Development of DSRC Device and Communication System Performance Measures

Recommendations for DSRC OBE Performance and Security Requirements

www.its.dot.gov/index.htm

Final Report – May 22, 2016

FHWA-JPO-17-483

U.S. Department of Transportation

Produced by Booz Allen Hamilton for the
National Highway Traffic Safety Administration
U.S. Department of Transportation

Notice

This document is disseminated under the sponsorship of the Department of Transportation in the interest of information exchange. The United States Government assumes no liability for its contents or use thereof.

The U.S. Government is not endorsing any manufacturers, products, or services cited herein and any trade name that may appear in the work has been included only because it is essential to the contents of the work.

Technical Report Documentation Page

1. Report No.
FHWA-JPO-17-483

2. Government Accession No.

3. Recipient's Catalog No.

4. Title and Subtitle
Development of DSRC Device and Communication System Performance Measures

Recommendations for DSRC OBE Performance and Security Requirements

5. Report Date
May 22, 2016

6. Performing Organization Code

7. Author(s)
Ed Adams, Scott Andrews, Mona Asudegi, Seyithan Ayhan, Patrick Chuang, John Collins, Justin Fisher, Dennis Fleming, Larry Frank, Derek Freckleton, Ben Fuja, Dominie Garcia, Stefanie Goodwin, Dwayne Henclewood, Christopher Hill, Raj Kamalanathsharma, Josh Kolleda, Virendra Kumar, Steven Le, Justin McNew, Nick Nahas, Jonathan Petit, Tyler Poling, Kelli Raboy, Ray Resendes, Sara Sarkhili, William Whyte

8. Performing Organization Report No.

9. Performing Organization Name And Address
Booz Allen Hamilton
8283 Greensboro Drive
McLean, VA 22102

10. Work Unit No. (TRAIS)

11. Contract or Grant No.
DTFH61-11-D-00019

12. Sponsoring Agency Name and Address
National Highway Traffic Safety Administration
1200 New Jersey Ave SE
Washington, D.C. 20590

13. Type of Report and Period Covered
Final Draft, July 18, 2014 – May 22, 2016

14. Sponsoring Agency Code

15. Supplementary Notes

16. Abstract
This report presents recommendations for minimum DSRC device communication performance and security requirements to ensure effective operation of the DSRC system. The team identified recommended DSRC communications requirements aligned to use cases, performance needs, DSRC functions, existing research, testing and simulation findings, and also developed compliance test procedure recommendations. The team also identifies recommended security functional requirements following the Common Criteria methodology which aligns requirements to a Target of Evaluation (TOE), threats, assumptions, security organizational policies, and security objectives. The report also includes discussions about outstanding decisions that will affect the operations and performance of the DSRC elements in the system. Next steps and additional analyses that could help further define performance and security requirements are also discussed.

17. Key Words
Connected vehicle system, connected vehicle program, Dedicated Short Range Communications (DSRC), performance requirements, security requirements, Vehicle-to-Vehicle (V2V), on-board equipment (OBE)

18. Distribution Statement

19. Security Classif. (of this report)

20. Security Classif. (of this page)

21. No. of Pages
293

22. Price

Table of Contents

Table of Tables

Table of Figures

Executive Summary

The U.S. Department of Transportation (USDOT) has established a multimodal research program on wireless communication among vehicles and with transportation infrastructure. Preliminary results of these efforts indicate the potential to dramatically improve transportation safety and to advance mobility and environmental goals. A key element in the connected vehicle program, as this research is known, is the Dedicated Short Range Communications (DSRC) network and the components that are linked through this network. The National Highway Traffic Safety Administration (NHTSA) has contracted with Booz Allen Hamilton (Booz Allen, or BAH) to provide recommendations on performance requirements and compliance testing procedures for DSRC devices and communications related to safety and security for the Vehicle-to-Vehicle (V2V) communications planned for the connected vehicle system. The purpose of these procedures is to ensure interoperability, enhance safety communications, reduce malfeasance and misfeasance of components, and promote the privacy protection of individuals. These recommendations relate specifically to in-vehicle DSRC devices. Key findings are highlighted in **bold**.

Background

During the "Development of DSRC Device and Communication System Performance Measures – Analysis of DSRC Operational Needs and Performance Measures" task, referred to as "Phase I" of this project, the Booz Allen team analyzed and developed the operational modes and scenarios, key functions, and qualitative performance measures for DSRC safety and security communications within the connected vehicle (CV) safety system. The team identified the critical Use Cases (UCs) that relate to safety and security communications and operations. The UCs informed the specification of functions and initial performance needs, which enabled the identification of qualitative performance measures focused on the V2V system.

The results from the Phase I work were the starting point for this task. This project, referred to as "Phase II", builds from the work of Phase I. The goal of Phase II of the project is to recommend measurable performance and functional requirements for communications and security of the DSRC network, primarily focusing on V2V communications. This task also includes potential certification tests that can be performed to ensure compliance with the performance and security requirements.

Purpose and Scope

The purpose of this report is to present recommendations for minimum DSRC device communication performance and security requirements to ensure effective operation of the DSRC system. The team identified recommended DSRC communications requirements aligned to use cases, performance needs, DSRC functions, existing research, testing and simulation findings, and also developed compliance test procedure recommendations. The team also identifies recommended security functional requirements following the Common Criteria methodology which aligns requirements to a Target of Evaluation (TOE), threats, assumptions, organizational policies, and objectives.

This research builds on the work conducted during Phase I and focuses on the light vehicle V2V system, although it may be extensible to Vehicle-to-Infrastructure (V2I), Infrastructure-to-Vehicle (I2V), Vehicle-to-Device (V2X), and heavy vehicle V2V communications. These are proposed recommendations for DSRC performance requirements and NHTSA will make the decision on final requirements.

The project scope encompasses CV operations (i.e., Basic Safety Messages [BSMs] and security management data transfer) using DSRC devices, and focuses on producing three outputs:

1) Recommended communications technical performance requirements that impact how effectively a DSRC device can support the needs of expected DSRC applications. This includes the on-board equipment (OBE) and roadside equipment (RSE) as the latter is used for security-related operations or communications between the OBE and the SCMS.

2) Recommended security functional requirements, guidelines, and/or best practices to support secure DSRC communications and operations. Development of security requirements followed the Common Criteria methodology outlined in International Organization for Standardization (ISO) 15408.

3) Recommended compliance testing approaches and procedures to be used by manufacturers to test products and certification labs or government organizations to ensure compliance with communications performance and security requirements.

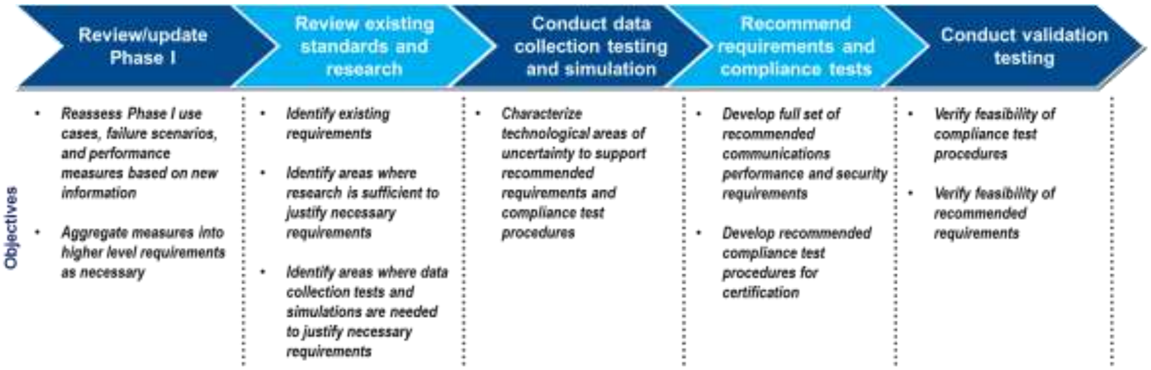
Communications performance and security requirements were developed and determined by analyzing the needs of the V2V system and DSRC device management in the context of the operating modes and functions identified for DSRC devices related to safety and security communications. Depending on what NHTSA decides to do with connected vehicles, there is a range of regulatory and non-regulatory approaches that NHTSA could use to implement its decisions on the requirements that are chosen. These are presented in Section 7.12, Use of Regulations or Other Approaches. Although the team is not specifying requirements for individual applications, the analyses and development of use cases were conducted based on the needs of a BSM.

Summary of Project Approach

The Booz Allen team approached the project focusing on developing a recommended set of requirements with associated compliance test procedures that ensure basic functionality, interoperability, privacy, and security of DSRC devices and the holistic CV system. The team started with existing research, such as the Phase I report and Crash Avoidance Metrics Partnership (CAMP) reports, to develop baseline communications performance and security requirements. Additionally, data collection testing and simulations were conducted to determine requirements in areas and for functions that have not previously been developed for existing systems. These requirements, and accompanying compliance test procedures, were refined based on further research, security assessments, stakeholder engagement, data collection testing and simulation findings, and validation testing and simulation findings. Final recommended requirements are not intended to replace existing technical standards, but are often parallel, with a comparison included within this report.

As shown in Figure 1, the approach to developing communications performance and security requirements is based on a logical evolution, from assessing prior research and existing requirements to conducting data collection in technological areas of uncertainty, which helped determine the minimum requirements necessary for interoperability, privacy, safety, efficient, and effective performance of DSRC communications within the CV safety system.

Figure 1: Approach to Recommended Requirements and Compliance Test Development (Source: USDOT)



Objectives

Review/update Phase I
- Reassess Phase I use cases, failure scenarios, and performance measures based on new information
- Aggregate measures into higher level requirements as necessary

Review existing standards and research
- Identify existing requirements
- Identify areas where research is sufficient to justify necessary requirements
- Identify areas where data collection tests and simulations are needed to justify necessary requirements

Conduct data collection testing and simulation
- Characterize technological areas of uncertainty to support recommended requirements and compliance test procedures

Recommend requirements and compliance tests
- Develop full set of recommended communications performance and security requirements
- Develop recommended compliance test procedures for certification

Conduct validation testing
- Verify feasibility of compliance test procedures
- Verify feasibility of recommended requirements

Findings and Recommendations

While updating the use cases, failure scenarios, and performance measures in the Phase I report, the Booz Allen team reviewed existing standards and research related to DSRC operations and performance. If there were reliable sources to justify initial requirement areas, the research was cited as the source of justification. If the team determined that potential requirement areas needed further research, a data collection test and/or simulation plan was created and executed to better understand the issue and develop new, empirically-based recommended requirements. Through these efforts, the team developed a recommended requirements matrix containing measurable and testable communications functional and performance requirements for DSRC OBE. These recommended requirements focus on:

- Communications Performance
  - Industry standard compliance (i.e., SAE J 2735, Institute of Electrical and Electronics Engineers [IEEE] 802.11, and IEEE 1609 suite)
  - Self-testing
  - Clock accuracy
  - Storage capacity
  - Communication with remote system management servers (e.g., SCMS)
  - Power radiation envelope
  - BSM transmission frequency
  - Message data accuracy
  - Message plausibility
  - Trust store and software updates
  - Congestion and hidden terminal effect mitigation
- Security
  - Industry standard compliance (i.e., IEEE 1609.2)
  - Audit
  - Cryptographic support
  - Data protection
  - Privacy
  - Authentication

- Physical security
- Threat detection
- Trusted paths and channels

The majority of data collection tests and simulations focused on characterizing congestion and hidden terminal effects and possibilities to mitigate those effects. The remaining tests focused on evaluating range performance as a function of data rate and power, clock time sync and stability, hazard detection reliability, and message plausibility assessment. After reviewing existing research on the subject and other system standards and tests, the team identified these as areas for new requirements. The tests and simulations produced results that allowed development of recommended requirements on clock accuracy, transmit power/antenna gain, BSM content accuracy, and plausibility based on empirical and defensible data. The team also identified new possibilities to mitigate congestion and hidden terminal effects which may be the most interesting findings of the effort.

The team found that higher data rates (i.e., 9, 12, and 18 Mbps), rather than 6 Mbps which is currently recommended by CAMP, substantially reduced the Packet Error Rate (PER) (the percentage of the packets not received) caused by congestion and hidden terminals. Based on these tests, the team believes that using a 9 Mbps data rate in a 10 MHz channel and possibly 12 or 18 Mbps in a 20 MHz channel would greatly reduce the negative effects resulting from congestion and hidden terminals. In addition, higher data rates would give the system more flexibility to change cryptographic algorithms if necessary in the future.

The performance impact of using the 9 Mbps data rate in a 10 MHz channel versus 6 Mbps in the same channel is small. These two data rates use the same modulation, and differ only in the degree of overhead error checking included in the packet coding. For small packets such as the BSM, the lower level of error coding for 9 Mbps does not appear to make a significant difference in the overall range performance of the system, but it supports 50% greater data throughput, which in turn reduces the channel load by about 50%. Using 12 or 18 Mbps in a 20 MHz channel is nearly the same as using 6 or 9 Mbps in a 10 MHz channel. This is because the ratio of data rate to channel bandwidth is the same (e.g., 6 Mbps in a 10 MHz channel vs. 12 Mbps in a 20 MHz channel). Similarly in the 20 MHz channel, the difference between 12 Mbps and 18 Mbps is one of error coding (the same as the difference between 6 Mbps and 9 Mbps in the 10 MHz channel). Use of the 20 MHz channel thus allows reliable use of the 18 Mbps data rate, which reduces the overall impact of congestion by 67% (i.e., it provides almost the same basic performance level with three times as many vehicles). The 10 MHz channel is currently accepted as the default channel bandwidth for DSRC safety communications[1], and the team recognizes that a change to a 20 MHz channel would require some rulemaking effort (e.g., a change in Federal Communications Commission [FCC] rules for the V2V safety channel allocation), but the impact on system performance appears to be significant, and therefore may warrant the change.

In short, the possible options to consider for data rate and channel bandwidth:

[1] The 6 Mbps and 9 Mbps data rates in DSRC use the same modulation, and thus require the same signal to noise ratio (without error correction coding). The difference between 6 Mbps and 9 Mbps is in the degree of error correction coding (6 Mbps uses more of the bits sent for error correction than 9 Mbps). Since the BSM is relatively small (300 bytes compared to the maximum packet size of up to 4,095 bytes), it is less affected by errors and the benefit from the additional error correction provided at 6 Mbps is minor. As a result, the data rates are expected (and have been demonstrated in tests) to exhibit identical range performance. A similar technical rational supports the use of 12 Mbps or 18 Mbps in a 20 MHz channel.

- 10 MHz Channel with the use of a 6 Mbps and/or 9 Mbps data rate
- 20 MHz Channel with the use of a 12 Mbps and/or 18 Mbps data rate

There are advantages and disadvantages based on the usage of various data rates and channel bandwidths that must be considered which are discussed within the body of the report.

The team also identified significant issues with the accuracy requirements on the data in the BSM (e.g., position, heading, speed, acceleration, and yaw rate). To assess the required accuracy, the team configured a simulated collision trajectory between two vehicles. Essentially this meant a series of BSMs were defined for two vehicles traveling on paths that were known to intersect at a single point at a specific time. Based on the data in the BSM, the team then predicted the trajectories of the vehicles to determine if the predicted paths would indicate a collision. The team set the target prediction time at three seconds into the future. This was set because this is approximately the amount of lead time required to predict the collision, warn the driver, and have the driver (hopefully) react appropriately. Based on this situation, the BSM represents the current state of the vehicle, and any safety detection application will need to predict the state of the vehicle about three seconds into the future, based on the data in the current BSM. As expected, since the paths were set up to collide with no errors in the data, the system predicted the collision with 100% reliability. The team then introduced errors in the BSM data. The initial simulations used the error statistics observed in the Safety Pilot project. Using BSMs with these error distributions, the reliability of collision prediction three seconds into the future fell to about 35%. What this means is that, based on standard physical models to predict the paths of the vehicles**, if the BSM data is only accurate to within the error tolerances stated for the Safety Pilot program, the system will be able to reliably predict collisions only about 35% of the time.**

The team then performed additional simulations aimed at determining what error tolerances would be needed in order to produce a system that would make correct collision predictions at least 90% of the time. **These tolerances are significantly smaller, as discussed elsewhere in this report. This represents an issue with the current system and existing BSM data elements and error tolerances,** since the driving motivation for a potential NHTSA DSRC mandate is to facilitate applications that may be able to use the BSM to address safety issues in transportation. It is worth noting that if the accuracy of the BSM data is not high enough to ensure that safety applications and their commensurate benefits are reliable (i.e., to allow these applications to make reliable collision determinations), then the system will fall short of several promises of significant safety benefits**. There appear to be several alternatives on how to proceed:**

1) **Do not impose any requirements on the accuracy of the data in the BSM;**
2) **Impose the Safety Pilot tolerances (currently accepted by CAMP);**
3) **Impose the tighter tolerances recommended in this report;**

The first approach (no requirement) appears to be unworkable since an automaker could comply with the V2V rule by sending BSMs with zero data values (i.e., no sensor data). Obviously this would not provide any safety benefit. The second approach appears to be (currently) acceptable to the auto industry, but based on the analysis it will fail to provide the desired levels of intended and reliable safety benefits. Moreover, since the data appears to be valid, the user of the data will be unable to know that the resulting collision prediction (or worse, the prediction of no-collision when one is imminent) is erroneous. The third approach represents a technical challenge (since the error tolerances are significantly tighter). However, it also provides a reliable and consistent collision prediction, and thereby enables user applications to provide consistent safety benefits.

If the NHTSA V2V rule requires vehicles to transmit BSMs, it appears necessary to impose requirements on content such that the imposition of the rule facilitates useful safety benefits.

In the area of security, the team identified several areas, which pose a challenge for rulemaking because it is important to set minimum performance standards in these areas, but those minimum performance standards are likely to change over time as attacks and defenses evolve. Areas include:

- Hardware security
- Software and Operating System (OS) security
- Denial of service prevention
- Misbehavior detection and reporting

In these areas it will likely be necessary to establish a process to provide up-to-date requirements that new devices must satisfy. It will also be necessary to monitor the effects of having a large number of devices in circulation that conform to older versions of these requirements.

In addition, there is a significant risk to the system from the potential future development of quantum computers. Quantum computers will eventually enable breaking the cryptographic algorithms currently used to protect the integrity, authenticity, and (where necessary) confidentiality of all data exchanged within the system, including the BSMs themselves. The team recommends that devices are designed in such a way that they can migrate cryptographic algorithms without needing to be physically replaced and have the flexibility to add/remove Root Certificate Authority (RCA) certificates. **This implies that hardware security modules should be provided as general purpose processors with a secure execution environment within a tamper-proof casing, rather than implementing cryptographic hardware security with custom circuits.**

Conclusions

This report provides the recommendations for foundational, minimum functional and performance requirements for secure DSRC communications. NHTSA may decide to base forthcoming rules on these recommendations and supporting research, or use other mechanisms as described in Section 7.12 to provide assurances that integrated vehicles can securely send and receive BSMs within the V2V DSRC network. At the moment, there are still unresolved decisions and issues that will need to be considered and finalized before final deployment of the system. Unresolved issues and decisions that relate specifically to implementation of recommended requirements and compliance tests include:

- Device certification
- Device bootstrap process
- Device End of Life management
- Collaborative Certificate Revocation List (CRL) distribution
- A stable misbehavior detection solution (local and global)
- An SCMS Manager
- A decision on cryptographic algorithms
- An interoperable solution to request and response transactions between the OBE and remote server management systems
- A complete channel congestion mitigation strategy
- A decision on DSRC spectrum sharing
- Vehicle sensor (BSM data content) accuracy requirements

1 Definitions

Note: Refer to Appendix A for additional acronyms

Term	Definition
Basic Safety Message (BSM)	The outgoing message sent by a vehicle that communicates information and data about its current state to a set of neighboring vehicles. That information or data is used by Vehicle-to-Vehicle (V2V) safety applications in the neighboring vehicles to warn users of crash-imminent situations.
Bootstrapping	The process of configuring and updating an uninitialized vehicle's on- board equipment (OBE), which results in the issuance of the OBE's enrollment certificate and transition to the Operating Mode.
Butterfly Keys	A set of public keys related to a single private key generated by the Registration Authority (RA) and Certificate Authority (CA). There are two – one for signing and one for encryption. The signing keys are used to validate BSMs signed by the OBE. The encryption keys are used to encrypt the certificates for transmission back to the OBE.
Caterpillar Keys	A pair of public and private key pairs generated by the OBE. There are two per set of OBE certificates requested. One pair is used for signing and one pair is used for encrypting. The public parts are sent to the Registration Authority (RA) where each is expanded into a set of keys that are sent to the Pseudonym Certificate Authority (PCA) as part of each certificate request.
Certificate Authority (CA)	In Public Key Infrastructure (PKI) security systems, a CA is a trusted entity authorized to create, sign, and issue public key certificates.
Certificate Identifier	A unique identifier in each certificate calculated from the linkage values specific to that certificate provided by the linkage authorities.
Certificate Management Entity (CME)	An organization that houses certain functions and activities necessary for the certificate management process.
Certificate Policy	The document that describes the roles and responsibilities for implementing a PKI , the rules governing how certificates are obtained, the technical requirements for generation and protection of private keys and certificates, and the requirements for periodic compliance audits and audit records.
Certificate Revocation List (CRL)	A list of certificate identifiers that the Misbehavior Authority (MA) function identifies to be misbehaving due to technical error or human malfeasance.

Term **Definition**

Certification Lab A function that tests devices (e.g., OBE) and tells the Enrollment Certificate Authority (ECA) that units of a particular type or class are eligible for enrollment certificates. Note that there may be additional types of certification labs, outside the purview of the Security Credentials Management System (SCMS) that will perform tests of batches of devices for performance and compliance with federal or industry standards.

Cocoon Keys A pair of public and private key sets generated by the Registration Authority (RA) from the caterpillar keys passed from the OBE. The purpose is to expand the caterpillar key into something the PCA can use to return information that only the OBE can read.

Common Criteria (CC) The Common Criteria (CC) for Information Technology Security Evaluation is an international standard (ISO / International Electrotechnical Commission (IEC) 15408) for computer security certification. It is currently in version 3.1 revision 4. Common Criteria provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standard and repeatable manner at a level that is commensurate with the target environment for use. (Source: Wikipedia)

Connected Vehicle Program The USDOT research program focused on the combination of applications, services, and systems necessary to provide safety, mobility, and environment data to users in a manner that protects privacy.

Connected Vehicle System The deployed system of connected vehicle devices, infrastructure, and back-end functions that will enable safety, mobility, and environment applications to be exchanged.

CRL Generator A sub-function of the MA, the CRL Generator is the function that creates and publishes CRLs so that other system components can access and download them.

Cryptography The combination of mathematical algorithms and computer science intended to protect users, networks, and messages sent throughout a network by encrypting messages. Only authorized users of the network have the necessary information or credentials to access the data within the network.

Dedicated Short Range Communications (DSRC) The one-way or two-way short-to-medium range wireless communication channels specifically designed for automotive use and a corresponding set of protocols and standards. DSRC is sometimes referred to as Wireless Access in Vehicular Environments (WAVE) in other literature.

Enrollment CA (ECA) The Certificate Management Entity (CME) that activates or initializes the OBE by issuing an enrollment certificate. The ECA was previously referred to as the CA_{ACT} and Long Term CA.

Term **Definition**

Enrollment Certificate The certificate used to demonstrate the trustworthiness of the OBE. The enrollment certificate authenticates the device to be part of the Security Credentials Management System (SCMS) and thus receive a batch of pseudonym certificates. Enrollment certificates are distributed by the ECA.

Hidden Terminal Problem In wireless networking, the hidden node problem or hidden terminal problem occurs when a node is visible from a wireless access point (AP), but not from other nodes communicating with that AP. This leads to difficulties in Media Access Control (MAC) sublayer. Hidden nodes in a wireless network are nodes that are out of range of other nodes or a collection of nodes.

IEEE 1609.2 The IEEE standard for WAVE security services for applications and management messages.

IEEE 1609.3 The IEEE standard for the WAVE Networking and WAVE Short Message Protocol (WSMP) layers.

IEEE 1609.4 The IEEE standard for the WAVE upper MAC layers, including channel switching.

IEEE 802.11p The IEEE standard for the DSRC physical layer and lower MAC layers (based on 802.11a).

Infrastructure-to-Vehicle (I2V) The wireless exchange of critical safety and operational data between highway infrastructure and vehicles, intended primarily to avoid motor vehicle accidents but also to enable a wide range of other safety, mobility, and environmental benefits.

Intermediate CA A CA that issues certificates for all CAs below it and that is not a Root CA. Its value is that it shields the Root CA from traffic and attacks. It may also allow for greater flexibility in permission granting.

Linkage Authority (LA) The CME entity responsible for generation and creation of linkage values at the request of the Registration Authority (RA).

Location Obscurer Proxy (LOP) A networking entity which hides the location of the requesting device from Security Credentials Management System (SCMS) components, such as the Registration Authority (RA).

Misbehavior The reference to technical errors and human malfeasance that have a negative impact on the effectiveness of the connected vehicle system.

Misbehavior Authority (MA) The CME function responsible for detecting, tracking, and managing potential threats to the Security Credentials Management System (SCMS) and connected vehicle system. The MA is also responsible for CRL creation, management, and publishing through the CRL Generator sub-function.

Term **Definition**

Multipath Interference Multipath interference is a phenomenon in the physics of waves whereby a wave from a source travels to a detector via two or more paths and, under the right condition, the two (or more) components of the wave interfere. The interference will arise owing to the two (or more) components of the wave having, in general, travelled a different length (as measured by optical path length, geometric length and refraction), and thus arriving at the detector out of phase with each other. The signal due to indirect paths interferes with the required signal in amplitude as well as phase which is called multipath fading.

On-Board Equipment (OBE) The user equipment that provides an interface to vehicular sensors for safety measures, as well as a wireless communication interface to the Location Obscurer Proxy (LOP) for Security Credentials Management System (SCMS) processes.

Packet Error Rate (PER) The percentage of DSRC packets not received.

Personally Identifiable Information (PII) Any form of information that can be used to identify, contact, or locate an individual person, directly or indirectly.

Private Key In public key encryption, the key held secretly by the subject of a PKI certificate that contains a related public key. It is not made available to any other entity. In signing operations, the private key is used for generating a signature and the public key is used for validating a signature. In encryption (key agreement) operations, the sender uses the recipient’s public key and the sender’s private key to generate a key for encryption. The recipient uses the recipient’s private key and the sender’s public key to generate the same key for decryption.

Probe Data Operational, position, and speed data collected by vehicles at periodic intervals, and reported to a probe data aggregator (generally using the Society of Automotive Engineers (SAE) J2735 Probe Data Message).

Provider Service Identifier (PSID) In the WSMP, the provider service identifier (PSID) conveys to the receiving equipment the types of applications that are used by the sending equipment. For example, user applications register with the radio stack to receive specific PSIDs. When a message bearing that PSID is received, it is delivered to any application registered for that PSID. In addition, the PSID is part of the certificate scope. A transmitting unit must be certified to send messages within the context of a limited set of PSIDs.

Pseudonym Certificates The implicit, short term certificates used during message exchange in the pseudonym system. These certificates do not explicitly contain the holder’s public key, but contain a reconstruction value which can be combined with the CA‘s public key to derive the holder’s public key. They are smaller than traditional certificates which contain the holder’s public key explicitly and offer performance advantages when messages are verified infrequently.

Term **Definition**

Pseudonym Certificate Authority (PCA)
The Security Credentials Management System (SCMS) epicenter responsible for certificate production, certificate validation, and coordinating misbehavior detection and management activities.

Public Key
In public key encryption, the public key is the counterpart to the corresponding private key (which is not distributed to anyone) and is used by relying parties to verify possession of the private key. In signing operations, the private key is used for encryption and the public key is used for decryption. In encryption operations, the opposite is true.

Public Key Infrastructure (PKI)
A set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates. PKI has been chosen as the mechanism to provide integrity and authentication within the connected vehicle system. This system creates and manages digital certificates that bind an identity to its public key to certify the sources of the messages.

Quantum Computer
A computer which uses quantum bits which can be a probabilistic combination of 1 and 0, and as such is capable of performing certain calculations exponentially faster than a normal “classical” computer.

Quantum Safe Cryptography
Cryptographic algorithms that are believed to be secure even when attacked by a quantum computer.

Registration Authority (RA)
The function responsible for authenticating OBE certificate requests, generating cocooned keys, obtaining linkage vales, assembling pseudonym certificate requests (PCRs), shuffling the requests with other OBE requests, and forwarding the requests to the PCA for certificate generation. The Registration Authority (RA) receives the encrypted certificates back from the PCA, assembles the complete set and sends them to the requesting OBE.

Request Coordination Authority
A functional element that ensures that a device does not request more than one set of certificates for a given time period. It is used to coordinate activities between different Registration Authorities (RAs) and therefore is only needed if a given device could request certificates via multiple RAs.

Roadside Equipment (RSE)
An infrastructure node that serves as an intermediary in Vehicle-to-Vehicle (V2V) two-way communications between CMEs and vehicles. RSE may also send its own messages to OBE.

Root Certificate Authority
The master CA that provides the signatures on the certificates for its subordinate CAs. The Root CA possesses a self-signed certificate that contains its own public key to differentiate itself from other CAs.

SAE J2735
The Society of Automotive Engineers (SAE) standard defining messages for various connected vehicle applications.

Term **Definition**

Security Credentials Management System (SCMS) The set of organizations that house the various functions and activities necessary for the certificate management process.

SCMS Entity Certificate The certificate issued to a CME (e.g., PCA, Registration Authority (RA), Linkage Authority [LA]) that authenticates its trustworthiness to all other entities and users in the system.

Signal Phase and Timing (SPaT) A message that is used to convey the current status of a signalized intersection. The receiver of this message is able to determine the current state of each phase and when the expected next phase is to occur.

Target of Evaluation (TOE) The Target of Evaluation (TOE) is the specific entity which is to be analyzed when taking a Common Criteria approach to developing security requirements. The selection of the boundary for the TOE can vary depending on the desired scope to be addressed in the Common Criteria Protection Profile.

Trip Trackability The ability to track an individual vehicle through either a portion of a trip or an entire trip.

Trust Distribution The way that the Root CA allows for other Security Credentials Management System (SCMS) functions to sign certificates and authorize users to participate in the system. Rules regarding trust distribution would be specified in the SCMS certificate policy when it is developed.

Trust Management The process of establishing and managing trust within the PKI system and the associated procedures, policies, and technical controls. Trust distribution and trust store management are components of trust management.

Trust Store Management A process that provides procedures to import, edit, and remove certificates trusted by the system for validation of a digital signature and certificates.

Vehicle-to-Device (V2X) The wireless communication exchange of messages and data between and among vehicles, infrastructure, and capable nomadic devices within the connected vehicle system.

Vehicle-to-Infrastructure (V2I) The wireless exchange of critical safety and operational data between and among vehicles and highway infrastructure, intended primarily to avoid motor vehicle accidents but also to enable a wide range of other safety, mobility, and environmental benefits.

Vehicle-to-Vehicle (V2V) A dynamic wireless exchange of data between nearby vehicles that offers the opportunity for significant safety improvements.

Virtual Machine The software implementation of a machine (e.g., a processor) that executes software code program instructions for the functions of the Security Credentials Management System (SCMS).

Term	Definition
WAVE Service Advertisement (WSA)	A message sent by DSRC Provider Terminals (e.g., Roadside Equipment (RSE)) announcing service and channel information so that DSRC User Terminals can determine which services are being offered on which service channels during the service channel interval.
WAVE Short Message (WSM)	A single packet message formed and sent in accordance with the WSMP (See IEEE 1609.3).
Wireless Access in Vehicular Environments (WAVE)	The IEEE networking, upper messaging, and security layers associated with DSRC.
X.509 Certificate	In cryptography, X.509 is an International Telecommunication Union - Telecommunication Standardization Sector (ITU-T) standard for public key certificates and attribute certificates. This international standard defines a framework for how certificates are formatted, revoked, and managed, among other things.[2]

[2] ITU-T, X.509 website: http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.509.

2 Introduction

The USDOT has established a multimodal research program on wireless communication among vehicles and with transportation infrastructure. Preliminary results of these efforts indicate the potential to dramatically improve transportation safety and to advance mobility and environmental goals. A key element in the connected vehicle program, as this research is known, is the DSRC network and the components that are linked through this network. NHTSA has contracted with Booz Allen Hamilton to provide recommendations on performance requirements and compliance testing procedures for DSRC devices and communications related to safety and security for the Vehicle-to-Vehicle (V2V) communications planned for the connected vehicle system. The purpose of these procedures is to ensure interoperability, enhance safety communications, reduce malfeasance and misfeasance of components, and promote the privacy protection of individuals. These recommendations relate specifically to in-vehicle DSRC devices.

This report summarizes the work of the Booz Allen team, which has taken place over two phases; the second phase forms the basis of this report. This document begins with an introduction to the Phase II report by briefly reviewing the Phase I activities, and providing an overview of the Phase II purpose, scope, and methodology used to develop recommendations for DSRC communications performance and security requirements, as well as compliance testing procedures.

Overview of Phase I

During the “Development of DSRC Device and Communication System Performance Measures – Analysis of DSRC Operational Needs and Performance Measures” task, referred to as “Phase I” of this project, the Booz Allen team analyzed and developed the operational modes and scenarios, key functions, and qualitative performance measures for DSRC safety and security communications within the CV safety system. The team identified the modes in which the DSRC system will operate and the critical Use Cases (UCs) that relate to safety and security communications and operations. Each UC included the preconditions, sequence of events, and post conditions for safety and security applications. The UCs informed the specification of functions and initial performance needs, which enabled the identification of qualitative performance measures focused on the V2V system. Though, in the future the qualitative performance measures may be extensible to Vehicle-to-Infrastructure (V2I), I2V, Vehicle-to-Device (V2X) (e.g., a mobile phone), and heavy vehicle V2V communications.

The Phase I project scope was on connected vehicle operations (i.e., BSM and security management data transfer) using DSRC –

1) The primary focus was on the technical performance measures that impact how effectively a DSRC device can support the needs of expected DSRC applications. This includes the OBE or on-board device and RSE insofar as the latter is used for security-related operations or communications between the OBE and the SCMS.

2) The secondary focus was on identifying failure/worst case scenarios. This led to the specification of additional performance measures to ensure the worst case scenarios are

managed by the system. Managing failure means designing systems that intend to diminish negative consequences, allow for recovery from the failure, and/or avoiding it entirely.

Initial performance measures were developed and determined by analyzing the performance needs of light vehicle safety applications (V2V) and DSRC device management in the context of the various operating modes and functions identified for DSRC devices related to security communications. The protection of Personally Identifiable Information (PII) is essential for user acceptance of the system and so from the outset privacy has been designed into the system ("privacy by design"). Regarding DSRC devices within the system, the focus of analysis was on Integrated Safety Devices (ISDs), although it is expected that many of the performance parameters identified will be relevant to other types of DSRC devices (e.g., after-market safety devices [ASDs]).

The results from the Phase I work (e.g., UCs, qualitative performance measures) were the starting point for this task. This project, referred to as Phase II, builds from the work of Phase I to recommend performance and functional requirements for communications and security of the DSRC network primarily focusing on V2V communications.

Phase II: Project Purpose and Scope

The purpose of this report is to present recommendations for minimum DSRC device performance requirements for communication and security to ensure effective operation of the DSRC network. In this report, the team identifies recommended functional and performance requirements for DSRC communications aligned to use cases, performance needs, DSRC functions, existing research sources, testing and simulation findings, and compliance test procedure recommendations. The team also identifies recommended security functional requirements following the Common Criteria methodology which aligns security functional requirements to a Target of Evaluation (TOE), threats, assumptions, organizational security policies, and security objectives.

The research builds on the research conducted during Phase I and focuses on the V2V system, though in the future it may be extensible to Vehicle-to-Infrastructure (V2I), I2V, and Vehicle-to-Device (V2X) communications (e.g., a mobile phone). This report utilizes the CAMP Security Credentials Management System (SCMS) designs as stated in released reports as the basis of understanding of the CV security system. Please note that these are *recommendations* for minimum communications and security requirements. The USDOT and NHTSA must determine what requirements, if any, are included in a future standard or regulation or other approach on V2V communications (see the subsection on "Use of Regulation or Other Approaches in Chapter 7).

The project scope is on connected vehicle operations (i.e., BSM and security management data transfer) using DSRC devices and primarily focuses on producing three outputs.

1) Recommended communications technical performance requirements that impact how effectively a DSRC device can support the needs of expected DSRC applications. This includes the OBE or on-board device and roadside equipment (RSE) insofar as the latter is used for security-related operations or communications between the OBE and the SCMS.

2) Recommended security functional requirements, guidelines, and/or best practices to support secure DSRC communications (i.e., privacy and protection against attacks) and operations (e.g., bootstrap and end of life uninitialization). Development of security

requirements followed the Common Criteria methodology outlined in ISO 15408 and focuses on the vehicle as the TOE.

3) Recommended compliance testing approaches and procedures to be used by manufacturers to test products and certification labs or government organizations to ensure compliance with communications performance and security requirements. Compliance testing procedures are grouped at different levels based on the associated requirements. Many of the recommended requirements may be evaluated by a single compliance test.

Communications performance and security requirements were developed and determined by analyzing the performance needs of light vehicle safety applications (V2V) and DSRC device management in the context of the various operating modes and functions identified for DSRC devices related to safety and security communications. Non-safety applications, such as those for mobility and environmental applications, were not considered explicitly but may share basic performance needs. Although the team is not specifying requirements for individual applications, the analyses and development of use cases were conducted based on the needs of a Basic Safety Message. Regarding DSRC devices within the system, the focus of the analysis is on embedded original equipment DSRC devices, although it is expected that many of the performance parameters identified will be relevant to other types of DSRC devices (e.g., ASDs).

Performance requirements identified are generally technology-agnostic, though the analysis is limited to those related to DSRC-based communications. Requirements are specific to the functions of the system, regardless of the technology used for communications.

Project Methodology

The Booz Allen team approached the project focusing on developing a recommended set of requirements with associated compliance test procedures that ensure interoperability, privacy, and security of DSRC devices and the holistic CV network. At a high level, the team started with existing research, such as the Phase I report and CAMP reports, to develop baseline communications performance and security requirements while also conducting data collection testing and simulation to determine possible requirements in areas of technological uncertainty (e.g., channel congestion mitigation) for the DSRC OBE. These requirements were then refined based on further research, assessment of security threats and objectives, communication with stakeholders, findings from data collection testing and simulation, and findings from validation testing and simulation. Final recommended communications performance and security requirements are not intended to replace existing technical standards such as SAE J2735, but are often parallel, a comparison included in this work.

The team started by reviewing the Phase I report and performance measures matrix to update use cases, failure scenarios, and performance measures based on new information about DSRC performance needs and functions to ensure interoperability, privacy, and security. Because the list of Phase I categorical performance measures were extremely granular, the team worked to aggregate measures where possible. Many of the granular requirements were naturally subsumed by higher level requirements. If the higher level requirement is met, all subordinate requirements are met by default.

The team also studied existing standards and research on V2V and DSRC communications, including all of the supporting reports published with the NHTSA Advanced Notice of Proposed Rulemaking

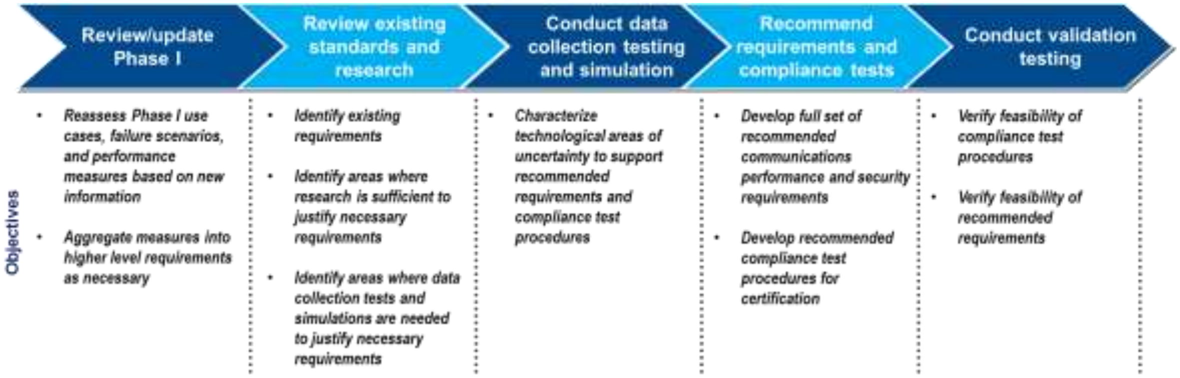
(ANPRM) for Federal Motor Vehicle Safety Standards: Vehicle-to-Vehicle (V2V) Communications, to determine existing requirements or areas where research was sufficient to justify necessary requirements. Along with researching existing requirements, the team also reviewed compliance test procedures associated with those existing requirements and others that could be extensible to future compliance test procedures for V2V performance requirements, such as the Laboratory Test Procedures for 49 Code of Federal Regulations (CFR) Part 563, Event Data Recorders.

Where there were not existing performance requirements or sufficient research results to justify proposed requirements, the team developed data collection procedures (i.e., physical tests and simulations) to characterize technological areas of uncertainty to substantiate requirements and associated compliance test procedures. The team executed additional simulations using field data to extrapolate the results of certain scenarios, such as congestion and hidden nodes, at larger vehicle quantities and ranges. The final set of recommended requirements reflect findings from the data collection testing and simulations coupled with research from past projects conducted by Booz Allen, CAMP, academia, industry consortia, and standards bodies.

Concurrently, the team developed recommended compliance test procedures to verify adherence to recommended requirements. To ensure feasibility of the actual recommended requirements and associated compliance tests, the team conducted validation testing on select test procedures and, based on results and findings, modified requirements and test procedures to ensure they are stated in achievable terms. The team was not able to conduct validation testing on all recommended requirements and testing procedures because the necessary equipment or systems have not yet been fully developed (e.g., SCMS).

As shown in Figure 2, the approach to developing communications performance and security requirements is based on a logical evolution, from assessing prior research and existing requirements to conducting data collection testing and simulation in technological areas of uncertainty, which ultimately helped determine the minimum requirements necessary for interoperability, privacy, safety, efficient, and effective performance of DSRC communications within the CV safety system.

Figure 2: Approach to Recommended Requirements and Compliance Test Development (Source: USDOT)


Review/update Phase I
Review existing standards and research
Conduct data collection testing and simulation
Recommend requirements and compliance tests
Conduct validation testing
Objectives

- *Reassess Phase I use cases, failure scenarios, and performance measures based on new information*
- *Aggregate measures into higher level requirements as necessary*

- *Identify existing requirements*
- *Identify areas where research is sufficient to justify necessary requirements*
- *Identify areas where data collection tests and simulations are needed to justify necessary requirements*

- *Characterize technological areas of uncertainty to support recommended requirements and compliance test procedures*

- *Develop full set of recommended communications performance and security requirements*
- *Develop recommended compliance test procedures for certification*

- *Verify feasibility of compliance test procedures*
- *Verify feasibility of recommended requirements*

3 Project Assumptions

This section lists the set of technical assumptions taken into account during performance and security requirements development. The team conducted analyses under a set of general assumptions and assumptions pertaining to DSRC device operating capabilities or system security. Some of the assumptions have been previously identified in various research reports, as illustrated in Appendix K. Notes are included in the description of assumptions that refer to potential findings in the results and recommendations that may change these current assumptions, and will address those in the recommendations and requirements discussions later in the paper. In addition, some assumptions were imposed by this team to have a foundation upon which to develop and analyze various functions and needs.

General Assumptions

1) The OBE uses the appropriate pseudonym certificate to sign all BSMs.
2) BSMs and other broadcast safety messages are signed and not encrypted per IEEE 1609.2.
3) Management of BSM certificates can be considered separate from certificates for other applications on the device.[3]

Assumptions about the Communications System

Component - DSRC ISD, i.e., OBE

1) “DSRC” messaging is defined by IEEE 1609.2, IEEE 1609.3, IEEE 1609.4, IEEE 1609.12, and IEEE 802.11. For this analysis, the application message content is as defined in Society of Automotive Engineers (SAE) J2735.
2) The FCC spectrum allocation will be unchanged from its current description. If the allocation is changed to require spectrum sharing (e.g., with IEEE 802.11 ac) then certain aspects of the analysis may need to be reviewed and revised.
3) The OBE is always on the safety channel when providing safety benefits. This can be accomplished in two ways. Option 1: Use two radios. One on the safety channel, and one that has the ability to use any channel. This second radio will typically monitor the control channel so that it determines when it is in the vicinity of an RSE. The RSE will broadcast a WAVE Service Advertisement (WSA) on the control channel. The WSA announces what services are available from the RSE, and on which service channel those services may be found. This approach would be used on the road, with RSEs that are actually on the roadside. Option 2: Use a single radio. Use the safety channel exclusively under normal operating conditions. When configured to do so, switch to a specific service channel to obtain pre-determined services. This approach would use RSEs in a service environment (e.g., at a dealer service bay). The system would be placed into this service mode by a technician or an automated process.
4) The OBE conforms to section 5.2 – BSM in the SAE Standard J2735 2015-04.

[3] BSM certificates include certificates for misbehavior reporting and other BSM management activities.

5) The OBE device complies with FCC 47 CFR Parts 0, 1, 2, and 95 amendments for DSRC, mask/class type C.
6) Nominal transmit power of the DSRC device is 20 dBm
   a. Note that while this is a current assumption about the OBE and its functionality, some of the tests and recommendations may deviate from it, which implies a potential need to optimize transmit power.
7) Sensitivity (receive side) and equivalent isotropic radiated power (EIRP) (power)(transmission) envelopes are geometrically the same
8) Position values are determined at 10 Hz (for BSMs) (i.e., ten times per second).
   a. Note that while this is a current assumption about the OBE and its functionality, some of the tests and recommendations may deviate from it, which implies a potential need to optimize position determination rates.
9) Positions are determined either by Global Positioning System (GPS) or by GPS plus dead reckoning.

Messages

1) All messages are signed by the originator (i.e., the party that last transformed or processed the information in the message). The system shall attach a certificate to a signed BSM if it has been more than .45 seconds since the system last generated a signed BSM with an attached certificate. Otherwise, the system shall attach a certificate digest.
2) Messages used to communicate through a backhaul via an RSE do not require transformation or processing. Only routing of corresponding Internet Protocol (IP) packets from the DSRC airlink to the backhaul network is required (e.g., for certificate management the RSE simply routes the message without transforming or processing it; therefore, the RSE does not need to secure it).

Data Elements

1) BSM Data Element accuracy will be specified in SAE J2945/1.

Roadway

1) The average distance between RSEs is about 8 miles, given a full deployment of 19,750 governmental RSEs on the National Highway System.
2) The RSE minimum encounter time is about 10 seconds at 60 mph.

Assumptions about the Security Solution

SCMS Design

1) Broadcast CRLs are signed and not encrypted per IEEE 1609.2.
2) A WAVE Service Advertisement is used to announce the availability of SCMS services over DSRC and Internet Protocol version 6 (IPv6).
3) Unicast (IPv6) certificate management messages exchanged between an OBE or RSE and the SCMS are protected (encrypted/authenticated) as described in IEEE 1609.2 and the CAMP certificate management design.
4) Other broadcast and unicast application messages (non-safety applications), other than BSMs, may require security processing. The additional processing load is not considered in

this project because the scale of this usage has not been identified. Only BSMs are in the scope of this report.

5) The OBE changes all broadcast fields that may be used as long-term identifiers when it changes the pseudonym certificates (e.g., MAC addresses, sequence numbers, etc.).
6) Any vehicle-specific or other PII associated with the OBE is held only by entities approved to hold that information (e.g., the ECA for vehicle specific information related to the enrollment certificate).
7) SCMS communications are secured as specified in the SCMS design documents.
8) Infrastructure entities (e.g., certain RSE, Registration Authority [RA], LOP) in frequent communication with the SCMS will have short-lived certificates (e.g., one week), limiting the need for checking the CRL. Revoked CAs and infrastructure entities which are not in frequent communication (including many RSEs) with the SCMS will appear on a CRL separate from the one issued for OBE pseudonym certificates.

Misbehavior

Misbehavior detection and analysis is an area of the security system that is still in a nascent stage of development. CAMP is in the process of developing proposed methods to address misbehavior detection at the vehicle level (local misbehavior detection) and at the SCMS level (global misbehavior detection). As these technical designs and algorithms become more developed and testable, these assumptions will have to be updated accordingly. Future security and/or functional requirements may need to be developed based on how misbehavior detection is eventually incorporated into the design of the hardware, software, and/or security specification on the DSRC device.

4 Developing DSRC OBE Performance Requirements

This section lists the final set of recommended performance requirements in a condensed spreadsheet (Table 1) and explains how the team developed the performance requirements. Existing research and standards or findings developed through data collection testing and simulation support all recommended performance requirements.

Final Set of Recommended Communications Performance Requirements (Condensed)

The Booz Allen team developed a recommended requirements matrix containing communications and performance requirements for DSRC OBE. This subsection contains the final set of recommended DSRC OBE requirements in a condensed spreadsheet. These are separate from the security requirements which are listed in Chapter 5. In addition to the information in the condensed spreadsheet below, the full requirements matrix also contains traceability to the associated DSRC operational state, data collection test/simulation, and test/simulation results. Refer to Appendix E to view the full set of recommended requirements.

Throughout the requirements matrix there are references to several accompanying documents, where additional level of detail is described for various requirements and standards (e.g., Standards Compliance Exceptions Document, Data Collection Testing and Simulation Analysis). All such references/detailed documents are contained in Appendices of this report.

This subsection also contains background on definitions for and purpose of denoting the identification (ID), DSRC element, operational objective, source, compliance approach, and compliance test procedure in the condensed spreadsheet. The requirements are ordered by compliance approach and compliance test procedure. ID numbers are not sequential and many recommended requirements have multiple numbers as a result of aggregating, deleting, or adding new requirements from Phase I.

4.1.1 Definitions and Purpose

ID (From Phase I) – This is the identification number for the requirement. Each ID is associated to a recommended compliance test in a different section. Some IDs are associated to data collection tests or simulations which provide justification for the requirement.

Requirement – This is the recommended requirement for DSRC operations and communications performance.

DSRC Element -- This describes the physical area or software layer within a Connected Vehicle system that the performance requirement addresses. The categories are as follows:

- Roadway – e.g., hazard detection reliability, RSE interactions

- Vehicle – e.g., vehicle transmit power and antenna gain envelope
- System – e.g., message security, message plausibility
- Sub-system – e.g., message storage, message transmission/processing, operational failure detection
- Component – e.g., radio behavior, radio protocol

Operational Objective -- This categorizes each performance requirement into one of three operational objectives:

- Communicate…with other devices
- Trust…the message (and its contents) from other devices
- Interpret…the message contents for use in safety applications

Source – This identifies the source of information that justifies the requirements. This could be a source of information from within this project (i.e., specific test, simulation, or analysis) or outside of this project (i.e., existing standard, research, or report).

Compliance Approach – This describes the anticipated verification or compliance approach recommended for the requirement (Refer to Appendix C for alignment to requirement types and examples). The categories are as follows:

- Vehicle Level Test – Aligns to a “Roadway,” “Vehicle,” or “System” designation as the DSRC Element
- OBE/Component Level Test – Aligns to a “Sub-system,” or “Component” designation as the DSRC Element

Compliance Test Procedure – This provides the name of the recommended compliance test suite and test. Refer to Appendix G for full recommended compliance test procedures.

Table 1: Recommended Communications Performance Requirements List (Condensed)

ID (Ph. I)	Requirement	DSRC Element	Operational Objective	Source	Compliance Approach	Compliance Test Procedure
2b	The OBE shall generate Basic Safety Messages in accordance with SAE J2735 and SAE J2945/1 with the exceptions identified in the Standards Compliance Exceptions Document (Appendix H in the DSRC Phase II Report) [Note: The BSM standard should be updated to include all data elements required in CAMP's Minimum Performance Requirement (MPR), or other analyses within a single Binary Large Object (BLOB)]	Component	Communicate	SAE J2735 (2015) SAE J2945/1 (2015) Standards Compliance Exceptions Document (Appendix H in the DSRC Phase II Report)	OBE/ Component Level	Standards Compliance: SAE J2735/J2945 Compliance
1012	The OBE shall comply with IEEE 1609.2, 1609.3, 1609.4, and 1609.12 with the exceptions identified in the Standards Compliance Exceptions Document	Component	Communicate	IEEE 1609.2 (2016) IEEE 1609.3 (2016) IEEE 1609.4 (2016) IEEE 1609.12 (2016) Standards Compliance Exceptions Document	OBE/ Component Level	Standards Compliance: IEEE 1609 Suite Compliance
1013	The OBE shall comply with IEEE 802.11-2012 with the exceptions identified in the Standards Compliance Exceptions Document	Component	Communicate	IEEE 802.11 (2012) Standards Compliance Exceptions Document	OBE/ Component Level	Standards Compliance: IEEE 802.11 Compliance
1, 3, 4, 60	The OBE shall be capable of generating and transmitting at least 10 BSMs/sec	Subsystem	Communicate	SAE J2735 (2015) Annex C-8: Implementation of V2V Safety Applications Using DSRC BSM, Part I Data Elements and Part II Data Elements	OBE/ Component Level	BSM Transmission and Processing: Message

ID (Ph. I)	Requirement	DSRC Element	Operational Objective	Source	Compliance Approach	Compliance Test Procedure
				Vehicle Safety Communications – Applications (VSC-A) p. 289: Nominal broadcast frequency is 10Hz Implied requirement: The time required to sign WAVE Short Message (WSM) (i.e., compute hash and signature) must be less than the minimum allowable BSM latency less any other delays (e.g., transmit delay)		Transmission under full load
47, 99	The OBE shall process all certificate management operations (i.e., updating the certificate trust store, performing the computations to generate the certificate IDs from the CRL entries, performing self-test to check against CRL, etc. [this is not all encompassing of functions where safety applications have precedence]) such that the OBE continues to meet all performance requirements (i.e., there should be no measureable functional or latency difference in operations as a result of trust store updates)	Subsystem	Communicate	New requirement derived by BAH to ensure that safety operations are always first priority. The transmission and reception of BSMs must come before all other operations	OBE/ Component Level	BSM Transmission and Processing: BSM Generation and Processing Impact
106	The OBE shall install all software updates such that the OBE continues to meet all performance requirements (i.e., there should be no measureable functional or latency difference in operations as a result of software updates)	Subsystem	Communicate	New requirement derived by BAH to ensure that safety operations are always first priority. The transmission and reception of BSMs must come before all other operations	OBE/ Component Level	BSM Transmission and Processing: BSM Generation and Processing Impact
1015	The OBE shall randomly select an integer value N between the ranges identified in the table below	Subsystem	Communicate	New requirement derived by BAH to ensure asynchronous transmission of BSMs to reduce the chances of BSM collision	OBE/ Component Level	BSM Transmission and

ID (Ph. I)	Requirement	DSRC Element	Operational Objective	Source	Compliance Approach	Compliance Test Procedure
	corresponding to the data rate being used to transmit the BSM. The OBE shall make this selection every time it changes a certificate. The BSM shall be transmitted at a time corresponding to the GPS Pulse per Second (PPS) event plus M*100+N*BSM_OFFSET_INTERVAL; where M is a sequence of integers ranging from 0 to 9 (to result in 10 messages per second), BSM_OFFSET_INTERVAL is found in the table below for the corresponding data rate being used to transmit the BSM, and N is a random integer between 0 and the specified maximum. Data Rate/In-Channel Time/BSM_OFFSET_INTERVAL 6 Mbps/500 usec/0-199 (100msec/500usec=200, 200-1=199) 9 Mbps/350 usec/0-284 (100msec/354usec=285, 285-1=284) 12 Mbps/250 usec/0-399 (100msec/250usec=400, 400-1=399) 18 Mbps/200 usec/0-499 (100msec/200usec=500, 500-1=499)					Processing: Asynchronous Message Transmission
1017	The OBE shall transmit BSM WSMs on a 10 MHz channel, at a data rate of 9 Mbps	Subsystem	Communicate	New requirement derived by BAH: There needs to be a common method for mitigating congestion and hidden terminal effects, otherwise there will be competing and non-cooperative strategies. This recommendation differs from the CAMP V2V-SE MPR Report,	OBE/ Component Level	BSM Transmission and Processing: Congestion Mitigation

ID (Ph. I)	Requirement	DSRC Element	Operational Objective	Source	Compliance Approach	Compliance Test Procedure
				4.3.2 Channel and Data Rate which states that "The subsystem shall transmit BSMs on a fixed DSRC channel (Channel 172)." and "The subsystem shall transmit BSMs at a 6Mbps data rate." Also differs from the possible recommended congestion control algorithms presented in the V2V-Interoperability reports (Algorithms X and Y). While the algorithms may still be necessary in extreme congestion situations, this approach should first be taken to mitigate the effects of hidden terminals and congestion. As stated above, The default channel bandwidth for BSM transmission is 10 MHz at 6 Mbps. A 20 MHz channel could be used to increase capacity and mitigate congestion further; however, only one channel can be used for interoperable communication. If the decision is made to continue using a 10 MHz channel, a 9 Mbps data should be used instead of 6 Mbps to increase channel capacity		
85a	The OBE shall have the capacity to store at least one CRL, three years' worth of pseudonym certificates at 20 certificates per week, a basic software load and any updates (non-volatile storage capacity of 1 megabyte (MB) plus size necessary for software storage and operations)	Subsystem	Communicate	New requirement derived by BAH to ensure sufficient storage capacity to conduct operations. SAE J2735 (2015) Annex D: Handling Newly Received Data Frames, Replacement Policy for Locally-Stored Messages, Valid Time Communications Data Delivery System (CDDS) Analysis for Connected Vehicles Report: Table 2. Data Loads by SCMS Transaction used to develop assumptions	OBE/ Component Level	Storage: General Storage

ID (Ph. I)	Requirement	DSRC Element	Operational Objective	Source	Compliance Approach	Compliance Test Procedure
1002	The OBE shall have the capacity to store up to at least 30 misbehaving messages (as defined in requirements 1006, 1018, and 1019) together with their corresponding security credentials, verification status, and the time and position at which they were received (i.e., the misbehavior report/package)	Subsystem	Trust	New requirement derived by BAH to limit needs for storage space of misbehavior reports while still communicating recent detected misbehavior to the SCMS, similar to how the 49 CFR Part 563 - Event Data Recorders specifies in 563.11 that "The Electronic Data Recorder (EDR) is designed to record data related to vehicle dynamics and safety systems for a short period of time, typically 30 seconds or less." Need a stable security solution (need target revocation rate, misbehavior rate, certificate strategy), uninstalled updates, CRL, RSE encounter for better calculations SAE J2735 (2015) Annex D: Handling Newly Received Data Frames, Replacement Policy for Locally-Stored Messages, Valid Time CDDS Analysis for Connected Vehicles Report: Table 2. Data Loads by SCMS Transaction used to develop assumptions See Appendix E for the full recommended requirements matrix with more information	OBE/ Component Level	Storage: Misbehavior Report Storage
1005	The OBE shall have a priority function to determine which misbehavior observations are most important and shall discard the lowest-priority stored misbehavior observations if necessary to store a higher-priority misbehavior observation. The priority function may be Original Equipment Manufacturer (OEM)-specific or may be standardized	Subsystem	Trust	New requirement derived by BAH team to reduce needs for storage space, similar to how the 49 CFR Part 563 - Event Data Recorders specifies in 563.11 that "The EDR is designed to record data related to vehicle dynamics and safety systems for a short period of time, typically 30 seconds or less."	OBE/ Component Level	Storage: Misbehavior Report Storage

ID (Ph. I)	Requirement	DSRC Element	Operational Objective	Source	Compliance Approach	Compliance Test Procedure
113, 105, 50, 57, 86, 122 #1	The OBE shall initiate a startup process, no longer than 60 seconds prior to key-on and should be completed no more than 30 seconds after key-on, that includes following checks: (1) Radius of horizontal position error distribution shall be less than 0.325 meters with at least 95% confidence (2) Vertical position error distribution less than 2 meters with at least 95% confidence (3) The OBE system clock used to time stamp messages and signatures, and perform internal position related computations is synchronized to GPS time to less than 2 millisecond standard deviation (4) All other vehicle sensors providing BSM parameter information should be present and available (5) The OBE's set of pseudonym certificate IDs are not on the Revoked certificate ID Table (6) All received and validated software updates have been installed (7) OBE is installed in the same vehicle for which it has been certified	Subsystem	Trust	New requirement derived by BAH to ensure the OBE performs a self-check at startup to validate readiness to transmit BSMs Other relevant sources: SAE J2735 (2015): 6.46 Data Element: DF_PositionalAccuracy, Data Element: DE_PositionConfidence, 11.1 On the use of TIME, 7.144 Data Element: DE_VINstring	OBE/ Component Level	Failure Detection: Start-up Failure Detection
50, 57, 86	The OBE shall be considered to be operational (in operational mode) when it has confirmed that all conditions for operation have been met at intervals of 100 seconds at most. These conditions are: (1) Radius of horizontal position error	Subsystem	Trust	New requirement derived by BAH to ensure the OBE only transmits BSMs when considered to be in an operational state Other relevant sources: SAE J2735 (2015): 6.46 Data Element: DF_PositionalAccuracy, Data Element:	OBE/ Component Level	Failure Detection: Operational Failure Detection

ID (Ph. I)	Requirement	DSRC Element	Operational Objective	Source	Compliance Approach	Compliance Test Procedure
	distribution shall be less than 0.325 meters with at least 95% confidence (2) Vertical position error distribution less than 2 meters with at least 95% confidence (3) The OBE system clock used to time stamp messages and signatures, and perform internal position related computations is synchronized to GPS time to less than 2 millisecond standard deviation. (4) All other vehicle sensors providing BSM parameter information should be present and available			DE_PositionConfidence, 11.1 On the use of TIME, 7.144 Data Element: DE_VINstring Alternative approach is to have parameter error estimates included within each BSM so that the receiving device can decide how to use the message		
113, 105, 50, 57, 86, 122 #2	Upon failing the startup or operational self-tests, the OBE shall cease sending BSMs (i.e., transition to quiet mode)	Subsystem	Trust	New requirement derived by BAH to limit the transmission of misbehaving messages when the OBE identifies self-misbehavior or inability to send complete BSMs V2V-Interoperability Phase 2 Volume 3 Report: 4.1 Transmit-Side Processing, states "Prior to composing and transmitting a BSM, self-diagnostics of internal sensors will need to be performed to ensure that the sensor data is valid. If a device detects a malfunctioning sensor which could cause misbehavior, if the standards allow, the device should transmit the BSM with the affected elements set as “Unavailable,” otherwise, it should stop transmitting messages. In the latter case, this will essentially lead to the device revoking itself, until the sensor issue is resolved, while not actually sending a Misbehavior Report	OBE/ Component Level	Failure Detection: Start-up Failure Detection Failure Detection: Operational Failure Detection

ID (Ph. I)	Requirement	DSRC Element	Operational Objective	Source	Compliance Approach	Compliance Test Procedure
				(MBR) for itself to the Misbehavior Authority (MBA)." The BAH team believes that the OBE should stop transmitting messages altogether rather than transmitting with affected elements set as "unavailable."		
17, 59	Transmit power and antenna gain shall be greater than -70 dBm when measured at 30 meters in all azimuth directions and between ±10 degrees elevation from the transmitting vehicle antenna(s), with the vehicle antenna(s) mounted to the vehicle in its production location and orientation	Vehicle	Communicate	More stringent requirement than IEEE 1609.3 derived by BAH to increase width of radiated signal band accommodating for road grade to enable message detection and limit radiation envelope requirements reducing diffraction and interference due to the effect of multipath fading Transmit Power/Antenna Gain and Sensitivity Envelope Analysis	Vehicle Level	Static Vehicle: Radiated Transmit Power and Antenna Gain Envelope
1010	OBE self-test shall be performed at key-on. It may also be performed no more than 60 seconds before key-on so long as the OBE does not transition to a fully powered-off state between the self-test and the key-on event	System	Trust	New requirement derived by BAH team to ensure diagnostic checks are completed at key-on to support effective OBE operations and message transmission. The actual checks and acceptable parameters are described in a separate requirement	Vehicle Level	Static Vehicle: Self-test
1009	OBE operations shall survive any key-off, key-on sequence	System	Trust	New requirement derived by BAH team to ensure any operations (e.g., trust store update, CRL processing, software install) shall survive any key-off, key-on sequence (i.e., turning the vehicle off and on) so that operations do not fail	Vehicle Level	Static Vehicle: Self-test
1011	The OBE shall activate a malfunction indication when not in operational mode (e.g., during a start-up check, failing a self-test). The malfunction indication shall be clearly visible from the driver's designated seating position	Vehicle	Trust	New requirement derived by BAH team to ensure the operator of the vehicle is aware when the OBE is not in operational mode, similar to requirements listed in Federal Motor Vehicle Safety Standard (FMVSS) 208 Occupant Crash Protection: S4.5.2, S4.5.4.3, S19.2.2; and FMVSS 126 Electronic Stability	Vehicle Level	Static Vehicle: Self-test

ID (Ph. I)	Requirement	DSRC Element	Operational Objective	Source	Compliance Approach	Compliance Test Procedure
				Control Systems: S5.3		
120	An active OBE malfunction indication shall persist until the OBE passes the self-test and clears all warnings (from previous failed self-tests)	Vehicle	Trust	New requirement derived by BAH team to ensure the operator of the vehicle is aware when the OBE is not in operational mode, similar to requirements listed in FMVSS 208 Occupant Crash Protection: S4.5.2, S4.5.4.3, S19.2.2; and FMVSS 126 Electronic Stability Control Systems: S5.3	Vehicle Level	Static Vehicle: Self-test
1014	The data parameters provided in a BSM generated by the host vehicle shall conform to the following maximum error tolerance requirements (See Source column for comparison to existing recommendations from CAMP) Parameter/Error Tolerance Horizontal position/0.325 meters Vertical position/2 meters Speed/0.015 meter/second Heading/0.1 degrees Time Accuracy/2 msec (GPS) Longitudinal acceleration/0.04 meters/second^2 Yaw Rate/0.12 degrees/second	System	Trust	V2V-SE MPR Report: 4.2 Positioning and Timing Requirements, 4.3 BSM Transmission Requirements - Lists required BSM data accuracy requirements. Parameter/Error Tolerance Horizontal Position/1.5 meter Elevation/3 meters Speed/0.35 meter/second Heading/3 degrees -less than or equal to 12.5 m/s; 2 degrees -greater than 12.5 m/s Time Accuracy/1 msec (UTC) The BAH team believes different error tolerances (those specified in the recommended requirement) are required to provide 90% accuracy of hazard detection 2-3 seconds from a collision	Vehicle Level	Dynamic Vehicle: BSM Parameter Accuracy
80B	Level 1 plausibility: The OBE shall identify as a suspect or implausible message any BSM for which the components of the vehicle dynamic state (position, speed, acceleration, and yaw rate) are outside the values as noted below Speed: 70 m/sec (252 km/hr)	System	Interpret	New requirement derived by BAH to assess message plausibility. This level 1 plausibility check assesses whether data parameters are realistic based on average vehicle performance and laws. The values in the requirement are on the edge or outside the capability of the majority of road legal vehicles and existing driving laws -Speed: Less than 70 m/s, 252 kmph, 156	Vehicle Level	Dynamic Vehicle: Simulated Implausible Messages

ID (Ph. I)	Requirement	DSRC Element	Operational Objective	Source	Compliance Approach	Compliance Test Procedure
	Longitudinal Acceleration - Acceleration: 12 m/s/s, Deceleration: -12 m/s/s Lateral Acceleration: 11 m/s/s Yaw rate: 1.5 radian/s Yaw rate, speed, and lateral acceleration consistent with $(V)^2=(AC)^2/(Y')^2$ (Where V= speed, AC=lateral acceleration, and Y'=yaw rate)			mph, Rationale: excludes various supercars, well over any typical speed limits -Longitudinal acceleration: 0-100 kmph in under 2.3 second (Less than 12 m/s2), Rationale: Based on Ariel Atom, fastest accelerating production vehicle -Longitudinal deceleration: 100-0 kmph in under 95 feet (Less than 12 m/s2), Rationale: Based on Corvette ZO6, fastest stopping production vehicle -Lateral Acceleration must be realistic; less than 11 m/s2 (1.12G), Rationale: Few production vehicles can exceed 1.0 G -Yaw Rate Must be Realistic; Less than 1.5 radian/s, Rationale: 1.5 radian/sec is about equivalent to taking a 15 mph right turn at 27 mph (1G); tighter corners are not feasible (>1G), and softer corners are lower yaw rate at 1G acceleration See Appendix E for the full recommended requirements matrix with more information		
63, 64, 67, 80	Level 2 plausibility: If a BSM would result in a positive application warning decision, the OBE shall identify as a message that fails level 2 plausibility any BSM for which the vehicle dynamic state (position, speed, acceleration, heading, and yaw rate) as described by the most recent BSM falls outside the 2 sigma distribution for the vehicle state as projected from the prior BSM to the time of the current BSM (i.e., the message is implausible if it is not on its expected	System	Interpret	New requirement derived by BAH for a level 2 plausibility check that determines whether the most recent BSM received from a vehicle is within 2 sigma distribution of the projected position from the prior BSM. 2 sigma represents the point at which there is less than 4.8% probability that the number is incorrect. This is a simple metric that assures that if the values are within 2 sigma, there is a greater than 95% chance they are correct V2V-Interoperability Phase 2 Volume 3	Vehicle Level	Dynamic Vehicle: Simulated Implausible Messages

ID (Ph. I)	Requirement	DSRC Element	Operational Objective	Source	Compliance Approach	Compliance Test Procedure
	trajectory within 2 sigma based on the received BSMs). If such a message fails the level 2 plausibility check, the OBE shall not raise an alert to the driver on the basis of that message and shall prioritize the message for misbehavior reporting			Report: Similar concepts discussed in 4.2.2 Proximity Plausibility - "a Host Vehicle (HV) attempts to identify a locally misbehaving vehicle that, when considered in the context of the HV and its RVs, is either partially or wholly occupying the same physical space as that of the HV and/or its RVs." 4.2.3 Motion Validation - "attempts to validate the reported position of a transmitting vehicle based on a model which takes into consideration the previously reported velocity and heading values of the vehicle." See Appendix E for the full recommended requirements matrix with more information		
81	The OBE shall have the processing capacity to perform level 1 plausibility checks on at least 5500 BSMs per second	System	Trust	New requirement derived by BAH. The OBE should be able to process the number of BSMs based on the capacity of the channel. 5500 BSMs is based on the channel capacity in a 20 MHz channel, 18 Mbps data rate, 300 byte message taking up 192 microseconds of channel time. Level 1 plausibility checks must be done on all arriving messages, and since in the worst case there could be as many as 550 vehicles in range, then at 10x per second per vehicle the system must be able to handle 5500 messages per second	Vehicle Level	Dynamic Vehicle: Simulated Implausible Messages
1016	The OBE shall have the processing capacity to perform level 2 plausibility checks on at least 200 BSMs per second	System	Trust	New requirement derived by BAH - 200 corresponds to about 20 of the closest or fastest closing vehicles (those that represent the greatest potential for threats	Vehicle Level	Dynamic Vehicle: Simulated Implausible Messages
1018	The OBE shall log within a misbehavior report (a) any message that (1) results	System	Trust	New requirement derived by BAH because any message that indicates a false positive is	Vehicle Level	Dynamic Vehicle:

ID (Ph. I)	Requirement	DSRC Element	Operational Objective	Source	Compliance Approach	Compliance Test Procedure
	in a warning or (2) would result in a warning but failed a level 2 plausibility check, or (b) any set of 10 continuous BSMs from the same vehicle that has consistently failed plausibility Level 1 checks			a potential misbehaving message. If the vehicle does not have the capability to determine false positives, the vehicle should log all messages that indicate a warning because warnings should actually be a rare occurrence which should not overwhelm the Misbehavior Authority. Also, the OBE should not necessarily report a single implausible message because the vehicle may not be misbehaving. However, a set of 10 sustained and continuous implausible BSMs from the same vehicle probably represents an instance of misbehavior		Simulated Implausible Messages Dynamic Vehicle: Simulated Signature Failure
1019	The OBE shall perform intrusion detection activities and shall flag as misbehaving any message detected as intruding	System	Trust	New requirement derived by BAH for a manufacturer to specify how the device handles received messages and interfaces to the vehicle such that the OBE and other vehicle system intrusions are not possible via received messages (with or without secured content). Note: intrusion attacks occur prior to the DSRC security mechanisms	None	None
1007	If a message fails any misbehavior check, the OBE shall flag the source of misbehavior and include the appropriate data (as identified by CAMP report, SCMS design document, and security requirements) in the misbehavior report	System	Trust	V2V-Interoperability Phase I Report: Table 12 and Table 16 - Lists similar potential sources of misbehavior/implausibility and thresholds V2V-Interoperability Phase 2 Volume 3 Report: Section 5 Reporting - Discusses similar misbehavior report situations, report types, and required reporting data	Vehicle Level	Dynamic Vehicle: Simulated Implausible Messages Simulated Signature Failure
1006	The OBE shall verify (i.e., check revoked certificates, verify signature, and verify certificate) at least all received messages that have been validated	System	Trust	V2V-Interoperability Phase 2 Volume 3 Report: 4.3 Combined Local Misbehavior Detection (LMBD) Concept, states as a potential method for verification "A threat-	Vehicle Level	Dynamic Vehicle: Simulated Signature

ID (Ph. I)	Requirement	DSRC Element	Operational Objective	Source	Compliance Approach	Compliance Test Procedure
	through plausibility tests and that result in a safety warning (verify on demand) (and flag for misbehavior reporting if the message fails verification)			detected processing state in which the authenticity of messages that have been identified as potential threats based on the safety application threat checks is verified to ensure the message is being transmitted by a trustworthy source." The BAH team believes this method should be used when verifying messages Other relevant sources: IEEE 1609.2 Section 5.3.6: Verify signed data, Section 5.5: Validity of signed communications		Failure
1003	The OBE shall send saved misbehavior reports to Misbehavior Authority when connectivity is available	System	Trust	Communications Data Delivery System (CDDS) Analysis for Connected Vehicles Report: Similar misbehavior reporting to the SCMS is mentioned throughout CAMP V2V-I Phase 2, Volume 3: Security Research for Misbehavior Detection Report: Similar reporting to the Misbehavior Authority is mentioned throughout	Vehicle Level	Simulated RSE Encounters: Simulated Misbehavior Report Transaction
18B	The maximum request/response transaction between the OBE and remote system management servers (e.g., SCMS [via the LOP], and software update servers) establishment time shall be less than 10 seconds. A request/response transaction shall be considered to be "established" when the transaction can be resumed, or continued at a subsequent RSE encounter (i.e., sufficient data has been exchanged to support either data	System	Communicate	New requirement derived by BAH which assumes a minimum encounter time of about 10 seconds, so that the basic transaction can be established in a single encounter between the OBE and an RSE. Roughly 60 mph in the RSE radio footprint Aftermarket Safety Device Certification Test: “Supplier B” Platform Test Report, May 2013: Security Copy Protocol (SCP) used to transfer various sized files from a simulated SCMS server via a 24’ elevated RSE and	Vehicle Level	Simulated RSE Encounters: Simulated Certificate Request Simulated RSE Encounters: Simulated Certificate Delivery I (Complete

ID (Ph. I)	Requirement	DSRC Element	Operational Objective	Source	Compliance Approach	Compliance Test Procedure
	exchange or resumption of data exchange at a later RSE encounter)			DSRC/IPv6/backhaul (fiber optic) communications link. Supplier B OBE receives the first WSA at approximately 750 meters and establishes the IPv6 link with the RSE at 670 meters at 20 mph (about 8 seconds). Results support requirements for server connections established within 10 seconds. However larger files took longer than 10 seconds to download which requires supporting service interruptions		Transaction)
18A	Request and Response transactions between the OBE and remote system management servers (e.g., SCMS [via the LOP], and software update servers) shall support service interruptions such that the transaction can be continued during a subsequent connectivity event (e.g., RSE encounter)	System	Communicate	New requirement derived by BAH: The OBE and SCMS must be able to stop and re-start transactions. This is session-less but the state needs to be maintained by the server (how many increments this package has) and the client (how many increments of this package do I have) See Appendix E for the full recommended requirements matrix with more information	Vehicle Level	Simulated RSE Encounters: Simulated Certificate Delivery II (Resumed Transaction)

Summary of Existing Supporting Standards and Research

While updating the use cases, failure scenarios, and performance measures in the Phase I report, the Booz Allen team reviewed existing standards and research related to DSRC operations and performance. If there were reliable sources of research to justify the initial requirement areas, the team cited the research as the source of justification (as seen in the condensed list of requirements within the previous section). If the team determined that potential requirement areas needed further research, a test and or simulation plan was created and executed to better understand the issue and develop new, empirically-based recommended requirements.

The subsections below contain summaries of the existing standards and research used to support recommended communications performance and security requirements.

4.1.2 Existing Standards

In this project, the Booz Allen team wanted to list all necessary requirements, some that exist today and some that do not. One of the first steps to accomplish this goal is to fully understand the current DSRC standards and requirements. The team reviewed existing standards and requirements to:

- Align recommended performance measures and requirements from Phase I, and those anticipated as being part of the final set, to existing standards
- Determine areas of uncertainty in DSRC performance needs and capabilities that require further research

The following standards are already fully developed by organizations with internal processes in place to amend and update as necessary. Industry accepts and adheres to these standards in developing wireless communication and DSRC devices that conform to them. As described in Section 7.12, as part of its overall performance requirements, the USDOT could consider a rulemaking requirement that all OBEs comply with these industry standards with the exception of certain specified sections and clauses. It is noted in the condensed set of requirements and the full set in Appendix E. Full DSRC OBE Recommended Performance Requirements Matrix where the exceptions to these standards exist.

Table 2: Existing DSRC Standards

Existing Standard	Description / Relevance
IEEE 802.11: Standard for Wireless Local Area Network (LAN) MAC and Physical Layer (PHY) Specifications	This standard describes information exchange between systems local and metropolitan area networks. It also describes specific requirements for Wireless LAN MAC and PHY specifications.

Existing Standard	Description / Relevance
(2012)	
IEEE 1609.2: Standard for WAVE – Security Services for Applications and Management Messages (2016)	This standard describes secure message formats and processing for use by WAVE devices, including methods to secure WAVE management messages and methods to secure application messages. It also describes administrative functions necessary to support the core security functions.
IEEE 1609.3: Standard for WAVE – Networking Services (2016)	This standard describes WAVE Networking Services to WAVE devices and systems, including Layers 3 and 4 of the open system interconnect (OSI) model and the IP, User Datagram Protocol (UDP), and Transmission Control Protocol (TCP) elements of the Internet model. The standard also describes management and data services within WAVE devices.
IEEE 1609.4: Standard for WAVE – Multi-Channel Operation (2016)	This standard describes multi-channel wireless radio operations, WAVE mode, MAC, and PHYs, including the operation of control channel (CCH) and service channel (SCH) interval timers, parameters for priority access, channel switching and routing, management services, and primitives designed for multi-channel operations.
IEEE 1609.12: Standard for WAVE – Identifier Allocations (2016)	This standard describes the use of these identifiers, indicates identifier values that have been allocated for use by WAVE systems, and specifies the allocation of values of identifiers specified in the WAVE standards.
SAE J2735: DSRC Message Set Dictionary (2015)	This standard comprises a complete list of all dialogs (messages exchanges), messages, data frames (complex elements), and data elements (atomic elements) which are used in the DSRC message set.

4.1.3 Existing Reports and Research

Along with reviewing existing standards pertaining to DSRC communications performance, security, and BSMs, the Booz Allen team assessed additional existing reports and research relevant to DSRC communications performance and security requirements. The focus of these reviews were to:

- Review current research findings and communications performance requirements recommendations
- Review current SCMS and security operations design
- Determine areas of uncertainty in DSRC performance needs and capabilities not fully characterized by existing research that require data collection testing and simulation within this project

The team sought existing research by focusing on reports and documents from standards organizations (e.g., IEEE, SAE), industry (e.g., CAMP, Car2Car), academia, and other government-commissioned studies. From these reports and studies, the team updated the use cases, failure scenarios, and performance measures developed during Phase I to reflect new research. However, the team also identified multiple areas of uncertainty in regard to the actual capabilities of the DSRC network and possible requirements to ensure consistent and efficient network performance. The team determined that these areas of uncertainty required additional testing to fully characterize and gather sufficient data to justify communications performance requirements. Table 3 lists and describes the reports and documents that were most beneficial to developing communications performance and security requirements, along with formulating a data collection testing and simulation plan to justify new requirements. Appendix I. Overview of Cybersecurity Guidance and Best Practice Management in Other Industries contains a full list of the reports and studies assessed during this project.

Table 3: Core Existing DSRC Reports and Related Research

Existing Report / Research	Description / Relevance
CDDS for Connected Vehicles (Booz Allen), May 2013	This report describes analyses conducted to evaluate different options for the communications network needed for eventual implementation of the connected vehicle system, including CV system design, network option capabilities, certificate revocation, cost modeling, and policy, organizational, and institutional requirements for multiple scenarios. The Booz Allen team referred back to the CRL Analysis portion of the report as an input when developing requirements focused on misbehavior.
Development of DSRC Device and Communication System Performance Measures: Analysis of DSRC Operational Needs and Performance Measures (Booz Allen), January 2014	This report is the predecessor to this current project. The report is commonly referred to as “Phase I” while this report is “Phase II.” The Booz Allen team used the Phase I report and artifacts as the starting point for developing the requirements and compliance tests recommended in this report.
Interoperability Issues of Vehicle-to-Vehicle Based Safety Systems Project (V2V-Interoperability) Phase 1 Final Report (CAMP), April 2014	This report describes the first phase of CAMP testing and findings completed to address DSRC technical issues related to interoperability, scalability, security, and data integrity and reliability. This report was of particular interest to the Booz Allen team because testing was conducted to characterize areas of uncertainty such as hidden terminal and congestion effects. While the data was informative, the Booz Allen team determined it necessary to conduct its own tests to characterize hidden terminal and congestion effects with different variables and controls.
Interoperability Issues of Vehicle-to-Vehicle Based Safety Systems Project (V2V-Interoperability) Phase 2 Final Report Volume 1 – Communications Scalability for V2V Safety Development (CAMP), February 2015	This report presents Volume 1 of the Phase 2 Final Report for the V2V-Interoperability Project. This phase increased the scale of Phase I testing and incorporated simulations to emulate up to 6000 OBEs in congested and hidden terminal environments. The three primary transmission control protocols (i.e., Baseline, Algorithm X, and Algorithm Y) were enhanced in an attempt to improve their performance in congested environments beyond those analyzed in Phase 1. These transmission control protocols were applied during tests and simulations to assess performance impacts. The Booz Allen team used the report to compare the performance of CAMP transmission control protocols against the performance improvements of adjustments to data rate and transmission control protocols tested during this project.
Interoperability Issues of Vehicle-to-Vehicle Based Safety Systems Project (V2V-Interoperability) Phase 2 Final Report Volume 3 –	This report introduces potential methods of addressing misbehavior within a V2V network. Misbehavior detection was separated into two smaller processes defined as LMBD and global misbehavior detection (GMBD). The team identified definitions and assumptions which helped set the scope of work and identify potential

Existing Report / Research	Description / Relevance
Security Research for Misbehavior Detection (CAMP), November 2014	misbehavior detection methods. The team also performed an analysis of a subset of attacks developed in previous CAMP projects which were deemed relevant for current safety applications. The attack analysis was used as input to develop potential LMBD and GMBD methods described in the report. The Booz Allen team reviewed the report to identify any gaps in the list of threats and plausibility related requirements.
Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application (NHTSA), August 2014	This report explores technical, legal, and policy issues relevant to V2V, analyzing the research conducted thus far, the technological solutions available for addressing the safety problems identified by the agency, the policy implications of those technological solutions, legal authority and legal issues such as liability and privacy. The Booz Allen team reviewed this report to assess areas of uncertainty, especially in regard to communications performance and security requirements, and policy implications of possible future requirements.
Vehicle-to-Vehicle Safety System and Vehicle Build for Safety Pilot (V2V-SP) – Final Report, Volume 2 of 2: Performance Testing, April 2014	This report describes performance and test results of V2V safety communications, based on DSRC and the use of the GPS. The performance tests were conducted in various regions of the US under real-world conditions in both rural and urban settings. The system components evaluated were inter-vehicle communications, which was based on DSRC, relative positioning, and V2V safety applications in-lane target classification. The Booz Allen team coordinated with CAMP and VTTI to access performance data from this project to develop a propagation model used to calibrate Opnet simulations.
Vehicle-to-Vehicle Systems Engineering and Vehicle Integration Research for Deployment (V2V-SE): On-board Minimum Performance Requirements for V2V Safety Systems (CAMP) Version 1.0, December 2014	This report provides the MPRs for an on-board V2V safety communications system capable of transmitting the SAE J2735 defined BSM over a DSRC wireless communications link as defined in the IEEE 1609 suite and IEEE 802.11 standards. The MPR addresses the on-board system needs for ensuring the transmission of BSMs in V2V safety communications provides the desired interoperability and data integrity to support the performance of the envisioned safety applications. The Booz Allen team reviewed this report to understand CAMP's minimum performance requirement recommendations. The Phase II report focuses on communications performance and security requirements in addition to those recommended by CAMP, which focus on what to implement from existing standards.
VSC-A (CAMP), August 2011	This report and associated appendices describe the development and testing of communications-based vehicle safety systems to determine if DSRC, in combination with vehicle positioning, can improve upon autonomous vehicle-based safety systems and/or enable new communications-based safety applications. The Booz Allen team reviewed the report and appendices to analyze test findings and recommended performance requirements, particularly those related to positioning, transmit power and antenna gain, and security.

Existing Report / Research	Description / Relevance
Vehicle Safety Communications – Applications: Multiple On-Board Equipment Testing (SAE/CAMP), April 2011	This paper focuses on scalability testing conducted during the VSC-A Project. A preliminary, multiple OBE testing effort was undertaken utilizing up to sixty DSRC radios to analyze PER and Inter-Packet Gap (IPG) distribution in multiple channel configurations and transmit characteristics with the goal of understanding DSRC communications performance of a large number of vehicles in congested traffic conditions. The Booz Allen team reviewed this report to understand CAMP testing that focused on congestion characterization and mitigation which influenced the data collection testing plan and performance requirement recommendations aimed at mitigating congestion effects.
Aftermarket Safety Device Certification Test: “Supplier B” Platform Test Report, May 2013	The Booz Allen Team consulted Section T IPv6 Data Packet Range and Transfer Test of the “Supplier B” Platform test report. This section outlines the field testing procedure for communication ranges. Specifically, different size files transfers are conducted, WSA detected distance is evaluated, and the connection established distance is verified.

Data Collection Tests and Simulations

As noted above, as the team developed categorical requirements, based on use cases, and reviewed existing research to see where existing requirements could be referenced. The team developed several requirement areas for the DSRC device for safety applications that do not currently exist. In order to recommend empirically sound metrics and requirements for these areas, the team developed a data collection and simulation plan. The tests and simulations were designed to understand what levels of requirements could be recommended for some of the needs of the system. Tests were conducted at multiple areas including field tests on the SmartRoad at Virginia Tech Transportation Institute and lab tests at Turner-Fairbank Highway Research Center and Petaluma, California. Simulations were conducted in Booz Allen Hamilton simulation environments. The findings of the tests and simulations are embedded in the recommended requirements, and noted in the tables above and in Appendix D. Data Collection Testing and Simulation Analysis.

Key objectives for the test and simulation were to more fully understand the options and tradeoffs associated with various communication parameters available in the DSRC system. For example, most prior DSRC assessments and field tests have been carried out using a 6 Mbps data rate in a 10 MHz channel (this is the current CAMP baseline). It is well understood that at this data rate channel congestion is a serious issue. The channel time for a 300 byte message at 6 Mbps is about 488 microseconds, which means with perfect Carrier Sense Multiple Access (CSMA) performance the system can support at most 204 vehicles transmitting BSMs at 10 Hz. Since dense traffic environments will often have 2 to 3 time this density within the range of any given DSRC device, the occurrence of message losses due to channel congestion is highly likely. Higher data rates should mitigate this issue (due to lower channel time per message), but some tests have indicated that the use of rates as high as 12 Mbps in a 10 MHz channel might result in poor range performance, although there has been somewhat limited documentation of any such tests.

It was also determined that the 6 and 12 Mbps data rates have what is known as “half rate coding,” so the error correction added to the data stream reduces the data rate by 50% from that which would otherwise be achieved for the selected modulation scheme (Quadrature Phase Shift Keying [QPSK] for 6 Mbps and 16 Quadrature Amplitude Modulation [QAM] for 12 Mbps). This coding was intended to support error correction in long packets (up to the maximum allowed by IEEE 802.11, which is 4,095 Bytes). However, the DSRC and IEEE 802.11 standards also allow for ¾ rate coding, which would result in a 9 Mbps data rate at QPSK modulation and an 18 Mbps data rate using 16 QAM. This lower coding rate may still provide acceptable performance for V2V communication because the BSM is relatively short (about 300 bytes), so extensive coding may not be necessary to assure reliable communication. These optional data rates have not been formally tested.

Of particular interest is that the range behavior of the DSRC system depends heavily on the modulation used, so it was expected that, for example, a 10 MHz channel should exhibit similar range performance for 6 Mbps compared with 9 Mbps and for 18 Mbps compared with 12 Mbps (higher order modulations for higher data rates require higher signal to noise ratio (SNR), and thus, at a given SNR higher order modulations will exhibit lower range performance). So, a first objective was to determine how the performance of 9 Mbps and 18 Mbps data rates in a 10 MHz channel would compare with 6 Mbps and 12 Mbps in the same 10 MHz channel.

In addition, the IEEE 802.11 standards allow for the use of 20 MHz channels. DSRC standards include two 20 MHz channels (channels 175 and 181). These have been little used because they overlay two 10 MHz channels and potentially create adjacent channel interference for envisioned V2I applications. If used for V2V, the existing 20 MHz channel allocations in DSRC standards would be an inefficient use of the DSRC band. An alternative could be to create two new 20 MHz channels combining either the two lowest or two highest 10 MHz channels to create 20 MHz channels at 173 or 183. More research is needed to determine if a 20 MHz channel is a viable approach; however, if it is found that use of 20 MHz channels can significantly mitigate the congestion and interference issues, then the effort associated with changing FCC rules may be a reasonable price to pay[4]. Thus, a second objective was to determine how the performance of 12 Mbps and 18 Mbps data rates in a 20 MHz channel would compare with 6 Mbps and 9 Mbps in the same 10 MHz channel. From a theoretical perspective these two combinations of channel bandwidth and data rate are expected to be nearly equivalent in performance.

This subsection contains the description, rationale, results, analysis, and findings for each data collection test and simulation used to learn more about areas of uncertainty to help support requirements to increase system performance.

For complete testing and simulation results and analysis, refer to Appendix D. Data Collection Testing and Simulation Analysis.

[4] The use of 20 MHz channels is provided for in IEEE 802.11. These channels have not been studied in any significant depth. While the tests and simulations indicate that the use of 20 MHz channels can significantly reduce congestion and hidden terminal interference issues by supporting higher data rates without significantly impacting communications range, the BAH team recognizes that there are other technical, policy, and regulatory aspects that must be considered before such an approach could be adopted with confidence. The objective on this project was to determine if the 20 MHz channels (e.g., Channels 175 or 181) could be used for safety applications, and if so, how effectively they might support safety communications. These are the designated 20 MHz channels per FCC. It is highly unlikely either would be used for V2V because of channel inefficiency and adjacent channel issues so use of a 20 MHz channels will likely take a new band plan (to create channels 173 and 183). Additional considerations that may positively or negatively impact the use of 20 MHz channels are described in the comparison tables provided in this report.

4.1.4 High Level Findings

Table 4 aligns tests and simulations with the informed requirement categories and high level findings. Note that some of the data collection tests were designed to inform related simulations, which were then used to help develop requirements. Thus, the second column includes both requirement categories ("req.") and simulations ("sim."), as noted.

Table 4: High Level Data Collection Test and Simulation Findings

Data Collection Test or Simulation	Informed Requirement Categories or Simulation	High Level Findings
Range vs. Power and Data Rate (Test) (also refer to Appendix J)	• Power radiation and sensitivity envelope (req. and sim.) • Data rate (req.) • Congestion mitigation (req.) • Hidden terminal (sim.)	• Exhibited better range than expected: up to 885m at 6 Mbps and even 500m at 18 Mbps in a 10 MHz channel. Note that these ranges are in a best case, rural environment. Vehicles in urban environments will have much less effective range (~220 m) as discussed in Appendix J • Transition from 0% PER to 100% PER is generally very abrupt • Laboratory and field range tests indicate that using a 20 MHz channel bandwidth (e.g., Channel 175 or another 20 MHz channel if a new band plan is developed) allows use of higher data rates with good range performance (12 and 18 Mbps in a 20 MHz channel have similar range to 6 and 9 Mbps in a 10 MHz channel). These higher data rates significantly reduce channel congestion and hidden terminal issues
Time Sync and Stability (Test)	• Clock accuracy (req.) • Self-test (req.) • Congestion mitigation (req.) • Plausibility and hazard analysis (sim.)	• Supplier B units exhibit well controlled time values • Supplier A units exhibit significant time value drift and clock jitter • Both types of devices exhibited clock jitter on the order of 3-5 milliseconds which appears to be higher than expected, but is unlikely to produce significant collision warning errors
Capture Ratio / Hidden Terminal (Test)	• Data rate (req.) • Hidden terminal (sim.)	• Hidden node effects observed for all data rates tested (6, 9, 12, and 18 Mbps). However, somewhat higher data rates exhibited less interference • Hidden node zone/range decreases as data rate increases • Effects worsen as message rate increases (higher probability of colliding messages)
Congestion (Test)	• Data rate (req.) • Congestion mitigation (req,)	• PER with 22 nodes at 90 Hz (198 effective units): ○ Sync messaging is 50%

Data Collection Test or Simulation	Informed Requirement Categories or Simulation	High Level Findings
	• Congestion (sim.)	○ Async messaging is 10% • PER improves at higher data rates • PER is significantly better with async messaging than sync messaging
Transmit Power and Antenna Gain and Sensitivity Envelope (Simulation)	• Power radiation and sensitivity envelope (req.)	• Isotropic design is insufficient because of multipath fading • Envelope pitch angle of 10 degrees reduces multi-path fading and accommodates maximum grade differential based on emergency stopping distance at 20-80 mph
Congestion (Simulation)	• Data rate (req.) • Congestion mitigation (req.)	• Incremental increase of data rate from 6 Mbps to 9 Mbps in a 10 MHz channel and up to 18 Mbps in a 20 MHz channel greatly decreases PER in high vehicle density environments
Hidden Terminal (Simulation)	• Data rate (req.) • Congestion mitigation (req.) • Hidden terminal mitigation (req.)	• Hidden terminal effects observed in scenarios; effected zone decreases as data rate is increased • Hidden terminal effect increases at higher device densities • Hidden node collisions account for about 20% of message losses when congestion is included in simulation of open road situation
Plausibility and Hazard Detection Analysis (Simulation)	• Plausibility (req.) • Startup (req.) • Self-test (req.)	• BSM parameter errors (time, message, speed, etc.) have the potential to cause misclassification of safety events • Message losses (PER), even in the most extreme scenarios (high speed, deep urban environment), had a negative but minimal effect on collision detection outcomes

As illustrated in Table 4, the majority of testing and simulation focused on characterizing hidden terminal and congestion effects, along with mitigating those effects. The team found that higher data rates (i.e., 9, 12, and 18 Mbps) rather than 6 Mbps which is currently recommended by CAMP substantially reduced the PER caused by congestion and hidden terminals. Based on these tests, the team believes that using a 9 Mbps data rate in a 10 MHz channel and possibly a 12 or 18 Mbps data rate in a 20 MHz channel would greatly reduce the negative effects resulting from congestion and hidden terminals. The use of a 10MHz channel is currently accepted as the default channel bandwidth for DSRC safety communications. However, the FCC regulations, and the DSRC standards also define 20 MHz channels, and there are advantages and disadvantages based on the usage of various data rates and channel bandwidths. Table 5 describes at a high level the tradeoffs between the use of a 10 MHz and 20 MHz channel.
Table 6 breaks down the tradeoffs between the use of a 6 and 9 Mbps data rate in a 10 MHz channel and a 12 and 18 Mbps data rate in a 20 MHz channel.

In short, the possible options to consider for data rate and channel bandwidth:

- 10 MHz Channel with the use of a 6 Mbps and/or 9 Mbps data rate – Recommend 9 Mbps when using a 10 MHz channel
- 20 MHz Channel with the use of a 12 Mbps and/or 18 Mbps – Recommend 12 Mbps when the Channel Busy Ratio (CBR) is below 50% and 18 Mbps when the CBR exceeds 50%; such transmission shall continue until the CBR falls below 30% (Refer to the Validation Testing and Simulation section for additional information)

Table 5: Advantages and Disadvantages of 10 and 20 MHz Channels

	10 MHz Channel		20 MHz Channel	
	Advantage	**Disadvantage/ Risk/Threat**	**Advantage**	**Disadvantage/ Risk/Threat**
Congestion/ Throughput		Complex congestion control algorithm required (less necessary at 9 Mbps than 6 Mbps)	May completely address congestion issues (especially at 18 Mbps)	
Packet Error Performance	Multipath-induced fading verified to be sufficiently mitigated	Potentially significant packet errors due to congestion and hidden terminals	• Significant reduction in PER from congestion and hidden terminals • Expected net gain in performance considering congestion and multipath-induced fading • No significant difference in range with same modulation and coding – i.e., 6 Mbps/10 MHz and 12 Mbps/20 MHz have similar range	• Minor degradation may occur due to multipath fading in urban environments. **(Recommend additional testing)** • Performance for 20 MHz vs. 10 MHz may be indistinguishable in the V2V environment; original research and channel spacing plan focused on V2I; 20 MHz spacing was not formally considered for V2V
Standards	Essentially complete		20 MHz channels already defined in IEEE 802.11	Modifications needed for IEEE 1609, SAE J2735 and J2945
FCC Rules	No change required	See next row	Requires updated rules (to create a more efficient band plan)	See next row
Band Sharing	Decreases the possibility and effectiveness of band	Questionable detection reliability if band sharing (with IEEE 802.11ac) is	Higher detection reliability if band sharing (with IEEE 802.11ac) is	Increases the possibility and effectiveness of band sharing

	10 MHz Channel		20 MHz Channel	
	Advantage	Disadvantage/ Risk/Threat	Advantage	Disadvantage/ Risk/Threat
	sharing	mandated	mandated (assuming aligned band plans and channel spacing)	
Notice of Proposed Rulemaking (NPRM) and Rulemaking Schedule	Largely tested/vetted	Congestion control approach is complex and may draw significant commenting; may affect application performance	May completely address congestion control (especially at 18 Mbps)	• Requires additional data collection testing • Schedule delay
Suppliers		Limited (many Wi-Fi chipmakers are expected to discontinue support for 10 MHz channels); although, at least few suppliers will maintain support	Extensive (every Wi-Fi Alliance certified product must support 20 MHz channels)	

Note: Higher data rates would also give the system more flexibility to change cryptographic algorithms if necessary in the future. Quantum computers will eventually enable breaking the cryptographic algorithms currently used.

The technical impact (packet error performance) of going from 12 to 18 Mbps in a 20 MHz channel is essentially the same as going from 6 to 9 Mbps in a 10 MHz channel, but without the congestion issues.

Table 6: Advantages and Disadvantages of the 6 and 9 Mbps Data Rates in a 10 MHz Channel

	6 Mbps Data Rate (10 MHz Channel)		9 Mbps Data Rate (10 MHz Channel)	
	Advantage	Disadvantage/ Risk/Threat	Advantage	Disadvantage/ Risk/Threat
Congestion/ Throughput		Complex congestion control algorithm required	Significantly reduces congestion risks (less dependence on congestion control algorithms)	Congestion control still needed
Packet Error Performance	Longer range (the measured range of 6 Mbps is far greater than 300 m as required)	Increases impact of hidden terminal and congestion issues in crowded traffic environments	Shorter range may mitigate hidden terminal and congestion issues with little sacrifice of safety performance	• Shorter range (~20% reduction, but still much greater than300 m) • Insignificant performance

	6 Mbps Data Rate (10 MHz Channel)		9 Mbps Data Rate (10 MHz Channel)	
	Advantage	**Disadvantage/ Risk/Threat**	**Advantage**	**Disadvantage/ Risk/Threat**
			(range is sufficient)	degradation in urban environments (Recommend additional testing)
Standards	No changes required		Same as 6 Mbps	
FCC rules	No changes required	See next row	Same as 6 Mbps	
Band Sharing	Decreases the possibility and effectiveness of band sharing	Questionable detection reliability if band sharing (with IEEE 802.11ac) is mandated	Same as 6 Mbps	
Schedule	Largely tested/vetted		Reduced risks for congestion control	Recommend minor testing
Suppliers		Limited (many Wi-Fi chipmakers are expected to discontinue support for 10 MHz channels).	Same as 6 Mbps	

To further mitigate risk in a 10 MHz channel, 9 Mbps can initially be made optional on transmit and mandatory on receive, so the system can be upgraded to transmit at 9 Mbps later when needed due to congestion. All radios currently being used for implementation already support 9 Mbps and any future radios using the 9 Mbps transmit rate would be backward compatible with 6 Mbps. 6 Mbps could initially be mandatory for both transmit and receive operations. The signaling contained in the beginning of each individual IEEE 802.11 packet, which carries the BSM, indicates the data rate and all IEEE 802.11 receivers can dynamically switch to the indicated data rate.

4.1.5 Software Development to Support Data Collection Testing

For the data collection tests the team created a software based OBE management system with two parts:

- One, on the OBE itself, controls the configuration of the OBE through a socket interface.
- The second, in the test system, interacts with a collection of OBEs maintaining a list of registered OBEs and a means for addressing and controlling each OBE individually.

This system allows the test conductor to set the operating configuration of every OBE under test, and to stop and start message generation for any or all OBEs from a central test monitor computer.

When activated, each OBE creates individual logs of transmitted and received messages. The format for these messages is defined by the Turner-Fairbank Vehicle Technology Test Support System (VTTSS), which was used to provide an accurate time base for the test. The stereotyped message format provided by the Turner-Fairbank testbed allowed the team to use existing and newly created scripts, in the Python and Shell software programs, to analyze the data.

In order to run the tests the team also developed a test message, a test message generator, and a test message receiver. The test message consists of a 300 byte WSM with the following fields:

- 32 bit message ID;
- 64 bit timestamp;
- 32 bit vehicle ID;
- 32 bit message count (from transmitter);
- 32 bit longitude;
- 32 bit latitude;
- 76 bytes filler bits to make up 300 bytes.

While the message does not actually require 300 bytes of data, it was padded out to this size to more accurately reflect the size of the BSM, so that congestion tests will reflect the same basic level of channel congestion as a fleet of vehicles generating BSMs.

The test message generator software was configured using the OBE management system. It allows the test conductor to define broadcast channel, transmit power, PSID, message repeat rate, and channel data rate. Once configured, the message generator will generate test messages at the configured rate, and cause the outgoing messages to be logged. The test message generator includes a means for setting the offset time for each OBE to generate its BSM messages. This offset represents a fixed number of milliseconds after the PPS event at which the next BSM is generated. Since the team planned to carry out the tests at message repeat rates of 10 Hz, 40 Hz, and 90 Hz, the offsets were configured so that at the 10 Hz rate, the offset increment was 250 microseconds, and the maximum offset was 99.75 microseconds (thereby allowing units to randomly select from about 400 possible start increments. At 40 Hz and 90 Hz, these increments were scaled down to support the larger number of messages. The system also allowed for synchronous sending (that is, all units starting their BSMs synchronous with the PPS event). This was used for hidden terminal testing.

The test message receiver software is also configured using the OBE management system. It allows the test conductor to define reception channel and PSID. Once configured, the message receiver will accept messages form the DSRC stack, and submit them to the logging subsystem where they will be time and position stamped and logged.

4.1.6 Range vs. Power and Data Rate Test

4.1.6.1 Description and Rationale

The project team conducted measurements to characterize the performance of 5.9 GHz DSRC as a function of range (distance between DSRC-enabled vehicles) in an unobstructed environment. The corresponding Received Signal Strength (RSS) and PER measurements were used to inform other data collection tests and simulations, along with contributing to general communications performance requirements development.

The objective of the range testing was to measure the following performance metrics as a function of range:

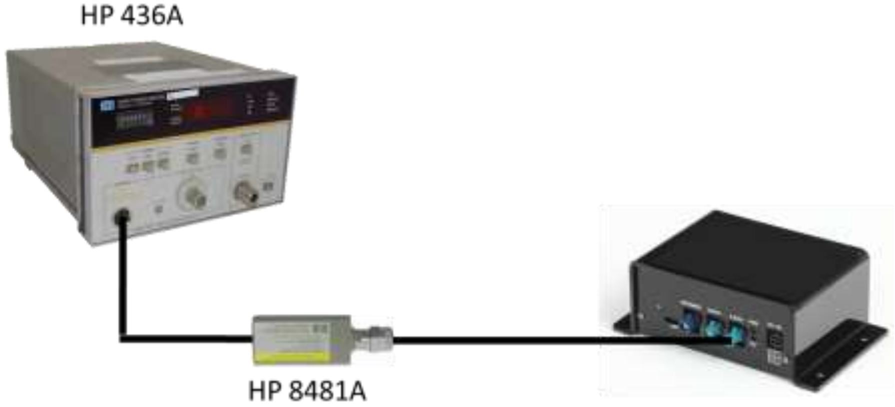
- Received power/signal strength (propagation loss)

- PER at data rates of 6, 9, 12, and 18 Mbps in a 10 MHz channel (and additional testing in a 20 MHz channel)

The received power/signal strength measurements were validated using standardized RF test equipment (a signal generator and a spectrum analyzer). Spectrum analyzer data was used as a baseline reference for measurements made with DSRC radios.

The first step was to verify the transmitter output power measurements of the DSRC radios. The team used a power meter and power sensor to accurately measure and validate the output power of the DSRC radios being used as the transmitters. Output power of both DSRC transmitters were measured individually prior to testing. The radios supported a special/continuous test mode used only for output power validation in this test configuration. Supplier A supports a maximum DSRC output power of +14 dBm and Supplier B supports a maximum of +20 dBm. For all testing in this plan, Supplier A was set to 10 dBm and Supplier B to 20 dBm.

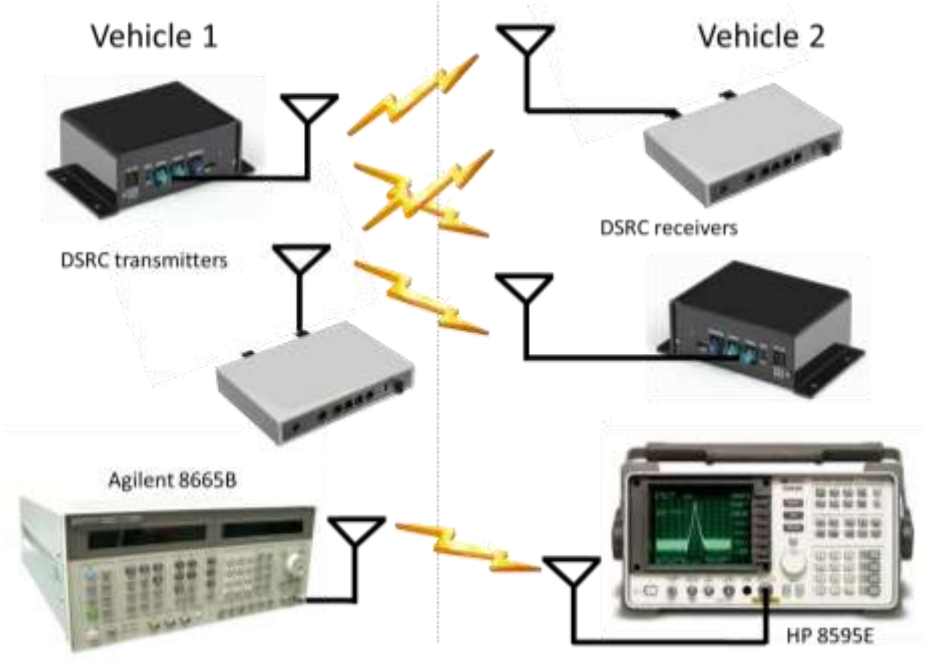
Figure 3: Measuring the Output Power of a DSRC Radio (Source: USDOT)



The signal generator and DSRC transmitters (one from each radio supplier) were installed in vehicle 1 (the measurements reference point). The spectrum analyzer and the DSRC receivers (one from each radio supplier for a total of two) were used in vehicle 2 to take multiple measurements at each incremental point in the range testing campaign.

The DSRC transmitters were configured to normal DSRC mode on channel (ch) 172 for this test configuration. Approximately 1000 300-byte test messages were transmitted at each range interval at 10 Hz for measuring signal strength and PER with the DSRC receivers. Each receiver in vehicle 2 supported special logging capabilities to log the signal strength and number of the data packets received from each of the DSRC transmitters at each range increment and each data rate. This data was post processed to determine the signal strength and PER (the percentage of the packets not received) versus range for each DSRC transmitter and receiver pair (two radio pairs total). External laptops (with corresponding test software) were connected to the DSRC radios to generate and log the transmitted and received packets.

Figure 4: Range vs. PER and Received Signal Strength Test Setup (6, 9, 12, and 18 Mbps) Test Setup (Source: USDOT)



After configuring the test setup as described in the previous paragraph and illustrated in Figure 4, the team began testing with vehicles 1 and 2 facing the same direction along the roadway (following vehicle scenario) with vehicle 2 twenty (20) meters in front of vehicle 1. Testers set the signal generator to transmit a Continuous Wave (CW) at 5.86 GHz and +13 dBm and logged the received power using the spectrum analyzer (SA Rx Pwr). After completing the measurements, the team turned off the signal generator to avoid interference with the DSRC radios. The team transmitted approximately 1000 DSRC packets at 10 Hz from vehicle 1 from each transmitter, Supplier A and then Supplier B separately, at 6 Mbps on channel 172 and used both DSRC receivers to log each received packet and its signal strength indicator for each transmitter/receiver pair. Testers repeated this test at the same range at 9, 12, and 18 Mbps data rates. The team moved vehicle 2 in 20 meter increments out to 950 meters and recorded received packets and RSS at each data rate.

After completion of the test, the data logged was imported into a spreadsheet for post processing and comparison with the logs from each DSRC receiver. For the signal strength measurements, the path loss derived from DSRC radio measurements was compared with the path loss as measured using the signal generator and spectrum analyzer. The team computed the path loss as measured by the DSRC radios by subtracting the received signal strength reported by each radio on vehicle 2 from the transmitted power of the corresponding radio on vehicle 1 for each packet and computing the average (mean) for all ~1000 packets. The DSRC units from each supplier differed in transmit power, but the measured path loss for all radio pairs were within a difference of less than 3 dB after factoring in antenna gains. Standard deviation was also captured as it may be useful in future analysis. Comparison of the means with baseline spectrum analyzer measurements provided accuracy characterization of the signal strength measurements by DSRC radios.

For the PER measurements, the percentage of the 1000 packets transmitted by each DSRC transmitter and not received for each range increment, data rate, and scenario was computed and logged alongside each signal strength measurement.

4.1.6.2 Results, Analysis, and Findings

VTTI Test Results

Preliminary results from the VTTI range testing and final results from the lab testing are provided below. The Supplier A tests are provided in Figure 5, and results from Supplier B are provided in Figure 6.

Figure 5: PER vs. Range and Data Rate (Supplier A) (Source: USDOT)

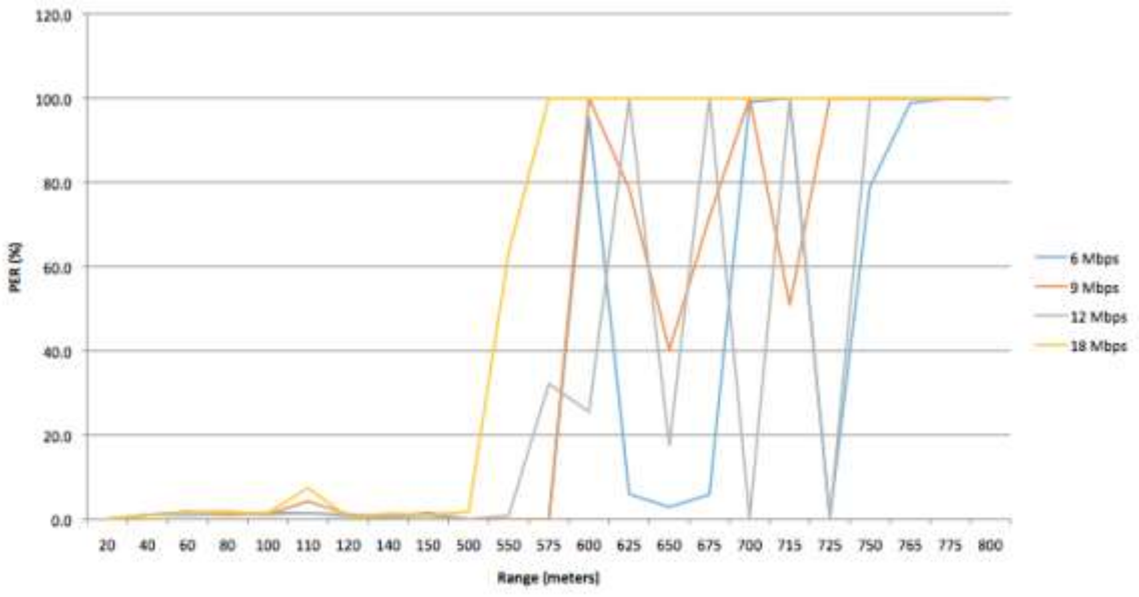
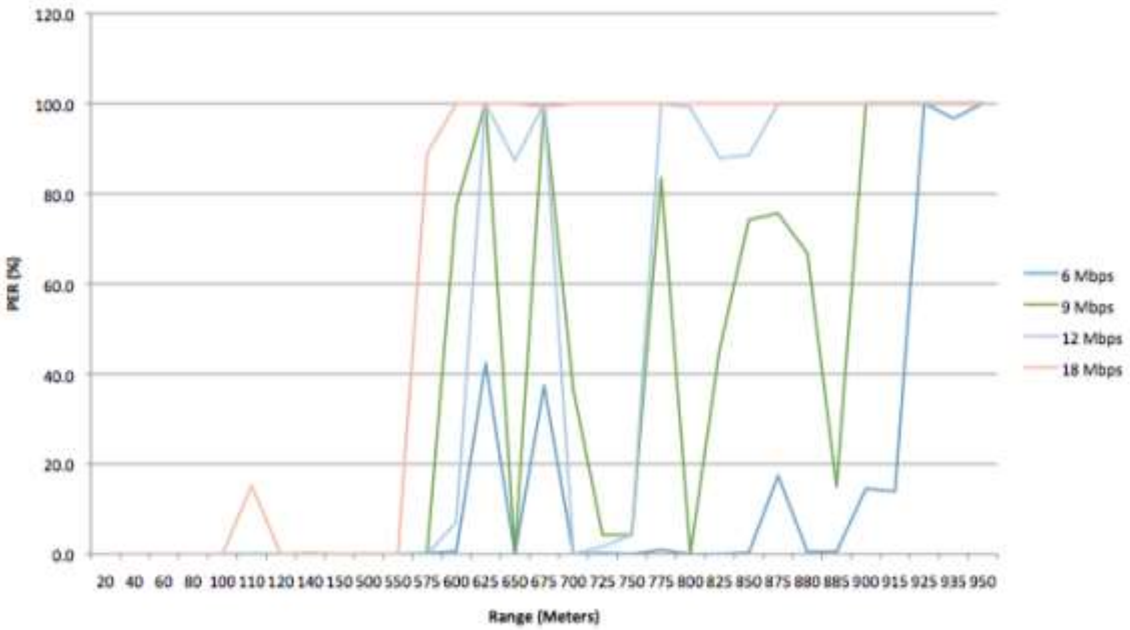


Figure 6: PER vs. Range and Data Rate (Supplier B) (Source: USDOT)



As can be appreciated from these figures, multipath is a serious factor in communications beyond about 500 meters range. Also note that these tests were performed in an open environment; the analysis shown in Appendix J. Analysis of Received Power vs. Range for Rural and Urban Environments indicates that the maximum range in an urban environment is approximately 220 meters.

The variation from near zero PER to nearly 40% or more at periodic intervals is representative of classic two ray multipath, which is what would be expected on the relatively flat open road at the VTTI facility. The dip between 100 meters and 120 meters at 18 Mbps is likely due to increased sensitivity to multipath fading at this higher modulation rate. The maximum “PER-Free range” (the range within which PER is below 20%), and the overall maximum range (beyond which PER is 100%) are summarized for the two types of units and for the various data rates in Table 7.

Table 7: PER Free and Max Ranges vs. Data Rate (Suppliers A and B)

Data Rate (Mbps)	Supplier A Ranges (Meters)		Supplier B Ranges (Meters)	
	PER Free	Max	PER Free	Max
6	575	750	600	915
9	575	725	575	900
12	550	750	600	775
18	500	550	550	550

20 MHz Channel Field Test Results

The Booz Allen team also conducted field tests in Petaluma, CA (originally planned to be conducted at SwRI during Validation Testing and Simulation) to further characterize OBE range and performance in a 20 MHz channel.

As described in Section 4.3.9, Congestion Simulation, when there are many vehicles communicating within range of each other, the probability of unsuccessful message transmission increases.

In previous simulations, the team assessed how different channel parameters might impact congestion. The team simulated and analyzed congestion performance at various data rates, different message transmission rates, and both 10 MHz and 20 MHz channel bandwidths in order to better understand the options and tradeoffs for managing congestion. The earlier range tests, however, were carried out before identifying the availability and possibilities of the 20 MHz channel.

This test was carried out to evaluate the performance of the DSRC units transmitting at higher data rates using the 20 MHz channel (Channel 175). These tests had been carried out earlier in the lab using Supplier B units (See below). This test was intended to perform these same evaluations in the roadway environment.

In this test 2000 packets were sent between a transmitter unit and a receiver unit and compared the number of packets received to the number sent to arrive at a PER for that range. The test was carried out in the lab using variable attenuators, and on a flat straight road using two vehicles located at specific ranges.

During initial testing at SwRI the team found that the units from Supplier B had been updated between the earlier tests and this test. Unfortunately, this update appears to have impacted the channel selection functions of these units, and most of the units on hand were only able to transmit on Channel 172. The team was able, however, to configure units from Supplier A to operate on both channel 178 (10 MHz) and channel 175 (20 MHz). These tests were carried out in Petaluma, California.

Initial Lab Test Results

PER vs. attenuation tests were initially carried out in a laboratory environment on units from Supplier B (did not test Supplier A units in this way because the tests were performed as part of the hidden terminal tests, and the Supplier A clocks were too unstable to support any level of message synchronization, so there was no representative hidden terminal performance data). Later tests were also performed using units from Supplier A.

The laboratory tests are unique in that they do not include any multipath effects (there are no ground reflections in the cabled environment), so the results are more pure, but less representative of real world performance.

Supplier B Lab Tests

Figure 7 shows the PER vs. range for the same 6, 9, 12, and 18 Mbps data rates as the field test data above. As can be appreciated from the chart, there is no multipath fading, and the maximum ranges are nominally the same as those observed in the field. For comparative purposes, these ranges are summarized in Table 8.

Figure 7: PER vs. Range and Data Rate Lab Test in 10 MHz Channel (Supplier B) (Source: USDOT)

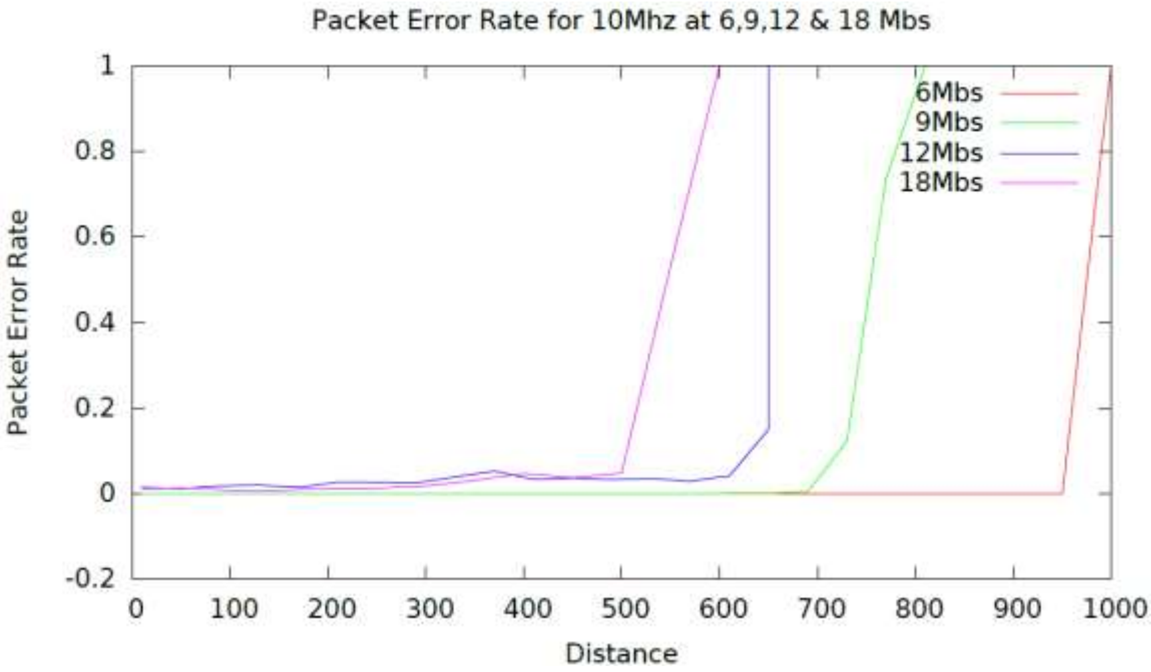


Table 8: Maximum Range for Supplier B, Lab Test vs. Field Test

Data Rate (Mbps)	Supplier B Lab Test Max Range (meters)	Supplier B Field Test Max Range (meters)
6	950	750
9	750	725
12	650	750
18	500	550

In addition, data was taken for the Supplier B unit using a 20 MHz channel. This data is shown in Figure 8 and Figure 9 in comparison to the 10 MHz channel performance.
Figure 8 shows the PER performance of the Supplier B unit at 6 and 12 Mbps in a 10 MHz channel, and at 12 Mbps in a 20 MHz channel. As expected, the performance of the unit at 6 Mbps in the 10 MHz channel is comparable to the performance at 12 Mbps in the 20 MHz channel.

Figure 8: PER vs. Range and Data Rate for 10 MHz and 20 MHz Channels (Supplier B) (Source: USDOT)

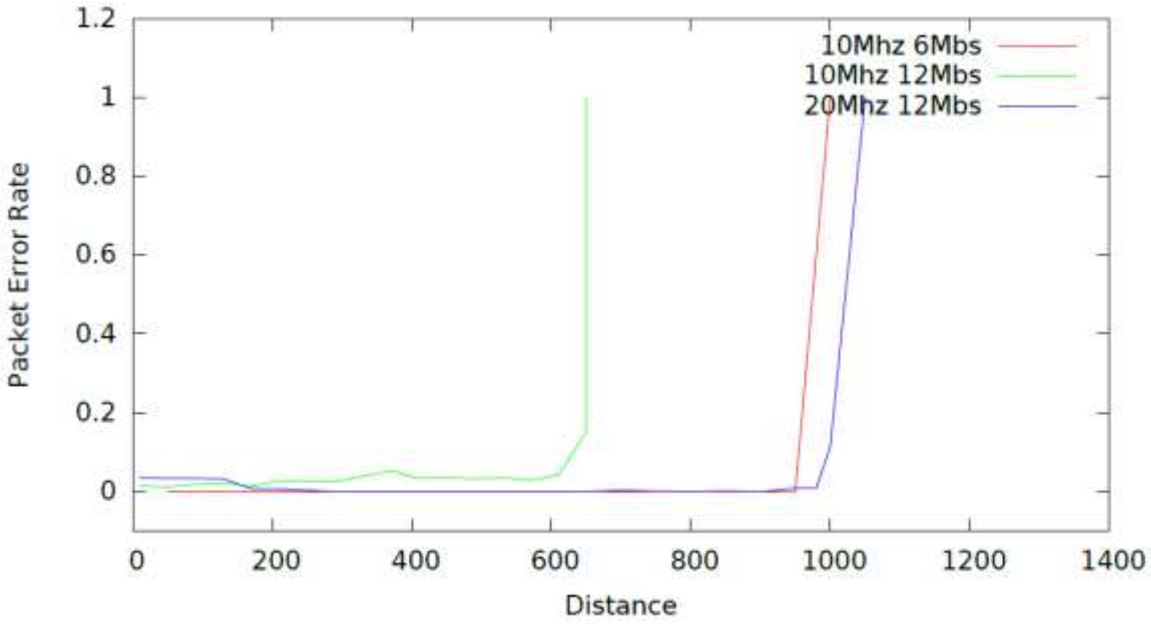
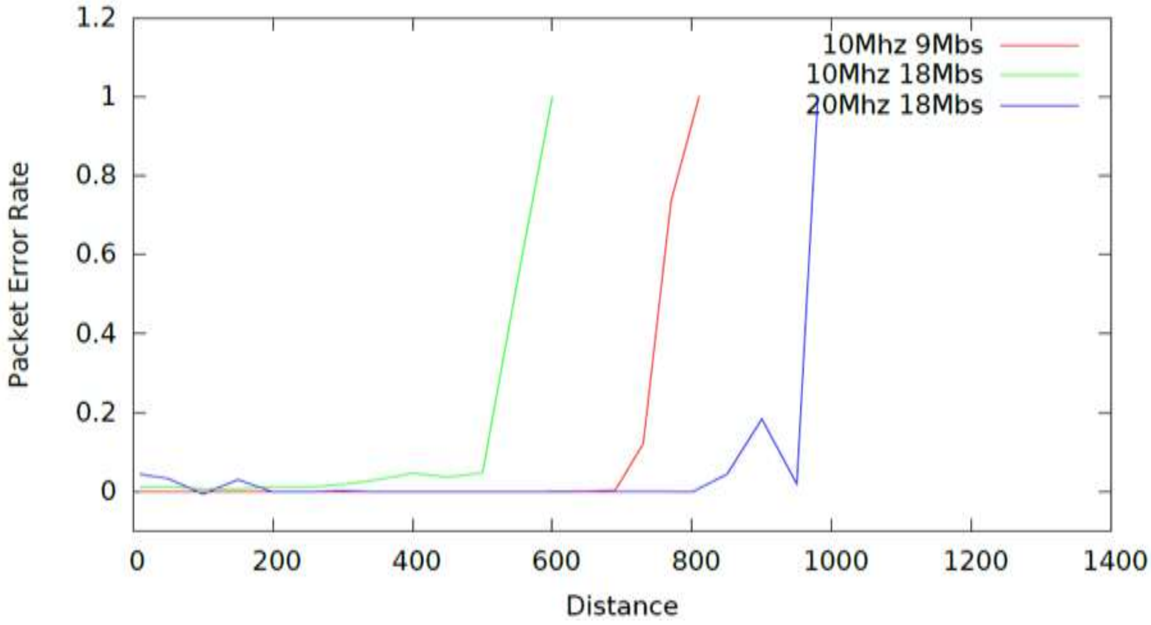


Figure 9 shows the PER performance of the Supplier B unit at 9 and 18 Mbps in a 10 MHz channel, and at 18 Mbps in a 20 MHz channel. The performance of the 20 MHz channel is slightly better than the same modulation at a lower data rate in the 10 MHz channel (10-9 vs. 20-18).

Figure 9: PER vs. Range and Data Rate for 10 MHz and 20 MHz Channels (Supplier B) (Source: USDOT)

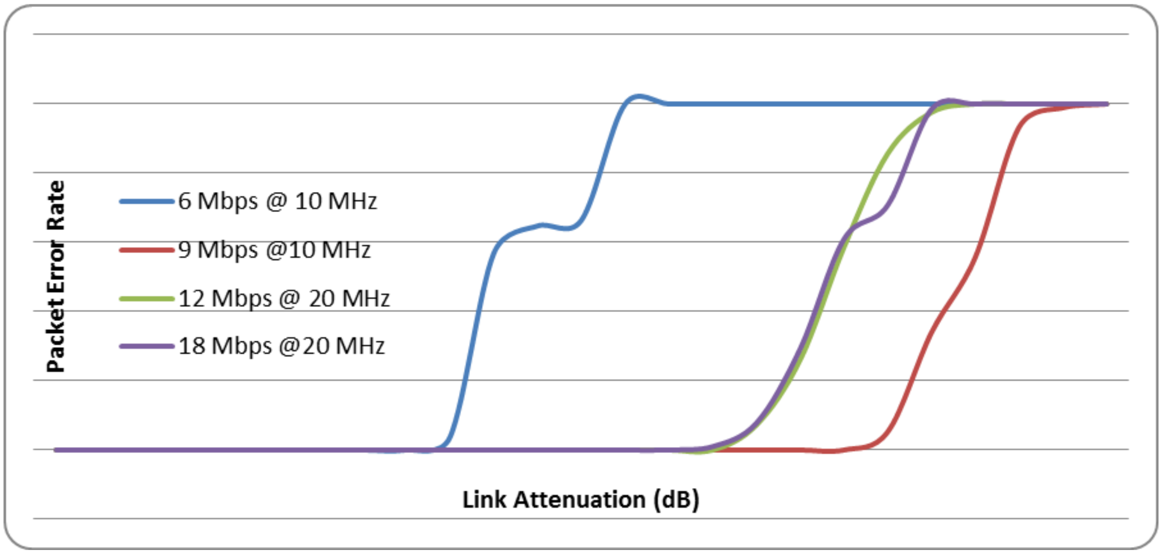


These results indicate that there may be advantages to using higher data rates to reduce congestion and interference, and possibly using higher bandwidth channels to offset the reduced range from the higher rates in a narrower 10 MHz channel. This is discussed in more detail in the following sections addressing congestion and interference.

Supplier A Lab Tests

Additional tests were carried out in the lab using units from Supplier A. For the 10 MHz tests, the team configured the transmitter to send on channel 178 (10 MHz) at 6 and 9 Mbps data rates. The signal level was adjusted using variable step attenuators. These tests were repeated at each attenuation level using channel 175 (20 MHz) and transmitting at 12 Mbps and 18 Mbps. The ratio of packets received to packets sent was recorded and plotted as shown in Figure 10 below.

Figure 10: Lab Test PER vs Link Attenuation (Supplier A) (Source: USDOT)



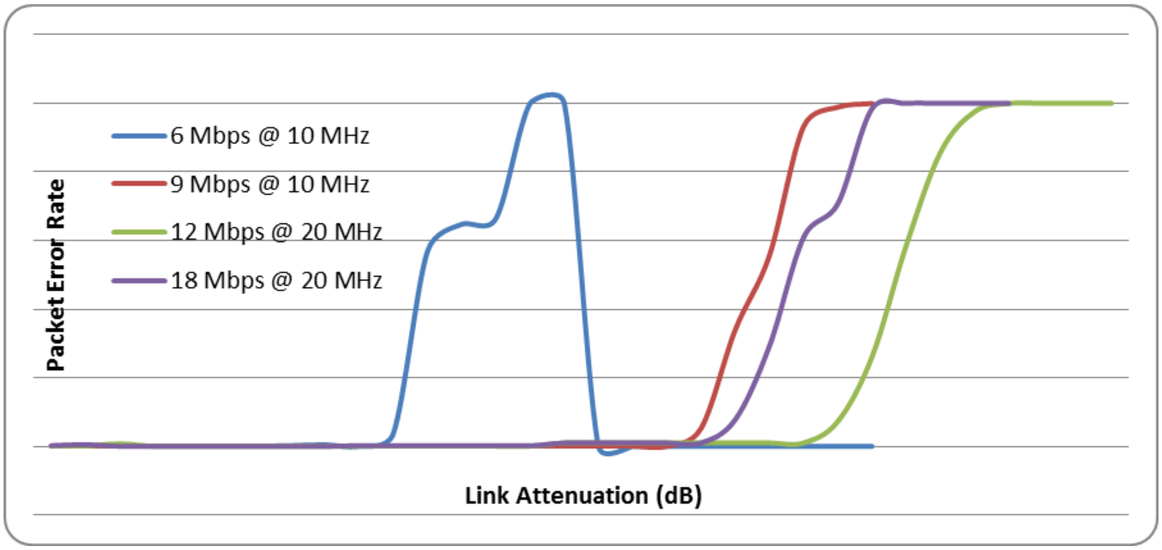
In these tests the team did not attempt to re-scale the attenutation levels to correspond to range since the objective was to compare the performance of the same unit operating with different combinations of data rate and signal channel (i.e., 10 MHz and 20 MHz).

This data was initially perplexing because it was expected that 9 and 18 Mbps would exhibit similar performance, and 6 and 12 Mbps would exhibit simiar performance. In followup tests, the team determined that the power output of the unit depended on both the data rate and the channel used. The difference in output power as a function of data rate was about 1-2 dB, but the difference between the 10 MHz and 20 MHz channels was between 5 and 7 dB. Figure 11 below represents the data from Figure 10 above normalized to a common power output level.

As can be appreciated from the figure below, 9 Mbps operating in a 10 MHz channel exhibits very close to the same perfromance as 18 Mbps operating in a 20 MHz channel. In addition, as expected by theory, 12 Mbps performs better than 9 Mbps and 18 Mbps due to the slightly higher noise immunity from the coding rate (1/2 rate coding vs. 3/4 rate coding).

The team was unable to explain the poor performance of these units operating at 6 Mbps in the 10 MHz channel. However, these units were known to have poorer range performance compared to other available DSRC terminals based on earlier evaluations. One theory is that there may be a firmware error in the units that causes errors when operating at 6 Mbps (none of the units were tested in earlier programs at anything other than 6 Mbps in a 10 MHz channel). As can be seen below, this anomalous behavior was also observed in the road tests.

Figure 11: Lab Test PER vs. Link Attentuation (Supplier A) Normalized Power Level (Source: USDOT)



This data indicates that the link performance of 9 Mbps in a 10 MHz channel is similar to 12 Mbps or 18 Mbps in a 20 MHz channel, and that (for these particular units) all of these performed better than 6 Mbps in a 10 MHz channel.

Supplier A Road Tests

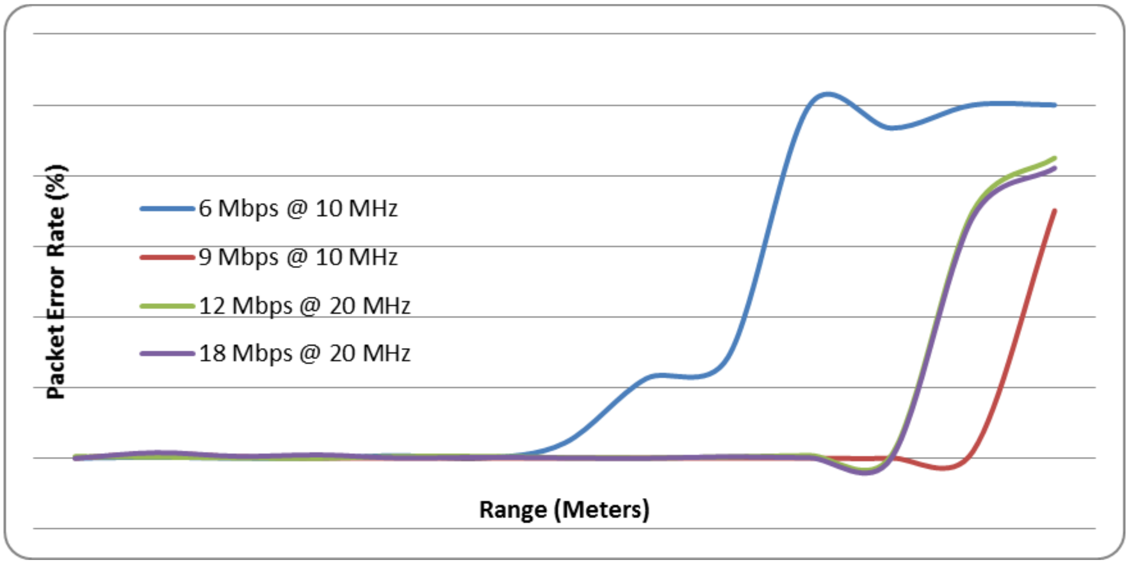
The team also performed tests of these units on the road. In these tests units were mounted to the roofs of two passenger vehicles and performed the same 2000 packet test as was performed in the lab. Instead of adjusting the link loss using variable attenuators, the team used the antennas provided with the units and varied the physical distance between the cars.

The results of these tests are shown in Figure 12 below. It is important to note that these results have not been normalized to account for the variation in output power level as a function of channel bandwidth and data rate. This means that they are comparable to Figure 11 above. It is assumed that were the output power levels adjusted to be the same, the results would be comparable to Figure 11 above. Note that the anomalous behavior of the 6 Mbps operation is also present in these road tests as well.

It is important to note that the absolute range values observed in Figure 11 are less important than the relative ranges between different combinations of channel bandwidth and data rate because the absolute range depends on the choice and orientation of the antennas.

The results do, however, indicate that, as was seen in the lab, higher data rates in the same channel bandwidth can be achieved by using lower levels of coding (e.g., 9 Mbps vs. 6 Mbps), and much higher data rates can be achieved using the wider channel bandwidth available (i.e., 20 MHz) in the DSRC standard. These tests were carried out on an open road without significant clutter, and with the vehicle stationary. Before a definitive conclusion can be drawn about the viability of these higher data rates, the team recommends additional testing to assess the behavior of this channel in these more difficult environments.

Figure 12: Road Test PER vs Range (Supplier A) (Non-Normalized Power Level) (Source: USDOT)



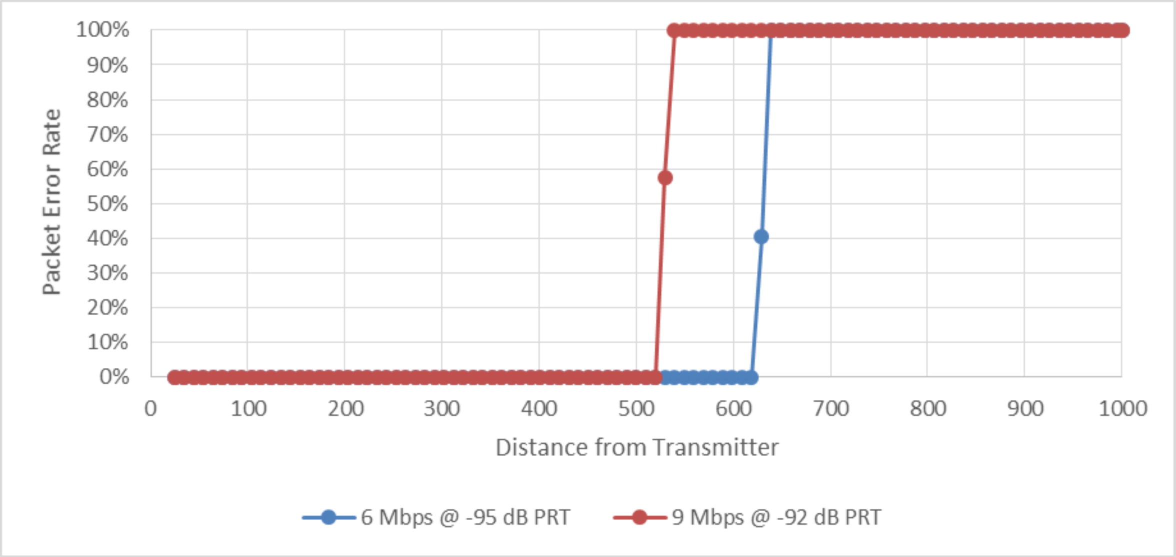
Simulation Results

The team also conducted PER vs. range and data rate simulations to compare results against the field and lab tests. The simulation consisted of two nodes, a transmitter and receiver. The receiver was set to move on a trajectory away from the transmitter to determine the changes in PER versus range. The figures that follow demonstrate the results of the following simulations for the two nodes:

- Varying the packet reception threshold between 6 Mbps & 9 Mbps
- Varying packet size at all data rates
- Varying antenna height to more closely align with the field test set-up

The following figure demonstrates the effective range for 6 Mbps and 9 Mbps data rates at -95 dB and -92 dB packet reception threshold, transmitting 300-byte packets. As it shows for 6 Mbps at -95 dB packet reception threshold, the transmission range is higher at about 619 meters compared to 520 meters for the 9 Mbps data rate at -92 dB, which is expected because the set power threshold is lower in the 6 Mbps case. Also note that, the results are binary (i.e., the PER is either zero or 100%). This is because the way the simulation is set up, no factor other than the power-loss is contributing to PER. The packets are all accepted up until the set power threshold and once the power goes below the threshold, the packets are considered a loss.

Figure 13: PER vs Distance – Varying Packet Reception Threshold (Source: USDOT)



The two figures below demonstrate the PER values for different data rates and for different packet sizes. Changing the packet size does not make a noticeable difference in the PER vs. range values. The 6 and 9 Mbps data rates result in almost the same plot for both cases. The determining factor is power loss and not packet size.

Figure 14: PER vs Distance – 10 Byte Packets (Source: USDOT)

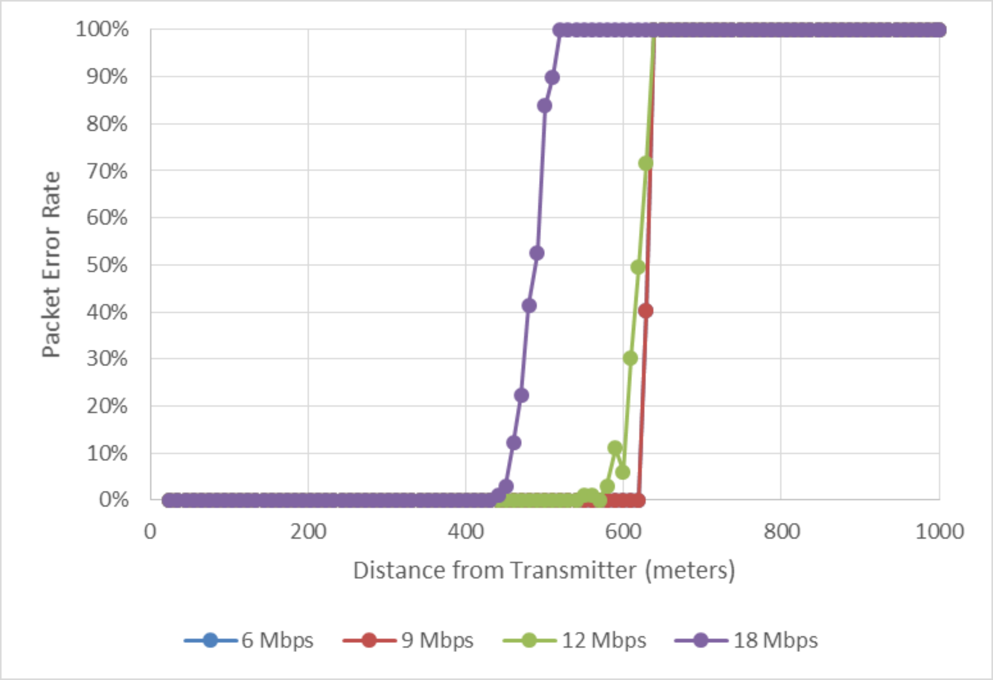
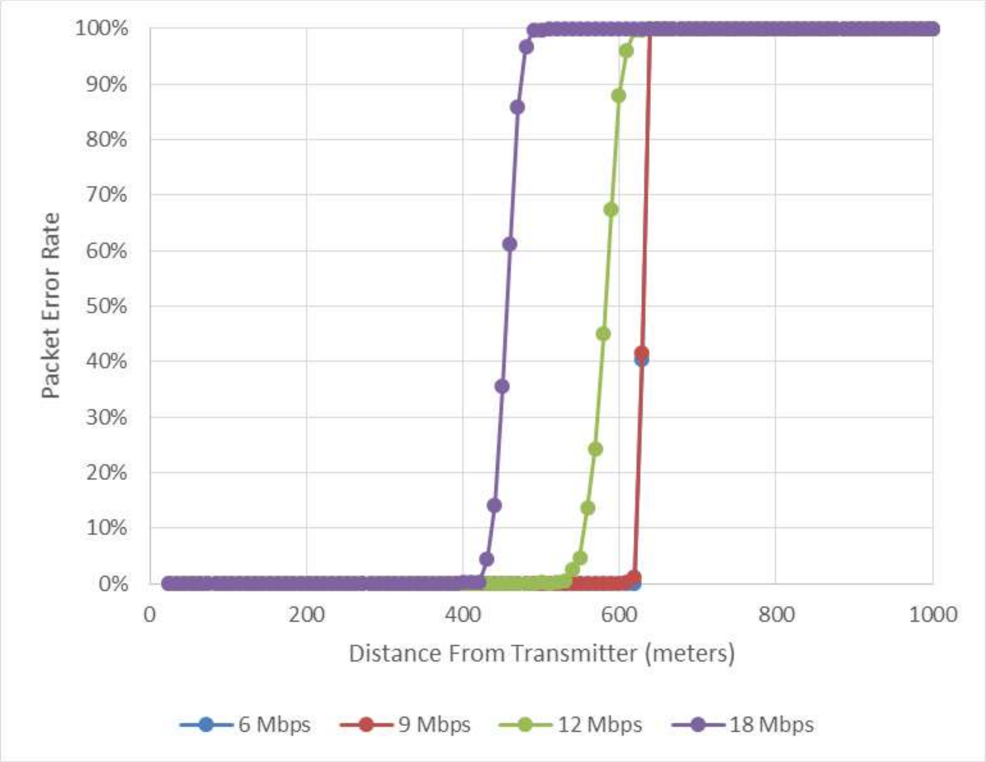
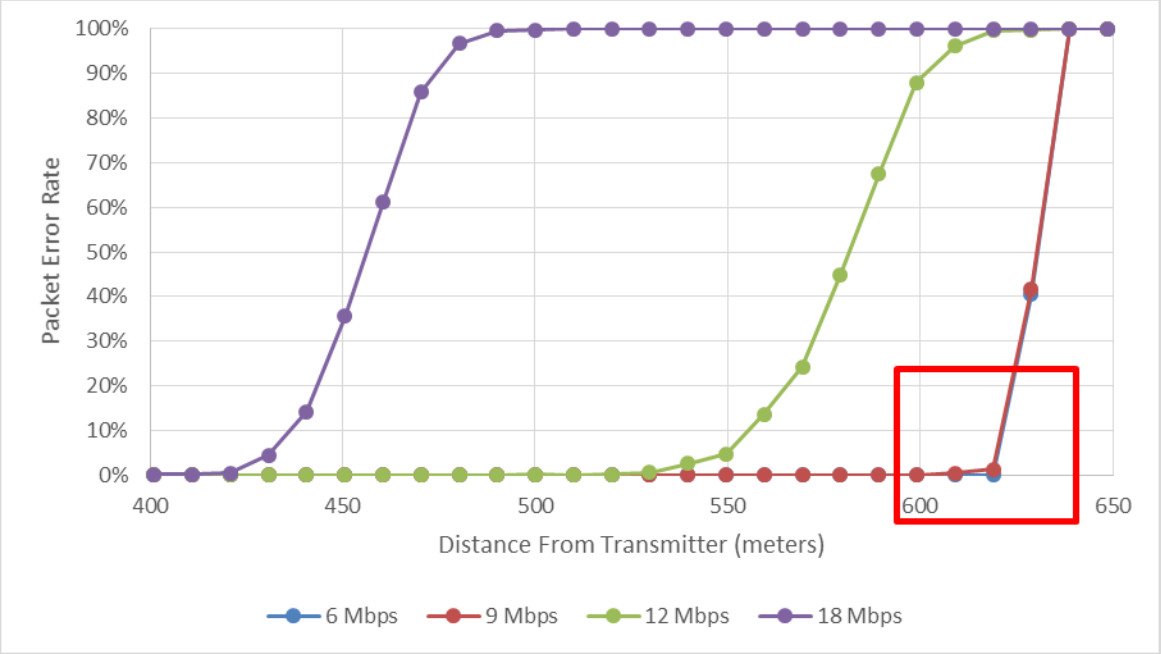


Figure 15: PER vs Distance - 4096 Byte Packets (Source: USDOT)



This figure provides a closer look at the difference observed between 6 Mbps and 9 Mbps data rates, which is minimal. Because there is a strict power threshold cut off due to pathway loss, the data rate is not the driving factor here and both 6 and 9 Mbps data rates can get very close to the cut-off. However, the power-loss limitation does not allow the transmission range to go beyond 620 meters, as shown in the figure (i.e., the 620 meter is the maximum transmission range limit that could be reached at the set -95 dB packet reception power threshold).

Figure 16: PER vs Distance - 4096 Byte Packets, a closer look (Source: USDOT)



If the antenna height is adjusted to 2 meters (close to what was used for the field test) instead of 1.5, the results are as follows with 300 byte packets.

Figure 17: PER vs. Distance from Transmitter -- Antenna Height 1.5 m (Source: USDOT)

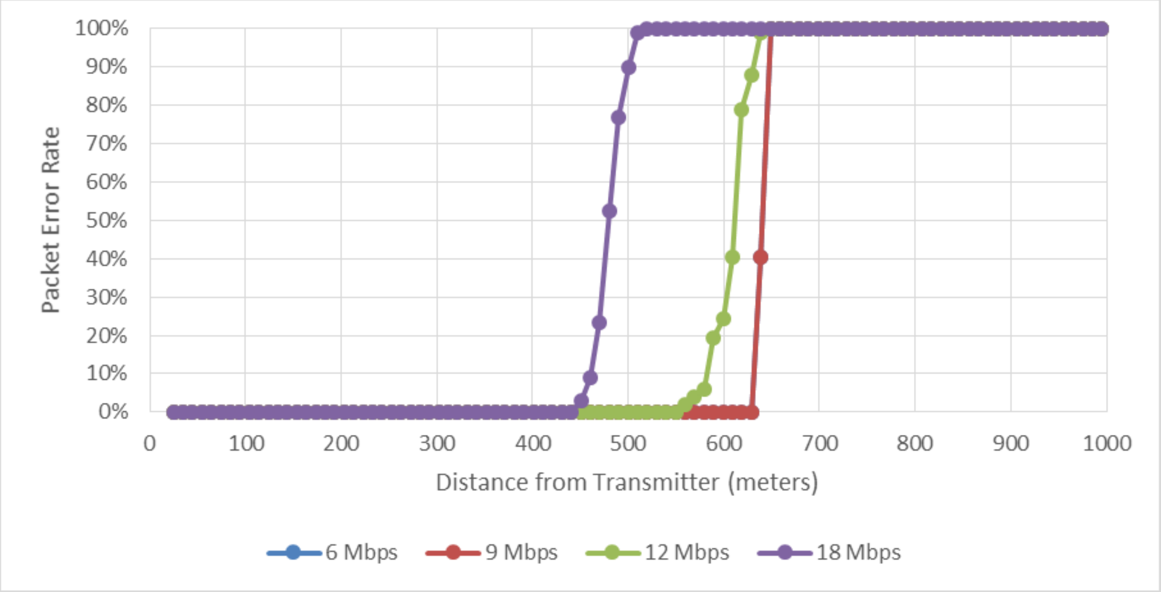
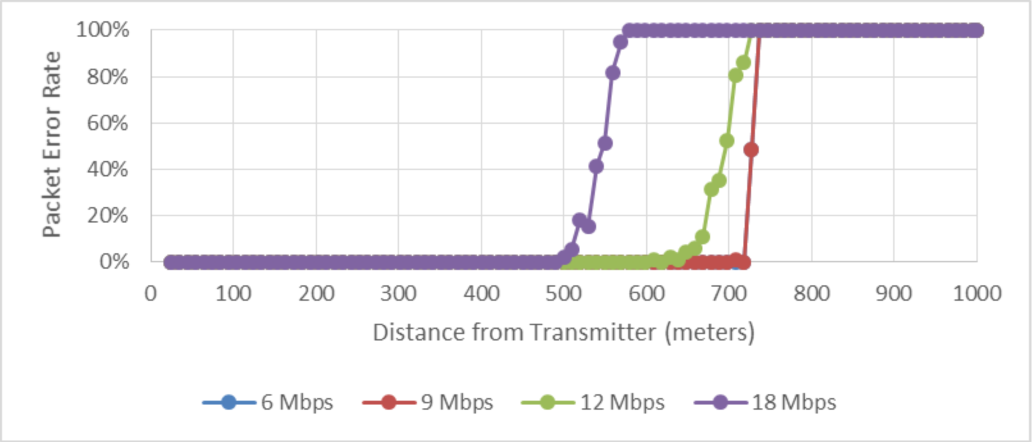


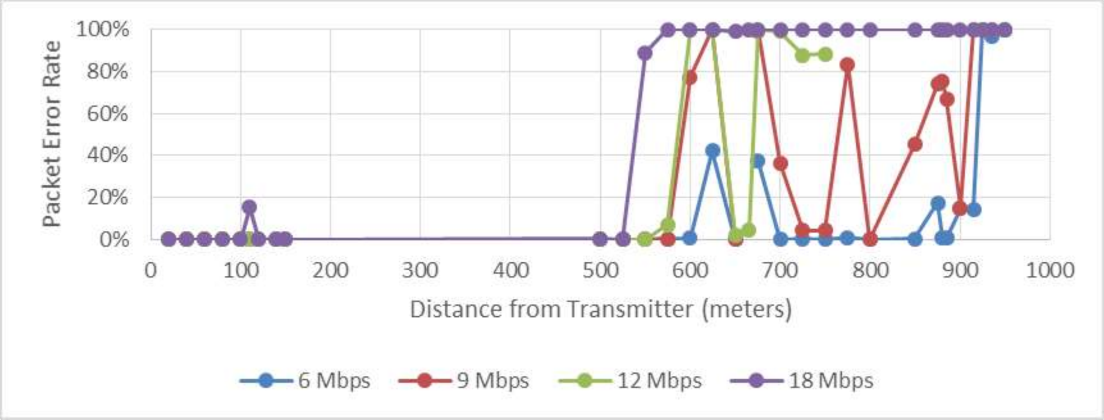
Figure 18: PER vs. Distance from Transmitter -- Antenna Height 2 m (Source: USDOT)



As expected, raising the antenna height will improve the effective distance.

For reference, and to see the difference, Figure 19 demonstrates the results of the field tests that were discussed in the previous section.

Figure 19: Field Test Results for PER vs. Range Tests (Source: USDOT)



As referred to previously, multipath is a serious factor in communications beyond about 500 meters range, which is the main source of difference observed between the results of simulation and field testing. The variation from near zero PER to nearly 40% or more at periodic intervals is representative of classic two ray multipath, which is what would be expected on the relatively flat open road at the VTTI facility. These types of variations are not observed in the simulations, however, due to having more control over the environment.

4.1.7 Time Sync and Stability Test

4.1.7.1 Description and Rationale

The purpose of this test was to determine the variations and stabilities of OBE system clocks to help understand their likely effects on position accuracy. Most connected vehicle safety applications rely in some way on a comparison of the predicted future host vehicle trajectory and the predicted trajectories of the nearby vehicles based on the data provided in the respective vehicle BSMs. While the BSMs should be generated using GPS time, the predicted trajectory depends on a set of time-based computations. These will be performed using some form of system time that is local to the OBE. This raises a concern that time differences between GPS time and the local system clock used for processing the BSM will produce errors in the predicted future position of the OBE relative to the BSM generating vehicles. Depending on the scale of the errors, this will lead to warning decision errors: either failure to detect an impending collision (false negative) or false alarms (false positive).

Clock errors, broadly, fall into three categories:

- Jitter, which relates to noise in the clock cycles, and is observable as a scattering of values around the actual time value.
- Drift, which relates to a systematic error in the duration of the clock cycles leading to continual divergence of the clock time value from the actual (or GPS) time value.
- Offset, which relates to clocks having an incorrect time value, but a time value that tracks the actual time (independent of jitter). This is similar to drift error, except that the error is a fixed offset.

This means that the clock errors translate to position errors in terms of the system’s ability to use BSM data to make warning decisions. The objective of this test was to characterize the jitter and drift of the internal clocks of the OBE to obtain a baseline to inform any clock stability requirements. The actual requirements will be derived from the plausibility simulations, but it is important that any requirements developed be realistically achievable in the context of commercially available products. With this knowledge one can more accurately assess the likely bounds for a clock in the simulations. Real requirements on a clock will be a cost-benefit analysis based on achievable accuracies from positioning technologies.

To measure clock stability, the team enlisted the capabilities of the Turner-Fairbank VTTSS testbed. With sub-microsecond accuracy [measured at ~100 nanosecond], this system provided a “ground truth” for time, which allowed measurement of the uncertainties of an OBE's system clock. Limitations on access to the local synchronization (GPS PPS) forced the team to broadcast the PPS from the VTTSS testbed via User Datagram Protocol (UDP) packets. The precision timestamp from the VTTSS testbed formed the payload of these packets, providing the listeners with a fairly accurate clock. The team isolated the network and connected a minimal number of systems in order to minimize latency. The difference between the timestamp of the PPS and the system timestamp at the receipt gave a good measurement of the variation of the system clock.

4.1.7.2 Results, Analysis, and Findings

The team measured the performance of the OBE clock from the two suppliers.

Drift

The OBEs from Supplier B appear to use “disciplined clocks.” That is to say, the system clocks regularly adjust themselves to stay synchronized to the GPS time value. For these units, the clock drift is limited to only what drift may occur between the PPS event (i.e., the drift over each one second interval between PPS events).

The OBEs from Supplier A do not appear to use disciplined clocks, and as a result the time value from these units exhibits significant drift over time. Figure 20 and Figure 21 illustrate the offset between GPS time and the device time value over a period of about an hour.

As can be seen from Figure 20, the time value of Supplier B does not exhibit any significant drift, but it does include significant jitter. The drift is so slight as to be effectively unmeasurable, but the jitter has a nominal level of about 4 msec, with peaks up to about 15 to 20 msec. Detailed statistics are provided below.

Figure 20: Clock Drift Supplier B Unit (Source: USDOT)

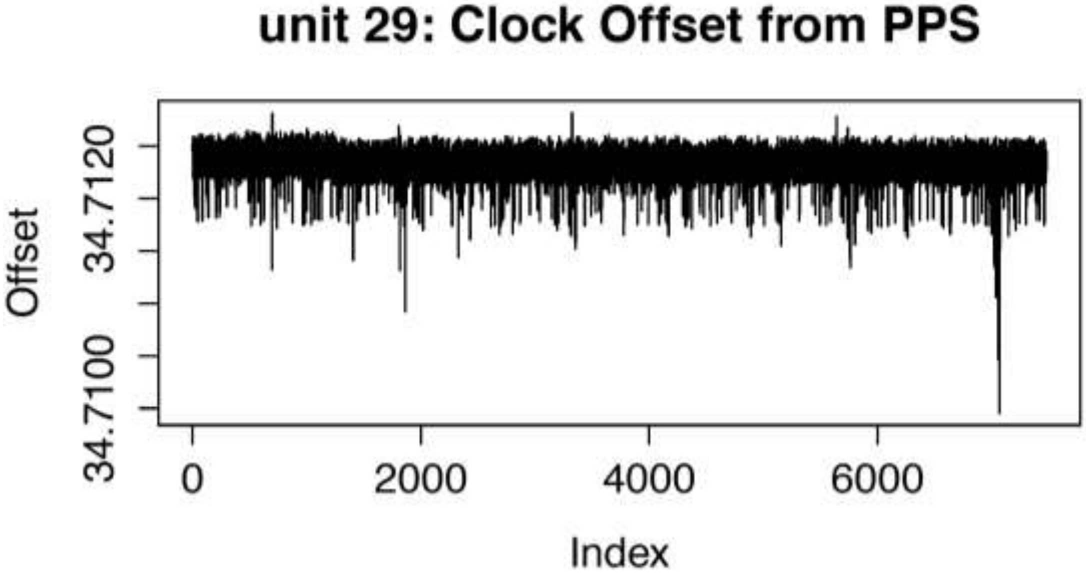
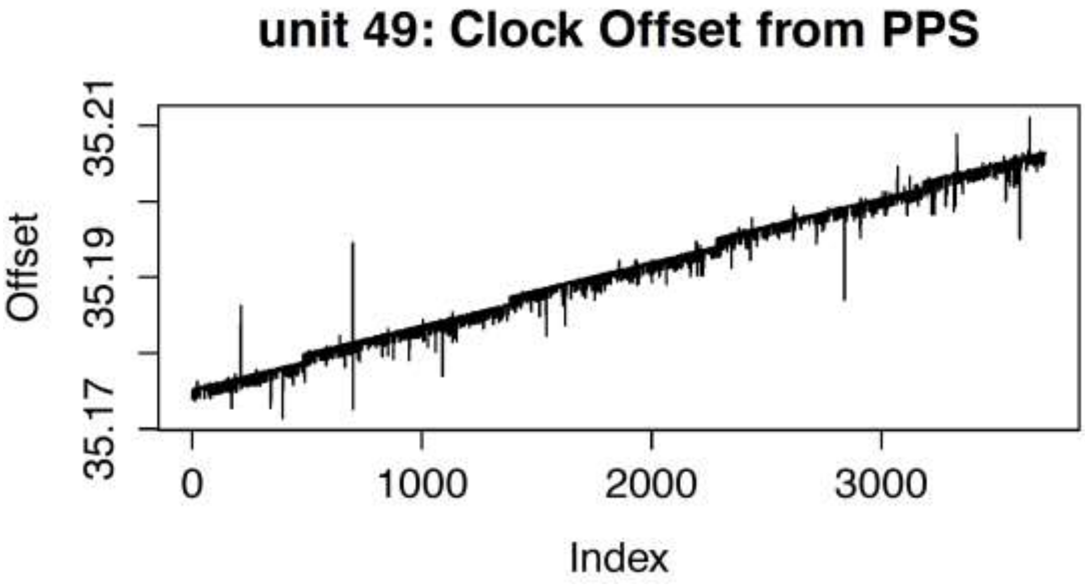


Figure 21 shows the drift of the clock in a unit from Supplier A. As can be seen in the figure, the clock includes both jitter and drift. The total drift for the Supplier A clock over 3600 seconds is about 40 milliseconds (about 10 ppm). While this level of drift is reasonable as clocks go, the fact that it does not appear to correct itself, indicates that over time the time value error could be quite large.

Figure 21: Clock Drift Supplier A Unit (Source: USDOT)



Jitter

The jitter statistics for OBEs from the two suppliers are provided in Table 9.

Table 9: Jitter Statistics for Suppliers A and B

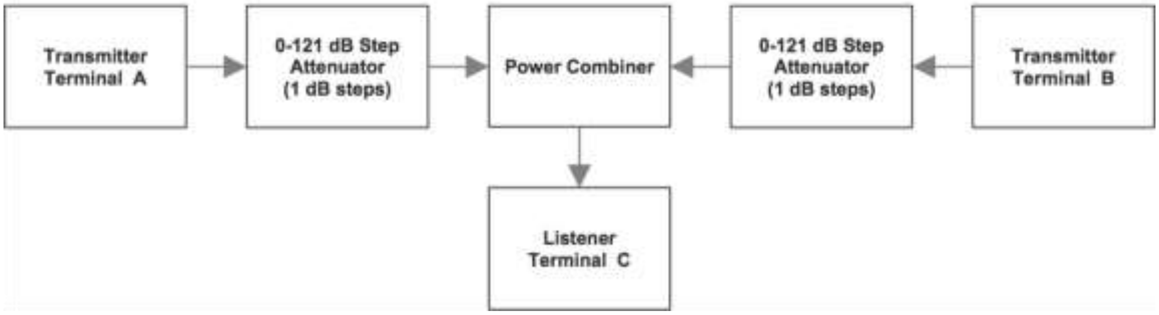
Supplier	Max Deviation	Standard Deviation
Supplier A	Not measured (10 ppm drift)	5.2 msec about drifting baseline
Supplier B	26.5 msec	2.15 msec

4.1.8 Capture Ratio / Hidden Terminal Test

4.1.8.1 Description and Rationale

The project team conducted measurements to characterize the hidden terminal phenomenon (See Appendix D) by creating a known hidden terminal situation using three DSRC units. These were set up in a laboratory configuration as illustrated in Figure 22.

Figure 22: Capture Ratio/Hidden Terminal Test Concept (Source: USDOT)



Conceptually the test used the attenuators and the directivity of the power combiner to assure that transmitters A and B were isolated from one another (i.e., hidden and unable to determine that the other was transmitting). The attenuation levels were then varied in a way that simulated listener Terminal C moving in 10 meter steps from a point close to Terminal A to the midpoint between the terminals.

The objective of this test was twofold:

1) Assess the impact of hidden node interference on PER in a controlled environment
2) Determine the power ratio at which packets from a closer terminal can be differentiated from interference from a terminal that is hidden from the closer terminal (i.e., a hidden terminal)

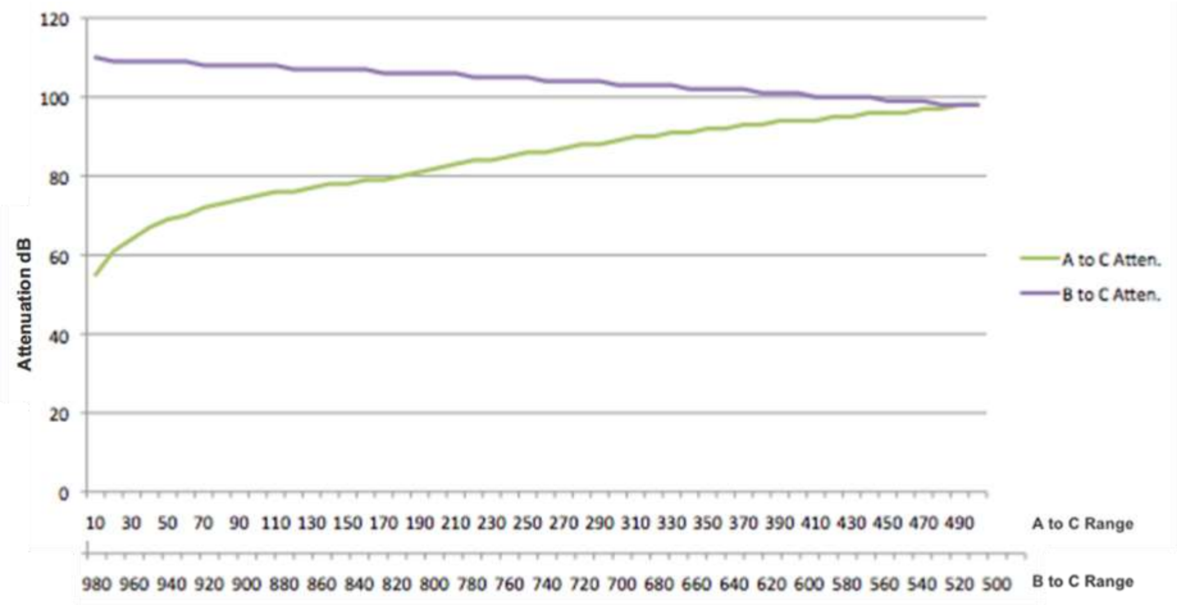
The results of these tests were to be used to calibrate and validate simulations of the same situation using larger numbers of terminals to determine the overall impact of hidden terminals in a high traffic density environment, and to separate out the impacts of congestion in high traffic environments from hidden terminals in the same environments.

This test involved several independent variables:

1) The relative attenuation levels between the two transmitters in order to simulate range
2) The data rate used by the transmitters (The team tested 6, 9, 12, and 18 Mbps data rates)
3) The message repeat rate. The nominal BSM rate is 10 Hz (i.e., 10 messages per second). However, if transmitters A and B are not synchronized, there is limited probability that they will send messages at the same time. In a real situation with numerous vehicles this probability of overlap will rise since there is a higher probability that some pair of terminals will send messages at the same time. To assess this impact, the tests were run at the nominal 10 Hz, at 40 Hz, and at 90 Hz.

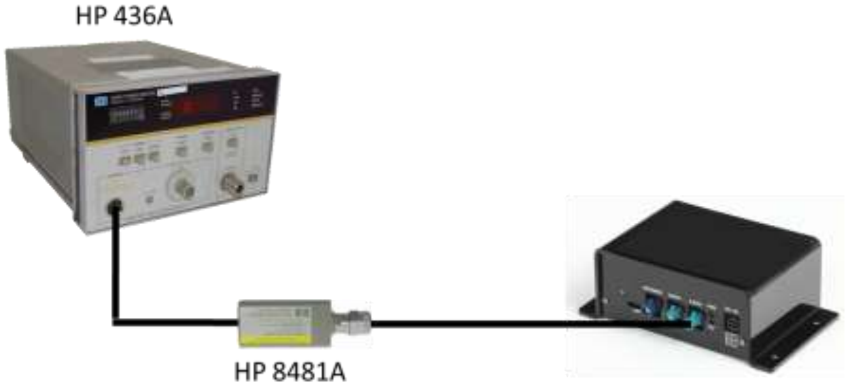
In order to assure that the relative attenuation levels would produce the proper relative signal levels for a terminal located between the two transmitting terminals, the path loss was computed using a two-ray model. The maximum attenuation level that could support any level of communication (i.e., 99% PER) was determined for each test and, using the path loss model, the attenuation value pairs (Transmitter A and Transmitter B attenuation levels) were found by “folding” the path loss values around the center point of the range that corresponded to the maximum measured range. An example of this process is provided in Figure 23.

Figure 23: Attenuation Levels to Simulate Motion of Terminal C between Terminal A and the Midpoint between Terminals A and B (Source: USDOT)



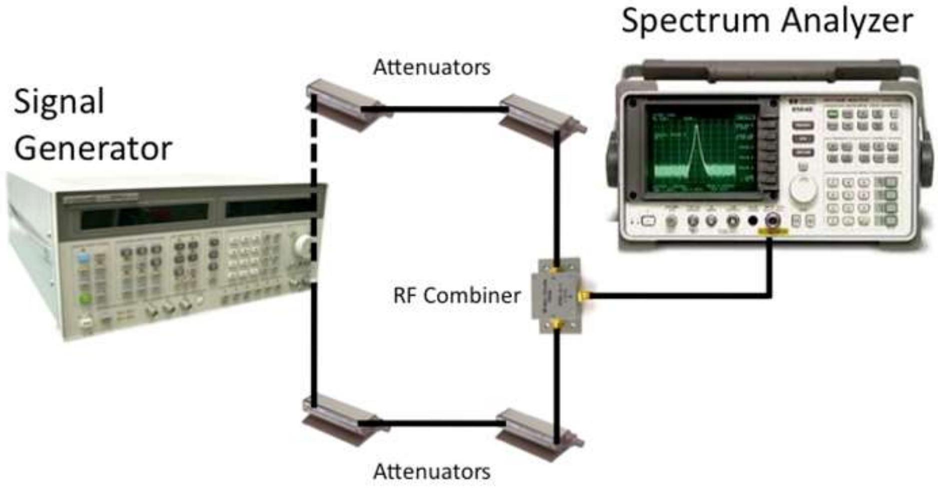
The team used a power meter and power sensor to accurately measure and validate the output power of the DSRC radios being used as the transmitters. Output power of both DSRC transmitters were measured individually prior to testing. The radios supported a special/continuous test mode used only for output power validation in this test configuration.

Figure 24: Measuring the Output Power of a DSRC Radio (Source: USDOT)



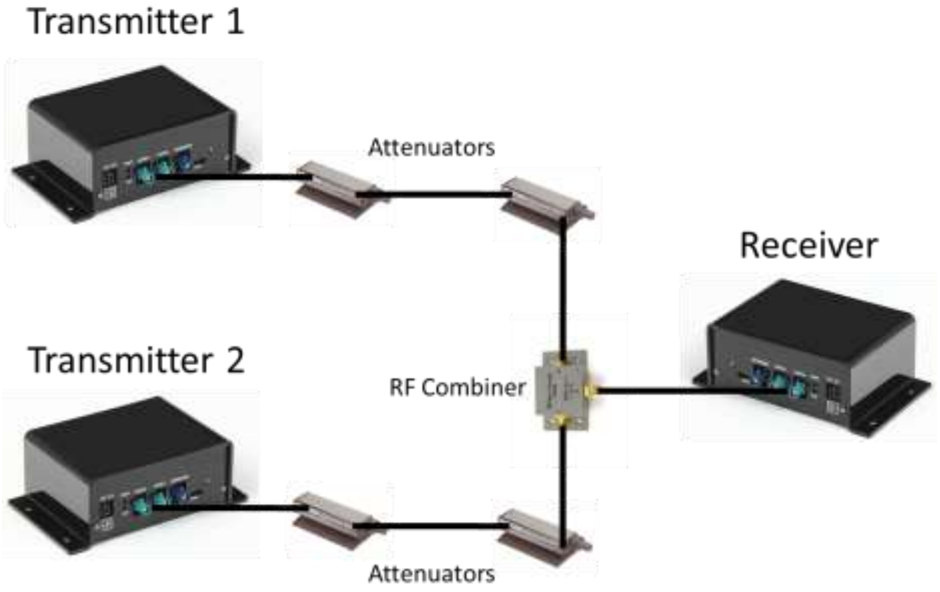
The next step was to validate the test apparatus and attenuation levels with the signal generator, step attenuators, RF combiner, and spectrum analyzer (without the DSRC radios). The team took separate measurements with the signal generator connected to each transmitter input to verify attenuation levels and account for insertion losses of the combiner, cables, and connectors.

Figure 25: Calibrating the Test Apparatus and Attenuation Levels (Source: USDOT)



The team also tested the capture ratio test apparatus with the DSRC radios, step attenuators, and RF combiner. When setting the attenuation levels, the team adjusted the attenuation by the additional loss measured during calibration.

Figure 26: Capture Ratio/Hidden Terminal Test Setup (Source: USDOT)



After completing the calibration and test setup, the team ran the capture ratio test using three DSRC units from Supplier A. After the test was completed with Supplier A, the same test was completed using three DSRC units from Supplier B.

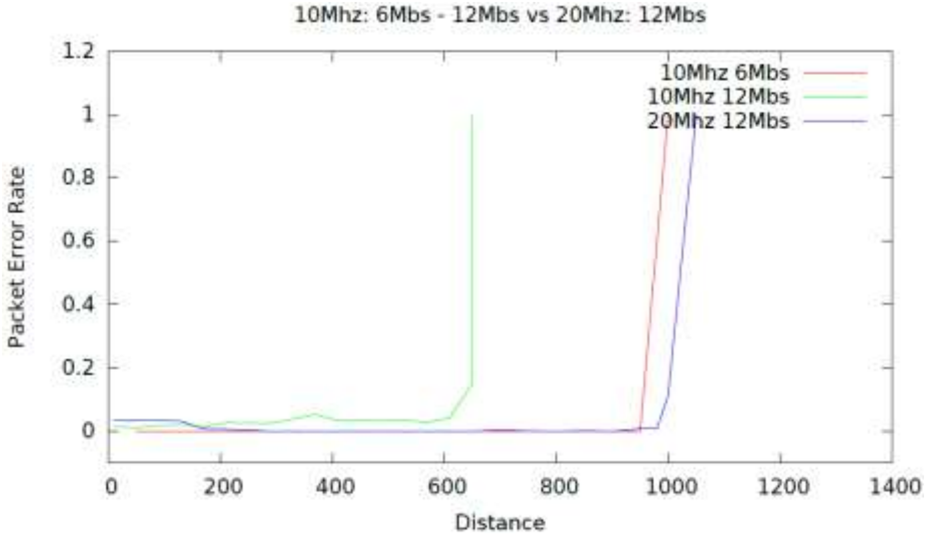
To run the test, the maximum attenuation level was determined and the attenuation pairs were computed as described above (see, for example Figure 26). The data rate and message rate was set for the two units and both sent and received packets were logged until Terminal C had received 1000 packets. The attenuation levels were then changed according to the computed values and the messages were again logged until Terminal C had received 1000 packets. The test was repeated at attenuation levels corresponding to range increments of 10 meters for message rates of 40 Hz and 90 Hz, and the entire procedure was repeated with the units set to transmit at 9, 12, and 18 Mbps data rates. It is important to note that to save time, this test was only performed for the region between Terminal A and the midpoint between terminals A and B. Other than minor differences between the terminals, it is expected that the results for the region between the midpoint and terminal B would be essentially the same (i.e., the problem is symmetrical around the midpoint of terminals A and B.

These tests were also run for each data rate at a 10 Hz rate using only one transmitter. This provided a baseline PER vs range measurement for each test condition, so that the impact of hidden terminal interference could be assessed. In order to understand the impact of hidden node interference on communications at different data rates, the team ran a set of tests with one of the terminals (Terminal B) not transmitting. This provided an interference-free baseline against which the interference data could be compared. The interference-free range baseline test was performed for the various data rates in a 10 MHz channel (Channel 174), and in a 20 MHz channel (Channel 175). The reason for this was to ascertain if the use of wider channels might offset the range and performance issues associated with higher data rates. In IEEE 802.11, 6 Mbps in a 10 MHz bandwidth channel uses QPSK modulation. 12 Mbps in a 10 MHz channel uses 16 QAM, so the 12 Mbps rate either requires a higher signal to noise ratio (SNR), or the performance will be lower at the same SNR. In contrast, 12 Mbps in a 20 MHz channel uses QPSK modulation, so it should perform comparably with 6 Mbps in a 10 MHz channel.

4.1.8.2 Results, Analysis, and Findings

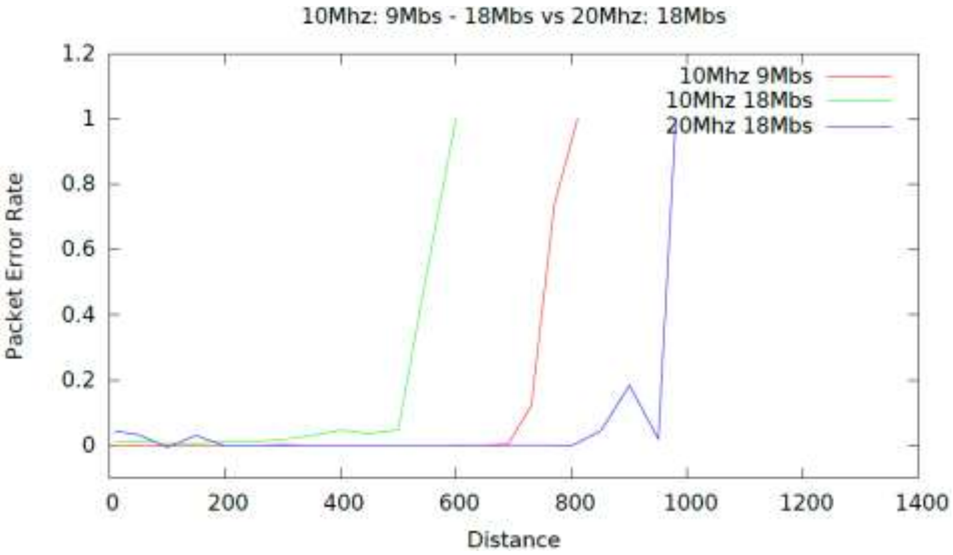
As noted above, the interference-free range baseline test was performed for the various data rates in 10 MHz and 20 MHz channels. Figure 27 shows the interference-free range baseline for 6 Mbps in a 10 MHz channel, 12 Mbps in a 10 MHz channel, and 12 Mbps in a 20 MHz channel (half rate coding). Figure 28 shows the interference-free range baseline for 9 Mbps in a 10 MHz channel, and 18 Mbps in a 20 MHz channel (3/4 rate coding).

Figure 27: Interference-Free Range at 6 Mbps and 12 Mbps (Source: USDOT)



As can be seen in the figures, the range for 6 Mbps in a 10 MHz channel is essentially the same as for 12 Mbps in a 20 MHz channel, and 12 Mbps in a 20 MHz channel represents a significant improvement over 12 Mbps in a 10 MHz channel.

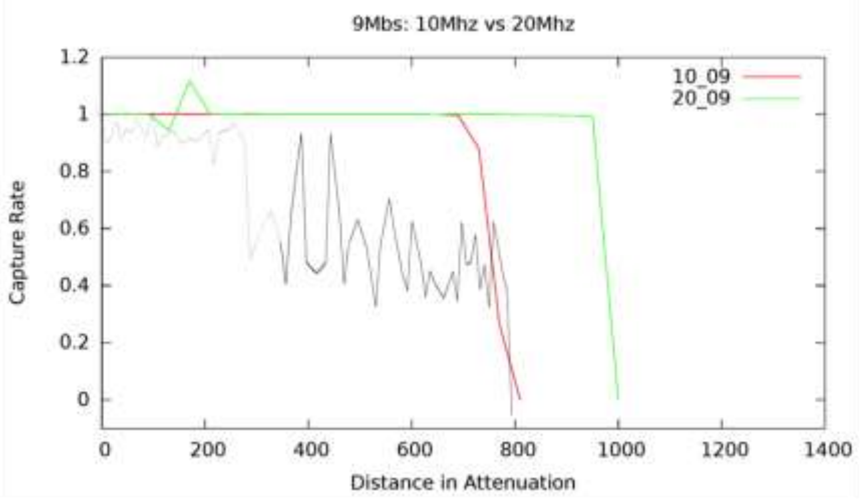
Figure 28: Interference-Free Range at 9 Mbps and 18 Mbps (Source: USDOT)



This figure shows similar results to the 6 and 12 Mbps data above, except that the 18 Mbps data rate in a 20 MHz channel shows improvement over 9 Mbps in a 10 MHz channel. This is likely a result of reduced error correction from the higher rate coding.

Figure 29 provides an example of the hidden terminal effect. These test results indicate that hidden terminal interference can cause significant degradation in overall channel performance.

Figure 29: Combined Baseline (No Hidden Terminal) and Hidden Terminal Performance (10 MHz Channel, 9 Mbps Data Rate, 10 Hz Message Rate) (Source: USDOT)



As can be seen in the figures, the baseline performance for a 10 MHz channel operating at 9 Mbps data rate (red line) indicates very good packet delivery rate (essentially 100%) from 10 meters range out to about 700 meters range. In contrast, the hidden terminal data (black lines) indicates that packet delivery is barely acceptable (about 90%) out to only about 275 meters, at which point it drops to about 55%. This behavior indicates two important mechanisms.

1) The packet delivery rate in the close-in (10-275 meters) region is somewhat impacted by the noise from the interfering terminal, but in general the test terminal (Terminal C) is able to resolve packets from the closer terminal (Terminal A) in the presence of interference from Terminal B out to about 275 meters. This is what was characterized as the “capture region” since Terminal C is able to “capture” transmissions from Terminal A even though Terminal B is transmitting at the same time
2) Between 275 meters and the limit of reception (about 700 meters) Terminal C is unable to consistently resolve packets from either Terminal A or Terminal B. This is the region of hidden terminal interference.

The “spikes” in the data, especially in the hidden terminal interference region appear to be due to jitter and drift in the timing between terminals A and B. During the tests, the team observed that the rate of packet reception at Terminal C would change over time, indicating that at sometimes the terminals were not transmitting at the same time (and the rate of packet reception would rise) and at other times they were synchronized and the rate of reception would fall, often to near zero. Without additional development work the team was unable to improve the synchronization, but it is anticipated that were the terminals fully synchronized to less than ½ packet duration, the effect of interference in the hidden terminal region would have resulted in nearly 100% communication failure. This was also demonstrated in simulations.

Other data rates and message rates exhibited similar performance. In general the higher message rates, especially in the 90 Hz region, appeared to be much worse, but it is unclear if this was due to higher messages density (likely) or over burdening the processor in the unit (from generating messages at 10 times the normal rate).

The ratio of the capture region to the interference region is an indicator of the degree of overall interference to be expected. As described in more detail in Appendix D, the larger the interference region, the more interferers will combine in any given location. In a roadway situation, where many vehicles may be located in a long moving line, these larger interference regions will overlap, creating higher probabilities of interference, and greater overall packet losses. The capture regions and interference regions for the various combinations of data rate and message rate are shown in Table 10 below.

As was expected, the impact of hidden terminal effect interference declines as the channel data rate increased (because each message occupies less time in the channel, so the probability of messages being set at the same time is lower), however, as can also be seen, higher data rates result in worse overall range performance. More importantly, because of the higher SNR requirements for higher data rates, the impact of interference in the capture region is worse. So, as data rates increase, the size of the interference region decreases, but the packet delivery rate in the capture region also decreases. It is also noteworthy that while the packet delivery rate changes as a function of message rate, the basic sizes of the regions do not. Said differently, the sizes of the capture and interference regions appear to be sensitive to data rate, but not to message rate.

Table 10: Capture Region and Interference Region Extent vs. Channel Data Rate

Channel Data Rate	Capture Region	Interference Region	Signal Power Capture Ratio*
6 Mbps	0-375 m	480-900 m	9 dB
9 Mbps	0-275 m	275-900 m	15 dB
12 Mbps	0-175 m	175-650 m	19 dB
18 Mbps	0-150 m	150-500 m	14 dB

* Signal power ratio in dB (i.e., the difference measured in dB) between the signal that is captured relative to the interfering signal

As can be seen in the table, the higher data rates exhibit smaller capture regions. This is apparently a result of the higher SNR requirements, which means that the Terminal C receiver cannot resolve the Terminal A data as effectively in the presence of interference from Terminal B. However, the higher the data rate the lower the potential probability of a collision due to shorter message channel occupancy times. A key step in assessing the impact of hidden terminals will be scaled simulations where there are many interferers.

These tests were carried out on DSRC terminals from Suppliers A and B. The Supplier A units did not exhibit any significant hidden terminal interference behavior. On closer examination it was found that the clock drift in the Supplier A units virtually assured that the messages were sent asynchronously, and as a result the messages seldom, if ever collided. As a result, the tests for the Supplier A units were generally inconclusive. While clock drift from Supplier A avoids the Hidden Terminal problem, as described above, the clock drift creates BSMs that may lead to warning decision errors: either failure to detect an impending collision or false alarms.

4.1.9 Congestion Test

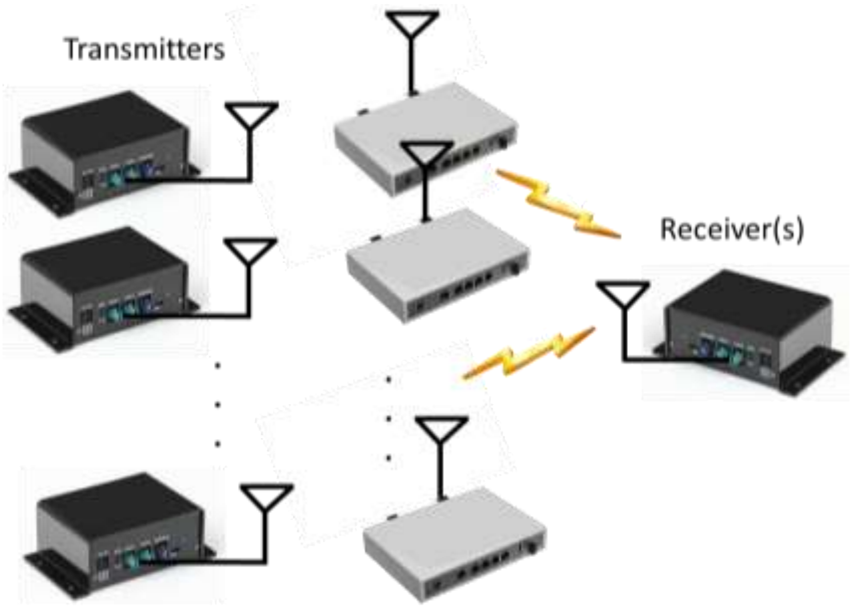
4.1.9.1 Description and Rationale

The project team conducted measurements to characterize the impact of congestion on PER and message latency. The objective of this testing was to measure the PER and packet latency at data rates of 6, 9, 12, and 18 Mbps and message rates of 10, 40, and 90 Hz in a congested network environment.

For the test, the team configured 22 radios as transmitters and two as receivers (the test probes). Of the 24 radios, 12 were from Supplier A and 12 were from Supplier B. All radios were within range of each other.

The transmitters were capable of including the time of transmission in each packet so that the receiver could calculate latency. All radios were synchronized (to within milliseconds) in order to record accurate latency measurements. The receiver probe was used to take the latency and PER measurements. The receiver probe had special logging capabilities (either internal or on an adjacent computer) to record each packet and its time of reception.

Figure 30: Congestion Test Setup (Source: USDOT)



The team configured all radios to transmit at 6 Mbps on Channel 172 and transmitted 10,000 300-byte packets at 10 Hz from each radio and logged all received packets in the receiver. This test was repeated at message rates of 40 Hz and 90 Hz to simulate higher levels message traffic. The tests were repeated at 9, 12, and 18 Mbps data rates.

Two different message timing schemes were used. The “Synchronous” timing triggered the message transmission based on the PPS. The expectation was that the clock skew and jitter in the units would be sufficient to prevent all messages from being transmitted at the exact same instant. If the messages are transmitted with perfect synchronism (i.e., at exactly the same time) they will collide. This is because the CSMA protocol looks at the channel, and if it is clear, it sends the message after waiting a small fixed interval. To the extent that all transmitters are synchronous, the channel will be clear when the CSMA system checks, and so all terminals will subsequently send at the same time. However, to the extent that the unit clocks exhibit jitter or drift, the timing will not be exact, and the CSMA mechanism should take care of overlapping messages.

Another approach to message timing was to intentionally offset the messages by half a message time interval. This was intended to prevent situations where the timing might accidentally be exact. The conjecture was that by deliberately offsetting each terminal by a different integer multiple of some base offset, the CSMA protocol would only need to deal with a small number of contenting terminals (as opposed to nearly all of them). To achieve this, each terminal was configured to send messages at the prescribed message rate, but to offset the message start time from the PPS signal by an integer multiple of half of the message time. This meant that there were always at least two terminals contending for the channel, but seldom more than a few contenders.

Using the data collected by the receiver probe, the team processed the information to determine the PER and packet latency for each data rate and message rate. Average latency, latency standard deviation, and PER for each test case were computed.

4.1.9.2 Results, Analysis, and Findings

The results from the congestion tests were consistent with theoretical expectations. Figure 31 and Figure 32 Illustrate the congestion performance for a receiver from Supplier A at various data rates and with and without message synchronization.

Figure 31: Supplier A Congestion Performance (Synchronous Messaging) (Source: USDOT)

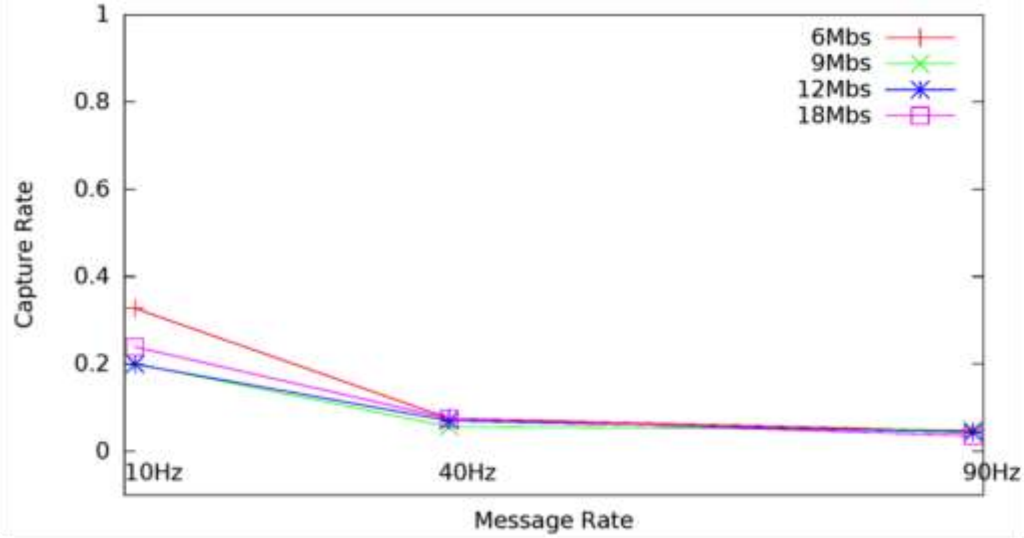
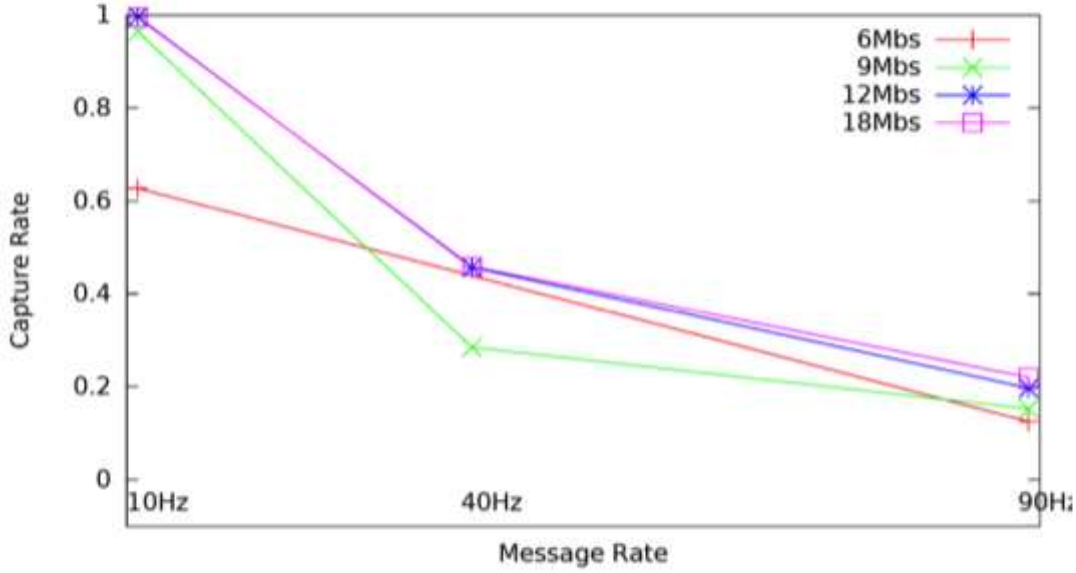


Figure 32: Supplier A Congestion Performance (Asynchronous Messaging) (Source: USDOT)



As can be appreciated from Figure 31, the synchronous message timing results in significant packet losses, even at low message rates (the 10 Hz rate corresponds to about 22 vehicles). As the message rates are increased, the packet losses approach 100%. While there are slight differences in performance as a function of data rate, these are not significant, and they effectively disappear at higher message rates.

Figure 32 shows the impact of separating the messages in time by a small amount. As can be seen in the figure, with higher data rates, there is no significant impact from congestion at the 10 Hz messaging rate. The losses are greater from higher message rates, and generally, the higher the channel data rate, the lower the losses from congestion.

The Supplier A units did not perform as well as the Supplier B units.

Figure 33 and Figure 34 illustrate the congestion performance for a receiver from Supplier B at various data rates and with and without message synchronization.

Figure 33: Supplier B Congestion Performance (Synchronous Messaging) (Source: USDOT)

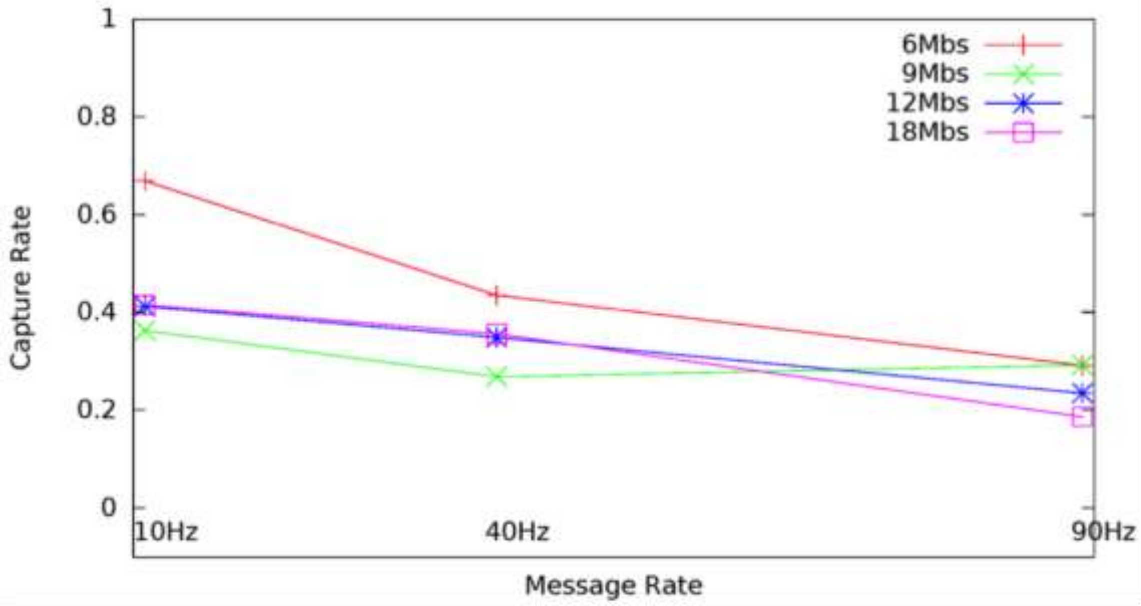
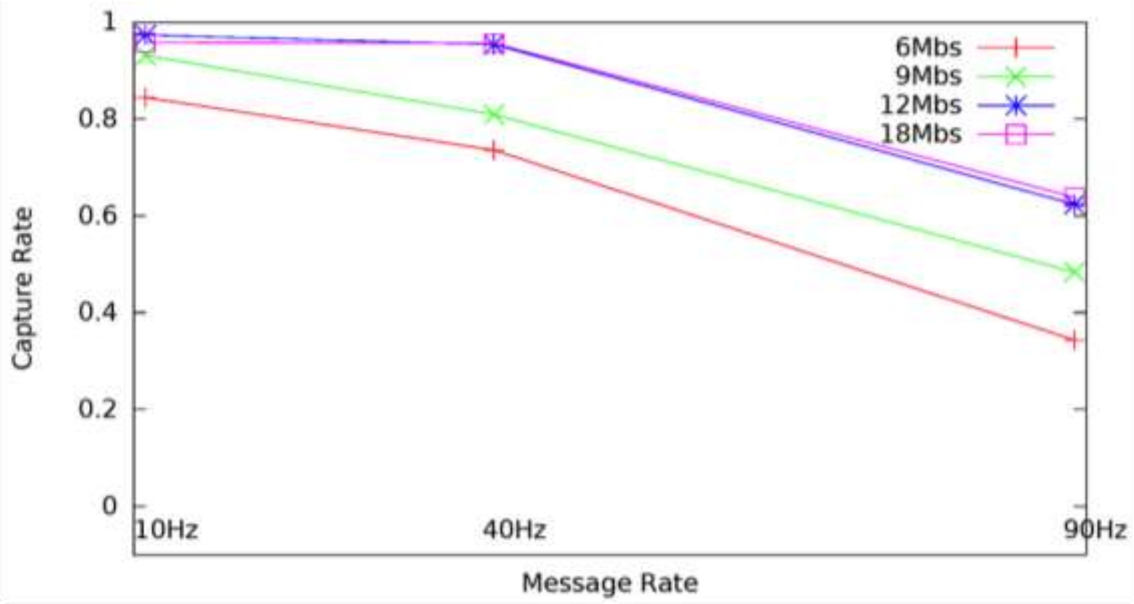


Figure 34: Supplier B Congestion Performance (Asynchronous Messaging) (Source: USDOT)



As can be appreciated from the figures, the Supplier B receivers perform substantially better in this environment. The reasons for this are unclear, since the congestion is generated from the same set of units as was used in the Supplier A tests. For synchronous messaging the packet losses are still significant, ranging between 40% and 65% for all data rates. The asynchronous performance, however, is substantially better. As with the Supplier A tests, higher data rates correspond to reduced losses from congestion. While there is reduction in packet success at higher message rates, the worst case is about 35% success at 6 Mbps at a 90 Hz message rate. This corresponds to about 178 vehicles. At 9 Mbps the packet success rate is slightly under 50%, and at 12 Mbps and 18 Mbps, the success rate is about 60%. It is unclear how much of the packet losses at the 40 Hz and 90 Hz rates is due to congestion, and how much may be due to other effects, since neither the Supplier A or Supplier B units were designed to run at these very high message rates,

The bottom line from these tests is that higher channel data rates can significantly reduce congestion.

4.1.10 Communication Simulations

The communication simulations address DSRC data transmitting and receiving requirements under stress conditions. These conditions include the impacts of the transmit power and antenna gain envelope on steep grades, the ability to receive messages in a congested environment, as well as the ability to receive messages in the event that nearby vehicles induce a hidden node effect. These conditions are examined in the following simulation scenarios:

- Transmit Power and Antenna Gain Envelope Simulation
- Congestion Simulation
- Hidden Node Simulation

In order to understand the impacts of different factors on these scenarios, the team used the Opnet Wireless Modeler to simulate them. Simulation offers the benefits of being able to scale the number of terminals in the computing environment, without the capital costs of procuring and settling up hundreds of terminals. Moreover, the environment allows the team to quickly alter scenarios and run iterations and trials with many parameter variations.

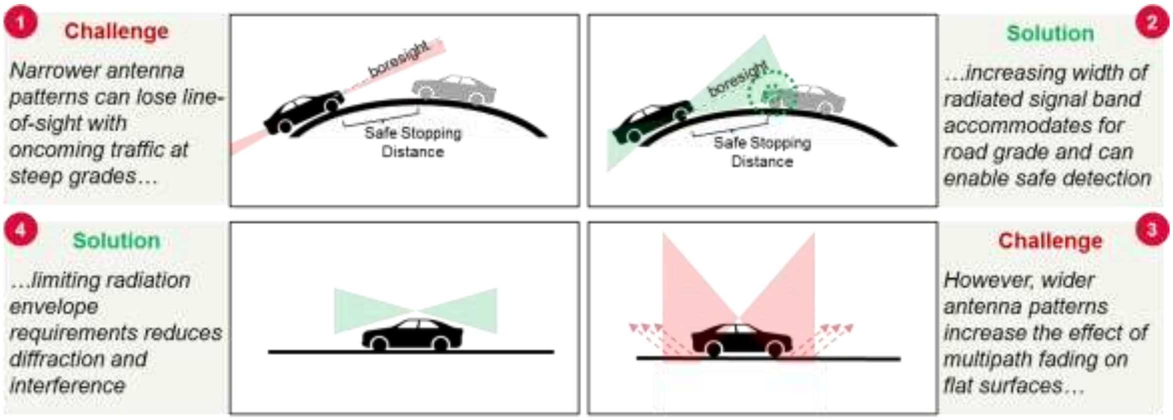
The findings of each of these simulation scenarios inform recommendations on antenna pattern design, optimum data rate, and optimum message transmission rate. Specifically, the antenna should be required to have a maximum pitch angle of 10 degrees to optimize the trade-off between line-of-sight and diffraction; and a 9 Mbps data transmission rate in a 10 MHz channel is recommended to reduce the impacts of congestion and hidden node effects. Also in a congested environment, reducing the message transmission rate could reduce the load on the channel and can improve PER. The narrative below discusses these findings and supports these recommendations through the simulation experiments.

4.1.11 Transmit Power and Antenna Gain and Sensitivity Envelope Analysis and Simulation

4.1.11.1 Description and Rationale

The design of the antenna pattern affects range, line of sight, and width of the radiated signal band. These measures are particularly important in the potentially hazardous example when two vehicles are approaching each other on opposite sides of a steep hill. Therefore, the geometry of the road should be considered in the analysis. More generally, narrow antenna patterns used on steep grades can lose line-of-sight of nearby vehicles. These concerns can be mitigated by changing the pitch angle of the antenna pattern. However, broadening this angle also has its challenges, as too broad a pattern causes an interference effect of multi-path fading. The solution is an optimal balancing of this angle. Figure 35 describes this challenge in more detail.

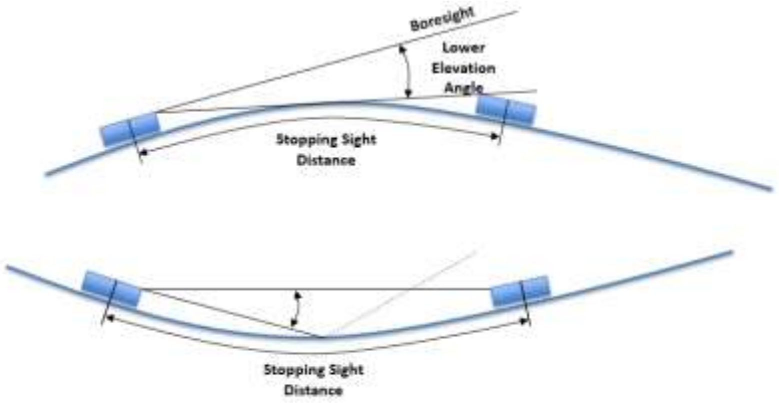
Figure 35: Antenna Design Trade-offs (Source: USDOT)


1
Challenge
Narrower antenna patterns can lose line-of-sight with oncoming traffic at steep grades…
boresight
Safe Stopping Distance
boresight
Safe Stopping Distance
2
Solution
…increasing width of radiated signal band accommodates for road grade and can enable safe detection
4
Solution
…limiting radiation envelope requirements reduces diffraction and interference
3
Challenge
However, wider antenna patterns increase the effect of multipath fading on flat surfaces…

4.1.11.2 Results, Analysis, and Findings

Figure 36 demonstrates the Stopping Sight Distance (SSD) versus elevation changes. The minimum elevation angle is determined by the SSD which is the minimum distance at which two vehicles will be able to communicate over the crest of a hill or in a sag of a valley.

Figure 36: Stopping Sight Distance vs. Elevation Angle (Source: USDOT)



To solve for this optimal pitch angle, Booz Allen analyzed the effective range at various pitch angles and based on different antenna patterns. The team used two-ray path-loss model for the propagation model in Opnet. Appendix D provides the details of the analysis. Table 11 is a summary of this analysis:

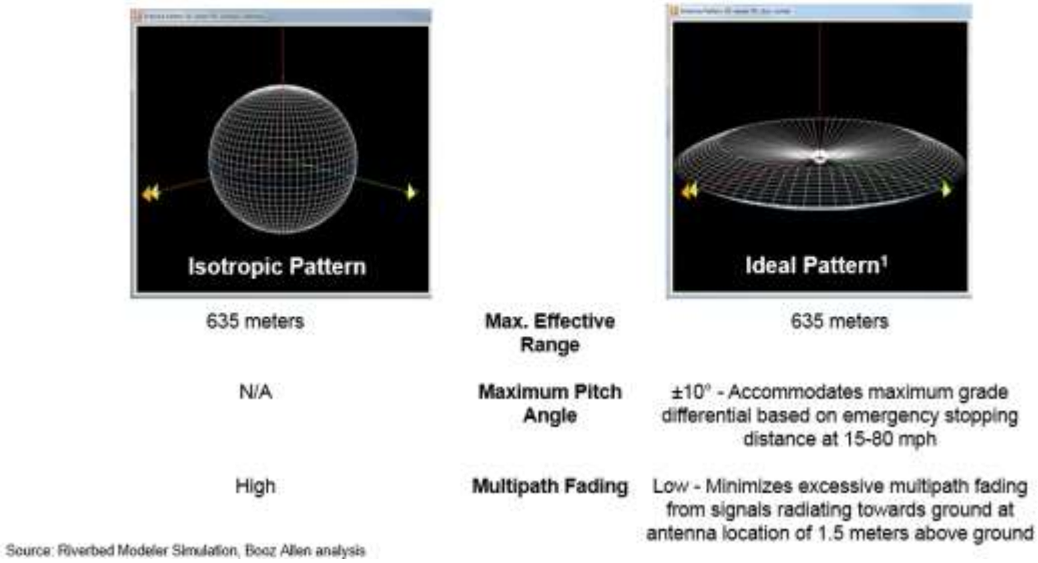
Table 11: Effective Antenna Gain and Range for Different Elevation Angles

Elevation Angle	Antenna Gain (dB)	Effective Range (m)
0° (along the azimuth)	0	635
5° from azimuth	-3	534
±10° from azimuth	-6	449
> 10° from azimuth[5]	-20	200

The results from the OPNET simulations validate the proposed antenna pattern specification. The gain pattern and range of the antenna used in the simulations maintains strong effectiveness along the boresight and azimuth while minimizing potential negative side effects of multipath fading. The simulation data verifies that an omnidirectional antenna with a narrow elevation gain pattern is effective well beyond the emergency stopping distance at all speeds and road grades that fall within federal regulations.

[5] The team recognizes that an antenna with precisely this pattern may not be technically feasible given packaging constraints on the vehicle. For safety reasons the gain values for elevation angles given in the table above should be considered as minimum values. To the degree that the gain does not fall off as rapidly as recommended (for practical reasons) the system may see increased multipath fading, but this may be a necessary side effect of making a practical system.

Figure 37: Antenna Pattern and Effective Range (Source: USDOT)

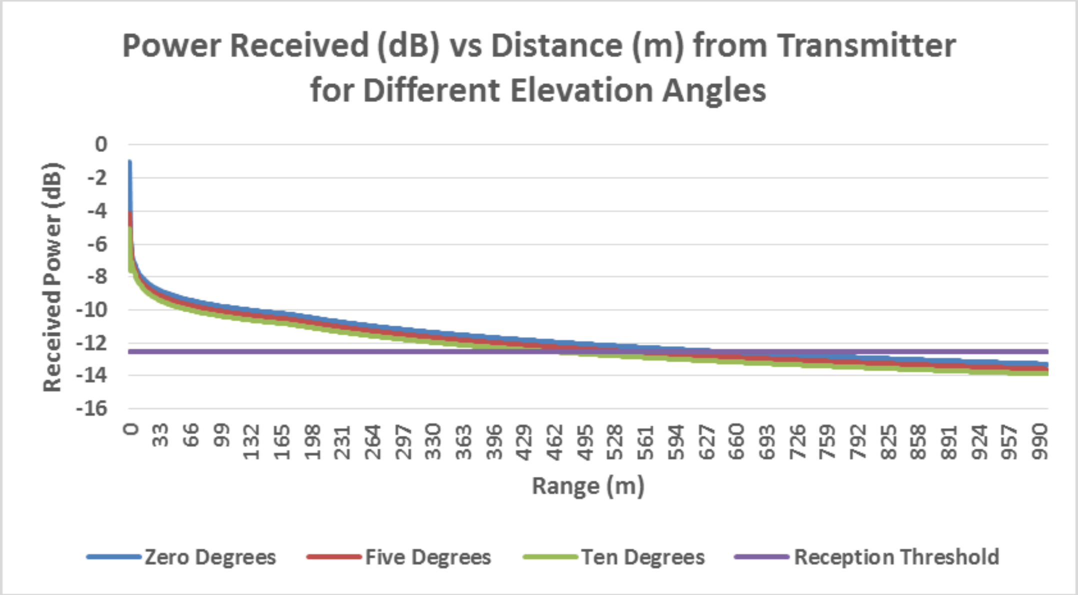


Isotropic Pattern		Ideal Pattern¹
635 meters	**Max. Effective Range**	635 meters
N/A	**Maximum Pitch Angle**	±10° - Accommodates maximum grade differential based on emergency stopping distance at 15-80 mph
High	**Multipath Fading**	Low - Minimizes excessive multipath fading from signals radiating towards ground at antenna location of 1.5 meters above ground

Source: Riverbed Modeler Simulation, Booz Allen analysis

Figure 37 confirms that the maximum effective range of ~ 450 meters is achieved within ±10° pitch angle from the azimuth. This distance still accommodates the emergency stopping distance requirement by USDOT which is in the range of 22-300 meter for the speed range of 15-80 mph for the dry road condition[6].

Figure 38: Power Received (dB) vs. Distance (m) from Transmitter (Source: USDOT)



[6] Source: http://safety.fhwa.dot.gov/speedmgt/ref_mats/fhwasa10001/#t2

4.1.12 Congestion Simulation

4.1.12.1 Description and Rationale

When many vehicles are within the communication range of each other, there is a potential for a congested network which could negatively impact the reception of BSMs—introducing potential vehicle safety risks due to the loss of information. Since DSRC users are not actively managed by a base station, there is technically no limit to the number of users that can be served by a DSRC channel. However, there are some practical limits that arise from the size of the radio footprint and the typical packing density for cars. That is to say the system can only serve the number of users that can realistically fit in the area of radio coverage.

The congestion mechanism has been actively studied by numerous researchers[7]. As noted in the introduction to this section, a primary purpose of this analysis was to assess how different channel parameters might impact congestion. This study was aimed at fully assessing the congestion performance at various data rates, different message transmission rates, and both 10 MHz and 20 MHz[8] channel bandwidths in order to better understand the options and tradeoffs for managing congestion.

The analysis indicates that changing the following factors improve the PER caused by network congestion:

1) Increasing the data rate – ideal value appears to be 9 Mbps *in a 10 MHz channel*
2) Using a 20 MHz channel bandwidth vs. 10 MHz
3) Decreasing message transmission rate (a key feature of the current CAMP congestion control algorithms)

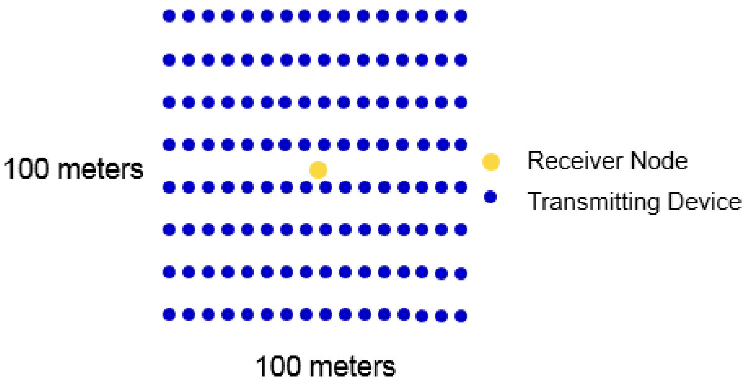
The team came to these conclusions through the use of the simulated environment by scaling up the number of terminals and changing different factors.

For example, consider a scenario in Figure 39, which illustrates an area of 100x100 meters occupied by a number of vehicles. In this scenario, all of the vehicles are within the communication range of each other, which helps with isolating only the effects of congestion and excluding the hidden node problem that will be discussed in the next section.

[7] See for example: Controlling Congestion in Safety-Message Transmissions by Gaurav Bansal and John B. Kenney; IEEE Vehicular technology Magazine; Dec. 2013; D. Jiang, V. Taliwal, A. Meier, W. Holfelder, and R. Herrtwich, "Design of 5.9 GHz DSRC-based vehicular safety communication," IEEE Wireless Commun., vol. 13, no. 5, pp. 36–43, Oct. 2006

[8] The use of 20 MHz channels is provided for in IEEE 802.11. These channels have not been studied in any significant depth. While the tests and simulations indicate that the use 20 MHz channels can significantly reduce congestion and hidden terminal interference issues by supporting higher data rates without significantly impacting communications range, the Booz Allen team recognizes that there are a variety of other technical, policy, and regulatory aspects that will need to be considered before such an approach could be adopted with confidence. The objective for this project was to determine if the 20 MHz DSRC channels (e.g., Channels 175 or 177) could be used for safety applications, and if so, how effectively they might support safety communications. Additional considerations that may positively or negatively impact the use of 20 MHz channels are described in the comparison tables provided in this report.

Figure 39: Congestion Scenario, Stable Traffic Flow (Source: USDOT)

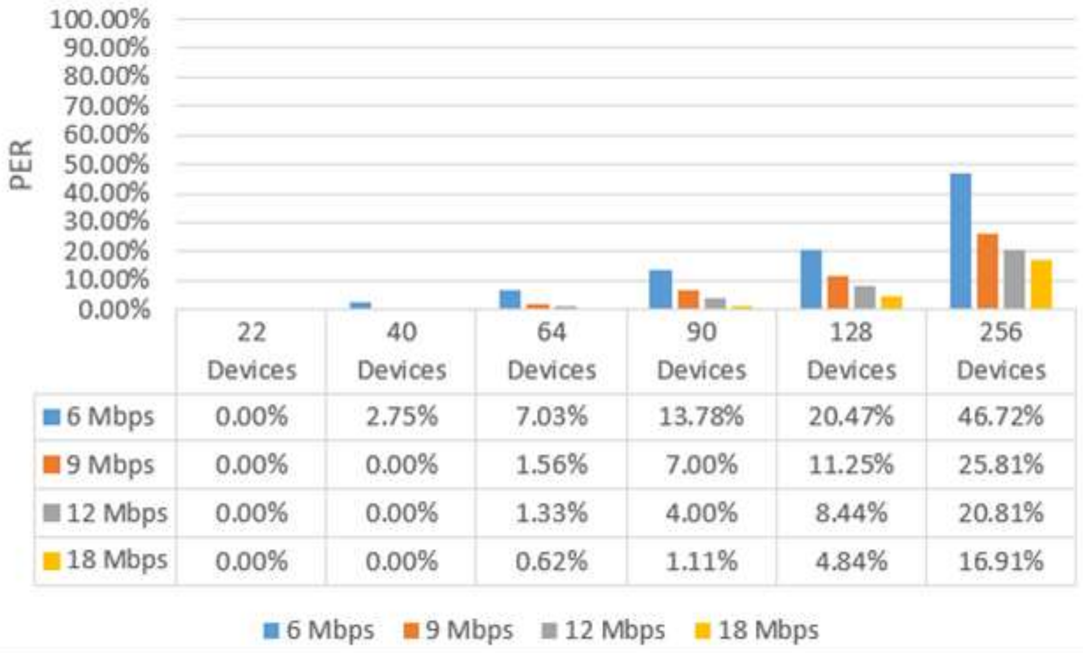


Various simulations were run changing the number of terminals in the population, data rates, channel bandwidth, message rates, and message synchronization. The overall packet error rate was determined by comparing those packets sent with the packets received by one of the terminals in the population.

4.1.12.2 Results, Analysis, and Findings

Figure 40 demonstrates the PER level in the scenario where a 10 MHz channel is used, changing the number of vehicles in the 100x100 meter coverage area (ranging from 22 to 256, with 256 vehicles representing the most congested scenario), and with various data rates.

Figure 40: PER in Various Levels of Vehicle Congestion (Source: USDOT)



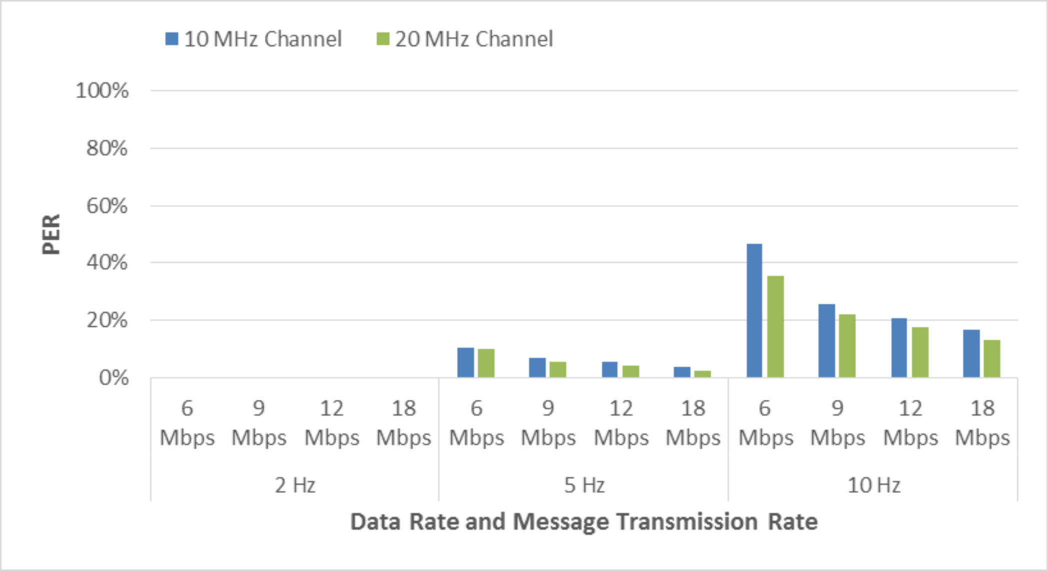
	22 Devices	40 Devices	64 Devices	90 Devices	128 Devices	256 Devices
6 Mbps	0.00%	2.75%	7.03%	13.78%	20.47%	46.72%
9 Mbps	0.00%	0.00%	1.56%	7.00%	11.25%	25.81%
12 Mbps	0.00%	0.00%	1.33%	4.00%	8.44%	20.81%
18 Mbps	0.00%	0.00%	0.62%	1.11%	4.84%	16.91%

As Figure 40 shows, in a highly congested scenario using a 6 Mbps data rate, more than 46% of the packets may be lost. However, this error can be reduced by half simply by increasing the data rate to

9 Mbps which represents a change in the coding rate but not the modulation (implying little or no impact on range performance. The figure also indicates that 12 Mbps and 18 Mbps may provide additional benefits in terms of congestion, but these require a different modulation, and this may not provide adequate range. As a result it appears that using a 9 Mbps data rate may provide improved congestion performance without sacrificing range performance.

The scenario described above is representative of the many scenarios and trials that were conducted for the analysis of congestion. In the simulations the team changed different factors (i.e., channel bandwidth, data rate, and message transmission rates) and studied the effect of these factors on the PER, which is summarized in Figure 41. In the simulation summarized in Figure 41, 256 vehicles were simulated communicating at different data rates, message transmission rates, and bandwidth in an area of 100x100 meters.

Figure 41: PER in a Congested Network (Source: USDOT)



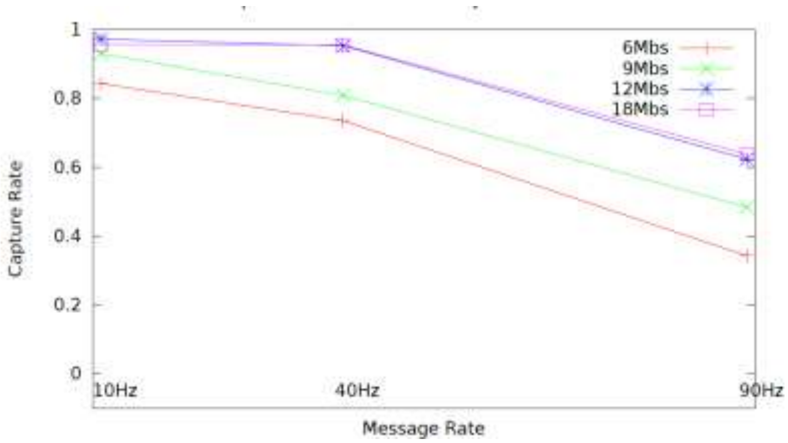
Note that at 2 Hz message transmission rate, there is no PER which is due to a very low message rate that reduces channel congestion drastically. The highest PER is for 6 Mbps data rate at 10 Hz message transmission rate using a 10 MHz channel. However, this error can be reduced by about 45% by increasing the data rate to 9 Mbps in a 10 MHz channel.

If a 20 MHz channel bandwidth is used, a 12 Mbps data rate can be used to obtain nominally the same range performance as with 6 Mbps in a 10 MHz channel (See range tests above). In this case, the PER drops by about 65% under the same congestion situation

Comparing the results with the lab test

The results of the congestion simulations discussed above are consistent with what was observed in the lab tests. The lab tests used 22 devices in a 3x6 meter lab transmitting messages at 10 Hz, 40 Hz, and 90 Hz to simulate congestion scenarios where there are 22, 88, and 198 vehicles transmitting. Figure 42 summarizes one of these tests. This test used devices from Supplier B and evaluated the performance at 6, 9, 12, and 18 Mbps in a 10 MHz channel.

Figure 42: Lab Congestion Test Results with Supplier B (Source: USDOT)



Please note that the vertical axis of Figure 42 shows the Capture Rate which is equal to 1-PER in this case. For example at 10 Hz, where there are 19 devices using a 6 Mbps data rate (red line), the PER would be about 15%. The results shown here are slightly better than the simulation results which could be due to the fact that in the lab there is no line of sight issue whereas the simulations considered the effects of line of sight.

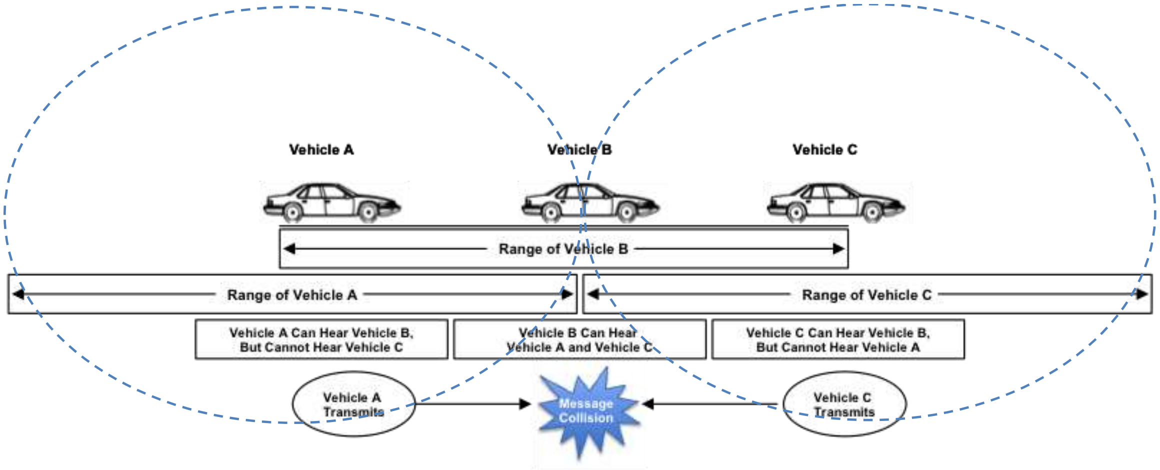
4.1.13 Hidden Terminal Simulations (with and without congestion)

4.1.13.1 Description and Rationale

In addition to the congestion issues discussed above, another key issue with DSRC in a crowded environment is what is known as the “hidden terminal effect” which is observed in the networks using the CSMA scheme.

As illustrated in Figure 43, vehicles A and C can hear Vehicle B. However, neither Vehicle A nor C can hear the other. According to CSMA rules, each will listen to the channel, and, if no other terminal is transmitting, each will hear no channel activity, so they will send their messages. Vehicle B will hear both messages at the same time, and will be unable to separate them, and the transmissions will fail. As can be appreciated from the figure, this situation will occur frequently in traffic situations, meaning that few of the messages that are sent will actually be received, since they are highly likely to collide with messages sent in the same general timeframe by out-of-range vehicles.

Figure 43: Hidden Node Situation (V2V) (Source: USDOT)


Vehicle A
Vehicle B
Vehicle C
Range of Vehicle B
Range of Vehicle A
Range of Vehicle C
Vehicle A Can Hear Vehicle B, But Cannot Hear Vehicle C
Vehicle B Can Hear Vehicle A and Vehicle C
Vehicle C Can Hear Vehicle B, But Cannot Hear Vehicle A
Vehicle A Transmits
Message Collision
Vehicle C Transmits

The hidden node effect has not been studied in the context of connected vehicles. One examination of this effect was observed in an experiment conducted by CAMP. In the CAMP study, Interoperability Issues of Vehicle-to-Vehicle Based Safety Systems Project Phase 1 Final Report, 51 vehicles in the center (Figure 44) travelled clockwise and were moved in and out of the communication range of the static vehicles (positioned in the upper left and lower right of the figure). In this test track experiment, a set of vehicles circulated on a course that took them into and out of range of two groups of parked vehicles. It was assumed that the vehicles in either of the groups could not detect messages from the other group, although there was no data provided to confirm that this was in fact the case. There were also apparently no interference-free baseline tests performed (for example, running the test cars on the circulation course with only one of the two groups transmitting). The CAMP report identified the results of this test as inconclusive, since they did not observe any significant packet losses that could be directly attributable to hidden terminal losses. The ambiguity of these tests was a primary motivation to more systematically characterize this phenomenon in order to assess its potential impact on communications reliability in a roadway environment. Where the CAMP test ran vehicles in a somewhat realistic environment, the nature of the test introduced many variables, so it is somewhat difficult to determine the root cause of the observed results. The tests performed as part of this project are somewhat limited in that they are specifically creating hidden terminal interference in order to study its impact and characteristics, but because of this, the stochastic nature of the interference (specifically the probability that two terminals may transmit at the same time) is not well captured, and using only two hidden terminals it is difficult to extrapolate to understand the aggregate behavior of a long line of vehicles on a roadway. Simulations of hidden terminals described below will augment the CAMP test data to provide a clearer picture of the impact of this issue, and provide insights into potential mitigations.

Figure 44: CAMP Hidden Node Test Scenario (Source: CAMP)

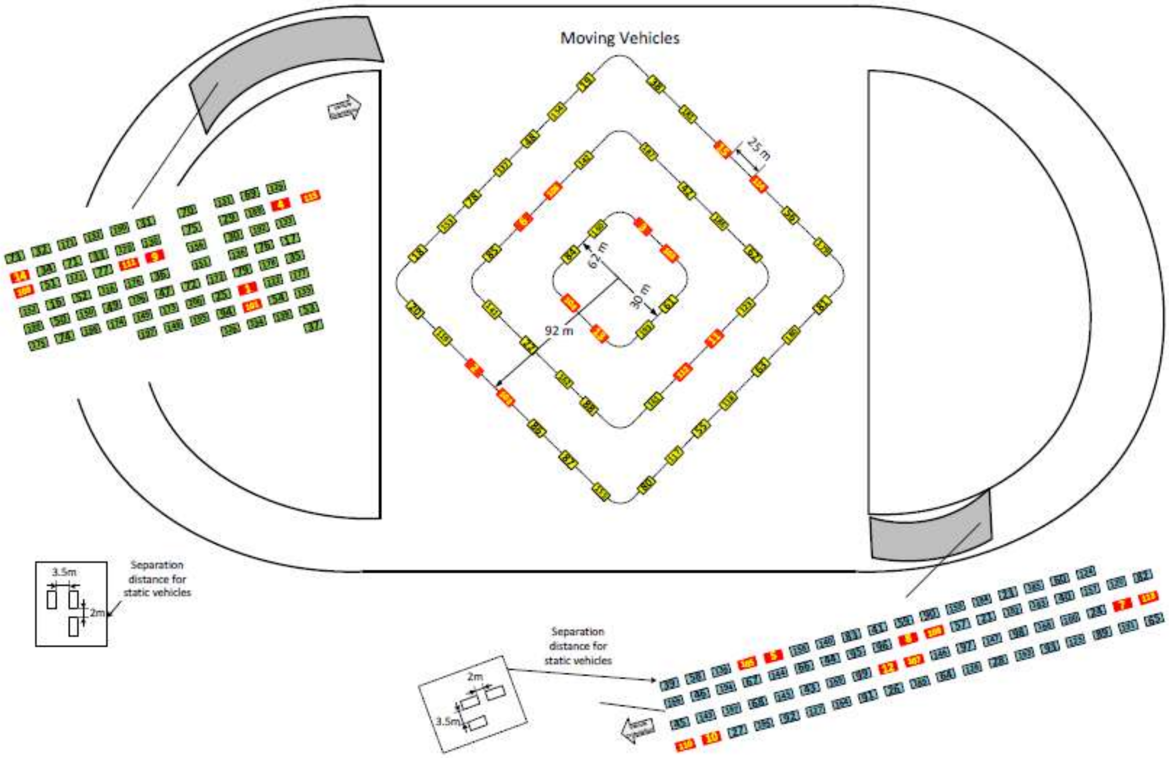
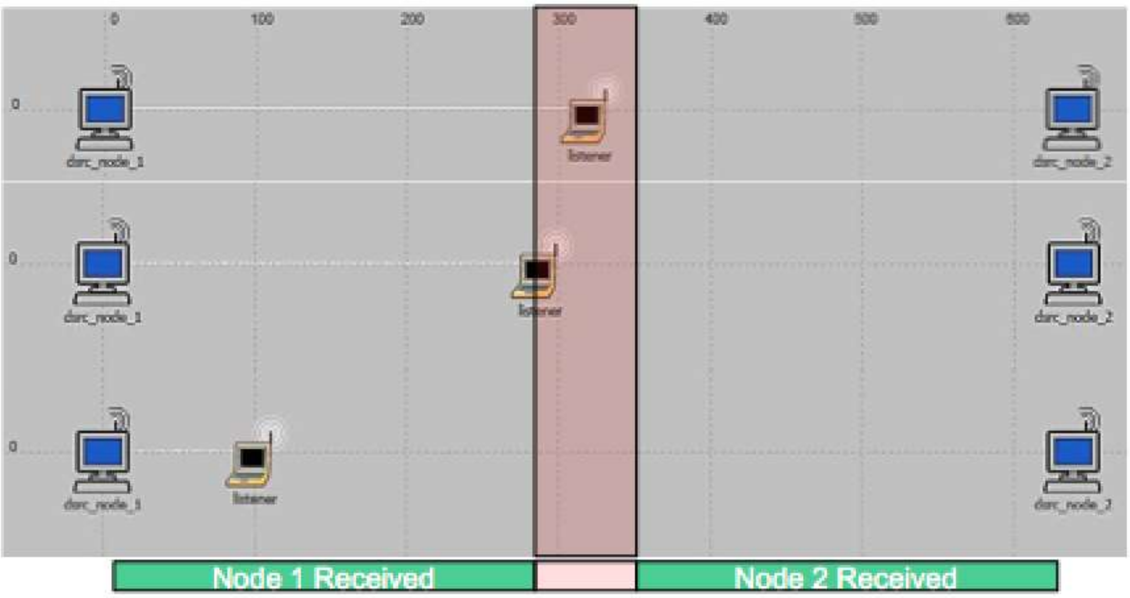

Moving Vehicles
25 m
62 m
30 m
92 m
3.5m
2m
Separation distance for static vehicles
Separation distance for static vehicles
2m
3.5m

Figure 44 is originally from the CAMP Interoperability Issues of Vehicle-to-Vehicle Based Safety Systems Project (V2V Interoperability) Phase I Final Report.

In simulations, the team examined this effect in two types of scenarios: the first scenario type, examines the effect in an evenly congested environment; while the second scenario type examines the effect in a randomly congested environment that could be a more natural on-road possibility.

To simulate the three terminal hidden node situation (as tested in the lab) the team set up two broadcasting terminals out of range from one another, and set a single listener terminal at the same distance as one of the broadcasting terminals. The message traffic generated by the two transmitting devices was synchronized to ensure that packets would collide if the system was unable to resolve a packet from one terminal that overlapped one from the other terminal. This is obviously a worst case situation, but it allowed validation of the existence of the hidden terminal effect and determination of the range at which one terminal could resolve packets over those from a more distant terminal. This setup is shown in Figure 45.

Figure 45: Hidden Terminal Simulation Setup (Source: USDOT)



In the evenly congested environment, depicted in Figure 46, the listening vehicle moves between two groupings of vehicles out of range from one another, while it is always within range of the 104 vehicles shown below. There was a total of 384 vehicles transmitting and one moving vehicle receiving (the listener). In the left block, there are 4 lanes of 64 cars in each lane (total of 256 devices). In the right block, there are 4 lanes of 32 cars in each lane (total of 128 devices). The listener vehicle begins in the center of space between two blocks.

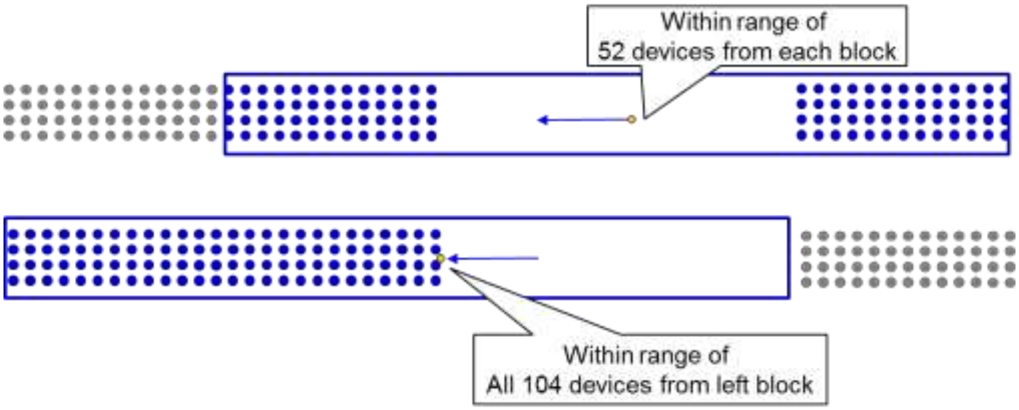
While the three terminal simulations described above were performed with synchronous message transmission, the subsequent tests of more realistic on-road conditions used asynchronous message transmission. Synchronous transmission – while clearly showing the effects of potential collisions – does not accurately reproduce the expected results outside of a simulation environment. While vehicles may have some natural asynchronism due to clock jitter and drift, there is no way to assure that this jitter will be sufficient to prevent synchronism, especially given the many synchronizing effects such as GPS data arriving at the same basic time for each vehicle, etc. In addition the requirements for reliable hazard determination will ultimately require fairly high levels of internal clock stability, so the degree of natural asynchronism may ultimately be quite small. It may thus be desirable to force some level of deliberate asynchronization to mitigate congestion and hidden terminal effects.

The uniform distribution setup simulated the situation where a large number of vehicles are lined up on a congested road. In this case the total number of vehicles is limited since, for the hidden terminal aspects of the simulation there is no point in including vehicles that would be out of range of the listener terminal. In practice there would be more vehicles, and these would cause hidden terminal effects for *other* vehicles and add to the congestion problem.

In the set up shown below, all vehicles start transmitting with uniform random distribution between 5-6 seconds. At 10 seconds into simulation, the listener moves towards the left (larger) block at a rate of 8 m/s (17.9 mph). The listener node continues on trajectory until stopping 50 seconds into simulation in front of the left block of devices. The listener moves from (0, 0) to (-320, 0) in 40 seconds.

This configuration allowed the team to focus mainly on the hidden node issue and minimize the effects of packet loss caused by congestion.

Figure 46: Hidden Node Effect in an Evenly Congested Road (Source: USDOT)



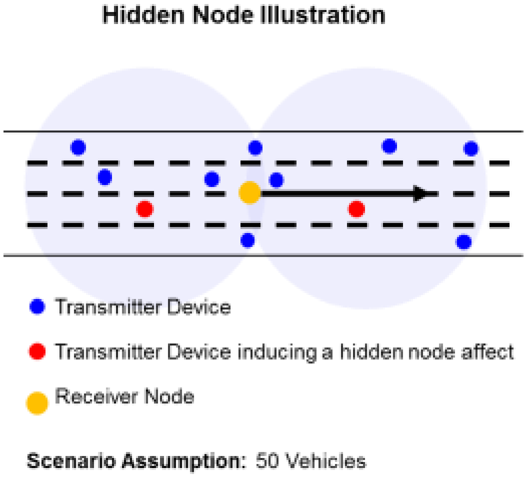
In the more natural environment, vehicles are distributed unevenly along a five kilometer stretch of four-lane highway. Again, there is only one listener vehicle that moves along the traffic. There are about 90-360 vehicles along the stretch of the highway that are transmitting.

In this scenario, the listener moves through typical highway setup with assorted device locations at “free,” “stable,” and “unstable” traffic flow conditions as described below:

- Free – n < 12 vehicles per mile per lane
- Stable – 12 < n < 30
- Unstable – n > 30
- Breakdown – n > 67

There were an average of 211 vehicles within effective range in the 8 lane highway setup.

Figure 47: Hidden Node in Randomly Distributed Vehicles on a Road (Source: USDOT)

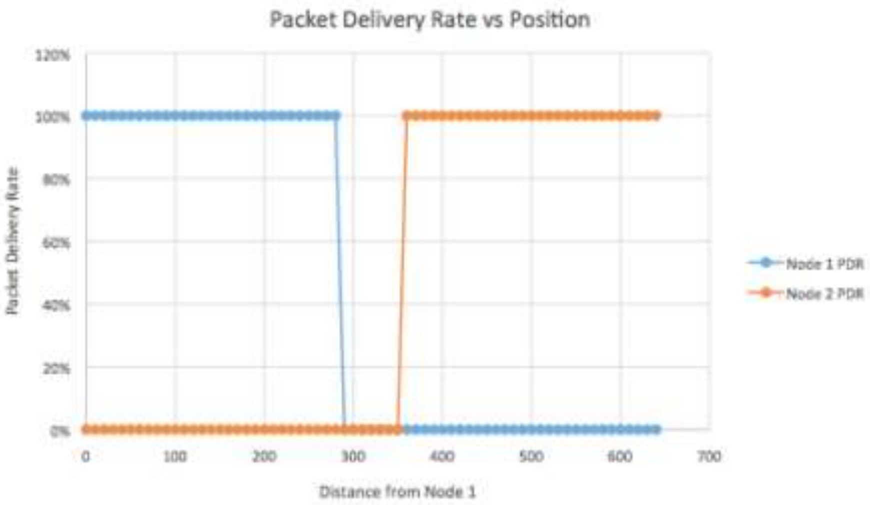

Hidden Node Illustration
● Transmitter Device
● Transmitter Device inducing a hidden node affect
● Receiver Node
Scenario Assumption: 50 Vehicles

4.1.13.2 Results, Analysis, and Findings

The analysis indicates that with synchronous message transmission the hidden terminal effect produces 100% PER in the interference region. In an evenly congested environment, the hidden node effect caused, on average, a 20% increase in PER; while in the more natural environment hidden node effect caused, as much as 5% PER. In contrast, the hidden node tests described earlier in this report indicated a worst-case loss of about 59% in the interference region.

The results of the three terminal hidden terminal simulations are shown in Figure 48.

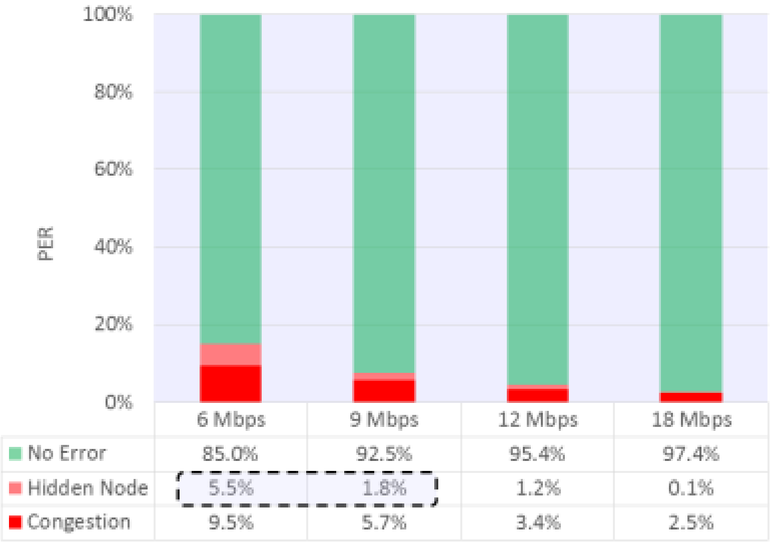
Figure 48: Packet Delivery Rate (PDR) in a 3-Node Hidden Terminal Scenario (Source: USDOT)



As can be seen in the figure, the PDR in the interference region between the terminals is zero (perfect message cancellation, or 100% PER). Within 275 meters from either terminal the PDR jumps to 100% (i.e., PER=0%). This is because at this range the relative signal levels between the messages from Node 1 on the left, and from Node 2 on the right are such that the receiver is able to resolve the signals from Node 1 and treats the signals from Node 2 as noise.

The uniformly distributed scenario simulation resulted in 15% PER at 6 Mbps and 7.5% PER at 9 Mbps. However, in this situation the number of vehicles in the test resulted in some of the packet losses occurring as a result of congestion effects, and not hidden terminal effects. About 5% PER was due to hidden node issue in the 6 Mbps case and 1.8% in the 9 Mbps case.

Figure 49: PER Caused by Hidden Node in a Randomly Distributed Vehicle Scenario (Source: USDOT)

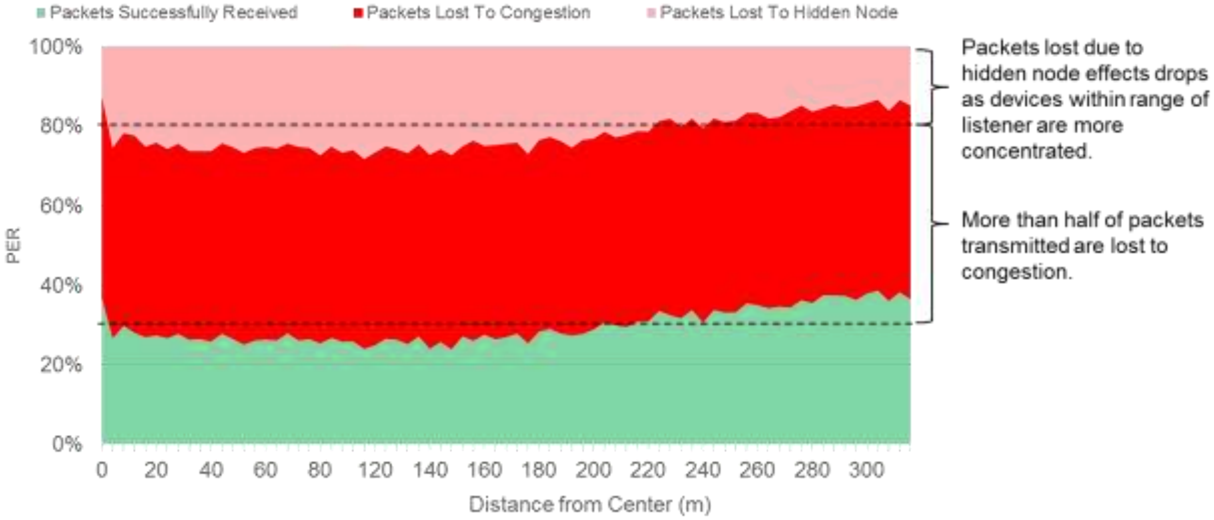


	6 Mbps	9 Mbps	12 Mbps	18 Mbps
🟩 No Error	85.0%	92.5%	95.4%	97.4%
🟥 Hidden Node	5.5%	1.8%	1.2%	0.1%
🟥 Congestion	9.5%	5.7%	3.4%	2.5%

The open road, randomly distributed scenario results are provided in Figure 49. It appears that a randomly distributed set of vehicles along the highway, which is closer to the real-world scenario, experiences less packet loss compared to the uniform distribution scenario discussed in the previous section. In both cases, increasing the data rate reduces the PER values.

Similar to the baseline hidden node, the PER was high when the listener was in the center and dropped suddenly at some point along the trajectory. The simulation of this scenario resulted in PER values shown in Figure 50. As shown, an average of approximately 20% of the packet loss is caused by the hidden node effect while about 40% of the PER is due to congestion effects when using the 6 Mbps data rate.

Figure 50: PER Caused by Hidden Node Effect in an Evenly Congested Road (Source: USDOT)

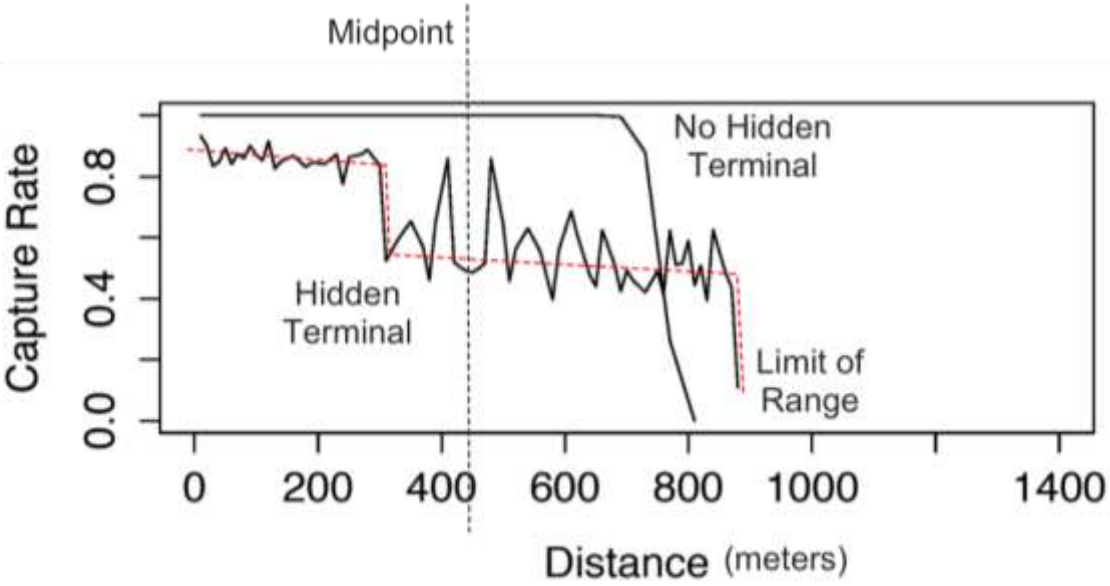


Comparing the results with the lab test

As described in more detail elsewhere in this report, the hidden node test conducted in the lab environment was done with three Supplier B devices, where two devices separated by attenuators to simulate being more an 900 meters apart (i.e., out of range of each other). The listening device was moved in the range between them by adjusting the attenuation levels between the moving unit and the two out of range terminals.

Figure 51 shows that when the listener node is in close proximity of one node (~0-300 meter), the capture ratio is around 85% (i.e., 15% PER) and as it moves toward the midpoint region between the two terminals (~300-450 meter) the capture ratio drops to around 55% (i.e., 45% PER). The 45% PER is due to the hidden node effect.

Figure 51: Capture Ratio Results for a 3-Node Hidden Terminal Lab Test (Source: USDOT)



Comparing the test to the simulation results for the three terminal test produces two observations:

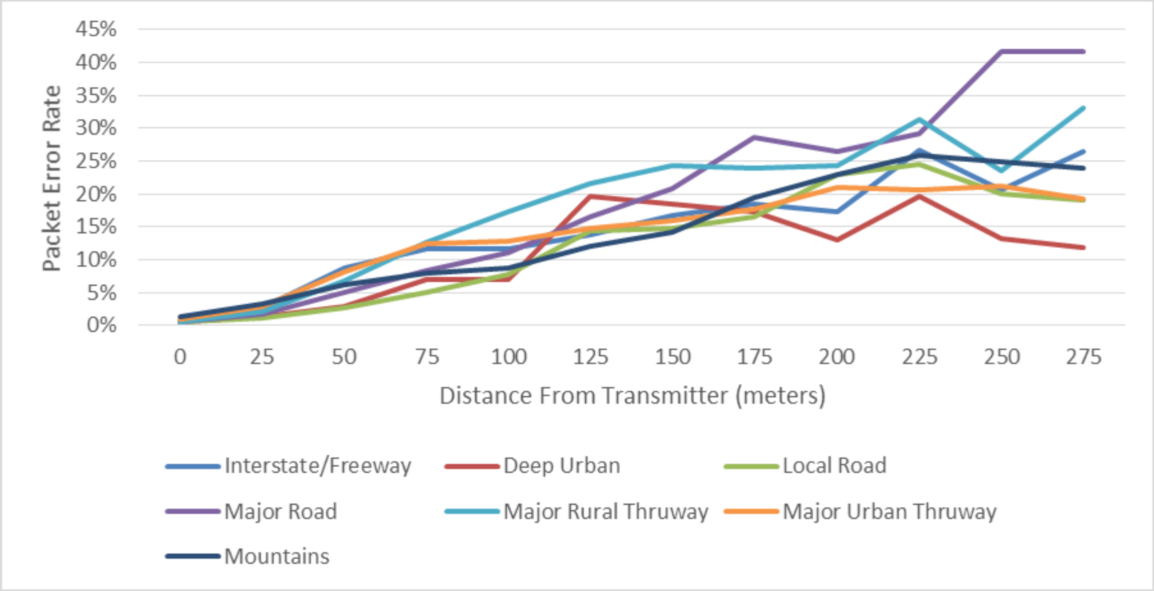
1) Both the simulation and test results indicate a “capture zone” (where the listener captures packets from the closer terminal in the presence of packets from the more distant terminal) at about 275 meters.
2) The packet delivery rate (labeled “capture rate” in Figure 51) is somewhat different between the tests and the simulations. In the simulations, the PDR is 100% in the capture zone, and zero in the interference zone. In the tests the PDR is about 85% in the capture zone and about 55% in the interference zone. The higher PDR in the interference zone appears to be due to clock jitter and drift between the two units. The clock tests indicated a standard deviation of about 2.5 milliseconds in the clock for Supplier B units. The entire message duration is only between 160 and 500 microseconds, even though the software was intended to cause synchronous message transmission, the clock jitter caused the message to become non-synchronized. The approximate 50% PER observed in the test result is indicative of losing about 50% of the interfering messages (when the clock caused the message to be sent at the same time as the other terminal, and receiving about 50% of the messages when the clock jitter causes the messages to fail to overlap in time). The small difference in PER (55% vs. 50%) is postulated to be due to the error correction inherent in the receiver. If the packets are only slightly overlapped, those packets may be saved by error correction, thus slightly biasing the PDR toward the higher value. It is not understood why the PDR in the capture region is lower than 100%, and lower than the tests when there is no hidden terminal.

4.1.14 Informing the Opnet Simulation with Field Test Data

In all the Opnet simulations discussed in the previous sections, the team used the two-ray path-loss propagation model (a standard propagation model within Opnet) which is the closest standard model for vehicular network communication. However, none of the available propagation models are the perfect match for how the electromagnetic waves broadcast in a vehicular network. It is perhaps best to use field test data for different environments.

In the CAMP *V2V Safety System and Vehicle Build for Safety Pilot (V2V-SP): Final Report, Volume 2 of 2: Performance Testing*, PER data was collected for vehicles communicating in different environments (i.e., urban, major roads, freeway, rural). This data provides PER values versus range for up to about 275 meter distance. Figure 52 captures the data that was collected from CAMP testing.

Figure 52: CAMP Field Test PER Data (Source: CAMP)



In all testing environments from CAMP testing, the amount of packet error observed was much greater at close ranges (less than 200 meters) than that of the base OPNET simulations. After conducting simulations using the two-ray path-loss model, the team decided to start building a more accurate and representative network simulation. To do this, the team created a custom packet error model based on CAMP field testing data. The custom packet error model uses a best-fit trend-line to extrapolate the trend present in the CAMP data and is configurable for all testing environments. With a linear regression, R2 values range from 0.5211 (Deep Urban) to 0.9688 (Major Road).

The team tried to use this data to establish a model for PER vs. range for each environment and use this model to inform Opnet simulations. However, there are several issues with the CAMP data.

1) The CAMP range testing data is only available up to a distance of 275 meters and the fidelity of this model is unknown when extended to greater ranges.
2) The data collected beyond 150 meter is sparse and does not follow the expected trend. The expected trend of an exponentially increasing PER with respect to transmission distance was not evident in any of the CAMP testing scenarios. Conversely, several of the scenarios show that the rate of increase in PER slows at greater distances.
3) It does not appear that the data collection has been repeated for each scenario and as a result the data may not be reliable.
4) In some instances, it was noticed that the standard deviation is greater than the mean, which makes the data questionable.

That said, the team used the data for the transmission distance of up to 150 meters and fitted a that could be used in Opnet. Figure 53 and

Figure 54 demonstrate the Opnet simulation results when using the default Opnet propagation models (two-ray path-loss model) and when using the PER model based on CAMP data. These figures also show the CAMP field test data.

Figure 53: Major Rural Thruway -- CAMP vs. OPNET Simulation (Source: USDOT)

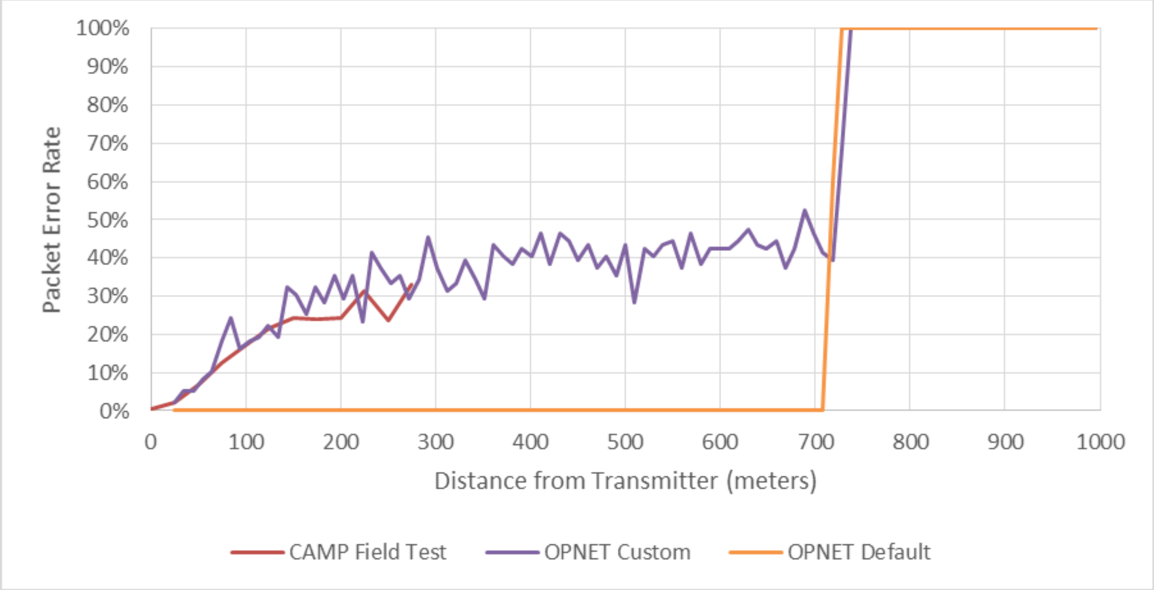
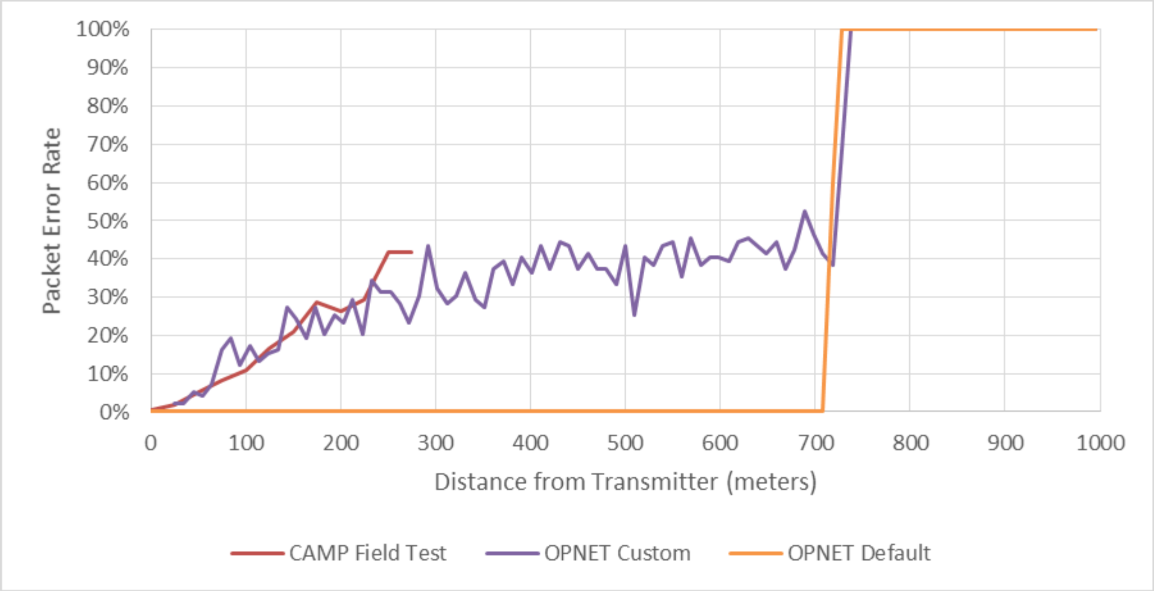


Figure 54: Major Roads – CAMP vs. OPNET Simulation (Source: USDOT)



The figures above are the simulations for only two environments: Major Rural Thruway and Major Roads.

The current Opnet model is ready to be used and provide more reliable results once a set of data with more fidelity is available. While the early simulation results support the initial motivation of a more representative packet error model, more reliable testing data is required in order to adequately model packet error across the entire effective distance of the device. The reliability of the testing data can be improved greatly by increasing the maximum transmission distance to 1000 meters, increasing the number of trials, and carrying out the testing at multiple data rates. With the new model and possible new propagation data in the future, the team could redo all simulations for more accurate results.

4.1.15 Plausibility and Hazard Detection Analysis and Simulation

4.1.15.1 Description and Rationale

The plausibility and hazard analysis is intended to inform several requirements. One set of requirements is those that govern the determination of plausibility for a received message. This is needed to support misbehavior detection. It is important that misbehavior detection be done in the same way by all vehicle systems, so there is a need to define a systematic mechanism for assessing plausibility.

In addition, the same mechanisms that are used to assess plausibility can also be used to ensure reliable and safe V2V safety operations given the inherent errors in onboard vehicle devices and errors attributable to the performance of DSRC in various environments. The core function of a connected vehicle safety system is that it be able to reliably predict a potential safety hazard using the current host vehicle dynamic state (position, speed, heading, etc.) and the data contained in Basic Safety Messages received from nearby vehicles.

To the degree that the system can identify implausible messages because they lie outside the realistic trajectory of a vehicle (including potential errors in the BSM data), it is able to reject and report implausible messages. By the same mechanism, to the extent that the BSM parameters, and/or the host vehicle state data (position, speed, heading, etc.) are in error, the system may produce faulty hazard determinations. Since both plausibility and hazard detection reliability use the same processing, and are subject to the same error effects, this simulation was intended to inform both of these aspects. Specifically, it was aimed at addressing how the system might assess plausibility, and it was also aimed at determining the maximum level of BSM errors needed to assure a given level of reliability in determining if a hazard exists.

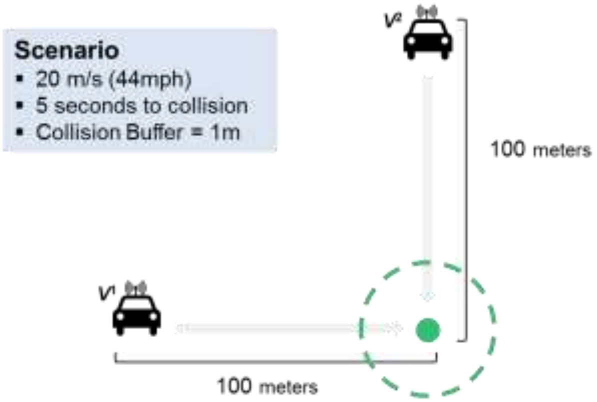
Inherent device errors being evaluated here include GPS based errors in position, speed, heading, and time synchronization as well as message losses (due to PER). Errors in yaw rate and longitudinal acceleration were also added in developing reliability metrics.

Safety implications pertaining to these errors are primarily attributed to location error distortions in the predicted trajectories of vehicles (projected positions) based on the data in the BSMs they have transmitted. In the case of location based errors, these projections may start with a point that is different from the actual vehicle position due to an inaccurate position, and/or they may introduce additional projected position errors due to errors in speed or heading. Packets lost because of communication faults mean that the projected vehicle trajectory is not updated as frequently, and this will accumulate additional position error. These inaccurate projections may cause safety applications to produce false positive results – warning the driver of a collision that is not imminent, or false negative results – not warning the driver about an impending collision. The possible consequences of these predictions can be significant since they may render the connected vehicle system unable to provide reliable safety benefits. As such, their safety implications need to be rigorously studied to determine performance measures to support safe V2V operations.

To study the safety implication of these errors, a simulation environment was constructed to microscopically model vehicle motion in a DSRC based system. This environment also has the capacity to ingest empirical estimates for the various errors and model their impact on the projections of vehicle trajectories. Safety implications were then examined with the aid of two sets of pre-defined vehicle trajectories, and their comparison with projected trajectories that incorporate the aforementioned errors. These two sets of vehicle trajectories are meant to reflect 1) a certain collision scenario, and 2) a near-miss scenario. For the certain collision scenario, the trajectories of the vehicles were configured so that the vehicles would collide in 5 seconds. Three sets of trajectories were simulated – 1) two vehicles approaching at 90 degrees at constant speed, 2) one of the vehicles having a straight trajectory at constant speed and the other having a curved trajectory at constant speed (to assess yaw rate errors) and 3) two vehicles approaching at 90 degrees with one of them having a longitudinally accelerating profile.

Figure 55 presents a high level overview of the 90-degree approach scenario for the collision case, while highlighting a few parameters of this scenario.

Figure 55: Pre-determined Collision Scenario to Evaluate the Impact of GPS-Based Error and PER on Traffic Safety (Source: USDOT)



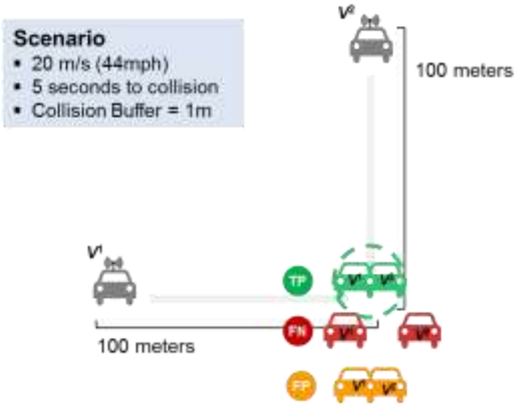
Each second prior to the collision, each vehicle’s position is projected through to the designated collision point. The end points of a pair of projected trajectories was then assessed to determine if a collision was forecasted (Collision is defined here as the distance between the vehicles at any time point in the future being less than 1.5 meters). During this assessment, multiple trials were undertaken, each trial drawing BSM parameter data for the designated trajectory from a distribution with specified statistical variances. Through multiple trials, the simulations then examined the effect of BSM parameter errors and PER (for an urban environment) in terms of the reliability of the classification of the vehicles’ predefined “collision” interaction.

Three types of classifications were defined for the types of possible vehicle-to-vehicle interactions in this scenario. These types of classifications are termed and summarized below:

- Correct Classification / Green (True Positive) – when projections correctly indicate a collision at the proper time and position;
- Accidental Correct Classification / Orange (False Positive) – when projections correctly indicate a collision but at the incorrect time and/or position;
- Missed detection / Red (False Negative) – when projections indicate no collision will occur, even though the vehicles are on a known collision course.

Figure 56 provides a visual representation of these classifications. In this figure True Positive (TP), False Negative (FN), and False Positive (FP).

Figure 56: Resulting Classification of Projected Vehicle Position in the Sure-Collision Scenario (Source: USDOT)

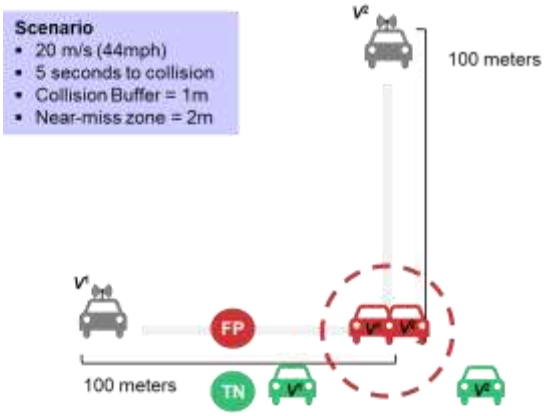


In the near-miss scenario vehicle trajectories are approximately the same as in the sure collision case. The difference in this scenario is that at the point collision the vehicles are expected to pass each other with up to 3 meters between vehicles. In this scenario only two types of vehicle-to-vehicle interactions are considered and classified. These the classifications are termed and defined below:

- Correct Detection / Green (True Negative) – when projections correctly indicate that vehicles will miss each other.
- Missed Detection / Red (False Negative) – when projections incorrectly indicate that vehicles will collide
- Accidentally Correct Detection / Yellow (True Negative) – when projections correctly indicate that vehicles will collide, but at a different location or time than the actual collision.

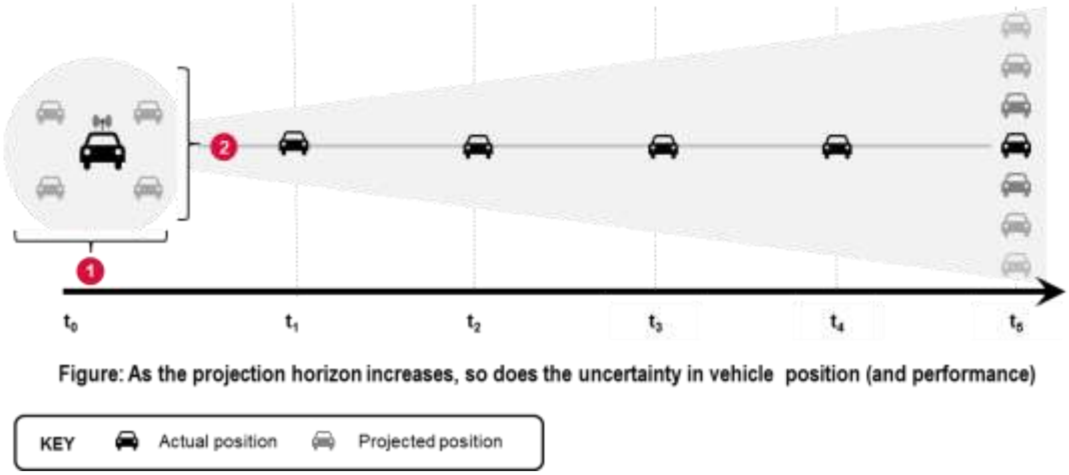
Figure 57 provides a visual representation of these classifications. In this figure True Negative (TN), and False Negative (FN).

Figure 57: Resulting Classification of Projected Vehicle Position in the Near-Miss Scenario (Source: USDOT)



These classifications of vehicle interactions are a function of the aforementioned sources of errors and how these errors affect the projection of vehicle position over time. The larger the projection horizon, the more uncertainty there is in a vehicle's future position. In propagating a vehicle's position, a new position is estimated every deci-second by using equations of motion in conjunction with perturbations in the BSM parameter values selected from empirically estimated sources. Figure 58 depicts this time propagation process.

Figure 58: Uncertainty in Projected Vehicle Positions due to GPS based and Communication Errors, and Time Horizon (Source: USDOT)


2
1
t₀
t₁
t₂
t₃
t₄
t₅
Figure: As the projection horizon increases, so does the uncertainty in vehicle position (and performance)
KEY
Actual position
Projected position

GPS position errors were obtained from a series of real world onboard device testing that had been used to determine which devices should be part of the Safety Pilot Model Deployment. The device testing exercise was intended to select a number of devices that satisfied GPS-based position, speed, and heading criteria for onboard devices developed for the Safety Pilot program. The essence of these criteria are:

- Latitude and longitude measures have to be within +/- 1.5m of the actual measurements 95% of the time

- Speed estimates have to be within +/- 0.5 m/s of the actual speed measurement 95% of the time
- Heading measures have to be within +/-2 degrees of the actual heading measurement 95% of the time

Errors due to time jitter / time synchronization per a given device collected data from an undisciplined and a disciplined clock were used. These data were collected under this task's Time Sync and Stability Testing. The collected data were then used to capture the error associated with the clock in an onboard device.

For this effort communication based error, which influences vehicle location projections, manifests itself in the form of PER. To model the traffic safety impact of PER a similar approach to incorporating GPS based errors was conducted. Raw data is modeled mathematically and incorporated into the simulation environment. Empirical PER data was obtained from CAMP's *Vehicle-to-Vehicle (V2V) Safety System and Build for Safety Pilot Project*. The data took the form of PER versus distance and was implemented in the simulation by omitting messages at a rate inferred by the PER for that range

Mathematical representations of the above errors were incorporated into the simulated environment in order to be combined with GPS based representations to perform a thorough analysis of the impact of likely errors in V2V DSRC on traffic safety.

For additional details regarding error representations incorporated throughout the analysis of their impact on traffic safety see Appendix D. Data Collection Testing and Simulation Analysis.

In representing vehicle interactions, the simulation environment facilitates the following inputs, given a predefined two vehicle scenario with a 90 degree approach angle:

- Time to Collision
- Collision Buffer (how close the vehicles must be to consider the interaction a collision)
- Position Error (Yes/No)
- Heading Error (Yes/No)
- Speed Error (Yes/No)
- Yaw Rate Error (Yes/No)
- Longitudinal Acceleration Error (Yes/No)
- Time Jitter / Time Synchronization (Yes/No)
- Packet Error Rate (for an deep urban environment) (Impacting – Yes/No)

Figure 59 provides a snapshot and summary of the features of the simulation environment that was developed to evaluate the traffic safety impacts due to prevailing errors associated with V2V communication via DSRC.

Figure 59: Summary of Simulation Environment to Evaluate Traffic Safety Impacts in V2V DSRC Domain (Source: USDOT)

Model Inputs and Assumptions

Scenario Inputs

- Sure-Collision / Near-Miss scenario
- Speed
- Approach Angle (Right angle, merge, lane change)
- Time collision
- Collision buffer
- GPS update frequency
- Environment type (urban, suburban, etc.)

Error Terms (Empirically Supported)

- GPS / OBE - based Errors (lat/long, heading, speed, clock discipline, yaw rate, and acceleration)
- PER

Propagation Assumptions

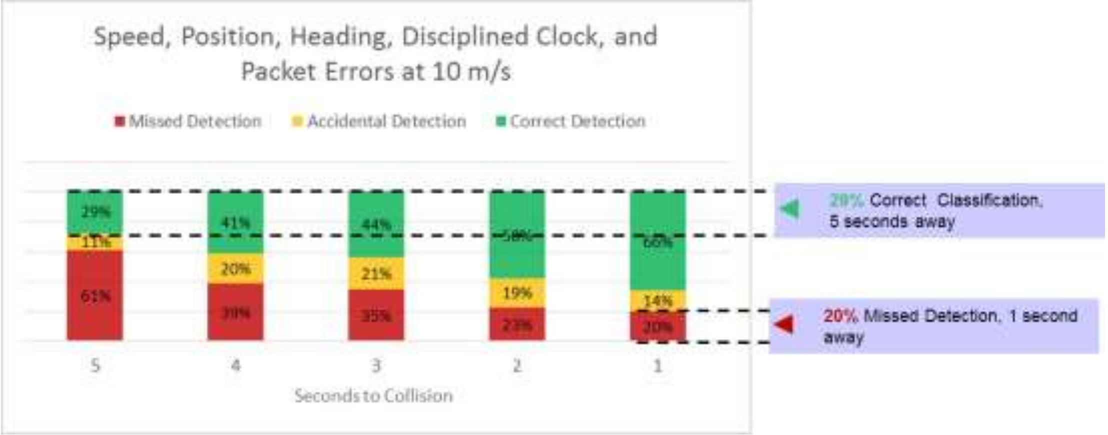
- Spatial propagation equations assumes mechanical motion
- Error propagation assumes recursive growth in errors

4.1.15.2 Results, Analysis, and Findings

In executing the certain collision scenario in the simulation environment, the primary finding is that BSM parameter errors, and those due to lost packets, have the potential to compound when propagated over time and can severely impact the plausibility reliability of hazard assessments. As such, this phenomenon has the potential to result in significant warning decision errors. Figure 60 illustrates percentages associated with the three different types of projection classifications. This figure includes five bars representing projection results each second before the crash. Each bar is comprised of the resulting classification of 1000 pairs of vehicle trajectory projections. The three colors making up each bar represent the three different resulting classifications of a pair of vehicle projections. As a reference each color is mapped to the three classification types presented in Figure 60.

As can be appreciated from the figure, the vehicles' resulting interaction (i.e., collision or miss) was misclassified 72% of time 5 seconds away from impact. The rate of misclassification was reduced to 34%, 1 second before collision. Despite this improvement, having only an 80% rate of detecting a collision in the sure collision case at 1 second before collision draws into question the safety integrity of the system, at least operating with the BSM parameter error distributions allowed for the Safety Pilot project. This conclusion is further supported by the observation that to be useful to a driver a warning should be provided about 3 or more seconds prior to any collision. Closer to the actual collision time than this does not provide sufficient time for the driver to receive, and understand the warning, and take appropriate action to avoid it. Because of this, the team used 3 seconds from the collision as a general reference point in determining effective reliability of the system.

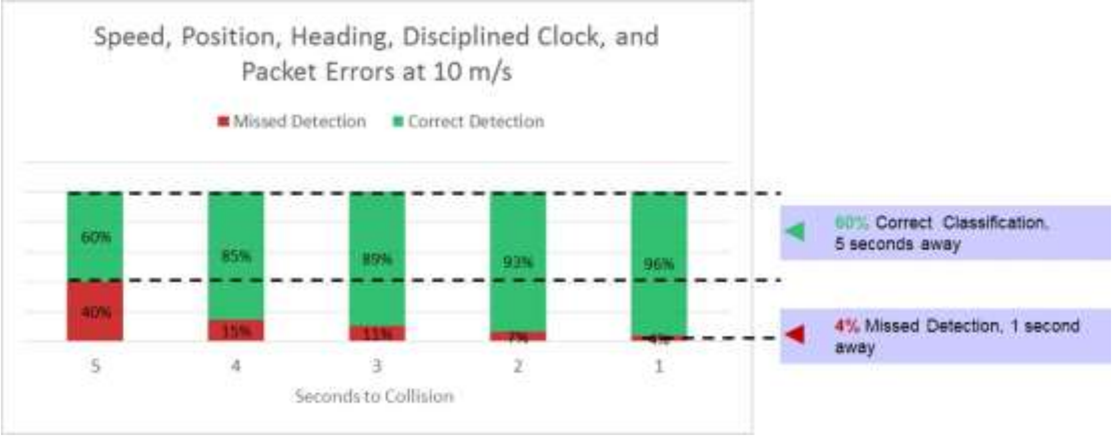
Figure 60: Percentages with each Resulting Classification from analyzing a pair of Projected Vehicle Trajectories in the Sure-Collision Scenario; each Second before Collision (Source: USDOT)



Traffic safety risks were also identified when evaluating the compounding effects of the above errors in the near-miss scenario. As expected, there are fewer traffic safety risks in this scenario from the perspectives of end result (safe passage) and that the misclassification of the vehicles' interaction will only result in an issuance of an unnecessary warning (false positive).

Figure 61 presents the results of the classification of vehicle interactions in the near miss scenario. Of note, 5 seconds away from the intersection point of the vehicles' trajectories there is a 40% chance that the prediction indicates that a collision will occur. The prediction is much better 1 second before these vehicle trajectories intersect as there is only a 4% chance that a collision warning may occur.

Figure 61: Percentages of with each Resulting Classification from analyzing a pair of Projected Vehicle Trajectories in the Near Miss Scenario; each Second before Collision (Source: USDOT)



In practice, while erroneous classifications of whether a collision is detected would provide potentially dangerous misinformation to a driver, it is anticipated that an aware driver would respond accordingly and maneuver the vehicle to safety. Notwithstanding, this study raises the awareness of risks associated with BSM parameter errors and communication based errors.

Comments

These simulations have informed two findings:

1) It appears to be possible to define message "plausibility" in terms of a deviation from the expected position at a given point in time. Since it is understood how errors will propagate over time, it is relatively straightforward to then define a plausible message as one that identifies the current vehicle position and state (speed, heading, etc.) as being within the error bounds of the previous position/state predicted from earlier data. Stated differently, if a new BSM states that the position and state of the vehicle are significantly different from what the receiving vehicle had predicted for the state of the vehicle at the time the new BSM was generated (taking into account the BSM parameter error tolerances), then either the initial BSM(s) were wrong, or the current BSM is wrong. In either case, the vehicle appears to be misbehaving, and may need to be inspected. The receiving vehicle may still choose to make use of the messages, but it may also discount the validity of the data from this suspect misbehaving vehicle.
2) Errors that fall within the currently accepted "normal behavior" of connected vehicle devices appear to create sufficient uncertainty in the predicted vehicle position, especially at prediction intervals that collision detection decisions (i.e., warning decisions) need to be made (i.e., the 2.5 to 3.5 second stopping sight distance). The team characterized and modeled these decision errors and have proposed initial accuracy requirements that would provide a 90% collision classification reliability. However, this would likely require a policy decision by NHTSA as to the allowable false detection or missed detection levels. For example, if the objective is that the system must not miss more than 5% of actual collisions, the resulting BSM parameter accuracy requirements will need to be much tighter. If the objective is 99.999% (0.001% classification failure) reliability, then the system is probably not viable. Once an allowable false alarm and/or missed detection rate is identified, one can use these simulation setups to analyze the allowable BSM parameter errors, and thereby arrive at an error allocation between the various BSM parameters.

4.1.15.3 Reliability of Results

The above section illustrates that errors associated with measures contained in BSMs can lead to misclassifications of vehicle interactions. Although the probability of misclassifications reduces as the time to collision decreases, the chance of a misclassification occurring, even at 1 second prior to collision, is concerning. To help inform an understanding of how to improve the accuracy with which vehicle interactions are classified, despite errors in BSM measures, this task established a two part criterion to reflect an acceptable level of classification accuracy, relative to a time to collision metric. This level of acceptability criterion for correctly classifying vehicle interactions was set to 90%, 3 seconds before collision. The parameters of this criterion can be thought of as putting forth an acceptable level of accuracy for hazard detection and a time gap that, under normal driving conditions, can afford a driver sufficient time to respond to an alert and execute the necessary maneuvers to avoid a collision.

With this criterion in place, attention is then placed on understanding the form of the errors that are associated with each measure within a BSM. Toward this end, a series of evaluations were conducted to determine what magnitude of BSM parameter errors will satisfy the above criterion. These evaluations were conducted with each error term in isolation and then all errors acting in concert in a given situation. Table 12 provides a set of error levels, for each error term acting in isolation, which satisfies the aforementioned criterion. These error levels / tolerance values are standard deviations from zero error and should be interpreted that at least 95 percent of the reported values must fall within an envelope of this standard deviation. Given that the errors assume a normal distribution, 95 percent of the reported values will fall within a standard deviation from the mean value.

Table 12: Derived error tolerance levels versus observed field errors

BSM Parameter	Maximum Isolated Values determined by Simulation	Safety Pilot Observed Capability
Positional Error	0.43 m	0.53 m
Speed Error	0.17 m/s	0.13 m/s
Heading Error	0.9 degrees	0.82 degree
Time Error	17 msec	Vary – un/disciplined clock
Packet Error Rate	10 percent	Vary with respect to distance
Yaw Rate Error	0.8 deg/s	Data not available
Longitudinal Acceleration Error	0.14 m/s/s	Data not available

Table 12 also includes standard deviations for these measures as derived from the field. While these values are of similar magnitudes, their impact on the classification of vehicle interactions, as indicated by the above results, are very different. The central difference, as compared to the above results, is that the 3 seconds from collision the field based errors enabled correct detection of a collision 65% of the time while the above error tolerance measures met the 90% criterion. Part of reason for this discrepancy in classification probability is that the analysis which included field based error tolerance measures was conducted with the errors acting in concert versus in isolation, which is the case when determining “Safety Pilot Observed Capability” in the table above.

When searching the solution space for individual error tolerance levels, so that when acting in concert the above criterion is met, several solution sets exists. Table 13 presents two sets of error tolerance levels and allocations for each measure that when acting in concert satisfy the pre-defined criteria, with vehicles traveling at 10 m/s. The magnitude of the sample set of error tolerance values are now different from the field based values above. This is a result of the need for more accurate measures to not only meet the above reliability criteria but to account for the compounding effects of these errors acting in concert.

Table 13: Sample sets error tolerance values for each BSM parameter versus field derived error tolerance values

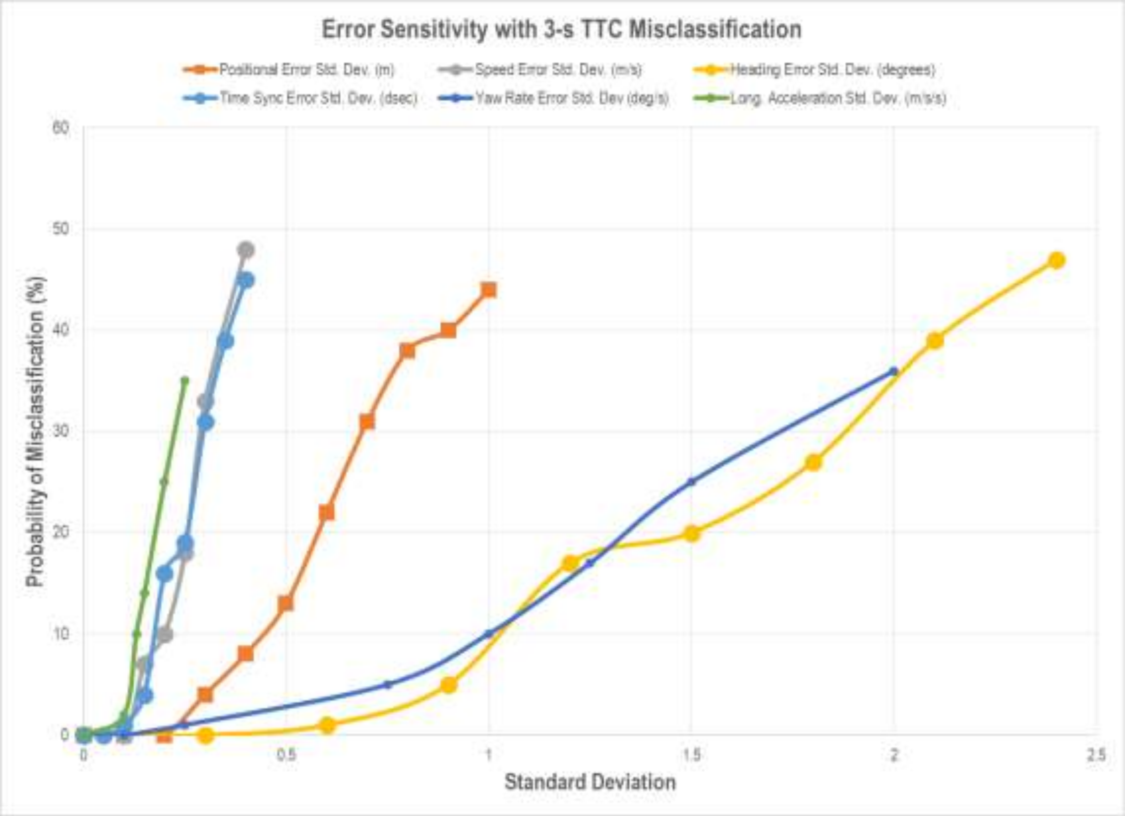
BSM Parameter	Example 1	Example 2	Field Based Std. Deviation (Safety Pilot Observed Capability)
Positional Error	0.2 m	0.15 m	0.53
Speed Error	0.15 m/s	0.11 m/s	0.13
Heading Error	0.2 degrees	0.15 degrees	0.82
Yaw Rate Error	0.1 deg/s	0.05 deg/s	Not Available
Longitudinal Acceleration Error	0.1 m/s/s	0.05 m/s/s	Not Available
Time Sync Error	2 ms	2 ms	Vary – un/disciplined clock
Packet Error Rate	2 %	2 %	Vary with respect to distance

An exact set of recommended error tolerance levels to ensure reliable, correct classifications requires a more robust series of analyses. The derivation of the above reliability criterion will also have to be evaluated as such a criterion ought to be on a spectrum to ensure that reliable classification of vehicle interactions are achieved under various driving conditions. While this series of analyses are outside the current scope of this report, the above communicates both the associated necessity and complexity of the problem. As such, it is conceivable that this set of analyses ought to be a part of another focused effort to derive a set of robust error tolerance measures and reliability criteria.

However, despite the need for a more complete set of analyses to develop a robust set of requirements for error tolerance levels, a preliminary set of values for these levels is possible given the data on hand. These preliminary set of values are determined from quantifying the sensitivity of the error tolerance level of each error term and representing their contributions to a predefined, acceptable probability misclassification of vehicle interaction. This acceptable rate of misclassification is born out of the above reliability criterion of correctly classifying vehicle interaction 90% of the time when time to collision is equal to three seconds. This criterion translates to an acceptable misclassification rate of 10%.

To derive a preliminary set of error tolerance levels, the rate of change in probability of misclassification with respect to variance in error measures were computed. This rate quantifies the sensitivity of each error measure. This assumed linear relationship between rate of misclassification and variance is evidenced in Figure 62.

Figure 62: Error Sensitivity with 3-s TTC Misclassification (Source: USDOT)



Also, assuming that each of these error terms equally contribute to the overall error when classifying vehicle interactions, the following equation was used to determine an acceptable error tolerance rate for each measure:

$$AErT_i = \frac{2 \times Err_{Max}}{N * S_i}$$

Where:

AErT$_i$ – Acceptable Error Tolerance (for each ith measure)
ErrMax – Maximum (Allowable) Error in vehicle interaction classification
N – Number of error terms
S$_i$ – Sensitivity Factor (for each ith error term)

Table 14 presents the results from applying this equation as well as the sensitivity factor for each error term. These values represent one possible solution set, wherein each parameter contributes equally to the overall classification error.

Table 14: Recommended error tolerance levels for each BSM parameter as informed

BSM Parameter	Sensitivity Factor	Acceptable Error Tolerance (STD)
Position	41 (%/m)	0.081 m
Speed	95 (%/m/s)	0.035 m/s
Heading	16 (%/degree)	0.209 degrees
Yaw Rate	12 (%/deg/s)	0.278 deg/s
Longitudinal Acceleration	30 (%/m/s/s)	0.11 m/s/s
Time Synchronization	97 (%/decisecond)	34 ms

However, having all the device errors contribute equally to the overall error is not necessarily the most realistic approach since different types of sensors have different error rates and priorities in BSM generation. Hence, weighted values may be utilized to determine these tolerable errors. For example, three scenarios of error weights are provided in this report:

1) Scenario 1 – Equal distribution of errors so that 10% allowable error is distributed equally for the six parameters.
2) Scenario 2 – 70 percent of allowable errors allocated to positional errors and the other 30 percent distributed among the remaining five parameters.
3) Scenario 3 – 70 percent of allowable errors allocated to positional errors and 1 percent allocated to time errors. The remaining 29 percent will be distributed among speed, heading, yaw rate and longitudinal acceleration.

These values are of errors, when used in the simulation, produce probabilities of misclassification as shown in the following table.

Table 15: Comparison of different scenarios of recommended error tolerance values and the resulting percentage of misclassification

Parameter	Scenario 1	Scenario 2	Scenario 3
Position	0.082 m	0.342 m	0.325 m
Speed	0.035 m/s	0.012 m/s	0.015 m/s
Heading	0.021 deg	0.075 deg	0.1 deg
Time Jitter	34 ms	12 ms	2 ms
Yaw Rate	0.28 deg/s	0.1 deg/s	0.12 deg/s
Longitudinal Acceleration	0.11 m/s/s	0.04 m/s/s	0.04 m/s/s
% Misclassification at 3s from collision time			
Speed = 10 m/s	4%	10%	9%
Speed = 20 m/s	14%	12%	10%

Clearly, scenario 3 is a more acceptable scenario as far as the probability of misclassification is concerned since positional accuracy requirement and others are relaxed when compared to the other two without sacrificing the accuracy of collision detection. While additional research is needed to declare final allowable error tolerances for each BSM measure, the results in the above table provide a preliminary set of values that each BSM measure be accurate within to meet the above reliability criterion. As further research is conducted, these tolerance levels should be modified to ensure applicability across the range of driving conditions as well as account for the interactions of these errors terms.

It is important to note that this analysis is not concerned with the feasibility of meeting these accuracy requirements. It is, instead, based on the objective of creating a V2V safety system that can reliably provide safety benefits (i.e., reliably predict collisions and near misses within the time frame that a resulting warning and driver action can mitigate the hazard). While it is tempting to entertain the alternative approach, wherein the BSM parameter error tolerances are governed by what may be achievable in a cost effective system, such a system, while affordable, is not likely to represent a good value because it will fail to deliver the promised benefits. A safety system that is feasible to build, but does not provide reliable safety benefits is not particularly useful. If these requirements are seen as challenging, then meeting them in a cost effective way should become a focus of next steps in research.

4.1.15.4 Previously Established Guidance on Error Tolerance for Select BSM Measures

For the Safety Pilot Model Deployment, an extensive set of device testing activities were conducted. One of the objectives of these tests was to ensure that devices participating in Model Deployment activities were able to support the goals of the deployment by supplying accurate and reliable collected and transmitted data. A product of these testing activities is a data set that presents the real-world performance of these devices in receiving and transmitting BSMs. These data sets were used above to develop error distributions that influenced vehicle interaction classification. While these data sets were used to determine if a device would be included in the Safety Pilot Model Deployment, they did not go as far as using these data to establish performance criteria for the devices.

It is also important to note that there have been no known on-road tests where vehicles were started on a deliberate and certain collision course with an un-prepared driver and then based on the BSM data the system generated warnings. Such tests are inherently dangerous since they will result in collisions if the system fails or if the driver fails to react appropriately. While the Safety Pilot program certainly accounted for the sending and reception of BSMs, there are relatively few vehicle interactions and no known identified situations where vehicles were on collision courses and the system properly warned the driver, or where vehicles were on a near miss course and the system accidentally warned the driver. There were indeed warnings issued, but the specific ground truth data for the vehicles is not available, and thus it is not known if these were actual collision courses or near miss courses, and thus cannot tell if the results were true or false. Lacking complete truth data, it is difficult to sort out the true positives, true negatives, false positives, and false negatives. In terms of the driver clinics performed several years ago, the use of professional drivers who were expecting the warnings indicates that, while these clinics were useful to demonstrate the concepts, they are not definitive in terms of assessing the level of BSM accuracy required to reliably predict collisions. Lastly, the origin of the Safety Pilot requirements appear to be in the original EdMap project. This project provided the first deep dive into the sort of map accuracy and position accuracy that might be required in connected vehicle safety systems. It appears, however, that the results of this study are aimed more at the level of accuracy needed at the time of collision (i.e., how accurately does the vehicle position need to be known at a potential collision point in order to properly classify the interaction - collision or miss). Viewed in this way, the resulting requirements appear to be consistent with the results of the current study. The difference being that in this study the team rolled back the clock to the time when the BSM (on which the collision detection is based) was sent, and examined how the propagation of initial errors in the BSM will evolve as the prediction is carried forward in time. In essence, it appears that in order to achieve the safety pilot (or EdMap) requirements at the moment of collision (or miss), the BSM on which a prediction of that collision (or miss) is based (i.e., the BSM sent 3 seconds earlier) must be significantly more accurate.

Table 16 presents the criteria used within the Safety Pilot Model Deployment, as “CAMP Recommended Maximum Error.” To compare the traffic safety impacts of these recommended maximums to the results from the above analyses, these values were modeled as error distributions. These error distributions are assumed to be normal with mean zero and standard deviation equivalent to half the recommended maximum error. This value for standard deviation was chosen so that 95% of all measured errors is less than the maximum recommended value, a reasonable assumption for the situation at hand. Entering this distribution into the developed modeling frame work from Table 16 in Appendix D. Data Collection Testing and Simulation Analysis generates the probability of misclassifying vehicle interaction 3 seconds before collision.

Table 16 also compares CAMP informed error values to those recommended by the above series of analyses. While CAMP’s recommendations were effective in supporting the Safety Pilot Model Deployment, it is evident that for wider deployment of this technology there will be a need to collect and transmit accurate reliable results to support traffic safety, at least in the situation being investigated, and tighter error tolerances are recommended by the above analysis[9].

[9] A simple cross check on these requirements is helpful in understanding them. At 27 m/s (100 kph) the vehicle travels 81 meters. If the heading is off by 3 degrees (the Safety Pilot heading tolerance from Table 15), then the predicted position 81 meters ahead will be off by 4.2 meters =2*81*sin(1.5), well outside the 1.5 meter “collision buffer” suggested. If all other parameters have zero error, then a 1.5 meter initial position error will result in a predicted position 3 seconds in the future that is 1.5 meters (the maximum allowable error) from the actual position. If both position and heading are in error by their maximum tolerances allowed in the Safety Pilot requirements, the predicted position 3 seconds in the future will be off by 6.7 meters (22 feet).

Table 16: Comparing CAMP informed error tolerance levels to those derived from this round of analyses

BSM Parameter	CAMP Recommended Error Tolerance	BAH Recommended Error Tolerance
Horizontal Position	1.5 m	0.32 m
Vertical Position	3 m	2 m
Speed	0.35 m/s	0.015 m/s
Heading	2 to 3 deg	0.1 deg
Time	1 ms	2 ms
Longitudinal Acceleration	0.1 m/s/s	0.04 m/s/s
Yaw Rate	0.5 deg/s	0.12 deg/s

5 Developing DSRC OBE Security Requirements

A critical part of developing a functioning and trusted system for V2V communications is having the right security system in place to allow for the trusted and verifiable exchange of messages between vehicles and between vehicles and the roadside infrastructure. While this project focuses on the performance requirements for DSRC devices to enable safety critical messages and warnings, the security requirements for those devices must also be enumerated. This section contains information on the Booz Allen team's efforts to develop DSRC OBE security requirements.

At a high level, there are two types of security requirements: communications security requirements and platform security requirements. Communications security requirements can be further subdivided into requirements for communications security itself, and requirements for management of information related to communications security – in this case, keys, certificates, and revocation lists (security management requirements). Communications security requirements give assurance that a message can be trusted, so long as the device sending the message has not been compromised. Platform security requirements give assurance that the device sending the message will not be compromised.

Communications security requirements are satisfied by conformance to the relevant specifications, in this case IEEE 1609.2 as profiled by SAE J2945/1. There are performance requirements associated with communications security, which are in general derived from a need to meet the performance requirements of the communicating applications.

Security management requirements include communications security requirements for the communication of security management information, and performance requirements for storage and processing time to support security management operations. Neither of these requirements are satisfied by conformance to existing (or about-to-exist) specifications, so this report provides recommended requirements for both of these categories. Note that CAMP is producing a specification for a protocol for security management operations, but it will not necessarily be required that devices conform to this specification, and as such there is value in this report providing an independently derived set of requirements for security management.

Platform security requirements are not satisfied by conformance to any existing or planned communications security standards and such are the main focus for the security work conducted in this project and reported on in this report.

The importance of understanding the implications of adequate security (or lack thereof) for connected vehicles cannot be understated. In recent events, two technology researchers were able to hack into Jeep vehicles, prompting Fiat Chrysler to recall 1.4 million vehicles. The researchers were not only able to gain control of features such as radio and air-conditioning, but they were also able to take control of the engine and brakes. This highlights the reality that hacking has moved into the safety and transportation realm.[10] Because DSRC devices will be connected to the control systems of the vehicle, NHTSA needs to consider how to protect the information and access on these devices.

On July 21, 2015 a bill (S.1806) was introduced in the Senate, named the “Security and Privacy in Your Car Act of 2015” or “SPY Car Act of 2015.” If the provisions were to become law, the legislation would establish a 6.5 year timetable for the Federal Trade Commission (FTC) to promulgate and make effective privacy standards for motor vehicles providing for transparency, consumer control, and limiting the use of personal driving information for marketing, with exceptions for crash avoidance technology, among other things. The legislation would also impose a 6.5 year timetable for NHTSA to promulgate and make effective security rules for vehicles. The scope of these rules entail: protection against hacking, providing for security of collected information, equipping vehicles with capabilities to detect, report and respond to hacking, and labeling the vehicle with a “Cyber Dashboard” to inform consumers the extent to which that vehicle exceeds the minimum standards set by the FTC. This Congressional interest further underscores the need to design security and privacy requirements into the framework of the system and not to try to include it as an afterthought. Since these requirements, if enacted, are years away from begin effective, there are no specific provisions that would currently impact this task or current security designs. However, due to recent recalls (Jeeps, for example), the Booz Allen team is aware of the aforementioned issues that are present by the legislation, so that the team can help NHTSA anticipate future rulemaking issues and solutions.

If offered as an amendment to House of Representatives (HR) HR-22, the USDOT Surface Transportation Reauthorization, the SPY Act would be a germane amendment since HR 22 reauthorizes the NHTSA programs. Additionally, it is important to note that the bill would face serious floor or committee objections, as one of the sponsors is the ranking democrat on the Senate Commerce sub-committee. Also, since the bill merely adds additional rulemaking authority, it is not likely to be objectionable to USDOT or the FTC.

This report contains security objectives and (in Appendix F. Full DSRC OBE Security Inputs Analysis) security functional requirements to provide: 1) performance requirements for secure communications and communications security; 2) performance requirements for security management; and 3) platform security requirements. These functional requirements are intended to be used to create a number of regulatory and/or industry control documents to which device suppliers and OEMs can determine conformance.

The team notes two important considerations to do with conformance claims.

1.) Format for conformance claims and methodology for testing: There are a number of different formats for stating platform security requirements such as the CC, or the Federal Information Processing Standard (FIPS) 140 or FIPS 199 standards produced by the National Institute of Standards and Technology (NIST). For these three different candidate formats there are different degrees of: (a) flexibility of the template for specifying security requirements and (b) availability of existing expertise in providing testing. The availability of existing expertise in testing for conformance to the specifications is a key factor as USDOT does not currently have this expertise in-house and would find it difficult to develop. A security standard that already supports a competitive market in conformance testing offers advantages to one for

[10] Fiat Chrysler Issues Recall Over Hacking, New York Times, http://www.nytimes.com/2015/07/25/business/fiat-chrysler-recalls-1-4-million-vehicles-to-fix-hacking-issue.html?emc=edit_th_20150725&nl=todaysheadlines&nlid=21472973&_r=0.

which multiple test labs are not currently available. This leads the team to recommend the development of a Common Criteria Protection Profile as the means of specifying platform security requirements. FIPS 140 has a large number of existing test labs but is not flexible. FIPS 199 is flexible but does not have a network of existing test labs. Only the Common Criteria meets both requirements. More detail is provided in Section 5.2.

2.) Security requirements may change over time: The security of the system depends in part on the following four factors:
    a. Hardware security
    b. Software and OS security
    c. Denial of service protection
    d. Misbehavior detection and reporting

For each of these, the appropriate definition of security will change over time as both attacks and defensive technologies will evolve. For purposes of this project the team simply identifies that all of these must follow current best practices. The team recommends that the industry establish an ongoing body with authority to make a statement of current best practices, the organizational and governance design of which is to be determined. In Appendix I. Overview of Cybersecurity Guidance and Best Practice Management in Other Industries, the team provides an overview of what best practices might mean and how evolving best practices are managed in other industries.

In addition to the above, the security of the system depends on the following factor that is likely to change over time, security of cryptographic algorithms.

It is extremely likely that the currently selected cryptographic signature algorithm, the Elliptic Curve Digital Signature Algorithm (ECDSA), will be made obsolete by the development of quantum computers. It is also nearly certain that quantum computers will be developed in the lifetime of the first vehicles produced under the mandate. As such it is vital that the system is developed in such a way as to survive a migration to a new cryptographic algorithm. This migration need not be done precipitously, as it is likely that there will be good notice of the technological advances that will lead to a break. However, the migration needs to be planned for on day 1. This task is made more complex by the fact that no algorithm has been identified that is a suitable successor to ECDSA, and all possible candidates have significantly larger keys and/or signatures.

To support the ability to migrate, the Booz Allen team has identified advantages by doing the following:

a. 20 MHz channels supporting 18 Mbps: this provides flexibility in migrating to cryptographic algorithms that result in great packet size overhead. The implications and additional decisions that need to be made for such a change are primarily described in Sections 4.3.1, 4.3.3, 7.1.4, and 7.2.
b. Implementation should support reconfigurable hardware of cryptographic algorithms: Both signing and verification should be implemented in software on physically and logically hardened general purpose processors to avoid the need for a recall and physical replacement of cryptographic processors when cryptographic migration becomes necessary
c. Implementation should support secure over-the-air firmware update on OBEs: Knowing that a change of algorithm will at some point become necessary, only secure over the air update allows for the system to migrate to new cryptography without the expense, disruption, and incomplete dissemination effects of a recall
d. Implementation should support either quantum-safe signature algorithms, or migration to quantum-safe signature algorithms, for authenticating updates: Secure firmware updates cannot rely on a quantum-vulnerable key burnt into hardware. The update mechanism must either be quantum-safe or itself be capable of update

Summary of Recommended Security Requirements

This subsection summarizes the recommended DSRC OBE security objectives that precede actual security functional requirements, contained in Appendix F. Full DSRC OBE Security Inputs Analysis. These requirements are technical in language, following standard Common Criteria norms, so objectives are included here as there is matching of objectives to requirements, but the latter are more digestible for a larger audience. The security functional requirements (SFRs) are meant for consideration by NHTSA as possible inclusion to an FMVSS or to be released as industry guidance or other approach as described in the subsection on "Use of Regulations or Other Approaches" in Section 7.12. The subsequent sections describe why the development approach was selected and include the summary information of the various pieces of a comprehensive requirements development process. Recommended core security functional requirements rely on the (yet to be completed) CAMP SCMS Specification and IEEE 1609.2 as the foundational specification and standard, respectively. Complying with the specification and standard will satisfy a significant number of recommended requirements as these are core specifications for secure V2V DSRC communication.

Security objectives reflect how to guard against threats at all stages of the device lifecycle for the safety applications use case. The team identified and described objectives for the vehicle (TOE) and the operating environment. These include 39 objectives for the vehicle (TOE), ten of which are optional and eight of which affect only receive-side. In addition, 27 objectives are specific to the operating environment. Appendix F. Full DSRC OBE Security Inputs Analysis contains the detail for all referenced sections.

5.1.1 Security Objectives

This section defines security objectives both for the TOEs and their Operational Environments (OEs). Table 17 states objectives corresponding to all threats, assumptions and security policies. Objectives for security policies and assumptions are derived directly from the security policies and assumptions and are included for completeness. The description of the objectives in the table is kept compact; for objectives that need a more detailed description, a description is provided in the notes after the table.

As with the specified policies, the objectives are at two levels of priority: recommended requirement (R) and recommended best practice (BP). Recommended requirements are believed by the Booz Allen team to be necessary for the success of the system. Recommended best practices are believed to be useful for the success of the system but the system can succeed without them. Where objectives are noted as (recommended) best practices rather than (recommended) requirements, a rationale is given for this.

The next two columns specify the applicability of different objectives: whether a given objective is applicable to send or receive side or both, and to what TOE level, such as the entire system, the vehicle, the DSRC device, or components inside the device.

The final column of Table 17 indicates whether the objective is met by conformance to the existing interface/communications security specifications, IEEE 1609.2 and the SCMS specification, is sufficient to meet the objective or whether additional testing/certification beyond conformance testing is necessary. It can be seen that conformance to the interface specifications provides assurance of meeting only a small proportion of the objectives.

Table 17: Security Objectives

Objective ID	R / BP	Send / Receive (S/R)	TOE Level	Description	Addressed by existing spec
O.Algorithm.1	R	R	Vehicle	If the TOE determines that a BSM warrants action, it shall verify the signature on any BSM before taking action on it.	X
O.Algorithm.2	R	S+R	Device	TOE shall use secure cryptographic schemes to perform different operations, such as sign BSMs, encrypt PCR, etc.	X
O.Algorithm.3	R	S+R	Device	TOE shall simultaneously change certificates and identifiable information from time to time as necessary to improve privacy protection.	
O.Algorithm.4	R	S	Device	TOE shall check the validity of certificates before using them to sign BSMs.	X
O.Component.1	R	S+R	Vehicle	Essential components (e.g., OBE, sensors, Global Navigation Satellite System [GNSS] receiver) within the TOE shall have secure connection with each other (see NOTE 1)	
O.Component.2	R	S+R	Vehicle	The TOE shall determine whether a secure connection exists between essential components and shall prevent the generation of BSMs if this secure connection does not exist. See NOTE 1 for discussion of secure connections.	
O.Component.3	R	S+R	Vehicle	TOE shall continuously monitor essential components within the TOE to ensure that the secure connections of O.Component.1 and O.Component.2 are in place and that components are functioning correctly. See NOTE 1 for discussion of secure connections. See NOTE 2 for discussion of correct functioning.	
O.Component.4	BP	S+R	Vehicle	TOE shall create secure logs based on its monitoring of essential components. **BP Rationale**: See P.Component.4.	
O.Component.5	R	S+R	Vehicle	TOE shall inform the driver when essential components (e.g., OBE, sensors, GNSS receiver) within the TOE are not functioning properly.	
O.Component.6	BP	S+R	Vehicle	TOE shall report to external authorities (i.e., SCMS) or maintenance services when essential components (e.g., OBE, sensors, GNSS receiver) within the TOE are not functioning properly. **BP Rationale**: See P.Component.6. See NOTE 3 for further discussion of reporting.	

Objective ID	R / BP	Send / Receive (S/R)	TOE Level	Description	Addressed by existing spec
O.Connect.1	R	S+R	Device	TOE shall have sufficient connectivity with SCMS for necessary security management operations including pseudonym certificate provisioning, downloading CRLs, and uploading misbehavior reports.	
O.CRL.1	R	R	Device	TOE shall have sufficient resources to store and process CRLs.	
O.CRL.2	BP	R	Device	TOE shall support mechanisms for collaborative distribution of CRLs. **BP Rationale**: See P.CRL.2.	
O.CRL.3	R	R	Device	TOE shall attempt to update CRLs based on the CRL update frequency.	
O.Data.1	R	S	System	TOE shall as far as possible use verified-correct GNSS data. See NOTE 4 for discussion of verified-correct GNSS data.	
O.Data.2	R	S	Vehicle	TOE shall ensure that sensor data is only used to create BSMs if it is plausible that the data could have been produced by sensors meeting the identified performance requirements. See NOTE 5 for discussion of plausibility checks.	
O.Data.3	R	R	Vehicle	TOE shall act on incoming BSMs (or other messages) only if they pass relevant plausibility checks defined in the specification of those messages. See NOTE 5 for discussion of plausibility checks.	X
O.DOS.1	R	S+R	System	TOE shall have mechanisms to determine if it is under a Denial of Service (DOS) attack and take appropriate measures to minimize the impact of such an attack. See NOTE 6 for discussion of DOS attacks.	
O.Hardware.1	R	S+R	Component	TOE shall only use security hardware (e.g., Cryptographic Module, security microcontroller) that has appropriate level of security. See NOTE 1 for discussion of hardware security	
O.Hardware.2	BP	S	Device	It shall be possible for an appropriately authorized operator to request that a TOE deletes some or all of its stored cryptographic keys. **BP Rationale**: See P.Hardware.2.	
O.Hardware.3	BP	S+R	Device	Cryptographic algorithms shall not be implemented in an application-specific integrated circuit (ASIC) but in a general purpose processor that is hardened against intrusion and side-channel attacks. **BP Rationale**: See P.Hardware.3.	

Objective ID	R / BP	Send / Receive (S/R)	TOE Level	Description	Addressed by existing spec
O.Init.1	R	S+R	Device	TOE shall support its secure initialization. See NOTE 7 for discussion of secure initialization.	
O.Misbehavior .1	BP	R	Device	TOE shall continually perform local misbehavior detection. See NOTE 8 for definition of local misbehavior detection. **BP Rationale**: See P.Misbehavior.1.	
O.Misbehavior .2	BP	R	Device	TOE shall report misbehavior when possible **according to the minimum performance requirements 1003**. **BP Rationale**: See P.Misbehavior.2. See NOTE 3 for further discussion of reporting.	
O.Platform.1	R	S+R	Compo nent	The TOE platform shall provide hardware support for appropriate secure software implementation on the TOE. See NOTE 1 for discussion of secure operations.	
O.Replay.1	R	S	Device	TOE shall use the IEEE 1609.2 BSM Security Profile to insert a timestamp to prevent replay.	X
O.Replay.2	R	R	Vehicle	TOE application processing shall not treat a BSM received multiple times as if it was multiple different BSMs.	X
O.Replay.3	R	S+R	Vehicle	TOE shall ensure that the system clock is only set backwards by a party entitled to do so and may choose to ensure that the system clock is never set backwards.	
O.Software.1	R	S+R	Vehicle	Software implementations on TOE shall follow best practices for secure implementation, including for example having proper access control, malware detection and preservation of a secure state in case of failures. See NOTE 1 for discussion of secure operations.	
O.Software.2	R	S+R	Vehicle	TOE shall perform system diagnostics, including industry best practice intrusion detection and reporting as appropriate, on a regular basis. See NOTE 3 for further discussion of reporting.	
O.Software.3	BP	S+R	Device	The system specification shall assign priorities to different tasks and, under situations of constrained processing power, TOE shall follow the priorities assigned to different tasks (For example, sending BSM may be a high priority task and updating CRL may be a lower priority task).	
O.Software.4	R	S	Device System	The system specification shall implement physical and logical isolation measures to separate critical systems from non-critical systems.	

Objective ID	R / BP	Send / Receive (S/R)	TOE Level	Description	Addressed by existing spec
O.Storage.1	R	S+R	Component	TOE shall store restricted information, such as private keys, certificates, etc. securely using appropriately secure physical storage and shall use the restricted information only within protected memory. See NOTE 1 for discussion of secure operations.	
O.Update.1	R	S+R	System	TOE shall update its software and/or data only using secure update mechanisms. See NOTE 1 for discussion of secure operations.	
O.Update.2	R	S+R	System	In case of a Root CA's compromise, TOE shall only use secure update mechanisms to obtain new public key(s). See NOTE 9 for discussion of secure update mechanisms	
O.Update.3	R	S+R	System	TOE shall have mechanisms in place for to secure re-initialization if necessary. See NOTE 7 for discussion of secure initialization.	
O.Update.4	BP	S+R	System	OBE shall have mechanisms in place to get securely re-bootstrapped if necessary. **BP Rationale**: See P.Update. 4. See NOTE 7 for discussion of secure initialization.	
O.Update.5	R	S+R	System	There shall be a documented mechanism by which a TOE may be updated to use new cryptographic algorithms. See NOTE 10 for discussion.	
O.Update.6	BP	S+R	System + Device	The TOE shall support secure over-the-air firmware updates. If the mechanism supported uses digital signatures, it shall include a migration path to a new signature algorithm. **BP Rationale**: See P.Update.6.	
OE.Algorithm.1	R	N/A	N/A	Global misbehavior detection algorithm shall be adaptive and evolve over time.	
OE.Algorithm.2	R	N/A	N/A	OE shall use specified secure cryptographic schemes to perform different operations, such as generate certificates, sign CRLs, etc.	X
OE.Cert.1	R	N/A	N/A	When the OE determines how many certificates to issue to a TOE, the number of concurrently valid certificates so issued shall be the minimum necessary to provide privacy unless the TOE demonstrates that its security against T.Extract.1, T.Extract.2, T.Extract.3, and T.Integrity.4 is sufficient to prevent it being used to launch Sybil attacks. See NOTE 11 for discussion of minimum necessary privacy protection.	

Objective ID	R / BP	Send / Receive (S/R)	TOE Level	Description	Addressed by existing spec
OE.Connect.1	R	N/A	N/A	OE shall provide sufficient connectivity to the TOE for pseudonym certificate provisioning, downloading CRLs, and uploading misbehavior reports.	
OE.CRL.1	R	N/A	N/A	OE shall provide access to CRLs in a timely fashion as per the CRL update frequency.	
OE.CRL.2	BP	N/A	N/A	OE shall have mechanisms to support collaborative distribution of CRLs. **BP Rationale**: See P.CRL.2	X
OE.CRL.3	R	N/A	N/A	CRL shall include information that allows a receiving device to determine which entries are most relevant to that device, allowing device to gain maximum protection if it cannot store all CRL information.	X
OE.Data.1	R	N/A	N/A	OE shall as far as possible provide verifiably correct GNSS data.	
OE.DOS.1	R	N/A	N/A	OE shall have mechanisms (technical and/or policy) to prevent DOS attacks; and if DOS attacks do occur, to recover from them and minimize their impact on the system.	
OE.DOS.2	R	N/A	N/A	OE shall have mechanisms to figure out if it is under a DOS attack and take appropriate measures to minimize the impact of such an attack.	
OE.Hardware.1	R	N/A	N/A	OE shall only use security hardware (e.g., Cryptographic Module, security microcontroller) that has desired level of security.	
OE.Init.1	R	N/A	N/A	OE shall have mechanisms in place to securely initialize essential components (e.g., OBE, sensors, GNSS receiver).	
OE.Misbehave.1	R	N/A	N/A	SCMS shall have mechanisms in place to identify misbehaving devices, which may include junk OBEs, and manage their impact on the system by revoking them and/or denying future requests for pseudonym certificates.	
OE.Platform.1	R	N/A	N/A	The OE platform shall provide hardware support for appropriate secure software implementation on the OE.	
OE.Regulation.1	BP	N/A	N/A	There shall be privacy regulations discouraging large scale BSM sniffers for tracking TOEs. **BP Rationale**: The technical protections for privacy in the system design still allow an attacker who records every message from a vehicle to reconstruct that vehicle's path. Regulation may form an additional deterrence to tracking.	

Objective ID	R / BP	Send / Receive (S/R)	TOE Level	Description	Addressed by existing spec
OE.Regulation .2	BP	N/A	N/A	There shall be privacy regulations preventing an attacker from tracking a specific TOE. **BP Rationale**: The technical protections for privacy in the system design still allow an attacker who records every message from a vehicle to reconstruct that vehicle's path. Regulation may form an additional deterrence to tracking.	
OE.SCMS.1	R	N/A	N/A	SCMS Manager shall have proper controls in place to enforce organizational separation among different SCMS components, especially RA, PCA, ECA, two LAs, and MA.	X
OE.SCMS.2	R	N/A	N/A	SCMS Manager shall have proper controls in place to enforce existence of only one instance each for all the intrinsically central SCMS components, especially MA.	X
OE.SCMS.3	R	N/A	N/A	SCMS shall implement all the security and privacy controls recommended in SCMS design documents and (wherever not contradictory with the former) standard industry practices required of a PKI.	X
OE.Security.1	R	N/A	N/A	Cryptographic algorithms used (e.g., ECDSA, SHA-256, Advanced Encryption Standard – Counter with Cipher Block Chaining Message Authentication Code [AES-CCM]) shall have desired level of security; and in case attacks are discovered on them, OE shall have mechanisms to recover from those attacks and replace the algorithms with secure ones (assuming they exist).	X
OE.Software.1	R	N/A	N/A	Software implementations of OE shall follow best practices for secure implementation, including for example having proper access control and malware detection. See NOTE 1 for discussion of secure operations.	
OE.Storage.1	R	N/A	N/A	OE shall store restricted information, such as private keys, certificates, etc. securely in FIPS 140-2 Level 2 or higher storage (or equivalent) and shall use the restricted information only within protected memory.	
OE.TOE.1	R	N/A	N/A	OE shall have mechanisms (technical and/or legal) to prevent physical vandalisms on TOE; and if they do occur, to recover from them and minimize their impact on the system.	

Objective ID	R / BP	Send / Receive (S/R)	TOE Level	Description	Addressed by existing spec
OE.Update.1	R	N/A	N/A	OE shall provide secure software update mechanisms for TOEs to update their software.	
OE.Update.2	R	N/A	N/A	In case of a Root CA's compromise, OE shall provide secure update mechanisms for TOEs to obtain new public key(s).	
OE.Update.3	R	N/A	N/A	OE shall provide mechanisms for re-initializing a revoked TOE.	
OE.Update.4	R	N/A	N/A	OE shall support deployment of new cryptographic algorithms to replace ones that are broken.	

NOTES

1) **Hardware, software, connection security**: A number of the objectives above refer to hardware, software, or connections within the TOE as being "secure." In this context, "secure" means that they resist attackers with an Attack Potential of less than some appropriate value. Section 5.4 within Appendix F. Full DSRC OBE Security Inputs Analysis provides a more in-depth discussion, including a definition of Attack Potential and recommended values. Since attacker capabilities will improve over time, and Attack Potential is a measure of the expense incurred by a successful attacker, the TOE capabilities required to protect against a given Attack Potential will increase over time. As such, best practices in hardware and software development to resist attacks with a given potential will also need to evolve. How best practices are specified, tested, and managed is the subject of a separate white paper (Appendix I. Overview of Cybersecurity Guidance and Best Practice Management in Other Industries) within this project
2) **Correct functioning**: In this context, "correct functioning" of a component within the TOE means that the component is meeting the approved performance requirements and security requirements
3) **Report to external authorities**: The objectives include two different types of reporting to external authorities: self-reporting or diagnostics (for malfunctions within the TOE) and misbehavior or intrusion detection reporting (for senders other than the TOE). The two types of report are different. Among possible differences: the authorities may be different – in fact, for diagnostics it may be more appropriate to refer to "maintenance services" rather than an "authority;" the structures used for one type of message need not be used for the other, and diagnostic messages may be proprietary; the information sharing model is different between the two cases, with diagnostic messages most likely used for maintenance diagnoses on an opt-in basis while misbehavior reports may be more widely shared and used for enforcement. For both of these reporting objectives it is necessary to define a format for the reports. This report format has not yet been defined for either diagnostic or misbehavior reporting, so this objective cannot currently be tested and cannot be anything more than a best practice.
4) **Verifiably correct GNSS data**: GNSS data is vulnerable to spoofing; existing civilian GNSS data does not include cryptographic authentication, and even if it did it would potentially be vulnerable to time-shifting. A good discussion of trustworthiness of GNSS data can be found in Markus G. Kuhn's *Signal Authentication in Trusted Satellite Navigation Receivers*. GNSS spoofing is detectable in some cases: for example, a spoofed GNSS signal will tend to be higher-power than a valid one; its power levels will change more rapidly as the receiver moves; it may not behave the same in all bands; its timestamps may not correctly match with actual time as measured by an independent local clock (note that *Signal Authentication in Trusted Satellite Navigation Receivers* addresses a more powerful threat model, where the spoofed signal replaces rather than simply overlaying the genuine one). Additionally, encrypted GNSS data may be

authenticated by delayed release of the secret spreading sequences, although neither this nor any other cryptographic authentication technique is currently implemented in any real-world civilian system. A supplier's Security Target document should document what measures are being taken to detect incidents of spoofing. In future, if cryptographically authenticated GNSS data becomes generally available, the use of this cryptographically authenticated GNSS data should become a requirement for new devices.

5) **Plausibility checks**: Plausibility checks should be carried out on two types of data: sensor data used to form BSMs; and data from incoming BSMs. A plausibility check on data asks the following question of the data:
   - Are the parameters within the expected performance envelope for the vehicle type (or for all vehicles)?
   - Based on the tracking for this vehicle is the currently received BSM within the error bound for tracking, and is it within the dynamic performance envelope for the vehicle type (or all vehicles).

   These checks can be carried out on both the sensor data used to form BSMs, and incoming BSMs on the basis of which actions might be taken. Sample plausibility tests on incoming BSMs or sensor data include rejecting any BSM that says the vehicle is traveling through other vehicle, faster than 252 km/hr, etc., and/or if it is behaving in an unrealistic manner (1.1g+ direction or speed changes), see DSRC Phase II Performance Requirement 80B for more details. For plausibility tests carried out on sensor data, the plausibility tests can be carried out anywhere within the TOE: so, for example, a sensor with a secure connection to the OBE could carry out its own plausibility checks, in which case the OBE would not have to carry out the plausibility checks; or the OBE could carry out the plausibility checks on the sensor data, considering that it already has the code to carry out plausibility checks on incoming BSMs.

   Data is plausible if it could have been produced by a real vehicle whose sensors meet the performance requirements.

   There is no definitive reference for plausibility checks for either BSMs or sensor data. Plausibility checks for BSMs will be defined as part of an ongoing CAMP project. Plausibility checks for sensor data are defined by the statement above that that data "could have been produced by sensors meeting the identified performance requirements." This definition of plausibility checks for sensor data is sufficiently precise to be used within the rulemaking but recommend the development of more low-level tests as a high priority.

6) **DOS:** Denial of service attacks on the channel can be detected as part of the standard medium activity sensing for channel access: a high level of channel activity, combined with a lower than expected number of successfully received application PDUs, indicates that there is some level of channel jamming going on. In fact, congestion due to excessive valid use and congestion due to a DOS attack have similar effects: in either case, the receiving unit has less assurance than might be necessary for correct operation of V2V safety alerts. A supplier's Security Target document should specify how the device behaves in the presence of sufficient interference that messages might not be received, whether or not this is due to malicious activity. The team recommends that at some point in the future, when the system is sufficiently widespread for drivers to have developed an expectation that there will be a warning if the is a hazard, USDOT considers requiring that drivers are notified if quality of service drops below expected levels. However, the team does not consider this requirement to be necessary for the current generation of devices.

7) **Initialization and re-initialization**: "Secure initialization" is any process that starts with the TOE being unprovisioned with software, security material, etc., and ends in the TOE being in a state such that when in operational mode it meets and enforces the security objectives. "Secure re-initialization" is any process that leaves the TOE in the same state that it is after a secure initialization.

8) **Local misbehavior detection**: Local misbehavior detection is a best practice in this document. Local misbehavior detection is similar to plausibility checking, except that it also covers behavior that may not be able to be identified as implausible until after it occurs. For example, a set of messages may appear plausible and may cause a forward collision warning, but the vehicle may not behave as if a forward collision was imminent (the driver gets a warning from a “ghost car” and drives through it). CAMP is defining local misbehavior detection practices and algorithms. Since local misbehavior detection is a best practice there are no testable requirements associated with it in this document.
9) **Secure update mechanism in the event of root CA compromise**: The supplier of a TOE should explain in the Security Target document how the device will be updated securely in the event of a root CA compromise. This may be stating that a maintenance operation will be carried out, or there may be an over the air firmware update procedure defined, or there may be some other approach. Any approach is acceptable which is secure against an attacker with less than the Attack Potential identified in Note 1. Note that CAMP is working on a specification for updating root CA information, but this is not yet publicly available for comment, let alone standardized or testable.
10) **Updating cryptographic algorithms**: The supplier of a TOE should explain in the Security Target document how cryptographic algorithms are updated. This may be as simple as stating that cryptographic hardware will be physically replaced, or there may be an over the air firmware update procedure defined. If this is defined, it must be secure against an attacker with less than the Attack Potential identified in Note 1.
11) **Minimum privacy requirements**: There are currently no standardized requirements for privacy. The current draft of J2945/1 states as requirements “The system shall support changing its certificate to preserve privacy” and “The system shall not change its certificate as long as one or more event conditions is met,” and provides guidance that the certificate should change approximately once every five minutes. If literally followed, this would lead to certificates being reused during the week, and it is conceivable that other strategies may come out of research that will preserve privacy better. A supplier’s Security Target document should provide a high-level description of the certificate change strategy and a description of how this provides privacy protection comparable to the baseline strategy of changing every five minutes.

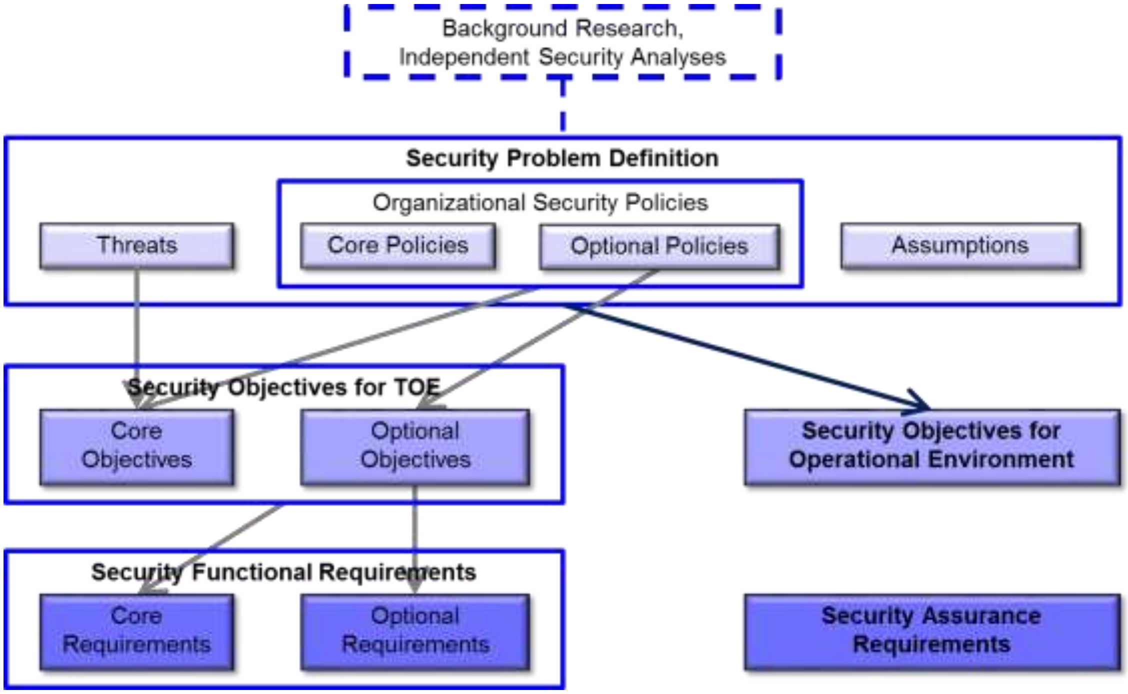
Building Blocks of Security Requirements

In following a systematic methodology to develop the security requirements, discussed in the following sections, several "building blocks" are developed. The Common Criteria Protection Profile (CC PP) methodology walks through a definition of the target of evaluation, and then a security problem definition, which includes: the enumeration of threats, assumptions, policies; development of objectives based on threats, assumptions, and policies; and final requirements derived from objectives, as illustrated in Figure 63. Since the Connected Vehicle security space is already well-researched, the Booz Allen team’s output included comparison with other relevant security requirements documents to ensure that no potential threats had been overlooked. Appendix F. Full DSRC OBE Security Inputs Analysis includes the full detail of each of these analyses, but summaries are provided.

It is important to note that while the CC PP methodology was followed to develop requirements and the team recommends NHTSA consider using the CC system to release its requirements and compliance testing as described in Section 7.12, Use of Regulations and Other Approaches, the inputs included in this document (in the chapter and Appendix F. Full DSRC OBE Security Inputs Analysis) are not an actual Protection Profile. The team foresees eventual writing of Protection Profiles

(PPs) (or other types of security standards and guidance) to be in several formats that would pull from the inputs developed within this project. The clarification of scope and breadth of the document versus final possible PPs is included throughout.

Figure 63: CC PP Requirements Derivation (Source: USDOT)


Background Research,
Independent Security Analyses
Security Problem Definition
Organizational Security Policies
Threats
Core Policies
Optional Policies
Assumptions
Security Objectives for TOE
Core Objectives
Optional Objectives
Security Objectives for Operational Environment
Security Functional Requirements
Core Requirements
Optional Requirements
Security Assurance Requirements

5.1.2 Target of Evaluation

The Target of Evaluation (TOE) is the specific entity which is to be analyzed. The selection of the boundary for the TOE can vary depending on the desired scope to be addressed in the CC PP. The TOE and associated security requirements can be defined at a number of different levels, with each level defining a TOE:

- The system – the entirety of the system, including sending and receiving devices
- The vehicle – the individual vehicles in the system, acting as sender or receiver with integrated devices
- The device – a device within the vehicle (or possibly a standalone device if it meets the security requirements)
- Components within the device, for example a hardware security module (HSM) that stores private keys

At any level, the requirements can be considered to fall into one of two groups:

- Functional security requirements (SFRs) on the TOE under consideration
- Operating Environment (OE) requirements impacting the TOE under consideration.

For example, consider three different TOEs under consideration: the entire system, an individual device, and the secure module within that device that stores private keys.

- At the *system* level, there is a functional requirement that private keys can only be used by processes that are authorized specifically to use those private keys.

- At the *device* level, there is a functional requirement that the device distinguishes between processes and restricts which processes may request the use of specific private keys, and a functional requirement that the device provides physical protection for private keys to prevent their extraction.
- At the *secure module* level, there is a functional requirement that the secure module provides physical protection for private keys, and an operating environment requirement that the secure module is used in an environment where only authorized processes can request the use of specific private keys.

In this document, the TOE is a **vehicle equipped with DSRC devices that generate and receive BSMs**. In Common Criteria terms, the vehicle is the "Target of Evaluation" (TOE). Therefore, the operating environment includes (but is not limited to) the following:

- GPS signals
- DSRC messages
- Other data input (if applicable)
- Physical phenomena observable by sensors
- People with physical access to the vehicle

While the team recognizes that traditional CC PPs define their TOEs in a more focused manner so as to facilitate testing, because the team is not actually writing a PP, but rather trying to include a comprehensive analysis that includes discussion and specification of requirements for all elements that will need to comply with various security requirements, the TOE is broader than those defined in standard CC PPs. The TOE was specified as the vehicle itself, rather than as any subsystem of the vehicle, for a number of reasons:

- Choosing the vehicle rather than a subsystem ensures that the security requirements are valid and do not depend on specific architectures. For example, security requirements derived using the vehicle as a TOE are valid whether security-critical functions are implemented in a single device or in multiple devices throughout the vehicle. This significantly simplifies the task and increases the applicability of specifying the boundary and interface around the TOE.
- The vehicle itself, not any component, will be the subject of any FMVSS issued, and OEMs will have to self-certify that the vehicle is roadworthy under that FMVSS. As such, the security requirements on the vehicle are the most relevant security requirements to both NHTSA and the vehicle OEMs.

As noted above, the team wanted to ensure that all elements that will impact the needs for security at the system (vehicle) level were analyzed for the sake of completeness, but do not anticipate it will be the final TOE for a fully formatted and industry compliance PP. The team anticipates that the inputs document can be used to develop multiple TOEs, as best decided upon by CC professionals, and will include the relevant portions of all sections for each of those TOEs. The information contained in this report and Appendix F. Full DSRC OBE Security Inputs Analysis are the inputs for future PPs.

5.1.3 Security Problem Definition

This section defines security threats, assumptions, and organizational security policies. They map to objectives as follows.

- Threats may map to objectives on the TOE or to objectives on the operating environment

- Organizational policies may map to objectives on the TOE or to objectives on the operating environment. Organizational policies can be thought of as the rationale for those objectives that do not directly map to specific threats.
- Assumptions map to objectives on the operating environment.

Where threats map to objectives, the objective is designed to counter or mitigate the threat. Where organizational policies or assumptions map to objectives, the objective is intended to formalize the policy or assumption. In practice, a policy or assumption frequently looks almost identical to the objective it motivates.

5.1.3.1 Threats

Table 1 in Appendix F. Full DSRC OBE Security Inputs Analysis provides a list of the threats identified in the system. Threats may be addressed by objectives on the OE or TOE. The purpose of this table is to have a comprehensive list of threats. This table does not go into the details of how the specific threats are carried out, but the details will be taken into account when defining security objectives to address those threats. This list of threats has been compiled with reference to Car-to-Car Communications Consortium (C2C-CC) Protection Profile, European Telecommunications Standards Institute (ETSI) TVRA, Sevecom Security Requirements Report, and CAMP Risk Assessment and Technical Analysis Report.

The team also performed a risk assessment of the threats identified above. The methodology follows NIST Special Publication 800-30, except that there are only 3 levels (as opposed to 5 levels) for both Likelihood and Impact of a threat: low, moderate, and high. The team also modified the corresponding risk matrix accordingly (cf. Table I-2 in NIST SP 800-30) as shown along with the rationale for those impact levels. For a system that is yet to be designed and implemented, the likelihood of an attack is largely unknown and any guestimate is very likely to be far off from the reality. Therefore, the team takes a slightly different approach compared to the one suggested in NIST SP 800-30: first estimate just the impact of all the threats, then for all the threats with moderate/high impacts, suggest countermeasures to bring the likelihood down to low/moderate, and finally carry out a full risk analysis (i.e., first estimate likelihood and impact of a threat, and then use the risk matrix of Table 2 of Appendix F. Full DSRC OBE Security Inputs Analysis to calculate risk) on the system along with countermeasures. The full list of risks and threat assessments is included in Table 3 of the Appendix.

5.1.3.2 Assumptions

A set of underlying assumptions must be enumerated. In the Common Criteria context, assumptions capture security properties of the system as a whole that cannot be ensured by testing the Target of Evaluation; in other words, they capture properties of the Operating Environment (OE). In this case, assumptions were used as educated strawman design decisions about the TOE itself; these are necessary given that the system is still very much in development. In the Common Criteria context, assumptions are listed in Table 4 of Appendix F. Full DSRC OBE Security Inputs Analysis. The reader should note that these assumptions are based on the current design of the SCMS, some elements of which are still in design and development phases. As these elements take shape, assumptions may change and the corresponding threats, objectives, and policies that relate to them may need to be updated. Appendix F. Full DSRC OBE Security Inputs Analysis provides a full traceability matrix so that future changes an easily be tracked as to downstream implications.

5.1.3.3 Policies

Organizational security policies specify multiple levels of behavior of the TOE (the vehicle) that are required, optional, and include both send- and receive- side requirements. The policies in turn lead to the objectives, many of which are the same or quite similar, and eventually lead to requirements. Table 5 of Appendix F. Full DSRC OBE Security Inputs Analysis lists all of the policies.

5.1.3.4 Objectives

As noted above, security objectives reflect how to guard against threats at all stages of the device lifecycle for the safety applications use case. The team identified and described objectives for the vehicle (TOE) and the operating environment. These include 39 objectives for the vehicle (TOE), ten of which are optional and eight of which affect only receive-side. In addition, 27 objectives are specific to the operating environment. The list of objectives is included above in Table 17 and also in Table 6 of Appendix F. Full DSRC OBE Security Inputs Analysis.

5.1.3.5 Security Assurance Requirements

The level of protection an organization or regulator seeks to ensure with a CC PP would typically require security assurance requirements at Evaluation Assurance Level (EAL) 4 as defined in Common Criteria Part 3: “EAL 4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL 4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line. EAL 4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.” In development of security requirements, the team does not make an explicit recommendation for EAL for the following reasons:

- The TOE in this document is the entire vehicle, and the specification of an EAL for the entire vehicle is contrary to the self-certification regime in operation in the USA. Please see previous discussions about the TOE for the purposes of developing complete sets of requirements, versus an eventual PP, which would imply a more narrowly defined TOE.
- The TOE in this document is the entire vehicle, but the vehicle is too large to be the subject of an evaluation at a certification lab. Any evaluation process would need to be defined on components, not on the vehicle as a whole, as otherwise any change to the vehicle that affected BSM generation or reception would require a costly re-evaluation.
- Recently, systems that use Common Criteria have moved away from a single EAL and towards specifying Assurance Activities for each of the SFRs. As such, it does not seem appropriate to provide an EAL requirement for this TOE.

The team recommends that a next step would be to work with the OEMs to derive PPs containing SFRs and Assurance Activities (AAs) for components within the vehicle, such that OEMs could use these PPs to guide their procurement activities if they so choose within the self-certification regime, and NHTSA could use for spot checking or testing, following the same PPs and AAs.

As described above, the threats, assumptions, policies, and objectives all align for the final articulation of the core security requirements included in Appendix F. Full DSRC OBE Security Inputs Analysis.

Background on Developing Security Requirements

The objectives listed above and the summary of the various steps in the process that allowed the team to arrive at those requirements all follow a CC PP development process. This section outlines how the team approached the choice for the best methodology to follow in developing these requirements, and the choice to use the CC methodology.

5.1.4 Approach in Selecting a Methodology

The goals of developing security requirements as part of the broader performance requirements for DSRC devices is to specify security requirements in a **standardized, testable way** for devices that are subject to any future USDOT rules on V2V Safety Communications. This includes DSRC-enabled devices that send and receive BSMs. To accomplish this goal, the team selected an approach that enables the specification of security requirements for additional application-services, namely the sending and receiving of BSMs that enable other applications such as signal phase and timing (SPaT) or signal prioritization requests.

The team analyzed the needs of the project and defined the basic elements that will be needed as part of the analysis and requirements.

5.1.5 Objective and Desired Properties

The primary desired properties of a methodology are as follows:

- It should be standardized
- There should be an existing system of test labs, or other certification processes, that can be used and a community of experts with domain knowledge in the methodology
- It should be clear how security requirements are to be stated within the methodology
- It should be clear how suppliers prepare a unit for testing and how they make statements about its conformance to the security requirements (see text following this list)
- It should cover all the different types of security requirements that have been identified as important for OBEs to be used for V2V Safety Communications

This section briefly expands on the fourth bulleted item, how to prepare units for testing and make statements about its conformance. Security requirements cover many different aspects of the device, from hardware to software to manufacturing processes. Many aspects of the security of a device cannot be demonstrated interactively over an interface and so are not amenable to standard conformance and interoperability testing. Additionally, some security aspects (e.g., hardware protection of keys) cannot be tested without physically destroying some part of the device, and other aspects (such as, to take a very specific example, there being no debug access once a given fuse is blown) cannot be demonstrated by interactive testing, because no test is comprehensive enough. Therefore, the demonstration that a device is compliant to security requirements must necessarily include proof by design as well as some proof by test. Suppliers providing a device for test should know how to provide this proof by design (i.e., what design documents must be provided, what is the structure of those documents, what is subject to proof by design, what level of scrutiny the design documents will undergo). The team favors a methodology that is clear and specific about the proof by design and the conformance documentation that must be provided.

5.1.5.1 Extended Objectives

The above would be sufficient for specifying security requirements for OBEs. However, the full V2X system will encompass a number of different units. In choosing a methodology and specific deliverables, it should support the following additional use cases:

- Mobile devices:
  - Non-inbuilt BSM generating devices such as ASDs
  - Nomadic BSM generating devices such as smartphones
  - OBEs or other BSM generating devices that run additional applications (and send messages from additional message sets) beyond the BSM-centric applications
  - OBEs or other mobile devices that request a higher level of privilege than used for sending BSMs: for example, emergency response vehicles or transit requesting signal prioritization
- Fixed devices:
  - RSEs that act as pass-throughs for messages generated elsewhere
  - RSEs that locally generate only low-value or low-privilege messages
  - RSEs that locally generate high-value or high-privilege messages

The team therefore favors a methodology that will make it straightforward to support devices of these types, without sacrificing the need to specify security requirements for the integrated OBEs.

5.1.5.2 Self-Certification

One of the primary considerations is that there is an existing system of test labs that can be used to certify devices. However, the understanding is that under the US system of self-certification for vehicles, OEMs are not required to use external test labs to make certification claims about their vehicles, though they may choose to. Nevertheless, the team considers existing test labs to be necessary for the methodology to be chosen for the following reasons:

- Test labs may be useful to OEMs, even though not required, if they want to carry out type certification of devices for internal purposes before integrating into a self-certified vehicle.
- The existence of test labs indicates that there is significant domain expertise in testing according to the given methodology. This expertise may be of use to OEMs in developing devices that meet requirements, even if the fact that the devices meet the requirements is not demonstrated specifically through the use of a test lab.

Note that although law mandates the self-certification regime[11], communications security is a special case. For the first time in the history of mass vehicular transport, one car will need to trust data sent by another car made by a different OEM. As such, ensuring that all devices in the system meet a minimum baseline of trustworthiness is vital to the system's success.

It is understood that NHTSA may choose to perform its own certification tests on various requirements that it has published. If the Administration chooses to do that for the security requirements, if conforming to a CC PP, the labs that can be used for such testing already exist and could serve as

[11] 49 U.S.C. 30115 - CERTIFICATION OF COMPLIANCE, United States Code, 2006 Edition, Supplement 5, Title 49 – TRANSPORTATION. Available from http://www.gpo.gov/fdsys/granule/USCODE-2011-title49/USCODE-2011-title49-subtitleVI-partA-chap301-subchapII-sec30115

valuable partners to the USDOT. This is the first time that security requirements are being considered for vehicles, and this area necessitates specialized knowledge that would be costly and difficult for NHSTA to bring internally into its operations. Because Common Criteria test labs and approaches are well-founded and accepted across multiple industrialized nations, and the certification for such labs is performed based on other federal standards (see discussion below in Section 5.3.6 Testing Process), this is a viable approach for NHTSA to consider to ensure that the appropriate security requirements are included from the beginning of connected vehicle implementations.

5.1.6 Existing Research

This section reviews the three document families that exist from which to choose an approach to develop security requirements. The aim of this section is to provide a background to these families and allow the reader to understand how the document or documents in each family are used to establish security requirements and make testable security assertions.

In brief, the source documents are as follows. These documents are not mutually exclusive. For example, a CC protection profile can require FIPS 140 validation as do some of the NIST SP 800-53 security controls. FIPS 140 is intended as a “stand alone” validation process for a system component.

1) FIPS 140-2. This is a document specifying requirements for cryptographic modules for use in federal information systems. Modules may be assessed for conformance to requirements in a number of different areas. Each area within a module is given a rating from 0-4. The overall rating of a module is the lowest rating that it gets under any individual area. There are dedicated labs that carry out FIPS-140 conformance testing, which are accredited by NIST. FIPS 140-2 is not particularly flexible and is focused on core cryptographic operations. Note: ISO/IEC 19790:2012, Information technology – Security techniques – Security requirements for cryptographic modules is based on FIPS 140-2 with an objective of creating a comparable consensus based internationally recognized standard. ISO/IEC 30104:2015, Information technology – Security techniques – Physical security attacks, mitigation techniques and security requirements, discusses the different types of physical attacks and defenses in detail which can be used by manufacturers in developing particular defenses that meet requirements identified in FIPS 140-2 or ISO/IEC 19790.
2) Common Criteria, which allows security requirements for a given TOE to be specified as a document known as a Protection Profile. The PP includes high-level security requirements and maps them to security functional requirements with traceability. The EAL, which is defined for that TOE by the PP, runs from 1 to 7 and reflects the extensiveness of the testing itself rather than being a statement about the security of the system under evaluation. A supplier of a system for testing provides a document known as a Security Target, which details how the system meets the requirements set out in the Protection Profile.
3) The Risk Management Framework of NIST SP 800-37. This involves a number of documents. FIPS 199 provides a Risk Management Framework (RMF) used to assess security requirements for federal information systems at a high level, using three security objectives, Confidentiality, Integrity, and Availability, with requirement levels of Low, Moderate, High, and Not Applicable for each. SP 800-53 provides a set of security controls appropriate for each objective at each requirement level. SP 800-37 provides an overall lifecycle flow within which FIPS 199 and SP 800-53 are used, as well as specifying how the use of these controls may be audited. The SP 800-37 process does not provide a common format for specifying the security controls.

Note that some of these documents (NIST-based documents, such as FIPS, etc.) are specifically targeted at security requirements for federal information systems. If used as the basis for Connected Vehicle requirements, this would technically constitute an expansion of their scope; however, this would not seem to be a compelling reason not to use them as a baseline. These documents also target a security assessment for a single system with many components. However, their application naturally produces security conformance requirements for the individual components, such as OBEs.

5.1.7 Consolidated List of Security Areas and Gap Analysis

A consolidated list of security areas from the documents along with notes on the relevance of each area for V2V security is below. The aim is to identify whether any security areas needed for V2V security are not included in the surveyed document families.

Table 18: Consolidated List of Security Areas and Gap Analysis

Security Area and Associated Document Family	Notes
1. Audit a. Security Audit (CC) b. Audit and Accountability (SP800-53)	Useful for servers, probably not required for OBEs
2. Communication a. Communication (CC) b. Trusted Path/Channels (CC) c. System and Communications Protection (SP800-53)	Necessary for OBEs to support initialization certificate establishment
3. Cryptography a. Cryptographic Support (CC) b. Cryptographic Module Specification (FIPS) c. Cryptographic Key Management I and II (FIPS)	Necessary for OBEs
4. Data a. User Data Protection (CC) b. Media Protection (SP800-53)	Necessary for OBEs
5. Authentication and Integrity a. Identification and Authentication (CC) b. Protection of the TSF (CC) c. Operational Environment (FIPS) d. Identification and Authentication (SP800-53) e. System and Information Integrity (SP800-53)	Necessary for OBEs
6. Assessment, Assurance, and Management a. Security Management (CC) b. Risk Assessment (SP800-53) c. Security Assessment and Authorization (SP800-53) d. Design Assurance (FIPS)	Likely necessary for OBEs
7. Privacy and Tracking a. Privacy (CC)	Necessary for OBEs

Security Area and Associated Document Family	Notes
8. Access a. TOE Access (CC) b. Access Control (SP800-53) c. Ports and Interfaces (FIPS)	Necessary for OBEs. This area covers input data validation, which is a factor for OBEs that generate BSMs based on sensor data.
9. Physical a. Physical and Environmental Protection (SP800-53) b. Physical Security (FIPS)	Necessary for OBEs

In this exercise the team has not identified any requirement types that are not already potentially included in at least one of the document families. The CC requirements are the most comprehensive.

5.1.8 Requirements Specification Process

In the CC, security requirements are specified in the PP; conformance claims about specific devices are made in the Security Target. Both are documents with a known format and a clear development process.

FIPS 140 does not support multiple device types, but it allows conformance claims by different devices (also documented in a Security Target) and provides a clear framework for specifying those conformance claims.

SP 800-37 allows individual security requirement specifications for different systems and so naturally supports different device types. However, it does not provide a specific template for the security plan to be used by developers and deployers.

5.1.9 Testing Process

Both CC and FIPS 140 have an established network of test labs and a format that may be used to specify conformance. As noted earlier, it is not clear that certification test labs are necessary under the US regime, but they are certainly useful. According to the National Information Assurance Partnership (NIAP) – Common Criteria Evaluation & Validation Scheme (CCEVS), there are 10 approved Common Criteria Testing Laboratories (CCTLs) that are accredited by the NIST National Voluntary Laboratory Accreditation Program (NVLAP) and meet CCEVS-specific requirements to assess conformance against the Common Criteria for Information Technology Security Evaluation, International Standard ISO/IEC 15408. One of these labs is the Booz Allen Hamilton CCTL in Linthicum, MD. There are also 55 additional CCTLs worldwide according to www.commoncriteriaportal.org. According to NIST, there are 12 approved FIPS 140-1 and FIPS 140-2 testing labs in the US (one of these is the Booz Allen Hamilton lab). There are also 13 additional approved FIPS 140-1 and FIPS 140-2 testing labs worldwide. All approved US labs are accredited by the NIST NVLAP.

Common Criteria testing can be expected to be in the six-figure range, but will depend on the selected EAL. In March 2006, the Government Accountability Office (GAO) GAO-06-392 report claimed the approximate time frames and costs for an approved test laboratory to evaluate a product at EALs 2 through 4:

- EAL 2: 4-9 months at $75k-$200k
- EAL 3: 6-13 months at $110k-$250k
- EAL 4: 9-24 months at $150k-$350k

The cost for FIPS 140-2 testing is inexpensive compared to Common Criteria with levels 1, 2, 3, and 4 costing about $30-35k, $40-45k, $55-65k, and $75k+, respectively. Of course, the overall cost depends on a number of factors such as number of tested platforms, overall complexity of the module, vendor ability to resolve issues, etc. Note that NIST charges the labs a cost recovery fee for each test report submitted and it increases based on level, which NIST expects the labs to pass through to the vendors. However, this testing can get more expensive because vendors typically contract with third party consultants to develop the documentation evidence that the lab validates and come up with ideas to fix areas of non-conformance (NIST prohibits labs from evaluating their own work so labs cannot do consulting unlike for CC).

For anything over EAL 4, it is assumed there would be joint testing between the approved testing lab and the government. If a device is changed significantly it may have to undergo additional conformance testing, increasing the cost to suppliers. Smaller level changes can usually be tested through a delta certification where only the changed components or software are tested. Since NIAP no longer supports EALs the assurance maintenance program for those types of evaluations has been retired. The new assurance maintenance program is:

- Get product certified initially (against a PP)
- All minor product updates are automatically covered for 2 years
- When the 2 years are up, the product is recertified however previous evidence can usually be reused with minor changes. You might be able to re-use a lot of evidence with minor changes but they treat it as if you’re starting over again from a policy standpoint

Subject matter experts from the Booz Allen CC Testing Lab have indicated that the US is moving away from the EAL concept, because it locks the supplier and testing lab into testing every requirement at the same level. For example, if the EAL was specified at 4, every single requirement would need to be tested at EAL 4, which is usually not necessary. Instead, it is now common to specify the target as adhering to EAL 1 as a whole while specifying higher EALs and assurance activities for specific security functional requirements that should meet a higher level of testing. Assurance activities are typically developed through technical communities where labs, schemes, customers, vendors, academics, etc. collaborate to determine the appropriate level of assurance that needs to be provided for each individual function. Additionally, conformance testing does not provide a cast-iron guarantee of security. For either approach, the team recommends NHTSA work with OEMs and CC labs as final security requirements are decided upon to understand which AAs would be required or recommended.

5.1.10 Selected Security Requirements Development Methodology

The team determined that the most appropriate course of action was to follow the CC process to develop input material for the PP or PPs used to make conformance claims for DSRC devices that send and receive BSMs. These inputs may be used to create either a single PP for the entire system, or multiple distinct PPs corresponding to different levels or parts of the system. A PP is an internationally usable standard, reflecting the global nature of the automotive supply chain. The C2C-CC is developing a PP for a V2X box, which USDOT could choose to harmonize and reduce development costs. The PP document format also provides both flexibility in the security controls that may be specified, and a framework for the document that makes developing the document in a structured way easier than with the other approaches.

6 Recommended Compliance Tests and Validation Testing

This section summarizes the recommended approaches to ensure compliance to performance requirements and provides the compliance test procedure objectives. This section also provides information on validation testing conducted by the project team for select compliance tests to check the feasibility of the test and associated performance requirements.

As mentioned previously in this report, for whatever requirements NHTSA decides to include in an FMVSS, there will need to be compliance tests to ensure that those requirements are met in production. The team anticipates that many (if not all) requirements will be self-certified by auto manufacturers, but also recognize that NHTSA needs to be aware of and able to replicate or perform its own tests if the Administration chooses to do so. In addition, it is critical to develop these test procedures to ensure feasibility and potential ability to comply with any recommended requirements. How NHTSA chooses to use these and develop them beyond the level of specificity included here, will be determined by future work that can take each test and perform it in as many scenarios as makes sense.

In developing recommended compliance test procedures and conducting validation testing, the Booz Allen team reviewed existing compliance testing procedures for other systems, such as the “Laboratory Test Procedure for Part 563, Event Data Recorders” to ensure the correct approach. The team began this process by developing a high level compliance test recommendation for each requirement developed in the full requirements matrix. The team aggregated these preliminary tests so that multiple requirements could be assessed in a single test, where possible, and grouped related tests into test suites. As requirements were finalized, the team added detail to the recommended compliance testing procedures and identified those that could be verified during validation testing. Refer to Appendix G. Full Recommended Compliance Testing Procedures for full compliance test procedures.

High-Level Compliance Tests Aligned to Performance Requirements

This subsection outlines the recommended compliance test procedures aligned to the recommended performance requirements. Refer to Appendix G. Full Recommended Compliance Testing Procedures for full recommended compliance test procedures. These tables are also found within the full requirements matrix located in Appendix E. Full DSRC OBE Recommended Performance Requirements Matrix. The team made every effort to limit the overall quantity of compliance tests by ensuring each test validates as many performance requirements as possible. Compliance tests were split into one of two approaches: OBE/Component Level and Vehicle Level.

This subsection also contains background on definitions for and purpose of denoting the test suite, test, fulfilled test objective(s), and associated requirement IDs. The compliance test summary spreadsheets are organized by the compliance approach (OBE/Component Level or Vehicle Level) and further broken down by test suites within each approach. The lowest level tests that could be completed by component manufacturers and OEMs come first and are followed by higher level vehicle level tests which can be self-certified by the OEM and validated by NHTSA.

6.1.1 Recommended Compliance Approaches

The Booz Allen team developed two high level compliance testing approaches aligned to the different DSRC elements and requirement types for communications performance. Security requirements testing is discussed within Chapter 5 and Appendix F. Full DSRC OBE Security Inputs Analysis. Refer to Appendix C. DSRC OBE Requirements and Verification Hierarchy for the DSRC OBE Requirements and Verification Hierarchy for the alignment of the DSRC elements, example requirement types, and certification approaches. The compliance approaches are then broken down into compliance test suites and tests with detailed procedures to evaluate requirements. Refer to Appendix G. Full Recommended Compliance Testing Procedures for the full compliance test procedures. Each requirement within the full requirements matrix embedded within Appendix E. Full DSRC OBE Recommended Performance Requirements Matrix is aligned to at least one of the compliance tests in this appendix, except for the requirement on Intrusion Detection. As stated in Chapter 7, further intrusion detection research should be conducted before developing a test. Also as with the majority of objectives and Security Functional Requirements (SFRs) specified, existing security testing labs would have the required expertise to test intrusion vulnerabilities.

OBE/Component Level Tests
This approach aligns to the Component and Subsystem DSRC elements, which include requirements focusing on:

- Radio behavior/protocol (i.e., IEEE 802.11 and the IEEE 1609 suite)
- Message storage
- Message transmission/processing
- Operational failure detection

The team sees this approach and low level testing as being the primary responsibility of the manufacturer of the DSRC components/unit and OEM because they can be conducted without the OBE integrated into a vehicle. However, NHTSA could conduct these tests to evaluate the requirements if deemed necessary. If the unit does not adhere to these foundational standards for DSRC communication and basic operational requirements, the device will not be able to communicate on the V2V or V2I DSRC network and would not pass the vehicle level tests.

Note: While standards testing is designated as OBE/Component level, the team did not write out specific test procedures since they would be hundreds of pages. If a vehicle completes the vehicle level test, it is compliant with the applicable DSRC standards by default. This discussion continues in the Certification Testing for Foundation Standards section within this chapter.

Vehicle Level Tests
This approach aligns to the System, Vehicle, and Roadway DSRC elements, which include requirements related to:

- Message handling (e.g., plausibility, security)
- Vehicle transmit power and antenna gain envelope
- Basic self-test
- BSM data validity
- RSE interactions

The team sees this approach as joint responsibility shared by both an OEM and NHTSA since both parties must ensure the OBE meets requirements when integrated within the vehicle. These types of requirements must be tested with an integrated vehicle as the vehicle dimensions and design could affect performance. While the OEM would be responsible for asserting compliance based on their own tests, these would also be the types of compliance tests NHTSA may consider testing to verify compliance.

6.1.2 Recommended Compliance Test Summary

The tables within this section give a summary of tests that can be used to evaluate compliance with recommended requirements. The tables include the recommended OBE/Component Level compliance test summary, recommended Vehicle Level compliance test summary, and the recommended Vehicle Level compliance testing sequence. Again, the standards related tests are technically OBE/Component Level tests but are validated by default within the recommended Vehicle Level Tests. Refer to Appendix G. Full Recommended Compliance Testing Procedures for full recommended compliance test procedures.

Definitions and Purpose

Test Suite – This is the name of the test suite. The OBE/Component Level and Vehicle Level tests are grouped into test suites based on the type of test, associated objectives, and associated requirements

Test – This is the name of the test. Each test suite is broken down into two or more focused tests to evaluate specific objectives and requirements

Fulfilled Test Objective(s) – This is the objective of a particular recommended compliance test. Refer to Appendix G. Full Recommended Compliance Testing Procedures for full recommended compliance test procedures

Associated Requirement IDs – This aligns the compliance test objective to the requirements that are verified during the compliance test. Refer to Appendix E. Full DSRC OBE Recommended Performance Requirements Matrix for the full requirements matrix.

Table 19: Recommended OBE/Component Level Compliance Test Summary

Test Suite	Test	Fulfilled Test Objectives	Associated Requirement IDs
Standards Compliance	IEEE 1609 Suite Compliance	Verify that the OBE adheres to all requirements under the IEEE 1609 suite	[1012]
	IEEE 802.11 Compliance	Verify that the OBE adheres to all requirements under IEEE 802.11	[1013]
	SAE J2735/J2945 Compliance	Verify that the OBE can produce all required messages with data frames and data elements following SAE J2735 and J2945/1	[2b]
BSM Transmission and Processing	Message Transmission under Full Load	Verify that under full load conditions, the OBE generates and sends BSMs at the proper rate	[1, 3, 4, 60]
	BSM Generation and Processing Impact	Verify that the OBE trust store updates do not impact BSM generation interval or BSM processing and hazard detection	[47, 99]
		Verify that the OBE software update installations do not impact BSM generation interval or BSM processing and hazard detection	[106]
	Asynchronous Message Transmission	Verify that the OBE is transmitting BSMs using the asynchronous message strategy	[1015]
	Congestion Mitigation	Verify that the OBE transmits BSMs on the correct 10 MHz channel at a data rate of 9 Mbps	[1017]
Storage	General Storage	Verify that the OBE can store at least one CRL, three years' worth of pseudonym certificates at 20 certificates per week, a basic software load and any updates, with non-volatile storage capacity of 1 MB plus size necessary for software storage and operations	[85a]
	Misbehavior Report Storage	Verify that the OBE can store up to 30 misbehaving messages into a misbehavior report and discards the lowest-priority stored misbehavior observations if necessary to store a higher-priority misbehavior observation and/or when storage capacity is reached	[1002] [1005]
Failure Detection	Start-up Failure Detection	Verify that the OBE initiates all start-up procedure tasks, can identify any failures, and ceases BSM transmission if a failure is detected	[113, 105, 50, 57, 86, 122]#1 [113, 105, 50, 57, 86, 122]#2
	Operational Failure Detection	Verify that the OBE can detect failures that would result in an erroneous BSM being generated (data outside limits, sending parameters faulty, etc.) and cease BSM transmission if a failure is detected	[50, 57, 86] [113, 105, 50, 57, 86, 122]#2

Table 20: Recommended Vehicle Level Compliance Test Summary

Test Suite	Test	Fulfilled Test Objectives	Associated Requirement IDs
Static Vehicle	Transmit Power and Antenna Gain Envelope	Assess transmit power and antenna gain of a full vehicle with production antenna. Test is vehicle dependent and must account for vehicle body, height, and antenna placement as well as any original equipment accessories such as roof racks	[17, 59]
	Self-test	Verify that the self-test initiates at key on	[1010]
		Verify that the OBE can survive all operations during any key-off, key-on sequence	[1009]
		Verify that the OBE activates a malfunction indication when not in operational mode. Verify that the malfunction indication clears upon successful start-up, self-test, and/or when in operational mode	[1011] [120]
Dynamic Vehicle	BSM Parameter Accuracy	Verify that BSMs generated by the OBE can conform to minimum error thresholds for position, speed, acceleration, heading, and yaw rate	[1014]
	Simulated Implausible Messages	Verify that the OBE can correctly differentiate between plausible BSMs and outlier BSMs with the required accuracy at a rate of 5500 BSMs per second for Level 1 plausibility and 200 BSMs per second for Level 2 plausibility	[80B] [81] [63, 64, 67, 80] [1016]
		Verify the OBE logs within a misbehavior report (a) any message that (1) results in a warning or (2) would result in a warning but failed a level 2 plausibility check, or (b) any set of 10 continuous BSMs from the same vehicle that has consistently failed plausibility Level 1 checks	[1018] [1007]
	Simulated Signature Failure	Verify that all messages that result in safety warning are first verified by the OBE and a misbehavior report is generated for BSMs that fail verification	[1006] [1018] [1007]
Simulated RSE Encounters	Simulated Misbehavior Report Transaction	Verify that the OBE sends the stored misbehavior report when SCMS connectivity is available	[1003]
	Simulated Certificate Request	Verify that the OBE can complete request and response transactions with remote system management services in less than 10 seconds	[18B]
	Simulated Certificate	Verify that the OBE can complete request and response transactions with remote	[18B]

Test Suite	Test	Fulfilled Test Objectives	Associated Requirement IDs
	Delivery I (Complete Transaction)	system management services in less than 10 seconds	
	Simulated Certificate Delivery II (Resumed Transaction)	Verify that the OBE can complete request and response transactions with remote system management services with service interruptions	[18A]

While the Vehicle Level tests naturally fall into the test suites shown in Table 20, the recommended testing sequence is organized differently for logistics and efficiency purposes. The Vehicle Level tests build off of each other in the sequence listed in Table 21 as will be understood when reading the full recommended compliance tests in Appendix G. Full Recommended Compliance Testing Procedures.

Table 21: Recommended Vehicle Compliance Test Sequence

Sequence Number	Vehicle Level Test
1	Self-test
2	Transmit Power and Antenna Gain Envelope
3	Simulated Certificate Request
4	Simulated Certificate Delivery I (Complete Transaction)
5	Simulated Certificate Delivery II (Resumed Transaction)
6	BSM Parameter Accuracy
7	Simulated Implausible Message
8	Simulated Signature Failure
9	Simulated Misbehavior Report

Certification Testing for Foundational Standards: SAE J2735, IEEE 802.11, and IEEE 1609 Suite

Certification testing is a critical process and necessary step toward ensuring compliance with standards and requirements, and thus functional interoperability of the DSRC onboard devices and roadside devices. However, development of standardized certification processes is a sophisticated and challenging endeavor that could face many issues and require legal, policy, technical, and institutional decisions from a variety of perspectives.

Recognizing the importance and complexity of DSRC device certification, the USDOT previously initiated two separate efforts to support the flagship connected vehicle project from 2011 to 2013 – the Safety Pilot Model Deployment (SPMD). The first project was to conduct qualification and certification testing on Vehicle Awareness Devices (VAD) for verification and validation of basic DSRC device functionality. The majority of testing focused on ensuring devices were compliant with applicable IEEE 802.11p, IEEE 1609, and SAE J2735 standards, particularly for the V2V BSM. Final test results were presented to the USDOT for a Qualified Product List (QPL) selection from the participating device manufacturers. Similarly, the second project was to conduct qualification and certification testing for ASDs and Retrofit Safety Devices (RSDs). In addition to verifying and validating VAD functionalities, this project tested message exchanges and message sequences between the ASD and the Security

Credential Management System (SCMS), as well as other ASD-only features, such as dual radios, continuous/alternate channel mode operations, etc. The University of Michigan Transportation Research Institute (UMTRI) that managed the Safety Pilot Model Deployment activities and the Saxton Transportation Operations Laboratory (STOL) located at USDOT's Turner Fairbank Highway Research Center (TFHRC) also conducted several rounds of interoperability tests and roadside equipment validation tests. All of these previous coordinated certification efforts were primarily aimed at providing qualified DSRC devices to support the SPMD operations. None of them were positioned for general and full spectrum certification needs. However, these test procedures can be leveraged to develop high-level compliance test procedures to determine foundational standards compliance.

In early 2015, the USDOT released another effort for the creation of the "Next Stage Certification Environment." A multiple layer approach has been proposed for devices and applications certification including device hardware/firmware, software, and radio components certifications to meet environmental and communications requirements. The objectives of this ongoing project are to conduct qualification and certification testing for various devices and applications used in the large scale deployment trials in the next few years (CV Pilots). Through these efforts, the project is also trying to kick start the certification process and push it over to industry by supporting participants that have experience in certification testing. The project focus is primarily on developing common interpretations of vehicle situation data, field situation data, and application protocol data which is at a much lower level than the focus of this report and accompanying requirement and compliance test recommendations.

To gauge industry efforts, the team reached out to the Automotive Interest Group within the Wi-Fi Alliance, a non-profit industry association that certifies Wi-Fi products, and found that the organization is planning to develop certification tests to ensure DSRC devices are compliant with IEEE 802.11 and thus interoperable. While DSRC device testing is new to the alliance, the organization plans to achieve this through developing a marketing task group that will determine what needs to be tested based on use cases with the assistance of industry stakeholders and a technical task group that will write the test procedures. While the Wi-Fi Alliance only plans to conduct industry certification on the lower layers, specifically IEEE 802.11, there is a precedent for having joint certification testing where the alliance focuses on one set of tests and another organization completes secondary tests. The Wi-Fi Alliance seems to have support for this testing structure through a liaison agreement with OmniAir and support through OEMs and Tier 1s such as General Motors (GM), Ford, and Denso.

The Booz Allen team has developed basic compliance test procedures for OBE/Component level tests, and recommends the USDOT consider relying on industry groups to develop the necessary detailed tests to ensure devices are compliant with foundational standards. This would take some burden off of the USDOT and allow innovative certification schemes. Also, devices will already have to be compliant with these standards to successfully complete the recommended compliance test procedures found in this report. Basically, the devices will be tested for existing standard compliance by completing the higher level tests.

Validation Testing and Simulation

This subsection provides information on the validation testing conducted by the Booz Allen team on selected recommended compliance tests to check the feasibility of the test and the associated performance requirements. The validation tests are not meant to be final compliance tests, but rather were designed to ensure that some of the new requirements developed in this project are feasible, and to test the impact of vehicle-level specifications and differences on various requirements that were derived through simulations, data collection, and engineering expertise.

6.1.3 Rationale for Selected Compliance Tests for Validation Testing and Simulation

This subsection describes the compliance tests selected for validation testing and the rationale for selecting those specific tests and not others. Some recommended compliance tests may not be feasible given current constraints such as the absence of a fully functional SCMS at this stage of development.

Compliance tests identified in Appendix G. Full Recommended Compliance Testing Procedures represent a suite of tests to be performed at the OBE/component level and Vehicle level to assure or verify that a given vehicle implementation meets the recommended requirements. Ideally these tests should be validated by running them against a candidate vehicle to illustrate a) how to perform the test and b) that the tests are able to efficiently screen out non-performing or non-compliant vehicles. However, many of these tests assume the existence of a test vehicle fitted with equipment developed to meet the recommended specifications, and most of these tests also require unique test equipment specifically designed to support these tests. The team strongly recommends developing a reference design vehicle test facility capability that can be used to carry out these vehicle levels tests in the future, as devices and integrated vehicles evolve. Refer to Appendix G. Full Recommended Compliance Testing Procedures for more information on the recommended compliance test facility and equipment requirements. This facility would include:

- A reference design test vehicle capable of generating BSMs within the recommended performance requirements. The vehicle would need to be developed as a reference design against the recommended requirements. It is possible that this could be done by a car maker, or it could be a standalone suite of connected vehicle test equipment added to an existing production vehicle.
- A vehicle test assembly that can be installed in (and removed from) a test vehicle for testing. This assembly would include a full suite of “ground truth” sensors together with the processing and radio capability to offload the truth data to the roadside test system in real time.
- A fixed roadside test unit that has the ability to generate simulated BSMs (valid, erroneous, and invalid) to test the vehicles ability to identify valid, erroneous, and invalid BSMs
- Either a link to an operational SCMS, or a simulated SCMS used to support testing of the various security elements of the requirements.

Since this facility has not yet been developed, it is difficult to carry out the vehicle level road test portions of the compliance tests. However it may be possible to carry out some compliance tests with existing equipment, and it may be possible to adapt existing test equipment developed earlier on this and other Saxton Transportation Operations Laboratory (STOL) Test Bed projects to “sketch out” the compliance tests and demonstrate that they are generally feasible and can produce useful results. These are described in the following section.

6.1.4 Selected Validation Tests and Simulations

The eventual tests selected as feasible for validation testing without significant supporting development (while providing the most value in requirements and compliance test development) included:

1) Transmit Power and Antenna Gain and Sensitivity Envelope Validation Test: 3-Dimensional radiated power tests (azimuth and elevation)
2) BSM Parameter Error Proof of Concept (POC) Test: A simple BSM parameter (position) accuracy test to illustrate how a more formal BSM parameter accuracy test might be developed and conducted.
3) Level 1 Plausibility Check Simulation: A simulation to test the feasibility of the recommended Level 1 Plausibility check requirement
4) Congestion Mitigation POC Simulation– 20 MHz Channel: A simulation to test the feasibility of using a 20 MHz channel and data rate switching strategy as a possible congestion mitigation solution
5) BSM Parameter Error Tolerance Validation Simulation: Additional BSM parameter error tolerance simulations to verify results for horizontal position, speed, heading, and time while determining tolerances for the additional parameters of vertical position, acceleration, and yaw rate. Refer to 4.3.12 for results.
6) Range vs. Power, Channel, and Data Rate Test: Additional communications reliability tests performed at 6 and 9 Mbps using a 10 MHz channel and 12 and 18 Mbps using a 20 MHz channel (these tests were not performed at VTTI earlier this year). Refer to 4.3.3 for results.

A full description and rationale for the tests/simulations, along with the results, analysis, and findings are in the sections below.

Many recommended requirements and compliance tests were not selected for testing because of time constraints in developing testing systems, could not be tested based on existing DSRC units and SCMS prototypes, or existing analogous tests are already well established. The requirement types not chosen for validation testing were:

- Foundational standards
- Certificate management operations
- Misbehavior/intrusion detection
- Software updates
- Storage capacity
- Self-tests
- Malfunction indications
- Plausibility Level 2
- Remote system management server (e.g., SCMS) transactions

6.1.5 Transmit Power and Antenna Gain and Sensitivity Envelope Validation Test

6.1.5.1 Description and Rationale

This test was designed to illustrate the envelope of sensitivity and radiated power at the vehicle level for DSRC antennas located at various places on the vehicle roof.

Conceptually, the ability for a vehicle to receive transmission from other vehicle and to transmit messages that can be received by other vehicles depends on the elevation angle of the radiation and sensitivity patterns. This is important because elevation changes in the roadway (i.e., hills and valleys) will mean that vehicles will be at different orientations to one another. This is illustrated in Figure 35 and Figure 36. To assure that they can communicate, the combined antenna and vehicle system must provide sufficient receive sensitivity and transmit power output at these elevation angles.

For this test, the team assessed radiated power and radio sensitivity of a vehicle with a commercial antenna (i.e., MobileMark: +5 dBi gain) located in front and rear positions on the vehicle roof to determine the feasibility of the recommended radiated power and radio sensitivity requirements and associated recommended compliance test procedures. The requirements and compliance tests are vehicle dependent and must account for vehicle body, height, and antenna placement as well as any original equipment accessories such as roof racks. The team used the turntable facility at Southwest Research Institute to conduct these tests.

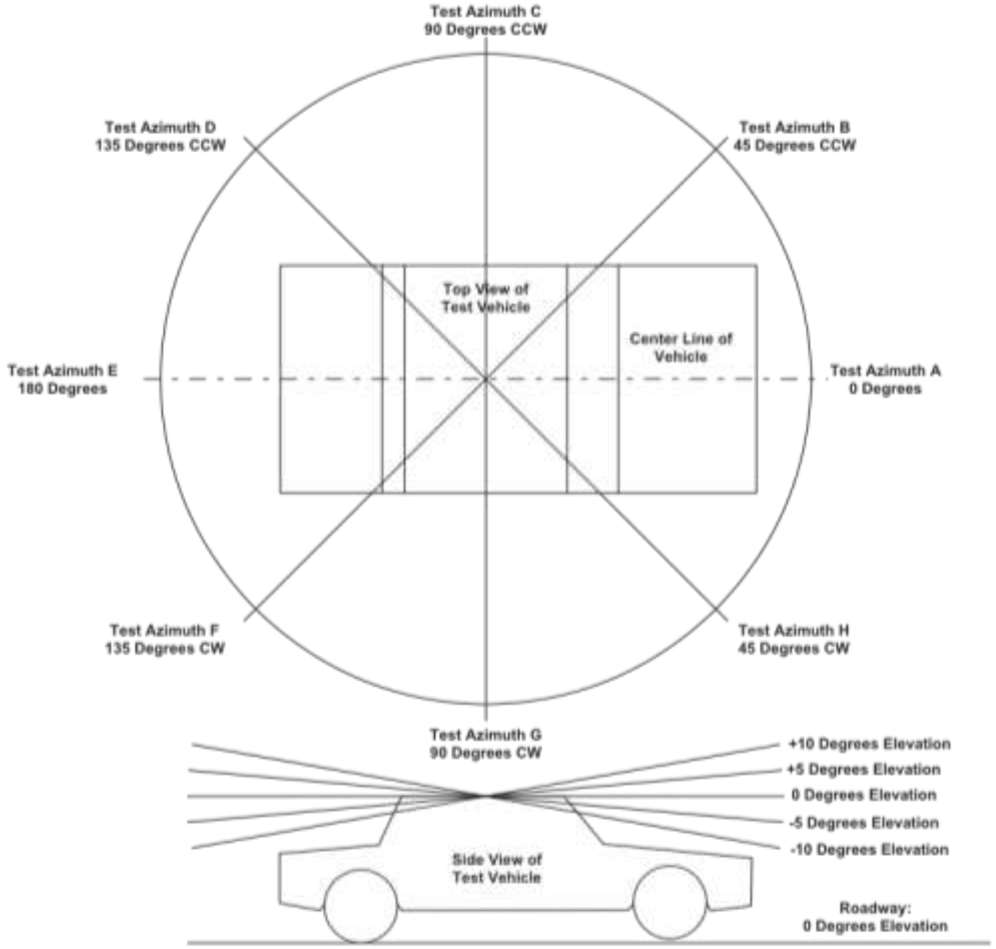
The original validation test procedure called for testing radiation power and sensitivity at different azimuths and elevation angles around the vehicle as represented in the figure below.
Sensitivity: Illuminate vehicle at 0 degrees elevation at nominal test range (30 meters); adjust power power level of test messages or CW signal) until OBE just fails to receive them (e.g., 10%PER 10%PER assessed in the field; log 2000 messages at each measurement orientation as shown in shown in

1) Figure 64 below.

Output power: Configure vehicle OBE to generate test messages or CW test signal; Set test receiver receiver at 0 degrees elevation and nominal test range (30 meters); Measure power level of sent sent messages (or CW signal) at each measurement orientation as shown in

2) Figure 64 below.

Figure 64: Radiation and Sensitivity Test Measurement Orientations (Source: USDOT)



6.1.5.2 Results, Analysis, and Findings

The test was conducted at the turntable facility of SwRI using two vehicles: the Nissan Altima and the Ford Escape. Neither vehicle was equipped with roof racks but each had an OEM antenna at the rear of the roof. Two Supplier B DSRC units (one each at the front and rear of the roof) were used at +20 dBm power with MobileMark (+5 dBi gain) antennas. A signal generator with the same type of MobileMark antenna generating at 20 dBm signal was used as the baseline. While the test plan was originally written to include both radiated transmit power and receiver sensitivity, the team realized that testing sensitivity was problematic since the only way to accomplish this at the vehicle level would be by measuring PER. PER typically does not exhibit a graceful degradation (it is either very low, or very high), and with the fixed distance measurement available at the test turntable a useful PER measurement would be impractical (it would require the insertion of attenuators in the signal path, which would then not really be a "vehicle level test." Instead, the team focused on evaluating radiated power. This is representative of both the radiated power envelope and the sensitivity envelope because the antennas are reciprocal (they work the same whether sending or receiving), and the spatial envelope (i.e., the azimuth and elevation variations) are due to the antenna, not the receiver sensitivity or the transmit output power. For this reason, the team recommends a requirement on the radiated power envelope instead of a requirement for both the radiated power and sensitivity envelopes.

The tests produced the results in the tables and figures below which met the recommended requirement for radiated power greater than -70 dBm when measured at 30 m in all azimuth directions between -5 and 0 degrees elevation. It must be stressed that these power levels are consistent with the relatively long ranges observed in earlier tests at VTTI and during other tests such as Safety Pilot. As noted elsewhere in this report, longer ranges are not necessarily a benefit for connected vehicles. The longer the range the greater the potential for channel congestion because more vehicles will be "in range." In addition it does not appear that many applications require such long ranges. As a result, it may be useful to reduce the required signal power over the geometric envelope described here (for example from -70 dBm to -80 dBm) and to impose an upper bound as well as a lower bound, or the congestion control algorithm should include a power-control facet as well.

The team was unable to perform measurements at -10, +5, and +10 elevation angles due to testing site limitations. Future testing sites should be able to assess +5 and +10 degree elevation angles by elevating the turntable and/or having a tower. Measuring -10 degrees elevation can also be tested with an elevated turntable, but it is not necessarily practical to perform it for every make and model. Future testing should also be able to assess whether it is necessary to test every make and model to -10 degrees elevation.

The magnitude of the signal measured around each vehicle varies by as much as 10 dB from front to rear and side to side, depending on the placement of the transmitter antenna. This variation can be cause by the quality of the antenna, the makeup of the roof of the vehicle and underlying wiring, and the test apparatus itself. The measurement differences between 0 and -5 degrees elevation were fairly consistent. As seen within the tables and figures, the stated requirement is definitely feasible. However, the OEM must determine the correct balance of antenna(s) type, placement, power, etc. to ensure the vehicle meets the requirement at all azimuth and elevation angles. A very controlled test is recommended to verify the antenna performance with respect to each made and model of vehicle.

Table 22: Nissan Altima Transmit Power and Antenna Gain Envelope at 30 meters

	Signal Generator (Center)		Front Antenna		Rear Antenna	
	-5° elevation	**0°**	**-5°**	**0°**	**-5°**	**0°**
0° azimuth	-66	-64	-55.7	-53	-63.2	-61.6
45°	-57.5	-55.7	-54.4	-53.8	-62.2	-59.7
90°	-60.7	-59.1	-56.6	-57.5	-57.2	-54.4

	Signal Generator (Center)		Front Antenna		Rear Antenna	
135°	-57.5	-55	-57.2	-56	-54.1	-52.5
180°	-58.2	-55	-67.2	-66	-63.2	-61
225°	-63.2	-61.9	-59.4	-59.1	-63.2	-60.7
270°	-58.2	-57.9	-66.9	-63.8	-65	-62.5
315°	-66.9	-63.2	-58.2	-55.7	-59.7	-59.4
Average	-61.025	-58.975	-59.45	-58.1125	-60.975	-58.975

Figure 65: Nissan Altima Transmit Power and Antenna Gain at 0 Degrees Elevation (Source: USDOT)

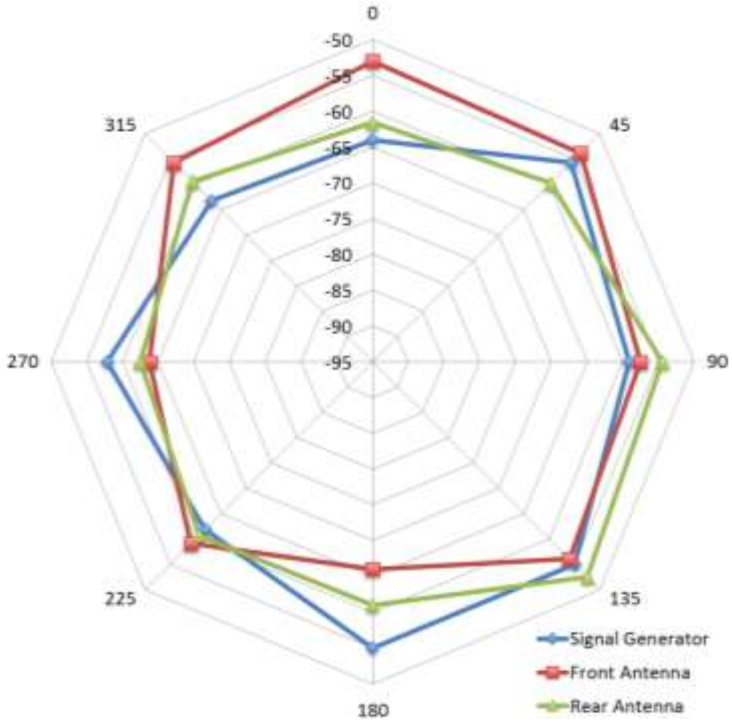


Figure 66: Nissan Altima Transmit Power and Antenna Gain at -5 Degrees Elevation (Source: USDOT)

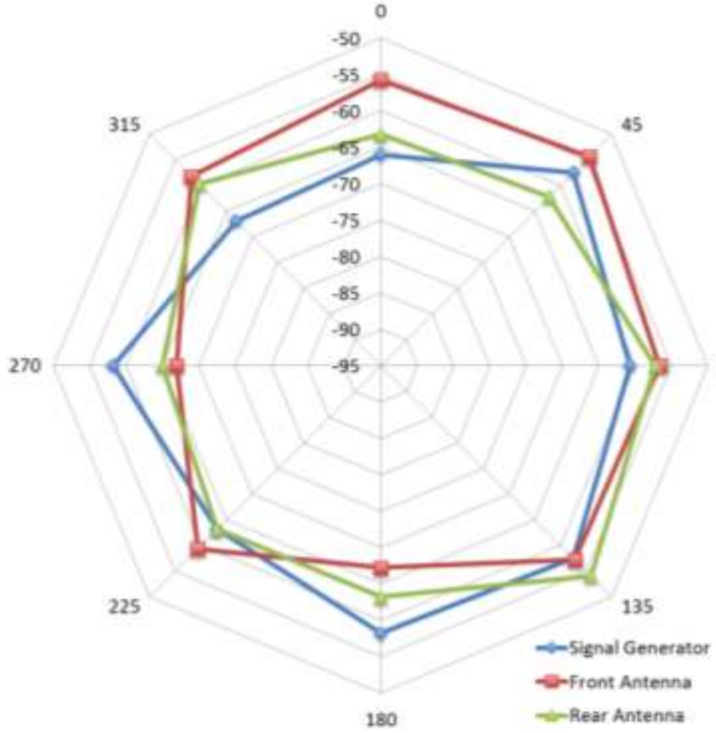


Figure 67: Nissan Altima Front Antenna (0 vs -5 degrees elevation) (Source: USDOT)

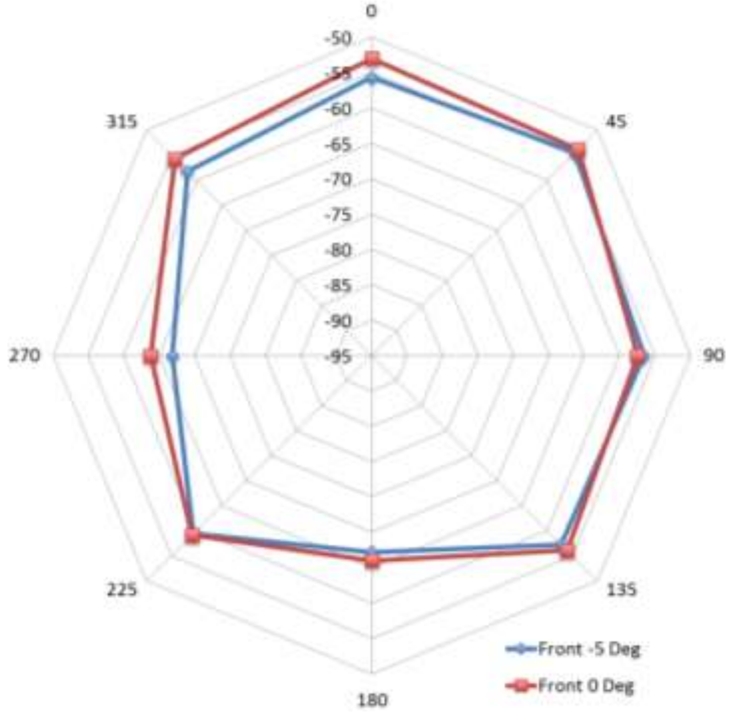


Figure 68: Nissan Altima Rear Antenna (0 vs -5 degrees elevation) (Source: USDOT)

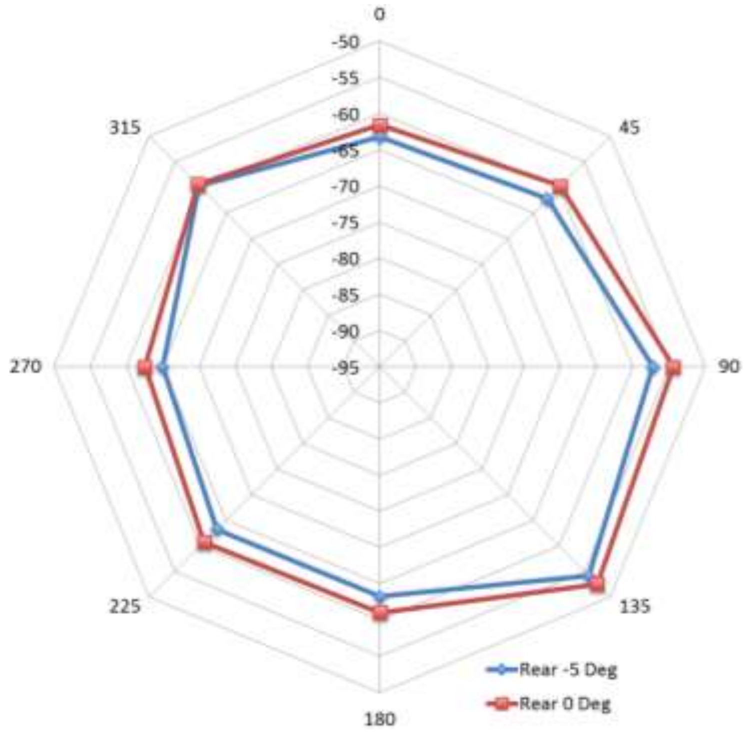


Table 23: Ford Escape Transmit Power and Antenna Gain Envelope at 30 meters

	Front Antenna		Rear Antenna	
	-5°	**0°**	**-5°**	**0°**
0° azimuth	-54.4	-56.3	-63.6	-62.2
45°	-56	-55.7	-61.9	-59.7
90°	-55.7	-55.4	-60.7	-58.2
135°	-59.1	-58.2	-53.8	-53.8
180°	-64.7	-66.9	-52.9	-58.5
225°	-64.1	-64.7	-61	-62.5
270°	-61.6	-64.7	-56.3	-57.5
315°	-57.9	-58.5	-68.2	-66.3
Average	-59.1875	-60.05	-59.8	-59.8375

Figure 69: Ford Escape Transmit Power and Antenna Gain at 0 Degrees Elevation (Source: USDOT)

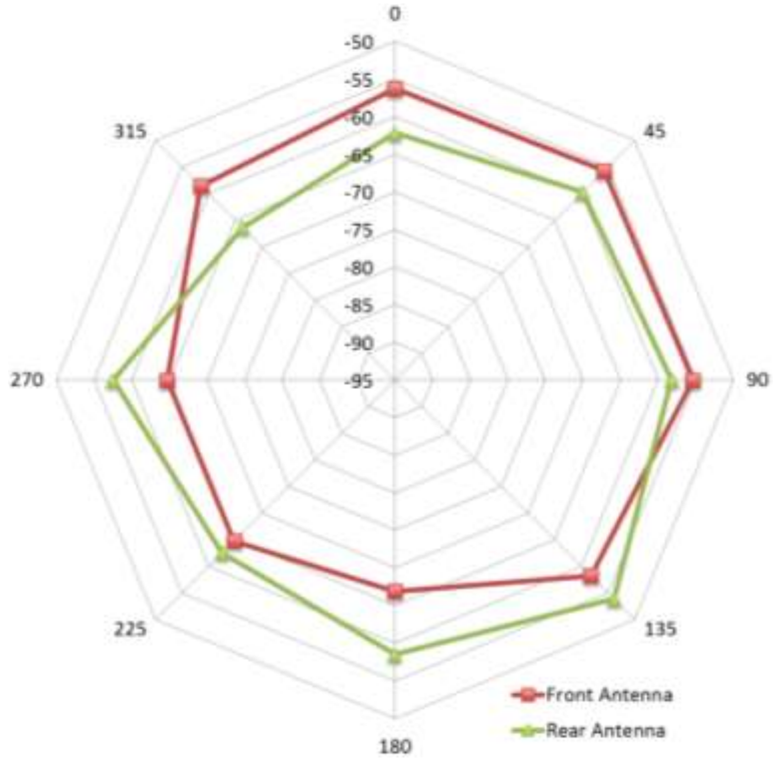


Figure 70: Ford Escape Transmit Power and Antenna Gain at -5 Degrees Elevation (Source: USDOT)

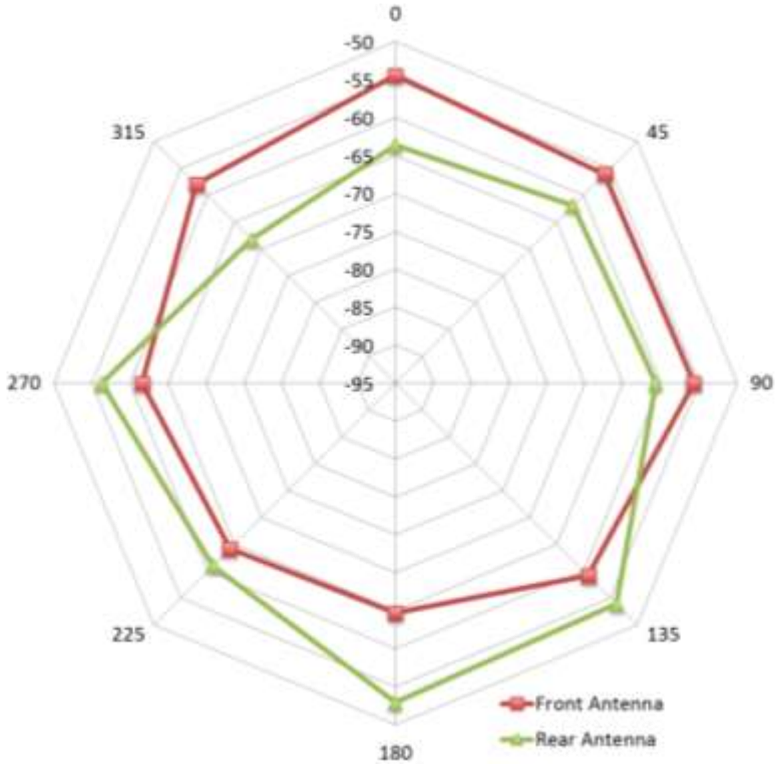


Figure 71: Ford Escape Front Antenna (0 vs -5 degrees elevation) (Source: USDOT)

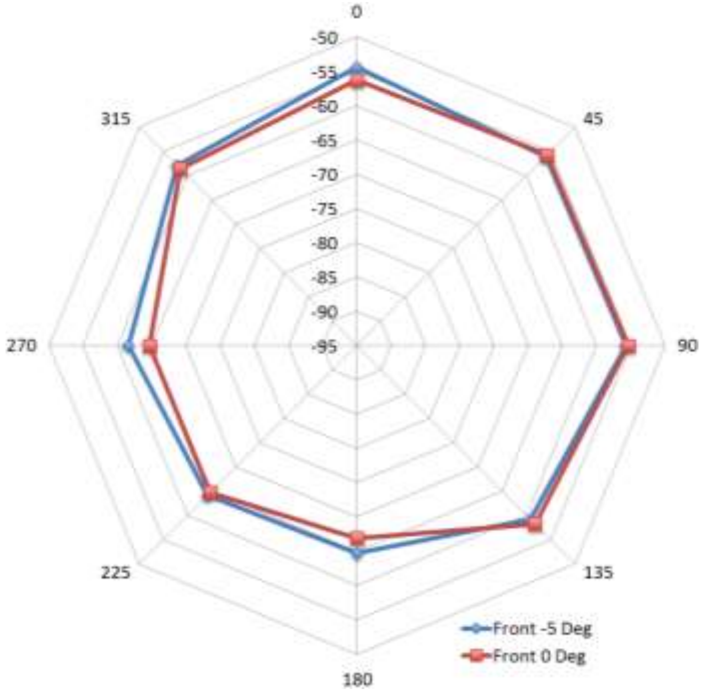
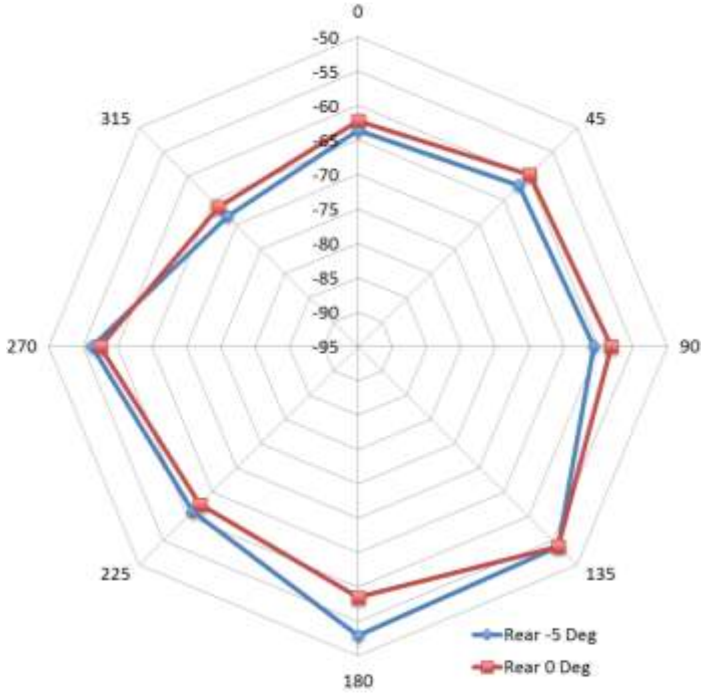


Figure 72: Ford Escape Rear Antenna (0 vs -5 degrees elevation) (Source: USDOT)



6.1.6 BSM Parameter Error Proof of Concept Test

6.1.6.1 Description and Rationale

The purpose of this test is to provide a first order demonstration of the BSM data sensor error test proposed to eventually be used as a vehicle level test for NHTSA. Because there was not a vehicle equipped to generate actual BSMs, this test was performed by measuring typical BSM (e.g., position) parameters using external sensors (i.e., not part of the vehicle). As a result, the parameters were not bundled in a BSM and transmitted, but instead were generated from sensors and logged directly in the vehicle together with vehicle ground truth data. The sensor data and ground truth data were then compared to assess the parameter errors. The validity of this test is not impacted by this change since sending the data over the air would not introduce any additional parameter errors.

The proof of concept test used a ground truth sensor/reference device mounted in a vehicle (NovaTel FlexPak 6 with OmniStar High Performance [HP] subscription), and commercial sensors (uBlox GPS receiver and Supplier B OBE with MobileMark antenna with integrated GPS) typical of a production implementation, that logged data from all three systems as the vehicle was driven around a test track at SwRI. The ground truth system was allowed about 20 minutes to converge to an accuracy of about 10 cm. The differences between the ground truth and production sensors were computed and analyzed.

A production vehicle level test would be carried out by having the test vehicle transmit BSMs using DSRC, receiving and logging those BSMs in the vehicle together with ground truth data, and then comparing the BSM data to the ground truth data (as described in the recommended compliance tests within the main report).

- Log sensor data associated with BSM parameters
- Log ground truth sensor data in vehicle
- Compare logged BSM data parameters with logged ground truth sensor parameters and determine errors

6.1.6.2 Results, Analysis, and Findings

This validation test proved the concept of conducting a BSM parameter error/accuracy compliance test to evaluate adherence to parameter accuracy requirements. However, the team did observe that the current consumer grade units (uBlox GPS receiver and Supplier B OBE with MobileMark antenna with integrated GPS) did not provide the level of accuracy recommended for horizontal position (0.325 meters error tolerance, comparatively exhibited by the yellow block in Figure 73). Figure 73 shows that the reference device horizontal position accuracy was within a range of about 0.2 meters, while the Supplier B device had a range of about 1.5-2 meters and the uBlox had a range of about 3 meters. Refer to 4.3.12 for a full explanation and justification of recommended BSM parameter accuracy requirements. Horizontal position was the only parameter evaluated during this POC test.

Figure 73: BSM Parameter Error POC – Stationary Data Plots (Source: USDOT)

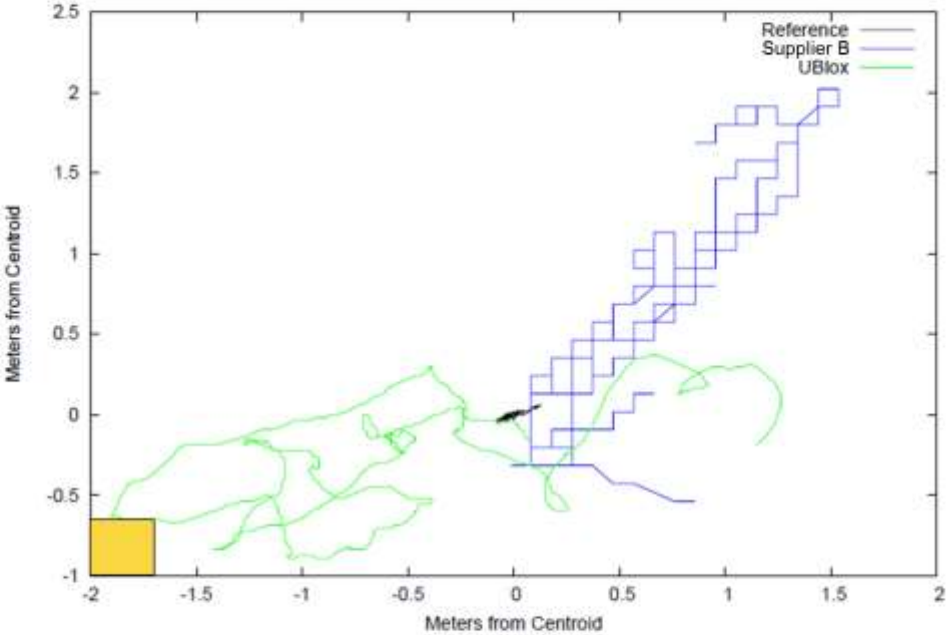


Figure 74 compares the positions indicated by each device while driving twice around the SwRI 1.16 mile track and back to the vehicle setup bay. While the reference and Supplier B devices clearly follow the path of the track and road, the uBlox device periodically drifts away from the route and completely loses position in some areas. It is clear that there are differences between the ground truth positions (black lines/dots) and the test sensor (green lines). Figure 75 and Figure 76 illustrate these differences in terms of latitude and longitude error as a function of test time (i.e., at various positions along the test course during the test). Only the reference and uBlox sensor data are shown in Figure 75, Figure 76, and Figure 77 because both sensors log data at one time per second while the Supplier

B sensor logs data at 10 times per second making it extremely difficult to align the reference and uBlox sensor with the corresponding Supplier B data point. However, the concept of the test has been proven in comparing the reference and uBlox data points.

Figure 74: BSM Parameter Error POC – Dynamic Data Plots (Source: USDOT)

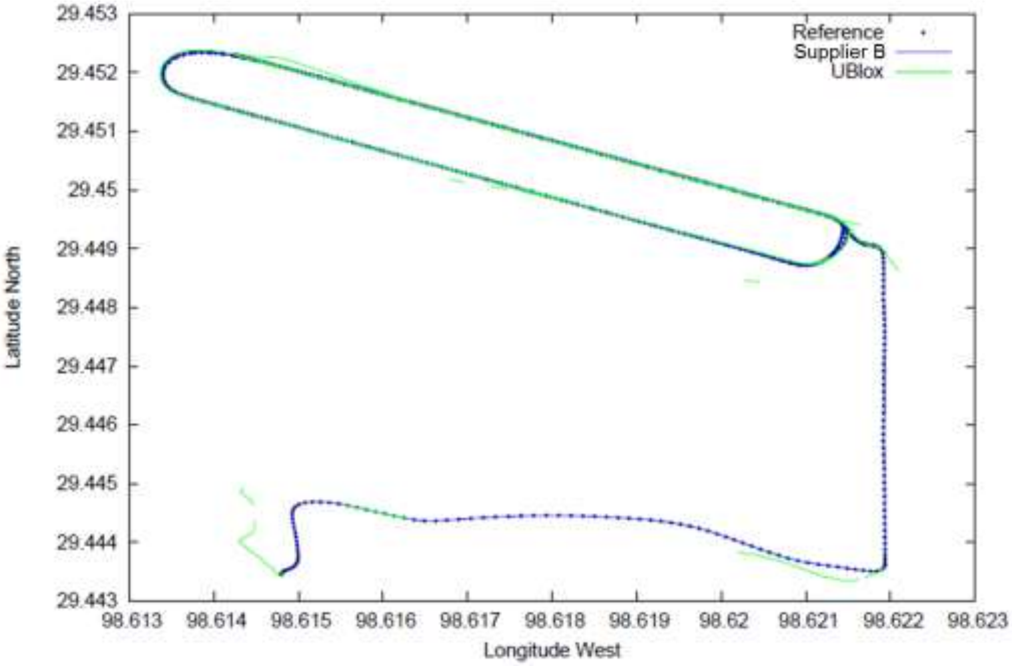


Figure 75: Latitude Error Truth Sensor vs. uBlox Sensor (Source: USDOT)

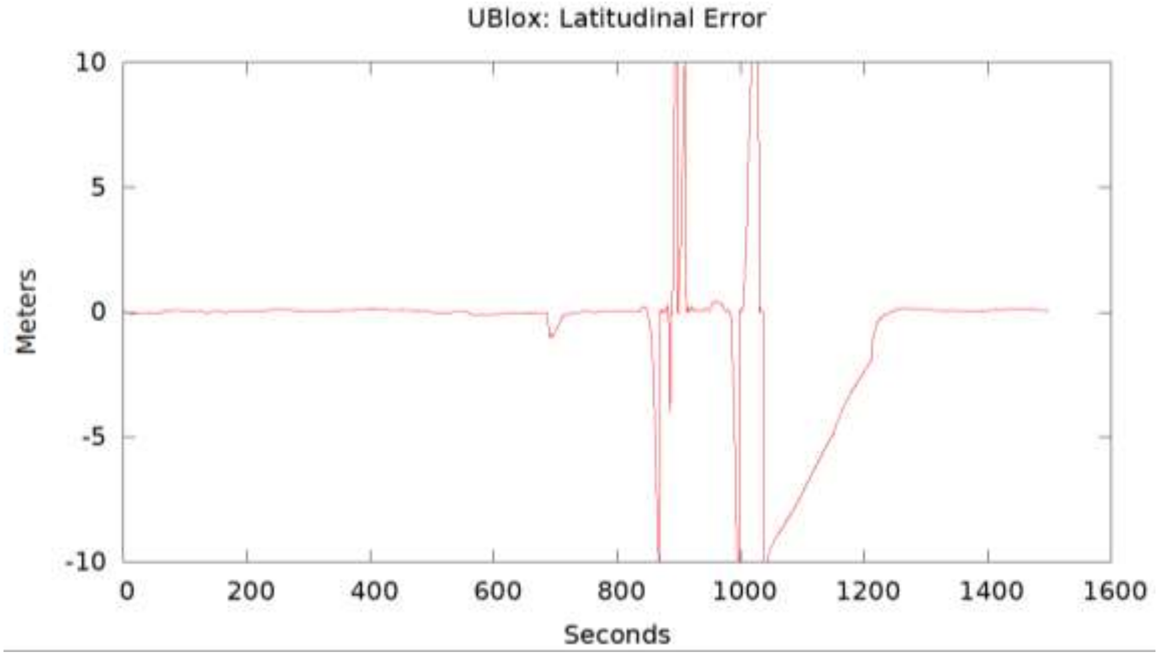


Figure 76: Longitude Error Truth Sensor vs. uBlox Sensor (Source: USDOT)

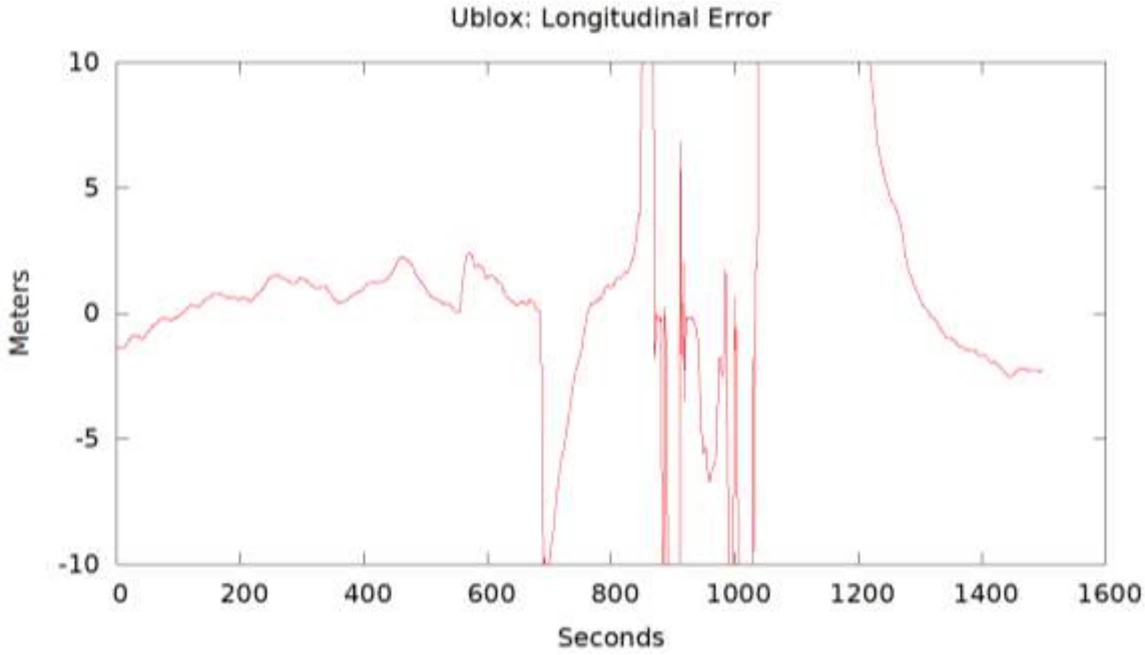
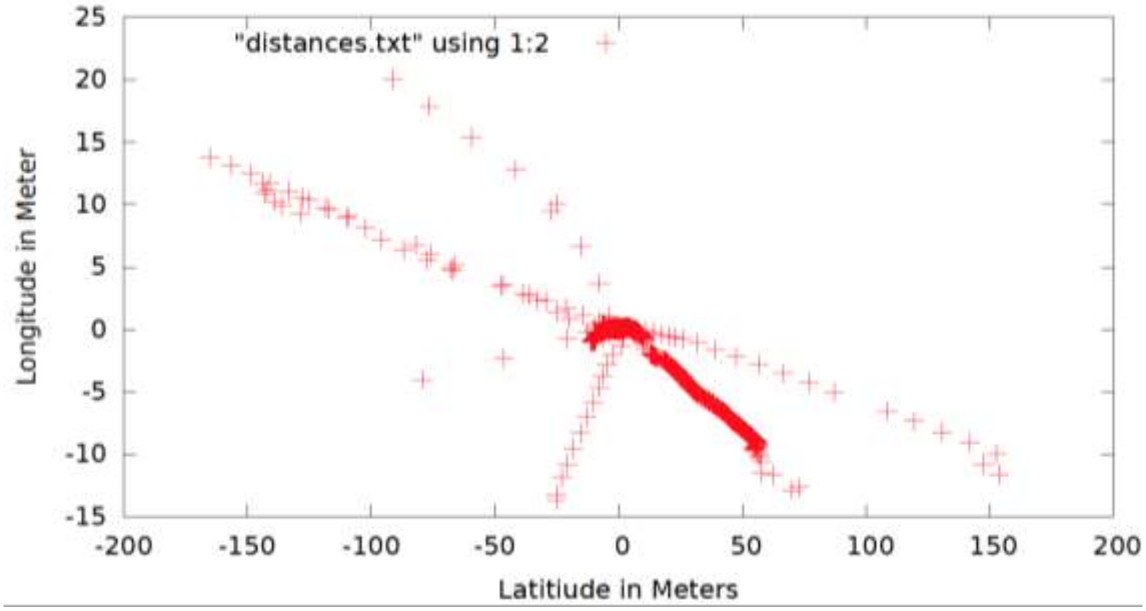


Figure 77 below illustrates the combined latitude and longitude error.

Figure 77: Latitude/Longitude Combined Error (Source: USDOT)



As can be seen from the error plots above, the uBlox sensor provides position performance accurate to about 1 meter over most of the test course. At times the sensor output deviates significantly (100 meters or more) from the ground truth data, and then recovers. This is presumably due to instability of the fix as the system loses one or more satellites and then regains them or regains lock on additional satellites. Clearly this behavior will impact the ability of any user applications to make accurate and reliable collision decisions, and argues for a more sophisticated and more stable position determination approach (for example a hybrid Inertial Measurement Unit (IMU) / GPS solution, which is well known in the industry).

6.1.7 Level 1 Plausibility Check POC Simulation

6.1.7.1 Description and Rationale

Current connected vehicle system concepts include provisions for "plausibility checks" on incoming messages. The recommended checks for plausibility include a Level 1 check, basically a boundary check, to determine if the parameters in the BSM are realistic (i.e., speed, acceleration and yaw rate values are less than some upper limits, and that they are internally consistent (i.e., reported yaw, lateral acceleration and speed values are mutually consistent given the physical laws that govern their relationship). The team is not recommending that the OBE automatically report a vehicle if one BSM fails a plausibility check. A vehicle could have parameters that are outside the established boundaries or not internally consistent in certain situations. For example, a vehicle could exceed the deceleration boundary if it hits a pothole or parameters may not be internally consistent according to the recommended equation if a vehicle is completely out of control (e.g., 360 degree spin on ice). However, sustained and continuous implausible messages from the same vehicle probably represents an instance of misbehavior. The recommended plausibility check requirements are described below. While the specific values identified in the recommended requirement for Level 1 plausibility can be adjusted as necessary, the ability to perform such checks on a large number of incoming messages is a necessary capability. The OBE must be able to perform the Level 1 Plausibility Checks on all incoming messages which will take a certain amount of processing time and memory.

The team developed a simulation in MATLAB to assess the processing latency associated with performing representative checks at various incoming message rates for up to 550 vehicles (equivalent to 5500 messages per second), using a variable core processor to carry out the mathematical operations at varying levels of message density. This is a highly congested scenario where the maximum message density is expected to be communicated among the vehicles in range of each other. The team then assessed the time associated with these mathematical operations, and the overall memory usage to determine if the proposed checks could realistically be carried out in a high traffic density environment. For the simulation, the team utilized one day sample BSM data collected from Safety Pilot Model Deployment testing in Michigan. The team extrapolated the sample data to produce more data to simulate a congested scenario and introduced random plausibility faults within the data set. 90% of the position speed and heading data were based on linear constant speed trajectory. In most trials, 10% of the data included data elements that are implausible (e.g., speed unrealistically high, speed not corresponding to change in position, heading changing unrealistically, heading not corresponding to changes in positon). The simulation was set to flag any BSMs that were outside of the recommended BSM parameter boundaries for speed, longitudinal acceleration, lateral acceleration, and yaw rate. It was also set to flag any BSMs were parameters were not mutually consistent.

Plausibility Level 1 Boundaries:

- <u>*Speed*</u>: Less than 70 m/s (252 kmph, 156 mph) which only excludes various supercars; well over any typical speed limits
- <u>*Longitudinal acceleration*</u>: 0-100 kmph in under 2.3 second (Less than 12 m/s^2). Based on Ariel Atom, fastest accelerating production vehicle

- *Longitudinal deceleration*: 100-0 kmph in under 95 feet (Less than -12 m/s^2). Based on Corvette Z6, fastest stopping production vehicle
- *Lateral Acceleration*: Less than 11 m/s^2 (1.12 G). Few production vehicles can exceed 1.0 G
- *Yaw Rate*: Less than 1.5 radian/s, Rationale: 1.5 radian/sec is about equivalent to taking a 15 mph right turn at 27 mph (1G); tighter corners are not feasible (>1G), and softer corners are lower yaw rate at 1G acceleration
- Values in BSM need to be internally consistent: Speed, lateral acceleration, and yaw rate are linked mathematically by the relation: $V^2=a_c^2/(Y')^2$. As a result, if the BSM includes speed, lateral acceleration, and yaw rate, the values in the BSM must follow this relationship within some allowable tolerance. For example, dividing the lateral acceleration value by the yaw rate should yield a speed value that is equal to (within some small tolerance) the speed value in the BSM.

The team conducted simulations with scenarios varying the number of vehicles, Central Processing Unit (i.e., computer) (CPU) cores, trial time duration, and BSM parameter error levels.

6.1.7.2 Results, Analysis, and Findings

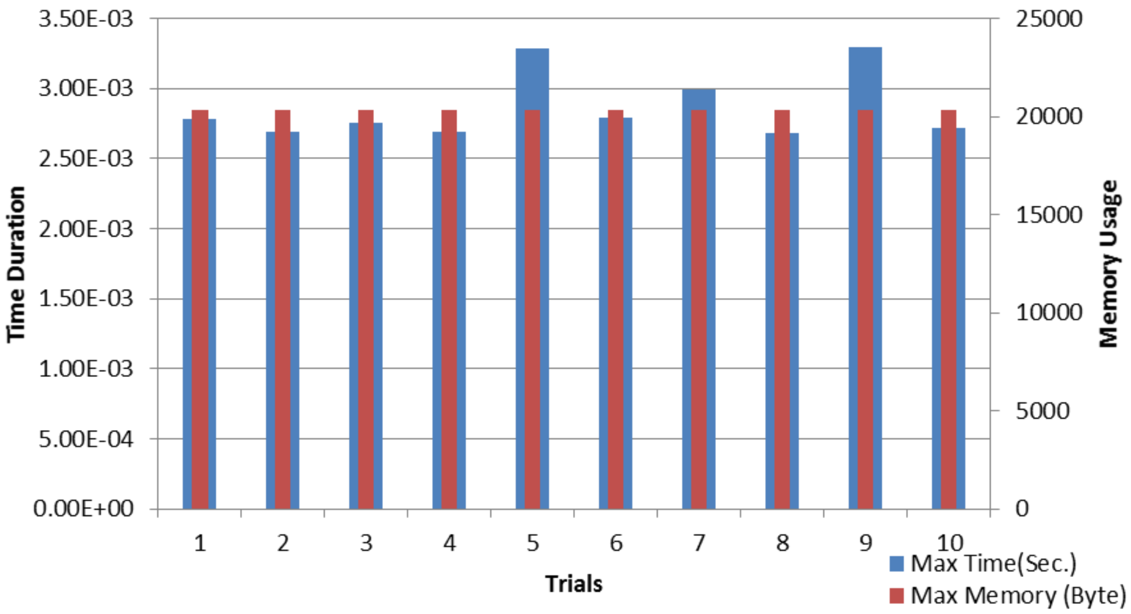
In the base simulation (Table 24 and

Figure 78), the program processed simulated BSMs generated every 0.1 second (10 Hz) with a mean BSM error of 10% from 550 vehicles in trials that ran for 30 seconds. The simulation was repeated 10 times. In each trial, the program successfully processed all 165000 BSMs, identifying all 16500 erroneous BSMs (those outside of established boundaries). For each 0.1 sec time step, 550 BSMs were processed in an average of 2.87 milliseconds while consistently using about 204 kilobytes of memory. The team found that the Level 1 Plausibility Check as specified in the recommended requirements (without other BSM processing actions) does not require a high level of processing time or memory. In another word, this plausibility check process does not require a significant amount of time and is well within the available working memory of commercially available processors. Complete simulation results for each scenario are in the tables and figures below.

Table 24: Level 1 Plausibility Check Simulation – Base Scenario Results

Trial Number	Max. Processing Duration (Sec.)	Processing Memory (Bytes)	Vehicle Number	Trial Time Duration (Sec.)	Time Step Sec. (Message Rate)	Mean Erroneous BSMs
1	2.78E-03	20350	550	30	0.1	10%
2	2.69E-03	20350	550	30	0.1	10%
3	2.76E-03	20350	550	30	0.1	10%
4	2.69E-03	20350	550	30	0.1	10%
5	3.29E-03	20350	550	30	0.1	10%
6	2.79E-03	20350	550	30	0.1	10%
7	3.00E-03	20350	550	30	0.1	10%
8	2.68E-03	20350	550	30	0.1	10%
9	3.30E-03	20350	550	30	0.1	10%
10	2.72E-03	20350	550	30	0.1	10%

Figure 78: Level 1 Plausibility Check Simulation – Base Scenario Results (Source: USDOT)



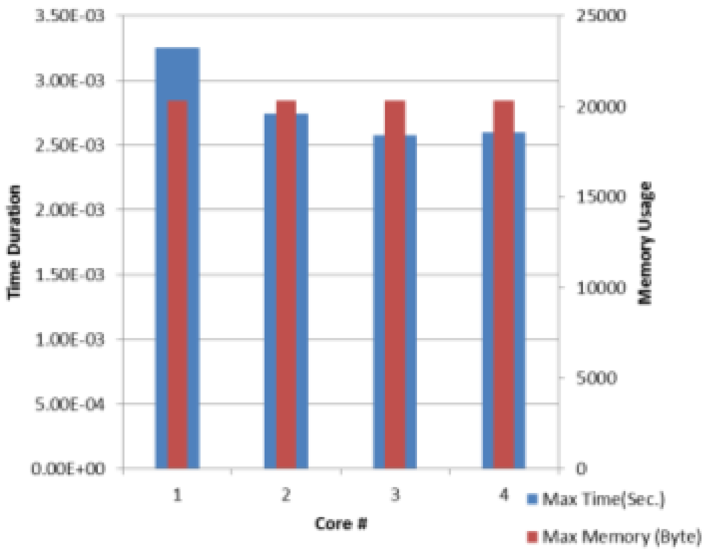
The team also ran a scenario with different cores to determine if the CPU has an effect on the usage. As seen in Table 24 and

Figure 78, the time and memory usage are similar or the same across the different cores. The average time is about 2.8 millisecond and the memory used is about 204 kilobytes.

Table 25: Level 1 Plausibility Check Simulation – Core Scenario Results

Max. Processing Duration (Sec.)	Processing Memory (Bytes)	Vehicle Number	Trial Time Duration (Sec.)	Time Step Sec. (Message Rate)	Mean Erroneous BSMs	Core Number
3.25E-03	20350	550	30	0.1	10%	1
2.75E-03	20350	550	30	0.1	10%	2
2.58E-03	20350	550	30	0.1	10%	3
2.60E-03	20350	550	30	0.1	10%	4

Figure 79: Level 1 Plausibility Check Simulation – Core Scenario Results (Source: USDOT)

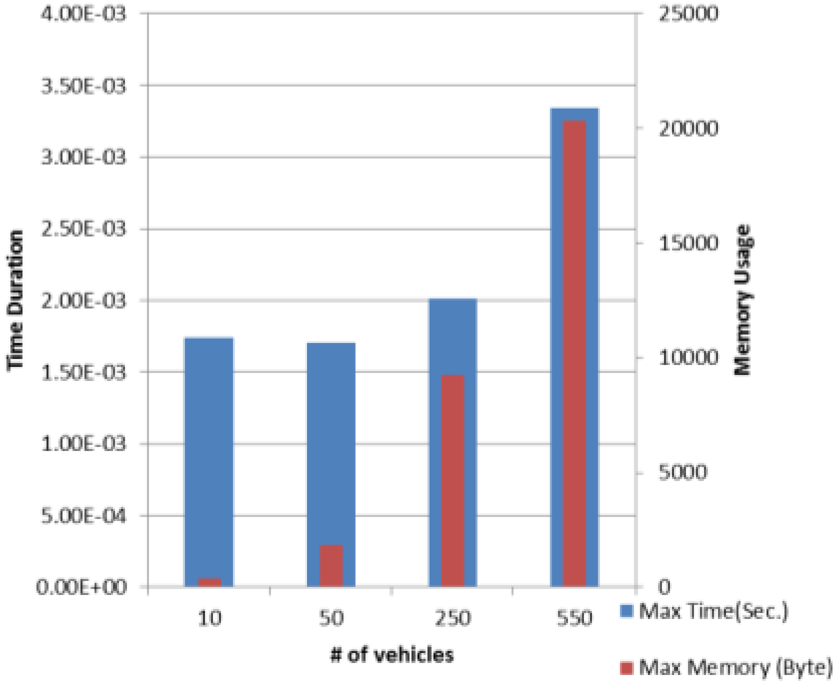


In the vehicle density scenario, the team ran the simulations for 10, 50, 250, and 550 vehicles. While time variance is negligible at an increase of only 1.6 milliseconds between the fastest (50 vehicles) and slowest (550 vehicles) processing times, the memory usage steadily increases as the vehicle number increases from 370 bytes to 204 kilobytes.

Table 26: Level 1 Plausibility Check Simulation – Vehicle Scenario Results

Max. Processing Duration (Sec.)	Processing Memory (Bytes)	Vehicle Number	Trial Time Duration (Sec.)	Time Step Sec. (Message Rate)	Mean Erroneous BSMs
1.74E-03	370	10	30	0.1	10%
1.71E-03	1850	50	30	0.1	10%
2.01E-03	9250	250	30	0.1	10%
3.34E-03	20350	550	30	0.1	10%

Figure 80: Level 1 Plausibility Check Simulation – Vehicle Scenario Results (Source: USDOT)

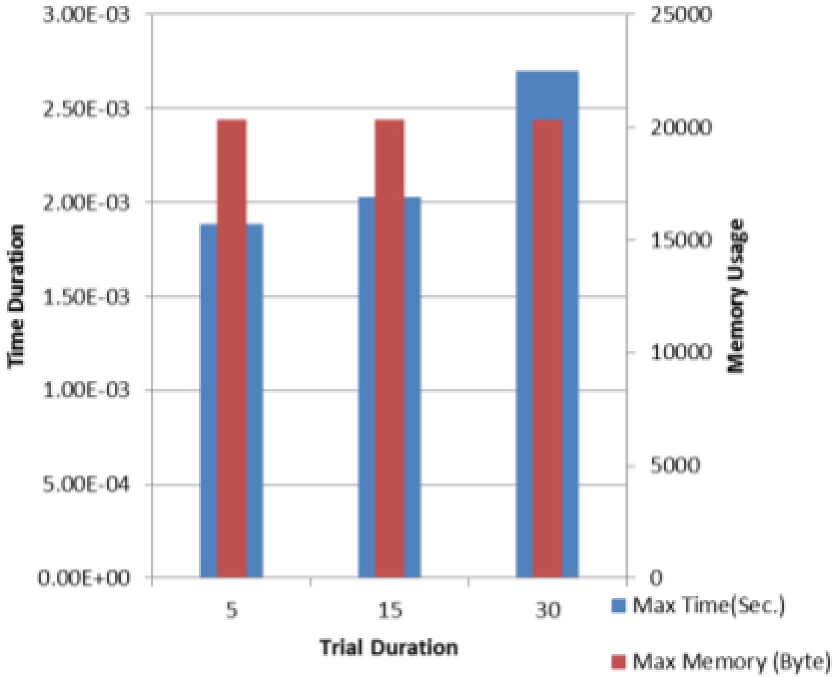


The team also ran varied the trial time duration (5, 15, and 30 seconds) of the simulations. There was no change in processing memory and less than 1 millisecond difference in maximum processing time duration. This is because the memory and time usage is again calculated for 0.1 second time steps. However, the insight observed is that the results are still consistent, no matter how long the simulation is running.

Table 27: Level 1 Plausibility Check Simulation – Trial Time Scenario Results

Max. Processing Duration (Sec.)	Processing Memory (Bytes)	Vehicle Number	Trial Time Duration (Sec.)	Time Step Sec. (Message Rate)	Mean Erroneous BSMs
1.89E-03	20350	550	5	0.1	10%
2.03E-03	20350	550	15	0.1	10%
2.70E-03	20350	550	30	0.1	10%

Figure 81: Level 1 Plausibility Check Simulation – Trial Time Scenario Results (Source: USDOT)

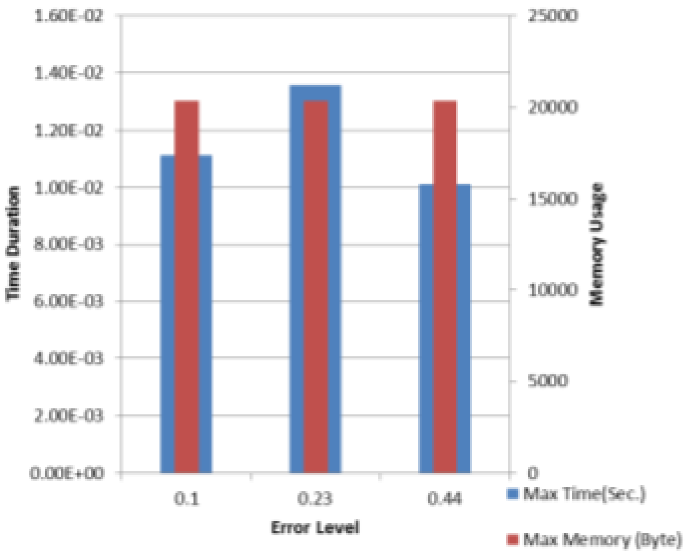


The team also varied the percentage of erroneous BSMs (10%, 23%, and 44%). There was no impact on processing memory and almost no impact on max processing time duration. This is because the number of calculations remains the same, albeit that various amount of errors are introduced in the datasets.

Table 28: Level 1 Plausibility Check Simulation – Error Level Scenario Results

Max. Processing Duration (Sec.)	Processing Memory (Bytes)	Vehicle Number	Trial Time Duration (Sec.)	Time Step Sec. (Message Rate)	Mean Erroneous BSMs
1.11E-02	20350	550	30	0.01	10%
1.36E-02	20350	550	30	0.01	23%
1.01E-02	20350	550	30	0.01	44%

Figure 82: Level 1 Plausibility Check Simulation – Error Level Scenario Results (Source: USDOT)



6.1.8 Congestion Mitigation POC – 20 MHz Channel Simulation

6.1.8.1 Description and Rationale

As mentioned in Chapter 4, Congestion Simulation, when there are many vehicles communicating within range of each other, the probability of unsuccessful message transmission increases. Since DSRC communication is based on all nodes broadcasting BSM messages where they are not actively managed by a base station, there is technically no limit to the number of users that can be served by a DSRC channel, except the limit that is introduced by the physical constraints (e.g., only so many cars could fit within 300 meter radius).

In the previous simulations, the team assessed how different channel parameters might impact congestion. The team simulated and analyzed congestion performance at various data rates, different message transmission rates, and both 10 MHz and 20 MHz channel bandwidths in order to better understand the options and tradeoffs for managing congestion.

The simulations suggested that in a congested network, it is possible to experience PERs as high as 46% which basically causes the system to be ineffective. As such, there is a need for a common method for mitigating congestion and hidden terminal effects which exacerbate as a result. Hence, the team introduced two considerations to address the issues by using a 20 MHz channel instead of the standard 10 MHz channel:

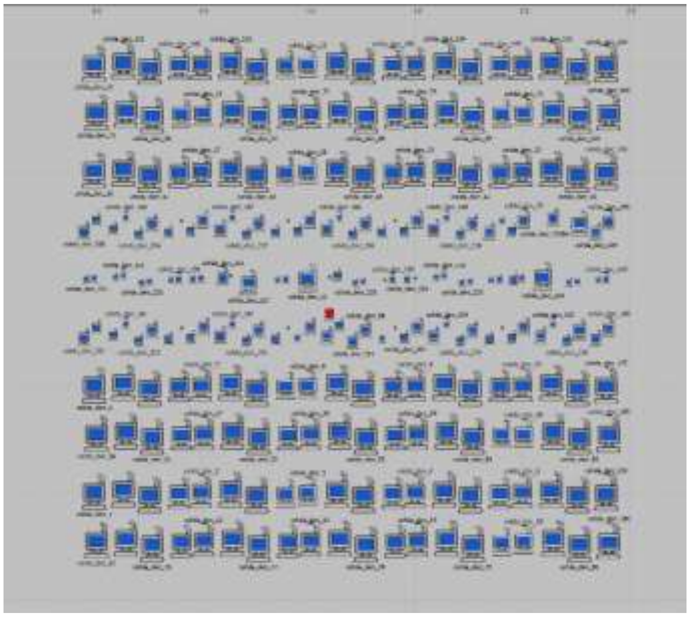
- The OBE shall transmit BSM WSMs on Channel 175 or equivalent (20 MHz channel), at a data rate of 12 Mbps when the CBR is below 50%
- The OBE shall transmit BSMs on Channel 175 or equivalent at a data rate of 18 Mbps when the Channel Busy Ratio exceeds 50%; such transmission shall continue until the Channel Busy Ratio falls below 20%

These initial requirements were set with arbitrary CBR percentages for switching the data rate. In order to validate these requirements, the team designed additional simulations to verify the aforementioned thresholds for CBR values when using the 20 MHz channel to mitigate congestion.

6.1.8.2 Results, Analysis, and Findings

The team started validation simulations with the congestion scenarios, previously designed. The scenario consisted of 256 transmitting devices within communication range of each other and one receiver in the middle:

Figure 83: Congested Network Simulation in Opnet (Source: USDOT)



This scenario puts the focus mainly on the congestion issue and minimizes the hidden node effect. Parameters were set as follows:

Table 29: Simulation Parameters

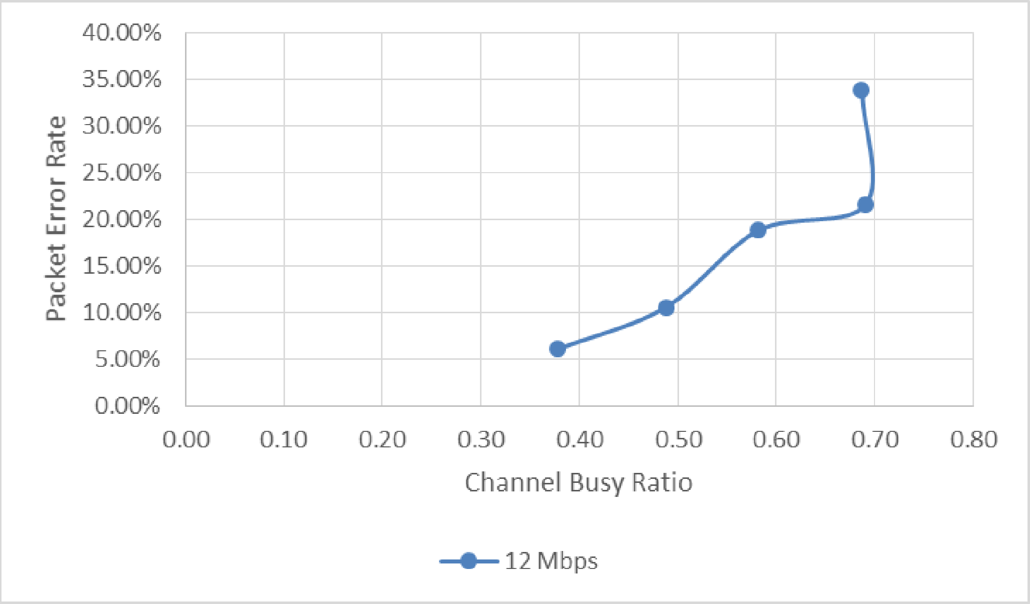
Parameter	Value	Parameter	Value
Minimum Frequency	5855 MHz	**Packet (message) Size**	300 bytes
Transmit Power	20 dBm	**Modulation**	Orthogonal Frequency-Division Multiplexing (OFDM)
Packet Reception Power Threshold	-95 dBm	**Message Transmission Rate**	10 Hz
Transmitter Antenna Height	1.5 meter	**Bandwidth**	20 MHz
Receiver Antenna Height	1.5 meter	**Data Rate**	12 Mbps

The simulation obtained the CBR value which was already above 50%. The team continued adding the nodes, up to 350 devices, and observed that the CBR reached about 70% which translated to PER value of about 34%:

Table 30: CBR and PER at Various Congestion Levels - 12 Mbps

Number of Devices	CBR at 12 Mbps	PER at 12 Mbps
150	37.78%	6.07%
200	48.77%	10.56%
256	58.21%	18.85%
300	69.09%	21.66%
350	68.67%	33.86%

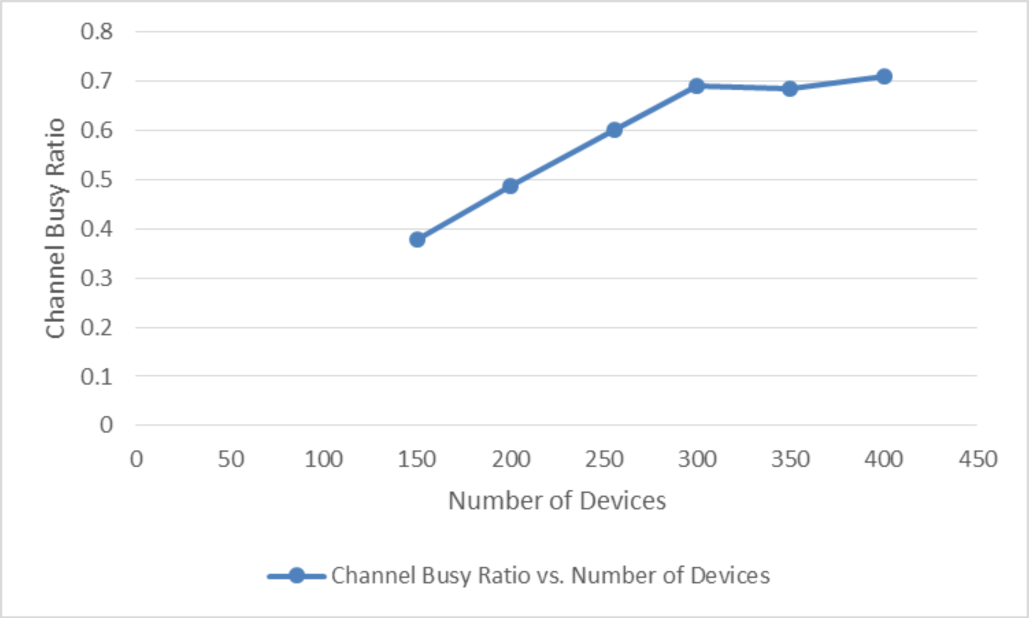
Figure 84: Congested Simulation – Packet Error Rate vs. Channel Busy Ratio, 12 Mbps (Source: USDOT)



As one can see in the figure above, the CBR plateaus around 70%. To better see this effect, the team continued adding to the number of vehicles, up to 400, to see how the CBR curve changes. As indicated in figure below, around 300 vehicles the CBR value does not change that much by increasing the number of vehicles. It plateaus around 70% and it stays there. 70% is about the expected throughput of a LAN that uses CSMA, measured in terms of medium occupancy rate or CBR, not data rate[12].

[12] Please see more details about CSMA throughput and CBR in Appendix D.

Figure 85: Channel Busy Ratio vs. Number of Devices – 12 Mbps (Source: USDOT)

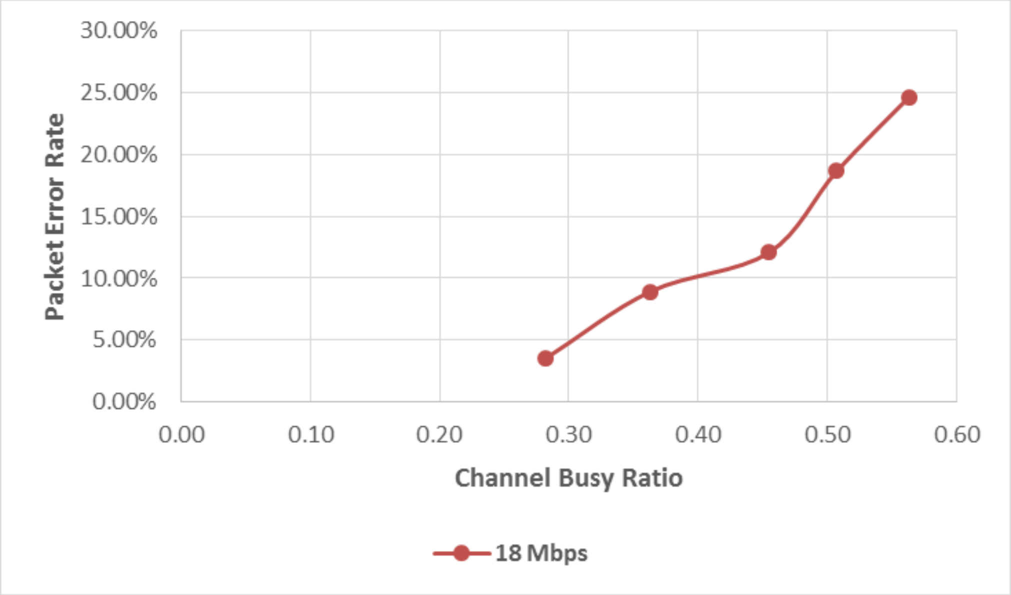


In order to determine the effect of data rate on CBR and PER values, the team switched the data rate to 18 Mbps and repeated the steps above, and the observed results were as follows:

Table 31: CBR and PER at Various Congestion Levels – 18 Mbps

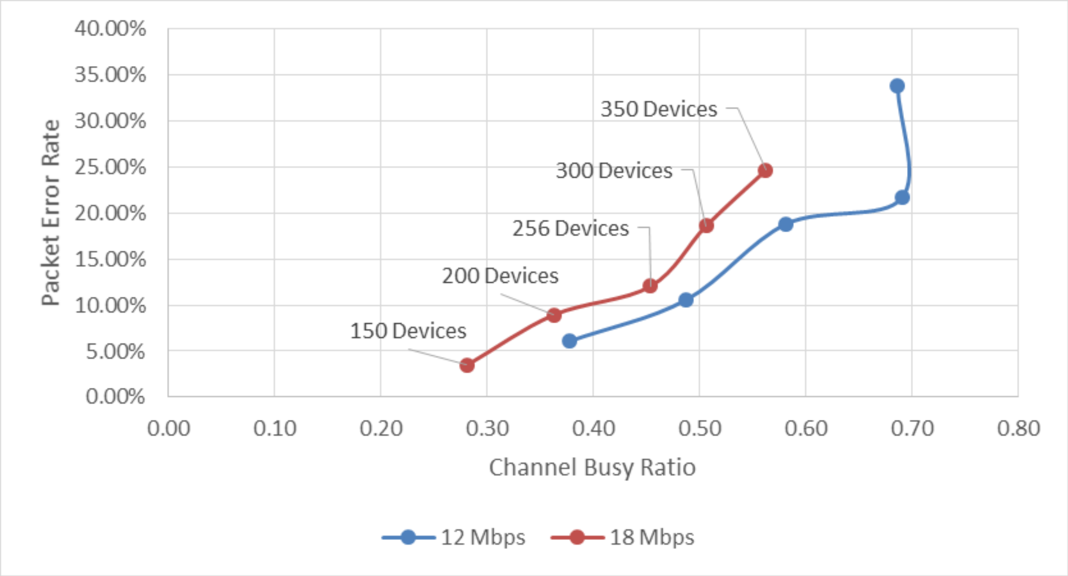
Number of Devices	CBR at 18 Mbps	PER at 18 Mbps
150	28.14%	3.47%
200	36.30%	8.94%
256	45.45%	12.07%
300	50.69%	18.66%
350	56.30%	24.68%

Figure 86: Congested Simulation – Packet Error Rate vs. Channel Busy Ratio, 18 Mbps (Source: USDOT)



The figure below compares the two scenarios and demonstrates how changing the data rate improves the situation:

Figure 87: Packet Error Rate vs. Channel Busy Ratio, 12 Mbps vs. 18 Mbps (Source: USDOT)



As is expected, increasing the number of devices within a fixed communication range, increases the CBR which results in increased PER. However, switching to the 18 Mbps data rate, greatly improves the packet delivery. Switching the data rate from 12 to 18 Mbps resulted in a PER drop of ~3 – 9% depending on the level of congestion.

At around 50% CBR in the 12 Mbps data rate situation, the PER is around 10% which is the accepted threshold. Once switched to 18 Mbps data rate, the CBR improves (36% vs 50%) and the PER improves as well (8% vs. 10%).

On the other hand, it appears that when transmitting at 18 Mbps and at around CBR value of 30%, it is safe to switch back to 12 Mbps data rate, as the PER would fall well below the 10% threshold.

The findings conclude that if the 20 MHz channel is used for DSRC communications, the OBE should transmit BSMs at a data rate of 12 Mbps when the CBR is below 50% (~210 vehicles and ~11% PER in a 300 m radius) and transmit BSMs at a data rate of 18 Mbps when the CBR exceeds 50%; such transmission shall continue until the CBR falls below 30% (~160 vehicles and ~5% PER).

7 Additional Considerations and Future Research Areas

This section provides information on any additional considerations for rulemaking and potential areas for future research.

Outstanding Technical Challenges for Deployment

This subsection describes outstanding technical issues that need resolution. Ideally, these technical issues would be resolved before finalizing requirements, but given the NHTSA rule-making timeline, it may not be possible for complete solutions to be included in the first rule. Appending additional requirements based on development of technical solutions may be a   consideration.

7.1.1 Stable Misbehavior Detection Solution (Local and Global)

A number of requirements rely on a stable security solution, including a complete misbehavior detection strategy, plausibility strategies, reporting requirements, etc. This is especially true for the suggested minimum storage requirements for misbehavior reports and certificates but could also impact CRL size and processing of certificate revocation status in certificate validation. Future strategies may also impact the suggested requirements related to plausibility. As shown in the full requirements list, these requirements are based on assumptions or previous analysis on misbehavior, what constitutes a plausible message, and the needs of the overall security system and storage. These strategies will likely be left to the future SCMS Manager and CMEs to decide and implement through industry policies and additional agreed-upon standards among these organizations and manufacturers of the necessary V2X communications system and SCMS equipment. Until there is a complete security solution including set misbehavior detection strategies and processes, recommended requirements and OBE design will continue to be based on assumptions and existing analysis released by NHTSA and its researchers such as CAMP and Booz Allen.

Further research should be conducted on CRL distribution strategies, attack vectors (such as GPS), and attack scalability. The outcomes of this research could greatly affect any misbehavior detection strategies by enabling more efficient CRL distribution and prioritizing the evaluation of more vulnerable vectors and attacks with higher consequences. Note that the comprehensive processing time and memory requirements associated with any plausibility and local misbehavior detection solutions should be tested for feasibility. While the team has determined that the recommended Level 1 Plausibility Check does not require significant processing time or memory, it was not tested in conjunction with parsing of the message, other plausibility checks, certificate verification, etc.

7.1.2 Certificate Change and Distribution Strategies

While this report and Appendix F. Full DSRC OBE Security Inputs Analysis specify security objectives and functional requirements for the distribution and use of certificates, the team purposely did not specify how the OBE should switch between pseudonym certificates during the life of those certificates or specify a prohibition on the use of peer-to-peer sharing for certificate distribution. There are countless possible pseudonym certificate change strategies (i.e., how the OBE switches certificates over the course of a day, week, etc.) that could be implemented to maximize efficient use of certificates while still maintaining privacy and security. Peer-to-peer distribution of certificates could also be a more efficient distribution strategy than requesting certificates through connecting to the SCMS via RSE and LOP. In many cases, this will be the decision of the OEM as long as selected practices adhere to the established requirements and any industry best practices or policies. However, for both considerations, further testing is required to determine feasibility of various strategies and to ensure options fulfill the ultimate objectives and requirements to maintain privacy and security. How the overarching SCMS policies and practices are developed and overseen is still an area to be investigated and decided upon, but it is expected that body would set such policies or industry-wide practices and standards to supplement any mandates or established requirements.

7.1.3 Request and Response Transactions

As the team states in the recommended requirements list, request and response transactions between the OBE and remote system management servers (i.e., SCMS via the LOP and software update servers) shall support service interruptions such that the transaction can be continued during a subsequent connectivity event (e.g., RSE encounter). This requirement is designed to mitigate the inevitable loss of connection during some interactions between the OBE and a remote system management server such as the SCMS. The OBE and remote system management servers must be able to stop and re-start transactions where paused, in order to not have to restart downloads of certificates, software, etc. The implementation of this requirement could take many different designs which could be decided through consensus among the SCMS Manager, CMEs, and OEMs. The team recommends a session-less transaction, but the state needs to be maintained by the server (how many increments are contained with the package) and the client/OBE (how many increments of this package have already been downloaded).

7.1.4 Congestion Mitigation Strategy

The existing congestion control strategies and algorithms as seen in the recent CAMP reports seem to address congestion issues but add another layer of complexity to DSRC message monitoring and transmission. These algorithms effectively reduce the loss of messages due to congestion by simply sending fewer messages, which effectively has the same net result: the applications must operate effectively with fewer messages per second (lost either to congestion or because the algorithm slowed down the message transmission rate). It is not clear if the impact of fewer messages (i.e., less frequent BSMs) on application performance has been studied. In addition, some of the congestion control algorithms include reducing the transmission power level. While reduced power will reduce the number of vehicles in range, and thereby will reduce congestion, this approach begs the question that if the applications are not impacted by reduced range, then the range should be reduced at the outset as opposed to dynamically reduced based on congestion. The number of vehicles in the region should not impact the range requirement for a given application. There may be many situations where there are many vehicles in the region, and a specific application still requires its design range. If this design range is lower than the capability of available receivers, then the range of the receivers should be reduced at the outset to avoid congestion, not adjusted dynamically.

The team believes the problematic effects of hidden nodes and congestion can be initially mitigated through the simpler use of higher data rates, and randomization (or spreading) of BSM transmissions across the 100 msec BSM repeat interval. The team also identified that use of a 20 MHz bandwidth channel (Channel 173 or 183 instead of channel 172) can allow the use of substantially higher data rates (12 Mbps and 18 Mbps) without any significant reduction in range in an open environment (more testing is needed to validate the performance of 20 MHz channels in an urban environment, but similar range performance is expected)[13]. These higher data rates, especially 12 Mbps and 18 Mbps, substantially reduce the time any message is in the channel, and thereby support significantly larger numbers of vehicles. The estimates indicate that with roughly three times the throughput, an 18 Mbps data rate operating in a 20 MHz channel with conventional vehicle densities is unlikely to exhibit any significant level of congestion from BSM transmissions.

As seen in the requirements list, the team believes the use of a 9 Mbps data rate in the 10 MHz channel (or possibly a 12 or 18 Mbps data rate in a 20 MHz channel) will greatly reduce PER in most congestion and hidden terminal scenarios while still maintaining more than adequate transmission range and RSS (in non-obstructed environments). An adjustment in data rate would most likely be a simpler solution compared to the complex algorithms X and Y while still maintaining the recommended 10 Hz message rate. As seen in the data collection testing and simulation results, this change in data rate along with the recommended requirement for the timing of the transmission based on a random offset from PPS will reduce PER to less than 10% in most situations involving congestion and hidden nodes. However, a congestion control algorithm may be necessary to mitigate effects in extreme congestion situations when using the 10 MHz channel.

The use of the 20 MHz channel may also help solve the problem of spectrum sharing (discussed in the next subsection).

DSRC Spectrum Sharing

DSRC spectrum sharing has increasingly become a topic of discussion with the reintroduction of the Wi-Fi Innovation Act which seeks to find ways for V2V communications and additional Wi-Fi spectrum to coexist. There are major supporters on both sides of the debate. At a minimum, V2V communications and the DSRC spectrum must be able to support safety related communications. As discussed in the data collection testing chapter and previous subsection, the use of a 20 MHz channel with a data rate of 12 or 18 Mbps for V2V safety communications instead of a 10 MHz channel at 6 or 9 Mbps could help mitigate congestion and hidden node effects. The switch to a 20 MHz channel could also potentially alleviate some of the issues in the DSRC spectrum sharing debate since the 20 MHz bandwidth channel is consistent with the channels in the proposed sharing arrangements. This means that it is much easier for potentially interfering terminals to sense the presence of vehicles using the channel, and thereby act to reduce interference. Without this, the IEEE 802.11 ac devices will require some sort of modification to allow them to differentiate between radio energy in Channel 172, and energy in the same 20 MHz band, but in an adjacent 10 MHz band. The team wants to stress that this is only a very preliminary possibility and more research and testing would need to be conducted in this area to ensure that additional Wi-Fi spectrum does not limit the effectiveness of DSRC safety related communications.

[13] As discussed in Section 4.3.11, Information the Opnet Simulation with Field Test Data, additional field testing should be conducted in a 10 and 20 MHz channel across the 6, 9, 12, and 18 Mbps data rates in different environments (e.g., rural, suburban, urban) out to 1000 meters to develop a true propagation model that can be used to reliably simulate DSRC communications in various scenarios. The Opnet model is ready to incorporate the required data when available.

Technological Flexibility

This subsection discusses the need for requirements to be flexible enough to embrace technological changes and advances. Requirements and associated certification tests must have an amendment process to incorporate updates and technological changes.

V2V communications technology will continue to evolve in coming years with inevitable new advancements in hardware and software to increase communications performance and available safety applications. Like other standards and requirements, any NHTSA mandate for V2V communication should be flexible enough to allow for these technological advancements and innovation. There is an important balance between creating requirements that ensure interoperability and performance but do not constrain the OEMs or other developers through innovation-limiting requirements and specifications. If the requirements do not leave space for different implementation methods, the rule will stifle innovation and competition from developing better products that increase safety for the consumer. Precisely for these reasons, the team has recommended requirements that are not overly prescriptive. The team recommends NHTSA take a similar approach when developing any future FMVSS or other approach as described in Section 7.12 to create V2V communication. V2V technology is advancing at such a rapid rate that NHTSA should be prepared for possible amendments that may be necessary to maintain its original intent and try to ensure the amendment process is not overly burdensome.

The need for technological flexibility is one of the reasons why the team is recommending requirements for the full existing standards related to DSRC operations (i.e., IEEE 802.11, IEEE 1609 suite, SAE J2735) with the exceptions of specific irrelevant sections and clauses of those referenced standards. These standards are foundational and are required for the OBE to operate in the DSRC environment. However, restating each requirement within these standards would be redundant and not allow for changes as these standards will be continually updated and rearranged. A good example of these frequent revisions are the recent new versions of SAE J2735 and the IEEE 1609 suite. Requirements specifying adherence to these existing standards should still allow room for modification.

SCMS Standup and Governance

Booz Allen has been part of the development of the SCMS for V2V and V2I safety applications and understands the technical design in-depth, along with the policy needs and implications. While CAMP is currently designing the SCMS prototype, there are still undecided decisions on policy and organizational governance models for the SCMS as a whole. More research should be conducted to determine the SCMS Manager purpose, strategy, and operations, government involvement, recommended internal organization structure, and funding models. Additional focused research on the SCMS Manager will give industry and USDOT the options and considerations necessary to start developing the policies and organizational structures required for effective SCMS management, ensuring security, interoperability, and deployment of industry processes, policies, and guidelines.

Hardware, Software, and Operating System Security

The team specifies high-level hardware, software, and OS objectives and security functional requirements based on the analysis of threats and the security levels necessary to mitigate those threats. The team understands the OEMs' sensitivity to cost and recommend further research on the costs and benefits of the levels of hardware, software, and OS be conducted to select the appropriate security levels and policies that meet the necessary protection at the best value. However, as mentioned throughout the report, these requirements and standards will not remain static. Hardware, software, and OS security requirements should be based on current guidance and best practices, which will evolve as attacks and solutions evolve. Appendix I. Overview of Cybersecurity Guidance and Best Practice Management in Other Industries, provides an overview of cybersecurity guidance and best practice management in other industries.

Cryptographic Agility

Cryptographic algorithms are never considered “absolutely” secure. They are intended to be good enough to work for some period of time and are always subject to an unanticipated break which will shorten that expected life. In a system with potentially long lived participants (such as integrated vehicles), the need to change algorithms or the algorithm parameters will likely arise. While the current choices of algorithms and key sizes are considered good enough for the foreseeable future, it is possible that one or more of the relied upon cryptographic algorithms will be broken by a cryptanalytic attack. If the components do not have built in flexibility (e.g., the ability to reprogram the algorithm or change key size or other parameters), the overall security of the system will be degraded by the need for backwards compatibility with early generation systems.

The current cryptographic algorithms to be used are referred to as “elliptic curve cryptography” (ECC). This is not a single cryptographic method. ECC has several variants, and even within those variants, the implementers can choose different curves. NIST specifies a set of curves to be used by the US Government. Europe has chosen different ones. It is not clear if either set is inherently better than the other but, unless the OBEs all implement the same set of curves, systems built to one or the other set cannot interoperate cryptographically. And, it is possible that one or more of the currently specified curves will be determined to have a specific vulnerability. As with algorithms, it would be necessary to be able to shift curves to maintain a reasonable level of security.

There is a significant risk to the system from the potential future development of quantum computers. Quantum computers will eventually enable breaking the cryptographic algorithms currently used to protect the integrity, authenticity, and (where necessary) confidentiality of all data exchanged within the system, including the BSMs themselves. The team recommends that devices are designed in such a way that they can migrate cryptographic algorithms without needing to be physically replaced and have the flexibility to add/remove Root CA certificates. This implies that hardware security modules should be provided as general purpose processors with a secure execution environment within a tamper-proof casing, rather than implementing cryptographic hardware security with custom circuits.

Intrusion Assessments and Hardening

Most of the security efforts to date have focused on mechanisms to assure the integrity of the security system and to manage the security credentials used to provide that assurance. However, recent high profile “hacks” of vehicles indicate that this approach to security, while beneficial, may not be adequate. To the extent that it may be possible to launch an attack on a vehicle using an otherwise legitimately signed message, the system provides little or no protection. These attacks have been shown to range from nuisances to full scale takeover of vehicle systems. The risk here is not that V2V messages will be forged, or spoofed, but that a seemingly benign message may embed malware in the system that then facilitates a larger scale takeover of the system. A simple example would be to include in a BSM Part 2 A La Carte field, data that effects a buffer overflow code injection into the OBE (similar to the recent Android attack involving a carefully mis-encoded image attachment). If such an attack were successful, it would sidestep the existing security system (or pass through it undetected) and would allow the takeover of the OBE. A more compelling concern is that, if such an attack could be made to propagate from OBE to OBE, the peer to peer nature of vehicle to vehicle communication would cause such an attack to propagate across the entire national vehicle fleet within days. While this sort of attack is arguably difficult to mount, the scalability of the attack and the potential to, for example, disable all DSRC equipped vehicles on the road simultaneously would make such an attack an attractive target for state sponsored terrorism.

The team recommends that a deliberate program be undertaken to explore such attacks on prototype systems so that effective countermeasures can be identified and so that the mechanisms of such attacks can be more fully understood. Relying simply on “industry best practices” does not seem prudent given that there are few known practices to lean upon.

One example of such an effort could be to organize and sponsor a “challenge” project with reference design attack targets, modest funding for qualified attack teams, and substantial cash prizes for well documented successful attacks. The team believes that only through this sort of broad, open approach can the connected vehicle industry really understand and address this threat.

Weather Impacts on Performance

As discussed in existing research, adverse weather can affect the accuracy of GPS receivers and the range of DSRC radio signals. While the team has made an effort to develop requirements that will not be affected by inclement weather, it is inevitable that transmit power and antenna gain envelope performance will be affected in certain conditions. Current (and future) OBEs should still provide enough range to perform adequately in adverse weather conditions and meet the transmit power and antenna gain and sensitivity envelope specified in the requirement list. However, NHTSA should consider that any requirements specifying warning times necessary for drivers to make use of safety warnings may need to take weather related issues into account. While the team has made all efforts to ensure the recommended compliance testing procedures are objective, weather impacts on performance should still be considered during testing. This also ties into the discussion on technological and requirement flexibility, because there may need to be future adjustments to requirements and compliance testing if objective tests cannot be completed due to weather effects.

Vehicle Sensor/BSM Parameter Accuracy

Vehicle sensor accuracy is extremely important in feeding the DSRC device to generate BSMs and determining whether another vehicle is a threat upon receiving a BSM. Vehicle sensors feed information (e.g., speed, yaw rate, position) to the OBE to create and transmit the BSMs. These BSMs are received by other OBEs and processed through safety applications to identify hazards based on the message parameters. As seen in the plausibility and hazard analysis, errors in sensor parameters can create false positives and worse, false negatives when safety applications are processing BSMs to identify hazards. While the team provides preliminary recommendations for certain BSM parameter accuracy, more research and testing should be conducted to determine the minimum sensor accuracy requirements. CAMP seems to be involved in this research based on the content of the V2V-SE Minimum Performance Requirements report and initial development of SAE J2945/1, although the Booz Allen team has not seen the data to justify the suggested requirements.

The team believes the approach to this analysis (simulated collision trajectories with a collision detection algorithm fed with simulated BSM data containing statistically reasonable errors within the specified standard deviations) is sound, and this approach suggests that much tighter tolerances on BSM data are needed in order to assure data sent from vehicles can be used to reliably predict imminent collisions and generate driver warnings or other mitigation actions. However, the team also appreciates that the resulting BSM error tolerances may be challenging to achieve. However, supporting achievable tolerances that are known to produce unreliable collision predictions hardly seems a useful exercise. If the system truly depends on this level of accuracy, then this is what is technically required.

A broader examination of this area should be undertaken. Specifically a set of reference design collision detection algorithms be developed and publicly reviewed for validity. These algorithms can then be used in Monte Carlo simulations to assess the level of BSM accuracy required, and the allocation of these error tolerances across the various BSM data parameters. Since these analyses indicate that significantly higher levels of accuracy are required, additional work on sensor technology and calibration should also be undertaken.

Safety Application Performance Requirements

Developing performance requirements for specific safety applications is out of scope for this project based on the understanding that NHTSA is currently focusing on the transmission of BSMs and not how OBEs should act on those messages (applications). However, this topic is somewhat related to the plausibility and hazard analysis simulations conducted during this effort, which have raised questions for additional research. The plausibility and hazard analysis simulation displayed the likelihood of a correct collision classification (true positive), a missed collision detection (false negative), and a false alarm (false positive) for different vehicle collision (or near miss) scenarios with various levels of position, speed, and time error. While this model was designed more to determine the outer bounds of error allowed for a message to be considered plausible, one can also see the importance of a specific application's performance in identifying hazards. It is assumed that most safety applications would have more sophisticated mechanisms, such as a Kalman filter, to determine hazards in the presence of data errors within BSMs. Nonetheless, there still exists the question of whether OEMs should have to adhere to certain application performance requirements when deploying a safety application. An example requirement would be that an application must provide a 95% reliability of detecting a hazard within the 2.5 second stopping sight distance or a similar requirement. This also ties in with the sensor accuracy discussion above, as sensors will have to provide a certain level of accuracy to meet the specified application reliability requirement. While the team has not focused on application performance during this project, additional research and testing should be conducted to determine whether safety application performance requirements are necessary to ensure the V2V communications system provides the intended safety benefits or if USDOT should let the market determine the optimum performance levels for safety applications.

Compliance Test and Test Facility Development

The vehicle level compliance tests are similar to vehicle crash tests, except that, because collision related messages can be synthesized, the tests do not require creating physical collisions with actual vehicles. However, these tests are likely to require significant development and refinement to assure that they are easily carried out, and to provide a basis for OEMs and third party testers to understand the tests and to design for them.

To support this, it is recommended that NHTSA carry out a test reference design as soon as possible. This effort should include the following elements:

- Specify, design and implement vehicle and roadside test equipment
- Develop example hazard detection application for test vehicle
- Assess and validate test equipment through developmental tests
- Develop detailed test procedures, and validate using test facility
- Perform third party tests using test facility
- Assess test results and effectiveness/stability of tests, and refine procedures and/or equipment as necessary

As discussed in Chapter 5 Developing DSRC OBE Security Requirements and Appendix F. Full DSRC OBE Security Inputs Analysis, the USDOT should consider using established testing labs to collaborate in developing and conducting security testing. These labs are widespread, relied upon by government and industry, and accredited by NIST. Developing a new security testing capability organic to the USDOT would most likely result in higher costs, longer schedules, and less thorough testing because existing labs are already highly skilled and experienced in the field.

Use of Regulations or Other Approaches

The Booz Allen team is making technical suggestions on requirements and recommendations and understands that NHTSA has a wide spectrum of approaches it can choose to use to meet its safety and security objectives. The range of approaches spans from promulgating regulations (prescriptive), to publishing guidance and/or policies, to “safe harbor” approaches, to recommended or best practices, to deference to industry practices (not at all prescriptive from NHTSA’s point of view), among others. NHTSA has the ability to use a combination of different approaches described below for different elements of the overall set of requirements it wishes to release.

In this subsection, the term non-public organizations (NPOs) includes the entire range of non-public entities that could be involved in the NHTSA chosen connected vehicle approach. NPOs could range from commercial companies like OEMs, tier 1 and subcomponent suppliers, as well as software and hardware developers, or private cyber security companies; to various contractors or consultants; to not-for-profit entities like trade organizations, universities and public consortia; and various others that have a role to play in the ultimate connected vehicle system.

Spectrum of Approaches- From Most Prescriptive to Least Prescriptive

- **Most Prescriptive**
    - **Design Standards.** The most prescriptive approach would be for NHTSA to issue design regulations through the formal notice and comment process that would specify the detailed requirements that non-public organizations (NPOs) would have to meet or be subject to regulatory sanctions. Design regulations are most appropriate when a single, interoperable and uniform approach is needed to achieve safety or security objectives. It has the benefit of certainty and the weakness of not allowing alternative approaches or improvements from the NPOs without revising the federal design standards. While the Booz Allen team thinks it is unlikely that NHTSA will want to use this approach, it is included here to define the ends of the spectrum of alternatives.

    - **Performance Standards.** A less prescriptive regulatory approach is to use performance standards developed through notice and comment rulemaking.

Performance standards specify outcomes and give greater flexibility to NPOs to develop the means to meet the required performance objectives. Performance standards are most appropriate where uniformity and certainty is necessary at certain points in the approach, but NHTSA wishes to allow NPOs freedom and flexibility to implement their own approaches within the “black box” that is below the specificity described by the performance standard.

- **Less Prescriptive**
    - **Adoption of Governmental Standards.** This approach uses standards that have been developed by other United States or foreign agencies and applies them to NPOs in the connected vehicle approach chosen. This is less prescriptive for NHTSA, but not for the regulated NPOs, since it assumes that the NPOs would not be subject to these standards “but for” NHTSA’s regulatory action. Of course, if the NPOs are already subject to these standards, no NHTSA regulatory action at all is required for this element.

    - **Adoption of Industry/Association Standards.** A less prescriptive approach is for NHTSA to adopt standards that have been developed by industries or associations, ideally through formal standard-setting mechanisms. This has the advantage of providing greater uniformity, certainty, and interoperability while keeping NHTSA out of the myriad of technical issues that often come into play in consensus standard setting. If NHTSA uses this approach it can specify a particular consensus standard and version to ensure uniform adoption or and later amend the version specified to accommodate improvements.

    - **Certification Process.** A less prescriptive approach is for NHTSA to require a certification process for hardware and software used in the connected vehicle approach chosen. This is often used in conjunction with performance standards where there is a risk that the performance standard could be met but in a way that did not achieve NHTSA’s safety and security objectives. NHTSA could require self-certification by OEMs. However, in light of recent concerns about some auto manufacturers’ adherence to existing regulations, additional oversight mechanisms may be considered. Often certified labs are used to conduct the certification to ensure an independent certification process. If there is a risk that the certified labs could certify hardware or software that did not meet NHTSA’s safety and security objectives, NHTSA could chose to set standards and requirements for those labs or have them meet standards established by other government agencies, industries or organizations (see above).

- **Much Less Prescriptive**
    - **Star Rating.** Another “regulatory” approach is not to use requirements and sanctions at all, but instead encourage safety and security choices by NPOs by using a star rating system. The star system, developed through public notice and comment, would identify outcomes desired by NHTSA and would award stars to NPOs (most likely OEMs) according to their ability to meet and exceed those outcomes. While NPOs are not required to achieve 5 Stars, NHTSA has successfully used its 5 Star Safety ratings to promote industry advancements because NPOs design and build cars to achieve higher safety ratings for better customer acceptance and higher market share.

    - **Recommended Practices.** This approach could also be called “Policy Guidance,” “Best Practices,” or “Safe Harbor” frameworks. In it, NHTSA describes the results of its research and analysis on safety and security practices of the NPOs that NHTSA believes are most helpful to the approach chosen by NHTSA for connected vehicles. Unlike the Star Rating which is designed to be simple so consumers can use it, this approach can include more detailed guidance that NPOs can choose to follow or not. The NPOs may not be motivated solely by the logic of NHTSA's guidance. However, an OEM could be incrementally motivated by the OEM's concerns that failure to follow the NHTSA recommended practices will increase its litigation liability exposure in crashes that could have been avoided if the recommended practices had been followed.

  - **Grants.** An approach that is contractual rather than regulatory is for NHTSA to use its grant making authority to promote safety and security options that enhance the adoption of the NHTSA's chosen connected vehicle approach. These grants can take the form of field operational tests, model deployments, standard setting activities, or funding enabling technologies, among others. NHTSA has already used this grant approach to get to this point with the Michigan Test Bed and the CAMP initiative. The issue for the future is the degree to which the right parties can be involved in ways that will improve the actual driver safety and security experience in a measurable way. One way NHTSA can do this is to include performance requirements in its connected vehicle grants that relate to actual connected vehicle implementation.

- **Least Prescriptive**
  - **Encourage State Action.** NHTSA could issue a report of its findings and conclusions and decide that Federal action was not required for some elements of the connected vehicle system. At that point, it could encourage states to act to fill the void and wait to see if any of those state actions bore fruit that was worth being adopted at the national level for those elements. Of course, the problem with this approach is that the OEMs and the drivers would be facing different, and perhaps incompatible, approaches for those elements for their vehicles that moved across state.

  - **Laissez-faire**. NHTSA could decide that the connected vehicle initiative, or elements of it, did not require NHTSA direct or indirect involvement at this time. This would mean that NHTSA believes that the best approach is to allow the NPOs or foreign entities to promote connected vehicles and NHTSA leadership is not required for those elements. While the Booz Allen team thinks it is unlikely that NHTSA will want to use this approach for the entire connected vehicle system, it is included here to define the ends of the spectrum of alternatives and for possible use for some elements of the connected vehicle system.

8 Appendix A. Acronyms

Acronym	Definition
AA	Assurance Activities
AASHTO	American Association of State Highway and Transportation Officials
AC	Acceleration (Lateral)
ACM	Association for Computing Machinery
AES-CCM	Advanced Encryption Standard – Counter with Cipher Block Chaining Message Authentication Code
ANPRM	Advanced Notice of Proposed Rulemaking
ARINC	Aeronautical Radio, Inc.
ASD	After-market Safety Device
ASIC	Application-Specific Integrated Circuit
ASTM	American Society for Testing and Materials
BAH	Booz Allen Hamilton
BLOB	Binary Large Object
BP	Best Practice
BSM	Basic Safety Message
BSS	Basic Service Set
C2C-CC	Car-to-Car Communications Consortium
CA	Certificate Authority
CAMP	Crash Avoidance Metrics Partnership
CBR	Channel Busy Ratio
CC	Common Criteria
CC PP	Common Criteria Protection Profile
CCEVS	Common Criteria Evaluation & Validation Scheme
CCH	Control Channel

Acronym	Definition
CCTL	Common Criteria Testing Laboratory
CDDS	Communications Data Delivery System
CFR	Code of Federal Regulations
CME	Certificate Management Entity
CPU	Central Processing Unit (i.e., computer)
CRL	Certificate Revocation List
CSMA	Carrier Sense Multiple Access
CV	Connected Vehicle
CW	Continuous Wave (or Continuous Waveform)
DC	Direct Current
DOS	Denial of Service
DOT	Department of Transportation
DSRC	Dedicated Short Range Communications
EAL	Evaluation Assurance Level
ECA	Enrollment Certificate Authority
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
EDCA	Enhanced Distributed Channel Access
EDR	Electronic Data Recorder
EIRP	Equivalent Isotropic Radiated Power
ESD	Entering Sight Distance
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
FHWA	Federal Highway Administration
FIPS	Federal Information Processing Standard
FMVSS	Federal Motor Vehicle Safety Standard

Acronym	Definition
FN	False Negative
FP	False Positive
FTC	Federal Trade Commission
GAO	Government Accountability Office
GM	General Motors
GMBD	Global Misbehavior Detection
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HP	High Performance
HR	House of Representatives
HSM	Hardware Security Module
HV	Host Vehicle
I2V	Infrastructure-to-Vehicle
ID	Identification
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IMU	Inertial Measurement Unit
IP	Internet Protocol
IPG	Inter-Packet Gap
IPv6	Internet Protocol version 6
ISD	Integrated Safety Device
ISO	International Organization for Standardization
IT	Information Technology
ITS	Intelligent Transportation Systems
ITU-T	International Telecommunication Union – Telecommunication Standardization Sector
JPO	Joint Program Office

Acronym	Definition
LA	Linkage Authority
LAN	Local Area Network
LMBD	Local Misbehavior Detection
LOP	Location Obscurer Proxy
MA	Misbehavior Authority
MAC	Media Access Control
MB	Megabyte
MBA	Misbehavior Authority
MBR	Misbehavior Report
MIB	Management Information Base
MPR	Minimum Performance Requirement
NHTSA	National Highway Traffic Safety Administration
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NPRM	Notice of Proposed Rulemaking
NVLAP	National Voluntary Laboratory Accreditation Program
OBE	On-board Equipment
OE	Operating Environment
OEM	Original Equipment Manufacturer
OFDM	Orthogonal Frequency-Division Multiplexing
OID	Object Identifier
OS	Operating System
OSI	Open System Interconnect
OTA	Over-the-Air
OUI	Organizationally Unique Identifier
PCA	Pseudonym Certificate Authority

Acronym	Definition
PCAP	Packet Capture
PCR	Pseudonym Certificate Request
PDR	Packet Delivery Rate
PER	Packet Error Rate
PHY	Physical Layer
PICS	Protocol Implementation Conformance Statement
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
POC	Proof of Concept
PP	Protection Profile
PPS	Pulse per Second
PSID	Provider Service Identifier
QAM	Quadrature Amplitude Modulation
QPL	Qualified Product List
QPSK	Quadrature Phase Shift Keying
RA	Registration Authority
RCA	Root Certificate Authority
RF	Radio Frequency
RITA	Research and Innovative Technology Administration
RMF	Risk Management Framework
RSE	Roadside Equipment
RSS	Received Signal Strength
RSU	Roadside Unit
RTK	Real Time Kinematic
S/R	Send/Receive
SA	Spectrum Analyzer

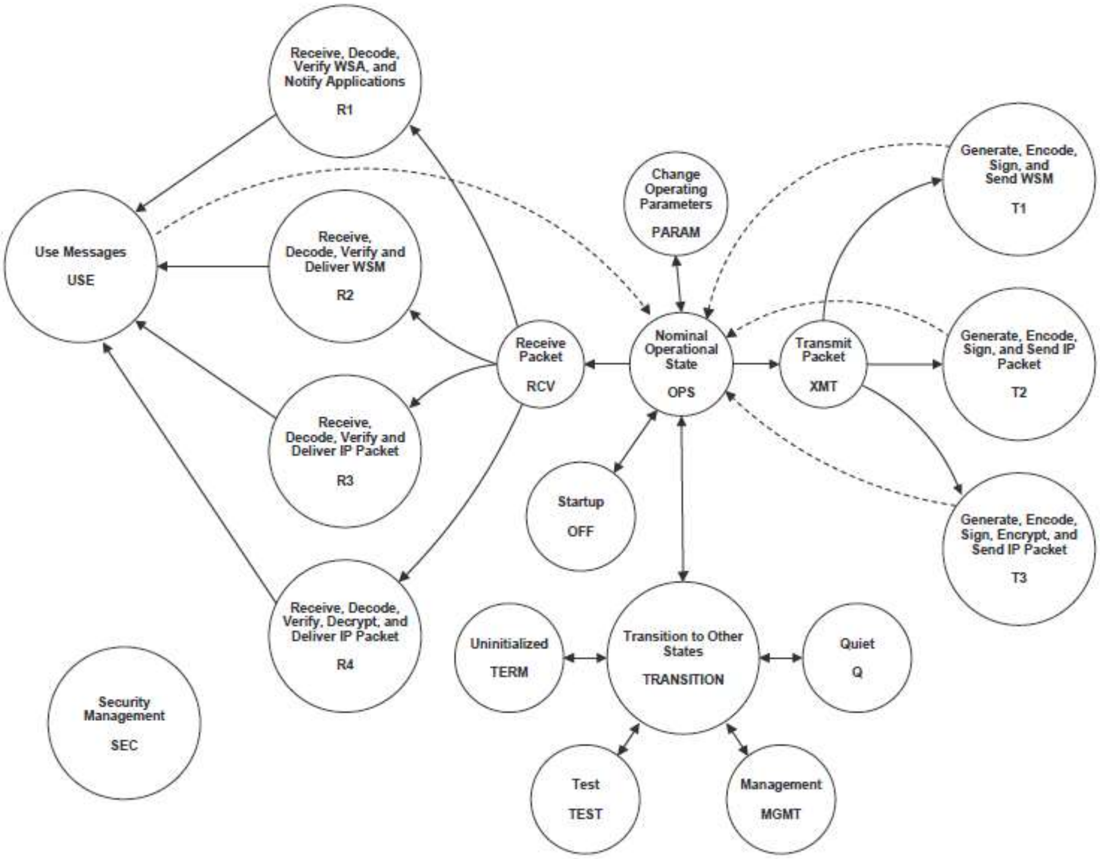
Acronym	Definition
SAE	Society of Automotive Engineers
SCH	Service Channel
SCMS	Security Credential Management System
SCP	Security Copy Protocol
SE	Systems Engineering
SHA	Secure Hash Algorithm
SNR	Signal-to-Noise Ratio
SP	Safety Pilot
SPMD	Safety Pilot Model Deployment
SPY	Security and Privacy In Your Car (Act)
SSD	Stopping Sight Distance
STD	Standard
STOL	Saxton Transportation Operations Laboratory
TBD	To Be Determined
TBR	To Be Reviewed
TCP	Transmission Control Protocol
TFHRC	Turner Fairbank Highway Research Center
TN	True Negative
TOE	Target of Evaluation
TP	True Positive
TSF	Target of Evaluation Security Functionality (or Functions)
TTC	Time-to-Collision
TVRA	Threat, Vulnerability, and Risk Assessment
UC	Use Case
UDP	User Datagram Protocol
UMTRI	University of Michigan Transportation Research Institute

Acronym	Definition
US	United States
USA	United States of America
USDOT	United States Department of Transportation
UTC	Universal Time Coordinate
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Device
VAD	Vehicle Awareness Device
VIIC	Vehicle Infrastructure Integration Consortium
VIN	Vehicle Identification Number
VSC-A	Vehicle Safety Communications - Applications
VTTSS	Vehicle Technology Test Support System
WAVE	Wireless Access in Vehicular Environments
WSA	WAVE Service Advertisement
WSM	WAVE Short Message
WSMP	WAVE Short Message Protocol

9 Appendix B. DSRC OBE Operational States

This appendix contains an explanation of the DSRC OBE operational states used to ensure all use cases and performance needs were considered in developing performance requirements.

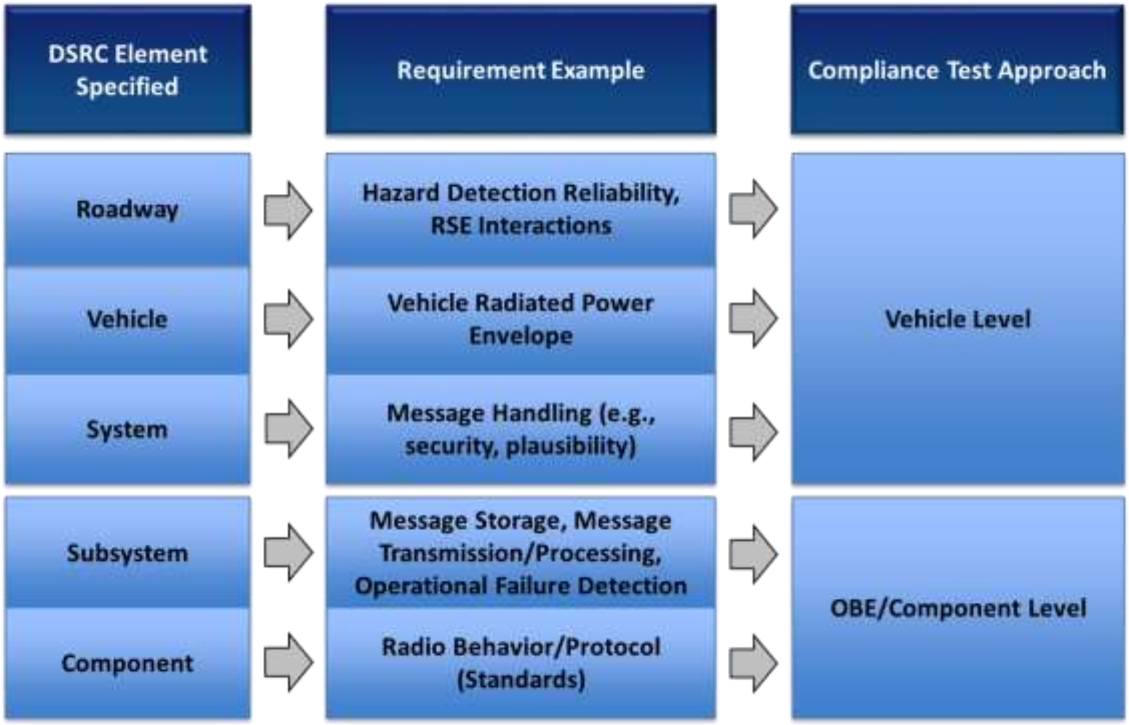
Figure 88: DSRC OBE Operational States (Source: USDOT)


Receive, Decode, Verify WSA, and Notify Applications
R1
Use Messages
USE
Receive, Decode, Verify and Deliver WSM
R2
Receive, Decode, Verify and Deliver IP Packet
R3
Receive, Decode, Verify, Decrypt, and Deliver IP Packet
R4
Security Management
SEC
Receive Packet
RCV
Change Operating Parameters
PARAM
Nominal Operational State
OPS
Startup
OFF
Transmit Packet
XMT
Generate, Encode, Sign, and Send WSM
T1
Generate, Encode, Sign, and Send IP Packet
T2
Generate, Encode, Sign, Encrypt, and Send IP Packet
T3
Uninitialized
TERM
Transition to Other States
TRANSITION
Quiet
Q
Test
TEST
Management
MGMT

10 Appendix C. DSRC OBE Requirements and Verification Hierarchy

This appendix contains an explanation of the DSRC OBE requirements and verification hierarchy used in developing and organizing performance requirements and associated compliance test procedures.

Figure 89: DSRC OBE Requirements and Verification Hierarchy (Source: USDOT)



DSRC Element Specified	Requirement Example	Compliance Test Approach
Roadway	Hazard Detection Reliability, RSE Interactions	Vehicle Level
Vehicle	Vehicle Radiated Power Envelope	
System	Message Handling (e.g., security, plausibility)	
Subsystem	Message Storage, Message Transmission/Processing, Operational Failure Detection	OBE/Component Level
Component	Radio Behavior/Protocol (Standards)	

11 Appendix D. Data Collection Testing and Simulation Analysis

This appendix contains the full data collection test and simulation analysis used to develop findings in support of performance requirement development.

Range vs. Power and Data Rate Testing

All information is found in the main body of the report except for raw data which is available on request.

Time Sync and Stability Testing

For the time sync and clock stability testing, the team used the PPS generated by the GPS module. The initial intent was to use is separately at each unit. Since the PPS can be measured to single digit nanosecond accuracy, the team felt it to be the best source for synchronization. Testing against the Turner-Fairbank VTTSS testbed, with its 100 nanosecond accuracy, would have provided a very accurate measure of each unit's system clock when comparing timestamps. However, the units did not provide any access to their own GPS PPS, and, in one vendor's units, the PPS is not available at the hardware level.

To circumvent this restriction, the team created a UDP socket interface from the Turner-Fairbank testbed. At each PPS, that system sends a timestamp through the interface as a broadcast message. At each unit, receipt of the packets trigger a log entry with both the PPS timestamp and the local unit's system timestamp. No allowances were made for network latency other than placing each unit under test in a dedicated network.

The figures below characterize time sync and stability for six clocks: three from Supplier A and three from Supplier B.

The power density figures show the unit power distribution. It is difficult to compare Supplier A and Supplier B because the spread of the Supplier A units is so large. To make comparisons meaningful, the team has included power density details from the Supplier A units to bring the scale closer to the Supplier B units. The statistics quoted below are better at showing how poorly the Supplier A units perform compared to the Supplier B units.

The deviation figures show the deviation from previous clock values. This shows how much the system clock moves in each second.

The absolute deviation figures show deviations from the timestamp associated with the PPS. These show the clock drift in the Supplier A units. Unit 49 has no absolute deviation because the errors were large enough to make the plot incomprehensible.

Table 32: Supplier A Unit 40 Clock Statistics

Min.	1st Qu.	Median	Mean	3rd Qu.	Max.	Std Deviation
0.6985	0.9998	1.0000	1.0000	1.0000	1.3010	0.009479664

Figure 90: Supplier A Unit 40 Power Density (Source: USDOT)

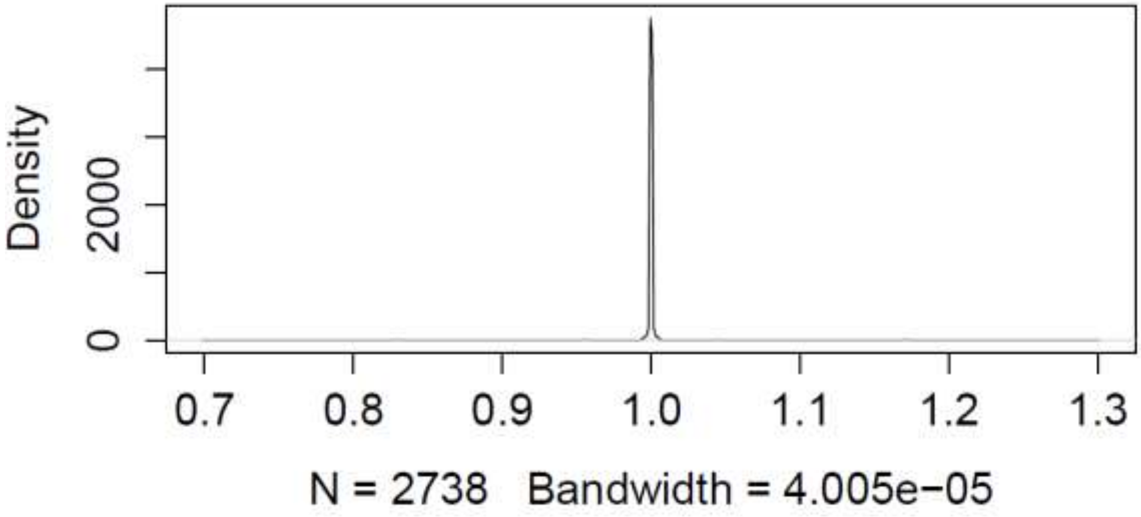


Figure 91: Supplier A Unit 40 Power Density Detail (Source: USDOT)

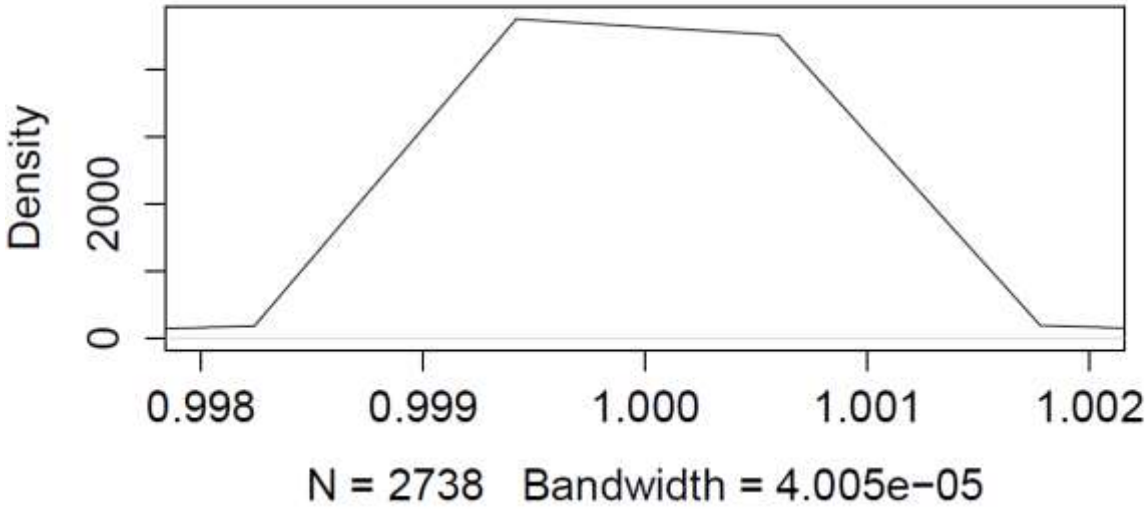


Figure 92: Supplier A Unit 40 Deviation (Source: USDOT)

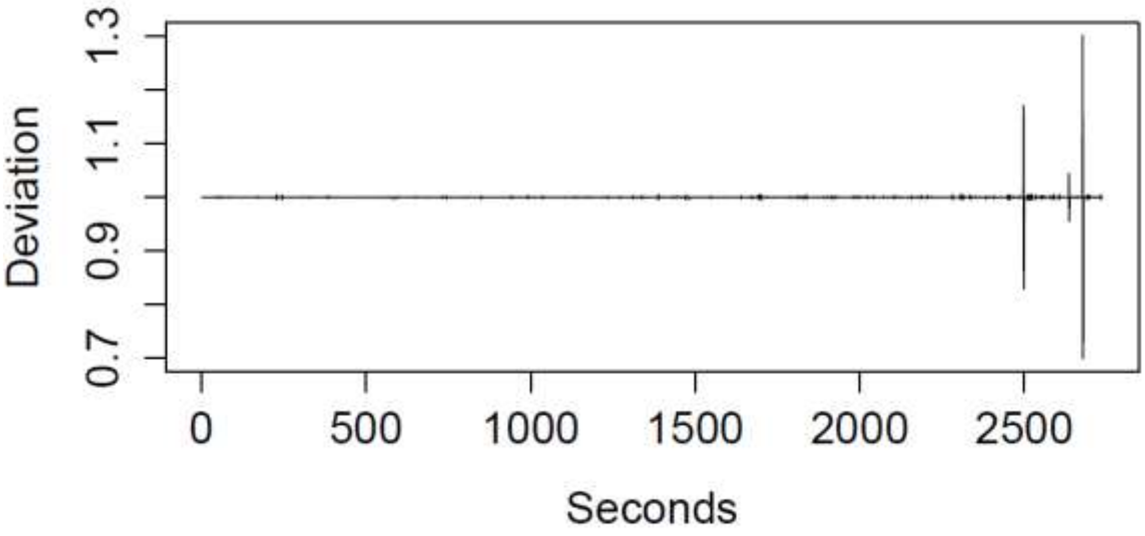


Figure 93: Supplier A Unit 40 Absolute Deviation (Source: USDOT)

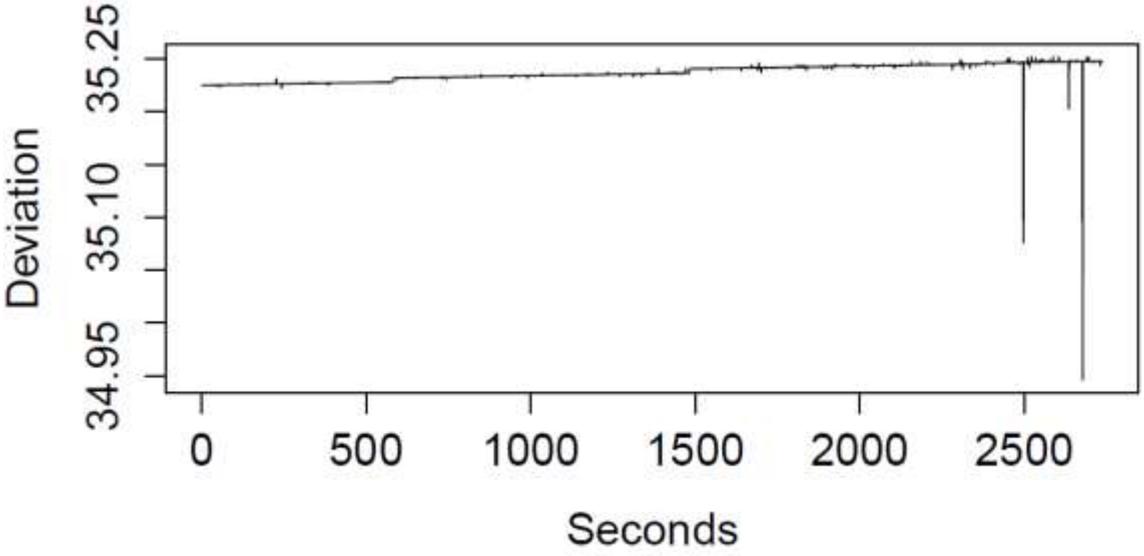


Table 33: Supplier A Unit 42 Clock Statistics

Min.	1st Qu.	Median	Mean	3rd Qu.	Max.	Std Deviation
0.9825	0.9999	1.0000	1.0000	1.0000	1.0170	0.00111771

Figure 94: Supplier A Unit 42 Power Density (Source: USDOT)

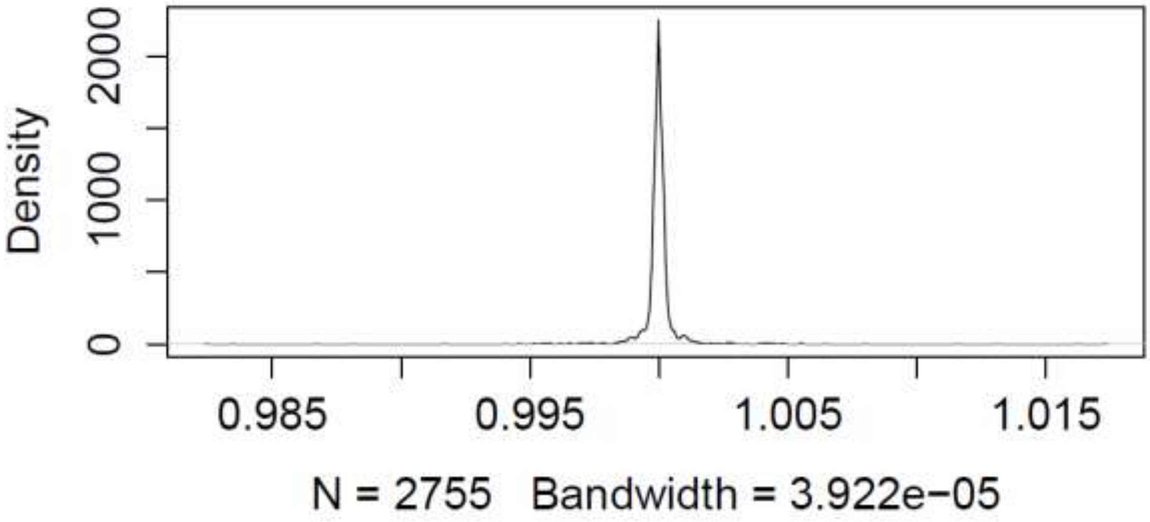


Figure 95: Supplier A Unit 42 Power Density Detail (Source: USDOT)

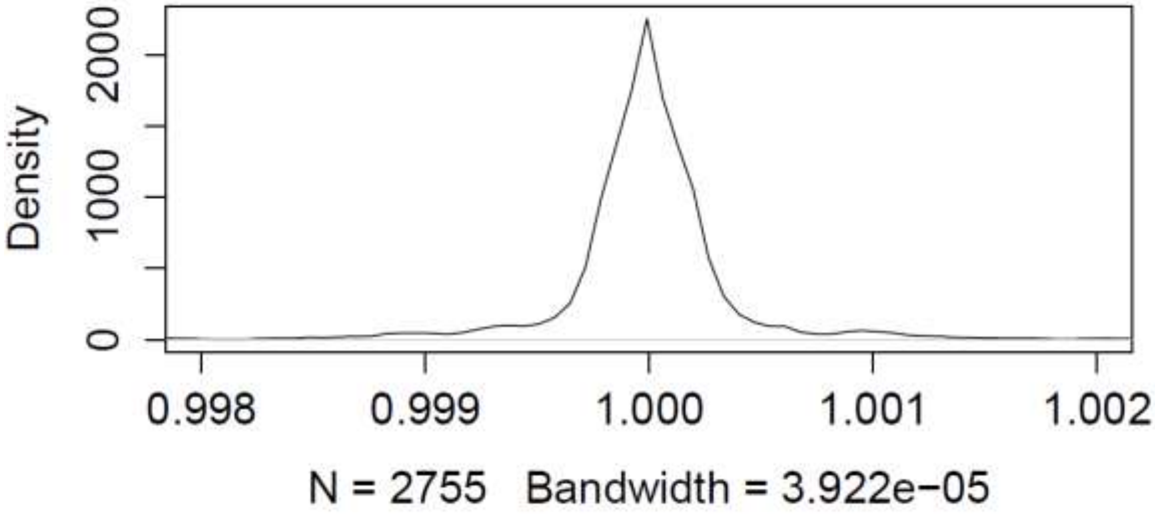


Figure 96: Supplier A Unit 42 Deviation (Source: USDOT)

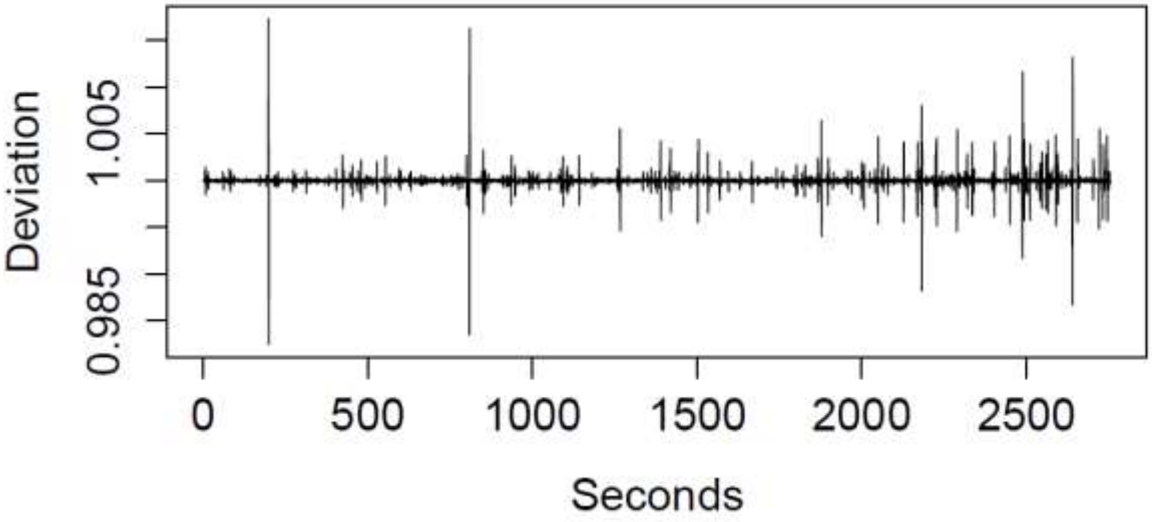


Figure 97: Supplier A Unit 42 Absolute Deviation (Source: USDOT)

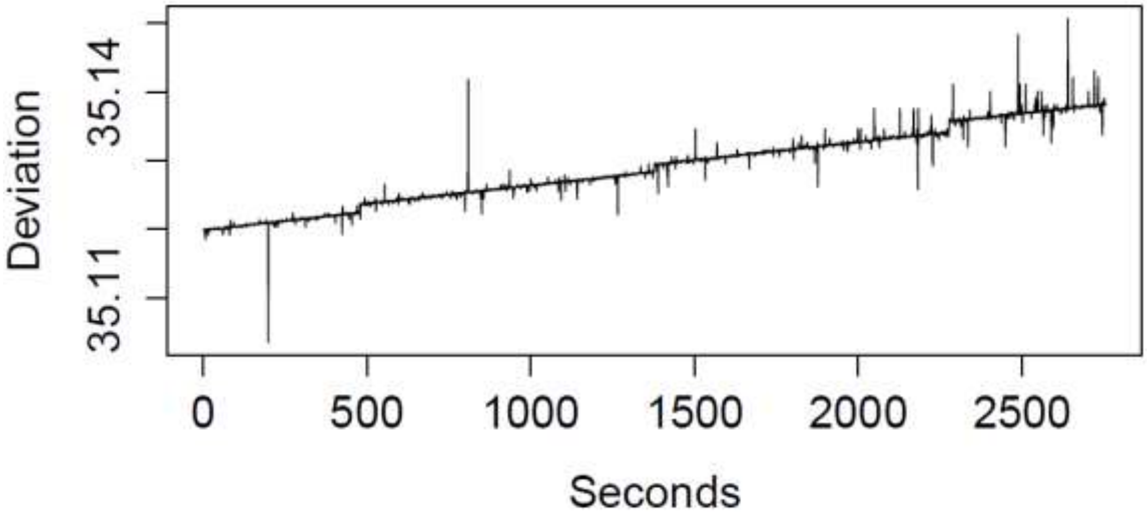


Table 34: Supplier A Unit 49 Clock Statistics

Min.	1st Qu.	Median	Mean	3rd Qu.	Max.	Std Deviation
0.003216	0.9995	1.0000	1.0000	1.0000	2.1680	0.1554563

Figure 98: Supplier A Unit 49 Power Density (Source: USDOT)

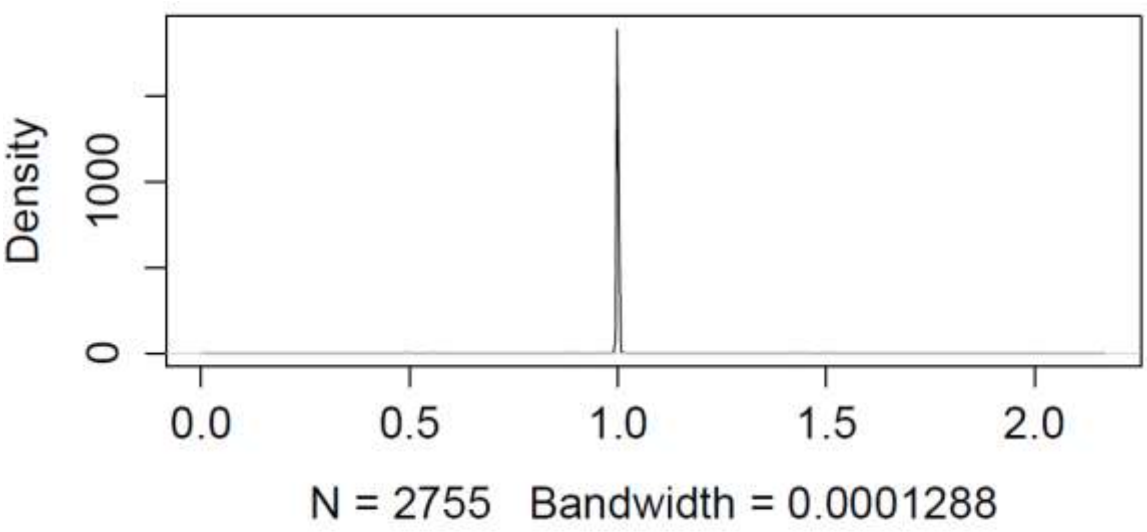


Figure 99: Supplier A Unit 49 Power Density Detail (Source: USDOT)

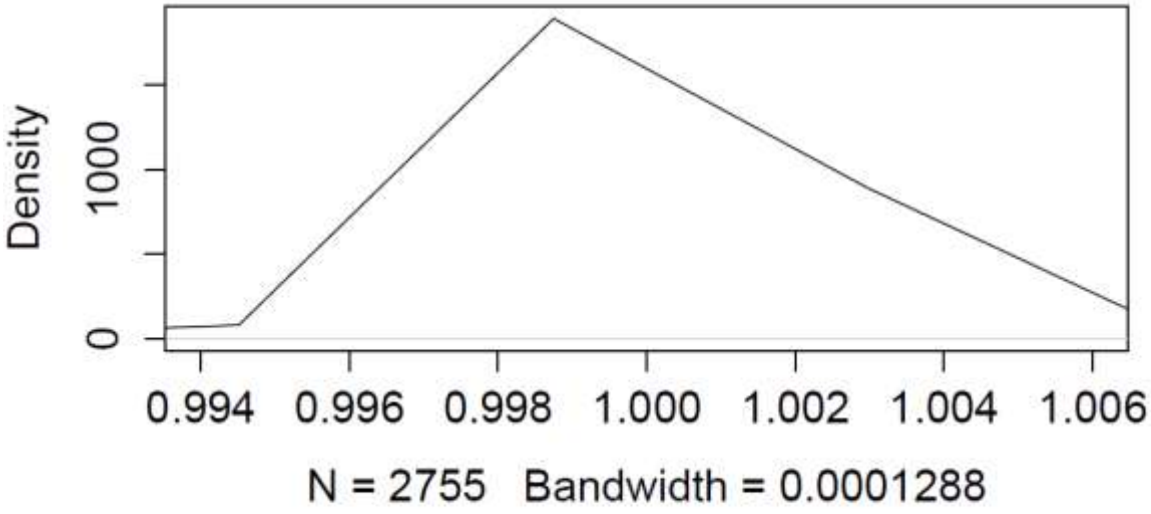


Figure 100: Supplier A Unit 49 Deviation (Source: USDOT)

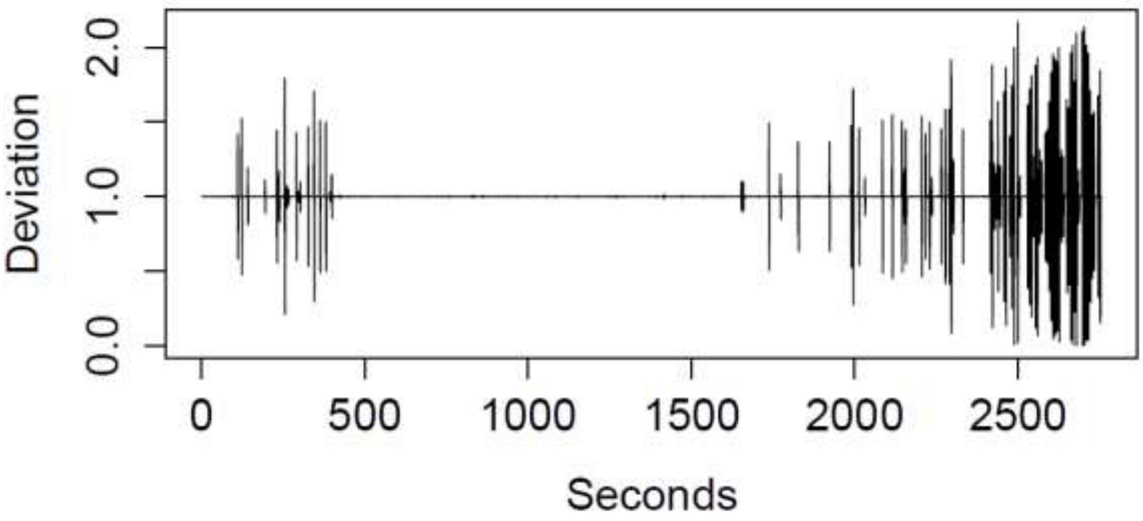


Table 35: Supplier B Unit 29 Clock Statistics

Min.	1st Qu.	Median	Mean	3rd Qu.	Max.	Std Deviation
0.9966	0.9998	1.0000	1.0000	1.0000	1.0040	0.0003554004

Figure 101: Supplier B Unit 29 Power Density (Source: USDOT)

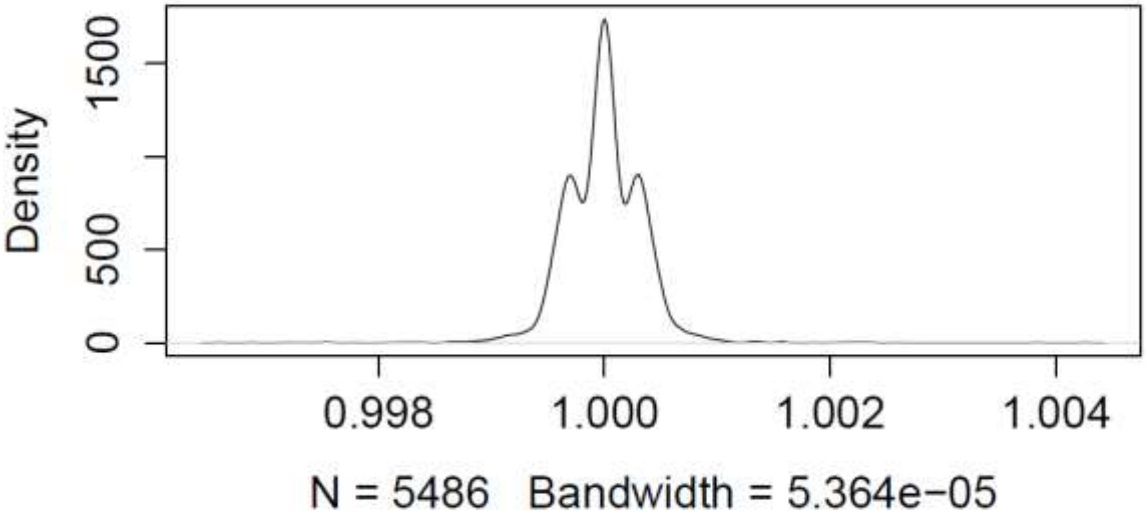


Figure 102: Supplier B Unit 29 Power Density Detail (Source: USDOT)

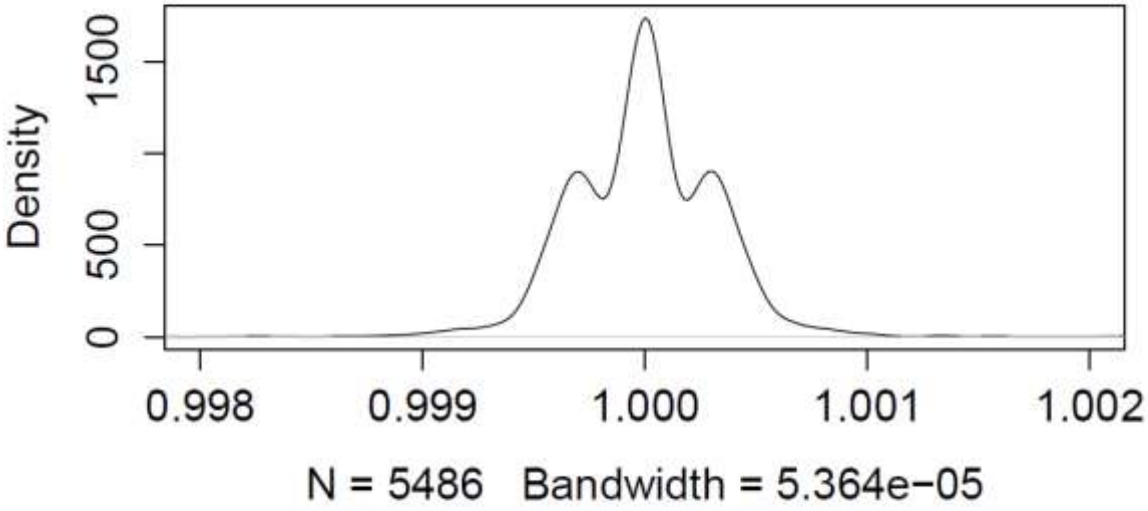


Figure 103: Supplier B Unit 29 Deviation (Source: USDOT)

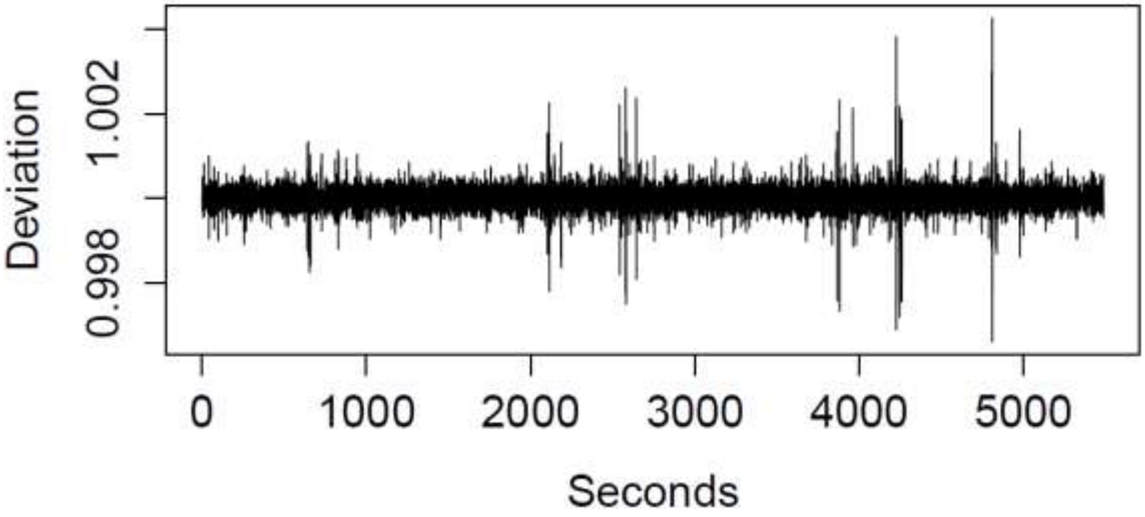


Table 36: Supplier B Unit 30 Clock Statistics

Min.	1st Qu.	Median	Mean	3rd Qu.	Max.	Std Deviation
0.9983	0.9999	1.0000	1.0000	1.0000	1.0020	0.0002064586

Figure 104: Supplier B Unit 30 Power Density (Source: USDOT)

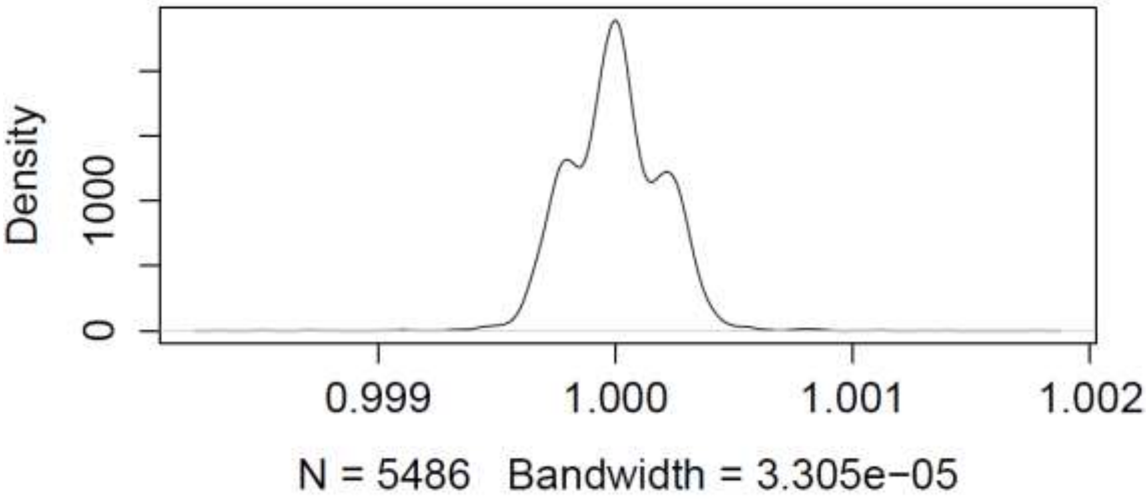


Figure 105: Supplier B Unit 30 Power Density Detail (Source: USDOT)

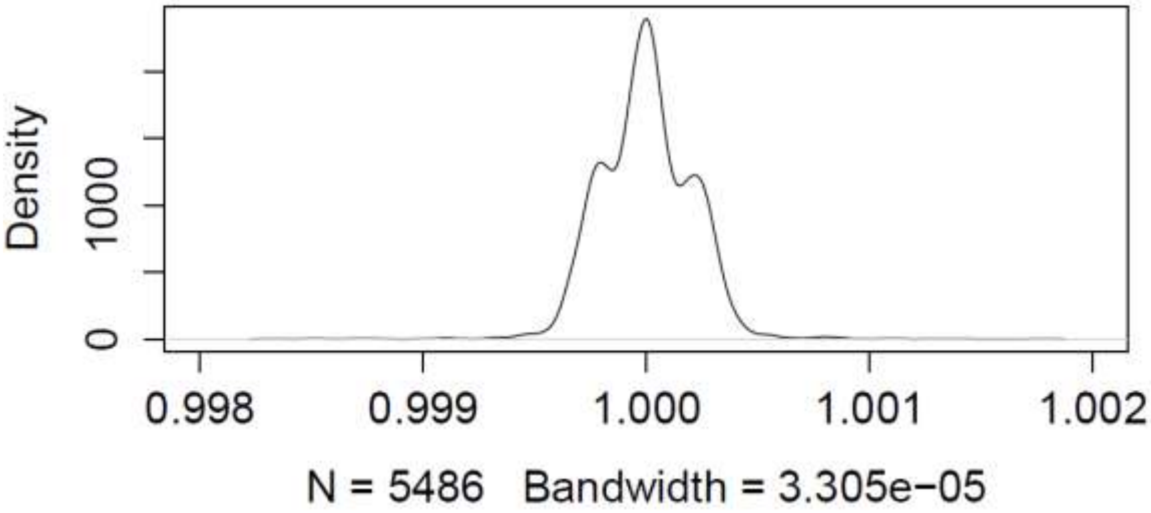


Figure 106: Supplier B Unit 30 Deviation (Source: USDOT)

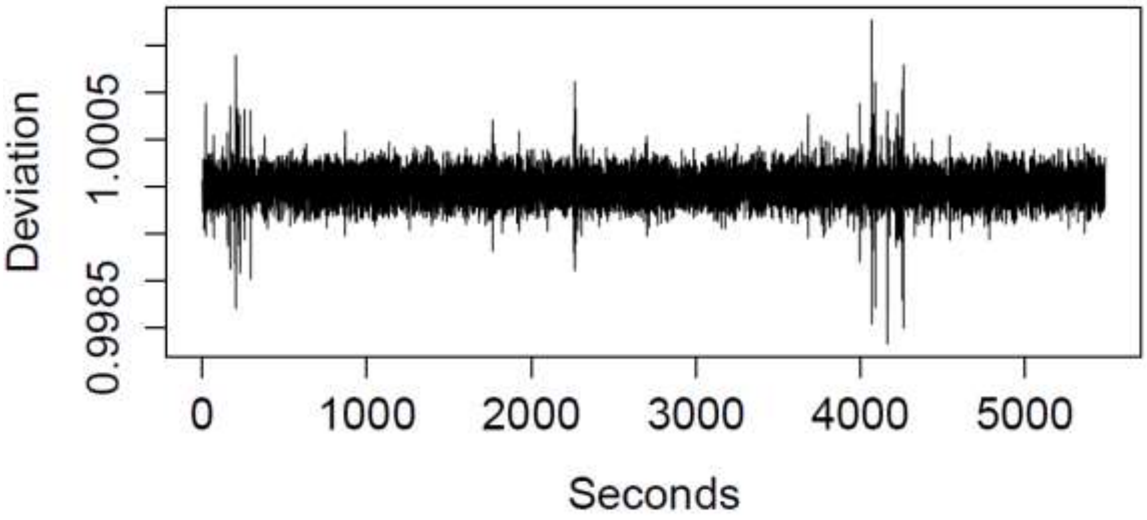


Table 37: Supplier B Unit 31 Clock Statistics

Min.	1st Qu.	Median	Mean	3rd Qu.	Max.	Std Deviation
0.9979	0.9998	1.0000	1.0000	1.0000	1.0030	0.000329685

Figure 107: Supplier B Unit 31 Power Density (Source: USDOT)

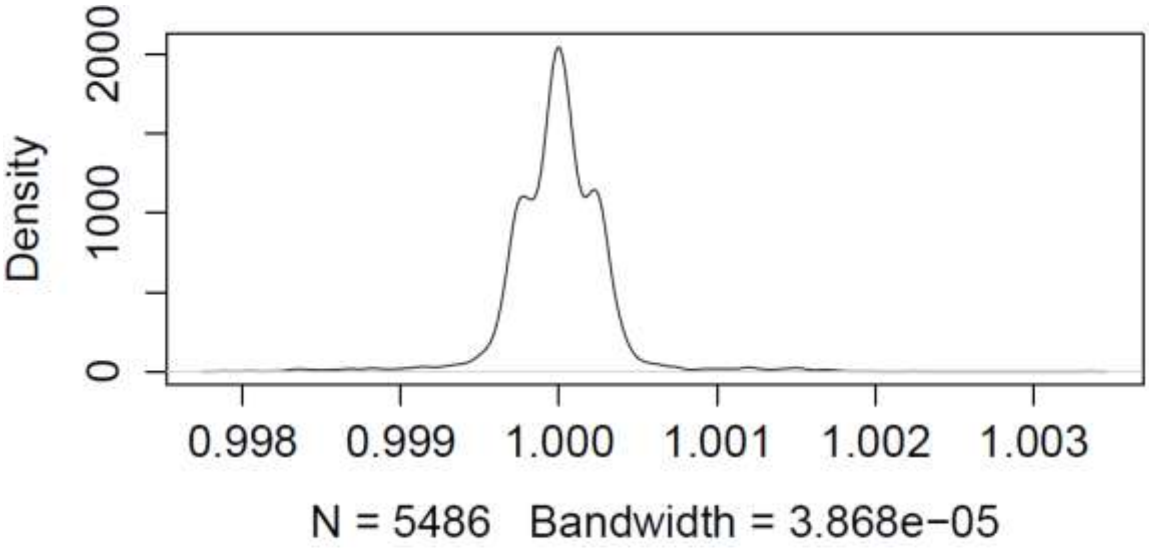


Figure 108: Supplier B Unit 31 Power Density Detail (Source: USDOT)

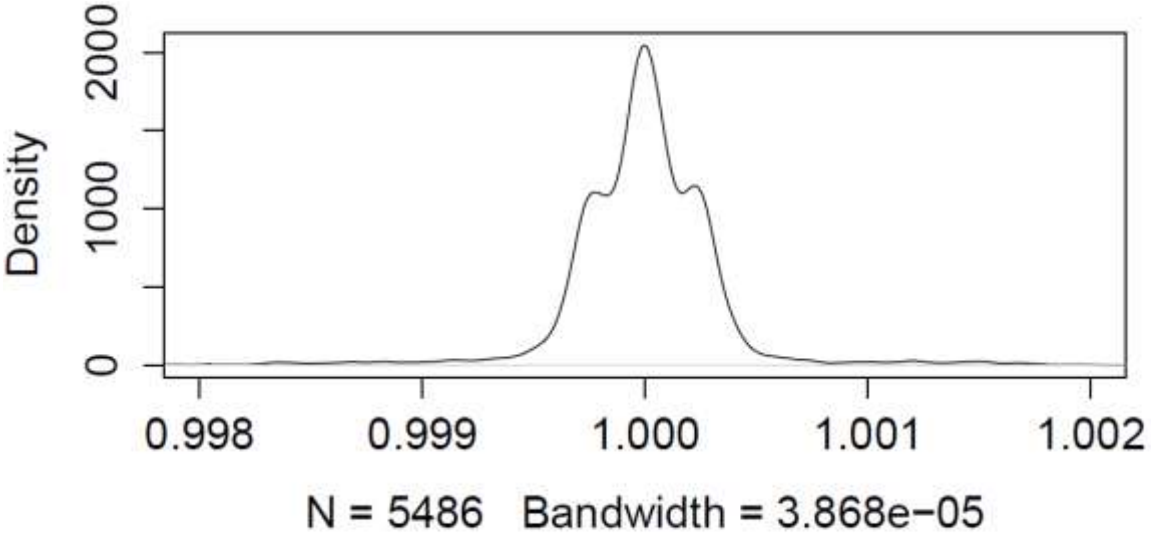
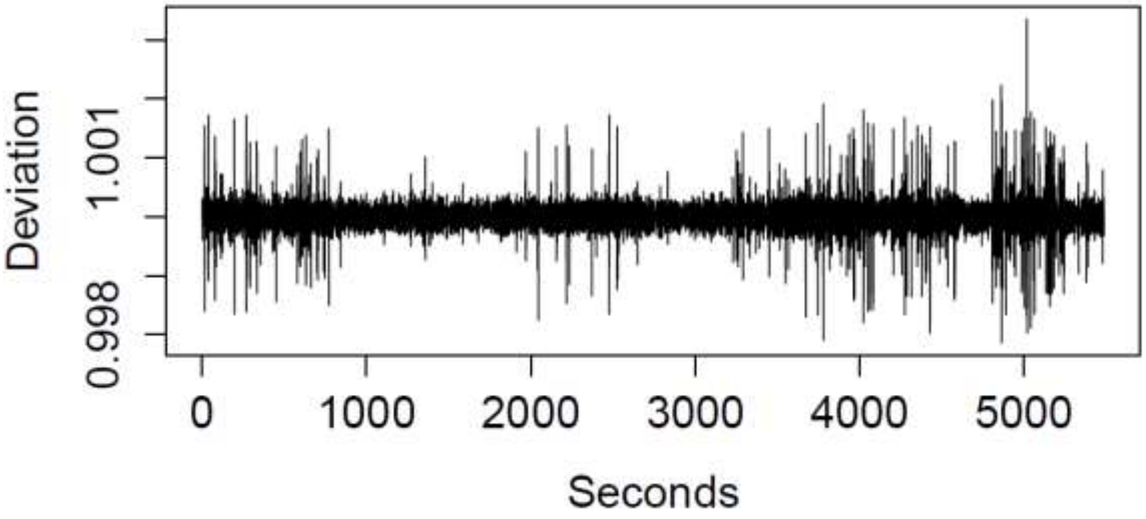


Figure 109: Supplier B Unit 31 Deviation (Source: USDOT)



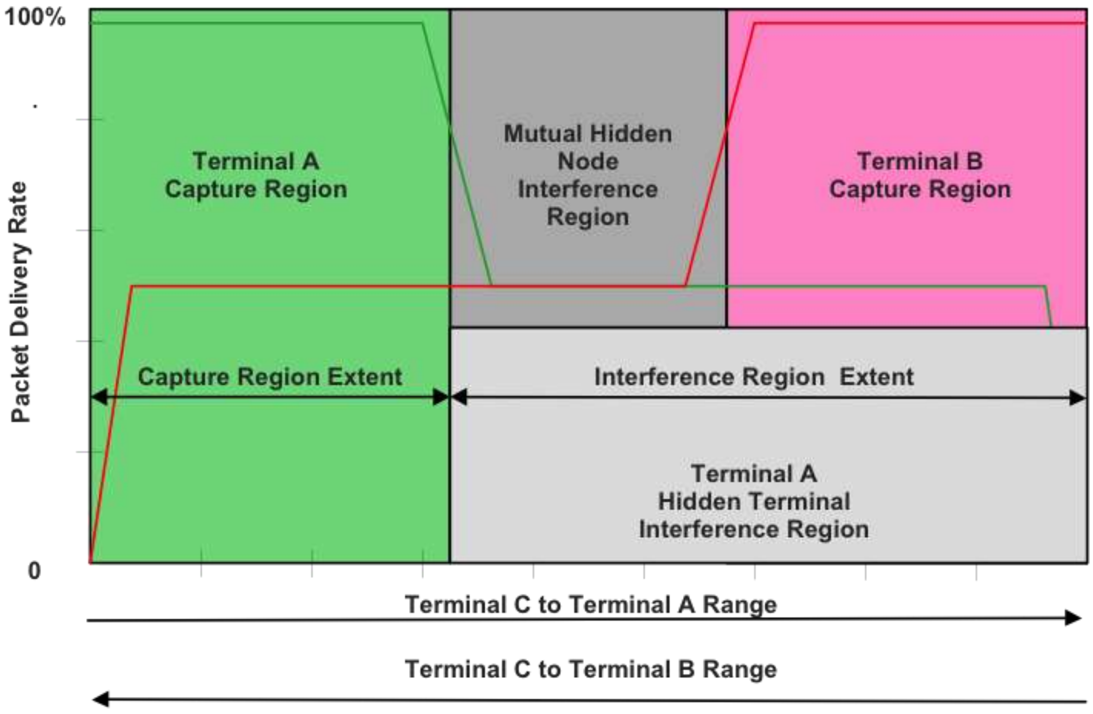
Capture Ratio Testing

This section analyzes the relationship between the capture region (the zone where a listener terminal can resolve messages from one nearby hidden terminal over interference from a more distant hidden terminal).

It is important to note that because of the symmetrical nature of the hidden terminal effect, one terminal will always dominate in the capture region, and the size of the capture region and the interference region will determine the overall scope of the interference.

The basic two interferer situation is illustrated in Figure 110.

Figure 110: Two Interferer Situation Capture Regions and Interference Region (Source: USDOT)


100%
0
Packet Delivery Rate
Terminal A Capture Region
Mutual Hidden Node Interference Region
Terminal B Capture Region
Capture Region Extent
Interference Region Extent
Terminal A Hidden Terminal Interference Region
Terminal C to Terminal A Range
Terminal C to Terminal B Range

As can be seen in this figure, if the extent of the interference region is greater than the extent of the capture region, a region of mutual interference will exist. In this region, Terminal C will be unable to receive messages from either Terminal A or Terminal B.

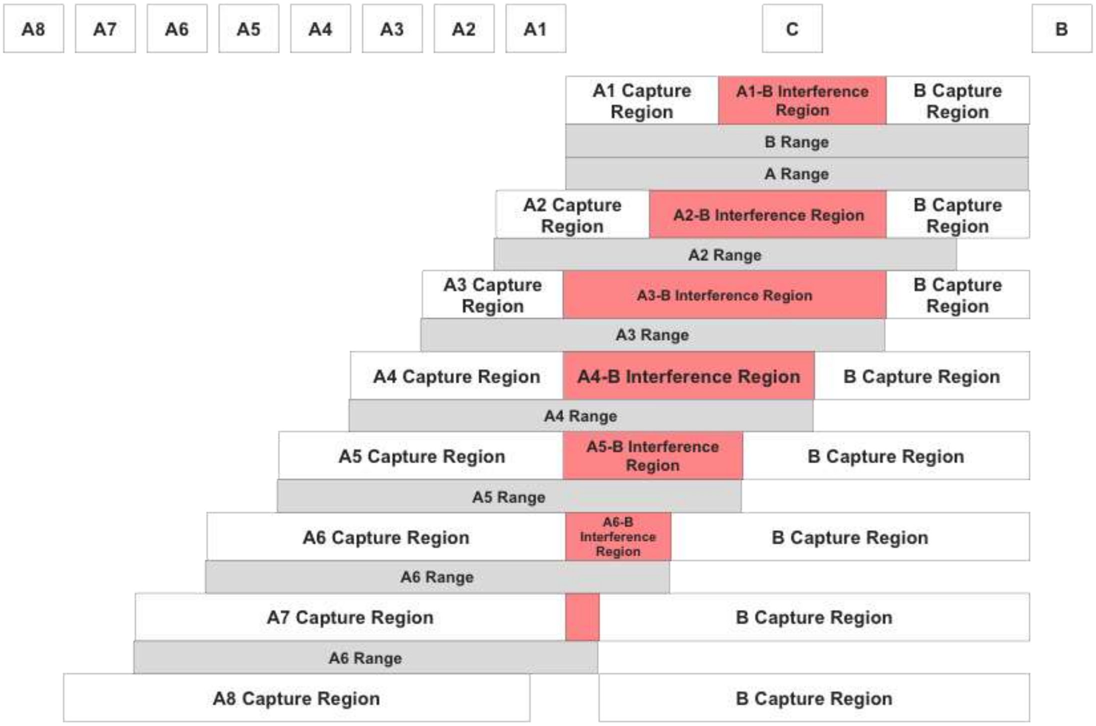
The lower bound situation occurs when terminals A and B are separated by the maximum communication range. At any closer range than this, the two terminals will be able to communicate, and thus they will not interfere, since the CSMA protocol will prevent them from transmitting at the same time.

The upper bound occurs when the range between the two terminals is twice the maximum communication range. At this point there is no region between the two terminals where a receiving terminal can receive communication from both terminals A and B.

The scope of interference is determined by the number of potential interference pairs that can exist, and this is governed by the distances associated with the aforementioned upper and lower bound ranges, and the typical minimum spacing of the terminals.

A simple analysis of the interference situation (or half of it), is provided in Figure 111.

Figure 111: Generalized Hidden Terminal Interference Situation (half of symmetrical setup) (Source: USDOT)



As shown in the figure, the lower bound interference situation has Terminal A separated from Terminal B by some maximum range R_0. In this situation there are two capture regions, one in which a receiver between the two terminals A and B will capture transmissions from Terminal A, and another where the receiver will capture transmissions from Terminal B. Between these lies an interference region, where the terminals cannot hear one another. If they transmit at the same time, the messages will collide and the receiver will not receive either message.

If additional terminals are located at incremental distances from Terminal B (labeled A2, A3, etc.), then these terminals will also create interference over at least part of the region between Terminals A and B. As can be seen in the figure, a terminal placed slightly farther from Terminal B than Terminal A will interfere over a region larger by the difference range between the terminals. This increase in the interference region size will continue until the distance between the terminal Ai and Terminal B is R_0+R_C, where R_C is the extent of the capture region. In this case, if Terminal C is located outside the range of Terminal Ai but in range of Terminal B, it will hear Terminal B. At this point the effective capture region of B increases for this pair of interferers. This increase in the size of the interference region will continue until the capture region for Terminal Ai is outside the maximum range of Terminal B. As additional terminal Ai are added at increasing ranges, the size of the interference region will decrease since it is limited by the overlap of the ranges of the terminals and the terminals are increasingly separated.

Since the terminals have a finite size and operate at finite separations, it is possible to compute the number of interfering terminals that can exist in a given physical situation. One can define the minimum separation between terminals in a lane as $S_{T.}$ Looking at each situation one can see that when the distance between Terminal A_1 and Terminal A_N is equal to R_0+R_C, the number of interferers per lane is given by:

$N=INT[(R_0+R_C)/S_T]$

When the region between R_0+R_C and $2R_{0,}$ is filed with interferers spaced at intervals S_T, the number of interferers is given by:

$K=INT[2R_0/S_T]$

Since the problem is symmetrical (i.e., there can also be additional terminals Bi to consider), and any terminal Bi can interfere with any terminal Ai, the total number of interfering pairs is:

$I_{TOT}=(N+K)^2= (INT[(R_0+R_C)/S_T]+INT[2R_0/S_T])^2$

Example:
For 9 Mbps data rate, the maximum range (R_0) is 700 meters, and the capture range is 275 meters. For passenger vehicles S_T is typically no less than 10 meters, thus:

$N=INT[(R_0+R_C)/S_T]=98$

$K=INT[2R_0/S_T]=140$

Because the problem is symmetrical about the center point, there will also be the same number of “Bi” terminals, thus there may be as many as 476 possible interferers. One way to mitigate this interference is to separate the messages in time. The notion of asynchronous BSM transmission was discussed elsewhere in this report. In order to mitigate hidden terminal interference with this many vehicles, it is apparent that at least 476 time slots must be used. This will not eliminate interference because some vehicles will randomly select the same slot, but it should significantly reduce packet losses since while the probability of a few pairs of vehicle choosing the same slot is relatively high, the probability that many vehicles will choose the same slot is relatively low.

Congestion Testing

All information is found in the main body of the report except for raw data which is available on request.

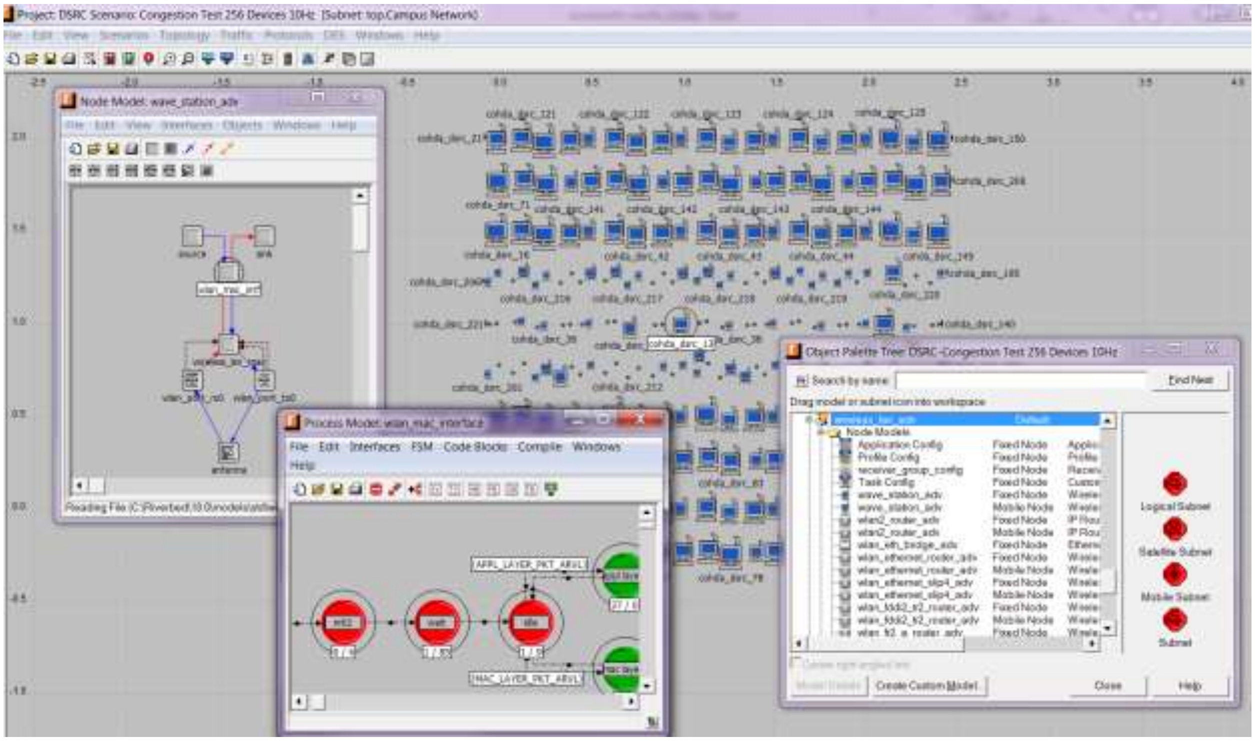
Communication Simulations

For simulating the communication aspect of the DSRC network analysis, the team used Riverbed[14] Wireless Modeler V.18.0 software, previously called Opnet. The Wireless Modeler Suite provides a comprehensive development environment supporting the modeling of communication networks and distributed systems. Both behavior and performance of modeled systems can be analyzed by performing discrete event simulations. The Modeler environment incorporates tools for all phases of a

[14] Riverbed Website: https://support.riverbed.com/content/support/software/steelcentral-npm/modeler-index.html

study, including model design, simulation, data collection, and data analysis. V.18.0 has the necessary requirements for simulating a vehicular network, including the IEEE 802.11p protocol.

Figure 112: An Overview of the Wireless Modeler Suite Simulation Environment (Source: USDOT)


Project: DSRC Scenario: Congestion Test 256 Devices 10Hz [Subnet: top.Campus Network]
Node Model: wave_station_adv
Process Model: wlan_mac_interface
File Edit Interfaces FSM Code Blocks Compile Windows Help
Object Palette Tree: DSRC-Congestion Test 256 Devices 10Hz
Find Next
Node Models
Logical Subnet
Satellite Subnet
Mobile Subnet
Subnet
Create Custom Model
Close
Help

Here are the list of common parameters used for all the simulation scenarios conducted:

Table 38: Common Simulation Scenario Parameters

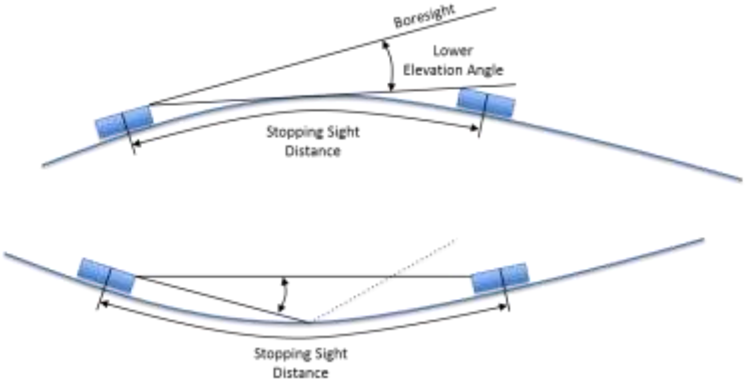
Parameter	Value	Parameter	Value
Minimum Frequency	5855 MHz	**Packet (message) Size**	300 bytes
Transmit Power	20 dBm	**Modulation**	OFDM
Packet Reception Power Threshold	-95 dBm	**Message Transmission Rate**	2, 5, 10 Hz
Transmitter Antenna Height	1.5 meter	**Bandwidth**	10 MHz and 20 MHz
Receiver Antenna Height	1.5 meter	**Data Rate**	6, 9, 12, 18 Mbps

Transmit Power and Antenna Gain and Sensitivity Analysis and Simulation

11.1.1 Elevation Line of Sight

Figure 113 demonstrates stopping sight distance versus elevation changes.

Figure 113: Stopping Sight Distance vs. Elevation Angle (Source: USDOT)



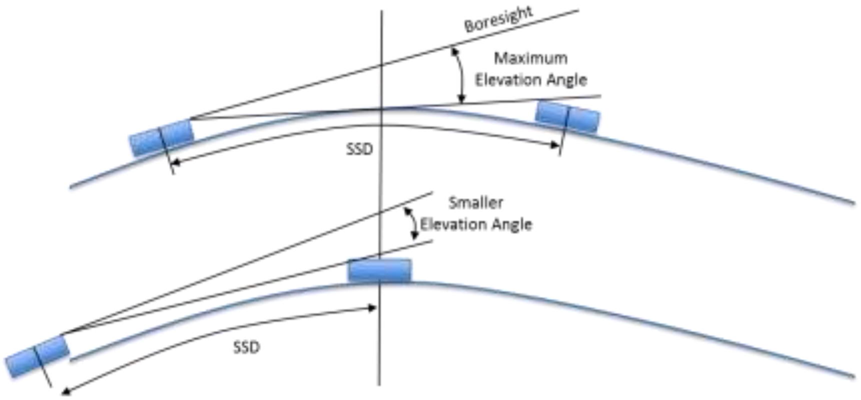
The minimum elevation angle is determined by the Stopping Sight Distance (SSD). It should be symmetrical around boresight. This minimum angle guarantees that the two vehicles will be able to communicate over the crest of a hill or in a sag.

The road geometry is very important in determining the minimum elevation angle. Vertical angles at grade changes are generally defined by parabolas (American Association of State Highway and Transportation Officials [AASHTO] Standard Specifications for Public Works Construction, "Greenbook").

The maximum elevation angle is the maximum angle observed along a curve with length equal to the SSD. SSD and grade change versus distance will be given by the road speed limit[15]. Maximum elevation angle will occur when two vehicles are half the SSD from the center of the crest or sag:

[15] http://safety.fhwa.dot.gov/speedmgt/ref_mats/fhwasa10001/

Figure 114: Maximum Elevation Angle (Source: USDOT)



$$\mathit{Sight\ Distance}\ (S) > \mathit{Curve\ Length}\ (L)$$
$$L = 2S - 200\left(\sqrt{h1} + \sqrt{h2}\right)^2/A$$
$$\mathit{Sight\ Distance}\ (S) < \mathit{Curve\ Length}\ (L)$$
$$L = \frac{A * S^2}{100\left(\sqrt{2h1} + \sqrt{2h2}\right)^2}$$

BVC = Beginning of Vertical Curve
EVC = End of Vertical Curve
g_1 = initial roadway grade, expressed in percent
g_2 = final roadway grade, expressed in percent
A = absolute value of the difference in grades (initial minus final), expressed in percent
h_1 = Height of the eye above roadway, measured in meters or feet
h_2 = Height of object above roadway, measured in meters of feet
L = curve length (along the x-axis)
PVI = point of vertical interception (intersection of initial and final grades)
tangent elevation = elevation of a point along the initial tangent
x = horizontal distance from BVC
Y (offset) = vertical distance from the initial tangent to a point on the curve
Y^1 = curve elevation = tangent elevation – offset

Figure 115: SSD vs. Crest (Source: USDOT)

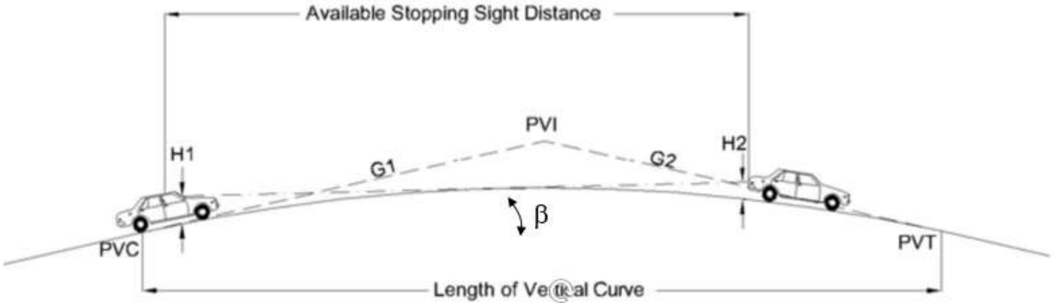


Figure 115 is the angle between the tangent to the road at the crest, and the boresight of the vehicle. G1 and G2 are the grades.
Worst case angle is when G1=-G2 (equal grades). In this case A=2G1 (in percent).

$$\text{Since } G1 = 100Tan(\beta), \beta = ArcTan\,(\frac{\frac{A}{2}}{100})$$

For the sag or valley situation, the geometry is the same, meaning that upper and lower elevations should be the same.

The crest situation is as follows. In the equations below, the team wants to solve for A such that L=S,

Sight Distance > Curve Length (S>L):

$$L = 2S - (200\frac{\left(\sqrt{h1}+\sqrt{h2}\right)^2}{A})$$

Sight Distance < Curve Length (S<L):

$$L = AS^2/100\ \left(\sqrt{2h1}+\sqrt{2h2}\right)^2$$

Therefore, solving for A in either equation results in:

$$A = 200\ \left(\sqrt{h1}+\sqrt{h2}\right)^2/S$$

Where h_1 and h_2 are about 1.5 meters.

Table 39 and Table 40 summarize the elevation angle requirements at different speeds, SSD/ESD, and Grade Difference (A).

Table 39: Elevation Angle Based on Stopping Sight Distance

Speed (mph)	Speed (kph)	SSD	Grade Difference (A)	Elevation Angle
20	32.2	107	11.2	3.2
40	64.4	313	1.9	1.1
60	96	634	1.9	0.5
80	128.8	845.3	1.4	0.4

Table 40: Elevation Angle Based on Emergency Stopping Distance

Speed (mph)	Speed (kph)	SSD	Grade Difference (A)	Elevation Angle

Speed (mph)	Speed (kph)	SSD	Grade Difference (A)	Elevation Angle
20	32.2	63	19	5.4
40	64.4	225	5.3	1.5
60	96	495	2.4	0.7
80	128.8	660	1.8	0.5

Based on the above, EIRP and Sensitivity requirement shall apply over 360 degree azimuth and ±10 degrees elevation.

11.1.2 Transmit Power and Antenna Gain Envelope Analysis

The power threshold for receiving packets in a DSRC network is up to -95 dBm. Therefore the minimum power threshold is as follows:

$$P_{min} = 1W * 10^{\frac{x-30}{10}} = 1W * 10^{\frac{-95-30}{10}} = 1W * 10^{-12.5} = 3.1623 * 10^{-13}W$$
$$P_{min} = -12.5\, dB$$

Using the two-ray path-loss model used in the simulation, the effective range for 0 elevation angle is as follows:

$$\frac{P_r}{P_t} = \begin{cases} \left(\frac{\lambda}{4\pi d}\right)^2, & d \leq d_c \\ \left(\frac{\lambda d_c}{4\pi d^2}\right)^2, & d > d_c \end{cases}$$

$$d_{max} = \sqrt{\frac{h_t h_r}{\pi} * \sqrt{\frac{P_t * 10^{\frac{G}{10}}}{P_{min}}}} = \sqrt{\frac{h_t h_r}{\pi} * \sqrt{\frac{0.1W * 1}{3.1623 * 10^{-13}W}}} = 635\, m$$

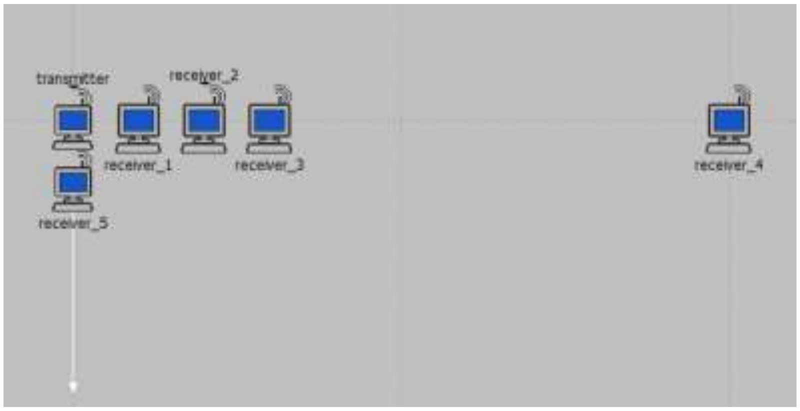
Consecutively the effective range for different angles are:

Along azimuth (φ = 90°, G=0): 634 meters
5° from azimuth (φ = 85°, 95°, G=-3): 534 meters
10° from azimuth (φ = 80°, 100°, G=-6): 449 meters
> 10° from azimuth (φ < 80° or φ > 100°, G=-20): 200 meters

A total of 5 scenarios were ran for this simulation as follows:

1) Transmit Power and Antenna Gain
This simulation scenario measured power received at 100m, 200m, and 300m away from the transmitter. It also measured the power level at a receiver that is moving on a trajectory from 100m to 420m away from the transmitter.

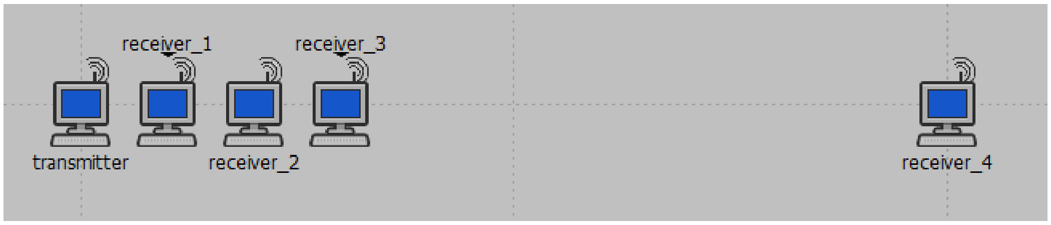
Figure 116: Transmit Power and Antenna Gain Simulation Schematic in Opnet (Source: USDOT)



2) Transmit Power and Antenna Gain Path-loss Test

This simulation scenario measured power received at 100m, 200m, and 300m away from the transmitter, with an added receiver at 1000m away from the transmitter to view the behavior at a position where the packet would be viewed as noise.

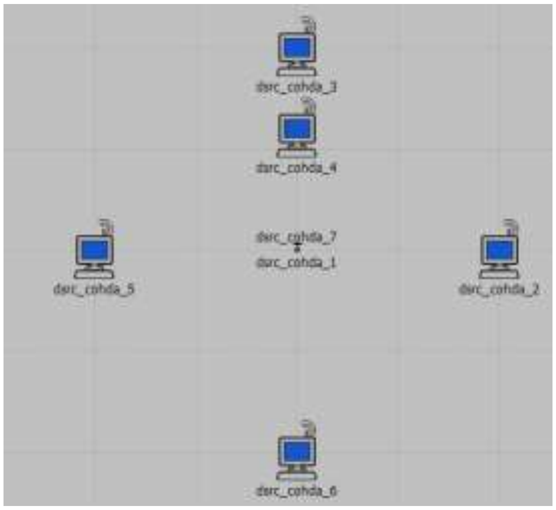
Figure 117: Transmit Power and Antenna Gain Path-loss Simulation (Source: USDOT)



3) Transmit Power and Antenna Gain Envelope 100 m

In this simulation, the team calibrated the antenna pattern and made sure that it was oriented correctly. Four receivers were placed along the azimuth at the same distance, one receiver above the transmitter, and one receiver at 30 degrees above the azimuth.

Figure 118: Transmit Power and Antenna Gain Envelope Simulation, 100 m (Source: USDOT)



4) Transmit Power and Antenna Gain Envelope 10 m, 30 Deg

This scenario was similar to the above, varying the pitch, yaw, and roll of a receiver.

Figure 119: Transmit Power and Antenna Gain Envelope Simulation, 10 m (Source: USDOT)

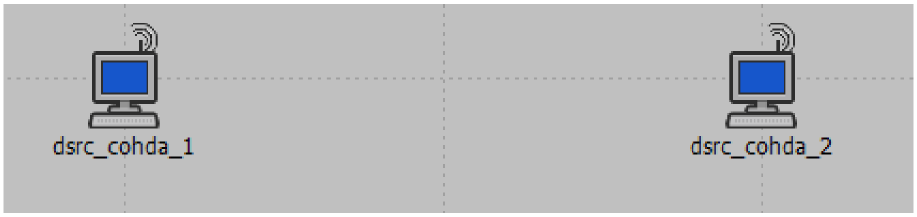


Figure 120 and Figure 121 summarize the observations for the above scenarios.

Figure 120: Packet Delivery Rate vs. Distance for Different Angles (Source: USDOT)

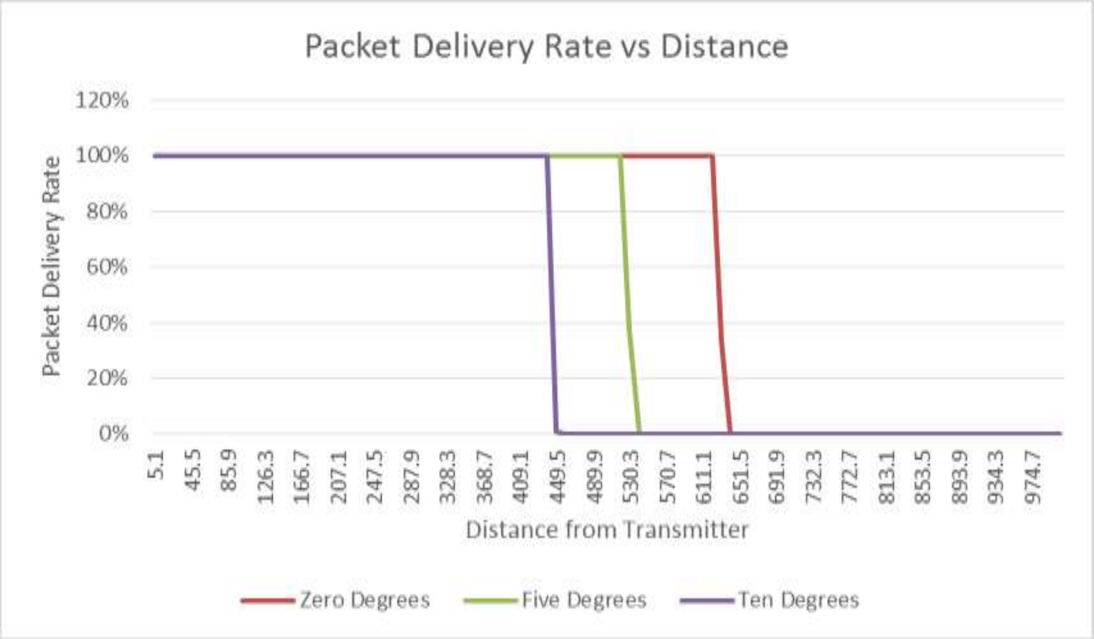
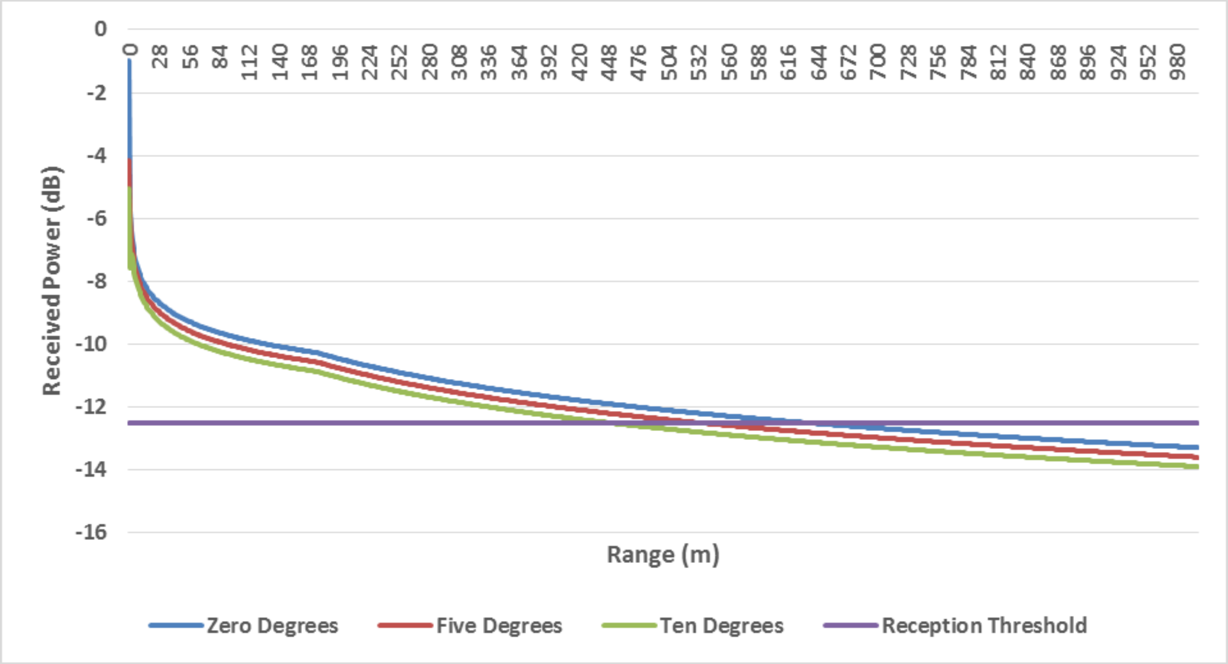


Figure 121: Power Received (dB) vs Distance (m) from Transmitter for Different Elevation Angles (Source: USDOT)



Congestion Simulation

Channel congestion means that there are too many vehicles seeking to send too much data and the channel is incapable of handling the data. In the worst case situation, the data flow actually declines because the CSMA function is seeking to avoid collisions, so little data is actually sent. Most research and simulations indicate that the vehicle densities found on typical roads will present a problem if BSMs are sent at the nominal 10 Hz rate (assuming full penetration of the vehicles within a given footprint). CSMA does not prevent transmission where two devices listen and then start broadcasting, which results in some direct interference. This limitation is manifested as reduced message reliability (i.e., the probability that a sent message will be receivable), which will translate directly to reduced safety system reliability.

Some of the contributing factors to the issues with channel congestion are as follows:

BSM Density
Under normal operation each vehicle is supposed to send the BSM at a 10 Hz rate, once every 100 milliseconds. However, the various messaging constraints may cause issues with this message rate.

First, the DSRC channel has a finite data rate and, depending on how many users are present, the total volume of data to be sent by all vehicles in the footprint may require more time to send than the 100 millisecond message repeat rate. The result will be that vehicles will need to wait longer to send their messages, and will be unable to maintain the 100 millisecond rate.

Second, the CSMA mechanism is designed to separate a modest number of users in time so their messages do not collide. When the number of users is significant, this mechanism becomes increasingly inefficient. At some point the number of users is so large that the rate of message collisions rises significantly, a condition known as “channel collapse.”

These first two issues relate to the ability to send the message in the DSRC channel. In addition to this, there is the problem of receiving and processing the messages. In the typical case of about 200 vehicles in the radio footprint, any given vehicle will be receiving about 2,000 messages per second. This may present a substantial processing burden on the vehicle OBE.

Data Rate Limitations
A typical BSM payload is 38 bytes in size. However, the WSMP includes other data; the digital signature adds about 200 bytes, and the encoding for transmission adds still more bytes. The total size of a signed BSM (Part 1) at the transmitter is about 285 bytes (2,280 bits).
At a data rate of 6 Mbps, each bit will effectively consume 167 nanoseconds of channel time. Thus a 285-byte signed BSM will require 380 microseconds of actual transmission time.

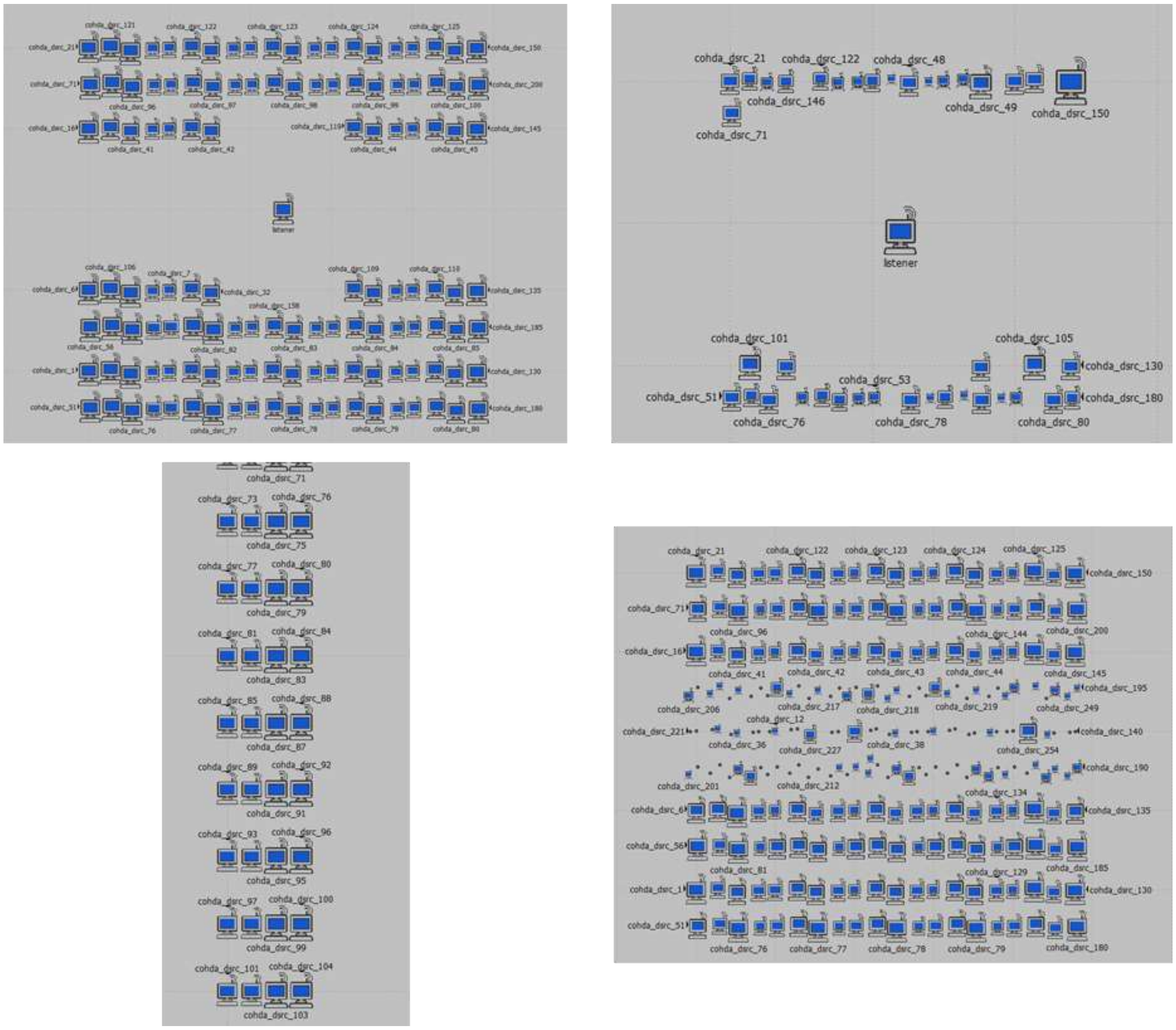
In addition to the transmission time, the CSMA process will require each sender to wait some time period before sending. One can assume that the average wait time is half of the contention window time. With 14 contention windows, each 9 microseconds long, the average wait time (where the channel is not busy but users are counting down slots in order to send) is 67.5 microseconds (9 x 15/2). If the contention window is raised to 1,023, then this empty time will be 4.6 milliseconds.

Thus, the time required to send a BSM will be between 448 microseconds (best case) and 4.95 milliseconds (worst case).

Using the best case channel access time value, the maximum number of BSMs that can be sent in a 100 millisecond interval is 223 messages. At the worst case channel access time value, the maximum would be only about 20 messages.

To demonstrate the effect of these limitations on channel congestion and the ways they could be addressed, several scenarios were simulated, changing a range of factors including: data rate, message transmission rate, bandwidth, and the level of congestion by varying the number of nodes (vehicles). Figure 122 shows the schematic for some of these scenarios:

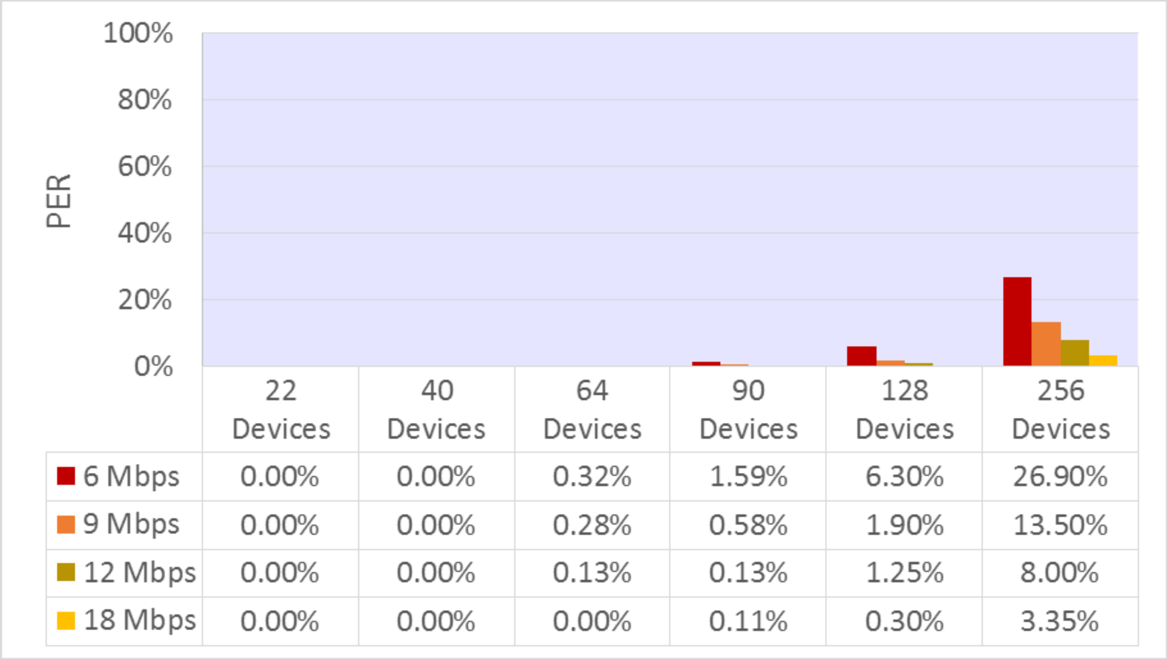
Figure 122: A Sample of Congestion Scenarios (Source: USDOT)



The above shows the situations where many vehicles are transmitting within communication range of each other (which minimizes the hidden node effect). PER was measured for each varying range of message rate, data rate, and bandwidth.

The figure on the lower right, is a highway situation where the hidden node issue will also have an effect on the PER levels. The results of these simulations are summarized in the figure below.

Figure 123: PER for Different Congestion Scenarios (Vehicles in 100x100 meter area) (Source: USDOT)



	22 Devices	40 Devices	64 Devices	90 Devices	128 Devices	256 Devices
🟥 6 Mbps	0.00%	0.00%	0.32%	1.59%	6.30%	26.90%
🟧 9 Mbps	0.00%	0.00%	0.28%	0.58%	1.90%	13.50%
🟫 12 Mbps	0.00%	0.00%	0.13%	0.13%	1.25%	8.00%
🟨 18 Mbps	0.00%	0.00%	0.00%	0.11%	0.30%	3.35%

Table 41 details the PER value derived from simulations for different values of message transmission rate, data rate, and vehicle density in a 100x100m area. Please note that the Error Correction Code threshold used is 25% (i.e., if more than 25% of the bits in a packet are erroneous, the packet is discarded).

Table 41: Packet Error Rate Values Varying Different Factors

		Vehicles within Range of Listener					
Message Rate	**Data Rate**	**22**	**40**	**64**	**90**	**128**	**256**
		Packet Error Rate					
2 Hz	**6 Mbps**	0.0%	0.0%	0.0%	0.0%	0.0%	0.2%
	9 Mbps	0.0%	0.0%	0.0%	0.0%	0.0%	0.1%
	12 Mbps	0.0%	0.0%	0.0%	0.0%	0.0%	0.1%
	18 Mbps	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
5 Hz	**6 Mbps**	0.0%	0.0%	0.0%	0.1%	1.4%	5.3%
	9 Mbps	0.0%	0.0%	0.0%	0.0%	0.5%	2.2%
	12 Mbps	0.0%	0.0%	0.0%	0.0%	0.4%	1.3%
	18 Mbps	0.0%	0.0%	0.0%	0.0%	0.1%	0.6%
10 Hz	**6 Mbps**	0.0%	0.0%	0.3%	1.6%	6.3%	26.9%
	9 Mbps	0.0%	0.0%	0.3%	0.6%	1.9%	13.5%
	12 Mbps	0.0%	0.0%	0.1%	0.1%	1.3%	8.0%
	18 Mbps	0.0%	0.0%	0.0%	0.1%	0.3%	3.4%

Shannon-Hartley Theorem

Consider a band-limited Gaussian channel operating in the presence of additive Gaussian noise:

The Shannon-Hartley theorem states that the channel capacity is given by:

$$C = B \log2(1 + S/N)$$

Where C is the capacity in bits per second, B is the bandwidth of the channel in Hertz, and S/N is the signal-to-noise ratio.

Hidden Terminal Simulations (with and without Congestion)

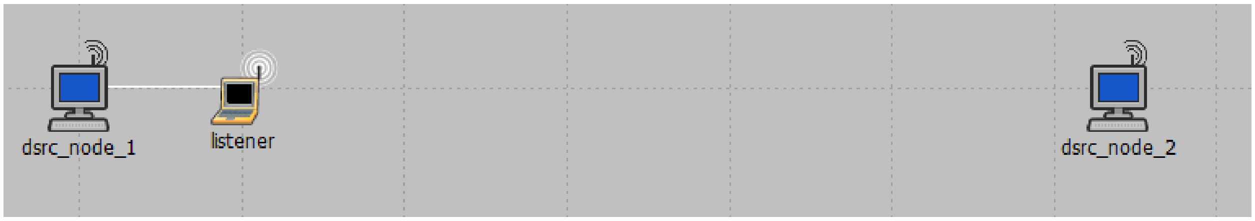
“Hidden terminal effect” is observed in the networks using the CSMA scheme. CSMA is essentially a formalization of the process of contending for a busy channel. People generally use an analogous process in conversation. Specifically, someone may listen, and if nobody is speaking, they may speak. If someone else is speaking, the next speaker may wait and then listen for silence again prior to speaking. When a DSRC radio has a message to send, it first examines the state of the “Channel Busy Indication.” This is an indication from the lower layers of the protocol (e.g., the physical radio layer) that someone is sending a message in the radio channel. If the channel is not busy the radio simply sends the message. If the channel is busy, the radio must contend for the channel.

As described, the CSMA mechanism requires that each terminal listen to the channel to determine if the channel is busy. This implies that each terminal is in range of every other terminal. Unfortunately, in the roadway environment, especially in traffic, this assumption is not valid.

In the simulations, the team tried to isolate the effects of hidden node in a vehicular network, with and without congestion.

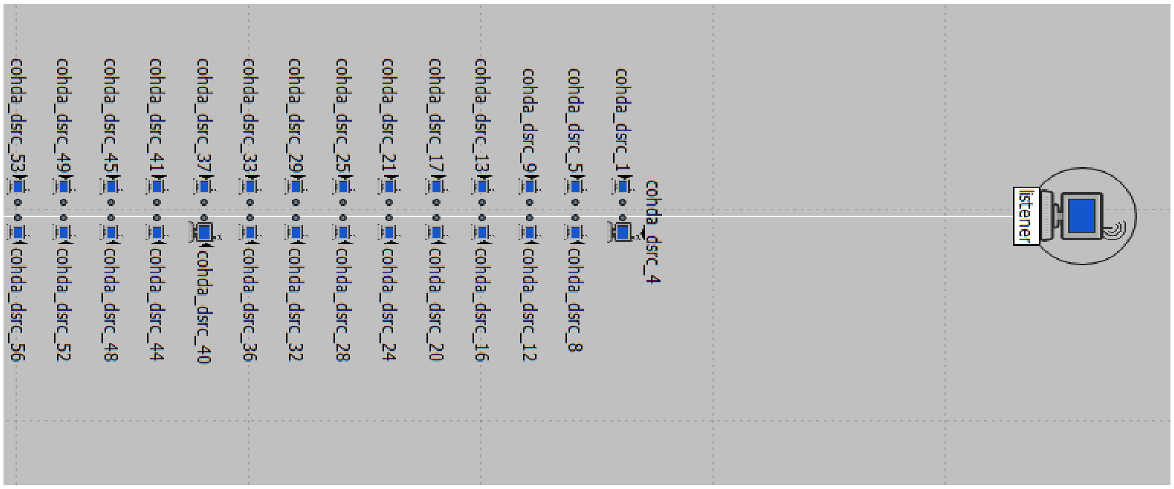
The team started with just 3 nodes to test the basic hidden node issue.

Figure 124: Basic Hidden Terminal Scenario (Source: USDOT)



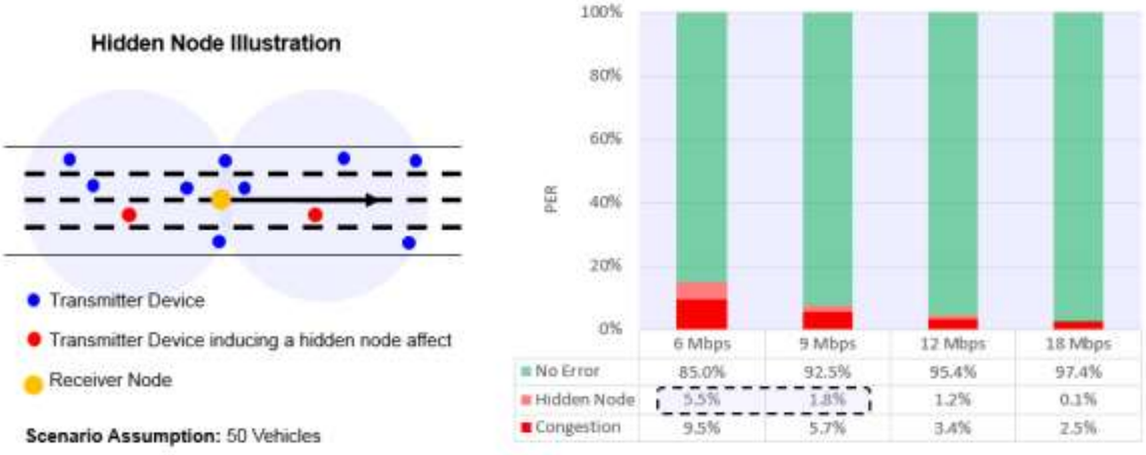
The team then added more nodes to the system to simulate a scenario of hidden node in a busy highway:

Figure 125: Hidden Node Scenario in a Busy Highway (Source: USDOT)



In these scenarios, the team changed different factors such as data rate, message rate, and number of vehicles to determine the effect of PER as a result of the hidden node issue. This is summarized in Figure 126:

Figure 126: Hidden Node Issue in a Stretch of Highway (Source: USDOT)

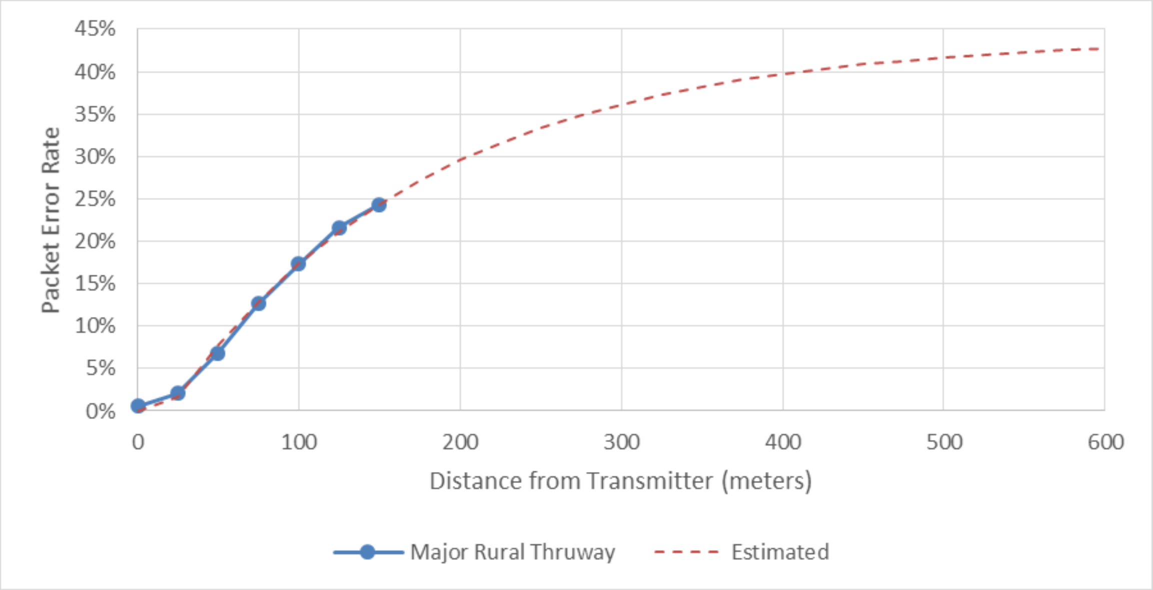


	6 Mbps	9 Mbps	12 Mbps	18 Mbps
🟩 No Error	85.0%	92.5%	95.4%	97.4%
🟥 Hidden Node	5.5%	1.8%	1.2%	0.1%
🟥 Congestion	9.5%	5.7%	3.4%	2.5%

Informing the Opnet Simulation with Field Test Data

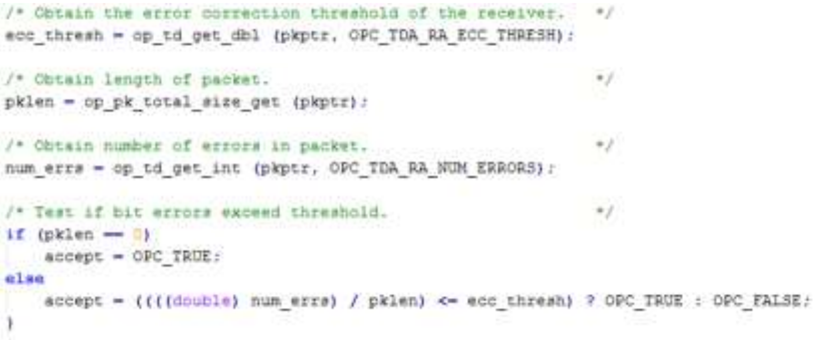
When using the CAMP data to inform Opnet models, the team used the Excel optimization tool to fit a curve to the data and determine the best fitted formula that describes the data. Figure 127 below demonstrates the data collected from CAMP vs. what was estimated using the excel optimization tool for a Major Rural Thruway. CAMP data was only used for the transmission range of up to 150 meters as those were the most reliable data.

Figure 127: CAMP Range Testing Data – Major Rural Thruway (Source: USDOT)



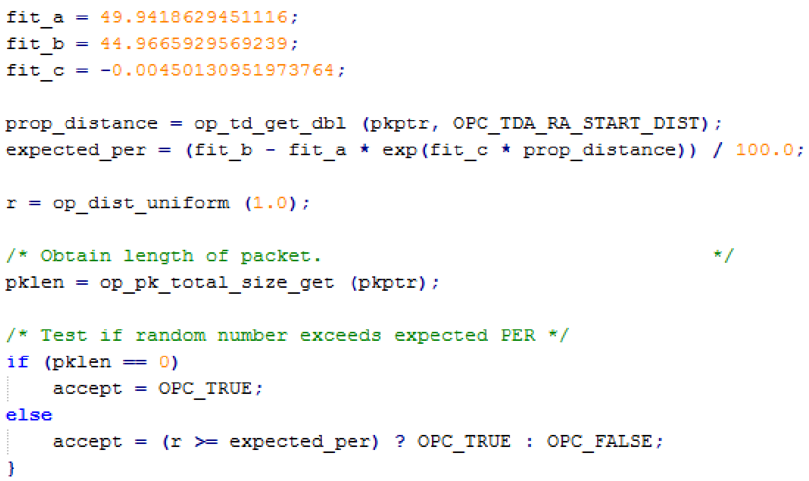
The formula that best fits this data is: $PER_{exp} = 49.3 - 43.9 * e^{-0.00615*d}$. This model was used in the Opnet simulation by modifying the PER pipeline stage in the C Code, *wlan_ecc_field.ps.c*, as follows.

The part of the code changed was:



```
/* Obtain the error correction threshold of the receiver.   */
ecc_thresh = op_td_get_dbl (pkptr, OPC_TDA_RA_ECC_THRESH);

/* Obtain length of packet.                                  */
pklen = op_pk_total_size_get (pkptr);

/* Obtain number of errors in packet.                        */
num_errs = op_td_get_int (pkptr, OPC_TDA_RA_NUM_ERRORS);

/* Test if bit errors exceed threshold.                      */
if (pklen == 0)
    accept = OPC_TRUE;
else
    accept = ((((double) num_errs) / pklen) <= ecc_thresh) ? OPC_TRUE : OPC_FALSE;
}
```

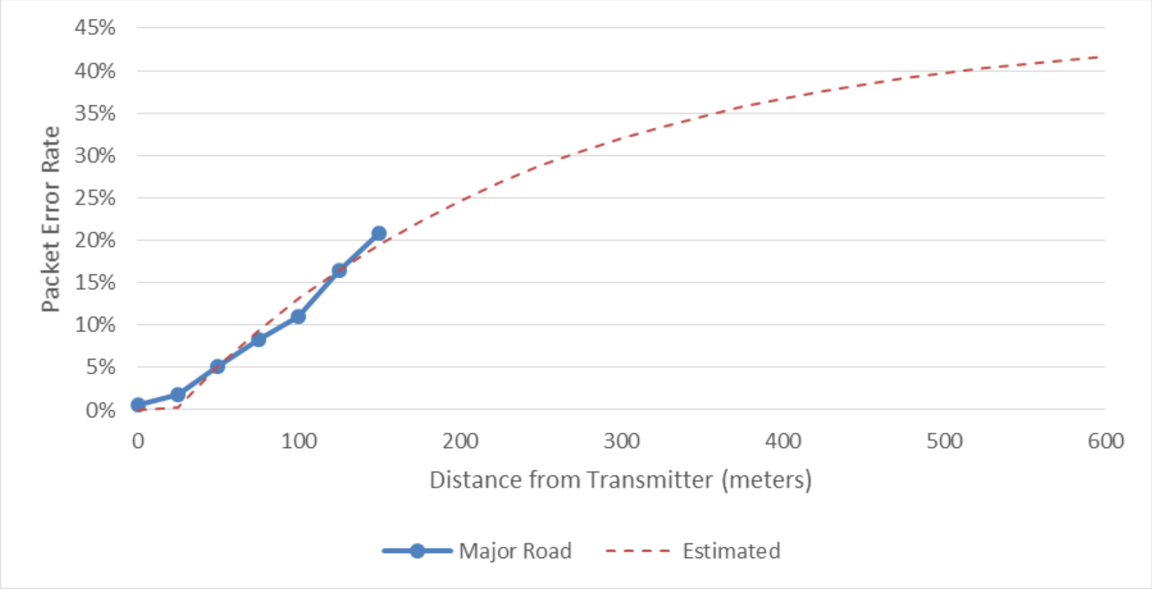
Which was modified as follows:



```
fit_a = 49.9418629451116;
fit_b = 44.9665929569239;
fit_c = -0.00450130951973764;

prop_distance = op_td_get_dbl (pkptr, OPC_TDA_RA_START_DIST);
expected_per = (fit_b - fit_a * exp(fit_c * prop_distance)) / 100.0;

r = op_dist_uniform (1.0);

/* Obtain length of packet.                              */
pklen = op_pk_total_size_get (pkptr);

/* Test if random number exceeds expected PER */
if (pklen == 0)
    accept = OPC_TRUE;
else
    accept = (r >= expected_per) ? OPC_TRUE : OPC_FALSE;
}
```

Figure 128 below demonstrates the best fit to data for Major Roads.

Figure 128: CAMP Range Testing Data – Major Road (Source: USDOT)

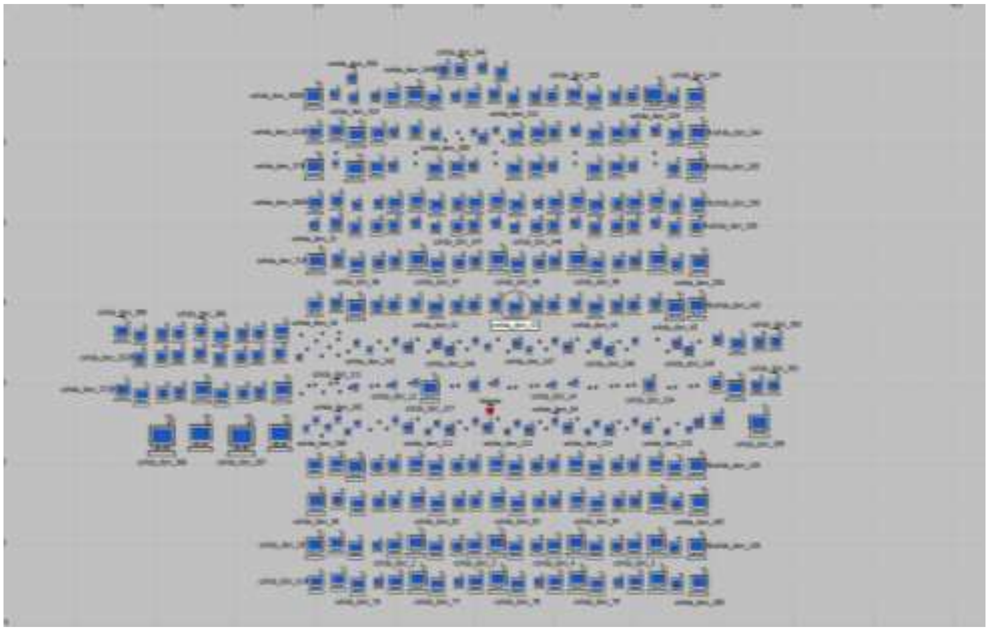


The formula that best fits this data is: $\boldsymbol{PER_{exp} = 49.9 - 45.0 * e^{-0.0045*d}}$. As described above, this model could be used to modify the C code in Opnet and create the PER simulation for Major Roads scenario.

Congestion Mitigation Simulations – 20 MHz channel

As discussed in Chapter 4, a congested network was simulated with 150-350 nodes to change the CBR values at 12 Mbps data rate using 20 MHz channel. At around 10% PER (equivalent of ~ 50% CBR), the team switched to 18 Mbps data rate to see how that improves the situation. The figure below shows the schematic of the node distribution.

Figure 129: Congestion Simulation -- 20 MHz Channel (Source: USDOT)



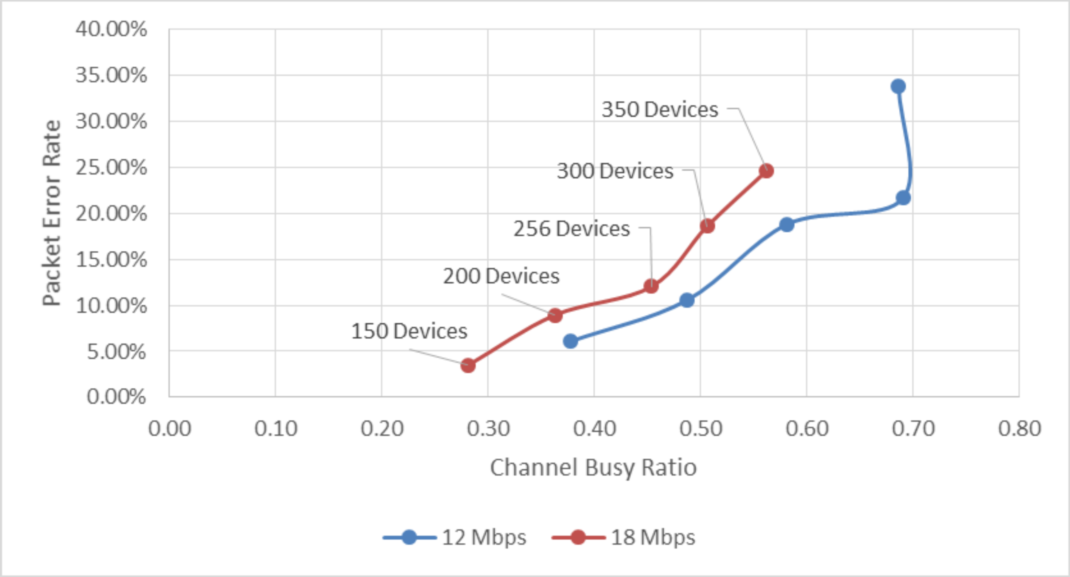
The table below shows the attributes for the nodes:

Table 42: Simulation Parameters

Parameter	Value	Parameter	Value
Minimum Frequency	5855 MHz	**Packet (message) Size**	300 bytes
Transmit Power	20 dBm	**Modulation**	OFDM
Packet Reception Power Threshold	-95 dBm	**Message Transmission Rate**	10 Hz
Transmitter Antenna Height	1.5 meter	**Bandwidth**	20 MHz
Receiver Antenna Height	1.5 meter	**Data Rate**	12 Mbps and 18 Mbps

The figure below summarizes the results of the simulation for 150-350 vehicles at two different data rates:

Figure 130: Packet Error Rate vs. Channel Busy Ratio, 12 Mbps vs. 18 Mbps (Source: USDOT)

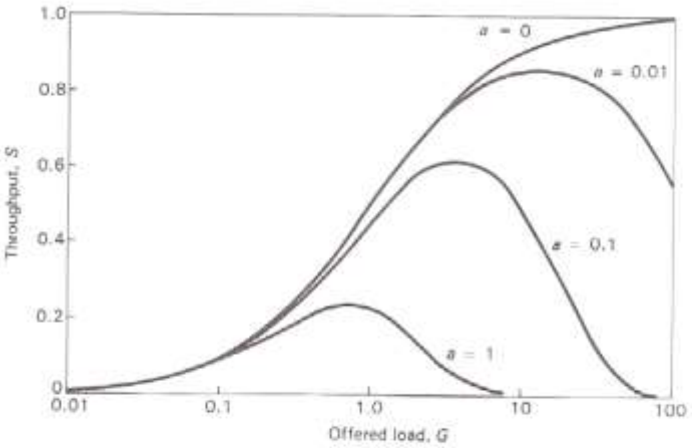


For each chosen number of devices, the simulations were run 5 times to get an average CBR. Results are shown in the figure above.

For the 12 Mbps figure, there is a saturation point for CBR at around 70%. 70% is about the expected throughput of a LAN that uses CSMA (measured in terms of medium occupancy rate or CBR, not data rate). Since the simulation has nodes that are all within range of each other, using BSM broadcasts only, the team essentially simulated an Ethernet that has 300-byte packets.

The figure below is a set of throughput curves for slotted CSMA, (IEEE 802.11). In the case a = .037. a is the ratio of packet size to sensing slot size, which is an 9 us slot time divided by 244 us packet transmit time. 244 us is the packet transmit time for a 300-byte packet at 12 Mbps in a 20 MHz channel.

Figure 131: Throughput, S, vs. Offered Traffic, G, for Slotted Nonpersistent CSMA[16]

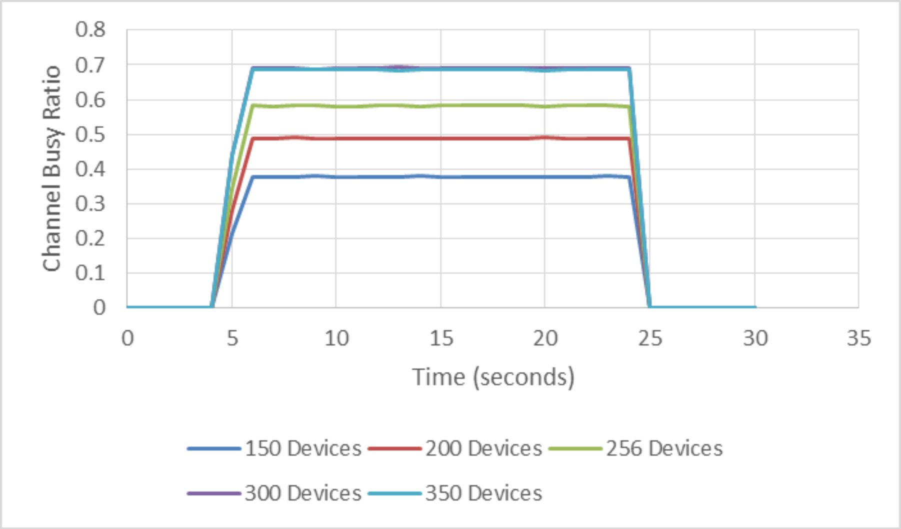


As seen in Figure 131 (comparing to the “a = 0.01” curve), with a packet size to sensing time ratio of .037, throughput should be right around 70% (or to be more accurate somewhere between 60% and 80%).

No packet switched protocol can provide 100% throughput. 70% is about best case in packet switched networks with only best-effort traffic (i.e., with no modern QoS mechanisms such as layer 2 data streaming).

Figure 132 provides the CBR value versus time (the 30 second duration of each simulation). The figure exhibits that it takes some time to get to a stable CBR value.

Figure 132: Channel Busy Ratio vs. Time (Source: USDOT)



[16] Source: Performance analysis of local computer networks, Joseph L. Hammond, Peter J. P. O'Reilly

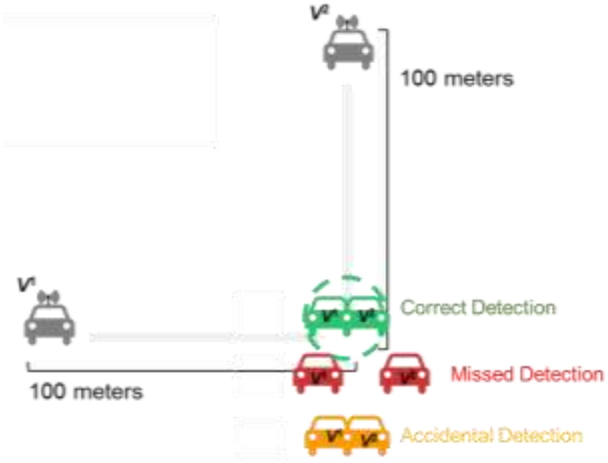
Plausibility and Hazard Analysis and Simulation

The plausibility and hazard analyses based on different sources of errors were done using Monte-Carlo simulations that simulate various scenarios of V2V interactions where BSM accuracy is critical. While generating BSMs that are transmitted between the vehicles, aggregated distributions of different sources of errors are used to constitute vehicle characteristics including speed, heading, position, etc. The simulator was coded in R-program and was given an interactive dashboard using R-shiny so that several different combinations of scenarios can be easily visualized and interpreted. Specifically, the simulations assume two moving individual vehicles that are set to interact at a fixed time in the future. This interaction could either be a sure collision or a near miss, based on their starting location, heading and speed, and trajectory. The overall analysis also assumes three sources of errors that could play a role in producing erroneous BSM messages, they are – GPS Device errors such as latitude, longitude, heading (digital compass error), yaw-rate, acceleration and speed (speed sensor), communication errors including PER, and the system time jitter. While each of these errors might be within the range that could be deemed safe, their net impact might cause BSMs to misinform connected vehicle applications. For example, a multi-vehicle interaction which should be a safe pass or near-miss, in reality might be deemed as an unsafe crash scenario which could unnecessarily urge driver action. Conversely, an interaction which is intended to result in a sure collision might be deemed as a safe-pass and, unfortunately, would not call for driver action.

Using basic Newtonian physics, these simulations seek to make future projections of vehicle locations under different error combinations, physical conditions, and roadway characteristics to find out the probabilities of misclassification of the intended interaction. In general, this analysis studies three types of interactions:

1) **Correct Detection** (True Positive) is made when the simulator detects a collision between the vehicles at the exact time and location as it will actually happen for the sure collision case. For a near-miss case, this represents the situation where a crash is NOT detected.
2) **Accidental Detection** (Accidental True Positive) is when the simulator detects a collision between the vehicles, but at a time and location different from the actual collision for the sure collision case. This type of interaction is not available for the near-miss scenarios.
3) **Missed Detection** (False Negative) is when the simulator fails to detect a collision between the vehicles over the projection time horizon for the sure collision case. For the near-miss scenarios, a missed detection implies that a crash is detected by mistake.

Figure 133: Three Types of Detection (Source: USDOT)



11.1.3 Simulation Analysis

The simulations are designed using basic Newtonian equations for the two cases – sure collision and near miss interactions. The simulator makes projections of the individual vehicle's future positions based on five different types of errors:

1) Positional errors that are applied to both latitude and longitude directions,
2) Heading errors that will simulate the error in the direction of vehicle's movement,
3) Speed errors that will involve altering the specific distance covered by a vehicle at each time-step.
4) Time Jitter that simulates the errors in the measurement of time by the DSRC clock versus the actual epoch time.
5) Packet Error Rate that represents the percentage of packets lost in transition between the two vehicles.

In order to assess the full spectrum of parameters within BSM messages, the R-based simulation framework was later modified to include two more error parameters:

1) Yaw rate errors that represents the error in the turn movement of the vehicle.
2) Longitudinal acceleration errors that represents the error in the vehicle's acceleration in the direction of movement.

The major inputs used by the simulation are:

1) Time to Crash or Projection Horizon: This time, in seconds, defines how long from the time of the prediction before the vehicles interact with each other. The projection horizon is kept the same so that the probabilities of misclassification for every time-step can be analyzed.
2) Collision Buffer: This is the distance between two vehicles that will qualify as a collision. This enables the simulator to consider vehicles as more than just points. The collision buffer can be adjusted to account for vehicle sizes.
3) Vehicle Speed: Both vehicles are assumed to be traveling at this speed.
4) Interaction Type: The simulator can simulate vehicle interactions at a right-angle where vehicles trajectories are at 90 degrees to each other or smaller angles such as for lane-change and weaving maneuvers. The smaller angles increase the probability to correctly detect crashes since vehicles will be closer to each other for a longer duration. The interaction type also included other types of vehicle trajectories such as curved (to assess yaw-rate errors) and accelerating profiles (to assess longitudinal acceleration errors).

5) Environment Type: Environment types are primarily used to define the PER associated with a given scenario and uses data from pre-defined functions for each of the stored environment types including deep urban, interstate/freeway, local road, major road, major rural throughway, major urban throughway, and mountains.
6) Number of Simulations: This represents the number of Monte Carlo simulations to be conducted at each time-step (up to the point of collision).

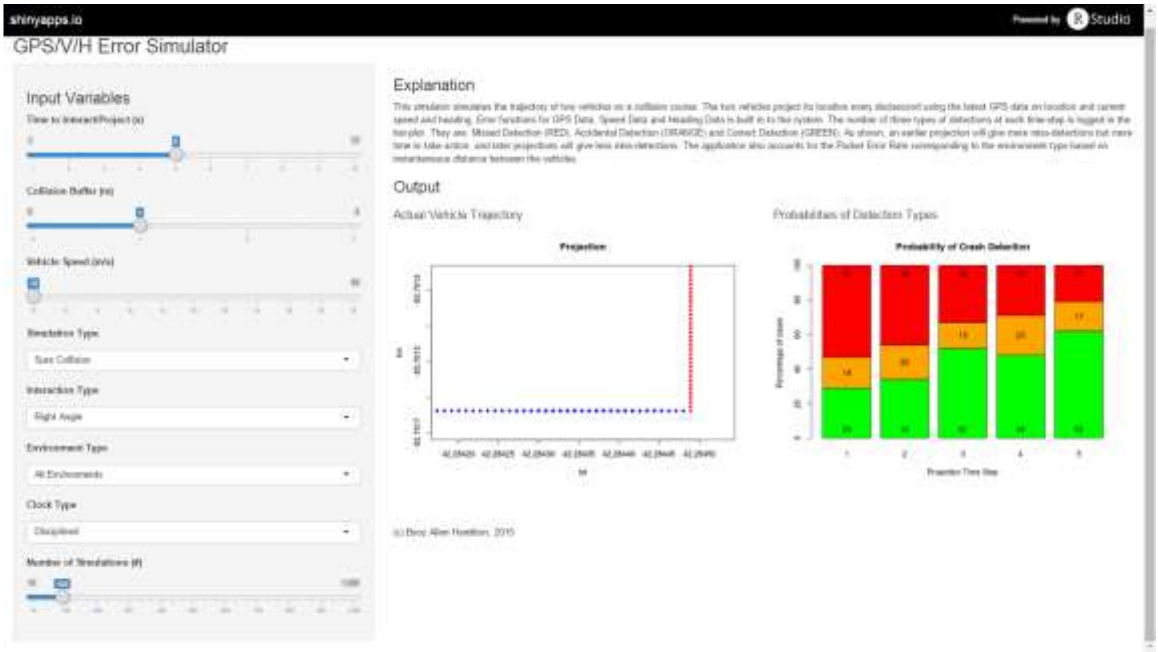
Once these inputs are set, the simulator uses fundamental equations of motion to generate two sets of trajectories - the ground truth (with zero error), and the projected trajectories using ground truth positions, as reference points, at each second. A comparison of these two sets of trajectories yield the aggregate change in the projected positions with respect to ground truth and thereby help determine the probabilities of misclassification of interaction. The pseudo-code on how the simulator works is given below along with a screenshot of the interactive R-program dashboard that lets users define and run the simulations.

Pseudocode:

```
1) Initialize vehicle positions, speed, yaw-rate, acceleration and heading, all of which are known values.
2) Generate "ground truth" positions for these vehicles assuming zero error at 1-second interval, using the initial position, speed, yaw-rate, acceleration and heading. Basic equations of motion is used at this step.
3) Perform the following steps for each pair of positions:
    a. Find the distance between the two vehicles.
    b. Compute the PER distribution for this distance in terms of mean and standard deviation for the given environmental scenario.
    c. Assume a projection interval, in seconds, that is equal to the time to collision from that position.
    d. Perform the following steps (i to iv) for each simulation:
        i. Make a projection based on the latest information on the vehicle positions for a percentage of cases characterized by (100 minus assumed PER for this time-step).
        ii. For rest of the cases, make a projection based on the vehicle positions at last time-step.
        iii. Making a projection:
            • Incorporate error from the corresponding normal distributions of latitude, longitude, speed, yaw rate, acceleration and heading.
            • Make projections for each deci-second in the remaining projection interval for both vehicles using their corresponding erroneous parameters.
            • For each pair of projections, log the cases with correct classification, accidental correct classification, and missed detection based on the temporal and spatial distribution of the projected positions.
        iv. Log the percentage classifications of each detection type.
4) Plot the percentage of classification of detection types for each projection interval.
```

For the sure-collision scenario, three types of detection are tracked including correct, accidental, and missed detection since the accidental detection also accounts for making the correct decision by the driver (or a driving system). However, for the near-miss scenario, the types of detection are assumed binary: correct detection (no collision is detected) and missed detection (collision is detected).

Figure 134: Interactive R-Program Simulator (Source: USDOT)



GPS/V/H Error Simulator

Input Variables

Time to Interact/Project (s)

Collision Buffer (m)

Vehicle Speed (m/s)

Simulation Type: Sure Collision

Interaction Type: Right Angle

Environment Type: All Environments

Clock Type: Disciplined

Number of Simulations (#)

Explanation

This simulator simulates the trajectory of two vehicles on a collision course. The two vehicles project its location every decisecond using the latest GPS data on location and current speed and heading. Error functions for GPS Data, Speed Data and Heading Data is built in to the system. The number of three types of detections at each time-step is logged in the bar-plot. They are: Missed Detection (RED), Accidental Detection (ORANGE) and Correct Detection (GREEN). As shown, an earlier projection will give more miss-detections but more time to take action, and later projections will give less miss-detections. The application also accounts for the Packet Error Rate corresponding to the environment type based on instantaneous distance between the vehicles.

Output

Actual Vehicle Trajectory

Probabilities of Detection Types

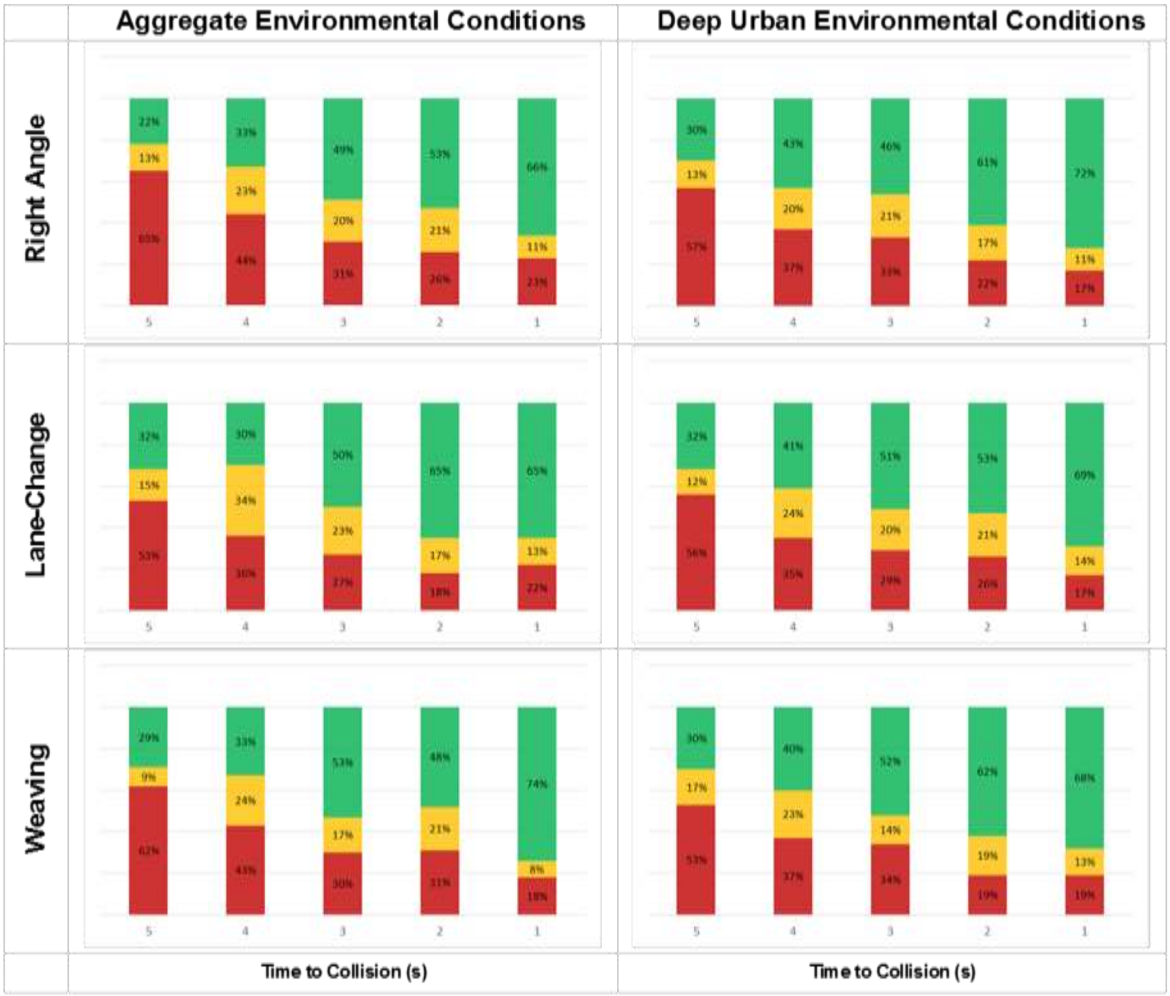
(c) Booz Allen Hamilton, 2015

Snapshot of Results

A set of sample results for the sure collision case are shown in

Figure 135 under six different conditions. The three interaction types used were right-angle collision, lane-change collision, and weaving collision. The two environmental conditions used were an aggregate environmental condition which averages the PER distributions under various types of roadway geometries, and the deep urban conditions, which show the highest PER distributions owing to the dense roadway network and tall buildings. At each time-step, 100 simulations were performed that randomly picked error measure for different components of the BSM for that instant and used it to extrapolate the vehicle profile for the next few time-steps. These extrapolated profiles were used to classify the possible future interaction as (a) correct collision, denoted by green in the plots, (b) no-collision, denoted by red and (c) accidental correct collision, denoted by orange.

Figure 135: Sample Results from Six Conditions (Source: USDOT)



As shown in the plots, the deep urban environmental which is subjected to the highest PER and therefore, the probability of correctly detecting collisions is less when compared to other environments. Lane-change and weaving interactions yielded higher probabilities of detecting a collision as compared with a right angle interaction. This is largely due to the fact that when changing a lane or weaving these vehicles are much closer than when they are on right-angle collision path. The closer the vehicles are moving, the higher the chance of collision detection which includes both green and orange bars (on the other hand, the closer they are, the less time the system has to effectively warn the driver as well).

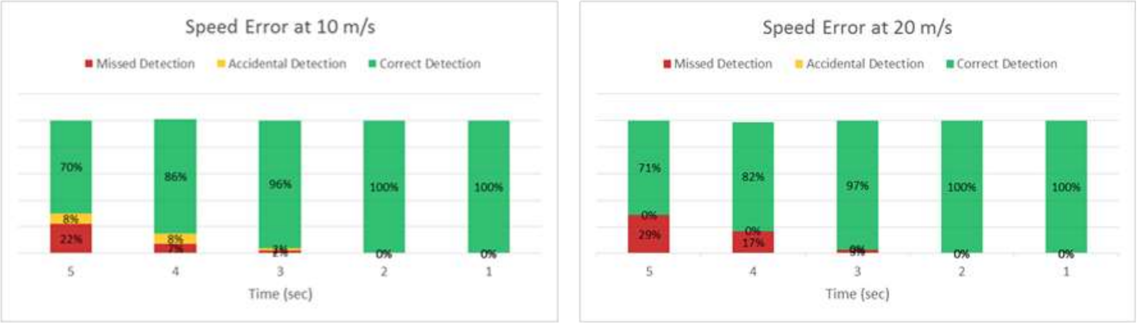
11.1.3.1 *Sure Collision Case:*

Under the sure collision case, the vehicles are set to collide at some fixed future point. The simulation tool integrates two levels of data for these vehicles – the ground truth trajectories and the trajectories computed using the generated BSM data from both vehicles. The simulation analysis for the two vehicles that are on a collision course assumes that these vehicles remain at their initial speed and heading. The simulator also incorporates error terms for the various sources of error that influence data elements in the Basic Safety Message. Even though the impact of these errors may seem to be negligible when considered individually, when combined their impact is more noticeable, particularly when these errors are propagated with their corresponding data elements when determining future positions. The simulator finally projects these vehicle positions to temporal and spatial future space to identify any misclassification of interactions.

In order to identify the effect of individual error terms in the misclassification of interactions, a series of sensitivity analyses was conducted. Specifically the error values used in this analysis are taken from an aggregate of real world GPS measurements obtained from *In-Vehicle Safety Device for Safety Pilot Model Deployment Test Reports, 2013.* Each sensitivity test included 1000 simulation runs and compares the effect of *individual* error terms for two vehicles moving at a right-angle with a Time-to-Collision (TTC) of 5 seconds. The analyses was done for both 10 and 20 m/s vehicle speeds and 1 meter collision buffer.

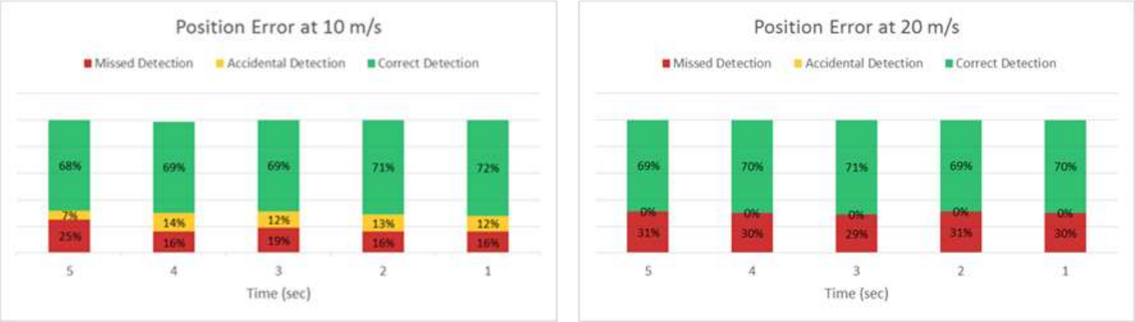
Sensitivity to Individual Errors in Speed:
The following plots show the variation of three types of detection of interaction type at two different vehicle speeds when there are errors in the reported vehicle speed. The reported errors are taken from real-world tests on test tracks from *In-Vehicle Safety Device for Safety Pilot Model Deployment Test Reports, 2013* as described previously and follows a normal distribution with a variance of 0.13 m/s. Even with individual speed errors of this magnitude, correct classification of the hazard was still above 90% at 3 seconds from collision. This analysis also included assessment of the sensitivity of speed errors in contributing to the overall probability of misclassification. This was done by assuming different levels of speed errors and assessing the resulting misclassification probability. Figure 136 shows this distribution where speed error variance is shown on X-axis and the probability of misclassification is shown on Y-axis. Please note that the sensitivity analysis was only done for 10 m/s speed.

Figure 136: Probability of Misclassification When Speed Errors are Present (Source: USDOT)



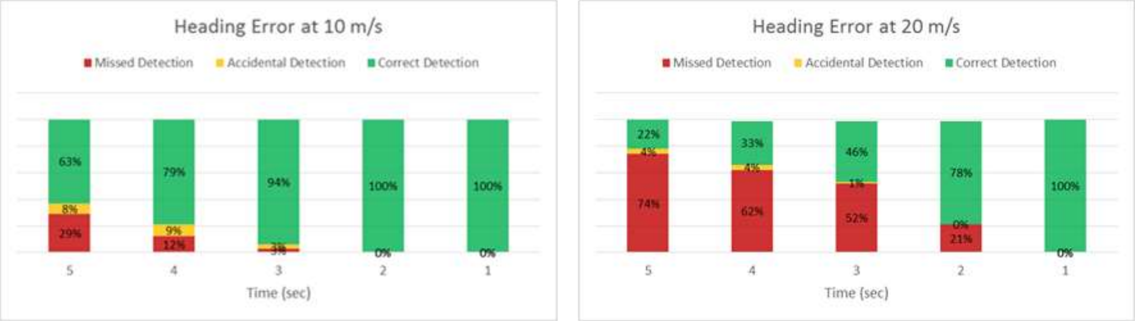
Sensitivity to Individual Errors in Position:
The following plots show the detection types when there are errors in the reported vehicle positions (latitude and longitude) when the two vehicles are on a right angle collision course. The reported errors are taken from real-world tests on test tracks and follows a normal distribution with a variance of 0.53 meters. To add to this analysis, a sensitivity analysis of positional errors with respect to probability of misclassification is done.
Figure 137 shows this distribution where positional error variance is shown on X-axis and the probability of misclassification is shown on Y-axis.

Figure 137: Probability of Misclassification When Positional Errors are Present (Source: USDOT)



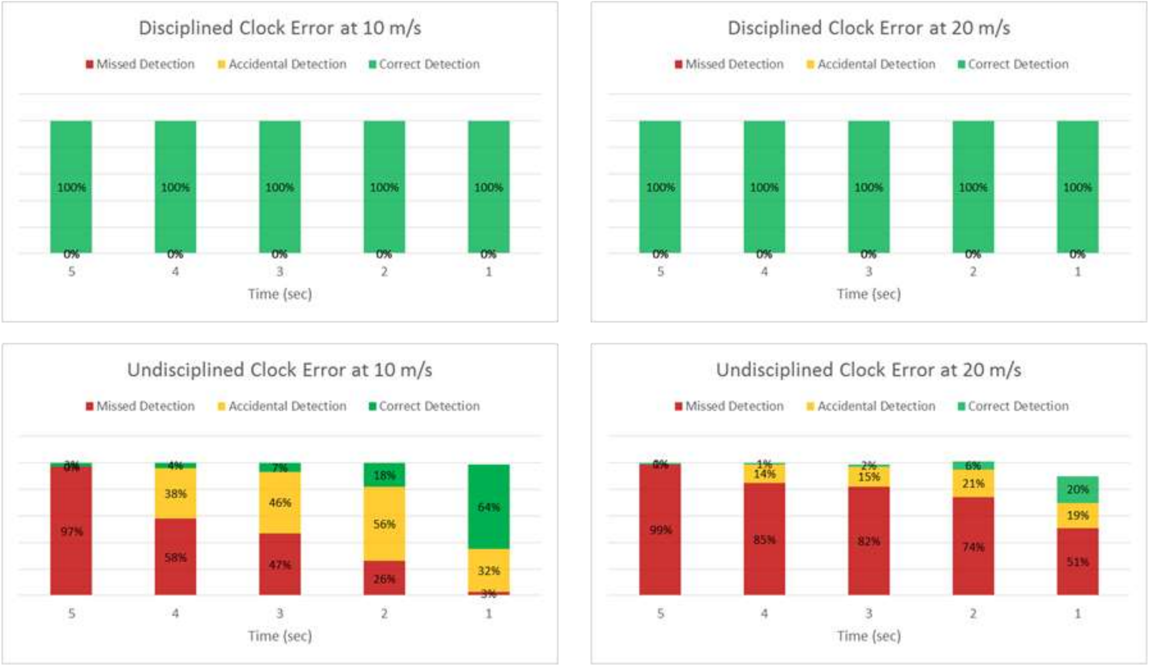
Sensitivity to Individual Errors in Heading:
The following plots demonstrate how errors in heading can affect the collision detection of two vehicles. This analyses used real-world GPS values under test conditions and follows a normal distribution with a variance of 0.81 degrees. To add to this analysis, a sensitivity analysis of heading errors with respect to probability of misclassification is done. Figure 138 shows this distribution where heading error variance is shown on X-axis and the probability of misclassification is shown on Y-axis.

Figure 138: Probability of Misclassification When Heading Errors are Present (Source: USDOT)



Sensitivity to Individual Clock Errors:
DSRC clocks also have inherent time sync errors and the data collected from this project's Time Sync and Stability Testing was utilized in comparing the misclassification when disciplined and undisciplined clocks are used. Clearly the effect of disciplined clocks are negligible and undisciplined clocks result in major misclassification errors. To add to this analysis, a sensitivity analysis of clock-sync errors with respect to probability of misclassification is done. Figure 139 shows this distribution where clock-sync error variance is shown on X-axis and the probability of misclassification is shown on Y-axis.

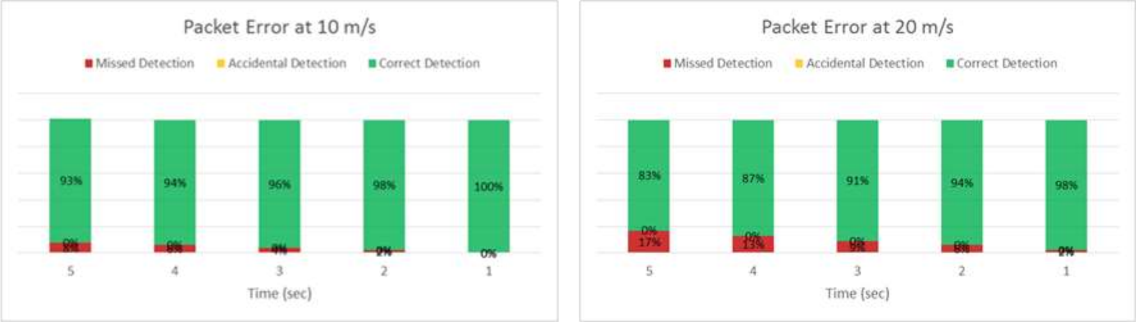
Figure 139: Probability of Misclassification When Clock Errors are Present (Source: USDOT)



Sensitivity to only Packet Error Rates:

Packet error rates are inherent to communication mediums and depends on the distance between the source and the sink as well as the wireless communication medium. The packet error analysis uses data from communication range tests and result in minor misclassification of interaction types which is proportional to the speed of vehicles.

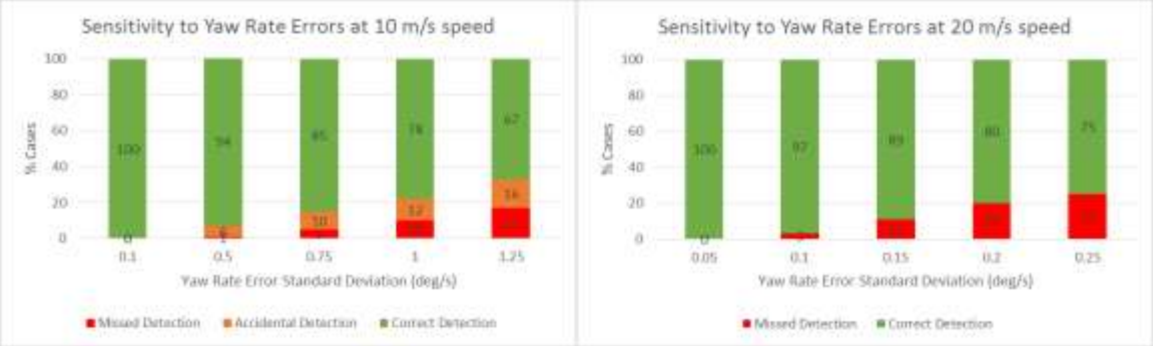
Figure 140: Probability of Misclassification in the Presence of Packet Errors (Source: USDOT)



Sensitivity to Yaw-Rate Errors

In order to assess the sensitivity of the simulations to yaw-rate errors, the vehicle trajectories were defined to be curved. For simplicity, a constant yaw rate value is used in the simulations. The error values were simulated using a Monte Carlo framework which attributes the yaw-rate with some degree of error in each projection time-step. Instead of using field-observed values, yaw-rate errors were assumed to follow a normal distribution with zero mean and a known standard deviation. The standard deviation value was varied to compute the effect of this error on the probability of misclassification. Figure 141 shows the probability of misclassification as a function of yaw rate errors. These results shows the percentage of cases where a detection was missed or accidentally made or correctly made at 3 seconds from collision when two vehicle trajectories were simulated at different speeds. A constant yaw rate of 3 deg/s was used in one of the vehicles and yaw rate errors were added from a normal distribution.

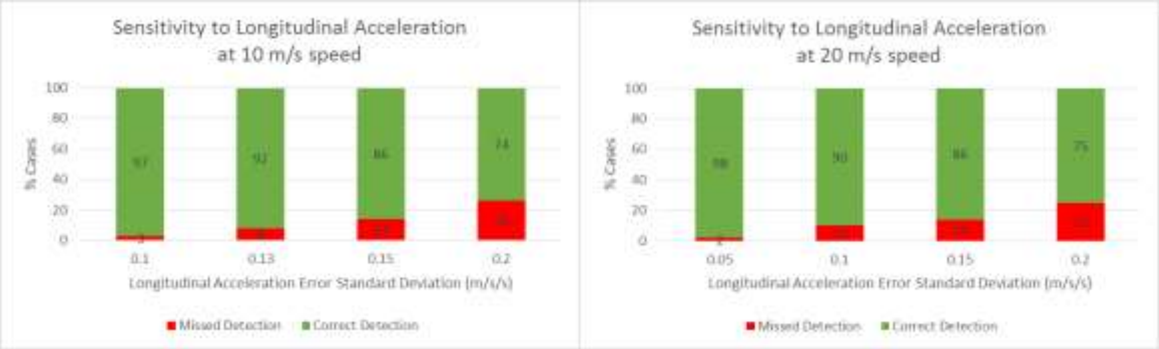
Figure 141: Sensitivity of Collision Detection to Yaw Rate Errors (Source: USDOT)



Sensitivity to Longitudinal Acceleration Errors

Similar analysis was done for longitudinal acceleration errors were the trajectories of vehicles were set on an acceleration course with constant rate of acceleration. The projections were made assuming an error in the reported acceleration values. The errors were derived from a normal distribution with zero mean and a known standard deviation. Figure 142 shows the probability of correctly or incorrectly detecting a collision in the presence of acceleration errors. As shown, the effect of having acceleration errors are independent of the speed of travel. For this analysis, two vehicles on a straight, right angle collision course were simulated with one vehicle accelerating at a constant rate of 1 m/s/s.

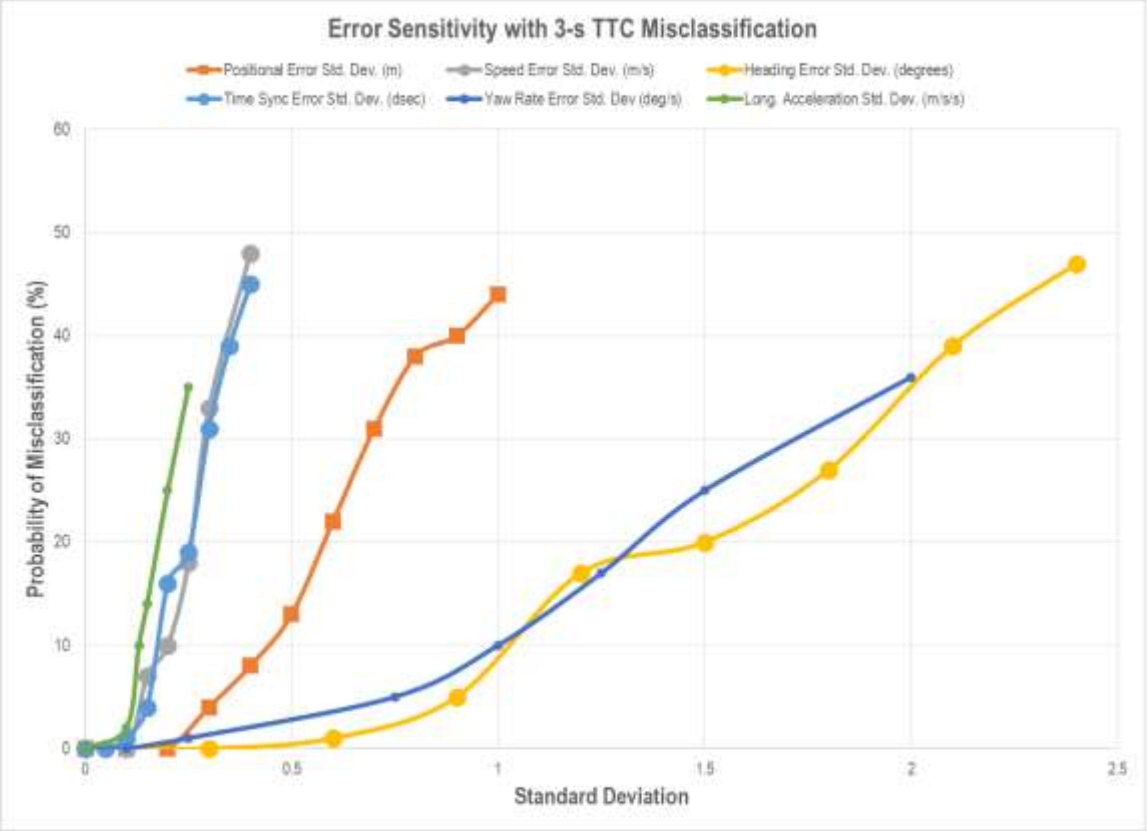
Figure 142: Sensitivity of Collision Detection to Longitudinal Acceleration Errors (Source: USDOT)



Overall Sensitivity:

While the previous sub-sections defined how individual observed values of sensor errors contribute to the misclassification of future events (crashes) using projected BSM messages, this subsection analyzes individual error sensitivities as they relate to the misclassification. In this exercise, individual error values were simulated using aforementioned Monte Carlo framework. Instead of using field-observed values or aggregated device values, specific values of assumed standard deviations were used when generating message sets so that its sensitivity can be assessed. This experiment was repeated for positional, speed, heading, and time-sync errors as shown in
Figure 143.

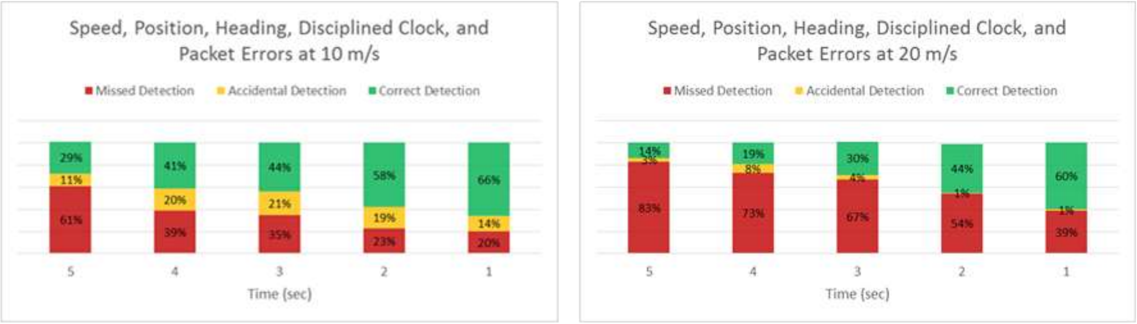
Figure 143: Error Sensitivity of Parameters with 3-second Time to Collision (Source: USDOT)



Combination of Errors:

In most cases, there will be a combination of all these errors and not only one type of error. In the following plots, the effect of these five types of errors are demonstrated for two vehicles heading toward each other at right angle. As shown, the probability of correct detection increases as TTC reduces. The tradeoff between detector errors and the available time to take action will be used to test the reliability of sensors that feed into the BSM generation.

Figure 144: Probability of Misclassification in the Presence of Speed, Position, Heading, Clock, and Packet Errors (Source: USDOT)

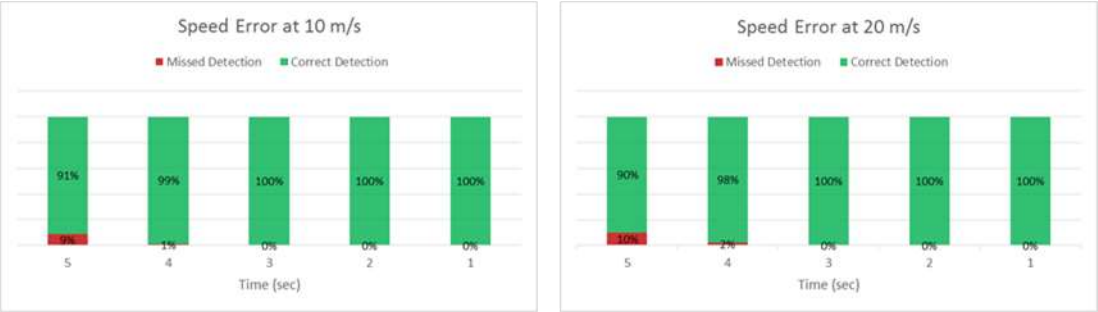


11.1.3.2 Near-miss Case:

Similar to sure-collision scenarios being misclassified as a near-miss and resulting in no hazard warning for the driver, near-miss situations could be misclassified as sure-collision and can initiate wrongful hazard warnings. Therefore, error sensitivity analyses are done on a near-miss case similar to the previous scenarios. Each sensitivity tests included 1000 simulation runs using right-angle movement of two vehicles at constant and equal speeds. The ground truth trajectory of vehicles are set up such that they will miss each other on a temporal and spatial plane by a near-miss. These analyses compare the effect of individual error terms for the two vehicles with a Time-to-Near-Collision of 5 seconds. The analyses were done for both 10 and 20 m/s vehicle speeds and a 2 meter collision buffer. Contrary to the sure-collision case, there are only two types of interaction classification here: Missed Detection (which is when the vehicles are classified to crash into each other) and Correct Detection (which is when the vehicles are classified to miss each other). Please note that for this analysis the distribution of errors in speed, heading, position, clock errors, and packet error rates are aggregated from a series of real-world tests done as a part of *In-Vehicle Safety Device for Safety Pilot Model Deployment Test Reports, 2013 (the same errors as in the sure collision case).*

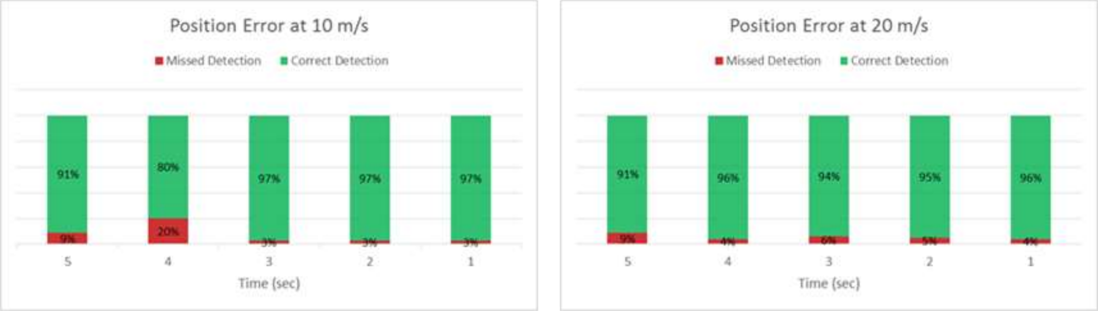
Sensitivity to Errors in Speed:
As shown below, the effect of speed errors on the classification is minimal with more than 90 percent of cases being classified correctly.

Figure 145: Probability of Misclassification in the Presence of Speed Errors (Source: USDOT)



Sensitivity to Errors in Position:
Positional errors have a greater impact on the probability of misclassification than speed errors as demonstrated in the following plots.

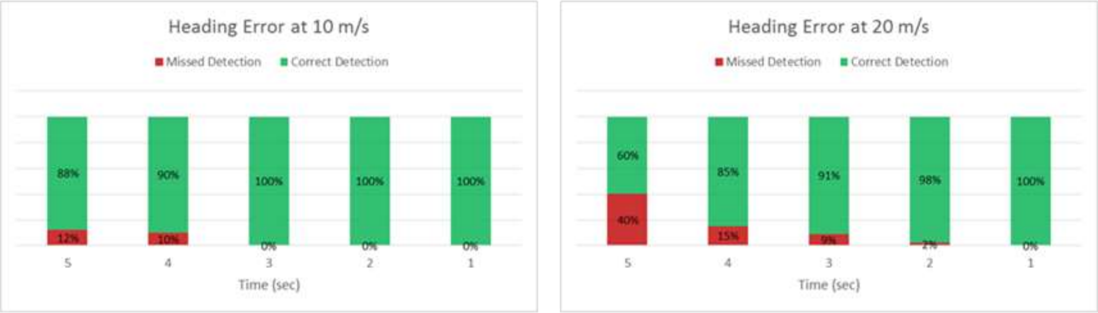
Figure 146: Probability of Misclassification in the Presence of Positional Errors (Source: USDOT)



Sensitivity to Errors in Heading:

Heading errors can cause misclassifications at higher speeds than lower speeds. As shown in the plots below, at 20 m/s, the misclassification of a near-miss for a 5-second time-to-near-collision is 40 percent versus a 12 percent at 10 m/s.

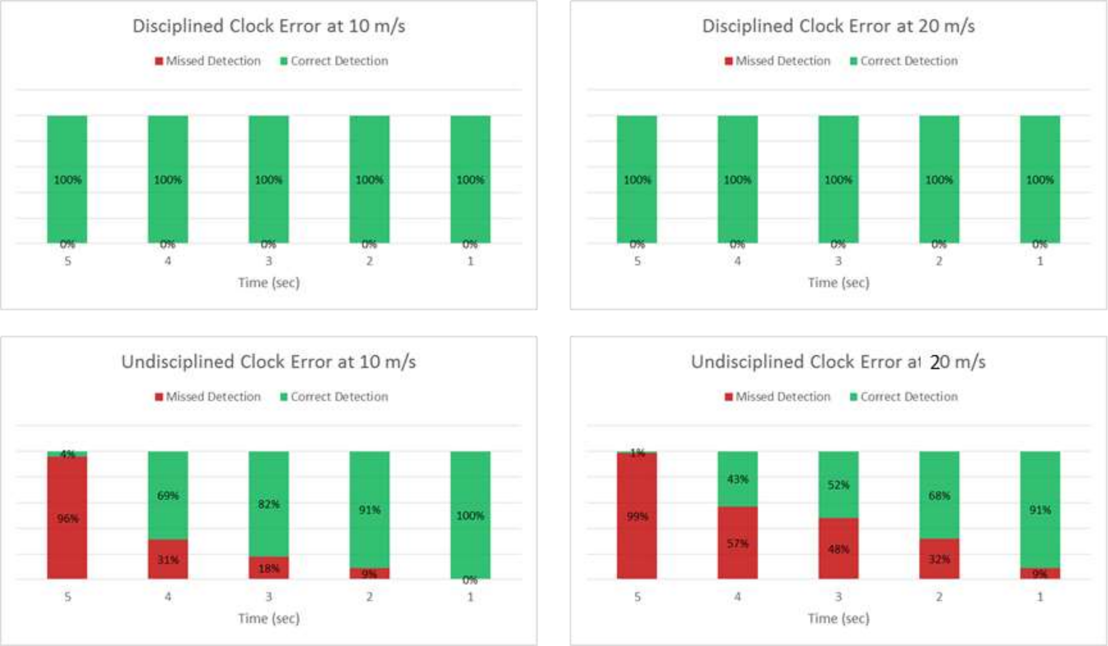
Figure 147: Probability of Misclassification in the Presence of Heading Errors (Source: USDOT)



Sensitivity to Clock Errors:

As shown in the following plots, the disciplined clock errors cause less than negligible misclassification on the near-miss case whereas the undisciplined clocks produce more than 90 percent misclassifications at 5-seconds.

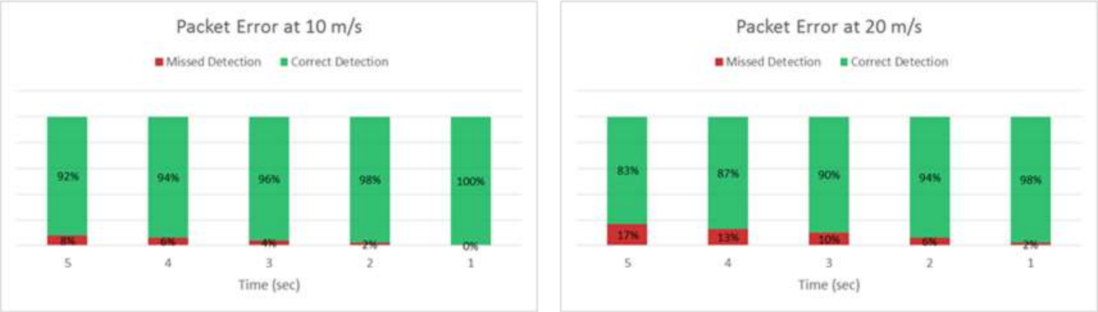
Figure 148: Probability of Misclassification in the Presence of Clock Errors (Source: USDOT)



Sensitivity to Packet Error Rates:

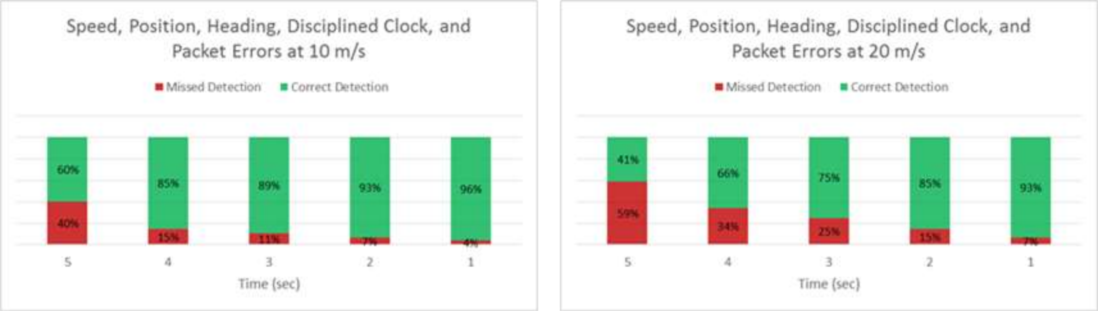
The following plots show the effect of packet error rates on the probability of misclassification under the two vehicle speeds.

Figure 149: Probability of Misclassification in the Presence of Packet Errors (Source: USDOT)



Combination of Errors:
In most cases, there will be a combination of all these errors and not only one type of error. In the following plots, the effect of these five types of errors are demonstrated for two vehicles heading against each other at a right angle in what would result as a near miss. As shown, the probability of correct detection increases as Time-to-Near-Collision reduces. The tradeoff between detector errors and the available time to take action will be used to test the reliability of sensors that feed into BSM generation.

Figure 150: Probability of Misclassification in the Presence of Speed, Positional, Heading, Clock, and Packet Errors (Source: USDOT)



11.1.4 Deriving Error Distributions

There are three types of errors that are included in this series of analyses:

1) GPS based error.
2) Error due to DSRC as the communication medium, which manifests as PER.
3) DSRC-radio error, which predominantly manifests itself as time-jitter error.

11.1.4.1 ***GPS Based Error***

GPS based error impact position (latitude, longitude), speed, and heading. To incorporate GPS errors in the referenced simulation environment the applied method involved obtaining real-world error measurements and subsequently developing a comprehensive mathematical representation of these errors. This mathematical representation will then be appropriately incorporated into the simulation environment. The set of real world, GPS error measurements were obtained from *In-Vehicle Safety Device for Safety Pilot Model Deployment Test Reports, 2013*. The report details the testing procedure and results of evaluating a number of devices to determine the accuracy with which they capture GPS base measurements. During the evaluation of these devices criteria for each relevant measurement was established to determine is a device ought to be used CV study efforts.

The data that were used to inform error estimates for this effort were only obtained from devices that satisfied the pre-established criteria for the measure being studied here. The data in this report was extracted from a series of images that captured error measurements in latitude and longitude, speed, and heading. Table 43 summarizes the number of images and the corresponding number of data points that were used to support the capture of errors in GPS based measurements.

Table 43: Number of Images and Corresponding Number of Data Points used to Capture Error in GPS Based Measures

Number of…	Speed	Heading	Position
Sample Plots	40	31	41
Total Extracted Data Points	44,941	68,715	7,690

A sample of these images are presented in Figure 151, Figure 152, and Figure 153, illustrating error measurements in position, speed, and heading respectively.

Figure 151: Raw Device Testing Data of Latitude and Longitude Measurement (Source: USDOT)

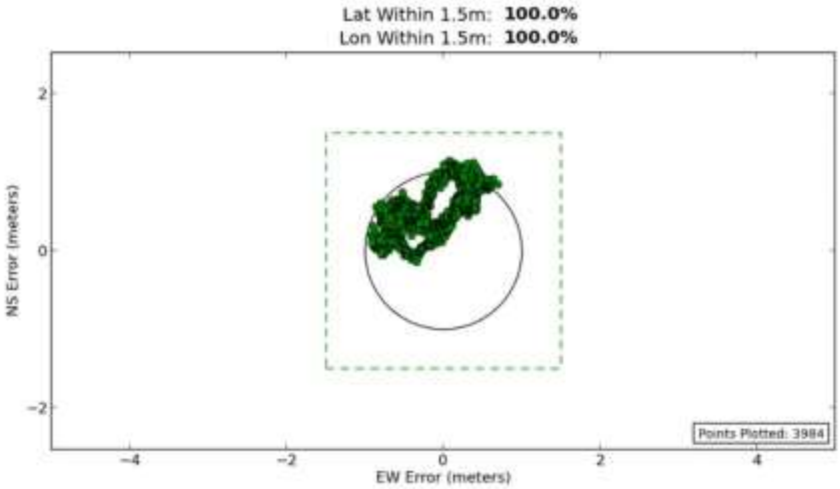


Figure 152: Raw Device Testing Data of Speed Measurement (Source: USDOT)

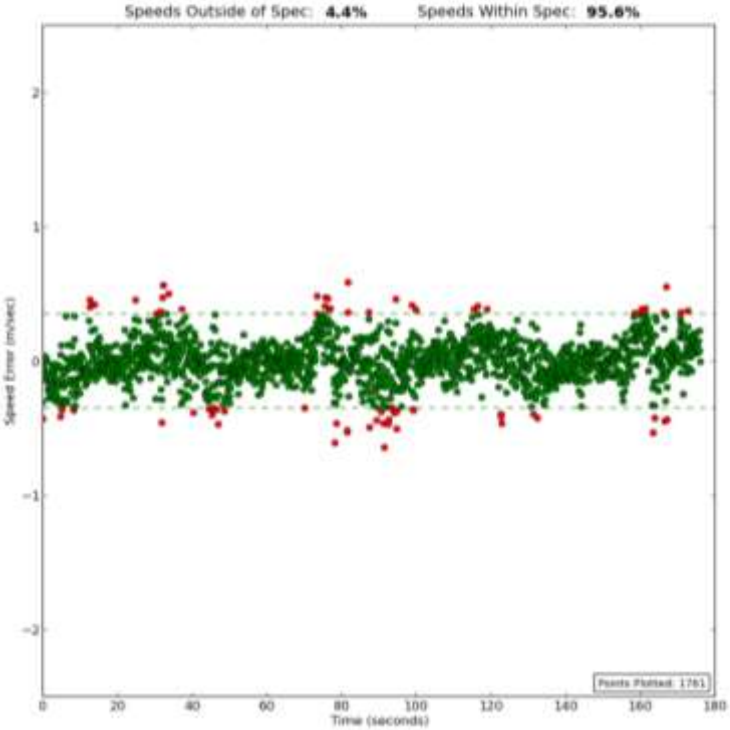
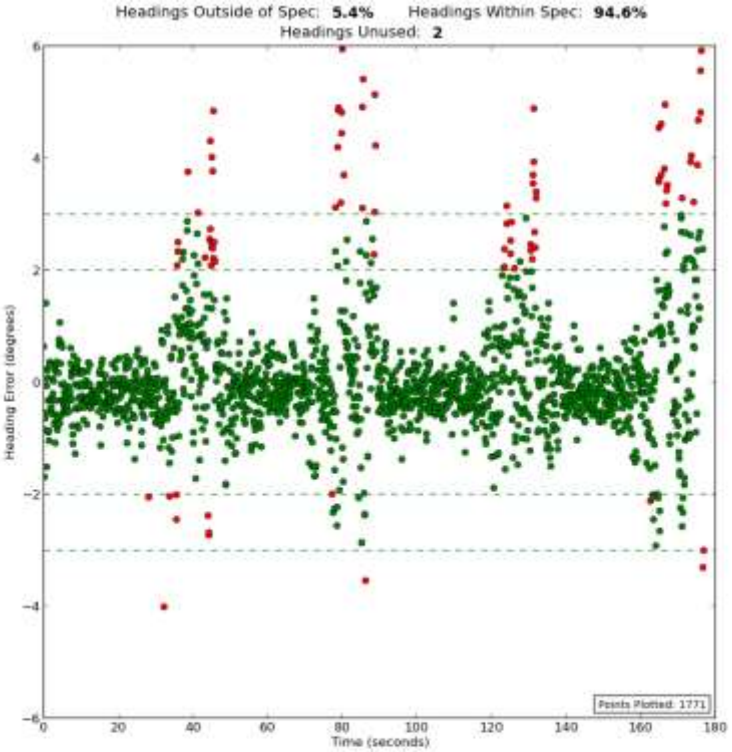
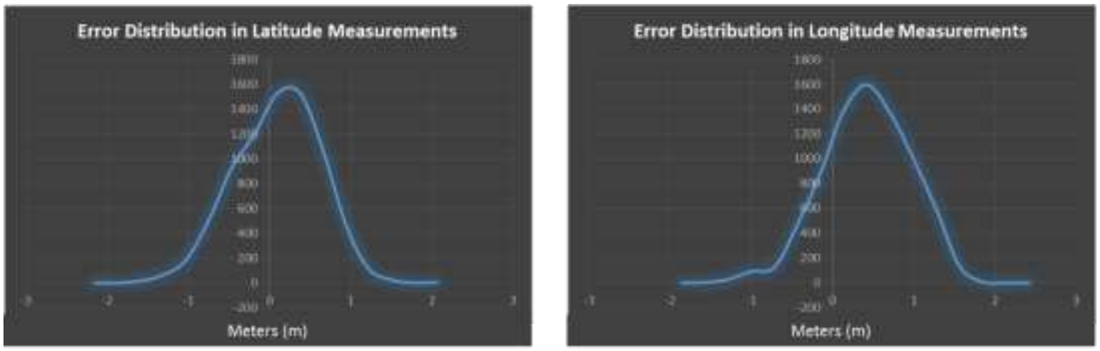


Figure 153: Raw Device Testing Data of Heading Measurement (Source: USDOT)



These images were digitized and values from the data points were extracted to create error distributions for each measurement. See Figure 154 and Figure 155.

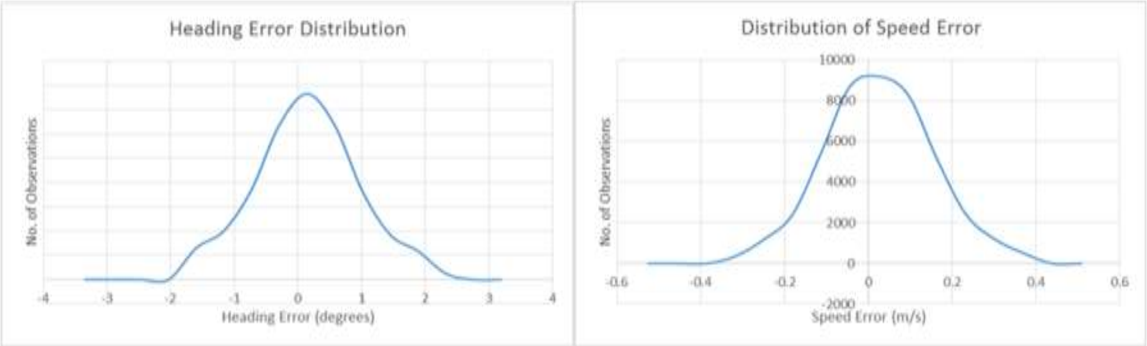
Figure 154: Empirically Derived Error Distribution in Latitude (a) and Longitude (b) (Source: USDOT)



(a)

(b)

Figure 155: Empirically Derived Error Distribution in Heading (a) and Speed (b) (Source: USDOT)



(a)

(b)

These error distributions were then mathematically represented to support implementation in the simulation environment. The above distributions resembled normal distributions, and as such, represented this assumption with values for mean and standard deviation.

Table 44: Empirically Derived Normal Distribution Parameters for Errors in GPS based Measures

Parameter:	Latitude	Longitude	Heading	Speed
Mean	-0.04661 m	0.28039 m	-0.074009 deg	-0.008546 m/s
Std. Dev.	0.525815 m	0.53403 m	0.8162397 deg	0.1291989 m/s

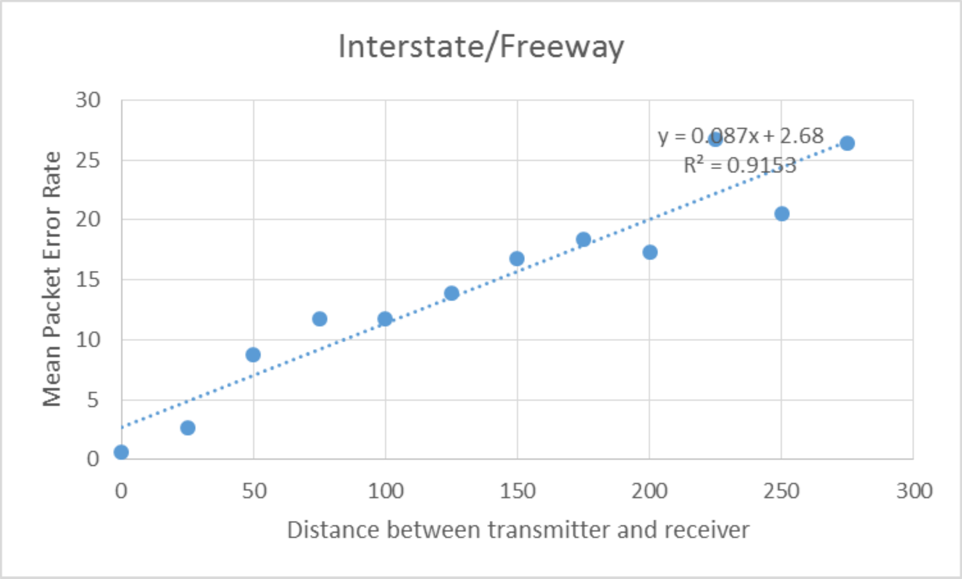
To implement these errors a randomly selected value from the corresponding normal distribution, *N(μ, σ)* is taken into account when projecting a set of these measures. Appropriately incorporating these errors terms with the corresponding equation of motion determines a vehicle's estimated location per a given time horizon.

This method of using empirical data to form distributions that can be represented in a simulated environment provides a valid opportunity to understand traffic safety implications given erroneous vehicle projections due to GPS based errors.

11.1.4.2 ***Packet Error Rate***

To model the traffic safety impact of PER, a similar method was conducted as in the case of incorporating GPS based errors. This method involved mathematically modeling empirical data and subsequently incorporating the model into a simulation environment. PERs were obtained from *Vehicle-to-Vehicle Safety System and Vehicle Build for Safety Pilot (V2V-SP) Final Report, Volume 2 of 2: Performance Testing, CAMP, 2014* for seven different environment types. This report provided the mean and standard deviation for PER in 25m bins, from 0m to 275m (Note: only observations up to 150m were considered for the Deep Urban environment due to a limited sample size beyond this distance). Scatter plots of mean (PER) versus distance, for each environment type, were developed, and a trend line, based on these data points, were calculated. These trend lines were then used to calculate PER at the separation distance between the vehicles at each time step in the simulation. See Figure 156 for a sample PER versus distance plot, with trend line information.

Figure 156: Sample PER vs. Distance Plot used to incorporate PER in the Simulation Environment (Source: USDOT)



11.1.4.3 ***Time Synchronization / Time Jitter Errors***

To capture traffic safety impact due to time jitter error, data from an undisciplined and a disciplined clock were used. Time jitter errors were obtained from this project's Time Sync and Stability Testing. For an undisciplined clock data, differences between the PPS timestamp and message submission timestamp were obtained for 2,247 instances across three experimental runs with the Supplier A units. For the disciplined clock data, the difference between the precision clock timestamp and the local clock timestamp was obtained for 7,265 instances across one 145 minute experimental run with a

Supplier B unit. The team introduced these error observations into the simulation by generating a random error deviate for time at each simulation step. Each random deviate was derived from normal distributions with parameters (mean and standard deviation) pulled from the empirical datasets. Then, each instance of time error was converted to a positional error using the following equation, derived from basic Newtonian equations of motion:

$$\delta x(t_1) = x(t_1) - x_1$$
$$\delta x(t_1) = x_0 + v\big(t_1 - (t_0 + \delta t)\big) - x_1$$
$$\delta x(t_1) = x_0 + vt_1 - vt_0 + v\delta t - x_1$$
$$\delta x(t_1) = x_0 + x_1 - x_0 + v\delta t - x_1$$
$$\delta x(t_1) = v\delta t$$

where $\delta x(t_1)$ is the positional error due to errors in time
$x(t_1)$ is the perceived position of the vehicle at t_1 given the error in time reporting;
x_1 is the actual position of the vehicle at t_1;
x_0 is the actual position of the vehicle at t_0;
v is the reported vehicle speed (which includes any speed errors);
t_1 is the time at the 1 time-unit;
t_0 is the time at the 0 time-unit; and
δt is the error in time reporting

11.1.5 Reliability Testing

While the previous subsections talked about the effect of errors found in real-world sensors on probabilities of misclassification of vehicle-to-vehicle interactions, this project also used the simulator to develop a framework to determine the error tolerances allowable to achieve a particular level of performance in correctly classifying vehicle interactions. Each measure in the Basic Safety Message may have errors impacting the accuracy of the measures. These errors in turn impact the safety of vehicles, which runs counter to the purpose of BSMs – whose intentions are to enhance safety by providing advanced (accurate) information to nearby vehicles. In this subsection, the team assessed individual error tolerance levels for a predefined performance criterion as well as discuss combined error tolerances levels. Currently, the performance criterion is defined as correct vehicle interaction classifications 90% of the time, 3 seconds before collision.

This criterion is subject to change as additional research is needed to develop a comprehensive understanding of the implication of the current value of the parameters of this criterion. The parameter values were born out of a combination of heuristics and a few overarching traffic engineering and driver reaction principles. An accuracy rate of 90% can be considered to provide enough reliability in terms of collision avoidance systems assuming that these devices would only be used at an advisory level and not a control level. However, the team is very cognizant that this level of accuracy may not be sufficient for a vehicle based safety system. As such, the parameter value for this criterion is mainly meant to illustrate the level of error tolerance that is required to achieve a relatively high level of correct vehicle interaction classifications. As for the “3 seconds before collision” component of this criterion, this is primarily geared towards providing sufficient time for drivers to be alerted, react, and perform the necessary escaped maneuver to avoid a collision (i.e., stopping sight distance). While 3 seconds may be sufficient time to avoid most collision scenarios, it is also known that there are cases in which 3 seconds is not enough time to react and maneuver a vehicle to avoid a collision scenario such as a high-speed head-on collision. However, for this exploratory exercise, a 3 second parameter value will sufficiently support insights into allowable error tolerances to avoid a collision 3 seconds away.

11.1.5.1 Individual Error Tolerance

There are seven types of errors being studied in this section, including positional, speed, heading, time, yaw-rate, longitudinal acceleration, and packet errors. While these errors seldom occur individually, the team analyzed the individual impact on the probability of misclassification to identify stronger and weaker correlations. The simulator was used to develop reliability measures or tolerable errors in these parameters to achieve 90 percent reliability in correct classifications at 3 second Time to Collision. Please note that this section uses 1000 simulation runs, vehicles at 10m/s and 20m/s speeds, 1 meter collision buffer, and a right-angle approach. The tolerance values provided are standard deviations from zero error and should be interpreted that at least 95 percent of the reported values must fall within an envelope of twice this standard deviation.

The tolerable values of errors are given in the following table:

Table 45: Individual Error Tolerance Variance for 10 m/s and 20 m/s Vehicle Speeds

Vehicle Speed:	10 m/s	20 m/s
Positional Error	0.43 m	0.37 m
Speed Error	0.17 m/s	0.15 m/s
Heading Error	0.9 degrees	0.44 degrees
Time Error	17 ms	8 ms
Yaw Rate Error	0.8 deg/s	0.15 deg/s
Longitudinal Acceleration	0.14 m/s/s	0.13 m/s/s
Packet Error Rate	10 percent	10 percent

11.1.5.2 Combined Error Tolerance

The previous subsection describes how individual error tolerance values are generated based on a fixed reliability scale to provide crash avoidance warnings to drivers. These values are applicable to a right-angle collision course assuming all the information required to take driver action comes from the BSM messages (which are then projected into the future to compute the trajectories of vehicles). However, in the real-world, individual errors seldom exist. The combination of errors from a single or multiple sensors will add to the BSM generation components for DSRC devices. These errors are dependent on each other in an intricate way and is beyond the scope of this study. Therefore, the two sets in Table 46 provide “tolerable” errors that will have a probability of misclassification less than 10 percent at 3 seconds TTC. These examples are provided below:

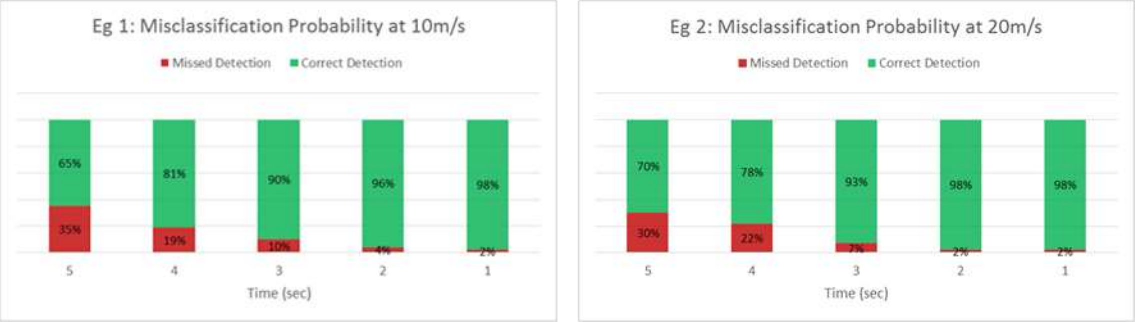
Table 46: Sample *Combined* Error Tolerance Level that Provides 90% Correct Classification, 3 Seconds before Collision

Parameter	Example 1	Example 2
Positional Error	0.2 m	0.15 m
Speed Error	0.15 m/s	0.11 m/s
Heading Error	0.2 degrees	0.15 degrees
Time Sync Error	2 ms	2 ms

Parameter	Example 1	Example 2
Yaw Rate Error	0.1 deg/s	0.05 deg/s
Longitudinal Acceleration	0.1 m/s/s	0.05 m/s/s
Packet Error Rate	2 %	2 %

It has to be noted that the values provided here are the standard deviations for the errors with a zero mean. As shown in Figure 157, the error values in Example 1 are good enough to provide 90 percent accuracy at 10 m/s. However, for 20 m/s speeds of vehicles, more stringent values in Example 2 should be used as the tolerable limits.

Figure 157: Misclassification Probability Histograms for Example 1's Set of Error Values (Source: USDOT)



Given that the PERs are very low when vehicles are close to each other (assuming 3-s time to collision), the errors in the other six parameters are divided in three different scenarios to get the 90% accuracy level. To enable this, the sensitivity of each parameter in contributing to errors is assessed and was used for building these scenarios. Sensitivity of the six parameters are given below:

1) Positional Error: 41% per meter of error
2) Speed: 95% per m/s of error
3) Heading: 16% per degree error
4) Time Jitter: 97% per decisecond error
5) Yaw Rate: 12% per deg/s error (for 10m/s) and 57% per deg/s (for 20 m/s)
6) Longitudinal Acceleration: 30% per m/s/s error

Given these sensitivity parameters, the following scenarios were assessed for error contributions from individual parameters:

1) Scenario 1 – Equal distribution of errors so that 10% allowable error is distributed equally for the six parameters.
2) Scenario 2 – 70 percent of allowable errors allocated to positional errors and the other 30 percent distributed among the remaining five parameters.
3) Scenario 3 – 70 percent of allowable errors allocated to positional errors and 1 percent allocated to time errors. The remaining 29 percent will be distributed among speed, heading, yaw rate and longitudinal acceleration.

Table 47: Comparison of different scenarios of recommended error tolerance values and the resulting percentage of misclassification

Parameter	Scenario 1	Scenario 2	Scenario 3
Position	0.082 m	0.342 m	0.325 m
Speed	0.035 m/s	0.012 m/s	0.015 m/s
Heading	0.021 deg	0.075 deg	0.1 deg
Time Jitter	34 ms	12 ms	2 ms
Yaw Rate	0.28 deg/s	0.1 deg/s	0.12 deg/s
Longitudinal Acceleration	0.11 m/s/s	0.04 m/s/s	0.04 m/s/s
% Misclassification at 3s from collision time			
Speed = 10 m/s	4%	10%	9%
Speed = 20 m/s	14%	12%	10%

11.1.5.3 Comparison with CAMP Recommendations

In order to compare the probabilities of misclassification of collision detection when CAMP recommended devices are used, specific error terms from the minimum recommended parametric values are used in the reliability framework. The CAMP recommended maximum errors are used as an input to the model as the standard deviation for the error terms, assuming that 95% of the values would be within the range. Misclassification of a sure collision for 3-seconds TTC are computed for individual errors and a combination of errors and is provided in the following table.

Table 48: Probability of Misclassification when CAMP-recommended Errors are Used

Error Parameter	CAMP Recommended Maximum Error	Percentage Misclassification at 3-seconds Time to Collision	
		10 m/s speed	20 m/s speed
Positional	1.5 m	32 %	55 %
Speed	0.35 m/s	17 %	21 %
Heading	2 to 3 degrees (based on speed)	12 %	68 %
Time Synchronization	1 ms	0 %	0 %
Longitudinal Acceleration	0.1 m/s/s	0 %	0 %
Yaw Rate	0.5 deg/s	17 %	25 %
Combined Errors		62 %	90 %

Table 49: Error Tolerance Recommendations

BSM Parameter	CAMP Recommended Maximum Error	BAH Recommended Maximum Error
Horizontal Position	1.5 m	0.32 m
Vertical Position	3 m	2 m (TBR)
Speed	0.35 m/s	0.015 m/s
Heading	2 to 3 deg	0.1 deg
Time	1 ms	2 ms
Longitudinal Acceleration	0.1 m/s/s	0.04 m/s/s
Yaw Rate	0.5 deg/s	0.12 deg/s

Table 49 demonstrates how CAMP recommendations compare with Booz Allen recommendations. Details on the calculations are provided in Chapter 4.

12 Appendix E. Full DSRC OBE Recommended Performance Requirements Matrix

This appendix contains the full DSRC OBE recommended performance requirements matrix aligned to supporting data collection tests, compliance testing approaches, etc. that is condensed within the body of the report.

Refer to file “FINAL_AppendixE_DSRC_Phase II Req Matrix” for the full DSRC OBE Recommended Performance Requirements Matrix.

Definitions and Purpose

ID (From Phase I) – This is the identification number for the requirement. Each ID is associated to a recommended compliance test in a different section. Some IDs are associated to data collection tests or simulations which provide justification for the requirement.

Requirement – This is the recommended requirement for DSRC operations and communications performance.

Use Case/Performance Need (From Phase I) – These are the system needs identified in Phase I of the project (those denoted with a letter/number combination) or identified during subsequent review. This provides a traceability to Phase I work and gives situational context for the related performance requirement.

DSRC Element -- This describes the physical area or software layer within a Connected Vehicle system that the performance requirement addresses. The categories are as follows:

- Roadway – e.g., hazard detection reliability, RSE interactions
- Vehicle – e.g., vehicle transmit power and antenna gain envelope
- System – e.g., message security, message plausibility
- Sub-system – e.g., message storage, message transmission/processing, operational failure detection
- Component – e.g., radio behavior, radio protocol

Operational Objective – This categorizes each performance requirement into one of three operational objectives:

- Communicate…with other devices
- Trust…the message (and its contents) from other devices
- Interpret…the message contents for use in safety applications

Associated Operational State – This describes the OBE operational state as defined Appendix B

Interoperability – This indicates whether this requirement is necessary for interoperable communication among OBEs

Sources – This identifies the source of information that justifies the requirements. This could be a source of information from within this project (i.e., specific test, simulation, or analysis) or outside of this project (i.e., existing standard, research, or report).

Aligned Data Collection Test/Simulation – This is a list of the tests and simulations that informed the associated requirement

Test/Simulation Results and Findings – This is a summary of the results and findings discovered during the tests and/or simulations

Compliance Approach – This describes the anticipated verification or compliance approach recommended for the requirement (Refer to Appendix C for alignment to requirement types and examples). The categories are as follows:

- Vehicle Level Test – Aligns to a “Roadway,” “Vehicle,” or “System” designation as the DSRC Element
- OBE/Component Level Test – Aligns to a “Sub-system,” or “Component” designation as the DSRC Element

Recommended Compliance Test Procedure – This provides the name of the recommended compliance test suite and test. Refer to Appendix G for full recommended compliance test procedures

Notes – This contains any additional notes and/or comments about the recommended requirement

13 Appendix F. Full DSRC OBE Security Inputs Analysis

Refer to file “FINAL_AppendixF_DSRC_PhaseII_Security_Inputs” for the full DSRC OBE Security Inputs Analysis.

14 Appendix G. Full Recommended Compliance Testing Procedures

This appendix contains the full recommended compliance testing procedures outlined within the body of the report. The appendix provides compliance test procedures in two main sections: OBE/component level tests and vehicle level tests. The team decided to split the test suites and tests into these two categories because there is a natural separation in the logical testing of requirements. While all OBE/component level tests could also be performed within an integrated vehicle, the vehicle should not affect performance or the outcome of the test. The team believes that the OBE/component level tests should be the responsibility of the OEM and its manufacturers, because the vehicle would not be able to pass the vehicle level tests without first meeting the OBE/component level tests. OEMs may also be responsible for ensuring compliance of the higher level requirements through vehicle testing, but NHTSA and any other regulatory entity could also perform these as a check, focusing on the vehicle level tests as they naturally subsume the OBE/component level tests.

Each requirement within the full requirements matrix embedded within Appendix E is aligned to at least one of the compliance tests in this appendix, except for the performance requirement on Intrusion Detection. As stated in Chapter 7, further intrusion detection research should be conducted before developing a test. Also as with the majority of objectives and Security Functional Requirements (SFRs) specified, existing security testing labs would have the required expertise to test intrusion vulnerabilities.

OBE/Component Level Tests

This section outlines OBE/component level test procedures. The OBE/component level tests are comprised of three test suites: storage, BSM transmission/processing, and failure detection. While a Standards Compliance test suite is seen in the OBE/Component Level test summary, the team did not create detailed test procedures due to the large level of effort required as the test procedures would likely be hundreds of pages. Based on discussions with industry organizations and other USDOT project areas, the team understands that foundational standards testing procedure development is covered by existing efforts. Any OBE and vehicle would be compliant with these standards by default when passing the Vehicle Level tests. The BSM Transmission and Processing test suite verifies the generation, transmission, and processing of BSMs under different strategies and scenarios. The Storage test suite focuses on the trust store storage capability and misbehavior report storage ability of the OBE. The scope of the storage test suite includes verifying that the OBE can store specific elements in the proper format and delete the oldest misbehavior report when storage capacity is reached. Finally, the Failure Detection test suite is comprised of the following tests: start-up failure and operational failure detection. These tests aim to verify that the OBE can identify failures that will prohibit the transmission of BSMs during start-up and operations.

The following sections present each test suite and associated compliance tests procedures in greater detail.

14.1.1 Standard Compliance Test Suite

While the team did not develop compliance test procedures for existing standards due to existing efforts by standards work groups, industry, and government, the objective of a standards compliance test suite would be to ensure an OBE and its components are compliant with the following industry standards: IEEE 1609 suite, IEEE 802.11, SAE J2735, and SAE J2945/1. The standards compliance test suite would most likely be comprised of three test categories, one for each family of standards: IEEE 1609 Suite Compliance, IEEE 802.11 Compliance, and SAE J2735/J2945 Compliance. The objective of the IEEE 1609 suite test would be to verify that the OBE adheres to all requirements under IEEE 1609. The objective of the IEEE 802.11 test would be to verify that the OBE adheres to all requirements under IEEE 802.11 to ensure BSMs can be transmitted and received with the proper headers and data elements. Finally, the objective of the SAE J2735 and J2945/1 compliance test would be to ensure that the OBE can produce all required messages with data frames and data elements meeting minimum performance requirements following SAE 2735 and SAE J2945/1.

14.1.2 BSM Transmission and Processing Test Suite

The BSM Transmission and Processing test suite verifies the generation, transmission, and processing of BSMs under different strategies and scenarios. Specifically, the BSM Transmission and Processing test suite is comprised of the following tests: message transmission under full load, BSM generation and processing impact, asynchronous message transmission, and congestion mitigation. The scope of the message transmission under full load test includes verifying the OBE generates and sends BSMs at the proper rate under full load conditions. The objective of the BSM generation and processing impact test is to two-fold. Firstly, the test aims to verify that the OBE trust store updates do not impact the BSM generation interval, or BSM processing and hazard detection. Secondly, this test aims to verify that any OBE software update installations do not impact BSM generation interval, or BSM processing and hazard detection. The asynchronous message transmission test verifies the OBE's ability to transmit BSMs using the asynchronous message strategy. The final test in this suite is the congestion mitigation test, which aims to verify that the OBE transmits BSMs on the correct 10 MHz channel at a data rate of 9 Mbps.

14.1.2.1 BSM Transmission under Full Load

Objective(s): Verify that under full load conditions, the OBE generates and sends BSMs at the proper rate.

Responsible Entity: OEM

Aligned Requirements:

- [1, 3, 4, 60] The OBE shall be capable of generating and transmitting at least 10 BSMs/sec.

Assumptions:

- SCMS is available and configured for this test

Test Setup:

1) Configure the tested OBE to generate and receive BSMs on the safety channel. If the tested OBE is equipped with one DSRC radio, ensure the radio is in alternating mode for channel switching. If it is equipped with two radios, one radio shall be designated to continuous mode for a safety channel.

2) Configure the tested OBE's logging capability for saving both transmitted messages and received messages.
3) Set up a DSRC protocol sniffer for over-the-air (OTA) message capture.
4) Configure the tested OBE to generate and receive BSMs on safety channel 172 with 9 Mbps data rate (on Ch175 or equivalent with 12 and then 18 Mbps if using a 20 MHz channel), set message frequency to 10 Hz, transmission power to 20 dBm.
5) Configure other surrounding OBEs in the testing area transmitting BSMs on Ch172 (on Ch175 or equivalent if using a 20 MHz channel) using desired message rates for creation of a “full load” environment.

Test Procedures:

1) Start the surrounding OBEs for transmitting approximately 5500 BSMs per second when using 9 Mbps. Note: If using a 20 MHz channel, also transmit 5500 BSMs per second when using 12 Mbps and 18 Mbps (550 vehicles is the maximum expected congestion level).
2) Verify the above “fully loaded environment” is reached and let it stabilize for 30 seconds.
3) Start the tested OBE to transmit and receive BSMs and run it for at least 2 minutes. All surrounding OBEs should continue to run.
4) Shut down the surrounding OBEs in sequence and then shut down the tested OBE.
5) Retrieve and review the logged file(s) from the tested OBE and OTA captures.
6) Calculate the message frequency statistics (mean and standard deviation) of the logged BSM transmitting message rate from the tested OBE for the entire testing period and verify that BSMs are generated at 10 Hz.
7) Calculate the message frequency statistics (mean and standard deviation) of the OTA captured BSM transmitting message rate from the tested OBE for the entire testing period and verify that BSMs are sent at 10 Hz.

14.1.2.2 BSM Generation and Processing Impact

Objective(s):

- Verify that the OBE trust store updates do not impact BSM generation interval or BSM processing and hazard detection.
- Verify that the OBE software update installations do not impact BSM generation interval or BSM processing and hazard detection.

Responsible Entity: OEM

Aligned Requirements:

- [47][99] The OBE shall process all certificate management operations (i.e., updating the certificate trust store, performing the computations to generate the certificate IDs from the CRL entries, performing self-test to check against CRL, etc. [this is not all encompassing of functions where safety applications have precedence]) such that the OBE continues to meet all performance requirements (i.e., there should be no measureable functional or latency difference in operations as a result of trust store updates)
- [106] The OBE shall install all software updates such that the OBE continues to meet all performance requirements (i.e., there should be no measureable functional or latency difference in operations as a result of software updates)

Assumptions:

- SCMS is available and configured for this test

Test Setup:

1) Configure the tested OBE to generate and receive BSMs on the safety channel. If the tested OBE is equipped with one DSRC radio, ensure the radio is in alternating mode for channel switching. If it is equipped with two radios, one radio shall be designated to continuous mode for a safety channel.
2) Configure the tested OBE's logging capability for saving both transmitted messages and received messages.
3) Set up a DSRC protocol sniffer for OTA message capture.
4) Ensure no other OBE or RSE in the testing area is transmitting any messages.
5) Obtain a tested OBE software update from an application developer.

Test Procedures:

<u>Trust store updates:</u>

1) Set the tested OBE transmission power to 20 dBm, data rate to 9 Mbps, message frequency to 10 Hz, and generating and receiving BSMs on channel 172. Note: If using a 20 MHz channel for BSM transmission, the 12 and 18 Mbps data rates should be tested instead of 9 Mbps.
2) Configure the tested OBE to download time-limited pseudonym certificates and the latest CRL from the SCMS. The certificates will expire in the next 10 minutes.
3) Configure the tested OBE to request a new set of time-limited pseudonym certificates 10 minutes prior to the current pseudonym certificates expiration.
4) Start to generate and transmit the J2735 BSM on channel 172 (on Ch175 if using a 20 MHz channel) for 11 minutes.
5) Observe the DSRC protocol sniffer real time capture to verify the tested OBE requests a new set of time-limited pseudonym certificates at the specified time.
6) Retrieve the logged BSM transmission file(s) from the tested OBE.
7) Calculate the message frequency statistics (mean and standard deviation) of the logged BSMs transmitted before requesting a new set of time-limited pseudonym certificates. Verify that BSMs are generated at 10 Hz and whether the OBE is processing BSMs.
8) Calculate the message frequency statistics (mean and standard deviation) of the logged BSMs transmitted after the start of requesting the new set of time-limited pseudonym certificates until completion of new certificate acquisition. Verify whether BSMs are generated at 10 Hz and whether the OBE is processing BSMs.

<u>Software updates:</u>

Note: This is only one option to test that software updates do not impact BSM processing and generation. This requirement could be met in a variety of ways and the test is dependent on the method of software update implementation.)

1) Set the tested OBE transmission power to 20 dBm, data rate to 9 Mbps, message frequency to 10 Hz, and generating and receiving BSMs on channel 172. Note: If using a 20 MHz channel for BSM transmission, the 12 and 18 Mbps data rates should be tested instead of 9 Mbps.
2) Start running an application in the tested OBE and start to generate and transmit BSMs on Ch172 (on Ch175 if using a 20 MHz channel) for 10 minutes (before software update installation phase).
3) Pause the tested OBE in the “hold” mode, mark the timestamp, and upload a software update into a specific location in the tested OBE so it can be recognized as soon as the tested OBE is back in “operational” mode.
4) Put the tested OBE back in “operational” mode so that it resumes transmitting BSMs and logging messages.

5) Observe the tested OBE recognizing and processing the software update until the update process is completed. Mark the time stamp (software update installation phase).
6) Continue to let the tested OBE transmit BSMs for 5 minutes and shut it down (after software update installation phase).
7) Retrieve the logged BSM transmission file(s) from the tested OBE.
8) Calculate the message frequency statistics (mean and standard deviation) of the logged BSMs transmitted before pausing the OBE (before software update installation phase). Verify that BSMs are generated at 10 Hz and whether the OBE is processing BSMs.
9) Calculate the message frequency statistics (mean and standard deviation) of the logged BSMs transmitted after pausing the OBE until the software update installation is complete (software update installation phase). Verify that BSMs are generated at 10 Hz and whether the OBE is processing BSMs.
10) Calculate the message frequency statistics (mean and standard deviation) of the logged BSMs transmitted after complete of the software update installation (after software update installation phase). Verify whether BSMs are generated at 10 Hz and whether the OBE is processing BSMs.

14.1.2.3 Asynchronous BSM Transmission

Objective(s): Verify that the OBE is transmitting BSMs using the asynchronous message strategy.

Responsible Entity: OEM

Aligned Requirements:

- [1015] The OBE shall randomly select an integer value N between the ranges identified in the table below corresponding to the data rate being used to transmit the BSM. The OBE shall make this selection every time it changes a certificate.

  The BSM shall be transmitted at a time corresponding to the GPS PPS event plus M*100+N*BSM_OFFSET_INTERVAL; where M is a sequence of integers ranging from 0 to 9 (to result in 10 messages per second), BSM_OFFSET_INTERVAL is found in the table below for the corresponding data rate being used to transmit the BSM, and N is a random integer between 0 and the specified maximum.

Data Rate	BSM_OFFSET_INTERVAL	Random Multiplier of N
6 Mbps	500 µsec	0 - 199
9 Mbps	350 µsec	0 - 284
12 Mbps	250 µsec	0 - 399
18 Mbps	200 µsec	0 - 499

Assumptions:

- SCMS is available and configured for this test

Test Setup:

1) Configure the tested OBE to generate and receive BSMs on the safety channel. If the tested OBE is equipped with one DSRC radio, ensure the radio is in alternating mode for channel switching. If it is equipped with two radios, one radio shall be designated to continuous mode for a safety channel.
2) Configure the tested OBE to generate and transmit BSMs on Ch172 with a 9 Mbps data rate (on Ch175 if using a 20 MHz channel), set message frequency to 10 Hz, and transmission power to 20 dBm.

3) Configure the tested OBE's logging capability for saving both transmitted messages and received messages.
4) Set up a DSRC protocol sniffer for OTA message capture. The sniffer should equip with a sufficiently accurate GPS clock that provides stable 10 MHz reference signal and a 1 PPS signal.
5) Ensure no other OBE or RSE in the testing area is transmitting any messages.

Test Procedures:

1) Start the tested OBE to generate and transmit BSMs and the sniffer to capture transmitted BSMs for at least 10 minutes.
2) Calculate the statistics (time offset mean and standard deviation) of the logged BSM transmitting time from the tested OBE for the entire testing period based on the N and BSM_OFFSET_INTERVAL in the table.
3) Verify whether BSMs are generated using the asynchronous message strategy, and that the asynchronous interval changes when the certificate changes, based on the logged messages.
4) Repeat steps (2) and (3) using the captured OTA files
5) If using a 20 MHz channel for BSM transmission, repeat steps (1) to (4) when the tested OBE data rate is set to 12 and 18 Mbps

14.1.2.4 Congestion Mitigation (10 MHz Channel)

Objective(s): Verify that the OBE transmits BSMs on the correct 10 MHz channel at a data rate of 9 Mbps.

Responsible Entity: OEM

Aligned Requirements:

- [1017] The OBE shall transmit BSM WSMs on a 10 MHz channel, at a data rate of 9 Mbps.

Assumptions:

- SCMS is available and configured for this test

Test Setup:

1) Configure the tested OBE to generate and receive BSMs on the safety channel. If the tested OBE is equipped with one DSRC radio, ensure the radio is in alternating mode for channel switching. If it is equipped with two radios, one radio shall be designated to continuous mode for a safety channel.
2) Configure the tested OBE's logging capability for saving both transmitting messages and receiving messages.
3) Set up a DSRC protocol sniffer for OTA message capture.
4) Configure the tested OBE to generate and receive BSMs on safety channel 172 with 9 Mbps data rate, set message frequency to 10 Hz, and transmission power to 20 dBm.

Test Procedures:

1) Start the tested OBE to generate and receive BSMs in Ch172 at a data rate of 9 Mbps
2) Using a spectrum analyzer, verify that the OBE is transmitting on Ch 172
3) Using the DSRC protocol sniffer, verify that the OBE is sending BSMs at a data rate of 9 Mbps

14.1.2.5 Congestion Mitigation (20 MHz Channel)

Objective(s): Verify that the OBE uses a congestion mitigation algorithm and is capable of sensing congestion and responding appropriately.

Responsible Entity: OEM

Aligned Considerations:

- The OBE shall transmit BSM WSMs on Channel 175 or equivalent, at a data rate of 12 Mbps when the Channel Busy Ratio is below 50%.
- The OBE shall transmit BSMs on Channel 175 or equivalent at a data rate of 18 Mbps when the Channel Busy Ratio exceeds 50%; such transmission shall continue until the Channel Busy Ratio falls below 30%.

Assumptions:

- SCMS is available and configured for this test

Test Setup:

1) Configure the tested OBE to generate and receive BSMs on the safety channel. If the tested OBE is equipped with one DSRC radio, ensure the radio is in alternating mode for channel switching. If it is equipped with two radios, one radio shall be designated to continuous mode for a safety channel.
2) Configure the tested OBE's logging capability for saving both transmitting messages and receiving messages.
3) Set up a DSRC protocol sniffer for OTA message capture.
4) Configure the tested OBE to generate and receive BSMs in safety channel 175 or equivalent with 12 Mbps data rate, set message frequency to 10 Hz, and transmission power to 20 dBm.
5) Configure other surrounding OBEs in the testing area transmitting BSMs on Ch175 or equivalent using desired message rates for generating the desired CBR.

Test Procedures:

1) Start the tested OBE to generate and receive BSMs in Ch175 or equivalent for 5 minutes
2) Start the surrounding OBEs to transmit BSMs in Ch175 or equivalent which will increase CBR. The background BSM traffic should be generated gradually until it reaches 7000 BSMs per second. This test period should occur within 15 minutes.
3) Shut down the surrounding OBEs gradually to reduce CBR until all surrounding OBEs are off. This test period should occur within 15 minutes.
4) Retrieve and review the logged file(s) from the tested OBE and OTA captures.
5) Calculate CBR values for the first 5 minutes, in 30 second intervals.
6) Calculate CBR values for the next 15 minutes, in 10 second intervals.
7) Calculate CBR values for the last 15 minutes, in 10 second intervals.
8) Determine the time points where Ch175 or equivalent CBR changed.
9) Verify Ch175 or equivalent data rates at where CBRs changed and determine whether the date rate changes are at appropriate level.
10) Repeat steps (5) to (10) for OTA captures, if needed.

14.1.3 Storage Test Suite

The Storage test suite focuses on testing the general storage ability of the OBE as well as the misbehavior report storage functionality of the OBE. Specifically, the objective of the general storage test is to verify that the OBE can store at least one CRL, three years' worth of pseudonym certificates at 20 certificates per week, a basic software load and any updates (non-volatile storage capacity of 1 MB plus size necessary for software storage and operations). The misbehavior report storage verifies that the OBE can store up to 30 misbehavior reports, and once the maximum storage capacity has been met, that the OBE deletes the oldest misbehavior report.

14.1.3.1 General Storage

Objective(s): Verify that the OBE can store at least one CRL, three years' worth of pseudonym certificates at 20 certificates per week, a basic software load and any updates, with non-volatile storage capacity of 1 MB plus size necessary for software storage and operations.

Responsible Entity: OEM

Aligned Requirements:

- [85a] The OBE shall have the capacity to store at least one CRL, three years' worth of pseudonym certificates at 20 certificates per week, a basic software load and any updates (non-volatile storage capacity of 1 MB plus size necessary for software storage and operations).

Test Setup:

1) Configure the tested OBE to generate and receive WSMs in the service/safety channel and control channel. If the tested OBE is equipped with one DSRC radio, ensure the radio is in alternating mode for channel switching. If it is equipped with two radios, one radio shall be designated to continuous mode for a safety channel.
2) Configure the tested OBE's logging capability for saving both transmitted messages and received messages.
3) If the SCMS is available, configure the RSE to broadcast a WSA with SCMS service information.
4) Obtain a tested OBE firmware update from the OBE manufacturer (only applies if OEM deploys updates while the OBE is in operational mode).
5) Delete all trust store storage, enrollment cert, pseudonym certificates, generated keys, log files, and software updates from the tested OBE.

Test Procedures:

1) Check and mark the available non-volatile storage of the tested OBE.
2) If the SCMS is available, start the tested OBE for requesting and downloading needed security credentials and CRLs, including pseudonym certificates for three years and a CRL as a minimum.
3) If the SCMS is not available, download the security credentials from a designated and authorized server and save them into a specific folder where the tested OBE can retrieve when needed.
4) Configure the tested OBE to generate and receive BSMs on safety channel 172 with 9 Mbps data rate, set message frequency to 10 Hz, transmission power to 20 dBm. Note: If using a 20 MHz channel for BSM transmission, the test must be conducted with the 12 and 18 Mbps data rates.

5) Start transmitting BSMs for at least 120 seconds.
6) Copy the firmware update into a folder in the tested OBE (only applies if OEM deploys updates while the OBE is in operational mode).
7) Verify security credential, BSM log file(s), and updated firmware are all saved in the tested OBE.
8) Check and mark the available non-volatile storage of the tested OBE and verify the remaining storage capacity.

14.1.3.2 Misbehavior Report Storage

Objective(s): Verify that the OBE can store up to 30 misbehaving messages into a misbehavior report and discards the lowest-priority stored misbehavior observations if necessary to store a higher-priority misbehavior observation and/or when storage capacity is reached.

Responsible Entity: OEM

Aligned Requirements:

- [1002] The OBE shall have the capacity to store up to at least 30 misbehaving messages (as defined in requirements 1006, 1018, and 1019) together with their corresponding security credentials, verification status, and the time and position at which they were received (i.e., the misbehavior report/package).
- [1005] The OBE shall have a priority function to determine which misbehavior observations are most important and shall discard the lowest-priority stored misbehavior observations if necessary to store a higher-priority misbehavior observation. The priority function may be OEM-specific or may be standardized.

Test Setup:

1) Configure the tested OBE to generate and receive WSMs on the service/safety channel and control channel. If the tested OBE is equipped with one DSRC radio, ensure the radio is in alternating mode for channel switching. If it is equipped with two radios, one radio shall be designated to continuous mode for a safety channel.
2) Configure the tested OBE's logging capability for saving both transmitted messages and received messages.
3) Download and save valid pseudonym certificates to a specific folder where the tested OBE can retrieve when needed.
4) Configure a "faulty" OBE (or a DSRC device) in the testing area which is capable of transmitting malformed BSMs.
5) Configure a "simulated SCMS" computer which receives misbehavior messages sent by the tested OBE.
6) Create 40 malformed BSMs by generating incorrect timestamps, positions, security credentials, etc.

Test Procedures:

1) Configure the tested OBE to generate/receive BSMs on Ch172 with 9 Mbps data rate, set message frequency to 10 Hz, and transmission power to 20 dBm. Note: If using a 20 MHz channel for BSM transmission, the test must be conducted with the 12 and 18 Mbps data rates.
2) Configure the "faulty" OBE to generate malformed BSMs on Ch172 with 9 Mbps data rate, set message frequency to 10 Hz, and transmission power to 20 dBm. Note: If using a 20 MHz

channel for BSM transmission, the test must be conducted with the 12 and 18 Mbps data rates.

3) Start the tested OBE to transmit and receive BSMs.
4) Start the “faulty” OBE to transmit the first 30 malformed BSMs and pause the “faulty” OBE.
5) Pause the tested OBE.
6) Verify the tested OBE generates and saves 30 correctly formatted misbehavior messages in the correct misbehavior report format.
7) Restart the tested OBE.
6) Restart the “faulty” OBE and transmit one more malformed BSM.
7) Pause the “faulty” OBE and the tested OBE.
8) Verify the tested OBE generates and saves the 31st misbehavior message correctly in the formatted misbehavior report and deletes the lowest priority misbehavior observation.

14.1.4 Failure Detection Test Suite

The Failure Detection test suite is comprised of the start-up failure detection and operational failure detection tests. The start-up failure detection test verifies that the OBE initiates all start-up procedure tasks and, in the event of a failure, identifies it accordingly. The operational failure detection verifies that the OBE can detect failures that would result in an erroneous BSM being generated in potential scenarios such as incorrect data parameters. Additionally, in the event of a failure, this test aims to verify that the OBE ceases to transmit BSMs.

14.1.4.1 Start-Up Failure Detection

Objective(s): Verify that the OBE initiates all start-up procedure tasks, can identify any failures, and ceases BSM transmission if a failure is detected.

Responsible Entity: OEM

Aligned Requirements:

- [113, 105, 50, 57, 86, 122] #1 The OBE shall initiate a startup process, no longer than 60 seconds prior to key on and should be completed no more than 30 seconds after key-on, that includes following checks:
  - (1) Radius of horizontal position error distribution shall be less than 0.325 meters with at least 95% confidence
  - (2) Vertical position error distribution less than 2 meters with at least 95% confidence
  - (3) The OBE system clock used to time stamp messages and signatures, and perform internal position related computations is synchronized to GPS time to less than 2 millisecond standard deviation
  - (4) All other vehicle sensors providing BSM parameter information should be present and available
  - (5) The OBE's set of pseudonym certificate IDs are not on the Revoked certificate ID Table
  - (6) All received and validated software updates have been installed
  - (7) OBE is installed in the same vehicle for which it has been certified
- [113, 105, 50, 57, 86, 122] #2 Upon failing the startup or operational self-tests, the OBE shall cease sending BSMs (i.e., transition to quiet mode).

Test Setup:

1) Connect OBE to vehicle sensors.

2) Configure the tested OBE for communicating with a simulated SCMS.
3) Generate and log BSMs from the tested OBE for 5 minutes.
4) OBE is in “key-off” position.
5) Ensure vehicle recognizes its “last-known” position by examining the logged BSMs.

Test Procedures:

1) Test the ability to recognize changes in GPS (position and time) errors.
    a. Cover the GPS antenna with a conductive cover that obscures 75 percent of the sky.
    b. Turn the OBE on.
    c. Check that the OBE self-test is completed after the device is started.
    d. Check that the OBE identifies a failure and does not enter operational mode.
    e. Turn-off and the OBE and remove the conductive cover.
2) Test the ability to recognize that a vehicle sensor providing BSM parameter data is not present and available
    a. Disconnect a vehicle sensor (e.g., speed sensor) or block the sensor from providing BSM parameter information.
    b. Turn the OBE on.
    c. Check that the OBE self-test is completed after the device is started.
    d. Check that the OBE identifies a failure and does not enter operational mode.
    e. Turn-off and the OBE and reconnect the sensor or remove the blockage/jamming.
3) Test the ability to recognize revoked certificates.
    a. Create a “simulated CRL” so that the tested OBE’s certificate is revoked and on the list.
    b. Turn the OBE on, observe that the OBE starts to communicate with the simulated SCMS, and requests the latest CRL.
    c. Verify the latest CRL is downloaded to the tested OBE.
    d. Check that the self-test is completed after the device is started.
    e. Check that the OBE identifies a failure and ceases BSM transmission.
    f. Turn off the simulated SCMS, OBE, and remove the simulated malfunction.
4) Test the ability to recognize need for software update.
    a. Turn on the tested OBE, placing an updated version of the software (with intentional errors) at a specific directory designated by the OBE vendor. Turn-off the OBE.
    b. After a minute, turn the OBE on. Check that the self-test is completed after the device is started.
    c. Check that the OBE identifies a failure and the OBE ceases BSM transmission.
    d. Turn off the OBE and remove the simulated malfunction.
5) Test the ability to identify that OBE is installed in the same vehicle for which it has been registered.
    a. Enact a known, simulated OBE malfunction. For example, push new vehicle identification information to OBE.
    b. Turn the OBE on. Check that the self-test is completed after the device is started.
    c. Check that OBE identifies a failure and ceases BSM transmission.
    d. Turn off the OBE and remove the simulated malfunction.

14.1.4.2 Operational Failure Detection

Objective(s): Verify that the OBE can detect failures that would result in an erroneous BSM being generated (data outside limits, sending parameters faulty, etc.) and cease BSM transmission if a failure is detected.

Responsible Entity: OEM

Aligned Requirements:

- [50, 57, 86] The OBE shall be considered to be operational (in operational mode) when it has confirmed that all conditions for operation have been met at intervals of 100 seconds at most. These conditions are:
    - (1) Radius of horizontal position error distribution shall be less than 0.325 meters with at least 95% confidence
    - (2) Vertical position error distribution less than 2 meters with at least 95% confidence
    - (3) The OBE system clock used to time stamp messages and signatures, and perform internal position related computations is synchronized to GPS time to less than 2 millisecond standard deviation
    - (4) All other vehicle sensors providing BSM parameter information should be present and available
- [113, 105, 50, 57, 86, 122] #2 Upon failing the startup or operational self-tests, the OBE shall cease sending BSMs (i.e., transition to quiet mode).

Test Setup:

1) Vehicle is in key-on position and OBE is operational.
2) Benchmark the GPS reference unit.
3) Data is being recorded at 10 Hz for a minimum period of 10 minutes. Location and time measurement accuracies of the GPS reference tools are ±10 cm and 1 millisecond, respectively.
4) Record positional and time accuracy through GPS reference test tool and packet capture (PCAP) BSMs with packet sniffer and GPS synchronization.

Test Procedures:

1) Test the ability to recognize GPS (position and time) errors.
    a. Cover the GPS antenna with a conductive cover that obscures at least 75 percent of the sky.
    b. Check that the OBE identifies the failure and ceases BSM transmission.
    c. Remove the malfunction and ensure the OBE is transmitting BSMs.
2) Test the ability to recognize that a vehicle sensor providing BSM parameter data is not present and available
    a. Disconnect a vehicle sensor (e.g., speed sensor) or block the sensor from providing BSM parameter information.
    b. Check that the OBE identifies a failure and ceases BSM transmission.
    c. Reconnect the sensor or remove the blockage/jamming and ensure the OBE is transmitting BSMs.

Vehicle Level Tests

The tests outlined in this test plan are intended to describe a series of Vehicle Level tests aimed at providing NHTSA with a basis for assessing vehicle system performance against the connected vehicle performance requirements. The goal is to provide tests that can be carried out on production vehicles without requiring NHTSA testing of individual system components. However, vehicles would be compliant with most OBE/Component Level requirements, including DSRC standards compliance, by default when passing the Vehicle Level tests. The overall tests described in this test plan are designed to evaluate the ability of a connected vehicle integrated with a DSRC system based on the NHTSA requirements to meet the overall performance requirements.

The overall objective of the connected vehicle safety system is to provide a safety benefit to vehicle users based on the ability of vehicles to communicate information that allows a suitably equipped vehicle to determine if a hazard condition exists and, if so, to take appropriate action. The specific action to be taken depends on the application, and NHTSA does not plan to specify or require any specific applications. However, it is apparent that each safety application will depend on the ability of the system to determine from information provided by other vehicles in proximity (via the Basic Safety Message) if a hazard exists. The common thread of this determination is the ability for the system to predict when a collision is likely (and when and where that collision is likely to occur) and to also differentiate between actual collisions and near misses. The ability of the system to make these predictions must also be within a predefined safety margin and specified level of reliability. The tests described herein are thus intended to provide an overall assessment that the vehicle is producing BSMs with accurate data parameters to allow other vehicles to reliably make hazard determinations, is able to differentiate between valid and erroneous/invalid BSMs, and that the vehicle can support the basic required security functions.

To accomplish this, the tests will use an in-vehicle truth system with a calibrated in-vehicle sensor suite to monitor the ground truth dynamic behavior of the vehicle, a DSRC radio to receive the BSMs generated by the vehicle system, and a logging system to record both the vehicle BSMs and the corresponding vehicle ground truth to assess the accuracy of the BSM data from the vehicle under test. The tests will also use a roadside test unit that has the ability to generate simulated BSMs, specifically those that are incorrectly signed and those that are erroneous in ways that the vehicle under test should determine are “implausible.”

Additional tests will simulate a roadside unit (RSE/RSU) encounter to assess the ability of the vehicle to support various security transactions and to evaluate its ability to support interrupted security exchanges. It is important to note that some vehicle manufacturers are proposing security updates at stationary locations (e.g., dealer service centers), in which case the interrupted RSE encounter test may need to be modified.

All of the proposed tests will be run on a closed test road.

14.1.5 Static Vehicle Test Suite

The Static Vehicle test suite will assess various vehicle level elements of the system while the vehicle is at rest under static conditions. Specifically, those elements that do not require other vehicles to test, but that may be unique to a particular installation of connected vehicle equipment on the vehicle under test (for example the impact of body contours and fixed equipment such as roof racks on the system performance). The suite will also assess the vehicle’s ability to initiate a self-test and if the OBE detects any failure, the system illuminates a malfunction indication light, and proceeds to operate in quiet mode (i.e., the OBE does not transmit BSMs). This test suite also aims to ensure that the indication light clears when in operational mode.

14.1.5.1 Transmit Power and Antenna Gain Envelope Test

Objective(s): Assess transmit power and antenna gain of a full vehicle with production antenna. Test is vehicle dependent and must account for vehicle body, height, and antenna placement as well as any original equipment accessories such as roof racks.

Responsible Entity: OEM; oversight entity

Aligned Requirements:

- [17, 59] Transmit power and antenna gain shall be greater than -70 dBm when measured at 30 meters in all azimuth directions and between ±10 degrees elevation from the transmitting vehicle antenna(s), with the vehicle antenna(s) mounted to the vehicle in its production location and orientation.

Test Setup:

1) Vehicle is within azimuth and elevation test facility with capability of measuring at 30 meters distance from the vehicle at all azimuth angles and between -10 and +10 degrees elevation

Test Procedures:

1) Configure vehicle OBE to generate test messages or CW test signal.
2) Set test receiver (e.g., spectrum analyzer) at 0 degrees elevation and 30 meters range.
3) Measure power level of sent messages (or CW signal) at 10 degree azimuth intervals from 0 degrees to 350 degrees, and at 1 degree elevation intervals from – 10 degrees to +10 degrees (azimuth intervals and elevation intervals can be widened to save testing time as necessary).

14.1.5.2 Self-test

Objective(s):

- Verify that the self-test initiates at key on.
- Verify that the OBE can survive all operations during any key-off, key-on sequence.
- Verify that the OBE activates a malfunction indication when not in operational mode. Verify that the malfunction indication clears upon successful start-up, self-test, and/or when in operational mode.

Responsible Entity: OEM; oversight entity

Aligned Requirements:

- [1010] OBE self-test shall be performed at key-on. It may also be performed no more than 60 seconds before key-on so long as the OBE does not transition to a fully powered-off state between the self-test and the key-on event.
- [1009] OBE operations shall survive any key-off, key-on sequence.
- [1011] The OBE shall activate a malfunction indication when not in operational mode (e.g., during a start-up check, failing a self-test). The malfunction indication shall be clearly visible from the driver’s designated seating position.
- [120] An active OBE malfunction indication shall persist until the OBE passes the self-test and clears all warnings (from previous failed self-tests).

Test Setup:

1) Software, certificate, or CRL update is available.
2) OBE is in special test mode (allows logging of received messages, and readout of log over DSRC, vehicle bus, or special OBE connector).

Test Procedures:

1) Start vehicle.

2) Check that the malfunction indication is on and the OBE is not transmitting BSMs prior to completing the start-up test.
3) Check that self-test initiates.
4) Ensure that the malfunction indication turns off and the OBE begins transmitting BSMs upon successful completion of the start-up test.
5) Initiate a specific operation (e.g., software, certificate, CRL update).
6) Turn vehicle to key-off immediately after the operation starts and before it is complete.
7) Turn vehicle back to key-on.
8) Determine whether the device continues the operation or starts the process from the beginning while ensuring the device is still operational after finishing the self-test and additional operations.

14.1.6 Dynamic Vehicle Test Suite

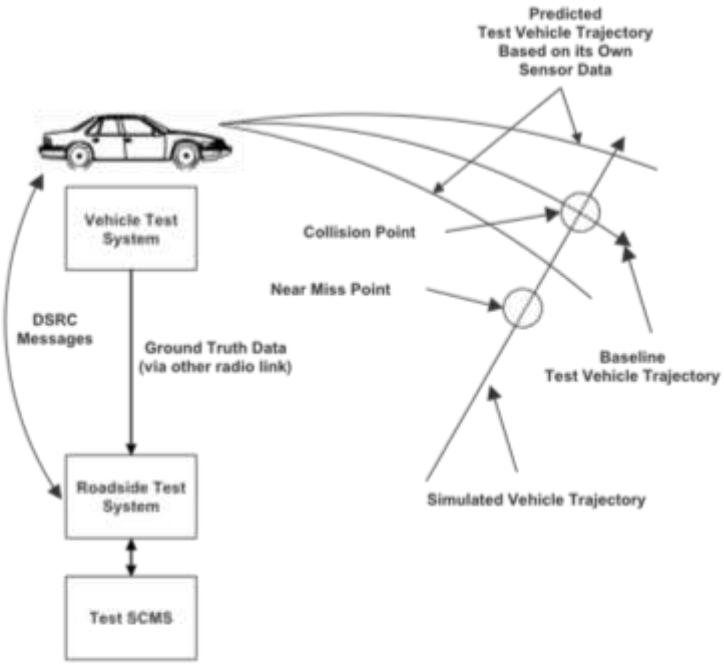
Three elements comprise the test system for the Dynamic Vehicle Test Suite:

- In-Vehicle Test System
- Roadside Test System
- SCMS Test System

These are illustrated conceptually in

Figure 158 below.

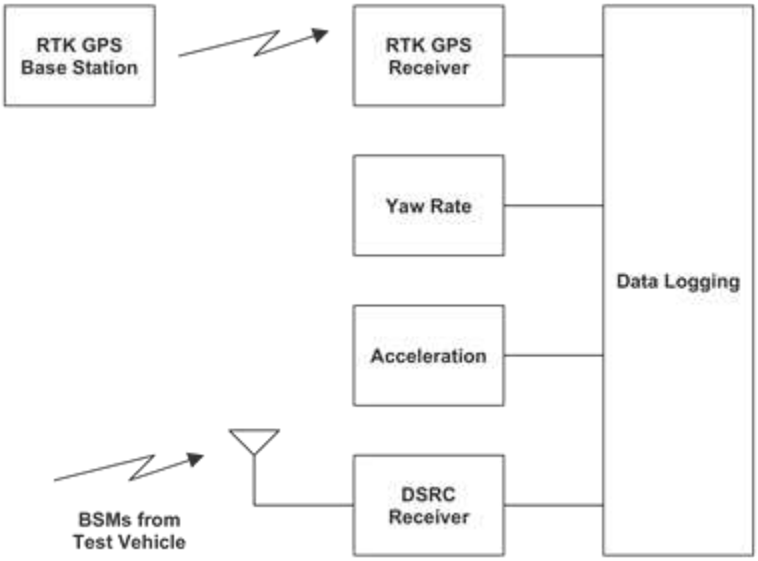
Figure 158: Vehicle Level Compliance Test Overview (Source: USDOT)



The In-Vehicle Test System uses a calibrated in-vehicle sensor suite to monitor the ground truth dynamic behavior of the vehicle, a DSRC radio to receive the BSMs generated by the vehicle system, and a logging system to record both the vehicle BSMs and the corresponding vehicle ground truth.

As shown in Figure 159, the In-Vehicle Test System will include a real time kinematic (RTK) GPS receiver to measure position, speed, and heading together with inertial sensors to assess acceleration and yaw rate.

Figure 159: In-Vehicle Test System (Source: USDOT)

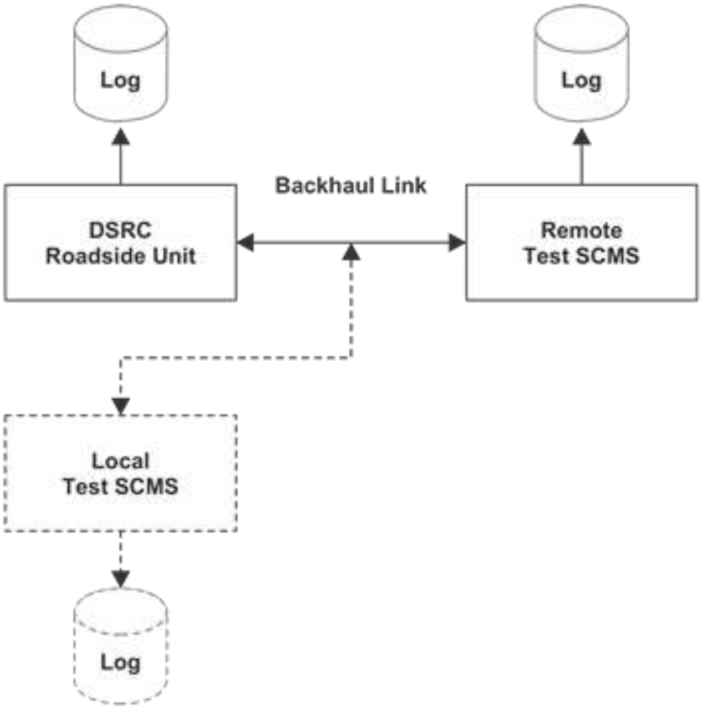


In-Vehicle Test System Reference Implementation

- Ground truth data system (including external RTK base station and radio link)
  - Position (RTK)
  - Speed (RTK)
  - Heading (RTK)
  - Yaw rate
  - Time
- DSRC Receiver
- Data Logging System (Ground Truth and Vehicle BSMs)
- Self-powered (or vehicle Direct Current [DC] adapter powered)

The Roadside Test System, shown in Figure 160, includes a conventional DSRC Roadside Unit, and a backhaul link to the test SCMS (or a local version of the test SCMS).

Figure 160: Roadside Test System (Source: USDOT)



Roadside Test System Reference Implementation

- DSRC RSU
  - Set up to advertise SCMS services
  - Route packets to/from vehicle to/from SCMS
  - Backhaul link to Test SCMS
  - Generate implausible/unsigned Test BSMs
- Test SCMS
  - Respond to certificate requests
  - Receive misbehavior reports

The Test SCMS may be the actual remote SCMS connected via backhaul to the Roadside Unit, or it may be a locally simulated SCMS used for testing only. The Test SCMS will include a server that can receive misbehavior reports and respond to certificate update requests. It is used to assess the ability of the vehicle to provide misbehavior reports and to evaluate the ability to dynamically request and update security credentials.

14.1.6.1 BSM Parameter Accuracy Test

Objective: Verify that the BSMs generated by the OBE can conform to minimum error thresholds for position, speed, acceleration, heading, and yaw rate.

Responsible Entity: OEM; oversight entity

Aligned Requirements:

- [1014] The data parameters provided in a BSM generated by the host vehicle shall conform to the following maximum error tolerance requirements.
  - Horizontal position: 0.325 meters
  - Vertical position: 2 meters
  - Speed: 0.015 meter/second
  - Heading: 0.1 degrees
  - Time Accuracy: 2 msec
  - Longitudinal acceleration: 0.04 meters/second^2
  - Yaw Rate: 0.12 degrees/second

Required Equipment:

- Vehicle Under Test
- Test DSRC Receiver
- Receiver Test Software
  - Receives and parses WSM containing BSM payload (BLOB)
  - Passes BSM BLOB to logger
- Data Logger Test Software
  - Logs received BSM provided by DSRC Test Receiver including received timestamp
  - Logs ground truth data including time and position stamp at least 100 msec intervals
- Ground Truth System
  - Generates vertical position, horizontal position, heading, speed, yaw rate, longitudinal acceleration, and lateral acceleration at least 100 msec update intervals

Setup:

1) Locate ground truth system in vehicle and connect to logger
2) Connect DSRC Test Receiver to Data Logger

Test Procedure:

1) With vehicle system generating BSMs and logging system logging both received BSMs and ground truth data, drive vehicle over prescribed course following predetermined speed profile (course and speed profile to be determined)

Post Processing:

1) Compare time stamp in BSM and receive time stamp to assess BSM latency and gross time errors

2) Use ground truth data and BSM generation time (inferred from time error and logger time stamp) to interpolate BSM Parameters from ground truth data
3) Compare data parameters from BSM with corresponding parameters derived from ground truth data to determine error level for each BSM Parameter
4) Compare average parameter error levels to tolerances specified in the requirement

14.1.6.2 Simulated Implausible Messages

Objective(s):

- Verify that the OBE can correctly differentiate between plausible BSMs and outlier BSMs with the required accuracy at a rate of 5500 BSMs per second for Level 1 plausibility and 200 BSMs per second for Level 2 plausibility.
- Verify the OBE logs within a misbehavior report (a) any message that (1) results in a warning or (2) would result in a warning but failed a level 2 plausibility check, or (b) any set of 10 continuous BSMs from the same vehicle that has consistently failed plausibility Level 1 checks.

Responsible Entity: OEM; oversight entity

Aligned Requirements:

- [80B] Level 1 plausibility: The OBE shall identify as a suspect or implausible message any BSM for which the components of the vehicle dynamic state (position, speed, acceleration, and yaw rate) are outside the values as noted below.
  - Speed: 70 m/sec (252 km/hr)
  - Longitudinal Acceleration - Acceleration: 12 m/s^2, Deceleration: -12 m/s^2
  - Lateral Acceleration: 11 m/s^2
  - Yaw rate: 1.5 radian/s
  - Values in BSM need to be internally consistent: Speed, lateral acceleration, and yaw rate are linked mathematically: $V^2=ac^2/(Y')^2$
- [63, 64, 67, 80] Level 2 plausibility: If a BSM would result in a positive application warning decision, the OBE shall identify as a message that fails level 2 plausibility any BSM for which the vehicle dynamic state (position, speed, acceleration, heading, and yaw rate) as described by the most recent BSM falls outside the 2 sigma distribution for the vehicle state as projected from the prior BSM to the time of the current BSM (i.e., the message is implausible if it is not on its expected trajectory within 2 sigma based on the received BSMs). If such a message fails the level 2 plausibility check, the OBE shall not raise an alert to the driver on the basis of that message and shall prioritize the message for misbehavior reporting.
- [81] The OBE shall have the processing capacity to perform level 1 plausibility checks on at least 5500 BSMs per second.
- [1016] The OBE shall have the processing capacity to perform level 2 plausibility checks on at least 200 BSMs per second.
- [1007] If a message fails any misbehavior check, the OBE shall flag the source of misbehavior and include the appropriate data (as identified in the CAMP report, SCMS design document, and security requirements) in the misbehavior report.
- [1018] The OBE shall log within a misbehavior report (a) any message that (1) results in a warning or (2) would result in a warning but failed a level 2 plausibility check, or (b) any set of 10 continuous BSMs from the same vehicle that has consistently failed plausibility Level 1 checks.

Test Setup:

1) Configure the RSU to generate and send test BSMs including some messages with implausible content.
2) Drive vehicle on course around RSU.

Test Procedures:

Note: This test assumes that Plausibility Level 2 checks are only conducted for BSMs that represent a hazard which is why the vehicle should be moving.

1) The Test Vehicle is driven at a constant speed along the test corridor/track.
2) The Roadside Test System transmits up to 5500 simulated BSMs (with erroneous BSMs to cause Level 1 and 2 Plausibility Check failures) using the Roadside Test System DSRC RSU.
3) As part of its connected vehicle equipment, the Test Vehicle will receive the simulated BSMs from the Roadside Test System, and based on its internal plausibility tests it will flag any messages that fail the Level 1 and 2 Plausibility checks.
4) The test is expected to include several runs with some simulated BSMs meeting the 10 sustained and continuous implausible BSMs from the same vehicle to trigger logging misbehavior as a result of Plausibility Level 1 checks and also BSMs outside of the 2 sigma trajectory projection to trigger logging misbehavior as a result of Plausibility Level 2 checks. Each run will include logged test data including the Test Vehicle BSMs received by the Roadside Test System and the plausibility test results from the Roadside Test System.
5) A passing test will indicate that the Test Vehicle properly identified implausible messages on the basis of the pre-defined plausibility parameters. Any instances of 10 or more sustained and continuous implausible BSMs from the same vehicle should be logged within a misbehavior report. If the vehicle fails to detect more than 90 percent of the implausible messages it will fail the test.

14.1.6.3 Simulated Signature Failure

Objective(s): Verify that all messages that result in a safety warning are first verified by the OBE and a misbehavior report is generated for BSMs that fail verification.

Responsible Entity: OEM; oversight entity

Aligned Requirements:

- [1006] The OBE shall verify (i.e., check revoked certificates, verify signature, and verify certificate) at least all received messages that have been validated through plausibility tests and that result in a safety warning (verify on demand) (and flag for misbehavior reporting if the message fails verification).
- [1007] If a message fails any misbehavior check, the OBE shall flag the source of misbehavior and include the appropriate data (as identified in the CAMP report, SCMS design document, and security requirements) in the misbehavior report.
- [1018] The OBE shall log within a misbehavior report any message that either results in a warning or indicates that the hazard detected is a false positive if the vehicle has sufficient capability, and any set of 10 continuous BSMs from the same vehicle that has consistently failed plausibility checks.

Test Setup:

1) Configure the Test Vehicle to send BSMs representing its best estimate of the BSM data parameters.

2) Configure the Roadside Test System to receive the BSMs transmitted from the Test Vehicle, and to compute BSM parameters for a simulated vehicle traveling on a collision course relative to the Test Vehicle (because the OBE is only required to verify messages that will result in a warning). These BSMs will be incorrectly signed with each message failing one of the security verification tests.

Test Procedures:

Note: This test assumes that BSM signatures are only checked for BSMs that represent a hazard which is why the vehicle should be moving.

1) The Test Vehicle is driven at a constant speed along the test corridor/track.
2) The Roadside Test System transmits incorrectly signed simulated BSMs using the Roadside Test System DSRC RSU.
3) As part of its connected vehicle equipment, the Test Vehicle will receive the simulated BSMs from the Roadside Test System and, based on its internal security processing, it will reject the messages and compile a misbehavior report.
4) The test is expected to include several runs. Each run will include logged test data including the Test Vehicle BSMs received by the Roadside Test System, the simulated BSMs from the Roadside Test System, and the security validation results from both the Test Vehicle and the Roadside Test System.
5) A passing test will indicate that the Test Vehicle properly identified non-verifiable messages sent from the Roadside Test System and that the messages sent from the Test Vehicle were all properly signed. If the vehicle fails to detect more than 99 percent of the non-verifiable messages, or if its own BSMs fail security verification it will fail the test.

14.1.7 Simulated RSE Encounter Test Suite

The RSE encounter tests are intended to verify that the connected vehicle system equipped vehicle is able to carry out the minimum required interactions with a remote server via a roadside unit. This is accomplished by using a roadside unit on a test roadway, and causing the vehicle to execute a variety of transactions with the SCMS (or a simulated SCMS). The transactions are:

- Simulated Misbehavior Report Transaction
- Simulated Certificate Request
- Simulated Certificate Delivery (with and without an interrupted data exchange).

These tests are run on a simulated roadway at 60 mph.

14.1.7.1 Simulated Misbehavior Report Transaction

Objective(s): Verify that the OBE sends the stored misbehavior report when SCMS connectivity is available.

Responsible Entity: OEM; oversight entity

Aligned Requirements:

- [1003] The OBE shall send saved misbehavior reports to Misbehavior Authority when connectivity is available.

Test Setup:

Note: During the Dynamic Vehicle Test Suite, the Test Vehicle encountered a variety of improperly signed messages. Each of these should result in the generation of a misbehavior report. Assuming this has been done and the vehicle has a misbehavior report to send, the test can be carried out.

1) Configure RSE to provide routing to the SCMS (or a simulated SCMS). It is assumed that the round trip time delay has been measured for the server and backhaul.
2) Configure the RSE to send a WSA on the control channel every 100 msec, including the channel information (e.g., IP address, available service channel for the routing service) at 20 dBm.

Test Procedures:

1) The Test Vehicle approaches an RSE which is advertising connectivity to the SCMS (or some similar suitable PSID associated with such a service) using a conventional WSA.
2) The Vehicle System receives the WSA and initiates an IP session to deliver the misbehavior report.
3) As the Test Vehicle approaches the RSE, the security management application will initiate the upload of the misbehavior report and send the report to the SCMS.
4) The sending action shall be logged in the Vehicle Test System and these logs will then be compared to the RSE logs to a) determine if the transaction was initiated, and b) determine the length of the transaction time.
5) A successful test will deliver the entire misbehavior report before the RSE encounter is complete and delete the misbehavior report after sending.

14.1.7.2 Simulated Certificate Request

Objective(s): Verify that the OBE can complete request and response transactions with remote system management services in less than 10 seconds.

Responsible Entity: OEM; oversight entity

Aligned Requirements:

- [18B] The maximum request/response transaction between the OBE and remote system management servers (e.g., SCMS [via the LOP], and software update servers) establishment time shall be less than 10 seconds. A request/response transaction shall be considered to be "established" when the transaction can be resumed, or continued at a subsequent RSE encounter (i.e., sufficient data has been exchanged to support either data exchange or resumption of data exchange at a later RSE encounter).

Test Setup:

Note: In order to perform the Dynamic Vehicle Test Suite, the Test Vehicle must be provisioned with security certificates. To accomplish this and to evaluate the vehicle’s ability to request and obtain certificates in a timely manner, this test carries out the certificate request and update sequence in a simulated roadway environment.

1) Configure RSE to provide routing to the SCMS (or a simulated SCMS). It is assumed that the round trip time delay has been measured for the server and backhaul.
2) Configure the RSE to send a WSA on the control channel every 100 msec, including the channel information (e.g., IP address, available service channel for the routing service) at 20 dBm.

Test Procedures:

1) The Test Vehicle approaches an RSE which is advertising connectivity to the SCMS (or some similar suitable PSID associated with such a service) using a conventional WSA.
2) The Vehicle System receives the WSA and initiates an IP session to request certificates.
3) As the Test Vehicle approaches the RSE, the security management application will send the certificate request to the SCMS.
4) The sending action shall be logged in the Vehicle Test System and these logs will then be compared to the RSE logs to a) determine if the transaction was initiated, and b) determine the length of the transaction time.
5) A successful test will deliver the certificate request to the SCMS within the time of the RSE encounter.

14.1.7.3 Simulated Certificate Delivery I (Complete Transaction)

Objective(s): Verify that the OBE can complete request and response transactions with remote system management services in less than 10 seconds.

Responsible Entity: OEM; oversight entity

Aligned Requirements:

- [18B] The maximum request/response transaction between the OBE and remote system management servers (e.g., SCMS [via the LOP], and software update servers) establishment time shall be less than 10 seconds. A request/response transaction shall be considered to be "established" when the transaction can be resumed, or continued at a subsequent RSE encounter (i.e., sufficient data has been exchanged to support either data exchange or resumption of data exchange at a later RSE encounter).

Test Setup:

Note: Assuming the certificate request has been made in the Simulated Certificate Request Test, the SCMS will require some finite time to process the request and generate the certificates. After this time has elapsed, the test can begin.

1) Configure RSE to provide routing to the SCMS (or a simulated SCMS). It is assumed that the round trip time delay has been measured for the server and backhaul.
2) Configure the RSE to send a WSA on the control channel every 100 msec, including the channel information (e.g., IP address, available service channel for the routing service, etc.) at 20 dBm.

Test Procedures:

1) The Test Vehicle approaches an RSE which is advertising connectivity to the SCMS (or some similar suitable PSID associated with such a service) using a conventional WSA.
2) The Vehicle System receives the WSA and initiates an IP session to retrieve certificates.
3) As the Test Vehicle approaches the RSE, the security management application will send the certificate retrieval request to the SCMS.
4) The sending action shall be logged in the Vehicle Test System and these logs will then be compared to the RSE logs to a) determine if the transaction was initiated, and b) determine the length of the transaction time.
5) The SCMS shall respond by sending the certificate bundle back to the Test Vehicle as a series of IP packets.
6) A successful test will deliver the requested certificates to the Test Vehicle within the time of the RSE encounter.

14.1.7.4 Simulated Certificate Delivery II (Resumed Transaction)

Objective(s): Verify that the OBE can complete request and response transactions with remote system management services with service interruptions.

Responsible Entity: OEM; oversight entity

Aligned Requirements:

- [18A] Request and Response transactions between the OBE and remote system management servers (e.g., SCMS [via the LOP], and software update servers) shall support service interruptions such that the transaction can be continued during a subsequent connectivity event (e.g., RSE encounter).

Test Setup:

Note: This test assumes that the vehicle system has the ability to support multi-encounter certificate data exchanges (and other multi-encounter data exchanges). Assuming the certificate request has been made in the Simulated Certificate Request Test, the SCMS will require some finite time to process the request and generate the certificates. After this time has elapsed, the test can begin.

1) Configure RSE to provide routing to the SCMS (or a simulated SCMS). It is assumed that the round trip time delay has been measured for the server and backhaul.
2) Configure RSE power level to limit the overall range of the RSE and the duration of the data exchange encounter.

Test Procedures:

1) The Test Vehicle approaches an RSE which is advertising connectivity to the SCMS (or some similar suitable PSID associated with such a service) using a conventional WSA.
2) The Vehicle System receives the WSA and initiates an IP session to retrieve certificates.
3) As the Test Vehicle approaches the RSE, the security management application will send the certificate retrieval request to the SCMS.
4) The sending action shall be logged in the Vehicle Test System and these logs will then be compared to the RSE logs to a) determine if the transaction was initiated, and b) determine the length of the transaction time.
5) The SCMS shall respond by sending the certificate bundle back to the Test Vehicle as a series of IP packets.
6) The vehicle will leave RSE radio coverage before the complete certificate bundle has been delivered.
7) The vehicle will then return to the RSE (or encounter another RSE with connectivity to the SCMS) and the certificate delivery session will resume.
8) A successful test will deliver the requested certificates to the Test Vehicle during the second encounter.

14.1.8 Recommended Vehicle Level Test Sequence

The tests may be run in any order. However, it is assumed that the following sequence will provide the simplest test logistics.

1) Self-test
2) Transmit Power and Antenna Gain and Sensitivity Envelope
3) Simulated Certificate Request
4) Simulated Certificate Delivery I (Complete Transaction

5) Simulated Certificate Delivery II (Resumed Transaction)
6) BSM Parameter Accuracy
7) Simulated Implausible Message
8) Simulated Signature Failure
9) Simulated Misbehavior Report Transaction

15 Appendix H. Standards Compliance Exceptions

Purpose
The purpose of this document is to itemize specific requirements identified in the various DSRC Standards that do not apply directly to V2V messaging, and are thus not included by reference (or are excluded by this document) from any general standard references in the NHTSA Requirements.

Background
In many case most of the requirements within a given standard must be met in order for the system to operate in the manner defined in the standard. In this case, it is impractical to identify those elements of a given standard that must be complied with. To simplify this process, and to relieve the overall NHTSA requirements form repeating most of any given standard, this document identifies specific elements of standards that are not applicable to V2V messaging.

SAE J2735 (2015) Exclusions
Message Sets (5.2 - the BSM is the only required message):

- 5.1
- 5.3 through 5.15

Data Frames:

- 6.2 through 6.7
- 6.10 through 6.32
- 6.34 through 6.36
- 6.38 through 6.43
- 6.45
- 6.47 through 6.63
- 6.65 through 6.68
- 6.71 through 6.73

Data Elements:

- 7.2 through 7.4
- 7.6
- 7.8
- 7.9
- 7.12 through 7.16
- 7.18 through 7.27
- 7.29
- 7.31
- 7.32
- 7.34
- 7.36
- 7.38 through 7.40
- 7.42 through 7.66
- 7.68 through 7.70

- 7.72 through 7.75
- 7.77 through 7.109
- 7.112
- 7.113
- 7.115
- 7.116
- 7.118 through 7.123
- 7.125
- 7.126
- 7.128 through 7.135
- 7.137 through 7.140
- 7.142
- 7.144 through 7.148

IEEE 802.11 (2012) Exclusions

Note: Additional certain features excluded as unnecessary for V2V may be required for overall standards compliance.

- MAC:
  - All Basic Service Set-related features (V2V uses only outside the context of a Basic Service Set (BSS): dot11OCBActivated = TRUE)
  - Data frames: everything but data frames of subtype QoS
  - Management frames: everything but the vendor specific action frame
- PHY:
  - Everything but the OFDM PHY
  - Everything but 10 MHz and 20 MHz channel spacing in the 5.9 GHz band
  - All data rates other than 6, 9, 12, and 18 Mbps may be excluded (the mandatory rate set of 802.11 requires support for additional rates, but they are not used for V2V)

IEEE 1609.2 (2013) Exclusions

The excluded features are used neither for BSM signing nor SCMS.

Exclusions based on the Protocol Implementation Conformance Statement (PICS) (Annex A of 1609.2)

- S2.1.2
- S2.1.3,
- S2.1.4.4 through 2.1.4.6.1 (the next standard version may offer alternative geographic regions that could be used for V2V)
- S2.1.7
- S2.1.8
- S2.1.10 through 2.1.12
- S2.1.15
- S2.1.17
- S2.1.19
- S2.2.6
- S3.2.1 through 3.2.3
- S3.2.14
- S3.2.18.2
- S3.2.18.3
- S3.2.25.2 through 3.2.25.3.1

- All of S5.1
- S5.2.16.2 through S5.2.16.3.1
- All of S6 (superseded by the safety pilot security documents published by RITA; may be reflected in the next revision of the standard)

IEEE 1609.3 (2010/Cor1-2012)
Note: Channel switching and synchronization, WSA reception, and IPv6 (including TCP and UDP) have not been excluded because these features may be required for certificate updates.

Exclusions based on the PICS (Annex C of 1609.3)

- N1.1.7
- N2.2.8
- N2.3.2.4 (could change depending on congestion control requirements)
- N2.3.2.5 (could change depending on congestion control requirements)
- N2.3.2.6 (could change depending on congestion control requirements)
- N3.2 and all sub-items (all provider role features may be excluded)
- N3.3.2
- N3.4, 3.4.1

If the decision is made to go with the two DSRC radio approach rather than one radio, the following additional requirements from the corresponding PICS may be excluded regarding WSAs and channel switching

- N2.2.2
- N2.2.3
- N2.2.4
- N2.2.5
- N2.2.5.1
- N2.2.5.2
- N2.2.5.3
- N2.2.5.4
- N2.2.6
- N2.2.7
- N3.1 and all sub-items (all user role features may be excluded)

IEEE 1609.4 (2010)
Note: Channel switching and synchronization, and IPv6 have not been excluded because these features may be required for certificate updates.

- Clause 5.4.3: Service channel priority (the V2V Enhanced Distributed Channel Access [EDCA] parameter set may be different than what is specified in 802.11)
- Clauses 6.2.4, 6.2.6, and 6.2.7 (the Time Advertisement frame may be excluded)

Exclusions using the PICS (Annex G of 1609.4):

- M2.
- M5.5.1.2
- M5.5.1.3
- M6.1 (there may be a discrepancy in the standard that needs to be fixed regarding user priority (EDCA must be used, but the parameter set can be different than the default)
- M6.3
- M6.3.1

- M6.4
- M6.5
- M7.2

If the decision is made to go with the two DSRC radio approach rather than one radio, the following additional requirements from the corresponding PICS may be excluded regarding WSAs and channel switching

- M5.1
- M5.3
- M5.4
- M5.5
- M5.5.2
- M5.5.3
- M6.7
- M7.1
- M7.4

IEEE 1609.12 (2012)

IEEE 1609.12 defines identifiers and their assignments for use in WAVE systems. The PSID is used to identify the service or application area (e.g. V2V safety awareness). The Ethertype is used to identify the type of message or datagram (e.g. WSM or IPv6), the Object Identifier (OID) is used to identify the Management Information Base (MIB) attributes associated with each standard as implemented in each device, and the Organizationally Unique Identifier (OUI) is used to identify the vendor specific action frame in 802.11 for sending WAVE service advertisements in accordance with IEEE 1609.3.

Exclusions:

- All PSIDs except hex 0x20 and 0x23 (0x20 is used to identify the BSM, and 0x23 is used to identify SCMS).

Note: All Ethertype, OID and OUI values cited in the standard are used (not excluded).

16 Appendix I. Overview of Cybersecurity Guidance and Best Practice Management in Other Industries

Refer to file “FINAL_AppendixI_DSRC_PhaseII_SurveyCybersecurityStandardsBodies” for the full overview of cybersecurity guidance and best practice management in other industries.

17 Appendix J. Analysis of Received Power vs. Range for Rural and Urban Environments

The analysis in this section includes a link analysis for V2V communications, based on two propagation models:

1. Two-Ray Approximation
2. Derived Urban Model

The two-ray approximation model provides the calculated path loss in a rural environment, which corresponds to the measurements discussed in section 4.3.3. The derived urban model was developed using a microcellular path loss model found in Siwiak's Radiowave Propagation and Antennas for Personal Communications (see references).

The path loss for the two-ray approximation is given as:

Two Ray Approx. Path Loss =

$20*\mathrm{Log}((4*\pi*d)/\lambda)$, for $d < d_{bp}$

$40*\mathrm{Log}((4*\pi*d)/\lambda) - 20*\mathrm{Log}((4*\pi\lambda*d_{bp})/\lambda)$ for $d > d_{bp}$

Where: λ is the wavelength (λ = c/frequency), where c = the speed of light, 3×10^8 meters/second), *d* is the distance in meters, and d_{bp} = 4*(transmitter height in meters)*(receiver height in meters)/λ

Based on the difference between the two-ray approximation and the microcellular model in Siwiak, the Siwiak model was calibrated for a transmitter and receiver height of 1.5 meters, and at a frequency of 5.9 GHz. This calibrated model is the derived urban model.[17]

Figure 161 shows the path loss of the two-ray model and the derived urban model. This analysis is used to calculate the received power at any given range as shown in

[17] The microcellular model from Siwiak is based on measurements for a microcellular transmitter height of 12 meters, a frequency of 1.965 GHz, and a typical mobile-height receiver antenna. It is given as follows:

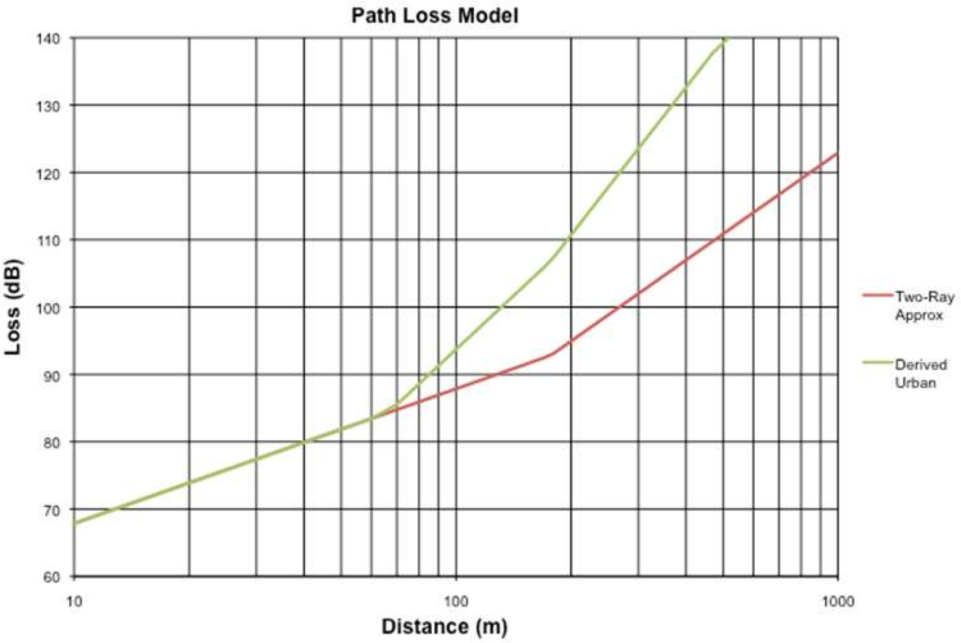
Path Loss = 71.2 +52.9 * Log (*d*/1000) + 65.9

Using the two-ray model at 1.965 GHz with a 12-meter transmitter antenna height and a receiver antenna height of 1.5 meters, the difference between this two ray approximation and the model in Siwiak was used to calibrate the model in Siwiak for V2V links at 5.9 GHz:

Derived Urban Path Loss = [Two Ray Approximation (5.9 GHz)] + [Siwiak (1.965 GHz) - Two Ray Approximation (1.965 GHz)], which applies when the path loss for the calibrated Siwiak model is greater than the two-ray approximation loss (otherwise the two-ray approximation applies). This calibrated model is the derived urban model for V2V links.

Figure 162.

Figure 161: Path Loss vs. Distance for the Two-Ray Model and the Derived Urban Model (Source: USDOT)



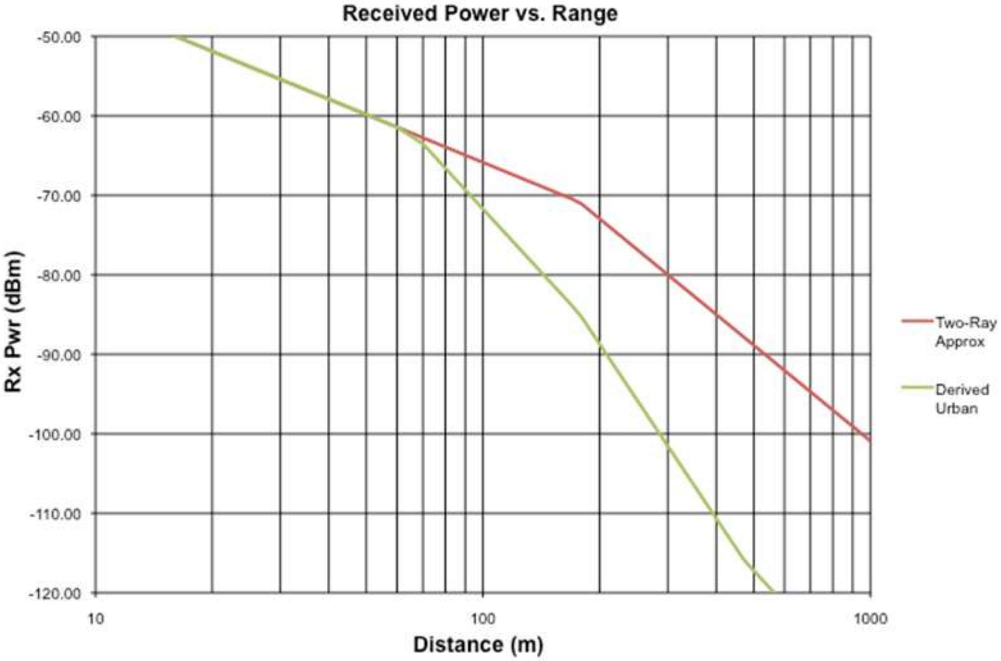
The following parameters were used to calculate received power versus range for each of the models:

Transmit Power:	20 dBm
Transmitter and Receiver Antenna Gain:	6 dB
Transmitter and Receiver Cable/Insertion Loss:	5 dB
Receiver Sensitivity:	-92 dBm (at 6 Mbps)

Using these parameters and the two models, the received power versus range calculations are shown in

Figure 162.

Figure 162: Received Power vs. Range Calculations (Source: USDOT)



The two-ray approximation model proves a quite accurate representation of a rural environment, given that with a receiver sensitivity (the minimum received power for a PER less than 10%) of -92 dBm, the calculated range is approximately 600 meters, and the range measurements in Section 4.3.3 show an error-free range of about 575 to 600 meters depending on the device supplier.

The derived urban model provides a good estimate of the performance in an urban environment, and with a receiver sensitivity of -92 dBm the maximum range is about 220 meters. As expected the performance in an urban environment is significantly degraded compared to an open environment such as that in which the measurements in Section 4.3.3 were collected. Future work may include validation of this derived urban model through measurements, which can be used to create a more real-world simulation environment resulting in accurate simulation results.

Refer to file “FINAL_AppendixJ_V2V_LinkBudget” for full DSRC V2V link budget analysis.

18 Appendix K. Extensibility of Recommended Requirements to Heavy Vehicles

While developing recommended communications performance and security V2V DSRC requirements and compliance test procedures, the team focused on the minimum necessary requirements for an interoperable, effective, and efficient system. In doing so, the team believes that the majority of the recommended requirements could also be applied to heavy vehicles. However, differences in the purpose and use of heavy vehicles from light vehicles may result in slightly different requirements in certain areas. In most cases, heavy vehicles are much larger, more expensive, more complex in terms of their internal systems, and pose a greater physical risk. Heavy vehicles may also carry high value and/or hazardous cargo (e.g., trucks) or a large number of people (e.g., buses) that create a higher impact in the event of physical accidents or cyber security incidents. Many heavy vehicles also have multiple aftermarket devices and systems designed to facilitated additional control and communication capabilities. This is another unique consideration in ensuring an integrated, secure vehicle that creates value rather than an additional burden or distraction.

Communications Performance

Although a more in depth study is required, the majority of recommended functional and performance requirements for light vehicles should also apply to heavy vehicles. The primary differences affecting communications performance in heavy vehicles are the vehicle dimensions, and possible presence of an articulating trailer. As a result, adjustments in the transmit power and antenna gain envelope, as well as the required BSM parameters, would be necessary for heavy vehicle requirements. It is also important to understand how trailer dimensions and relative position and angle of trailer and cab would be reflected in the BSM.

18.1.1 Transmit Power and Antenna Gain Envelope

The existing recommended requirement for transmit power and antenna gain envelope is based on light vehicles with an average height of 1.5 meters. Current recommended requirement:

- Transmit power and antenna gain shall be greater than -70 dBm when measured at 30 meters in all azimuth directions and between ±10 degrees elevation from the transmitting vehicle antenna(s), with the vehicle antenna(s) mounted to the vehicle in its production location and orientation

While the transmit power and antenna gain would still need to be greater than -70 dBm when measured at 30 meters in all azimuth directions, the ± degrees in elevation would need to be adjusted considering the height of heavy vehicles. The degrees in downward elevation would need to be increased while the degrees in upward elevation could probably be decreased. These angles may also differ based on the various heavy vehicle class segments. Additional analysis and simulation would be necessary to determine the new elevation angles to ensure heavy vehicles could reliably communicate with light vehicles in general, as well as at the crest of a hill and sag of a valley.

In addition, the impact of a large trailer on the DSRC antenna gain envelope is not well understood. If the antenna is mounted to the cab of the vehicle, then it is unclear how the presence of a trailer will impact the communications performance to the rear of the vehicle, or to the rear sides of the vehicle when turning. It might be necessary to investigate a multiple antenna solution.

18.1.2 BSM Parameters

The recommended BSM accuracy requirements are based on simulations with light vehicles in various collision and near miss scenarios and a collision buffer zone of 1.5 meters. Current recommended requirement:

- The data parameters provided in a BSM generated by the host vehicle shall conform to the following maximum error tolerance requirements
    - Horizontal position: 0.325 meters
    - Vertical position: 2 meters
    - Speed: 0.015 meter/second
    - Heading: 0.1 degrees
    - Time Accuracy: 2 msec (GPS)
    - Longitudinal acceleration: 0.04 meters/second2
    - Yaw Rate: 0.12 degrees/second

While all of these parameters would likely stay the same for heavy vehicles, the BSM will have to take the size of the vehicle into account along with whether it has an articulating trailer. During the plausibility, hazard detection, and BSM parameter error tolerance simulations, the team used a collision buffer of 1.5 meters for simulating light vehicles. New simulations would have to be conducted to determine the BSM parameter accuracy requirements and/or the need for an enhanced BSM for the much larger heavy vehicles. A solution would have to consider articulated vehicles and longer non-articulated vehicles. The team understands that CAMP has already provided recommendations for a Tractor-Trailer BSM (TT BSM) that modifies the BSM Part II to account for articulating trailers.

An additional issue is the correspondence between the tractor cab of the truck and the trailer. In many cases the trailer and tractor are separate units, possibly owned by different entities, and typically not always operating together (i.e., tractor cabs operate with many different trailers and vice versa). This means that a cab that would presumably be generating BSMs must either have some means for determining any characteristics of the trailer or its contents that would need to be transmitted in a BSM (for example, at a minimum the size and weight of the trailer), or the trailer must generate and send its own BSMs which would then need to be linked with the cab BSMs by the receiver.

Security

Heavy vehicles have a number of unique characteristics that may require different and/or more stringent security requirements than light vehicles. Heavy vehicles of all classes are being equipped with aftermarket features and functions (e.g., wireless interfaces and automation) that result in new attack surfaces. These surfaces have already been demonstrated to serve as entry points and launching pads for attacks on passenger cars. Many of these newer features facilitate information exchange and are connected to electronic and control systems, including interfaces to the future

DSRC radio and processors. In addition, fleets that outfit a large number of heavy vehicles with vulnerable after-market devices create inviting targets for attackers who can develop and use a single attack across a large number of targets. A number of heavy vehicles operating on the highway in cooperative platoons might also represent an inviting target for an attacker who simply wants to disrupt the platoon's efficiency, cause the platoon to change course, apply unintended braking, or use the platoon as a weapon. While light-vehicle applications of DSRC are currently targeted at warning-only, these heavy vehicle applications intend to use DSRC for safety-sensitive control applications. Heavy vehicle transport that can be slowed or stalled could have a significant impact on the economy and the delivery of goods and raw materials. Heavy commercial vehicles may also have a longer life than passenger cars; thus, the risks over the extended life of a heavy vehicle could be more significant.

While some of the privacy-related requirements may possibly be less stringent for heavy vehicles, there will likely need to be additional and more detailed security requirements. Some aspects of privacy, such as individual privacy and non-trackability are not as critical since most organizations with heavy vehicle fleets keep track of their vehicles/operators (but would not want to be tracked or identified by the general public or competitor organizations). These vehicles are highly regulated and already track hours of service, load origin/destination, etc. A crucial difference in heavy vehicles and light vehicles is the modular design and prevalence of aftermarket equipment designed to monitor the health of the vehicle and optimize operations. These are additional attack surfaces that need to be considered in regard to securing connections between sensors, etc.

While considerably more research is necessary to determine final recommended V2V heavy vehicle security requirements, the team has identified four primary areas where requirements may differ from those recommended for light vehicles. These are the Component, Hardware, Platform, and Software objective areas and the associated security functional requirements.

18.1.3 Component

While the heavy vehicle Component objectives would likely remain very similar to those recommended for light vehicles, O.Component.4 and O.Component.6 are only recommended as best practices for light vehicles and should probably be requirements for heavy vehicles. Current recommended objectives:

- O.Component.4: TOE shall create secure logs based on its monitoring of essential components.
- O.Component.6: TOE shall report to external authorities (i.e., SCMS) or maintenance services when essential components (e.g., OBE, sensors, GNSS receiver) within the TOE are not functioning properly.

18.1.4 Hardware

Heavy vehicles may require more secure hardware than light vehicles because of the more significant impact misbehavior could play on a much larger and more expensive vehicle that could possibly be hauling high value and/or hazardous goods. This could possibly mean adhering to FIPS 140-2 Level 3 instead of Level 2 as recommended for light vehicles, along with additional hardening against intrusion and side-channel attacks. Current recommended objectives:

- O.Hardware.1: TOE shall only use security hardware (e.g., Cryptographic Module, security microcontroller) that has appropriate level of security.

- O.Hardware.3: Cryptographic algorithms shall not be implemented in an application-specific integrated circuit (ASIC) but in a general purpose processor that is hardened against intrusion and side-channel attacks.

18.1.5 Software

As with the hardware objectives and requirements, the software used in heavy vehicles would probably need to resist attackers with a higher Attack Potential than the software in light vehicles because the more significant impacts that hacking and intrusion activities could cause on heavy vehicles. Current recommended objectives:

- O.Software.1: Software implementations on TOE shall follow best practices for secure implementation, including for example having proper access control, malware detection and preservation of a secure state in case of failures.
- O.Software.2: TOE shall perform system diagnostics, including industry best practice intrusion detection and reporting as appropriate, on a regular basis.
- O.Software.4: The system specification shall implement physical and logical isolation measures to separate critical systems from non-critical systems.

18.1.6 Platform

As a result of different Hardware and Software objectives and requirements, heavy vehicles could need a more secure platform in which to provide proper implementation. Current recommended objective:

- O.Platform.1: The TOE platform shall provide hardware support for appropriate secure software implementation on the TOE.

19 Appendix L. References

Unless otherwise specified within the report, all graphics were developed by the Booz Allen team.

Abdel-Hafeez, K., Zhao, L., Ma, B., & Mark, J. W. (2013). Performance Analysis and Enhancement of the DSRC for VANET's Safety Applications. IEEE.

Al-Khalil, A. B., Al-Sherbaz, A., & Turner, S. (2013). Enhancing the Physical Layer in V2V Communication Using OFDM–MIMO Techniques. Architecture, 1, 10.

Andrews, S. Systematic Development of Positioning Requirements for Vehicle Applications. Aeronautical Radio, Inc. (ARINC) Incorporated under contract for the USDOT.

ARINC Incorporated. (April 2012). Vehicle Positioning Trade Study for Intelligent Transportation (ITS) Applications. Washington, DC: ITS Joint Program Office (JPO), RITA, USDOT Publication.

American Society for Testing and Materials (ASTM) International. (2010). Standard Specification for Telecommunications and Information Exchange Between Roadside and Vehicle Systems — 5 GHz Band DSRC MAC and PHY Specifications. West Conshohocken, PA.

Bai, F., Stancil, D. D., & Krishnan, H. (September 2010). Toward understanding characteristics of DSRC from a perspective of vehicular network engineers. In Proceedings of the sixteenth annual international conference on Mobile computing and networking (pp. 329-340). Association for Computing Machinery (ACM).

Booz Allen Hamilton Inc. (15 May 2013). Aftermarket Safety Device Certification Test. [Supplier B] Platform Test Report, Washington D.C., USDOT.

Booz Allen Hamilton Inc. (2011). 5.9 GHz DSRC Aftermarket Safety Device Specification Version 3.0, Count 6, Washington D.C., USDOT.

Booz Allen Hamilton Inc. (2012). 5.9 GHz DSRC Roadside Equipment Device Specification Version 3.0, Count 7, Washington D.C., USDOT.

Booz Allen Hamilton Inc. (2012). 5.9 GHz DSRC Vehicle Awareness Device Specification Version 3.6, Count 17, Washington D.C., USDOT.

Booz Allen Hamilton Inc. (May 2013). Communications Data Delivery System Analysis for Connected Vehicles – Revision 5, Federal Highway Administration (FHWA), USDOT.

Booz Allen Hamilton, Inc. (January 2014). Development of DSRC Device and Communication System Performance Measures: Analysis of DSRC Operational Needs and Performance Measures. Washington, DC: NHTSA, USDOT.

Booz Allen Hamilton Inc. (2013). In-Vehicle Safety Device (Aftermarket Safety Device) Certification Testing Final Test Reports (Savari, Arada, Denso and Cohda), Washington D.C., USDOT.

Crash Avoidance Metrics Partnership. (April 2014), Interoperability Issues of Vehicle-to-Vehicle Based Safety Systems Project (V2V Interoperability) Phase I Final Report, FHWA/NHTSA, USDOT.

Crash Avoidance Metrics Partnership. (February 2015). Interoperability Issues of Vehicle-to-Vehicle Based Safety System Project (V2V-Interoperability) Phase 2 Final Report Volume 1 – Communications Scalability for V2V Safety Development, USDOT.

Crash Avoidance Metrics Partnership. (November 2014). Interoperability Issues of Vehicle-to-Vehicle Based Safety Systems Project (V2V-Interoperability) Phase 2 Final Report Volume 3 – Security Research for Misbehavior Detection, USDOT.

Crash Avoidance Metrics Partnership. (December 2014). Vehicle-to-Vehicle Systems Engineering and Vehicle Integration Research for Deployment (V2V-SE) - On-board Minimum Performance Requirements for V2V Safety Systems, v1.0, USDOT.

Crash Avoidance Metrics Partnership. (2011).
VSC-A. Final Report and Appendices. (Report No. DOT HS 811 466, 811 492A, 811 492B, 811 492C, 811 492D). Washington, DC: NHTSA, USDOT.

Crash Avoidance Metrics Partnership. (April 2011). Vehicle Safety Communications-Applications: Multiple On-Board Equipment Testing, SAE International.

Crash Avoidance Metrics Partnership. (July 2014). Vehicle Safety Communications Security Studies, Study 1: Security Credential Management System. USDOT.

Crash Avoidance Metrics Partnership. (July 2014). Vehicle Safety Communications Security Studies, Study 3 Final Report: Definition of Communication Protocols between SCMS Components and Specification of the Components Pseudonym Certificate Authority, Registration Authority, and Linkage Authority. USDOT.

Dubey, A. K., Jain, A., Upadhyay, R., & Charhate, S. V. (2008). Performance Evaluation of Wireless Network in Presence of Hidden Node A Queuing Theory Approach. IEEE.

Ekici, O. & Yongacoglu, A. (2008). Modeling Hidden Terminals in IEEE 802.11 Networks. IEEE.

Fullmer, C. L. & Garcia-Luna-Aceves, J. J. (1997). Complete Single-Channel Terminal Problems in Solutions to Hidden Wireless LANs. IEEE.

Ghaboosi, K., Latva-aho, M., Xiao, Y., & Khalaj, B. H. (2009). Modeling IEEE 802.11 DCF using Parallel Space – Time Markov Chain: Multi-Hop Ad Hoc Networks. IEEE.

Harding, J., Powell, G., R., Yoon, R., Fikentscher, J., Doyle, C., Sade, D., Lukuc, M., Simons, J., & Wang, J. (August 2014). Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application. (Report No. DOT HS 812 014). Washington, DC: NHTSA, USDOT.

Hassan, I., Vu, H. L., & Sakurai, T. (2011). Performance Analysis of the IEEE 802.11 MAC Protocol for DSRC Safety Applications. IEEE.

Hassan, M. I., Vu, H. L., & Sakurai, T. (June 2010). Performance analysis of the IEEE 802.11 MAC protocol for DSRC with and without retransmissions. In *World of Wireless Mobile and Multimedia Networks (WoWMoM), 2010 IEEE International Symposium on a* (pp. 1-8). IEEE.

Hill, C. J., & Garrett, J. K. (2011). AASHTO connected vehicle infrastructure deployment analysis. (No. FHWA-JPO-11-090).

Jaber, N., Rahman, K. A., Abdel-Raheem, E., & Tepe, K. E. (2011). A Quantitative Analysis of Improved DSRC System using Repetition Based Broadcast Safety Messaging with Hidden Terminals. IEEE.

Khurana, S., Kahol, A., Gupta, S. K., & Srimani, P. K. (1999). Performance evaluation of distributed co-ordination function for IEEE 802.11 wireless LAN protocol in presence of mobile and hidden terminals. In *Modeling, Analysis and Simulation of Computer and Telecommunication Systems, 1999. Proceedings. 7th International Symposium on* (pp. 40-47). IEEE.

Khurana, S., Kahol, A., & Jayasumana, A. P. (October 1998). Effect of hidden terminals on the performance of IEEE 802.11 MAC protocol. In *Local Computer Networks, 1998. LCN'98. Proceedings., 23rd Annual Conference on* (pp. 12-20). IEEE.

Korea Information Security Agency (May 2009). Protection Profile for Mobile Devices v2.0, National Intelligence Service Information Technology (IT) Security Certification Center.

Korea Internet & Security Agency (June 2010). ePassport Protection Profile v2.1, National Intelligence Service IT Security Certification Center.

Lan, K. C., Chou, C. M., & Jin, D. J. (2012, April). The Effect of 802.11 a on DSRC for ETC Communication. In Wireless Communications and Networking Conference (WCNC), 2012 IEEE (pp. 2483-2487). IEEE.

LeBlanc, D., & Belzowski, B. (September 2012). Interoperability Issues for Commercial Vehicle Safety Applications. (Report No. DOT HS 811 674). Washington, DC: NHTSA, USDOT.

Leith, D. J., & Malone, D. (May 2010). Field measurements of 802.11 collision, noise and hidden-node loss rates. In *Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt), 2010 Proceedings of the 8th International Symposium on* (pp. 412-417). IEEE.

Ma, X., Zhang, J., & Wu, T. (2011). Reliability Analysis of One-Hop Safety-Critical Broadcast Services in VANETs. IEEE.

Morrell, D. (1996). EEE 598C: Statistical Pattern Recognition.

SAE International (2009). DSRC Message Set Dictionary.

SAE International. DSRC Minimum Performance Requirements.

Sassi, A., Charfi, F., Kamoun, L., Elhillali, Y., & Rivenq, A. (2014). OFDM transmission performance evaluation in V2X Communication. arXiv preprint arXiv:1410.8039.

Senthilkumar, T. D., Krishnan, A., & Kumar, P. (2008). New Approach for Throughput Analysis of

IEEE 802.11 in Ad Hoc Networks. IEEE.

Shulman, M., & Deering, R. (June 2007). Vehicle safety communications in the United States. In *Conference on Experimental Safety Vehicles*.

Siwiak, Kazimierz. (1998). Radiowave Propagation and Antennas for Personal Communications, Second Edition (pp. 207-209). Artech House.

Sjoberg, K., Uhlemann, E., & Strom, E. G. (September 2011). How severe is the hidden terminal problem in VANETs when using CSMA and STDMA?. In *Vehicular Technology Conference (VTC Fall), 2011 IEEE* (pp. 1-5). IEEE.

Strom, E. G. (2013, November). On 20 MHz channel spacing for V2X communication based on 802.11 OFDM. In Industrial Electronics Society, IECON 2013-39th Annual Conference of the IEEE (pp. 6891-6896). IEEE.

Subramanian, S., Werner, M., Liu, S., Jose, J., Lupoaie, R., & Wu, X. (2012). Congestion Control for Vehicular Safety: Synchronous and Asynchronous MAC Algorithms. ACM.

Tan, W. L., Bialkowski, K., & Portmann, M. (2010). Evaluating Adjacent Channel Interference in IEEE 802.11 Networks. IEEE.

Transportation Research Institute, Oregon State University. (February 1997). Stopping Sight Distance and Decision Sight Distance, Oregon DOT.

Tsertou, A. & Laurenson, D. I. (2008). Revisiting the Hidden Terminal Problem in a CSMA/CA Wireless Network. IEEE.

U.S. Government Accountability Office. (November 2013). Intelligent Transportation Systems: Vehicle-to-Vehicle Technologies Expected to Offer Safety Benefits, but a Variety of Deployment Challenges Exist, GAO-14-13. Washington, DC.

Vehicle Infrastructure Integration Consortium (VIIC). (December 2010). Device Certification White Paper. VIIC Deployment Analysis and Policy Support Work Order #4, Task 13 Roadmap General Support Addendum.

VIIC. VIIC Key Policy Issue – DSRC Device Validation, Qualification and Certification.

Ware, C., Wysocki, T., & Chicharo, J. (2001). Hidden Terminal Jamming Problems in IEEE 802.11 Mobile Ad Hoc Networks. IEEE.

Wilshusen, G.C. (March 2006). INFORMATION ASSURANCE: National Partnership Offers Benefits, but Faces Considerable Challenges, Government Accountability Office.

Zhou, Y. & Nettles, S. (2005). Balancing the Hidden and Exposed Node Problems With Power Control In CSMA/CA-Based Wireless Networks. IEEE.

U.S. Department of Transportation
National Highway Traffic Safety Administration
1200 New Jersey Avenue, SE
Washington, D.C. 20590

Toll-Free "Help Line" 866-367-7487
www.its.dot.gov

FHWA-JPO-17-483

U.S. Department of Transportation