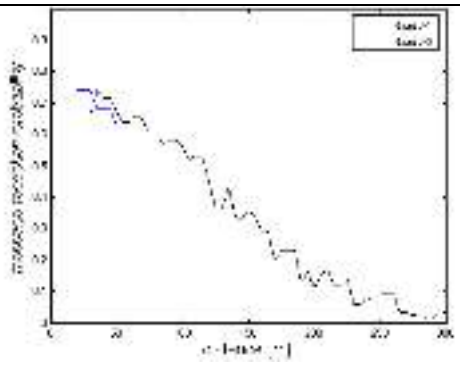
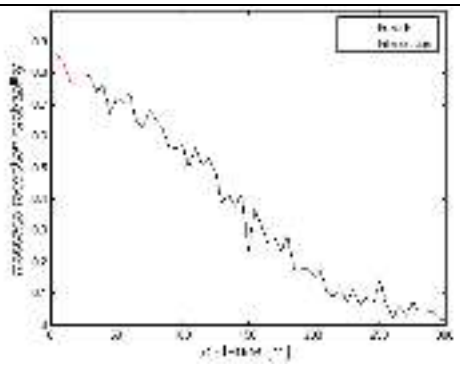
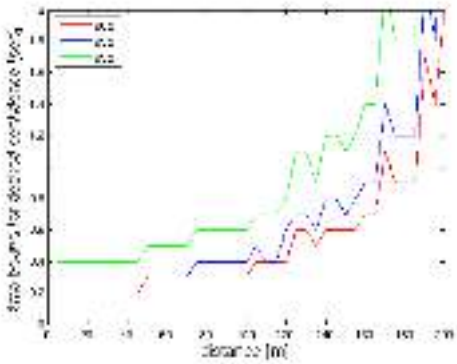
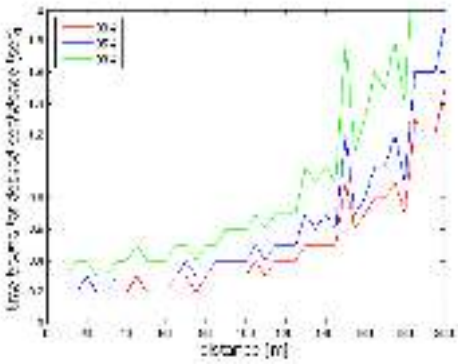


Figure 8-130: Reception Probability of Emergency Messages-Scenario 11, Sender RSU

8.8.2 Time Bound for Emergency Messages

Number.	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
11	Distributed	Building	RSU	200m	ON	10Hz, 300 byte	200m	

	Emergency Messages	
	Road A	Road B
Reception probability	 **Figure 8-131: Reception Probability of Emergency Messages-Scenario 11, Road A, Sender RSU**	 **Figure 8-132: Reception Probability of Emergency Messages-Scenario 11, Road B, Sender RSU**
Time bound for needed confidence	 **Figure 8-133: Time Bound for Desired Confidence, Emergency Messages - Scenario 11, Road A, Sender RSU**	 **Figure 8-134: Time Bound for Desired Confidence, Emergency Messages - Scenario 11, Road B, Sender RSU**

8.8.3 Reception Probability of Routine Messages

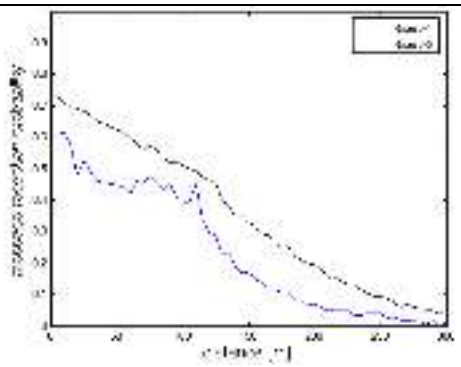


Figure 8-135: Reception Probability of Routine Messages on Road A, Scenario 11

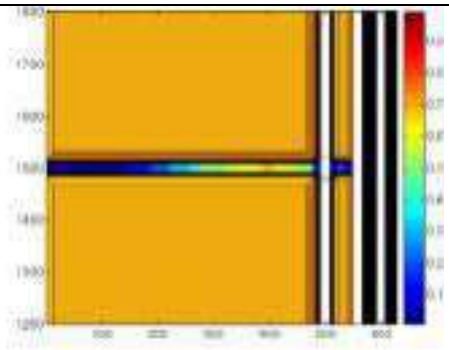


Figure 8-136: Reception Probability of Routine Messages on Road A, Scenario 11

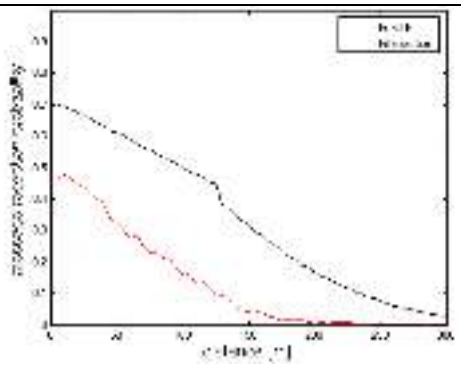


Figure 8-137: Reception Probability of Routine Messages on Road B, Scenario 11

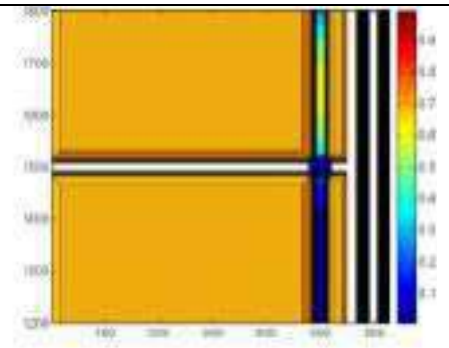


Figure 8-138: Reception Probability of Routine Messages on Road B, Scenario 11

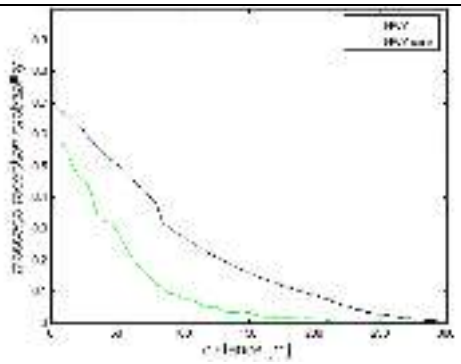


Figure 8-139: Reception Probability of Routine Messages on HWY, Scenario 11

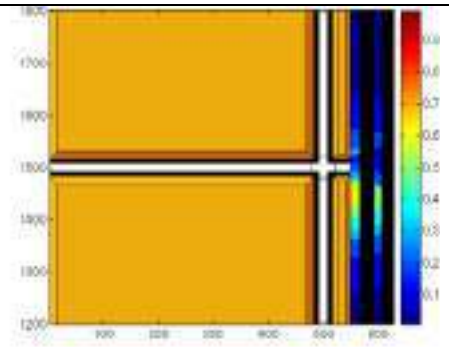
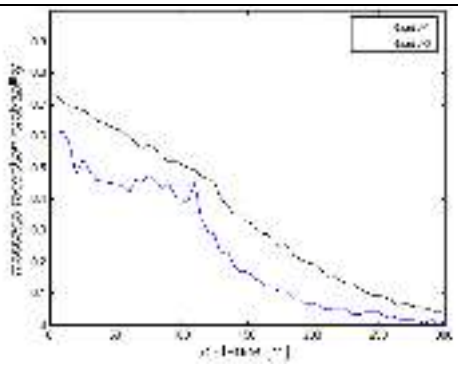
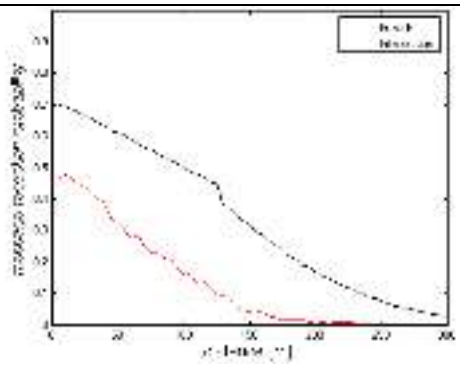
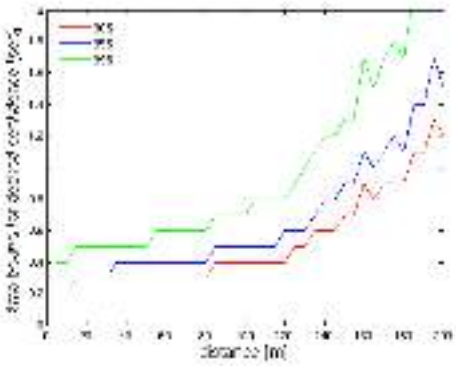
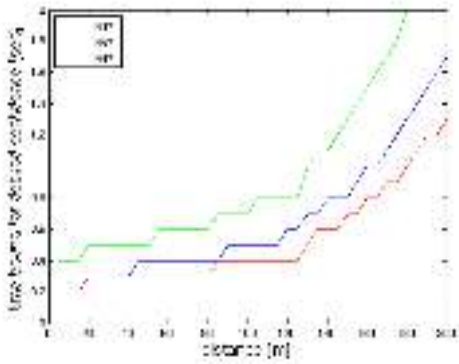


Figure 8-140: Reception Probability of Routine Messages on HWY, Scenario 11

8.8.4 Time Bound for Routine Messages

Number .	RF Model	Corner Model	Emergency Message Sender	Emergency Message Range	Commercial RSU	Routine Safety Message Frequency	Routine Safety Message Range	Emergency Message Cascading Protocol
11	Distributed	Building	RSU	200m	ON	10Hz, 300 byte	200m	

	Routine Messages	
	Road A	Road B
Reception probability	 **Figure 8-141: Reception Probability of Routine Messages on Road A, Scenario 11**	 **Figure 8-142: Reception Probability of Routine Messages on Road B, Scenario 11**
Time bound for needed confidence	 **Figure 8-143: Time Bound for Desired Confidence, Routine Messages - Scenario 11, Road A**	 **Figure 8-144: Time Bound for Desired Confidence, Routine Messages - Scenario 11, Road B**

Appendix J:
WAVE/DSRC Standards

TABLE OF CONTENTS

1 BACKGROUND 1-1

2 DSRC STANDARDS PROGRESS 2-1

2.1 DSRC STANDARDS ROADMAP 2-1
2.2 ISO/OSI REFERENCE MODEL 2-3
2.3 FCC RULEMAKING 2-4
2.4 ASTM E2213 LOWER LAYER DSRC STANDARD 2-5
2.5 IEEE 802.11P LOWER LAYER WAVE STANDARD 2-6
2.6 IEEE P1609 UPPER LAYER WAVE STANDARDS 2-7
2.7 IEEE P1556 SECURITY STANDARD 2-7
2.8 SAE DSRC TECHNICAL COMMITTEE DEVELOPMENTS 2-8
2.9 POTENTIAL SAE RECOMMENDED PRACTICES FOR DSRC VEHICLE SAFETY APPLICATIONS 2-9

3 INCORPORATION OF VSCC POSITIONS INTO DSRC/WAVE STANDARDS 3-11

3.1 BROADCAST-TYPE MESSAGES 3-11
3.2 RANDOM MAC ADDRESSES 3-12
3.3 SHORT HEADER FOR VEHICLE SAFETY MESSAGES 3-12
3.4 ANTENNA CHARACTERISTICS 3-13
3.4.1 Omni-Directional Antenna Coverage 3-13
3.4.2 Vertical Antenna Polarization 3-13
3.5 VEHICLE SAFETY MESSAGES ON CONTROL CHANNEL 3-13
3.6 HIGH-AVAILABILITY, LOW-LATENCY CHANNEL 3-14
3.7 PRIORITY FOR VEHICLE SAFETY APPLICATIONS 3-15
3.8 MESSAGE SET STANDARDIZATION 3-15
3.9 DSRC / WAVE SECURITY 3-16

4 EVALUATION OF PROPOSED DSRC / WAVE STANDARDS 4-18

4.1 LOWER LAYER STANDARDS 4-18
4.1.1 ASTM E2213-03 4-18
4.1.2 ASTM E2213-x 4-18
4.1.3 IEEE 802.11p 4-19
4.1.4 FCC Channel Rules 4-19
4.2 UPPER LAYER STANDARDS 4-19
4.2.1 IEEE P1609 Upper Layer Standards 4-19
4.2.2 IEEE P1556 Security Standard 4-20
4.3 IDENTIFIED ISSUES 4-20
4.3.1 High-Availability, Low-Latency DSRC Channel 4-20
4.3.2 Potential Control Channel Congestion 4-21
4.3.3 Potential Priority Conflicts in RSU Zones 4-21
4.3.4 IEEE 802.11p Lower Layer Standards Developments 4-21

4.3.5 Upper Layer Interoperability 4-22
4.3.6 Application and Message Priorities 4-22
4.3.7 DSRC / WAVE Security Considerations 4-23
4.3.8 Potential Interference from Other Services 4-23
4.3.9 Privacy Concerns 4-23

TABLE OF FIGURES

FIGURE 1. DSRC STANDARDS ROADMAP – SEPTEMBER 2004 2-2
FIGURE 2. ISO/OSI REFERENCE MODEL 2-3
FIGURE 3. FCC RULEMAKING TIMELINE 2-4
FIGURE 4. ASTM TIMELINE 2-5
FIGURE 5. IEEE 802.11P TIMELINE 2-6
FIGURE 6. IEEE P1609 TIMELINE 2-7
FIGURE 7. IEEE P1556 SECURITY STANDARD TIMELINE 2-8
FIGURE 8. SAE DSRC TECHNICAL COMMITTEE TIMELINE 2-9
FIGURE 9. POTENTIAL SAE RECOMMENDED PRACTICES TIMELINE 2-9

1 Background

The purpose of this appendix is to summarize the findings of standards-related tasks - Task 5 and Task 13 - of the Vehicle Safety Communications (VSC) project. The VSC project goals related to DSRC standards were to:

- Work with standards development organizations to ensure that proposed DSRC communications protocols meet the needs of vehicle safety applications;
- Investigate specific technical issues that may affect the ability of DSRC (as defined by the standards) to support deployment of vehicle safety applications; and
- Assess the ability of proposed DSRC communications protocols to meet the needs of safety applications.

The VSCC has been participating in the development of the DSRC standards currently underway through organizations such as the American Society for Testing and Materials (ASTM), the Institute of Electrical and Electronic Engineers (IEEE), and the Society of Automotive Engineers (SAE). The VSCC participation was focused upon ensuring that vehicle safety applications requirements were addressed. Results from Tasks 4 and 6 of the VSC project were provided as input to DSRC standards development. The VSCC established liaisons with other related projects, such as those undertaken by Virginia Tech and the DSRC Industry Consortium (DIC).

Early in the VSC project, it was recognized that there were many DSRC-related standards either under development or that needed to be developed before vehicle safety applications could be successfully deployed. There were many different groups, some with conflicting interests, who were involved in the standards development process. Some of these vested interests were known to be in direct opposition to the anticipated communications needs of possible future vehicle safety applications. The direct participation of the VSCC in the DSRC Standards Writing Group appears to have been a highly efficient way to understand, analyze, and influence the development of the majority of DSRC standards over the course of the VSC project. Active participation in standards development organizations (SDOs) included the development of the vehicle-to-vehicle safety message set standard in SAE.

The basic premise for the operation of the 5.9 GHz DSRC band is for shared usage between public and private users, and between safety and commercial uses of this spectrum; the theory being that commercial applications are likely to help subsidize roll-out of infrastructure and vehicle transceivers that will also support safety applications. It is expected that the safety applications will have the highest priority in terms of access to the spectrum, but commercial applications will also share the 75 MHz bandwidth. The commercial applications will use this bandwidth, as long as they comply with the prioritization scheme.

The DSRC standards group devised a channel switching scheme that includes a control channel in order to support a site licensing system for roadside transponders, a general priority system for applications, and still use the full spectrum of the DSRC band. The 75

MHz of spectrum was divided into seven channels, one control channel and six service channels. The basic concept is that the control channel will support very short announcements or messages only, and any extensive data exchange will be conducted on service channels.

The FCC released its 5.9 GHz DSRC Report & Order in February 2004. This DSRC rulemaking contained a number of features that were of benefit to the potential deployment of vehicle safety communications using 5.9 GHz DSRC. The FCC rulemaking mandated the ASTM E2213-03 standard as required for operation at layers one and two on the 5.9 GHz DSRC spectrum. However, this does not include, for example, the limitation of channels to particular usage (such as the high-availability, low-latency channel), the operation of the control channel, the channel-switching scheme, or the priorities of the applications.

The high-availability, low-latency channel was not specified in the FCC Report and Order. At the present time, upper layer protocol standards, rather than FCC regulation, were expected to specify the necessary channel utilization. However, these upper layer standards need to be specified and enforced for use in the 5.9 GHz spectrum.

The FCC rulemaking specified licensing of On-Board Units (OBUs) on a license-by-rule basis, as recommended by the VSCC. As well, the licensing rules specified for Roadside Units (RSUs) are expected to allow rapid deployment of RSUs to support vehicle safety communications. The RSU licensing rules also appear to allow for the rapid deployment of commercial services, as lower priority users of the spectrum. The commercial services may help to subsidize the infrastructure costs, and contribute to a more rapid deployment of RSUs to support vehicle safety and public safety application.

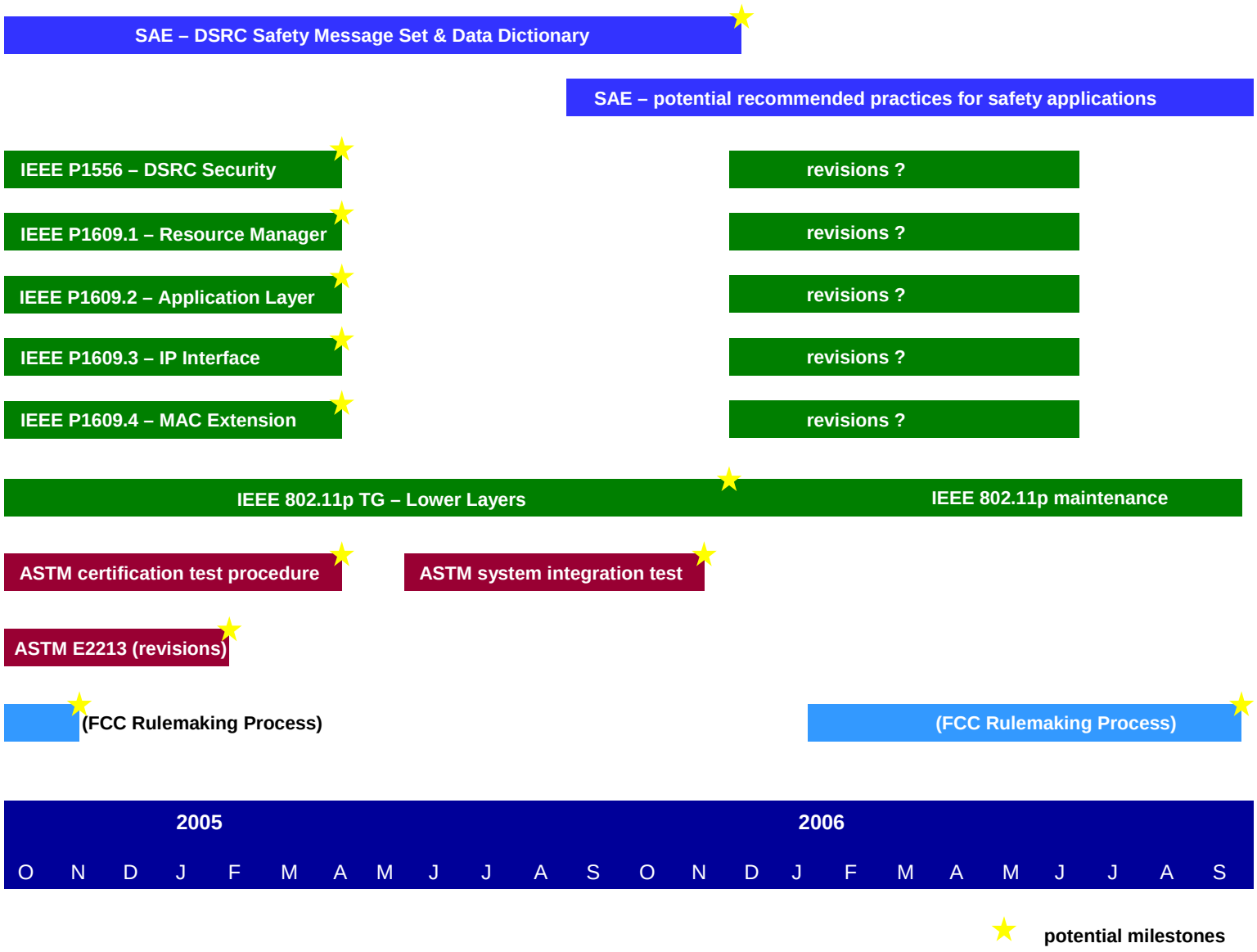
2 DSRC Standards Progress

2.1 DSRC Standards Roadmap

The DSRC standards roadmap illustrates the expected future development of the many DSRC-related standards within various Standards Development Organizations (SDOs) as of September 2004. The time line shown in the roadmap illustration (Figure 1) extends until the third quarter of 2006.

Testing and validation of the DSRC standards is expected to begin as soon as software that implements the DSRC standard protocols on generic host computers, and/or standards-compliant prototype equipment, becomes available. Revisions to the standards are likely to be required as a result of this testing and validation by various stakeholders. If such revisions are required, fully validated DSRC standards may be available by the middle of 2006.

Figure 1. DSRC Standards Roadmap – September 2004

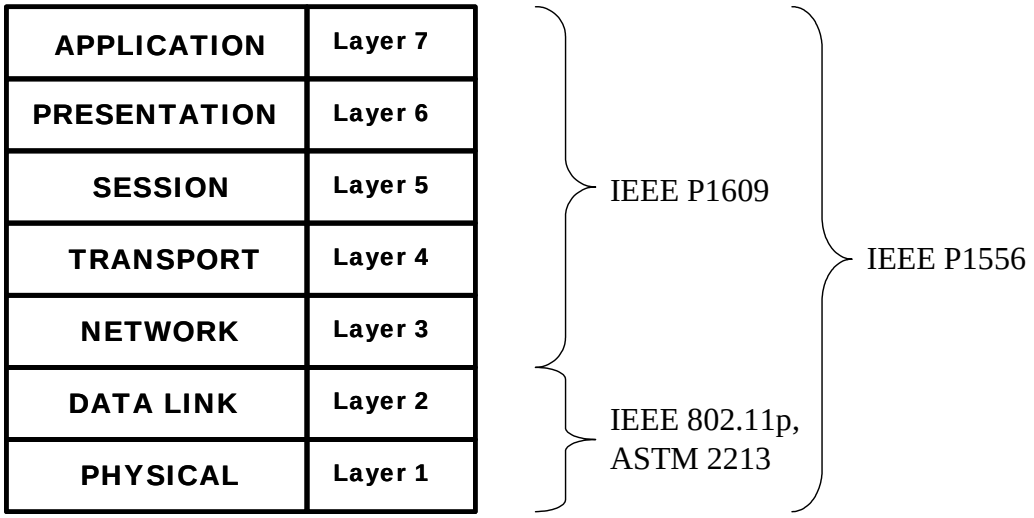


NOTE: This figure is best viewed in color, and may not reproduce well in black and white format.

2.2 ISO/OSI Reference Model

Much of the organization for DSRC standards development is based upon a layer approach toward protocol development. The most widely used model is the seven-layer ISO/OSI reference model. This model is shown in Figure 2, along with the protocol layer relationships of various DSRC standards.

Figure 2. ISO/OSI Reference Model



ISO/OSI Reference Model

In this model, each layer provides services to support those layers above it. The protocol implementations for many common systems do not completely follow this model. The Internet protocol, for example, has layers that do not exactly match the ISO/OSI model. The main benefit of the model is that it provides a logical, structured approach toward understanding and developing protocol stacks.

Layers 1 and 2 are often called the “lower layers”. This reference model therefore forms the basis for the “lower layer” designation of the ASTM standard, for example. In general, the IEEE 802.11 working group only prepares standards that apply to layers 1 and 2. The existence of standard lower layer protocols allows various upper layer systems to use the same lower layers. For example, the same IEEE 802.11 Medium Access Control (MAC) is used “on top of” various modulations on different frequencies (e.g., 2.4 and 5.8 GHz) to provide common services for upper layer protocol stacks over 802.11b, 802.11g and 802.11a.

2.3 FCC Rulemaking

This section outlines the current FCC Rulemaking and expected follow-on process. The current expected timeline is shown in Figure 3. However, at this time, it is not possible to accurately forecast the timing or completion of these processes. For example, comments for reconsideration have been submitted, requesting the commission to keep the current docket open until the revised ASTM lower layer standard is completed, in order to change the FCC mandate to the newer version of this standard.

Figure 3. FCC Rulemaking Timeline

This diagram shows a milestone in November 2004. This milestone marks the anticipated finalization of the FCC Report & Order that was published in February 2004. This document can be found at:

http://www.itsa.org/ITSNEWS.NSF/4e0650bef6193b3e852562350056a3a7/7904e45fa730413885256e36006bf0fc?OpenDocument.

This Report and Order contains the details of the rulemaking for the use of the 5.9 GHz DSRC spectrum. The DSRC rulemaking provides a number of features that are of benefit to the deployment of vehicle safety communications using 5.9 GHz DSRC.

The rulemaking specifies vehicle safety and public safety as high-priority users of this spectrum. This effectively addresses the expressed concern that vehicle-to-vehicle safety applications cannot fit within the established definitions of public safety, and these definitions cannot be changed without an act of Congress. The current text of the FCC rulemaking provides a solution that appears to support the needs of vehicle safety communications in this regard.

The FCC Report and Order mandates the use of the ASTM E2213-03 lower layer standard for all operations on the 5.9 GHz DSRC spectrum. This is an optimistic development for vehicle safety communications, since the VSCC has been actively involved in the development of the ASTM E2213-03 standard in order to ensure that it can support the anticipated communications requirements of vehicle safety applications. The mandating of this single standard provides the level of interoperability at the lower layers that is essential for vehicle safety applications. The FCC Report and Order also specifies licensing of On-Board Units (OBUs) on a license-by-rule basis. This approach for OBU licensing was recommended by the VSCC for technical reasons, in order to

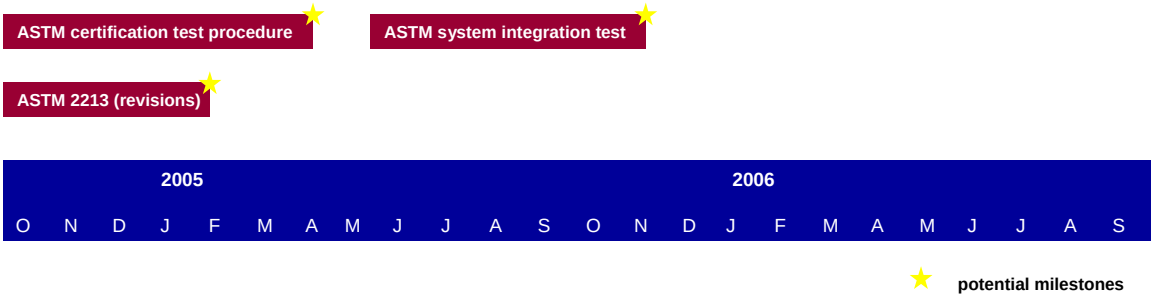
ensure interoperability among vehicles produced by different manufacturers, as well as between various vehicles and roadside units (RSUs).

The FCC Report and Order did not meet the needs of vehicle safety communications in one critical area: the high-availability, low-latency channel (proposed for channel 172). The FCC was reluctant to designate any channel for a particular usage. At the present time, upper layer protocol standards, rather than FCC regulation, are expected to specify the necessary channel utilization. However, if low-priority RSUs, such as commercial users, are licensed and deployed using channel 172, this may limit the capability of DSRC to support some of the critical vehicle safety applications in the future.

2.4 ASTM E2213 Lower Layer DSRC Standard

The expected timelines for potential revisions of the ASTM E2213 lower layer standard, the ASTM certification test procedure standard, and the actual DSRC system testing are shown in Figure 4.

Figure 4. ASTM Timeline



Some modifications have been proposed for the lower layer standard, as a result of technological considerations in the development of the upper layer standards. These modifications are expected to bring the lower layer standard more closely in line with the basic IEEE 802.11a standard. As of September 2004, the proposed modifications were being made to the ASTM lower layer standard, and the revised standard is expected to proceed through the formal voting process for approval within the ASTM organization.

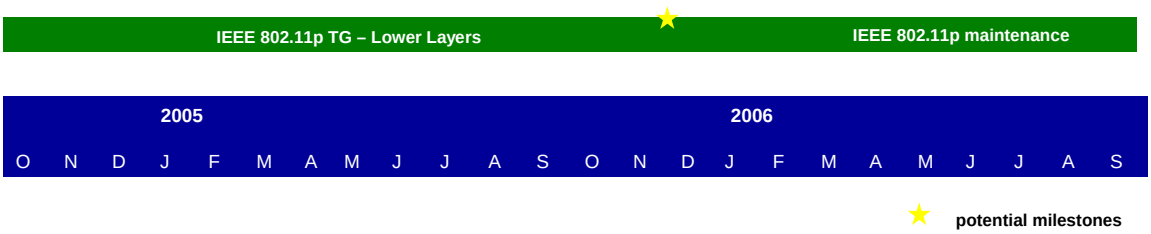
The ASTM certification test procedure standard has been under development for some time. This test procedure document has not yet been completed, however, since the modifications to the lower layer standard must be finalized before the certification test procedure document can be finished.

The system integration testing requires standards-compliant, prototype DSRC units to be available. As shown in Figure 4, this testing is expected to be completed by the fourth quarter of 2005. If this testing, or parallel testing performed by the VSCC and other potential users of the technology, identifies problems that require revisions to the standards, then retesting may be required after the completion of the required revisions to the standards. This retesting is not shown in the diagram.

2.5 IEEE 802.11p Lower Layer WAVE Standard

As of September 2004, IEEE 802.11p was formally approved by the IEEE as a task group to prepare a WAVE standard. Figure 5 illustrates the expected timeline for the IEEE 802.11p WAVE standards development. The completion of IEEE 802.11p by the end of 2005 is a rough estimate at this time, since uncertainty remains regarding the technical consensus process within this task group. After approval of the IEEE 802.11p WAVE standard, continuous maintenance activities will be required in order to keep the IEEE 802.11p standard consistent with ongoing developments within other IEEE 802.11 task groups.

Figure 5. IEEE 802.11p Timeline



One of the main reasons cited for moving the lower layer DSRC standard development into IEEE 802.11 was to ensure that a stable standard would be available over the longer term and would be supported by appropriate experts in wireless technology. A long-term, stable standard would be required in order to deploy the necessary vehicle and infrastructure systems to support enhanced vehicle safety and ensure interoperability between vehicles made by different manufacturers, and with roadside infrastructure in different geographic locations. The IEEE 802.11a standard offers an excellent technology base for these operations. The ASTM DSRC standard was based upon IEEE 801.11a for this reason. An IEEE 802.11p WAVE standard is expected to provide a credible standard that can be maintained in concert with other ongoing developments in IEEE 802.11, as well as a stable standard that can support long-term deployment plans for vehicle safety. The synergy with IEEE 802.11a chipset designs is expected to help ensure the necessary production economies of scale that will allow a quicker, more cost effective deployment of vehicle safety applications.

The IEEE 802.11 working group has a very large member base and the plenary meetings are often attended by more than 800 members. This is also a very successful, high-profile standards group, since the group's 802.11b standard forms the technological basis for the "WiFi" networks that are rapidly becoming ubiquitous in airports, hotels, offices, and homes.

The size and success of this group provides substantial inertia that must be overcome in order to proceed with the development of a new standard like the proposed IEEE 802.11p. As well, since the IEEE 802.11 working group is such a large working group, it has adopted a dense and complex aggregation of rules, administrative procedures and

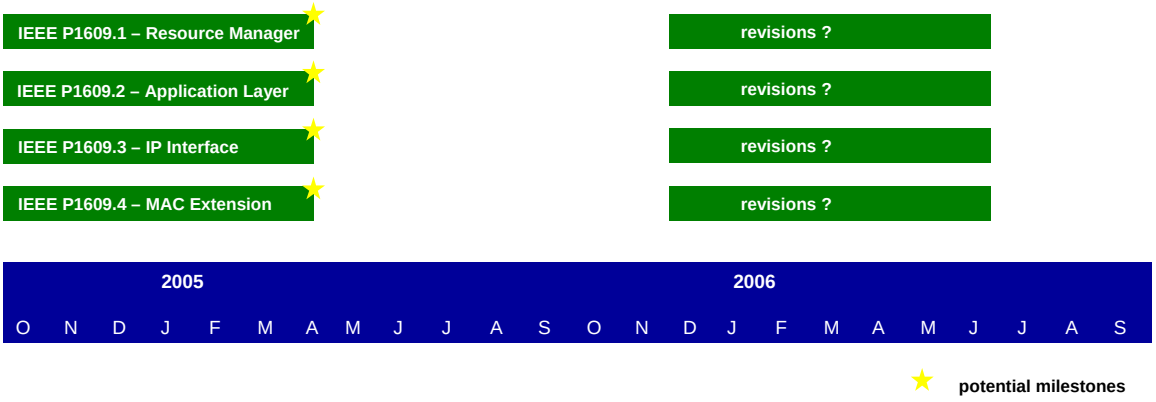
policies. These bureaucratic structures may represent formidable obstacles toward gaining approval of any new standards that are developed.

2.6 IEEE P1609 Upper Layer WAVE Standards

The estimated timeline for the completion of the upper layer WAVE standards is shown in Figure 6. This timeline estimate takes into consideration the drafting activities being undertaken by the DSRC Industry Consortium (DIC) as of September 2004. The milestones shown on the chart represent stated plans for the completion of these standards, as well as estimates for the development of consensus and completion of balloting procedures within the IEEE.

Besides the formal testing and validation planned for these standards, the VSCC may be able to evaluate these standards in detail in future projects in terms of support for vehicle safety communications. These evaluations may uncover areas of the standards that will need to be revised. The possible revision segments shown (December 2005 – June 2006) provide recognition that such revisions may be required after evaluations during most of 2005.

Figure 6. IEEE P1609 Timeline



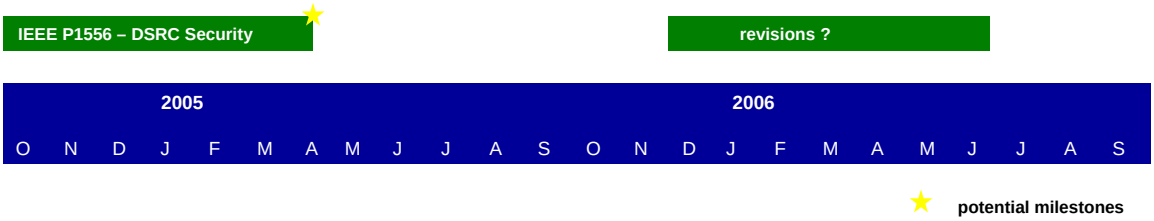
The implementation of the standards into operational production units will likely be the final validation testing for the standards. If the previous pre-production evaluation, validation and testing have been completed thoroughly enough, problems should have been identified and resolved before operational production units are being produced.

2.7 IEEE P1556 Security Standard

Figure 7 shows the estimated timeline for the completion of the IEEE P1556 DSRC security standard. There are some significant uncertainties in this estimate, since very diverse security needs must be integrated into the final standard. The security experts that the VSCC employed as consultants have generated a potential security architecture that

may be able to support vehicle safety communications. It is hoped that his potential solution can become a fundamental part of the overall security solution that will be specified in the IEEE P1556 standard. However, the integration effort has not yet been completed. As well, this initial security solution proposed by the VSCC has not yet been tested.

Figure 7. IEEE P1556 Security Standard Timeline



For widespread deployment of DSRC vehicle safety applications, effective security must be provided. An effective mechanism for key management and administration must be established before full-scale DSRC deployment can begin. Beyond the technical considerations of security solutions, there are policy issues that must be resolved. Some of these policy issues related to the P1556 standards concern key management for roadside and public safety DSRC units.

2.8 SAE DSRC Technical Committee Developments

The SAE initiated a DSRC technical committee with the initial focus of developing a standard message set and data dictionary for vehicle safety communications using DSRC. Vehicle safety communications in this context includes both vehicle-to-vehicle and vehicle-to/from-infrastructure communications. The anticipated timeline for the completion of these standards is shown in Figure 8. The milestone shown (December 2005) represents the expected completion of standard message sets for the high-priority vehicle safety applications, as well as a related data dictionary.

Figure 8. SAE DSRC Technical Committee Timeline

Within the SAE DSRC technical committee, there are three subcommittees, as of September 2004:

- Vehicle Safety Messages
- Vehicle Non-Safety Messages
- Message Framework

Many of the VSCC technical members have been actively participating in this technical committee, and several members have been elected to leadership positions. This automotive focus in the leadership of the committee and subcommittees is expected to result in a standard that is useful for vehicle manufacturers.

2.9 Potential SAE Recommended Practices for DSRC Vehicle Safety Applications

The potential activity to develop recommended practices for vehicle safety applications is anticipated, but not yet planned. As more complex vehicle safety applications that use DSRC communications are developed, the development of recommended practices for vehicle safety applications may be the best way to support interoperability between safety applications installed on vehicles produced by different manufacturers, as well as between vehicles and infrastructure systems installed by various road authorities.

Figure 9. Potential SAE Recommended Practices Timeline

The development of recommended practices could provide an agreed framework for the particular vehicle safety applications, without totally constraining the application design or precluding technological improvements and enhancements.

The SAE has developed recommended practices for vehicle safety applications in the past, and appears to be well-positioned to undertake such developments for DSRC vehicle safety applications if, as expected, this is deemed to be desirable. For this reason, it seems that the SAE would be the most likely standards development organization to prepare any of these potential recommended practices that relate directly to vehicles.

At the present time (September 2004), recommended practices development activities are expected to be required within the next two years. The timeline illustrated in Figure 9 represents an estimated starting time in the third quarter of 2005. However, it is not clear exactly when these activities may be initiated. The development activities can be expected to continue for some time into the future, as indicated by the arrow in the figure.

3 Incorporation of VSCC Positions into DSRC/WAVE Standards

As part of the Task 5 and Task 11 activities, the VSCC actively participated in meetings of the DSRC Standards Writing Group, and associated ASTM E2213, IEEE P1609, IEEE P1556 meetings. As well, the VSCC actively participated in IEEE 802.11 Working Group meetings, beginning when the DSRC lower layer standards development was moved to the IEEE 802.11 Working Group from the ASTM E17.51 DSRC group. In addition, the VSCC has assumed leadership positions in the newly formed SAE DSRC Technical Committee, and actively participated in the meetings of this committee.

As a result of the consistent, active participation at DSRC standards meetings, the VSCC was able to present and interpret the communications requirements of vehicle safety applications into the DSRC standards development process. This allowed the standards to be modified and further developed in a number of areas in order to support, or better support, the communications requirements of vehicle safety applications. These areas are described in the following subsections.

Sporadic participation in DSRC standards development activities in the various SDOs would be much less effective in promoting support for the communications requirements of vehicle safety applications. One reason for the lower effectiveness of the sporadic attendance approach is that the voting rights in the SDOs typically require ongoing attendance, with very little allowance for missed meetings. Most SDOs operate on an individual representation basis, rather than organizational membership, precluding the sending of substitute attendees to maintain voting status. Another consideration is that there is a technical learning curve associated with each aspect of the standards development, and the basis for many standardization decisions is a dynamic, evolving knowledge base that is shared among the regular, active standards development participants.

The approach that was mainly used for the necessary active participation in DSRC standards development during the VSC project was for a single representative from the VSCC automobile manufacturer members to input and interpret vehicle safety communications requirements to the standards development groups. The representative would also report DSRC standards developments and issues back to the VSCC members and the USDOT. This approach was fairly effective during the VSC project time frame, but standards developments may not be currently optimized for vehicle safety. A more direct approach may be required in the future if automobile manufacturers and the USDOT desire to optimize the DSRC standards to most effectively support vehicle safety applications.

3.1 Broadcast-Type Messages

Broadcast-type messages were identified by the VSCC as the most likely transmission mechanism to support the initially identified range of vehicle safety applications. One of the main reasons for this assessment was that a vehicle would be unlikely to have *a priori*

knowledge of the network address of another vehicle of interest in the dynamic, mobile environment of public roadways. As well, the dynamics of vehicle interactions at roadway speeds appeared to require update rates roughly equivalent to those of vehicle sensors for active safety systems. These considerations defined the preliminary communications requirements for vehicle safety applications that were input into the DSRC standards development process. Through active participation in the DSRC standards developments in ASTM, IEEE and SAE, the VSCC secured effective support for broadcast-type messages to support vehicle safety applications in the completed and planned DSRC standards. It should be noted that this broadcast approach has been regularly questioned within DSRC standards development organizations. The role of VSCC participation has been instrumental in conveying the communications requirements of safety systems to the standards development community. This type of safety system requirements interpretation, however, appears to be required on an ongoing basis, since new participants continue to join the various standards development groups. These new participants must be informed of the communications requirements of vehicle safety so that these requirements are not forgotten or ignored in the ongoing development of the standards.

3.2 Random MAC Addresses

Early in the VSC project, privacy was identified as a fundamental requirement for vehicle safety applications enabled or enhanced by DSRC. The concept of Random Medium Access Control (MAC) addresses for On-Board Units (OBUs) was introduced and promoted by the VSCC. This technique was accepted by the DSRC Standards Writing Group and became embedded in the DSRC standards. It appears that the use of this technique, as written into the DSRC standards, will allow privacy to be protected, since no one should be able to explicitly identify a particular vehicle by its DSRC transmissions.

3.3 Short Header for Vehicle Safety Messages

Full IPv6 (Internet Protocol version 6) adoption throughout the DSRC protocol stack, including the over-the-air message format, was strongly proposed by a number of DSRC standards development participants. In order to allow the maximum number of vehicles to simultaneously use the control channel, the VSCC insisted that full IPv6 headers not be required for vehicle safety broadcast transmissions. The full IPv6 packet headers contained more bytes than the entire expected vehicle safety message payload, and the mandatory use of these headers would have greatly reduced the number of vehicles that could use the control channel at the same time. Instead, several approaches were identified to allow efficient vehicle safety transmissions. One of these approaches was planned to be embedded into the DSRC standards.

3.4 Antenna Characteristics

Since the development of the DSRC standards had been underway for several years before the VSC project became involved, there were a number of aspects of the proposed standards that were designed in a way that did not support the safety communications requirements of automobile manufacturers. These vehicle safety communications requirements were introduced to the DSRC standards development process through the active participation of the VSC project. In particular, two aspects related to vehicle antennas had been proposed in ways that would not support the communications requirements of vehicle safety applications. If these initially-proposed standards had not been able to be modified through the VSC project participation in the standards development, DSRC would not have been able to effectively support vehicle safety applications.

3.4.1 Omni-Directional Antenna Coverage

The initial drafts of the ASTM E2213 lower layer standard specified horizontal and vertical antenna directionalities that would have been very favorable for the design of electronic toll collection systems. The VSCC successfully made the case in the ASTM standards meetings that the majority of anticipated vehicle safety applications required omni-directional antenna coverage. This portion of the standard was subsequently revised to support the omni-directional antenna coverage necessary to support vehicle safety applications.

3.4.2 Vertical Antenna Polarization

Polarization was another antenna issue in which the initially-proposed standards were optimized for toll collection applications. The initial balloted and approved version of the ASTM lower layer standard for 5.9 GHz DSRC specified that “all DSRC antennas shall use right-hand, circular polarization”. This designation would have made it difficult and expensive to implement omni-directional antennas. This also appeared to introduce a great deal of cost and complexity into vehicle antenna design. The VSCC insisted that vertical polarization also be allowed for DSRC antennas. The VSCC, therefore, secured agreement for a revised version of the ASTM standard to allow vertical polarization as well as right-hand circular polarization. This accommodation was written into a revision that was integrated into the current version (ASTM E2213-03) of the lower layer standard, which was mandated by the FCC DSRC Report and Order.

3.5 Vehicle Safety Messages on Control Channel

In the band plan that was initially proposed to the FCC, channel 172 was specified as the “vehicle-to-vehicle” channel, at the prior suggestion of the DSRC Standards Writing Group. When the VSCC analyzed the communications requirements of the identified potential vehicle safety applications, it became apparent that both vehicle-to-vehicle and vehicle-to/from-infrastructure vehicle safety communications must operate on the same

channel. The VSCC made this argument effectively in the DSRC Standards Writing Group, and convinced the group that vehicle-to-vehicle safety communications should be allowed to operate on the control channel along with vehicle-to/from-infrastructure safety communications.

There were serious concerns expressed within the DSRC Standards Writing Group regarding the loading of the control channel that may result from the repetitive transmission of vehicle safety messages by all vehicles in a dense traffic environment. Simulation results of DSRC communications in dense traffic environments were presented at meetings of the DSRC Standards Writing Group. These results indicated that full-powered transmissions of rapidly repeating vehicle safety messages from all vehicles in such environments may result in overloading of the control channel. An overloaded control channel would prevent the effective operation of vehicle safety applications, as well as other applications. The main issue for vehicle safety communications in this environment continues to be how to intelligently control the power and/or repetition rates in order to allow the effective operation of vehicle safety applications. This issue is discussed further in Section 3.10.

3.6 High-Availability, Low-Latency Channel

From the standpoint of vehicle safety, one of the major benefits of 5.9 GHz DSRC is the potential for high-availability, low-latency communications. Portions of the 5.9 GHz DSRC spectrum can be designated for high-availability, low-latency access, and used, for example, for two vehicles on an imminent collision course to exchange vital information during the last 500 milliseconds before impact. This vital information exchange could potentially allow the vehicles to better prepare to protect the occupants from the impact.

An immediate, massive deployment of vehicle-to-vehicle and vehicle-to/from-infrastructure safety applications on the control channel (channel 178) is not expected, due to the existing base of non-DSRC equipped vehicles, and required infrastructure deployment time frame. In the future, though, a significant penetration of these applications, in conjunction with other uses of the control channel, may significantly impact the control channel capacity. To plan for that time, some portion of the 5.9 GHz DSRC band must be dedicated so that high-priority safety applications can have low-latency access for urgent emergency communications, even if all the other channels are fully loaded with more routine communications.

It is imperative for automobile manufacturers to have assurance that this communications capability will be available in the longer-term, in order for a commitment to be made by the manufacturers to deploy 5.9 GHz DSRC-based vehicle safety applications. Channel 172 should therefore be re-dedicated as the High-Availability, Low-Latency DSRC channel to effectively support vehicle safety and other high-priority applications. This channel should be limited to only transmissions related to vehicle safety and other high-priority applications, in order to prevent low-priority transmissions from limiting the availability of the channel, or increasing the latency of communications on the channel.

The DSRC community reached a consensus to support this dedicated use of channel 172, as proposed by the VSCC. The necessity of this channel was illustrated by the pre-crash application scenario: when two vehicles determine that a crash is imminent, they need to immediately switch to a channel that is uncluttered with routine communications and effectively exchange information in the final few hundred milliseconds before the crash that can be used to help mitigate the effects of the crash on the occupants of the vehicles.

3.7 Priority for Vehicle Safety Applications

The DSRC standards group devised a channel switching scheme that includes a control channel to use the full spectrum of the DSRC band, and a general priority system to allow some applications to have preferred access to the spectrum. The 75 MHz of spectrum was consequently divided into seven channels: one control channel and six service channels. The basic concept is that the control channel will support very short announcements or messages only, and any extensive data exchange will be conducted on the service channels.

The basic premise for the operation of the 5.9 GHz DSRC band is for shared usage between public and private users, and between safety and commercial uses of this spectrum. The theory is that the commercial applications are likely to help subsidize the roll-out of infrastructure and vehicle transceivers that will also support safety applications. It is expected that the safety applications will have the highest priority in terms of access to the spectrum, but commercial applications will also share the 75 MHz bandwidth. The commercial applications will use this bandwidth, as long as they comply with the prioritization scheme.

The legal definitions for “public safety” services did not apply for the types of vehicle-to-vehicle safety applications considered by the VSCC. Changing the definitions for public safety would have required an Act of Congress. This issue was raised within the DSRC Standards Writing Group, and was subsequently conveyed to the FCC. In deference to this intervention, the FCC Report and Order specifically described “vehicle safety” and “public safety” services as the high priority users of the 5.9 GHz DSRC spectrum.

3.8 Message Set Standardization

There were divergent views within the DSRC Standards Writing Group concerning how to ensure interoperability at the applications level in DSRC systems. One view was that DSRC applications should be standardized. The alternate view was that message sets and usage contexts could be standardized, and this would lead to sufficient interoperability. The problem with standardizing applications is that a standards development process must be undertaken for each individual application, and also for any subsequent technological improvements to the application. The alternate view – message set standardization – seems to be more commonly held within the DSRC group. The standardization of message sets and usage contexts seems to allow for different versions of similar applications to be interoperable, without forcing a particular application implementation to be adopted by everyone. This approach was supported by VSCC

members, since this would allow applications to be custom-designed to address the particular customer profiles of different brands and models.

As a result of further discussion within the DSRC Standards Writing Group, the decision was taken to establish a standardization activity for DSRC message sets and data dictionary. The message set development was initially planned for IEEE P1609. The SAE was identified as the most likely SDO to undertake this work, and was approached to take on this assignment. The SAE consequently worked to develop a two-year project plan, and successfully submitted the plan for funding. A DSRC message set and data dictionary technical committee was established by the SAE, and initial development efforts were focused on the common vehicle-to-vehicle safety message set. This rearrangement of responsibilities allowed IEEE upper layer work to be adjusted to include the required MAC extension.

3.9 DSRC / WAVE Security

The vehicle safety applications appeared to require enough security to be reasonably certain that any transmission received came from a legitimate DSRC unit, and that the contents of the message had not been altered. The main issue related to this type of security revolved around the one-way broadcast nature of the expected communications of many of the vehicle safety applications. Providing adequate security for one-way broadcast communications presented potential problems, since most security schemes for data communications were developed for local area and wide area networks, where two-way communications sessions represented the main operational mode, and node relationships were relatively long-term compared to the mobile environment. As well, the private, commercial services that are anticipated for DSRC appeared to require mainly security for two-way financial transactions. This presents a dichotomy in security requirements for DSRC standards. Most existing security technologies had been designed to operate on networks where two-way, point-to-point communications sessions were used. Consequently, the available security techniques were generally not appropriate for one-way, broadcast communications.

In Task 6B of the VSC project, research was conducted to determine from which threats vehicle safety applications needed to be secured, and whether or not these needs could be met by known security approaches. Further work continues to be required (as of September 2004) to integrate the security schemes appropriate for vehicle safety applications with the security schemes appropriate for financial transactions, and incorporate such an integrated approach into the DSRC security standard.

As a result of this research, the VSCC defined the security threat model for identified vehicle safety applications, and identified the associated constraints to develop a security solution that could meet the requirements of the vehicle safety communications. Based upon this security threat model, the VSCC employed expert security consultants to generate a potential security architecture that may be able to support vehicle safety communications, both for RSU and OBU installations.

In conjunction with Task 6B, the VSCC provided significant input into the IEEE P1556 DSRC security standard development. However, further work continues to be required (as of September 2004) to integrate the security schemes appropriate for vehicle safety applications with the security schemes appropriate for the needs of other stakeholders, and incorporate such an integrated approach into the DSRC security standard.

4 Evaluation of Proposed DSRC / WAVE Standards

The evaluations in this chapter focus on the adequacy of the proposed DSRC / WAVE standards to support the preliminary communications requirements of the vehicle safety application scenarios identified in Task 3 of the VSC project. Section 4.3 describes standardization issues that have been identified and remain unresolved as of September 2004.

4.1 Lower Layer Standards

There were a number of aspects to proposed lower layer standards. In a liberal interpretation of the physical layer, the FCC channel rules were also included in this section.

4.1.1 ASTM E2213-03

The ASTM E2213-03 lower layer standard was mandated by the FCC in the DSRC Report and Order. This standard formed the basis for much of the testing conducted during the VSC project.

The VSC field testing results demonstrated a range of communication capability well beyond the maximum required range of 300 meters for the vehicle safety application scenarios identified in Task 3. Field testing at highway speeds confirmed that the underlying lower layer technologies operating effectively in this highly mobile environment. Even in dense traffic conditions field test results exceeded initial expectations in terms of the percentage of packets received. Transmissions with up to three sender units appeared to be robust enough to support a variety of vehicle-to-vehicle and vehicle-to/from-infrastructure applications.

The final portions of field testing in Task 10 were conducted with new test kits which more closely approximated the implementation of the ASTM 2213-03 standard. These field tests confirmed the positive assessment of the performance of the lower layer DSRC / WAVE technology to potentially support vehicle safety applications.

4.1.2 ASTM E2213-x

Updates to the ASTM E2213 standard have been proposed in the DSRC Standards Writing Group. These revisions reflected developments in the upper layer standards that indicated lower layer approaches that appeared to better support the overall DSRC protocol requirements.

At the time this report was written (September 2004), the proposed changes appeared to be favorable for the support of vehicle safety applications, as well as bringing the DSRC lower layer more closely in line with the IEEE 802.11a standard.

Final assessment of the proposed revisions will require completion of the revisions to the standard, development of equipment to implement the revised standard and field testing to validate the effective operation of the revised DSRC technology.

4.1.3 IEEE 802.11p

The initial ASTM lower layer standard was heavily based upon IEEE 802.11a, so IEEE 802.11p developments, based upon the ASTM lower layer standard, can be expected to remain generally consistent. Since many of the emerging standards of potential relevance to the DSRC standards were being developed within 802.11, it should be desirable to have the DSRC lower layer standard also in the 802.11 family. This should help to ensure ongoing consistency with other developments in wireless local area networks. As previously mentioned, there is a remaining risk that the different stakeholder groups represented in IEEE 802.11 may be motivated to change some portions of the existing ASTM lower layer standard in ways that will not be conducive to vehicle safety applications.

As with the evaluation of the proposed revised ASTM lower layer standard, final assessment of the IEEE 802.11p standard will require completion of the standard, development of equipment to implement the standard and field testing to validate the effective operation of the IEEE 802.11p technology.

4.1.4 FCC Channel Rules

The FCC Report and Order was viewed as generally supportive to the communications requirements of vehicle safety applications. In the case of the channel plan included in the Report and Order, however, one important change would be necessary to adequately support the needs of vehicle safety applications. Channel 172 should be dedicated as the high-availability, low-latency DSRC channel to effectively support vehicle safety applications. This issue is discussed in Section 4.3.1.

4.2 Upper Layer Standards

4.2.1 IEEE P1609 Upper Layer Standards

The IEEE P1609 series of upper layer standards were being drafted by the DSRC Industry Consortium (DIC) as of September 2004. This drafting arrangement was designed to expedite the completion of these standards, and ensure that they were consistent with the prototype equipment developed by the DIC. These standards were to be based upon the requirements established in the IEEE standards development process. The draft standards were to be presented to the IEEE upper layer standards group for consideration for standardization.

Any effective evaluation of these upper layer standards will require future field testing to determine how well vehicle safety applications would be supported. This field testing would require the implementation of the standards in software or equipment. There

appears to be a significant potential for revisions based upon these field testing and validation results.

4.2.2 IEEE P1556 Security Standard

The IEEE P1556 security standard was also being drafted by the DIC as of September 2004, for the same reasons as described for P1609 standards. The P1556 security standard, once completed, will require a strategic "practicality" review from a systems level perspective.

The IEEE P1556 security standard will also require technical testing and validation for determination of support for vehicle safety applications. As with the P1609 standards, there will be a strong potential for revisions based upon testing results.

4.3 Identified Issues

During the course of the VSC project, a number of issues have been identified, particularly in areas relating to standards development. The issues described in the following subsections present various elements of unresolved risk toward the effective deployment of vehicle safety applications.

4.3.1 High-Availability, Low-Latency DSRC Channel

As described in Section 3.6, there is a strong requirement for channel 172 to be dedicated as the high-availability, low-latency DSRC channel to effectively support vehicle safety and other high-priority applications. However, in the DSRC Report and Order, the FCC did not designate specific uses for channels, other than the control channel. The FCC indicated that it was premature to assign specific channels, since in their opinion an open channel structure could best provide flexibility in DSRC system design. The FCC maintains the initial basic concept that both public safety and non-public safety licensees should be authorized to share access to the full band. This has raised a serious issue for the potential implementation of vehicle safety applications.

The FCC announced that DSRC licenses would be issued beginning in October 2004. This raised the prospect that even if future field and simulation testing demonstrates the necessity of the high-availability, low-latency dedicated channel to the FCC, there may be incumbent licensees on this channel using low-priority applications. It may be very difficult to vacate the channel at that time, and classes of vehicle safety applications, like pre-crash scenarios, requiring high-availability and low-latency may not be able to be supported using DSRC technology.

This situation would raise the prospect of requiring the designation of separate spectrum, potentially in a different frequency band, to support the communications requirements of these vehicle safety applications. If that were the case, other vehicle safety applications would likely use this different spectrum, in order to integrate vehicle safety applications onto one transceiver. If this happens, then the synergies between commercial applications and safety applications will not be able to be realized. This would also invalidate, to a

large extent, the original safety rationale for the allocation of the 5.9 GHz DSRC spectrum.

4.3.2 Potential Control Channel Congestion

The loading of the control channel that may result from the repetitive transmission of vehicle safety messages at high power levels by all vehicles in a dense traffic environment is considered to be a major issue. Since an overloaded control channel would prevent the effective operation of vehicle safety applications, devising effective approaches to provide the necessary congestion mitigation would be clearly in the best interests of the VSCC. However, further research would be required to design and test potentially effective technological congestion mitigation approaches, like intelligent power control or situationally variable transmission repetition intervals.

4.3.3 Potential Priority Conflicts in RSU Zones

A potential conflict between application priority levels accessible to OBUs and RSUs exists within RSU communication zones. A command and control model guides the proposed communications between RSUs and OBUs within an RSU communication zone. Recent standards proposals included the concept of RSUs providing synchronized timing through beacons. Close scrutiny of evolving upper layer standards proposals will likely be required in order to preserve the OBU's capability of initiating high-priority communications for vehicle safety applications within RSU zones. As well, RSUs may be given the capability of sending OBUs to a service channel in order to complete lengthy lower priority applications. Preserving the capability for vehicle safety applications to have low-latency access to adjacent vehicles, while in a RSU communications zone, will also likely require ongoing interaction with the upper layer standards development process.

Finally, there appears to be a belief on the part of a number of DSRC standards development stakeholders that RSUs should inherently have access to a higher level of priority than OBUs. This issue is related to the larger issue of priority assignment and enforcement (see Section 3.10.6), but also may extend into the design of the protocol mechanisms being designed into the standards to support priority discrimination.

4.3.4 IEEE 802.11p Lower Layer Standards Developments

While there were major potential benefits associated with the movement of the lower layer DSRC standards to the IEEE 802.11 Working Group, there were significant risks as well. The IEEE 802.11 Working Group has high credibility with regard to its technical capabilities in the area of wireless networks. As well, many of the emerging standards of potential relevance to the DSRC standards were being developed within 802.11. Having the DSRC lower layer standard also in the 802.11 family will help to ensure ongoing consistency with other developments in wireless local area networks. However, there is a remaining risk that the different stakeholder groups represented in IEEE 802.11 may be

motivated to change some portions of the existing ASTM lower layer standard in ways that will not be conducive to vehicle safety applications.

At the time this report was written, the expectation was that there would not be much reason for such changes, since the ASTM standard drew so heavily upon the 802.11a standard. Additionally, the FCC has already mandated the ASTM lower layer standard for DSRC, and this may provide a major incentive for 802.11 not to change any of the DSRC technology. One further concern with this change in venue for the lower layer standard was that the completion of the lower layer standard within IEEE 802.11 may be delayed for some time, mainly due to the formal processes in the IEEE 802.11 Working Group.

4.3.5 Upper Layer Interoperability

The FCC DSRC Report and Order mandated the ASTM lower layer standard for use on 5.9 GHz DSRC spectrum. However, this mandate did not include any of the upper layer protocols. For interoperability, rules for the use of the 5.9 GHz DSRC spectrum need to specify the use of the upper layer standards, in addition to the lower layer standards.

The mandated ASTM lower layer standard specifies the required operations at layers one and two. However, this does not include, for example, the specific operation of the control channel, the channel-switching scheme, or the priorities of the applications. These types of DSRC operations are being specified in the upper layer DSRC standards, and need to be mandated for interoperability up to the application layer.

It remains unclear how such rules will be made and enforced. The DSRC Standards Writing Group proposed that the USDOT initiate a rule-making process that would apply to vehicles. There was also discussion of a USDOT rule-making that might apply to federal highways and other roadways with federal funding. The USDOT appeared to be in the best position to determine the optimal approach toward rule-making, or another approach, that would ensure DSRC interoperability at the upper layers. The chosen approach would need to operate in a complementary manner with the FCC Report and Order for the use of the 5.9 GHz DSRC spectrum.

4.3.6 Application and Message Priorities

There have been general discussions in the DSRC Standards Writing Group to the effect that safety applications will be assigned a higher priority than private applications. This group even drafted preliminary suggested priorities for identified applications. However, there was not yet any defined process to establish a priority framework, let alone evaluate applications and assign priorities to them. As well, no process or responsible authority had been established to set and maintain the priority levels for various applications.

The FCC Report and Order also described general rules for the assignment of priorities for applications. However, specific aspects were not defined, nor were methods of assignment or enforcement.

The process that is put into place to determine and assign priorities for applications is likely to require public/private cooperation, as well as authority to enforce the priorities of applications.

4.3.7 DSRC / WAVE Security Considerations

At the time this report was written (September 2004), there was a remaining risk within the VSCC security developments that the solutions that have been proposed to provide adequate security may be too costly, or too bandwidth inefficient, to be deployed. There were also significant remaining risks involved with coordinating such a solution with the security solutions of other stakeholder groups.

As additional major considerations for the IEEE P1556 security standard, a number of policy and implementation issues will need to be resolved before deployment can proceed.

4.3.8 Potential Interference from Other Services

An interference assessment of adjacent band Fixed Satellite Service (FSS) earth station uplinks was conducted in association with the DSRC Standards Writing Group. The analysis suggested a minimum impact of 40 dBm for DSRC channels 172-180, and approximately 50 dBm at channel 184 in the direct vicinity of these earth stations. An estimated 4 km distance would be required to avoid interference on channels 172-180, while 22 km would be required for channel 184. Mitigation of this potential interference was seen as an issue to be resolved for the effective deployment of DSRC.

United States military radars were viewed as potentially a larger threat to DSRC. However, military radars within 75 km of DSRC stations must be coordinated in new FCC rules. Apparently, there were only a few of the potentially interfering military radars deployed. Shipboard radars may also interfere with DSRC, but these radars were expected to be disabled during the time that the ships were in port.

Under a practical assessment of the interference issue, there were not too many places where this interference would be expected to be realized in actuality. The antenna directionalities, narrow antenna beam widths and distance of sites from roadways were all viewed as potentially mitigating factors. In the final analysis, DSRC units will need to be designed to accept this interference, and be protected from damage from these high-level signals.

4.3.9 Privacy Concerns

Privacy was a significant constraint for security considerations. However, privacy was a core requirement for automobile end users, and therefore for automobile manufacturers. The level of privacy provided in the proposed DSRC standards depended upon the use of a temporary random MAC address to provide only a relative identification of the vehicle. This approach was not able to solve all privacy concerns, however, since information

resident in other vehicles, or the infrastructure, may be able to be linked to a particular vehicle in conjunction with other sensors (e.g., video detection) or events (e.g., crashes).

The level of anonymity provided by random MAC addresses must be maintained in practice as user-specific applications are implemented on DSRC systems. This may become a significant issue in conjunction with the use of Internet-connected devices within the vehicle. These devices may have fixed IP addresses that could be used to identify the vehicle. In addition, applications that need positive identification of the user, like those that entail financial payments, might contain aspects that compromise the privacy of the end user.