Determining the Interruption of Services While Performing V2I Communication Using the SPMD Prototype

Binaya Raj Joshi
University of Nebraska at Omaha, bjoshi@unomaha.edu

Follow this and additional works at: https://digitalcommons.unomaha.edu/studentwork

Part of the Infrastructure Commons, Other Computer Sciences Commons, Science and Technology Studies Commons, and the Transportation Commons

Please take our feedback survey at: https://unomaha.az1.qualtrics.com/jfe/form/SV_8cchtFmpDyGfBLE

Recommended Citation
https://digitalcommons.unomaha.edu/studentwork/342

This Thesis is brought to you for free and open access by DigitalCommons@UNO. It has been accepted for inclusion in Student Work by an authorized administrator of DigitalCommons@UNO. For more information, please contact unodigitalcommons@unomaha.edu.
DETERMINING THE INTERRUPTION OF SERVICES WHILE PERFORMING V2I COMMUNICATION USING THE SPMD PROTOTYPE

A thesis

Presented to the School of Interdisciplinary Informatics Department,

College of Information Science & Technology

and the

Faculty of the Graduate College

University of Nebraska

In Partial Fulfillment

of the Requirements for the Degree

Master of Science in Information Assurance

University of Nebraska Omaha

by

Binaya Raj Joshi

November 2016

Supervisory Committee
Dr. Ken Dick – Chair
Dr. Bill Mahoney
Dr. Robin A. Gandhi
Dr. Matt Germonprez
DETERMINING THE INTERRUPTION OF SERVICES WHILE PERFORMING V2I COMMUNICATION USING THE SPMD PROTOTYPE

Binaya Raj Joshi, M.S.in IA

University of Nebraska, 2016

Advisor: Ken Dick, Ph.D.

ABSTRACT

The use of Vehicle to Vehicle (V2V), Vehicle to Infrastructure (V2I), Vehicle to Roadside Unit (V2R) and Vehicle to Other (V2X) communications are increasingly applied over existing and upcoming transportation means by the United States Department of Transportation (USDOT) and other federal agencies. From previous statistical data, these technologies would primarily avoid or mitigate vehicle crashes and would provide more safety, mobility and various other benefits on the roads (“Traffic Safety Facts 2012,” 2013; “Traffic Safety Facts 2013” 2014). During the communication processes between vehicles, infrastructures and roadside units’ various sensitive data such as positions and speed of the vehicles, are transmitted which are currently highly vulnerable. These facts are generated from this research experiment results performed on the provided data sets from the University of Michigan Transportation Research Institute (UMTRI). An interference to the vehicular communications is possible by intentional or unintentional malicious users or other elements which puts drivers at greater risk with the upcoming vehicular technology. Moreover, different agencies and private companies are
utilizing collected data from the USDOT to improve the operational volume of roads and services while avoiding accidents. They are also trying to provide other third-party Internet-based services to the consumers based on the live streaming information.

This research paper gives a detailed description of all aspects of the vehicular communications protocol (i.e. DSRC, CA, 802.11p protocol, smart infrastructure, etc.). This research paper will provide details of all identified security features (i.e. encryption methods, certificate management, physical securities, data management lifecycles, etc.) that have been applied to these mechanisms to protect the safety of drivers (Cronin, 2013). The USDOT has currently approved the implementation of a 5.9 GHz band, along with the 802.11p standard wireless protocol for dedicated short-range communications used in vehicular communication (Shankland, 2014). This research paper will also provide details of current standards and regulations which will be in effect for the upcoming vehicular technologies in the future in the US along with the susceptibilities to the interruptions of services.

Finally, this research will utilize the actual data sets compiled using the actual safety pilot model deployment (SPMD) provided by the UMRTI researchers. The analysis of these results will validate that this protocol is susceptible to interference during communications. This will be shown by plotting the latitudinal and longitudinal coordinates and thus demonstrating the occurrence of gaps within communication (i.e. interference to the vehicular communication) in the existing SPMD prototype data sets.
ACKNOWLEDGMENTS

There are several people who have contributed to this project. Dr. Ken Dick significantly and continually provided constructive techniques, principles, feedback and help. His guidance’s has kept me away from other distraction preventing from going out of track throughout this project. Credit also goes to my advisors Dr. Bill Mahoney and Dr. Robin Gandhi for their continuous advice, patience and support during the overall project.

I would also like to thank Walt Fehr, the Assistant Secretary for Research and Technology | ITS Joint Program Office in the U.S. Department of Transportation for his contribution to the project. Without his suggestion and direction toward SPMD data sets, this project would not have been a success.

But most of all I also like to thank my parents, my brothers and my cousin for their continuous support and encouragement. Especially my cousin Rajendra Adhikari, his wife Sarita Sunwar and daughter Serena Adhikari for providing me everything I needed and their unconditional support throughout my graduate study here at UNO. You all made this an unforgettable memory while changing my life. Thank you very much!!

Lastly, I would like to thank all my friends from IA department here at UNO for all their helpful discussions and suggestions toward my research project.
# Table of Contents

ABSTRACT .......................................................................................................................... ii

ACKNOWLEDGMENTS ........................................................................................................ ii

LIST OF TABLES .................................................................................................................... v

LIST OF FIGURES ................................................................................................................ vi

ACRONYMS ........................................................................................................................... viii

CHAPTER 1   INTRODUCTION ............................................................................................. 1

1.1 Vehicular Technology ...................................................................................................... 1

1.2 Vehicle to Vehicle communications (V2V) ................................................................... 3

1.3 Vehicle to Infrastructure communications (V2I) .......................................................... 3

1.4 Vehicle to Roadside Unit (V2R) ..................................................................................... 4

1.5 Vehicle to Others (V2X) [pedestrian, bicycle, etc.] ...................................................... 4

1.6 Dedicated Short Range Communications (DSRC) ......................................................... 5

1.7 Certificate Authority (CA) .............................................................................................. 5

1.8 Vehicular Networks ........................................................................................................ 5

Summary ................................................................................................................................. 6

Research Question ................................................................................................................ 7

CHAPTER 2   REVIEW OF LITERATURE ............................................................................. 8

2.1 Vehicular communication prototypes ............................................................................. 8

2.2 Smart Infrastructure architecture ...................................................................................... 9

2.3 Security challenges in overall design ............................................................................ 10

2.4 Automobile safety issue .................................................................................................. 11

2.5 Data management life cycle ............................................................................................ 12

2.6 U.S. Federal Government proposed guidance and recently proposed bill ..................... 13

Summary ................................................................................................................................. 14

CHAPTER 3   ARCHITECTURE OF VEHICULAR TECHNOLOGIES .................................. 16

3.1 Vehicular technology overall structure .......................................................................... 16

3.1.1 Wireless Network Prototype ...................................................................................... 18

3.1.2 Cryptography Algorithm ............................................................................................ 19
LIST OF TABLES

4.1 Vehicles crash Reports findings presented by NHTSA from 2005 to 2014

5.1.2 Detail Description of all RSE units used during actual experiment
LIST OF FIGURES

1.1 An example demonstrating overall vehicular communication technology

3.1 Overall structure of Vehicular technologies

3.2 Structural design in a vehicle equipped with vehicular technology

3.3 On Board Unit prototype

3.4 Overview of SCMS structure

3.5 Vehicle to Vehicle communication structure

3.6 An example demonstrating Structural design of V2I systems

3.7 Vehicle to other communication structure

4.1 Fatalities and Fatality Rate per 100 million Vehicle Miles Traveled by Year

5.1.2 Images and description of actual Safety Pilot Devices

5.1.3 Overall structure of Safety Pilot Deployment Data [27]

C.1 One Day Multi Vehicles (i.e. Overall 25000) - Zoomed out

C.2 One Day Multi Vehicles (i.e. Overall 25000) - Zoomed in from figure C.1

C.3 One Day Multi Vehicles (i.e. Overall 25000) - Zoomed in from figure C.2

C.4 One Day Multi Vehicles (i.e. Overall 25000) - Zoomed in Satellite view from figure C.3

D.1 One Day One Vehicle (Rx Device-10116) - Zoomed out

D.2 One Day One Vehicle (Rx Device-10116) - Zoomed in from figure D.1

D.3 One Day One Vehicle (Rx Device-10116) - Zoomed in Satellite view from figure D.2

E.1 One Day One Vehicle (Rx Device-10134) - Zoomed out

E.2 One Day One Vehicle (Rx Device-10134) - Zoomed in from figure E.1
E.3 One Day One Vehicle (Rx Device-10134) - Zoomed in Satellite view from figure E.2
F.1 One Day One Vehicle (Rx Device-10145) - Zoomed out
F.2 One Day One Vehicle (Rx Device-10145) - Zoomed in from figure F.1
F.3 One Day One Vehicle (Rx Device-10145) - Zoomed in Satellite view from figure F.2
G.1 Multi Days One Vehicle (Rx Device-10116) - Zoomed out
G.2 Multi Days One Vehicle (Rx Device-10116) - Zoomed in from figure G.1
G.3 Multi Days One Vehicle (Rx Device-10116) - Zoomed in Satellite view from figure G.2
H.1 Multi Days One Vehicle (Rx Device-10134) - Zoomed out
H.2 Multi Days One Vehicle (Rx Device-10134) - Zoomed in from figure H.1
H.3 Multi Days One Vehicle (Rx Device-10134) - Zoomed in Satellite view from figure H.2
I.1 Multi Days One Vehicle (Rx Device-10145) - Zoomed out
I.2 Multi Days One Vehicle (Rx Device-10145) - Zoomed in from figure G.1
I.3 Multi Days One Vehicle (Rx Device-10145) - Zoomed in Satellite view from figure I.2
# ACRONYMS

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BSM</td>
<td>Basic Safety Message</td>
</tr>
<tr>
<td>CA</td>
<td>Certificate Authority</td>
</tr>
<tr>
<td>CV</td>
<td>Connected Vehicle</td>
</tr>
<tr>
<td>CVE</td>
<td>Connected Vehicle Environments</td>
</tr>
<tr>
<td>DSRC</td>
<td>Dedicated Short Range Communications</td>
</tr>
<tr>
<td>ECU</td>
<td>Electronic Control Units</td>
</tr>
<tr>
<td>FCC</td>
<td>Federal Communications Commission</td>
</tr>
<tr>
<td>FHWA</td>
<td>Federal Highway Administration</td>
</tr>
<tr>
<td>GHz</td>
<td>Gigahertz - frequency measurement</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers</td>
</tr>
<tr>
<td>IPV6</td>
<td>Internet Protocol version 6</td>
</tr>
<tr>
<td>ITS</td>
<td>Intelligent Transport Systems</td>
</tr>
<tr>
<td>LTE</td>
<td>Long-term Evolution</td>
</tr>
<tr>
<td>MAC</td>
<td>Medium Access Control</td>
</tr>
<tr>
<td>MANET</td>
<td>Mobile Ad hoc NETwork</td>
</tr>
<tr>
<td>NHTSA</td>
<td>National Highway Traffic Safety Administration</td>
</tr>
<tr>
<td>OBU</td>
<td>On Board Units</td>
</tr>
<tr>
<td>RSU</td>
<td>Road side Unit</td>
</tr>
<tr>
<td>SPMD</td>
<td>Safety Pilot Model</td>
</tr>
<tr>
<td>SCMS</td>
<td>Security Certificate Management System</td>
</tr>
<tr>
<td>SPAT</td>
<td>Signal Phase and Timing</td>
</tr>
<tr>
<td>TTL</td>
<td>Time to Live</td>
</tr>
<tr>
<td>USDOT</td>
<td>U.S. Department of Transportation</td>
</tr>
<tr>
<td>VANET</td>
<td>Vehicular Ad hoc NETwork</td>
</tr>
<tr>
<td>V2I</td>
<td>Vehicle to Infrastructure</td>
</tr>
<tr>
<td>V2V</td>
<td>Vehicle to Vehicle</td>
</tr>
<tr>
<td>V2X</td>
<td>Vehicle to Other [pedestrian, bicycle, etc.]</td>
</tr>
<tr>
<td>V2R</td>
<td>Vehicle to Roadside Unit</td>
</tr>
<tr>
<td>WAVE</td>
<td>Wireless Access in Vehicular Environment</td>
</tr>
<tr>
<td>WLAN</td>
<td>Wireless Local Area Network</td>
</tr>
</tbody>
</table>
CHAPTER 1  INTRODUCTION

1.1 Vehicular Technology

Vehicular technology refers to wireless communications systems between two or more vehicles or vehicles to roadside infrastructures and others those are available in the streets regardless of their state of motion. In general, vehicles equipped with vehicle technology consists of equipment’s such as Vehicle On-Board Unit (OBU) used in the vehicle, Road Side Unit (RSU) used over in the infrastructures at intersections, gas stations and safe communication channel used between transmission of data to the minimal level.

Vehicular network utilizes the dedicated short-range communications (DSRC) devices, vehicular networks, certificate authority for handling quick secure transition between vehicles and infrastructure. The vehicular communications also include fast handling algorithms that use live-streaming data exchanged between vehicles and infrastructure elements to perform calculations. The transmitter presented in the OBU and RSU equipment would use the dedicated portion of wireless spectrum, new wireless standard 802.11p to authenticate each message (Faezipour, Mehrdad, Adnan, and Addepalli, 2012, pg. 90-100; Weimerskirch, n.d.)

During the vehicular communication, different critical information of vehicles such as speed, acceleration and distance along with general information such as weather and traffic are being transmitted which assist the drivers in a timely manner (“2015 FHWA Vehicle to Infrastructure”2014). Based upon the
information gathered, sorted from different vehicles during the process, it recognizes high-risk situations ahead of time and produces driver alerts and warnings. This is also known as signal phase and timing (SPAT) information, which is one of the most important advantages of using vehicular technologies (Peter, Zsolt, Szilard, 2014, #ch-9).

The effectiveness of such vehicular technologies is due to the reliability of wireless communication and transmission of vehicle data. The live data feeds from the vehicular communications at all times will initially assist drivers with the help of active safety features and can even engage in applying brakes or steering to avoid collision without the driver’s involvement in some cases.

**Figure1.1**: An example demonstrating overall vehicular communication technology [20]

The above figure shows a general architecture of how vehicular technology functions in a real world which has been presented by the wired insights for connected vehicles. It illustrates how connected vehicles would be able to communicate with each other and with smart infrastructures. This would
symbolize how the future road structure will look like with the presence of smart units in each vehicle which are capable of communicating with other vehicles and all smart technologies while secure vehicular communications take place. The following section further discusses in detail how each inter and intra vehicular communication takes place and all its necessary components which are listed as follow:

1.2 **Vehicle to Vehicle communications (V2V)**

Vehicle to Vehicle communications (V2V) refers to wireless communications between two or more vehicles, regardless of the state of motion. The upcoming vehicles would have smart on board units’ presence in each vehicle which are capable of communicating and sharing information with another vehicle. This exchange of information among vehicles are intended to improve better safety and decrease motor vehicle collisions (Peter, Zsolt, Szilard, 2014, #ch-9).

1.3 **Vehicle to Infrastructure communications (V2I)**

Vehicle to Infrastructure communications (V2I) refers to wireless communications between vehicles and the smart infrastructure, regardless of the state of motion. The smart infrastructure would include traffic light, and other infrastructures which are governmentally owned and operated. Also V2I requires cryptography operations to calculate over 200 digital signatures generated, and transmit over 1000 messages per second between the infrastructure and vehicle to efficiently perform its duty (Faezipour, Mehrdad, Adnan, and Addepalli, 2012,
It is estimated that V2I communications will help reduce additional 12 percent of crashes which had not been addressed by V2V communications (Weimerskirch, n.d.).

1.4 **Vehicle to Roadside Unit (V2R)**

Vehicle to roadside unit communications (V2R) refers to wireless communications between vehicles and the roadside unit such as businesses via internet access. V2R would be different from V2I communications as the mechanism implemented could be privately owned and operated by local businesses and services. It is estimated that with the help of smart roadside unit technology, this would not only reduce the number of road accidents, but also will help reduce travel speed while decreasing fuel consumption, making transportation more efficient. The RSU would act as a gateway to have all live traffic information provided to vehicles during the vehicular communication process. RSU would have paid services containing live feeds of info such as weather forecast, emergency vehicles notifications, parking information, and other businesses related to help people find the nearest distance to stop the vehicle (Faezipour, Mehrdad, Adnan, and Addepalli, 2012, pg. 90-100).

1.5 **Vehicle to Others (V2X) [pedestrian, bicycle, etc.]**

Vehicle to Vehicle communications (V2X) refers to wireless communications between vehicles and pedestrian or bicycle, regardless of the state of motion. The live data feeds used during vehicle to other (V2X) communications at all times
will initially assist drivers with the help of active safety features and can even engage in applying brakes or steering to avoid collision without the driver’s involvement in some cases.

1.6 Dedicated Short Range Communications (DSRC)

The DSRC is also considered as the heartbeat of this technology as it includes information such as geographic location, timestamp and speed which is being broadcasted at all-time (Peter, Zsolt, Szilard, 2014, #ch-9). Vehicular network utilizes the dedicated short-range communications (DSRC) devices which work in 5.9 GHz band with bandwidth of 75MHz spectrum and approximate range of 1000 meters (Harding, Powell, Yoon, Fikentscher, Doyle, Sade, Lukuc, Simons and Wang, 2014).

1.7 Certificate Authority (CA)

The vehicular technologies consist of Certificate Authority (CA) which generates cryptographic key which help vehicles to communicate over TLS to the RSU as it would mostly be connected at all-time (Peter, Zsolt, Szilard, 2014, #ch-9; Weimerskirch, n.d.; “2015 FHWA Vehicle to Infrastructure”2014)

1.8 Vehicular Networks

The vehicular technology uses a variation of the 802.11p wireless network standards which are used in the laptops and mobile devices which would create
communications and share speed and position information among other vehicles in 10 times per second.

Summary

The research performed and data collected will define how USDOT, NHTSA, FHWA has been more focus on the safety based upon the number of fatalities and vehicle accidents each year rather than assuring security and privacy to US citizens. During vehicular communications processes between vehicles, infrastructures, road side units and others various sensitive data such as driver’s identification, positions and speed of the vehicles, are transmitted which makes people concern about their privacy along with safety issues. Moreover, different agencies and manufacturing companies are utilizing data collected by the department of transportation to improve the structural capacity of roads, services while avoiding accidents. They are trying to provide other third party internet based services to the consumers based on the live streaming information. This exchanges are intended to improve better safety and decrease motor vehicle collisions according to the USDOT (Peter, Zsolt, Szilard, 2014, #ch-9). This paper will provide overview of the current state of overall vehicular technology; its open issues and the necessary implementations for future as recommended for the US based implementation.
Research Question

This research performed will provide detail analysis and study of results of issues listed below:

1. Can we determine that the SPMD (Safety Pilot Deployment Model) protocol is susceptible to the interruption during V2I (vehicle to infrastructure) communication and thus verify our proposed objectives using the SPMD data sets?
CHAPTER 2 REVIEW OF LITERATURE

Research primarily based on the past studies for vehicular communication technologies have focused more on the safety of human lives than the privacy and security of an individual her in the United States. There have been numerous cyber-attacks and security breaches on businesses, financial institutions, and government’s IT systems almost every day with the increase in the advancement of information technology. The danger of cyber threats in vehicular communication technologies will as well certainly rise when vehicles are online at all time, to be connected with each other or to smart infrastructures. This project illustrates the necessity for providing better safety to drivers in the United States with the upcoming vehicular communications technologies. A brief description and previous research studies concerning different aspects of vehicular communication technologies are discussed as below:

2.1 Vehicular communication prototypes

There exist large volumes of research over the vehicle to vehicle (V2V), vehicle to infrastructure (V2I), vehicle to roadside unit (V2R), vehicle to others (V2X) such as pedestrians or bicycles, and other vehicular networking technologies. An increasing amount of innovative studies are being carried out about using upcoming smarter sensor and communication mediums over vehicular technologies in order to make the roads safer, cleaner with (Festag, Alban, Roberto, Long Le and Dirk, n.d.). According to “In Vehicle Network: Attacks, Vulnerabilities and Proposed Solutions” research paper, the recent approaches applied in the implementation of future vehicular communications by
the U.S Government implies approaching vehicle which require transmitting information are at risk and are susceptible to attacks (Carsten, Todd, Mark and Jeffrey, 2015).

2.2 Smart Infrastructure architecture

The process of wireless exchange of critical safety data and active data between vehicles and the road’s smart infrastructures are known as Vehicle to Infrastructure communications. This exchange is intended to improve better safety and decrease motor vehicle collisions (Faezipour, Mehrdad, Adnan, and Addepalli, 2012, pg. 90-100). Many studies have proven that implementation of intra vehicular communications are improving. The smart architecture would be design to handle, process and store large amounts of data containing personal identifiable information of individuals which is major challenge towards implementing mandatory regulation by the US federal government in the upcoming vehicular communications (“2015 FHWA Vehicle to Infrastructure”2014).

The 2015 FHWA Vehicle to Infrastructure deployment guidance and products document mentions “FHWA will develop materials needed to support deployment (e.g. guide tools and best practices); ensure that deployed services are geographically interoperable and ensure that deployed services are developed in accordance with the requirements in Part 940 of Title 23 within the Code of Federal Regulations (23 CFR 940) and other applicable regulations” (“2015 FHWA Vehicle to Infrastructure”2014). With the continuous progression of
capability and complexity of vehicular technologies, security issues arise to both intra-vehicle and inter-vehicle systems evolving in our daily lives (Zheng, Wenchao Li, Gerard, Zhu, and Shankar, 2015). The research paper “Future Cars: Necessity for an Adaptive and Distributed Multiple Independent Levels of Security Architecture” describes how security must be treated holistically and the design be suitable for adaptability and must also provide multiple independent levels of security for each architecture (Camek, Christian, Alois, 2013, pg. 17-24). This research argues the upcoming vehicular communication technologies proposed in the United States would have security challenges, privacy concerns along with safety issue for protecting more human lives (Camek, Christian, Alois, 2013, pg. 17-24; Zeman, 2015; “2015 FHWA Vehicle,” 2014). Some studies have delineated the following aspects:

2.3 **Security challenges in overall design**

With the evolving smart infrastructure in place by the US government for gathering experimental data and also while trying to mandate it as regulation, upcoming vehicular technologies rises a lot of security challenges as debated by numerous scholar’s research papers. It has been shown from research records that most manufacturing industries producing vehicles with vehicular products lack appropriate security measures to protect against sophisticated hackers (Zeman, 2015). “The Security Certificate Management System (SCMS) is a critical component of the CV environment designed to protect the security of the BSM data exchanged by vehicles and between vehicles and infrastructure” (“2015
FHWA Vehicle to Infrastructure”2014). Multiple research papers and experiments have proven the lack of adequate security measures by the US Government to the upcoming vehicular technology which will threaten the confidentiality and safety of all citizens, while trying to mandate these measures as law to provide safety. As discussed by few research papers, the advancement in the security policy by the USDOT & FWHA must ensure the minimum requirements and limitations on the use of DSRC broadcasted information by police or DMV, and must clearly outline the revocation and re-installation procedure of DSRC unit to identify any made-up revocation for wrong operation (Weimerskirch, n.d.). One of the recommendations delivered by a research study for reliability of expected packets sent through the smart infrastructure was to implement the level of trustworthiness for DSRC unit that could display the applied level of physical security (Weimerskirch, n.d.).

2.4 Automobile safety issue

According to the research performed in the town of Ann Arbor, Michigan, by the University of Michigan and NHTSA, it was found that the vehicular technology could prevent more than half a million accidents and more than a thousand fatalities in the United States every year (Shankland, 2014). These experiments were performed using over 3000 cars equipped with vehicular communications devices to evaluate the overall significance of the vehicular networking technology (Shankland, 2014). Also it has been reported by the NHTSA that the number of people who died in roadway crashes decreased from
33,561 on 2012 to 32,719 on 2013; a 3.1 percent decrease in roadway crash fatalities (“Traffic Safety Facts 2012”, 2013; “Traffic Safety Facts 2013”, 2014). The NHTSA also reported the number of people injured in 2013 due to vehicular collisions was 2.31 million, 2.1 percent less than in 2012 (Markey, Blumenthal, 2015). On average, the U.S highways experience approximately 43,000 fatalities per year more than 14,000 crashes per day (Faezipour, Mehrdad, Adnan, and Addepalli, 2012, pg. 90-100). This information demonstrate how the US based research are focused more towards safety rather than providing more privacy and security to an individuals and several research papers have agreed upon these testimonials (Graig, 2014; Heijden, 2010; “Traffic Safety Facts 2012”, 2013; Weimerskirch, n.d.).

2.5 Data management life cycle

Research primarily based on a draft of deployment guidance and products have revealed that the FHWA, NHTSA and USDOT do not have any applicable policies or procedures for the overall data management processes (“2015 FHWA Vehicle to Infrastructure”2014). “In general, Federal law does not assign ownership, access, and use limitation to broadcast data. As a result, the US.DOT and FHWA do not currently have a specific policy assigning data ownership or limiting access to BSM data” (“2015 FHWA Vehicle to Infrastructure”2014). The U.S. department of transportation and the Federal Highway Administration must ensure strong security and enforce well-structured policies for each step during the entire data management life cycle.
2.6 U.S. Federal Government proposed guidance and recently proposed bill

“Connected Vehicle Environments (CVE) are systems comprised of hardware, software, and firmware that allow for the dynamic transfer of data between vehicles and between vehicles and the infrastructure including, at a minimum, Wireless Access in Vehicular Environment (WAVE) messages defined in Society of Automotive Engineers (SAE) J2735 that are broadcast on Dedicated Short Range Communications (DSRC)” (“2015 FHWA Vehicle to Infrastructure” 2014). The USDOT has currently approved to implement a 5.9 GHz band, along with a 802.11p standard for vehicular technologies dedicated short range communications (Shankland, 2014). The USDOT currently has a well-defined and stable design to deploy the vehicular technology application but must try to resolve most of the open concerns such as geo-networking, misbehavior detection, physical security and security controllers, bootstrapping and security policies that has been discovered by some of the research studies (Weimerskirch, n.d.).

Multiple scholars of evolving vehicular technologies have stated that the implementation of US Government policies and technical implementation would jeopardize the security and privacy of any individuals using such technology. Thus a current bill has been purposed by Senators Markey and Blumenthal cited as the “Security and Privacy in your Car Act of 2015” or the “SPY Car Act of 2015” in order to protect U.S. citizens from security and privacy threats to their motor vehicles and for other purposes (Markey, Blumenthal, 2015). A copy of
SPY Car 2015 Act has been reference to Appendix D of this document. This would reveal how the US government has started a process to re-identify critical and key issues to provide better safety to all citizens while providing safety by having reduced accidents with the vehicular technology.

Research studies have led the United States government to implement such techniques into transportation development projects for better safety of its citizen while on roads. The US Federal Highway Administration has proposed a mandate to take effect by 2020 in order to prevent human life loss in road accidents (Graig, 2014). This would allow USDOT and other transportation agencies to accomplish additional research, which would tighten up the security features of applications and also have strong standards implemented by then. The US based project focuses on V2V safety, communication security, and single hop V2I communication to load security credentials (Weimerskirch, n.d.).

Summary

There have been several studies completed that support the safety of drivers but few have only concentrated on the security of the vehicular communication devices which will be used by drivers. Different groups of vehicles are developed for different developmental regions based upon geographical locations and will have differences with the mechanism, spectrum and software collaboration. These protocols have proven to be much more efficient, reliable and convenient while providing safer environments for all drivers while on the road. But it is crucial for all nations to have comparably standard implementations and procedure to provide additional safety, and security of drivers with the upcoming vehicular technologies.
These studies validate how providing more safety of drivers within the US by various unauthorized users, substances and agent are becoming major challenges towards upgrading to support the vehicular technologies.
CHAPTER 3  ARCHITECTURE OF VEHICULAR TECHNOLOGIES

3.1 Vehicular technology overall structure

The vehicle communication systems are made up of hardware, software, wireless protocols, and firmware which allows means of transportation to get interconnected to be able to transfer data with other vehicles and infrastructure. According to the IEEE Vehicular Technology Magazine, guest editors have described the upcoming automobile as “Vehicle are no longer a piece of the mechanical machine but a system of computerized and highly sophisticated electronic devices with hundreds of sensors embedded with and all over them” (Zhuang, Jamalipour, Bai, Vinel, 2015). Below figure 3.1 show the overall structure and vision of vehicular technologies by different nations including the United States, the European nations, and others.
Figure 3.1: Overall structure of Vehicular technologies

In general, vehicular communication technologies consist of equipment’s and components such as vehicle On-Board Unit (OBU), Basic Safety Message (BSM), Dedicated Short Range Communication (DSRC) protocol, Wireless Access in Vehicular Environment (WAVE) protocol, Road Side Unit (RSU) protocol, Certificate Authority (CA) and Security Certificate Management System (SCMS) mechanisms.

Figure 3.2: Structural design in a vehicle equipped with vehicular technology (“2015 FHWA Vehicle to Infrastructure”2014)

These protocols are being utilized for secure channel communication purposes between vehicles, infrastructures, and others to improve road traffic safety through various smart interactive mediums. The figure 3.2 shown below shows how the On board unit prototype looks and functions in a vehicle. The OBU will be able to deliver various useful information to the vehicle not only to avoid any sort of collisions but also improve the road efficiency and safety by integrating wireless communications and informatics technology.
Above figure 3.3 shows a general structure of how the on board units’ functions in a real world. Figure 3 demonstrates a complete view of overall on board unit in a vehicle providing live feed information regarding safety to the driver of the vehicle. The live data feeds from vehicular communications at all times will assist drivers with active safety features and can even engage in applying brakes or steering to avoid the collision without the driver’s involvement in some cases.

The other different components which are essentials for vehicular communications technologies are discussed as follow:

### 3.1.1 Wireless Network Prototype

The vehicular technology uses a variation of the 802.11 wireless network standards as the core communications standard which are consumed in the laptops and mobile device to establish efficient communication regarding speed and position information among other
Vehicular network consumes the dedicated short-range communications devices which work in 5.9GHz band with bandwidth of 75MHz spectrum and approximate range of 1000 meters (Harding, Powell, Yoon, Fikentscher, Doyle, Sade, Lukuc, Simons and Wang, 2014). The DSRC is also considered as the heartbeat of this technology as it includes information such as geographic location, timestamp, and speed which is broadcasted at all-time (Weimerskirch, n.d.). The transmitter presented in the OBU and RSU equipment would use the dedicated portion of the wireless spectrum, new wireless standard 802.11p to authenticate each message (Weimerskirch, n.d.; “2015 FHWA Vehicle to Infrastructure”2014).

3.1.2 Cryptography Algorithm

Vehicular technologies utilize an incorporated cryptography algorithm to communicate efficiently and securely among vehicles and smart infrastructures. All calculations that could identify a collision or risk situation on the road would be transmitted in seconds to all vehicles in advance thus providing maximum safety of an individuals. Thus, the best advantages of such communications are the signal phase and timing (SPAT) information which transmits safety advisories and a warning to drivers among vehicle via other vehicles or infrastructure (Peter, Zsolt, Szilard, 2014, #ch-9). The vehicular technologies also consist of Certificate Authority (CA) which generates the cryptographic key and
communicates over TLS to the RSU as it would always be connected at all-time (Peter, Zsolt, Szilard, 2014, #ch-9; Weimerskirch, n.d.; “2015 FHWA Vehicle to Infrastructure”2014). The most important role of TLS protocol would be to ensure that no eavesdrop or tampering of devices takes place during any communication processes between two vehicles or vehicles to infrastructure thus providing complete assurance of security in vehicular technologies. The RSU would act as a gateway having all live traffic information provided to vehicle during the vehicular communication process. RSU would also have paid services containing live feeds of info such as weather forecast, emergency vehicles notifications, parking information, and other businesses related to helping people find the nearest distance to stop the vehicle (Weimerskirch, n.d.).

3.1.3 SCMS Manager

It stands for Security Credential Management Systems, and its purpose is to provide secure system design to the vehicular communication technologies by verifying authentic messages that are being transmitted between vehicles or the smart infrastructures. “The SCMS encompasses all technical, organizational, and operational aspects of the V2V security system that is needed to support trusted, safe/secure V2V communications and to protect driver privacy appropriately. The primary managerial component of the envisioned SCMS (called the SCMS Manager) would be responsible for managing all other component entities
(called Certificate Management Entities or CMEs) which support the different V2V security functions that, together ensure the operational integrity of the total system.” (“Vehicle-to-Vehicle Security”, 2014) It would also mitigate attacks or identify misbehavior during the vehicle communication to protect against attacks so as to ensure the privacy of all i

Figure 3.4: Overview of SCMS structure (“V2V Communication Security”, 2014)

The figure 3.4 shown above shows how SCMS Manager works and functions in the overall structure to ensure better safety and privacy of drivers during vehicular communications. The figure demonstrates a complete view of overall technical and operational aspects of SCMS Manager.
The following sections further discussed in detail about how vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), vehicle-to-roadside unit (V2R), and vehicle-to-other (V2X) structure regarding functionality, components required and how each structure differentiate among one another:

3.2 Vehicle to Vehicle (V2V)

![Vehicle to Vehicle communication structure](ZTE Corporation, n.d.)

**Figure 3.5**: Vehicle to Vehicle communication structure (ZTE Corporation, n.d.)

Above figure 3.5 shows a general structure of how Vehicle to Vehicle functions in a real world. The figure demonstrates how one vehicle communicates to other vehicles and also to the smart Infrastructures thus sharing various types of information and data essentials to aware all roads conditions among each other. From the figure shown above, we can also agree that Vehicular communication technologies are similar to that of mobile cellular networks but are specifically
developed for vehicle mobility to have better efficiency and safety of all individuals on the road.

3.3 Vehicle to Infrastructure (V2I)

![Diagram of V2I system](image)

**Figure 3.6:** An example demonstrating Structural design of V2I systems (Camek, Christian, Alois, 2013, pg. 17-24)

Above figure 3.6 shows a general architecture of how V2I systems functions which was presented by the ITS Joint Program Office, USDOT (Camek, Christian, Alois, 2013, pg. 17-24). The figure demonstrates how antenna located on OBU connects using DSRC to the antenna of RSU during V2I communications process. It too illustrates how the RSU processor connects to the router of the infrastructure would then have the IPv6 network connection, have Certificate Authority over the Centers to distribute the gathered information. It has been similarly cited in research papers that RSU would help prioritize messages to be shown based on the criticality of the messages (Peter, Zsolt, Szilard, 2014, #ch-9;
Harding, Powell, Yoon, Fikentscher, Doyle, Sade, Lukuc, Simons and Wang, 2014; Markey, Blumenthal, 2015). RSU would act as a gateway having all live traffic information provided to the vehicle during the V2I communication process. RSU would also have paid services containing live feeds of info such as weather forecast, emergency vehicles notifications, parking information, and other businesses related to helping people find the nearest distance to stop the vehicle (Weimerskirch, n.d.).

3.4 **Vehicle to Others (V2X)**

![Figure 3.7: Vehicle to other communication structure [23]](image)

Above figure 3.7 shows a general structure of how Vehicle to Others functions in a real world. The figure demonstrates a complete view of overall vehicular communications among multiple vehicle, infrastructure, and pedestrians. The figure shows how pedestrians would be obstacles for vehicle, and the vehicle could avoid the collision by getting the notification ahead of time.
CHAPTER 4  EFFECTS OF VEHICULAR TECHNOLOGIES

On average, the U.S highways experience more than five million vehicle crashes every year which includes approximately more than 30,000 fatalities (“2015 FHWA Vehicle to Infrastructure”2014). The report presented by the NHTSA has found that 32,675 people killed in roadway crashes during 2014 which is 25 percent less than the year 2005 in which 43,443 people were dead (“Traffic Safety Facts 2012”, 2013; “Traffic Safety Facts 2013”, 2014). The NHTSA has also reported the number of people that were injured in 2014 to be 2.3 million which is 13 percent less than in 2005, which shows 2.69 million of people injured due to vehicle collisions (“Traffic Safety Facts 2013”, 2014). The data gathered by the NHTSA from 2005 to 2014 in the crash records finding are shown in the table below:

**TABLE 4.1: Crash Reports findings presented by NHTSA from 2005 to 2014**


<table>
<thead>
<tr>
<th>Year</th>
<th>Number of Fatalities</th>
<th>Fatalities Rate</th>
<th>Number of injured people (million)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014</td>
<td>32,675</td>
<td>3.2</td>
<td>2.3</td>
</tr>
<tr>
<td>2013</td>
<td>32,719</td>
<td>3.2</td>
<td>2.31</td>
</tr>
<tr>
<td>2012</td>
<td>33,782</td>
<td>3.3</td>
<td>2.36</td>
</tr>
<tr>
<td>2011</td>
<td>32,367</td>
<td>3.2</td>
<td>2.21</td>
</tr>
<tr>
<td>2010</td>
<td>32,885</td>
<td>3.2</td>
<td>2.23</td>
</tr>
<tr>
<td>2009</td>
<td>33,808</td>
<td>3.3</td>
<td>2.22</td>
</tr>
<tr>
<td>2008</td>
<td>37,423</td>
<td>3.7</td>
<td>2.34</td>
</tr>
<tr>
<td>2007</td>
<td>41,059</td>
<td>4.1</td>
<td>2.49</td>
</tr>
<tr>
<td>2006</td>
<td>42,642</td>
<td>4.2</td>
<td>2.57</td>
</tr>
<tr>
<td>2005</td>
<td>43,443</td>
<td>4.3</td>
<td>2.69</td>
</tr>
</tbody>
</table>
Figure 4.1 shows a graph of the number of people who died in motor vehicle traffic crashes in the United States from 2005 to 2014. It has been projected that with the help of vehicular technologies, this would not only reduce the number of road accidents but also will assist in reducing travel speed while decreasing fuel consumption, and making transportation more efficient. The US Federal Highway Administration has proposed a mandate to take effect in the mid-2020s to prevent human life loss in road accidents (Graig, 2014). The upcoming new era connected vehicular technologies would consist of safety feature, and also the security concerns. The connected vehicles would be an improvement toward increased safety of human lives but would also concerns the security of all drivers.
The following sections further discusses in detail how both positive and negative aspects perform a significant role to the upcoming vehicular technologies which are listed as follow:

### 4.1 Improvement to the automobile safety

An experiment was performed between 2012 and 2014 by researchers at the University of Michigan in collaboration with the National Highway Traffic Safety Administration (NHTSA). During the experiment nearly 3000 cars were equipped with experimental vehicular communication technologies to study the communications records of those vehicles. Based on the reduced number of accidents and fatalities, reported by the University of Michigan, NHTSA concluded that the new vehicular technology could prevent more than half of the total accidents that occurs every year within US (Weimerskirch, n.d.). Also, NHTSA concluded that the upcoming vehicular technology would revolutionize the entire transportation industry by preventing thousands of fatalities thus would want to ultimately mandate the use of vehicular technology for safety purposes in the future (Harding, Powell, Yoon, Fikentscher, Doyle, Sade, Lukuc, Simons and Wang, 2014; “Traffic Safety Facts 2012”, 2013; “Traffic Safety Facts 2013”, 2014; Weimerskirch, n.d). The experiment performed also evaluates the overall significance of the upcoming vehicular networking technology.

The 2015 FHWA Vehicle to Infrastructure deployment guidance and products document does mention clearly in its report that “FHWA will develop materials needed to support deployment (e.g. guide tools and best practices); ensure that deployed services are geographically interoperable and ensure that deployed services
are developed in accordance with the requirements in Part 940 of Title 23 of the Code of Federal Regulations (23 CFR 940) and other applicable regulations.” (Zeman, 2015). It is similarly stated in most of the research paper that vehicular technologies will be able to take benefit of existing and evolving vehicular technologies services which are additional features or an upgrade to current vehicular technologies (“2015 FHWA Vehicle to Infrastructure”2014).

4.2 Securities threats

The protocols that have are voted for the current intra-vehicular technologies will not provide adequate security to protect against intentional and unintentional threats. There have been numerous cyber-attacks and security breaches on businesses, financial institutions, and government’s IT systems almost every day with the increase in the advancement of information technology. The danger of cyber threats in vehicular communications technologies will as well, without doubt, rise when vehicles are online at all time to connect with each other’s or the smart infrastructures.
CHAPTER 5  DETERMINING THE INTERRUPTION OF SERVICES

In this chapter, we will explore weaknesses of upcoming vehicular technologies protocol based upon the Safety Pilot Model Deployment (SPMD) Research/experiment data. The research data was obtained from https://www.its-rde.net/home website as suggested by Walton Fehr, the Assistant Secretary for Research and Technology | ITS Joint Program Office in the US Department of Transportation (USDOT).

5.1 Experimental Setup

5.1.1 Safety Pilot Model Data (SPMD) data set

The SPMD is a complete data collection effort by the researchers at the University of Michigan Transportation Research Institute (UMTRI) involved with other different research entities to test the vehicular communication devices under the real world condition (United State Department of Transportation, 2012; Basic Safety Message, 2016). Based on the facts provided in the UMTRI website, the federal agencies supporting the project are the USDOT, National Highway Traffic Safety Administration (NHTSA), Research and Innovative Technology Administration (RITA), Federal Highway Administration (FHWA), Federal Motor Carrier Safety Administration (FMCSA) and Federal Transit Administration(FTA) (United State Department of Transportation, 2012; Basic Safety Message, 2016). During this experiment nearly 3000 vehicles which includes cars, truck and transit buses were equipped with
experimental vehicular communication technologies to analyze the communications records between vehicles (United State Department of Transportation, 2012; Basic Safety Message, 2016). The entire purpose of this experiment was to demonstrate how vehicular technologies would operate in a real environment by evaluating the interoperability of Dedicated Short Range Communications (DSRC) and also the possibility, scalability and security of the protocol devices.

5.1.2 Actual SPMD experimental setup and device utilized

There were three safety pilot devices installed in multiple vehicles to perform vehicular communication during the actual experiment at Ann Arbor [27]. The list is as follow:

a. Vehicle Awareness Device (VAD)
b. Aftermarket Safety Device (ASD)
c. ASD+ Data Acquisition System (DAS)
re 5.1.2: Images and description of actual Safety Pilot Devices (United State Department of Transportation, 2012).

Above figure 5.1.2 shows the actual devices image with detail description provided by the UMTRI safety pilot website.

There were also approximately 27-30 Roadside Equipment (RSE) units that were installed around University area in Ann Arbor for the research purposes. The actual document provides information on how the devices installed includes twenty-one signalized intersections, three curve locations, and five freeway locations.

**TABLE 5.1.2:** Detail Description of all RSE units used during actual experiment [27] [28]

<table>
<thead>
<tr>
<th>RxDevice</th>
<th>SpId</th>
<th>Manufacturer</th>
<th>Location</th>
<th>Latitude</th>
<th>Longitude</th>
<th>RseCategory</th>
<th>RSEID</th>
</tr>
</thead>
<tbody>
<tr>
<td>18001</td>
<td>127</td>
<td>Savari</td>
<td>Fuller-Glen</td>
<td>42.28537</td>
<td>-83.7354</td>
<td>Signal</td>
<td>127</td>
</tr>
<tr>
<td>18002</td>
<td>126</td>
<td>Savari</td>
<td>Fuller-Maiden</td>
<td>42.28647</td>
<td>-83.73249</td>
<td>Signal</td>
<td>0126-A</td>
</tr>
<tr>
<td>Lane</td>
<td>Lane</td>
<td>Longitude</td>
<td>Latitude</td>
<td>Type</td>
<td>Number</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------</td>
<td>------------</td>
<td>------------</td>
<td>----------</td>
<td>--------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>18003 170 Savari Fuller-Cedar Bend</td>
<td>42.28714</td>
<td>-83.72381</td>
<td>Signal</td>
<td>170</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18004 171 Savari Fuller-Bonisteel Blvd</td>
<td>42.29032</td>
<td>-83.71918</td>
<td>Signal/Csw</td>
<td>0171-A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18005 194 Savari Fuller-Glazier Way</td>
<td>42.28595</td>
<td>-83.711</td>
<td>Signal</td>
<td>194</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18006 173 Savari Fuller Court</td>
<td>42.28363</td>
<td>-83.7111</td>
<td>Signal</td>
<td>173</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18007 175 Savari Fuller-Huron High Drive</td>
<td>42.2808</td>
<td>-83.70635</td>
<td>Signal</td>
<td>175</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18008 94 Savari Fuller-Geddes</td>
<td>42.2776</td>
<td>-83.699</td>
<td>Signal</td>
<td>94</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18009 153 Arada Main-Depot</td>
<td>42.28914</td>
<td>-83.7473</td>
<td>Signal</td>
<td>153</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18010 76 Savari Plymouth-Barton</td>
<td>42.29635</td>
<td>-83.7307</td>
<td>Signal</td>
<td>76</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18011 192 Savari Plymouth-Murfin Ave</td>
<td>42.29155</td>
<td>-83.71911</td>
<td>Signal</td>
<td>192</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18012 159 Savari Plymouth-Traverwood Dr.</td>
<td>42.30206</td>
<td>-83.71213</td>
<td>Signal</td>
<td>159</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18013 157 Savari Plymouth-Nixon Rd</td>
<td>42.30247</td>
<td>-83.70724</td>
<td>Signal</td>
<td>157</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18014 81 Savari Plymouth-Huron Pkwy</td>
<td>42.30258</td>
<td>-83.7043</td>
<td>Signal</td>
<td>81</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18015 86 Savari Plymouth-Green</td>
<td>42.30489</td>
<td>-83.6926</td>
<td>Signal</td>
<td>0086-A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18016 137 Savari Washtenaw-Huron Pkwy</td>
<td>42.25653</td>
<td>-83.6954</td>
<td>Signal</td>
<td>137</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18017 15 Savari Washtenaw-Pittsfield Blvd</td>
<td>42.25589</td>
<td>-83.69065</td>
<td>Signal</td>
<td>15</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18018 16 Savari Washtenaw-Yost Blvd</td>
<td>42.25517</td>
<td>-83.68771</td>
<td>Signal</td>
<td>16</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18019 38 Savari Washtenaw-US23 Ramp</td>
<td>42.2552</td>
<td>-83.68635</td>
<td>Signal</td>
<td>38</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18020 191 Savari Plymouth-Pointe West</td>
<td>42.29823</td>
<td>-83.72196</td>
<td>Csw</td>
<td>191</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18021 190 Savari Plymouth-Pointe East</td>
<td>42.29905</td>
<td>-83.7267</td>
<td>Csw</td>
<td>190</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18022 100 Savari Plymouth-Murfin Ave</td>
<td>42.29155</td>
<td>-83.71911</td>
<td>Signal</td>
<td>100</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18024 193 Savari Fuller-Glazier Way West</td>
<td>42.28744</td>
<td>-83.71449</td>
<td>Csw</td>
<td>193</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18025 172 Savari Fuller-Glazier Way East</td>
<td>42.286</td>
<td>-83.71102</td>
<td>Csw</td>
<td>0172-A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18026 862 Savari Plymouth-Green</td>
<td>42.30489</td>
<td>-83.6926</td>
<td>Signal</td>
<td>0186-B</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18027 1712 Savari Fuller-</td>
<td>42.29032</td>
<td>-83.71918</td>
<td>Signal/Csw</td>
<td>0171-B</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
5.1.3 SPMD overall structure

Below figure 5.1.3 shows the overall structure of the Safety Pilot Deployment Data and the data sets collected based on each functionality. “The SPMD data environment contains sanitized mobility data elements that were collected from nearly 3000 vehicles, equipped with connected vehicle technologies, traversing the Ann Arbor, MI transportation network. Data collected from Roadside Equipment installed at multiple locations along the transportation networks are included (United State Department of Transportation, 2012; Basic Safety Message, 2016). The data in this data environment was collected during two separate months, October 2012 and April 2013” (Basic Safety Message, 2016).
Figure 5.1.3: Overall structure of Safety Pilot Deployment Data (Basic Safety Message, 2016).
5.1.4 Actual Experiments Data Set

The genuine data sets that were gathered from the original experiments comprises of millions of individual data collected which are over 100 GB presented in multiple .csv files which are available on the USDOT Federal Highway Administration’s Research Data Exchange website (https://www.its-rde.net/home). The data sets accumulate of Basic Safety Message, Data Acquisition Systems 1, Data Acquisition Systems 2, Network, Roadside Equipment, and Weather data (Basic Safety Message, 2016). The primary goal of the field test data to be available to the public is for demonstration the actual experiment while also allowing the users to implement queries, an algorithm for better Data Warehousing purposes.

5.1.5 SPMD Samples Data Analysis

For my thesis experiment purposes, I did utilize the SPMD-one-day sample and SPMD- multi-days sample as per suggestion by Walt Fehr from the USDOT. Each of the BSM data units contains the latitude, longitude, and elevation of the vehicle and a temporary identifier as the data unit was transmitted to the road side units (Basic Safety Message, 2016). The Roadside Equipment (RSE) Data Set (BSM) subsets of data that is mainly being utilized over this experiment is:
1. Roadside Equipment (RSE) Data Set (BSM)

It contains all of those data units received at the 27 equipped intersections. The experiments also contains eight .csv files of one-day sample and thirty-two .csv for multi-day sample which were obtained from the (https://www.its-rde.net) website.

A small batch of data from both one-day and multi-days’ sample were utilized to analyze the complete the SPMD data sets assessment experiment. Python program referenced in Appendix A is written to collaborate all .csv files and write it into a single database (MongoDB) for easier sorting and analyzes. Once the database was created, then it was converted to JSON file format. Another python program referenced in Appendix B is written to visualize the JSON file format which would specify and visualize multiple maps including Geolocation points consisting Latitude, and Longitude is plotted into a single map using Google Maps.

5.2 Result Analysis

The primary goals for utilizing these data sets over this experiment was to plot sampled points of the data units transmitted within radio range of the intersection in the second set into a map. We sampled multiple devices sets containing both latitude and longitude data sets while utilizing the code referenced in Appendix B to verify the gap communication. The map is referenced in Appendix C of this document. The places where data exchange
between vehicle and transmitter does not occur verifies the interference to the vehicular communication presented in the SPMD protocol. The causes for the gap in communication are beyond the scope of this experiment and is subject to future work.

The short description of the data sets used in my experiments are defined as follow:

**RxDevice** is the ID number of the device that logs the Basic Safety Message (BSM).

**BSMID** is the ID number that is transmitted from an equipped vehicle.

**TemporaryId** is the temporary 4-byte random device identifier provided to give anonymity of vehicle. The life span of these identity remains for 5 minutes only

**DSeconds** is the time taken between the data transmission between the vehicle and roadside units.

**Latitude** is the geographical latitude of the vehicle which is represented as 32 but value

**Longitude** is the geographical longitude of the vehicle which is represented as 32 but value
CHAPTER 6  SUMMARY AND CONCLUSIONS

6.1 General Conclusions

The USDOT has currently approved the implementation of a 5.9 GHz band, along with 802.11p standard for V2V, V2I, V2R and V2X dedicated short range communications (Shankland, 2014). USDOT currently has a well-defined and established design to deploy the vehicular technology application but must try to resolve most of the open concerns such as geo-networking, misbehavior detection, physical security and safety controller, bootstrapping and security policies that have been discovered by some of the research studies (Weimerskirch, n.d.). The National Telecommunications and Information Administrator and Federal Communications Commission must guarantee that no unlicensed device be able to interfere with the Vehicle to Roadside Unit operations as unauthorized access over these mechanisms could potentially cause significant human destruction.

Two Major Contributions during my thesis research project are listed as below:
1. The detection of gaps in the SPMD data sets provided by the USDOT
2. The methodology used for analyzing the large data set for V2I communication

6.2 Answers to Research Questions

In Chapter 1 the problem statements were presented together with the research questions. After the detail analysis and thesis research performed below are the answered based upon the findings to the research questions.
1. **Can we determine that the SPMD (Safety Pilot Deployment Model) protocol is susceptible to the interruptions during V2I (vehicle to infrastructure) communication and thus verify our proposed objectives using the SPMD data sets?**

As discussed in sections 5.1 and 5.2 of this research paper, the maps representing the SPMD data sets clearly show the gaps in the communication when occurred between vehicles and roadside units.
CHAPTER 7  FUTURE WORK

7.1 Significant of the gaps between V2I communication

More data from the actual experiment done at Ann Arbor by UMTRI can be utilized to analyze the significance of the gaps between the communication in the Safety Pilot Model Deployment protocol. Advance technology and methodology might be utilized in future to identify whether the significant of gaps are caused due any available hotspot in the region or other factors.

7.2 Identify the causes of gaps

Acquiring any of the SPMD protocols products to analyze actual V2I communication data would take the research to the next level. Further detail analysis for the significant of the gaps in communication could then lead in the detection of the intentional and unintentional attack causing the gap in communication. So, moving forward if a real experiment with cars that have SPMD protocol for V2I communication can be used to find the main causes of the gaps between the communication. That way any other exposures presented in the protocol could be identified and resolved ahead of time.
BIBLIOGRAPHY


Gaspar, Peter Dr., Petra Dr. Aradi, Annamaria Decsei-Paroczi, Szilard Aradi, Zsolt Dr. Szalay. “Chapter 9 Vehicle to Infrastructure interaction (V2I)”. http://www.mogi.bme.hu/TAMOP/jarmurendszerek_iranyitasa_angol/math-ch09.html#ch-9.1


Marker animations with setTimeout(). (n.d.). from https://developers.google.com/maps/documentation/javascript/examples/marker-animations-iteration
Markey, Edward J. [D-MA], Blumenthal Richard. “To protect consumers from security
and privacy threats to their motor vehicles, and other purposes.” July, 2015.

Peter, Dr. Gaspar, Zsolt, Dr. Szalay, Szilard, Aradi, “Chapter 2. Vehicle to Infrastructure
interaction (V2I).”
http://www.mogi.bme.hu/TAMOP/jarmurendszerek_iranyitasa_angol/math-
ch02.html

Shankland, Shankland. “US to push for mandatory car-to-car wireless communications.”
wireless-communications/


U.S. Department of Transportation (2012). Safety Pilot Technology overview
[screenshots] Retrieved from
http://safetypilot.umtri.umich.edu/index.php?content=technology_overview

Vehicle-to-Vehicle Security Credential Management System; Request for Information

V2V Communication Security: A Privacy Preserving Design for 300 Million Vehicles
from

“What’s Next V2V (Vehicle-to Vehicle) Communication with Connected Cars.”
http://www.wired.com/insights/2014/09/connected-cars/


Proceeding in Communications of ACM


ZTE Corporation from


import fnmatch
import os
import csv
from collections import OrderedDict
from pymongo import MongoClient
from geopy.geocoders import Nominatim
import googlemaps

def initDatabase():
    mongo_url = 'localhost:27017'
    databaseClient = MongoClient(mongo_url)
    return databaseClient

def setupCollections():
    databaseClient = initDatabase()
    SPMD = databaseClient['SPMD']
    return SPMD

def reverseGeo(latitude, longitude):
    latlon = latitude + ',' + longitude
    geolocator = Nominatim()
    location = geolocator.reverse(latlon)
    return location.address

def get_files_list():
csv_files = []

for file in os.listdir("."):  
    if fnmatch.fnmatch(file, '*.csv'):
        csv_files.append(os.path.abspath(file))
        # print(os.path.abspath(file))

return csv_files

def csv_reader(csvfile):
    rows_list = []

    with open(csvfile, 'r') as csvread:
        print("[+] Reading CSV File {}".format(csvfile))
        csvreader = csv.reader(csvread, delimiter=',' , quotechar='|')
        next(csvreader, None)  # skip the headers
        for row in csvreader:
            # Rows from a CSV File
            required_data = OrderedDict([ )
                ('RxDevice', row[0]),
                ('BSMID',row[1]),
                ('TemporaryId', row[4]),
                ('DSeconds', row[5]),
                ('Latitude', row[6]),
                ('Longitude', row[7])
            ])

            # Modified Latitude and Longitude
### For Latitude

latitude = str(required_data['Latitude'])

if '-' in latitude:
    latitude = list(latitude)
    latitude.insert(3, '.')
else:
    latitude = list(latitude)
    latitude.insert(2, '.

required_data['Latitude'] = ''.join(latitude)

### For Longitude

longitude = str(required_data['Longitude'])

if '-' in latitude:
    longitude = list(longitude)
    longitude.insert(4, '.
else:
    longitude = list(longitude)
    longitude.insert(3, '.

required_data['Longitude'] = ''.join(longitude)

rows_list.append(required_data)

# Return all rows for a CSV File

to_return = rows_list

if __name__ == '__main__':
    SPMD = setupCollections()
SPMD_one_day_collection = SPMD['OneDaySample']
csv_files = get_files_list()

for csvfile in csv_files:
    # print("[+] Attempting reading {}".format(csvfile))
    rows_list = csv_reader(csvfile)
    for line in rows_list:

        # Request directions via public transit
        if SPMD_one_day_collection.find_one(line) is None:

            # Look up an address with reverse geocoding
            line['Address'] = reverseGeo(line['Latitude'], line['Longitude'])
            post_id = SPMD_one_day_collection.insert_one(line).inserted_id
            print(post_id)
APPENDIX B
<! DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<title>Geolocation map out with <code>setTimeout()</code></title>
<! -- Defining the css values for button -->
<style>
html, body {
    height: 100%;
    margin: 0;
    padding: 0;
}
#map {
    height: 100%;
}
#floating-panel {
    position: absolute;
    top: 10px;
    right: 5%;
    z-index: 5;
    background-color: #fff;
    padding: 5px;
    border: 1px solid #999;
}
<div id="floating-panel">
  <button id="drop" onclick="drop()">Drop Markers</button>
</div>

<script>
<! -- Pass all Latitude and Longitude value into the latlong array -->

var latlong = [

];

var markers = [];

var map;
function initMap() {
    map = new google.maps.Map(document.getElementById('map'), {
        zoom: 12,
        center: {lat: 42.2976126, lng: -83.728420}
    });
}

function drop() {
    clearMarkers();

    for (var i = 0; i < latlong.length; i++) {
        addMarkerWithTimeout(latlong[i], i * 200);
    }
}

function addMarkerWithTimeout(position, timeout) {
    window.setTimeout(function() {
        markers.push(new google.maps.Marker({
            position: position,
            map: map,
            animation: google.maps.Animation.DROP
        }));
    }, timeout);
}
function clearMarkers() {
    for (var i = 0; i < markers.length; i++) {
        markers[i].setMap(null);
    }
    markers = [];
}

<! -- Clearing the markers initially when map with center position is only loaded -->

<! -- Using Google api with key to map the geolocation -->

<script async defer src="https://maps.googleapis.com/maps/api/js?key=AIzaSyDIyIDCB_bCzjDoPRYHoyY3wIUG7LZomoY&callback=initMap">
    
    </script>

</body>
</html>

Note: This code has been directly used from google and modified to utilize a specific Latitude and Longitude. [29]
Google Maps with plotted points

**Figure C.1:** One Day Multi Vehicles (i.e. Overall 25000) - Zoomed out

**Figure C.2:** One Day Multi Vehicles (i.e. Overall 25000) - Zoomed in from figure C.1
Figure C.3: One Day Multi Vehicles (i.e. Overall 25000) - Zoomed in from figure C.2

Figure C.4: One Day Multi Vehicles (i.e. Overall 25000) - Zoomed in Satellite view from figure C.3
One Day - Single Vehicle Sample

Rx Device – 10116

**Figure D.1:** One Day One Vehicle (Rx Device-10116) - Zoomed out

**Figure D.2:** One Day One Vehicle (Rx Device-10116) - Zoomed in from figure D.1
**Figure D.3:** One Day One Vehicle (Rx Device-10116) - Zoomed in Satellite view from figure D.2
Figure E.1: One Day One Vehicle (Rx Device-10134) - Zoomed out

Figure E.2: One Day One Vehicle (Rx Device-10134) - Zoomed in from figure E.1
Figure E.3: One Day One Vehicle (Rx Device-10134) - Zoomed in Satellite view from figure E.2
RxDevice – 10145

Figure F.1: One Day One Vehicle (Rx Device-10145) - Zoomed out

Figure F.2: One Day One Vehicle (Rx Device-10145) - Zoomed in from figure F.1
Figure F.3: One Day One Vehicle (Rx Device-10145) - Zoomed in Satellite view from figure F.2
Multi Days - Single Vehicle Sample

Rx Device – 10116

Figure G.1: Multi Days One Vehicle (Rx Device-10116) - Zoomed out

Figure G.2: Multi Days One Vehicle (Rx Device-10116) - Zoomed in from figure G.1
Figure G.3: Multi Days One Vehicle (Rx Device-10116) - Zoomed in Satellite view from figure G.2
RxDevice – 10134

Figure H.1: Multi Days One Vehicle (Rx Device-10134) - Zoomed out

Figure H.2: Multi Days One Vehicle (Rx Device-10134) - Zoomed in from figure H.1
Figure H.3: Multi Days One Vehicle (Rx Device-10134) - Zoomed in Satellite view from figure H.2
RxDevice – 10145

Figure I.1: Multi Days One Vehicle (Rx Device-10145) - Zoomed out

Figure I.2: Multi Days One Vehicle (Rx Device-10145) - Zoomed in from figure G.1
Figure I.3: Multi Days One Vehicle (Rx Device-10145) - Zoomed in Satellite view from figure I.2
APPENDIX D
To protect consumers from security and privacy threats to their motor vehicles, and for other purposes.

IN THE SENATE OF THE UNITED STATES

Mr. MARKEY (for himself and Mr. BLUMENTHAL) introduced the following bill; which was read twice and referred to the Committee on

A BILL

To protect consumers from security and privacy threats to their motor vehicles, and for other purposes.

Be it enacted by the Senate and House of Representa-
SECTION 1. SHORT TITLE.

This Act may be cited as the “Security and Privacy in Your Car Act of 2015” or the “SPY Car Act of 2015”.

SEC. 2. CYBERSECURITY STANDARDS FOR MOTOR VEHICLES.

(a) IN GENERAL.—Chapter 301 of title 49, United States Code, is amended—

(1) in section 30102(a)—
(A) by redesignating paragraphs through (11) as paragraphs (10) through (17), respectively;

(B) by redesignating paragraphs through (3) as paragraphs (4) through (6), respectively;

(C) by inserting before paragraph (3), as redesignated, the following:

“(1) ‘Administrator’ means the Administrator of the National Highway Traffic Safety Administration;

“(2) ‘Commission’ means the Federal Trade Commission;

“(3) ‘critical software systems’ means software systems that can affect the driver’s control of the vehicle movement;’; and

(D) by inserting after paragraph as redesignated, the following:

“(7) ‘driving data’ include, but are not limited to, any electronic information collected about—

“(A) a vehicle’s status, including, but not
limited to, its location or speed; and

“(B) any owner, lessee, driver, or pas-

senger of a vehicle;
'entry points’ include, but are not limited
to, means by which—

‘(A) driving data may be accessed, directly
or indirectly; or

‘(B) control signals may be sent or re-
ceived either wirelessly or through wired con-
nections;

‘(9) ‘hacking’ means the unauthorized access to
electronic controls or driving data, either wirelessly
or through wired connections;’’; and

(2) by adding at the end the following:

‘§ 30129. Cybersecurity standards

‘(a) CYBERSECURITY STANDARDS.—

‘(1) REQUIREMENT.—All motor vehicles manu-
factured for sale in the United States on or after the
date that is 2 years after the date on which final
regulations are prescribed pursuant to section
2(b)(2) of the SPY Car Act of 2015 shall comply
with the cybersecurity standards set forth in para-
graphs (2) through (4).

‘(2) PROTECTION AGAINST HACKING.—
```
(A) IN GENERAL.—All entry points to the

electronic systems of each motor vehicle manu-

factured for sale in the United States shall be
```
equipped with reasonable measures to protect against hacking attacks.

“(B) ISOLATION MEASURES.—The measures referred to in subparagraph (A) shall incorporate isolation measures to separate critical software systems from noncritical software systems.

“(C) EVALUATION.—The measures referred to in subparagraphs (A) and (B) shall be evaluated for security vulnerabilities following best security practices, including appropriate applications of techniques such as penetration testing.

“(D) ADJUSTMENT.—The measures referred to in subparagraphs (A) and (B) shall be adjusted and updated based on the results of the evaluation described in subparagraph (C).

“(3) SECURITY OF COLLECTED INFORMATION.—All driving data collected by the electronic systems that are built into motor vehicles shall be
reasonably secured to prevent unauthorized access—

“(A) while such data are stored onboard

the vehicle;

“(B) while such data are in transit from

the vehicle to another location; and
“(C) in any subsequent offboard storage or use.

“(4) DETECTION, REPORTING, AND RESPONDING TO HACKING.—Any motor vehicle that presents an entry point shall be equipped with capabilities to immediately detect, report, and stop attempts to intercept driving data or control the vehicle.

“(b) PENALTIES.—A person that violates this section is liable to the United States Government for a civil penalty of not more than $5,000 for each violation in accordance with section 30165.”.

(b) RULEMAKING.—

(1) IN GENERAL.—Not later than 18 months after the date of the enactment of this Act, the Administrator, after consultation with the Commission, shall issue a Notice of Proposed Rulemaking to carry out section 30129 of title 49, United States Code, as added by subsection (a).

(2) FINAL REGULATIONS.—Not later than
years after the date of the enactment of this Act, the Administrator, after consultation with the Commission, shall issue final regulations to carry out section 30129 of title 49, United States Code, as added by subsection (a).
(3) UPDATES.—Not later than 3 years after final regulations are issued pursuant to paragraph (2) and not less frequently than once every 3 years thereafter, the Administrator, after consultation with the Commission, shall—

(A) review the regulations issued pursuant to paragraph (2); and

(B) update such regulations, as necessary.

(c) CLERICAL AMENDMENT.—The table of sections for chapter 301 of title 49, United States Code, is amended by striking the item relating to section 30128 and inserting the following:


(d) CONFORMING AMENDMENT.—Section 30165(a)(1) of title 49, United States Code, is amended by inserting “30129,” after “30127,”.

SEC. 3. CYBER DASHBOARD.

(a) IN GENERAL.—Section 32302 of title 49, United States Code, is amended by inserting after subsection (b) the following:
“(c) CYBER DASHBOARD.—

“(1) IN GENERAL.—All motor vehicles manufactured for sale in the United States on or after the date that is 2 years after the date on which final regulations are prescribed pursuant to section
3(b)(2) of the SPY Car Act of 2015 shall display a ‘cyber dashboard’, as a component of the label required to be affixed to each motor vehicle under section 32908(b).

“(2) FEATURES.—The cyber dashboard required under paragraph (1) shall inform consumers, through an easy-to-understand, standardized graphic, about the extent to which the motor vehicle protects the cybersecurity and privacy of motor vehicle owners, lessees, drivers, and passengers beyond the minimum requirements set forth in section 30129 of this title and in section 27 of the Federal Trade Commission Act.”.

(b) RULEMAKING.—

(1) IN GENERAL.—Not later than 18 months after the date of the enactment of this Act, the Administrator, after consultation with the Commission, shall prescribe regulations for the cybersecurity and privacy information required to be displayed under section 32302(c) of title 49, United States Code, as added by subsection (a).
22 (2) FINAL REGULATIONS.—Not later than 3 years after the date of the enactment of this Act, the Administrator, after consultation with the Commission, shall issue final regulations to carry out section
MDM15C25

. L.C.

8

1 32302 of title 49, United States Code, as added by
2 subsection (a).
3
4 (3) UPDATES.—Not less frequently than once
5 every 3 years, the Administrator, after consultation
6 with the Commission, shall—
7
8 (A) review the regulations issued pursuant
9 to paragraph (2); and
10
11 (B) update such regulations, as necessary.
12
13 SEC. 4. PRIVACY STANDARDS FOR MOTOR VEHICLES.
14
15 (a) IN GENERAL.—The Federal Trade Commission
16 Act (15 U.S.C. 41 et seq.) is amended by inserting after
17 section 26 (15 U.S.C. 57c-2) the following:
18 
19 "SEC. 27. PRIVACY STANDARDS FOR MOTOR
20 VEHICLES.
21 "(a) IN GENERAL.—All motor vehicles manufactured
22 for sale in the United States on or
23 after the date that
24 is 2 years after the date on which final
25 regulations are
26 prescribed pursuant to subsection (e) shall
27 comply with
the features required under subsections (b) through (d).

“(b) TRANSPARENCY.—Each motor vehicle shall pro-
vide clear and conspicuous notice, in clear and plain lan-
guage, to the owners or lessees of such vehicle of the col-
lection, transmission, retention, and use of driving data

collected from such motor vehicle.

“(c) CONSUMER CONTROL.—
```
“(1) IN GENERAL.—Subject to paragraphs (2) and (3), owners or lessees of motor vehicles shall be given the option of terminating the collection and retention of driving data.

“(2) ACCESS TO NAVIGATION TOOLS.—If a motor vehicle owner or lessee decides to terminate the collection and retention of driving data under paragraph (1), the owner or lessee shall not lose access to navigation tools or other features or capabilities, to the extent technically possible.

“(3) EXCEPTION.—Paragraph (1) shall not apply to driving data stored as part of the electronic data recorder system or other safety systems on-board the motor vehicle that are required for post-incident investigations, emissions history checks, crash avoidance or mitigation, or other regulatory compliance programs.

“(d) LIMITATION ON USE OF PERSONAL DRIVING INFORMATION.—
```
“(1) IN GENERAL.—A manufacturer (including an original equipment manufacturer) may not use any information collected by a motor vehicle for advertising or marketing purposes without affirmative express consent by the owner or lessee.
(2) REQUESTS.—Consent requests under paragraph (1)—

(A) shall be clear and conspicuous;

(B) shall be made in clear and plain language; and

(C) may not be a condition for the use of any nonmarketing feature, capability, or functionality of the motor vehicle.

(e) ENFORCEMENT.—A violation of this section shall be treated as an unfair and deceptive act or practice in violation of a rule prescribed under section 18(a)(1)(B).

(b) RULEMAKING.—

(1) IN GENERAL.—Not later than 18 months after the date of the enactment of this Act, the Commission, after consultation with the Administrator of the National Highway Traffic Safety Administration (referred to in this subsection as the ‘‘Administrator’’), shall prescribe regulations, in accordance with section 553 of title 5, United States Code, to carry out section 27 of the Federal Trade
Commission Act, as added by subsection (a).

(2) FINAL REGULATIONS.—Not later than 3 years after the date of the enactment of this Act, the Commission, after consultation with the Administrator, shall issue final regulations, in accordance with section 553 of title 5, United States Code, to carry out section 27 of the Federal Trade Commission Act, as added by subsection (a).

(3) UPDATES.—Not less frequently than once every 3 years, the Commission, after consultation with the Administrator, shall—

(A) review the regulations prescribed pursuant to paragraph (2); and

(B) update such regulations, as necessary.