D-STOP

Technical Report 135

Evaluation of Routing Protocols for Vehicular Ad hoc Networks (VANETs) in Connected Transportation Systems

Research Supervisor
Chandra Bhat
Center for Transportation Research

February 2018

Data-Supported Transportation Operations & Planning Center (D-STOP)

A Tier 1 USDOT University Transportation Center at The University of Texas at Austin

D-STOP is a collaborative initiative by researchers at the Center for Transportation Research and the Wireless Networking and Communications Group at The University of Texas at Austin.

DISCLAIMER

The contents of this report reflect the views of the authors, who are responsible for the facts and the accuracy of the information presented herein. This document is disseminated under the sponsorship of the U.S. Department of Transportation's University Transportation Centers Program, in the interest of information exchange. The U.S. Government assumes no liability for the contents or use thereof.

Technical Report Documentation Page

1. Report No.
D-STOP/2017/135

2. Government Accession No.

3. Recipient's Catalog No.

4. Title and Subtitle
Evaluation of Routing Protocols for Vehicular Ad hoc Networks (VANETs) in Connected Transportation Systems

5. Report Date
February 2018

6. Performing Organization Code

7. Author(s)
Jeffrey Andrews, Todd Humphreys, Chandra Bhat, Robert Heath, Lakshay Narula, Chang-sik Choi, Jia Li

8. Performing Organization Report No.
Report 135

9. Performing Organization Name and Address
Data-Supported Transportation Operations & Planning Center (D-STOP)
The University of Texas at Austin
3925 W. Braker Lane, Stop D9300
Austin, Texas 78759

10. Work Unit No. (TRAIS)

11. Contract or Grant No.
DTRT13-G-UTC58

12. Sponsoring Agency Name and Address
Data-Supported Transportation Operations & Planning Center (D-STOP)
The University of Texas at Austin
3925 W. Braker Lane, Stop D9300
Austin, Texas 78759

13. Type of Report and Period Covered

14. Sponsoring Agency Code

15. Supplementary Notes
Supported by a grant from the U.S. Department of Transportation, University Transportation Centers Program.

16. Abstract

Recognizing the fundamental role of information flow in future transportation applications, the research team investigated the quality and security of information flow in the connected vehicle (CV) environment. The research team identified key challenges and their potential solutions. Concerning information quality, the team conducted comparative analysis of two major enabling technologies for V2V (vehicle-to-vehicle) and V2I (vehicle-to-infrastructure) communication, namely LTE (Long-Term Evolution) and DSRC (dedicated short-range communication). Their technology standards, performance, and cost are analyzed. To facilitate the analysis, the team developed separate tools to simulate network information flow and estimate the deployment costs. Concerning information security, the team provided a critical review of potential attacks on CVs and limitations of existing DSRC standards to address these threats. The team developed a strategy based on game theory to tackle a wide range of potential attacks on CVs. Also identified were open issues that remain unsolved by existing technologies and security protocols.

17. Key Words
Connected Vehicle, V2X Communication, Information Flow Quality, DSRC Security, Cyber-Attacks

18. Distribution Statement
No restrictions. This document is available to the public through NTIS (http://www.ntis.gov):
National Technical Information Service
5285 Port Royal Road
Springfield, Virginia 22161

19. Security Classif.(of this report)
Unclassified

20. Security Classif.(of this page)
Unclassified

21. No. of Pages
20

22. Price

Disclaimer

The contents of this report reflect the views of the authors, who are responsible for the facts and the accuracy of the information presented herein. This document is disseminated under the sponsorship of the U.S. Department of Transportation's University Transportation Centers Program, in the interest of information exchange. The U.S. Government assumes no liability for the contents or use thereof.

The contents of this report reflect the views of the authors, who are responsible for the facts and the accuracy of the information presented herein. Mention of trade names or commercial products does not constitute endorsement or recommendation for use.

Acknowledgements

This research was partially supported by the U.S. Department of Transportation through the Data-Supported Transportation Operations and Planning (D-STOP) Tier 1 University Transportation Center. This work was also sponsored by the Texas Department of Transportation under Project 0-6845 entitled *Connected Vehicle Problems, Challenges and Major Technologies*.

Contents

List of Figures

List of Tables

Executive Summary

Connected vehicle (CV) technologies enable a wide range of transportation applications in safety, mobility, and infotainment. These applications range from blind spot and do-not-pass warning to variable speed limit and point-of-interest notification. While holding tremendous promise, the success of these CV-enabled applications will rely on the quality and security of the underlying information flow.

Recognizing the fundamental role of information flow in future transportation applications, this project aims to develop an up-to-date understanding of critical information flow quality and security issues, challenges, and potential solutions in CV environments. Our investigations took a two-pronged approach:

1. **Information Quality Problems**: Two major technologies, namely LTE (Long-Term Evolution) and DSRC (dedicated short-range communication), enable vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications. This report compares and analyzes these two technologies, in terms of their technology standards, performance and cost. To facilitate the analysis, the research team developed separate tools to simulate network information flow and estimate the deployment costs.

2. **Information Security Problems**: The team provided a critical review of potential attacks on CVs and the limitations of existing DSRC standards in addressing these threats. The team proposed a game-theoretic strategy to tackle a wide range of potential attacks on CVs. We also identified open issues that remain unsolved with existing technologies and security protocols.

This project's major findings and contributions can be summarized as follows:

1. **Performance of DSRC and LTE**: We found DSRC-based VANETs (vehicular ad hoc networks) are at a severe disadvantage for most situations, with the exception of extremely short-range one-hop communication between slowly moving vehicles. We tentatively concluded that DSRC may find limited use outside of short-range applications.

2. **Cost of DSRC and LTE**: The preliminary analysis indicates that the infrastructure and operations costs to ensure comprehensive DSRC-based V2I coverage would be very high. Since the LTE network already provide nation-wide coverage in most urban areas, leveraging this network is envisioned to save the infrastructure cost substantially.

3. **CV safety**: The research team established the position and velocity accuracy requirements for safe operation of CVs. We found that a vehicle's own position must be estimated with decimeter-level accuracy for lane-keeping, and that the vehicle must be able to verify a neighbor's position to within a meter to disambiguate the lane that the neighboring vehicle occupies.

4. **CV security**: We found that even if a malicious neighbor cannot present itself as a credible node of the CV network, it can perform man-in-the-middle attacks to render the CV technology ineffectual.

Based on the findings, the research team makes the following recommendations for TxDOT's consideration:

1. **Recommendation on Information Quality**: Given the limitations of the DSRC standard, we suggest TxDOT take a skeptical view as to what can be achieved with DSRC in the near future. To achieve a reliably and widely connected vehicular network, leveraging cellular technology appears to be a more plausible course of action.

2. **Recommendation on Information Security**: Infrastructural control is critical to establish secure vehicular communication, and LTE-based cellular networks provide such infrastructure. DSRC, or any alternative communication technology for CVs, should be used in combination with other modern vehicle sensors such as radar or optical cameras to enhance the security of neighbor position verification protocols. It is also suggested that standards for credential revocation in CVs be revamped to prevent attacks against CV networks.

Chapter 1

Introduction

1.1 Background

Although advancements in automotive technologies have provided improved public safety on US roads over the last two decades, further steps are required. According to the National Highway Traffic Safety Administration, in 2013 there were more than 3,000 deaths on Texas roads and more than 30,000 deaths in the United States, an alarming number. It is widely believed that emerging technologies can further decrease the number of fatalities. Connected vehicle (CV) is an application of communication technologies on vehicles. It utilize wireless communications to communicate in real-time among vehicles, network infrastructure, and/or passengers personal communications devices. It has been estimated that mature CV technology could potentially eliminate more than 80 percent of all vehicle-related crashes. CV technology presents many possible applications, provided that reliable communication takes place between moving vehicles and the network infrastructure, namely access points or base stations that are connected to the terrestrial wired network and the Internet. These applications range from collision prevention to optimal traffic control to Internet access. Although our focus is safety, mature CV technology can also have a significant impact on the U.S. economy. Given that the cost of congestion was estimated at $87.2 billion in 2011 (not to mention the environmental costs of emissions), CVs can provide economic benefits by solving congestion-related transportation problems. Many unforeseen efficiencies and economic opportunities are also likely to be opened up by CVs.

Governments, transportation agencies, private-sector companies, and academia have been actively researching and developing CV technologies for more than 10 years. Governments and regulatory agencies from the U.S., Europe, and Japan have set up rules for vehicular networks and have defined specifications to serve CVs. In addition, organizations that set standards for the field, including the Institute of Electrical and Electronic Engineers (IEEE) and the Society of Automotive Engineers (SAE), have defined communication protocols that provide interoperability among different manufacturers, such as IEEEs wireless amendments for vehicular environment (WAVE) standards protocol. In the meantime, researchers have studied challenging problems in area of vehicular ad hoc networks (VANETs) wherein the vehicles themselves form the network with little or no assistance from the network infrastructure.

1.2 Overview of Connected Vehicle Applications

1.2.1 Safety Applications

In this report we do not consider any semi- or full automated driving functions when talking about CV applications. Here safety applications specifically refer to systems designed to inform drivers of imminent or potential threats caused by vehicles or natural incidents. These applications require the target information or packets to be successfully decoded at the destination, whether vehicle or infrastructure. Safety messages that contain the host vehicles location, speed, and type are broadcast to nearby vehicles regularly or when requested. After decoding the messages, an onboard unit (OBU) on a vehicle evaluates their relevance and takes action, such as notification, warning, and even intervention. Following are some examples of important safety applications.

1. **Emergency brake warning**: When a vehicle with a communication device brakes suddenly, the vehicle broadcasts an emergency braking signal to nearby vehicles. Safety signaling is designed to reach vehicles whose vision is limited due to inclement weather or obstructing vehicles. Thus, the affected vehicle warns other drivers of potential threats in the immediate area.

2. **Blind spot and lane change warning**: As described above, a safety message including the position, speed, and acceleration of the hosting vehicle is broadcast on a regular basis. Using the messages, OBUs on the vehicles calculate and predict the trajectories of each other. If a vehicle attempts to change lanes and the two trajectories threaten to collide, the affected OBUs warn the drivers.

3. **Do-not-pass warning**: Sometimes a driver attempts to pass a slow-moving vehicle on the left without realizing that another vehicle is approaching from the opposite direction, which is particularly hazardous on roads that lack a passing lane. This

application warns the faster-moving vehicle to not pass the slow vehicle. Similarly, if a driver attempts to pass a car and there is another car ahead of it in the same lane that blocks the safe passing zone, this application informs the passing driver of that undetected danger.

4. **Cooperative forward collision warning**: A moving (and generally assumed to be autonomous driving) vehicle is informed of a vehicle approaching from behind via periodic safety messages transmitted from the approaching vehicle. Decoding the safety messages and evaluating the potential threat, the approaching vehicle triggers a forward collision warning. When nearby vehicles decode the warning message, they cooperate to avoid possible crashes by assisting drivers or taking actions cooperatively.

1.2.2 Mobility Applications

Efficient traffic control is achievable when traffic information is exchanged between neighboring vehicles and infrastructure.

1. **Variable Speed Limit**: Variable speed limit (VSL), also known as speed harmonization, has both significant mobility and safety benefits. VSL provides speed guidance to drivers, which varies smoothly over space and time based on prevailing traffic condition. Through reducing sudden brakes, it can reduce crashes as well as mitigate stop-and-go and shock waves in traffic flow.

2. **Enhanced Route Guidance and Navigation**: Roadside units (RSUs) continuously collect information about vehicles in large areas, and then acquire the latest traffic information. If a vehicle approaches a congested area, nearby RSUs inform the driver of the congested area. Drivers receiving such en-route information will be able to change their routes. This application alleviates congestion by reducing surplus demand to bottlenecks and thus increases the network-wide efficiency.

3. **Green Light Optimal Speed Advisory**: RSUs provide vehicles with information about traffic signals and surrounding traffic flow. Based on such information, if the traffic is uncongested, vehicles will be able to adjust their approaching speeds to reduce number of stops or idling time at intersections. This will help to improve driver comfort and fuel efficiency.

1.2.3 Infotainment Applications

Infotainment applications provide passengers with information about nearby attractions and can introduce new opportunities for local businesses. Furthermore, vehicles can possibly provide Internet connectivity, much like Wi-Fi hot spots, assuming they can establish a reliable connection themselves into the network. Such applications may have two impacts. From a system standpoint, such applications could reduce the idling and cruising time to seek a location, thus reducing congestion and emissions. On the other hand, excessive information may distract drivers and raise safety concerns. Last but not least, providing secure and efficient bandwidth for transmitting data would be a challenge in a hybrid system that integrates DSRC and cellular infrastructures.

1. **Point-of-interest notification**: This application allows local businesses, tourist attractions, or other points of interest to advertise to nearby vehicles. In this application, RSUs broadcast information about the places of interest and OBUs capture the information. For example, if the fuel tank is low, the vehicle display lists nearby fueling stations to the driver.

2. **Affordable in-vehicle Internet access**: CVs based on DSRC (described in the next section) can provide passengers with Internet access, turning vehicles into hot spots at a reasonable price. This application does not interfere with the current cellular communication or the in-vehicle Wi-Fi hotspots because DSRC uses different spectrum. However, we believe that providing high-speed access reliably and ubiquitously will be much harder and more expensive than DSRC proponents claim. Further, the amount of spectrum available to DSRC is an order of magnitude less than for cellular networks.

As described above, these safety and non-safety applications are available only if reliable vehicle-to-vehicle (V2V) and/or vehicle-to-infrastructure (V2I) communication is available. Because V2V and V2I communication involves reliable wireless links, modern wireless technologies are essential to the implementation of CV applications. As a result, quantitative metrics such as end-to-end delay, packet error rates, throughput, and communication overhead are major parameters that will significantly influence the performances of CV applications. Although the effectiveness of CVs is affected by qualitative factors such as market penetration and human drivers abilities to react to the provided information, this report mainly focuses on the quantitative aspects.

1.3 Scope and Outline

CV technologies underpin a large number of potential applications in safety, mobility and infotainment. Towards deployment of these applications in an effective and secure fashion, industry and academia have paid considerable attention to making connections between vehicles as secure as possible while maintaining efficient wireless network use and protecting the privacy of users of CV technology. The scope of this project is to provide an up-to-date understanding of information flow quality and security issues in CV environments, as well as preliminary guidelines for optimizing information flow in Texas. This report summarizes the key findings in this project and provides tentative recommendations for TxDOT's consideration in optimizing CV-based transportation management applications in future scenarios.

This report is organized as follows. In Chapter 2, two important CV-enabling technologies, DSRC and LTE, are reviewed and compared. In Chapter 3, security issues in CV environments are identified and potential solutions are discussed. In Chapter 4, we present two case studies on CV-enabled transportation management applications and estimates of their respective costs and information quality and security. In Chapter 5, recommendations are made based on technology features, system cost estimations and feasibility of potential business model. The report is concluded in Chapter 6 with a summary of research findings.

Chapter 2

DSRC and LTE Standards

This chapter explains current communication technologies for the CV and compares their performances and deployment costs. We consider two possible standards: DSRC and LTE. The performances of DSRC are numerically obtained by system-level simulations. Then the numerically obtained network performances such as packet delivery ratio or average throughput per vehicle are compared to that of LTE cellular communications. A cost analysis and comparison between DSRC and LTE are given.

2.1 DSRC Overview

In the United States, DSRC employs the IEEE 802.11p at the physical (PHY) layer for wireless access in vehicular environments (WAVE). This is an adaptation of the famous IEEE 802.11a standard previously used in Wi-Fi systems. DSRC also employs the IEEE 1609.2, 1609.3, and 1609.4 standards for security, network services, and multi-channel operation at higher layers in the network stack, and the SAE J2735 Message Set Dictionary for the basic safety message (BSM I and II) [1, 2]. The network layer stack for DSRC is shown in Figure 2.1.

The PHY layer of DSRC controls the transmission and reception of electromagnetic signals. The standard is very similar to the Wi-Fi standards (IEEE 802.11a, IEEE 802.11g). The spectrum between 5.850 GHz and 5.925 GHz is allocated by the Federal Communications Commission (FCC) for transportation applications. The 75 MHz spectrum is subdivided into seven channels. The seven channels (172-184) comprise six service channels (SCHs) and one control channel (CCH). Channels 172 and 184 are reserved for safety applications and channel 178 is designed for control signaling. On the other hand, channels 174, 176, 180, and 182 are reserved for non-safety applications. In order to support safety

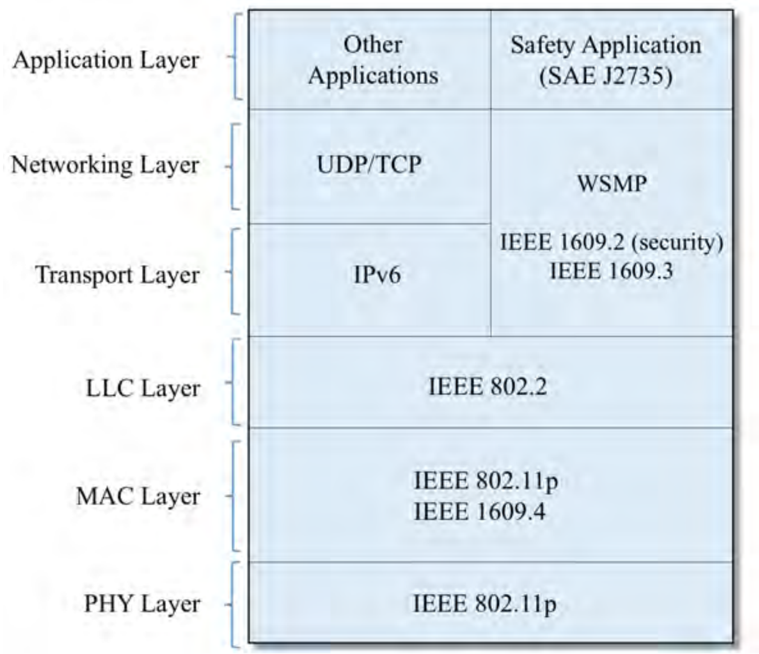


Figure 2.1: Network Layer Stack for DSRC Protocol

and non-safety applications, devices must switch between the service channels. If safety messages are congested due to the large volume of vehicle, not being able to be handled by those channels, they are transmitted via an extended channel.

IEEE 1609.4 enables devices to operate in multiple channels. The CCH is designated as a rendezvous channel; devices search for each other in the control channel and tune to a certain SCH they want to listen to. According to IEEE 1609.4, all devices should switch between SCH and CCH and the alternation is based on the time divisions.

IEEE 1609.3 is designed to enable one-hop communication with a relatively small packet size. The short packet size increases the chances of successful communications and mitigates interference. The short message is composed of a header (less than 20 bytes) and a payload (less than 200 bytes). The payload contains the host vehicles location, speed, and vehicle type.

Another important characteristic of DSRC is the protocol that is often called OCB (outside of the context of basic service set). Traditional IEEE 802.11 defines the basic service set (BSS) where messages can be exchanged. Establishing a secure BSS necessitates announcement, scanning, synchronization, and association and the time required is extremely undesirable in vehicular environments. In DSRC, the rule has been modified to support direct and nearly instantaneous link setups. Vehicles transmit wild-card messages that are designed to allow any device to process the packet instantaneously instead of joining the

BSS. This significantly reduces the time to connection.

2.2 DSRC in CV Environment

2.2.1 Physical Layer

The physical PHY layer of a VANET controls the transmission/reception of electromagnetic signals and their associated waveforms. In particular, the PHY layer is responsible for reliable communication of information bits over an established link, where the link is established by the medium access control (MAC) layer. Although the PHY layer is the most challenging and sophisticated of the layers, the technology behind it is quite mature and stable. The PHY layer in DSRC is specified by IEEE 802.11p in [3]. The IEEE 802.11 family of standards primarily comprises wireless local area network (WLAN) applications, and is best known for the now ubiquitous Wi-Fi. Although Wi-Fi includes several different and incompatible versions such as 802.11a, 802.11b, 802.11g, 802.11n, and now 802.11ac, the technology is very well developed. 802.11p is most closely related to 802.11a. In particular, 802.11a [4] is for the several unlicensed bands in the 5 GHz unlicensed band (5.155.35 GHz, 5.475.825 GHz). Since DSRC uses the spectrum between 5.850 GHz and 5.925 GHz for its 802.11p operation (in the US), it is most commonly compared to 802.11a; we summarize and compare the two standards in Table 2.1. Note that in Europe, the spectrum between 5.875 GHz and 5.905 GHz is reserved for vehicular applications, which is thus a subset of what is available in the U.S

Parameters	802.11p	802.11a
Channel bandwidth	10 MHz	20 MHz
OFDM symbol duration	8.0 μsec	4.0 μsec
Guard time (CP)	1.6 μsec	0.8 μsec
Total number of subcarriers	64	64
Number of information subcarriers	48	48
Carrier spacing	0.15625 MHz	0.3125 MHz
Modulation	BPSK, QPSK, 16-QAM, 64-QAM	BPSK, QPSK, 16-QAM, 64-QAM
Coding rate	1/2, 3/4	1/2, 3/4
Data Rates (Mbps)	3, 4.5, 6, 9, 12, 18, 24, and 27	6, 9, 12, 18, 24, 36, 48, and 54
Max Transmit Power (EIRP)	28 dBm	28 dBm
Maximum Range[1]	150 meter	60 meter
Setup speed	Instantaneous (wild card messaging)	Slow

Table 2.1: IEEE 802.11p and 802.11a Parameters

Orthogonal Frequency Division Multiplexing

The key PHY technology behind both 802.11a and 802.11p is what is known as orthogonal frequency division multiplexing (OFDM). OFDM is a computationally efficient way of overcoming the self-interference caused by multipath channels, which is a fundamental problem in high-data-rate wireless communication systems. Essentially, the many echoes created by reflections of the signal between the transmitter and receiver result in interfering versions of the signal that must be resolved in order to successfully decode the signals information symbols. This interference is called intersymbol interference (ISI) and ISI is efficiently canceled out by OFDM technology.

DSRC spectrum

The FCC assigns the bandwidth between 5.85 GHz to 5.925 GHz to the transportation applications. The DSRC bandwidth of 75 MHz is subdivided into seven 10-MHz bandwidth channels and one 5-MHz guard band. The communications in different sub channels does not interfere with each other. See Table 2.2 for details.

Channel number	Ch 172	Ch 174	Ch 176	Ch 178	Ch 180	Ch 182	Ch 184
Bandwidth	5855-5865	5865-5875	5875-5885	5885-5895	5895-5905	5905-5915	5915-5925
Class	SCH	SCH	SCH	CCH	SCH	SCH	SCH
Application	Primary safety	Extended safety		Control			Secondary safety

Table 2.2: DSRC Spectrum

The channels 172 and 184 are used only for safety purposes while other service channels serve infotainment or traffic efficiency applications.

2.2.2 MAC Sublayer

The MAC sublayer provides addressing of wireless node (station) and control wireless channel resources.

Session-based Rule

IEEE 802.11 defines the BSS of STAs (Stations) within which messages are exchanged. The order of the setup procedure is announcement, scanning, synchronization, and association. The time required to achieve an association is relatively substantial. Although the time required is acceptable for indoor communications, it is highly undesirable in the vehicular applications. The session-based rule in IEEE 802.11p has been improved dramatically to support direct and instantaneous setups. In this OCB transmission, a new six-byte BSS identifier with a wild card value is defined and the wild card frames allow any device to process the frame without joining as a BSS.

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

In addition to the enabling OCB communication, IEEE 802.11p defines a mechanism for medium control. Without proper resource control, VANETs quickly become very inefficient due to their decentralized access to wireless resources. IEEE 802.11p defines CSMA/CA to control limited resource and to manage the quality of services for various applications. The main philosophy in CSMA/CA is that a STA senses a channel and accesses it if the channel is not used by any other STAs.

2.2.3 Network and Transportation Layer

IEEE 1609.4 [5] and 1609.3[6] are standards for the DSRC middle layer. Note that DSRC supports both WAVE short message protocol [6] and IP (Internet Protocol) type communication.

MAC Extension

IEEE 1609.4 [5] allows WAVE devices to operate in the multi-channel DSRC spectrum. In order to support safety and non-safety applications, WAVE devices should switch between the channels. The 1609.4 standard introduces control channel and time division to enable multichannel operation. The control channel is a rendezvous channel for devices to meet; WAVE devices search for each other in the control channel and tune to a certain service channel. All devices should switch between service and control channels in a time division fashion.

Network and Transport Layer

In order to avoid high overhead by TCP/IP, the WAVE short message protocol is developed to enable one-hop communication with a relatively short packet size. The protocol increases the chances of successful reception and mitigates channel congestion.

2.2.4 Routing Protocols in VANETs

Table 2.3 summarizes different routing protocols. TBR refers to topology-based routing, GBR refers to geographic-based routing, and BBR stands for broadcast based routing, and CBR refers to cluster-based routing. The table shows that carry-and-forward protocols are implemented effectively in most delay-tolerant networks. The carry-and-forward algorithms increase end-to-end delay; however they can manage disconnected routes in urban areas where buildings or vehicles obstruct possible routes.

In the table, the column labeled Prediction based identifies whether a protocol uses a predictive method to decide the forward direction. Vehicle-assisted data delivery (VADD) and D-mincost predict the traffic patterns and use them to identify forward direction. Most recent protocols utilize GPS and global maps to discover the shortest paths [2].

Protocols	Class	Message forwarding	Delay tolerant	Traffic pattern	Prediction based	Overlay network	Global map	GPS	Deployment scenario
DSDV [7]	TBR	Multihop	No	No	No	No	No	No	Urban
OLSR [8]	TBR	Multihop	No	No	No	No	No	No	Urban
TBRPF [9]	TBR	Multihop	No	No	No	No	No	No	Urban
AODV [10]	TBR	Multihop	Yes	No	No	No	No	No	Urban
ZRP [11]	TBR	Multihop	No	No	No	No	No	No	Urban
GPSR [12]	GBR	Greedy	No	No	No	No	No	Yes	Highway
GSR [13]	GBR	Greedy	No	No	No	Yes	Yes	Yes	Urban
GPCR [14]	GBR	Greedy	No	No	No	Yes	Yes	Yes	Urban
GPSRJ+ [15]	GBR	Greedy	No	No	Yes	Yes	No	Yes	Urban
LOUVRE [16]	GBR	Greedy	No	Yes	Yes	Yes	Yes	Yes	Urban
CAR [17]	GBR	Greedy	No	Yes	No	No	Yes	Yes	Urban
VADD [18]	GBR	Greedy	Yes	Yes	Yes	No	Yes	Yes	Urban
D-mincost[19]	GBR	Alternating	Yes	Yes	Yes	No	No	Yes	Both
SADV [20]	GBR	Store&FWD	Yes	Yes	No	No	Yes	Yes	Urban
CBR [21]	CBR	Multihop	Yes	No	No	No	Yes	Yes	Urban
CBDRP [22]	CBR	Multihop	Yes	No	No	No	Yes	Yes	Urban
LORA-CBF [23]	CBR	Greedy	Yes	No	No	No	Yes	Yes	Urban
BROADCOMM [24]	BBR	Multihop	Yes	No	No	No	No	No	Highway
UMB [25]	BBR	Broadcast	Yes	No	No	No	No	Yes	Highway
UV-CAST [26]	BBR	Broadcast	Yes	No	No	No	Yes	Yes	Urban
SmartBC [27]	BBR	Broadcast	Yes	Yes	No	No	Yes	Yes	Highway

Table 2.3: Routing Protocols in VANETs

[2] Short wireless link where packets are forwarded; not the shortest road for the vehicles.

2.3 LTE in CV Environment

Although many novel techniques have been proposed to address their inherent technical challenges, VANETs still suffer from problems including broadcast storm, unbounded delay, and lack of deterministic quality of service (QoS). Those challenges stem from the absence of a central system. Establishing ad hoc networks with more than two hops is very challenging. One obvious candidate for vehicular networking is the 4G mobile communication standard LTE, created by the 3rd Generation Partnership Project (3GPP), a collaboration of seven telecommunications standard- development organizations. LTE is designed to handle large amounts of data traffic via a packet-switched network as well as mobility and other aspects. As explained in [28], LTE has the following aspects:

- 72 Mbps per downlink base station
- Mobility up to 120 km/h without major throughput degradation (maximum 350 km/h)
- Communication range up to 5 km
- Latency less than 100 msec

These aspects satisfy all the key requirements for reliable vehicular communications. Research communities have investigated the plausibility of LTE for vehicular networks [29, 30, 31], comparing IEEE 802.11p and LTE in vehicular scenarios by measuring end-to-end delay, overhead, and packet error rate. Among other studies, [32] mentioned RSUs in VANETs can be replaced with LTE base stations. [30] revealed the superiority of LTE with respect to the delay. [33] and [34] pointed out that LTE supports V2V links based on the device-to-device (D2D) communication protocol. Table 2.4 compares these technologies.

Protocol	802.11a	802.11p	UMTS	LTE	mmWave
Channel Bandwidth (MHz)	20	10	5	5,10,20	100-1000
Frequency (GHz)	2.4,5.2-5.8	5.85-5.925	<3.5	<3.5	¿15
Data Rate (Mbps)	6-54	3-27	up to 2	up to 72/site	¿1 Gbps
Max transmission	60 m	150 m	5km	3km	150-200m
Coverage	Intermittent	Intermittent	Ubiquitous	Ubiquitous	Ubiquitous
Mobility Support	Low	Medium	High	High	Probably low
V2I	Yes	Yes	Yes	Yes	TBD
V2V	Yes	Yes	No	Yes(D2D)	TBD
Market Penetration	High	Low	High (decreasing)	High	None (2022)

Table 2.4: Comparison of Technologies for CV

2.3.1 LTE

Structure

The LTE standard supports both frequency division duplex, which encodes information-bearing samples across frequency, and time division duplex, which encodes information-bearing samples across time. LTE uses OFDM transmissions for downlink in what is known as OFDM access and its close relative single-carrier frequency division multiple access (SC-FDMA), is used for transmission for the uplink.

Downlink

The key downlink transmission technology for LTE is OFDM access. OFDM overcomes the interference caused by multipath fading. In addition to canceling the ISI, LTE base stations divide the frequency and time resource and then use them to bear multiple users information. This is called scheduling. The QoS can be met by scheduling. Channel side information is required at the base stations to perform scheduling. LTE adapts multiple-input-multiple-output (MIMO) transmission and hybrid auto repeat requests [28].

Uplink

For uplink transmission, a single carrier is used. It is similar to OFDM except that SC-FDMA uses only one subcarrier to transmit information. It uses less bandwidth and energy. It is very useful to mobile devices given their limited battery power.

Upper Layer and Mobility

In the LTE upper layer, the QoS Class Identifier (QCI) is defined in [35] to meet the desired QoS.

2.3.2 Applicability of LTE in Vehicular Networks

Guaranteed Quality of Service

In vehicular networks, various applications require different QoS and it is extremely important to satisfy the QoS. Although 802.11p defines the OCB communication to support QoS, it is impossible to introduce the detailed and guaranteed QoS that LTE can provide because LTE processes each packet through the QCI technique. The enhanced supports of QoS provided by LTE are extremely valuable to the delivery of safety messages in congested urban areas [36].

Robust to Interference

Since VANETs are basically uncoordinated and distributed networks, it is more prone to interference than conventional cellular networks where transmissions are coordinated and orchestrated. For example, when a number of safety messages are broadcast through OCB in a small area, interference in the area increases rapidly, retransmissions of the error packets multiply the interference, and finally the area is saturated with interference. The current VANET standards, including 802.11p, cannot alleviate this escalating interference phenomenon because of the ad hoc structure. In contrast, LTE definitely handles the interference through MIMO transmission and user scheduling [37, 29].

Geocast and Unicast

LTE employs multiple broadcast and multicast service [38]. This technology supports multicast/broadcast by delivering the same content to a set of users. This technique is useful in vehicular environments where vehicles want to disseminate messages in a given area, such as foward collision warning. Geocast, which delivers the same messages via multiple BSs (base stations) or a single BS, reduces the number of channels used significantly, and then effectively suppresses unnecessary interference [39]. The unicast addresses each vehicle individually, and consequently the channel is used as much as the number of relevant vehicles. On the other hand, geocast addresses the multiple vehicles simultaneously and this reduces the number of channel used and alleviates the interference too.

Device-to-Device

In LTE-Advanced, Proximity Service (ProSe) [40] was proposed. The service was intended to support social networking, local advertising, or public safety applications. In a vehicular network, ProSe would be enabled to support V2V one-hop safety communication. D2D communication is a viable tool especially if BSs are not available.

Market Penetration

Since LTE networks are deployed by private companies with maximum coverage, they show high penetration rates with near-optimal deployment configurations. As a result, LTE base stations naturally take the role of infrastructure in CV applications.

2.4 Comparison of Performance

This section focuses on showing various simulation results under DSRC protocol and comparing them to the LTE requirements. We use the network parameters given in Table 2.5. The parameters are obtained from [30].

Routing protocol for multihop messages	**AODV** or OLSR
Number of nodes in the network	50, **100**, 150, or 200 nodes
Number of data sinks for multihop messages	**10**, 20, or 30 nodes
Transmit power of basic safety messages	10, **20**, or 28 dBm (10, 100, 1000 mWatts)
The model for wave propagation loss	**Two ray** or Nakagami (m=1)
The speeds of vehicles on the network	**22**, 33, 44, or 55 mph
The size of safety messages	100, 125, 150, 175, or **200** bytes
The frequency of BMS broadcasting	**0.1**, 0.2, 0.3, or 0.4 sec
Simulation window	300 m $\times$1500 m

Table 2.5: Simulation Parameters (bold indicates default value).

2.4.1 Performance Metrics

Using the parameters described in Table 2.5, we describe network performance with respect to network performance metrics. Packet delivery ratio (PDR) is represented as the following equation.

$$\text{PDR} = \frac{\text{Packets successfully received}}{\text{Total packets transmitted}} \tag{2.1}$$

where the packet indicate the smallest unit for communication. PDR addresses the ratio of successful transmissions by dividing the received packets by total transmitted packets. When packets experience deep fading or the receivers are in the interference limited environment, the transmitted packets are lost and not received by the receiver. Those packets are counted as transmitted but not received. In this study, we use PDR as a metric to capture the reliability of WAVE packet transmission in VANETs.

Another important metric is the transmission range. It can be computed easily by link budget analysis that calculates the received signal power using

$$P_{\text{received}} = \frac{P_{\text{transmit}} G(\lambda/4\pi)^2}{d^{\alpha}} \tag{2.2}$$

where G denotes the antenna gains, λ indicates wavelength, d represents the communication distance, and α indicates the path loss exponent. In a rural area, α is between 2 and 3. In a dense urban area, the path loss exponent becomes 4. We obtained the maximum communication distance d by assuming practical antenna gains and $\alpha = 3$.

2.4.2 Simulation Study

Computer-based system-level simulators mimic elements of wireless communication networks, including physical and medium control elements such as mobility of transmitters and receivers, multi-path fading, path loss, propagation of packets, channel access, and routing control. By creating wireless networks with those elements, we can identify the statistical characteristics of the wireless networks. To obtain insights from the simulation results, we use key parameters, such as the number of vehicles in the network. We use the NS-3 software which tracks the transmission and reception of basic safety packets and multihop application packets from vehicles simultaneously. It is important to acknowledge that the system-level simulator does not reveal all the interactions among network parameters. Throughout the simulation studies, we aim to answer the following question:

Can DSRC deliver critical safety information in time reliably over the necessary range, especially when the wireless network is congested?

Table 2.6 summarizes the simulation results obtained from NS-3 and system-level requirement for LTE communications. We assume 10 vehicles per cell which then gives almost the same ranges for DSRC and LTE.

	DSRC	LTE
Packet delivery ratio	0.82 (100 nodes at distance of 50 m)	≥ 0.95 [30]
Max transmission range	130 m	3500 m
Throughput	760 kbps/vehicle	72 Mbps/cell, 7.2Mbps/vehicle
average end-to-end delay	230 msec	50 msec [37]

Table 2.6: NS-3 Simulation Results and LTE Requirements

We learned the following

1. At a distance of 50 meters, the PDR of DSRC is approximately 0.8, which is low for reliable safety applications.
2. Assuming 5 base stations and all 100 vehices are scheduled to serve, throughputs per vehicle are 7.2 Mbps for LTE, which is almost 10 times greater than that of DSRC.
3. The average end-to-end delay of DSRC is 230 msec. The maximum allowed latency for LTE is 50 msec [37]. LTE enables communication that is almost four times faster than the DSRC can perform.
4. LTE offers a vastly superior range to DSRC.
5. DSRCs maximum range can be expected to be at least 100 meters, and at most about 600 meters, depending on the physical environment.
6. Safety messages can be delivered to a distance less than 150 meters by one-hop communications. For longer distances, multi-hop communications will be needed.

2.5 Comparison of Deployment Cost

This section provides a preliminary and itemized estimate of the cost of establishing DSRC infrastructure in Texas.

2.5.1 DSRC Cost Estimate

The cost estimates are speculative.

- RSU equipment: this includes the cost of RSU, power connection, communication connection, and additional traffic sensors. The cost is derived from recent DSRC deployment data [41]. Specifically, a DSRC RSU costs $3,000, RSU incidentals cost $1,030, communication and power connections cost $1,450, and additional equipment costs $2,000.

- RSU installation: this includes the cost of installation labor, ($2,475) and inspection construction ($1,075).

- Network planning: this includes the cost of identifying radio interference, optimizing RSU sites, developing local maps, and controlling local traffic during construction. Radio surveying was estimated at $1,000; obtaining local map and site planning cost $1,550; and design, traffic control, and system integration at $4,100.

- Backhaul connection: note that the cost of backhaul connection varies greatly depending on the capacity and location, desired applications, and the state of existing backhaul infrastructure in the vicinity. In many cases, backhaul for traffic lights is already installed. Roughly speaking, if the traffic light backhaul provides enough capacity (typically less than 10% of existing backhaul capacity is used), upgrading the backhaul cost will run about $3,000. However, the cost increases to $40,000 if new backhaul for CV applications is required, as may be the case if more than 40% of the existing backhaul capacity is already in use. Thus, depending on the level of utilization of existing backhaul, the backhaul cost would range from $3,000 to $40,000. Leasing existing backhaul is an option, but would increasing the operating expenses due to the leasing fee.

- Operation: this cost includes electricity fees and maintenance, plus future replacement cost. Electric fee is calculated at $100 based on the US average and annual maintenance cost is assumed to be 5% of RSU equipment cost and RSU installation cost. The replacement cost of $738 is calculated based on the assumption that a RSU will be replaced every ten years.

- Rental fee: We assume that the site rental fee is $200, but this is in fact a very important variable and could in many cases add significantly to the operating costs. For example, site rental for a single LTE base station can run above $2000/month, although in some cases this includes other operating costs such as electricity and backhaul. We assumed a minimal value here due to the nature of these networks, which in many cases will allow public resources (land, lampposts, etc.) to be leveraged.

These items are summarized in Table 2.7. Assuming that the actual deployment cost follows the model in Table 2.7, we estimate the cost to provide comprehensive coverage. We also assume that DSRC subscribers are half of total Texas car owners. These costs provide a benchmark showing the minimum cost that TxDOT would spend. Note that connection to the core network is critical to enable CV applications such as traffic efficiency and infotainment. We did not calculate the cost of adding DSRC to the vehicle itself. Table 2.8 shows cost estimate with respect to the coverage scale.

Capital expenditure	RSU equipment cost	\$7,480
Capital expenditure	RSU installation cost/site	\$3,597
Capital expenditure	Network planning cost/site	\$6,650
Capital expenditure	Backhaul cost/site	\$5,000
Operating	Power consumption/year	\$100
Operating	Rental fee/year	\$200
Operating	Maintenance cost/year	\$332
Operating	Replacement cost/year	\$738

Table 2.7: Assumptions on Deployment Costs

Coverage	Miles	No. of RSUs	Yearly cost	Monthly cost (vehicle owner)
All of Texas	313,228	1.5 M	\$5.7 B	\$95.10
Local roads	211,378	1.0 M	\$3.8 B	\$64.18
Major minor collectors	65,154	325 T	\$1.2B	\$19.78
Principal highways and minor arterials	33 T	166,400	\$610 M	\$10.10
Interstates only	3 T	17,075	\$62 M	\$1.04

Table 2.8: Cost Estimates with Respect to Coverage Scales

2.5.2 LTE Deployment Cost

We do not include the deployment cost for LTE infrastructure because the LTE network already covers the entire nation. Here, we assume that vehicle owners would pay a monthly fee and compare it to the monthly subscription fee that mobile users pay for LTE. Table 2.9 describes current cellular data plans, which are for smartphone-type subscriptions. Currently mobile users pay an average of \$10 for 1 GB of LTE data per month. However, with increasing applications for "Internet of Things" connections, we expect more flexible and competitive pricing plans to become available in the next 2 to 3 years for a variety of vehicular applications [42]. For example, some vehicle manufacturers including Audi and

Service provider and data	Monthly rate	Modem price
T-mobile unlimited data	$95	Free (2 year contract)
Sprint unlimited data	$75	Free (2 year contract)
AT&T 5GB data	$50	Free (2 year contract)
Verizon 6GB data	$50	$49 (2 year contract)
Sprint 6GB data	$50	Free (2 year contract)
AT&T Infotainment for Vehicle	$10	Free (For Audi and Porsche)
AT&T Internet of Thing 5GB	$8	$99

Table 2.9: LTE Data Plans (as of November, 2016)

Porsche made an agreement with network operators to enable CV applications (5G device hot spot, news and weather alerts, and some infotainment applications).

2.6 Implementation Considerations

While DSRC has its technological limitations as is well documented in this report and elsewhere, we believe that DSRC is still the leading candidate technology for implementing V2V. Here are some reasons:

- **Public Agency's Perspective**: The DSRC spectrum is not commercially licensed, and this enables the DOTs to transmit data in the designated spectrum without obligations to engage commercial entities. This is a major advantage of DSRC over competing technologies such as LTE and 5G, as it greatly simplifies the administration of communication infrastructure from the perspective of public agencies. To our best knowledge, while Public-Private Partnership (PPP) holds great potentials, a mature PPP model for management and operations of CV infrastructures is still missing.

- **Automaker's Perspective**: The outdated physical layer technology used in DSRC is often cited as a shortcoming of DSRC. Nonetheless, the automotive industry might actually favor such a technology. The cellular standards evolve very rapidly and it would not be trivial for the automakers to keep up with these changes. This is especially true since safety is a primary considerations to car manufacturers and every part of a vehicle must be tested extensively before deployment. The maturity of DSRC should make it more favored from automaker's perspective.

- **User's Perspective**: DSRC-equipped vehicles are self-contained in that they do not rely on infrastructure to operate and do not incur any user fee. LTE, in contrast, requires a monthly subscription. These factors make DSRC more favored from an average user's perspective. In addition, it should be recognized that the LTE coverage is still not ubiquitous even there has been many years since its introduction.

While DSRC seems to have almost no technological advantage over other V2V options, it does make a good case from the perspective of policymakers, car manufactures and average users. Out of these considerations, we believe that DSRC will be operational at least over the next 10-15 years. This makes the discussion about DSRC security relevant and justifies our choice of case study.

Chapter 3

Security Challenges

This chapter discusses the security challenges associated with communication of safety critical messages between connected vehicles, such as the BSM. Safe operation of CVs relies on the validity and authenticity of the information exchanged among the vehicles. The designers of some of the earlier communication protocols in transportation, such as Automatic Dependent Surveillance-Broadcast (ADS-B) in the aviation industry, did not consider the critical security issues in protocol design and thus some research efforts have questioned the utility of ADS-B in safety-of-life applications [43, 44, 45]. The designers of DSRC have paid considerable attention to making communication between vehicles as secure as possible while maintaining efficient wireless network use and protecting the privacy of the users. Even so, recent research has shown that the security measures in existing standards are deficient and must be augmented for safe operation of CVs [46, 47, 48, 49, 50]. In this chapter, the major security concerns addressed in this project are summarized, and some guidelines and recommendations are presented.

While CV technology presents a multitude of advantages, it also faces the possibility of attacks and misuse that can jeopardize the safety and integrity of coordinating and connected vehicles [46, 47, 48]. This is especially true as CVs become more automated, bypassing traditional human oversight. For example, a malicious attacker could suddenly transmit data falsely purporting to come from a vehicle in the immediate vicinity of one or more unsuspecting vehicles, forcing them into evasive action and potentially endangering the safety of passengers in the victim vehicles. The possibility of such attacks necessitates implementation of strong security measures as a prerequisite to widespread adoption of CVs.

At this point it must be noted that the scope of this report is to analyze the security of connected vehicles independent of other upcoming vehicular sensors such as radar, optical camera, IMU, LiDAR etc. While it is clear that a fusion of these sensors helps to secure the overall system, the following arguments justify an independent DSRC-centric security analysis for connected vehicles:

- Following the notice of proposed rulemaking (NPRM) issued in December 2016, V2V technology is on the verge of being mandated in the US. Despite its major shortcomings, as described earlier in this report, DSRC is currently the leading candidate technology to be implemented for V2V. In fact, at times the NPRM used DSRC interchangeably with V2V. As a result, it is important for TxDOT to understand the security concerns in the DSRC protocol.

- It is highly unlikely that the majority of vehicles will be equipped with advanced sensors *for localization* by the time V2V is mandated in the US. This implies that at least over the next 15 years, GNSS-based location and velocity will be used by V2V systems. It is even more unlikely that automated driving will be commonplace prior to the V2V mandate. Hence, the security vulnerabilities of DSRC (and V2V, in general) and GNSS-based localization must be discussed independently of automated driving technology and related sensors. The discussion in this report does not imply that emerging vehicular sensors are not useful in making DSRC and GNSS secure in some capacity, but that an independent study of DSRC and GNSS vulnerabilities is justified.

- Even with availability of other vehicular sensors, the V2V system has the unique feature of being able to sense vehicles and pedestrians beyond the line-of-sight. As a result, even with an advanced sensor suite, the V2V system will be standalone in beyond line-of-sight sensing. Consequently, some of the analysis presented in this report will apply even after significant penetration of advanced vehicular sensors.

- Finally, even though it is attractive to look at the security from a system perspective, the best practice is to analyze the security of each sensor at a lower level. It is more tractable to establish theoretical performance and security guarantees at the sensor level prior to fusion, than at the system level. Theoretical and formal methods are especially useful in transportation where the required failure rates, on the order of 10^{-6}, require driving billions of miles for empirical testing and verification.

The rest of this chapter on security issues is organized as follows: All possible attacks against CV network are outlined in Section 3.1. Section 3.2 provides a brief review of the current DSRC standards and the security measures built-in to the standard that solve some of the attacks mentioned in Section 3.1. Section 3.3 provides a brief overview of the current state of research literature on defending against attacks that are not covered by the DSRC standards. This section also outlines the major open challenges that exist in securing connected vehicles. Security recommendations related to deployment of connected vehicle technology in Texas are presented in Section 5.2.

3.1 Attacks against Connected Vehicles

Following are some of the vulnerabilities of CVs:

- *Location Spoofing and Jamming*: CVs must know their own location with a standard deviation of about 10 cm (see Section A for the derivation) in order to participate safely in a CV network. However, secure self-localization is not guaranteed due to the jamming and spoofing threat against localization systems. Global navigation satellite system (GNSS) is the most widely used positioning system in ground transportation. Multiple incidents of GNSS jamming have been reported regularly both in the US and worldwide. GNSS jamming can be achieved using inexpensive off-the-shelf equipment. Furthermore, spoofing civil GPS receivers has been demonstrated. GNSS spoofing is a bigger concern than jamming because of its ability to feed false position information. Jamming, on the other hand, is only a denial-of-service attack. A recent incident of GPS spoofing was reported and verified near the Kremlin in Russia [51].

- *Malicious Self-Spoofing*: The GNSS spoofing and jamming attacks described above are directed by an adversary towards victim vehicles. It is also possible that an attacker could modify its own sensor data in order to use DSRC equipment to report incorrect information. This attack is simpler to execute than spoofing or jamming. The attacker can modify the data as it goes from sensors to the processing unit. For example, in the case of a GNSS sensor, the attacker can replace the NMEA (National Marine Electronics Association) messages output by the GNSS receiver with fake NMEA location messages. The DSRC transmitter would take this falsified data, package it into the BSM and share it with other neighboring vehicles, thereby jeopardizing the safety of the CV network. Notice that in this attack, the attacker has valid credentials required for participation in the CV network, but chooses to broadcast malicious false information to disrupt safe CV operation. We call this class of attacks an *internal attack*. These attacks are especially difficult to guard against because they do not violate any authentication or encryption security measures.

- *Fake Messages and Message Tampering*: If effective authentication measures are not put in place, then an *external attacker* (a vehicle that is not a legitimate member of the CV network - that is, does not have a valid certificate or authentication keys) can generate and transmit false information to neighboring vehicles. Similarly, without proper encryption techniques, an external attacker can selectively tamper with the information being exchanged between two victim vehicles.

- *Man-in-the-Middle (MITM) Attacks*: A MITM attacker can record DSRC messages from a passing vehicle, and then replay these messages at a later time to other vehicles. The information shared by CVs becomes invalid very quickly because of high velocities involved in CV networks. As such, it is dangerous to make decisions based on information that was transmitted even one second ago.

- *Attacks against Privacy*: Another important concern in CV technology is to preserve the privacy of the owners and occupants of these vehicles. The possibility of revealing the owner's identity and movements to third parties is undesirable from a privacy perspective. Thus, tracking the movements of a CV using its messages, and linking this information to the vehicle's owner is another attack that must be considered in the CV paradigm. Nonetheless, preserving user privacy must not be prioritized over the safety and security of CVs.

- *Masquerading Attack*: In a CV network, different types of nodes have different privileges. For example, an emergency vehicle must be able to request a clear path by sending alert messages to other vehicles. However, such selective privileges can lead to attacks wherein an attacker pretends to be an emergency vehicle and requests a clear path. An attacker may use such a trick to reduce its own travel time.

The first two attacks (GNSS spoofing and self-sensor spoofing) mentioned above cannot be prevented using data security techniques since they involve attackers that have the required authentication keys. These attacks must be considered at the PHY layer. The other four attacks can be prevented by judicious use of authentication, encryption, time-stamping, and pseudonyms. These techniques have been implemented in the DSRC security standard and are described briefly in the next section.

3.2 DSRC Standards and Security Measures

The two most important aspects of the DSRC standards from a security standpoint are the IEEE 1609.2 standard used for message security and the IEEE 802.11p standard used at the PHY layer. Thus, IEEE 1609.2 protects message integrity, whereas IEEE 802.11p can help to prevent the attacks that cannot be detected at higher network layers.

Designers of DSRC recognized the threat of attacks against CV technology, as well as the need for privacy of vehicle owners. IEEE 1609.2 defines authentication and encryption mechanisms for security-critical messages exchanged between vehicles. It aims to protect messages from attacks such as eavesdropping, alteration, and replay. Also, it attempts to maintain privacy of CVs as much as possible without compromising security, and does not reveal personal data or linkable information to third parties. The major objectives of the IEEE 1609.2 standard are summarized in Figure 3.1.

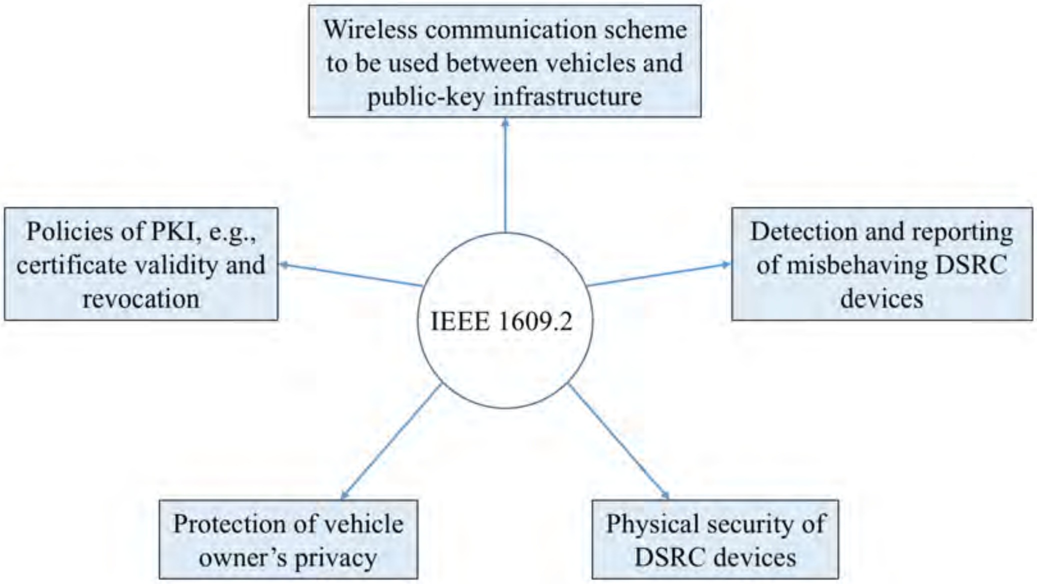

Wireless communication scheme to be used between vehicles and public-key infrastructure
Policies of PKI, e.g., certificate validity and revocation
IEEE 1609.2
Detection and reporting of misbehaving DSRC devices
Protection of vehicle owner's privacy
Physical security of DSRC devices

Figure 3.1: CV Security Infrastructure Managed by IEEE 1609.2 Standard

IEEE 1609.2 Certificates, Authentication, and Encryption IEEE 1609.2 uses Public Key Infrastructure (PKI) for authentication of messages. This authentication enables verification that received data originated from a legitimate node within the CV network, and that the transmitting node had the privilege to send such a message. PKI consists of a hierarchy of Certificate Authorities (CA) that grant valid authentication keys to vehicles [49, 50]. Each vehicle has two types of credentials: a Long-Term Certificate (LTC) that is issued once for each vehicle and acts as a long-term identity, and a set of *pseudonyms* that are short-lived public-private key pairs that have pre-determined temporal validity. Changing pseudonyms frequently prevents straightforward long-term tracking of CVs. Each pseudonym is typically valid for only 5 to 10 minutes. In current standards, the pseudonym acquisition event is infrequent (about once a year), and a large number of pseudonyms (about 100,000) are loaded simultaneously [50, 52, 53]. Multiple pseudonyms are never valid at the same time in order to prevent attacks where one vehicle acts as multiple valid entities (Sybil attacks).

DSRC uses the Elliptic Curve Digital Signature Algorithm (ECDSA) to authenticate the messages with the vehicle's private key, and the Advanced Encryption Standard in Counter with Cipher Block Chaining Message Authentication Code mode (AES-CCM) or Elliptic Curve Integrated Encryption Scheme (ECIES) to encrypt the transmitted data. Although authentication using ECDSA and encryption using AES-CCM or ECIES does not provide information-theoretic security [54], they are sufficient for defense against a reasonably powerful adversary attempting to generate fake DSRC messages or to tamper with messages being exchanged between victim vehicles.

MITM attacks are mitigated in the IEEE 1609.2 standard by using generation time-stamps and embedding them into the messages being transmitted. If a MITM attacker replays an old DSRC message, the receiver rejects that message if the generation time is outdated. Note that since the embedded generation time-stamp is encrypted, the MITM cannot modify this time-stamp. It must be pointed out that while a message with a large delay (more than a second) can be rejected based on message generation timestamp, it would not be possible to reject a message that has been delayed by only a few microseconds. At first it may appear that such a small delay would not be troublesome for the CV network. However, in Section 3.4.2 we show that even such small delay attacks can disrupt certain operations of CVs.

In summary, a compliant implementation of IEEE 1609.2 prevents all attacks that can be detected at the higher network layers. Examples of the attacks that DSRC authentication and encryption mitigate include the following:

- Vehicle tracking by external nodes (wardriving attack).
- Sniffing of unicast messages exchanged between nodes (eavesdropping).
- Alteration of messages exchanged between nodes.
- Generation of valid messages by external attackers (frame injection).

However, these authentication measures do not provide any means to defend against internal attacks. They also fail when an attacker spoofs the positioning sensors of a CV. Section 3.3 reviews the state-of-the-art research on these security topics.

DSRC Credential Management Certificate and credential management is an important part of a PKI [49, 50]. The CA must recognize and keep track of misbehaving nodes, make legitimate nodes aware of revoked certificates, and have laws for protecting the CV network against wrongdoers. At present, the DSRC guidelines regarding revocation of misbehaving nodes are under development. The leading candidate for implementation in the US is the Secure Credential Management System (SCMS) described in [55]. This system for credential management is an improvement over the European system [52]. The shortcomings of the European credential management system are outlined in Section 3.4.3 so that the same mistakes are avoided in the US implementation.

3.3 Literature Review of Security Techniques in CVs

As discussed in the previous section, internal attacks and sensor spoofing attacks are not prevented by the security measures implemented in the DSRC standards. This section presents some of the research efforts that have attempted to solve these issues.

While it is clear that internal attacks and GNSS spoofing in connected vehicles would lead to exchange of unreliable position and velocity information between vehicles, it is also important to know how this unreliable information impacts the safe operation of connected vehicles. However, it is not straightforward to make a general statement about this since the potential impact depends on how the automakers and motorists use the information received from other connected vehicles.

This report claims that, at worst, internal attacks and GNSS spoofing can lead to vehicle crashes. Consider a scenario in which an internal attacker suddenly claims to be approaching a blind intersection at high speed, such that the V2V system in a legitimate vehicle approaching the same intersection advises the driver to brake as hard as possible. Such sudden braking could lead to a rear-end collision or even a multiple-vehicle collision. It is clear that if such attacks are possible, then it is in fact better to not have such technology in the vehicles. At the same time, it must be noted that many studies have shown that connected vehicle technology can make roadways safer so long as authentic information is exchanged between vehicles. Thus, an effort must be made to make connected vehicles secure against attacks, instead of abandoning the idea of connected vehicles or treating the V2V information as unreliable at all times.

It must also be noted that in the above scenario it might not be possible to use other vehicular sensors such as cameras or radar to detect the presence or absence of the vehicle approaching the intersection if the line-of-sight view is blocked by a building, house, or trees. Thus, it is the kind of accident that V2V technology aims to prevent, but at the same time a false alarm of such an event can make the V2V technology counter-productive.

3.3.1 Secure Own-Vehicle Position and Velocity

GNSS is the most common mode of own-vehicle navigation in use today. GNSS jamming and spoofing, and their corresponding defenses, has been an active topic of research for over a decade [56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69]. Following are some of the common GNSS spoofing techniques:

- *Jamming followed by spoofing*: In this attack, the attacker first jams the receiver such that it loses lock on the authentic GNSS signals. Subsequently, the attacker transmits fake GNSS signals with greater power than the authentic signals to take control of the victim receiver [56]. This spoofing method is conspicuous because of the initial jamming phase.

- *Covert spoofing*: In this spoofing attack, the attacker first transmits its spoofing signals such that they are identical to the true signals at the victim's receiver. The attacker slowly increases its transmit power to take control of victim's tracking loops. Once in control, the spoofer drags-off the victim's tracking loops away from the true correlation peak [66].

- *Nulling attack*: A more sophisticated spoofer might transmit two signals for each satellite. One signal attempts to drag-off victim's tracking loops, while the other attempts to cause phase-reversed destructive interference with true signals at the victim's antenna to make the true signals unavailable [67]. Nulling attack is difficult to carry out, but has been shown to be possible in a laboratory setting.

Spoofing defense techniques have also been proposed in the literature in response to the exposed vulnerabilities of GNSS receivers [56, 69, 57, 58, 59, 60, 61, 62, 65, 68]. A combination of these techniques must be used in CVs to prevent spoofing of own-vehicle positioning. Some of the most effective spoofing defense techniques are the following:

- *Received Power Monitoring*: Received power monitoring (RPM) keeps track of the total power received at the RF (radio frequency) input [62]. This is one of the simplest spoofing defense that is effective at preventing the spoofer from using very high transmit power in order to drown the authentic signals or capture the victim's tracking loops. However, if the increase in spoofer power is not sudden then it can be hard to detect.

- *Correlation Distortion Monitoring*: Before the spoofer completes correlation peak drag-off, the complex correlation function at the victim's receiver is distorted because of interaction of true and spoofed signals [68]. This can be detected using a large number of signal processing correlators. However, this distortion is more or less identical to the distortion caused by GNSS multipath signals. Also, this defense does not work once the drag-off is complete.

- *Redundant Tracking Channels*: The defending receiver can employ redundant tracking channels to detect if it is receiving multiple signals corresponding to the same satellite [56]. This defense works even if the drag-off is complete. However, this defense breaks down under a nulling attack.
- *Two-Antenna Defense*: This defense exploits the fact that true signals arrive from a variety of directions but the spoofed signals arrive collectively from the same direction. This technique assumes that the spoofer transmits from one direction, which is a practically reasonable ratinale. The defending receiver uses beat carrier-phase measurements from the two antennas to monitor the direction of arrival of signals [69].

The various defenses presented above have complementary failure modes, and thus a combination of two or more defenses is generally recommended. Note that all these methods only help in detection of spoofing, and thus make the system unavailable if they detect a spoofing attack. No attempt is made to recover the authentic signals to generate a valid navigation solution. Once own-vehicle navigation is made secure using the above methods, the vehicles seek to verify the claims made by their neighbors.

3.3.2 Neighbor Position Verification (NPV)

As discussed before, a CV could receive an invalid position and/or velocity claim if a hitherto legitimate internal node goes rogue and claims a false position. The problem of NPV has been studied extensively in the literature [70, 46, 48, 47, 71, 72, 73, 74]. Neighbor velocity verification can be performed with multiple rounds of position verification per second. The current DSRC standards recommend that the BSM containing position, velocity, and other safety-related information be transmitted once every 100 milliseconds.

First, it must be mentioned that NPV has been proven to be impossible under an attack model that permits colluding attackers with directional antennas [71]. Nonetheless, several NPV protocols have been proposed under a more relaxed attack model. Fiore et al. propose a robust and fully distributed cooperative NPV protocol in [70] that can be implemented easily using custom hardware. This protocol is shown to be secure against both independent and colluding adversaries as long as the legitimate verifiers are not outnumbered by colluding adversaries. Their attack model assumes that the adversaries do not use directional antennas, but allows the adversaries to collude. In a scenario with multiple coordinating legitimate nodes, the verifier V uses time-of-flight (ToF) measurement techniques to compute the range between each pair of neighboring nodes. It then runs a series of tests to categorize each neighbor as one of the following:

- *Accepted*, i.e., V deems the neighbor to be at the claimed position.
- *Rejected*, i.e., V deems the neighbor to have announced an incorrect position;
- *Unverifiable*, i.e., V cannot prove location claim to be either correct or faulty, due to insufficient information.

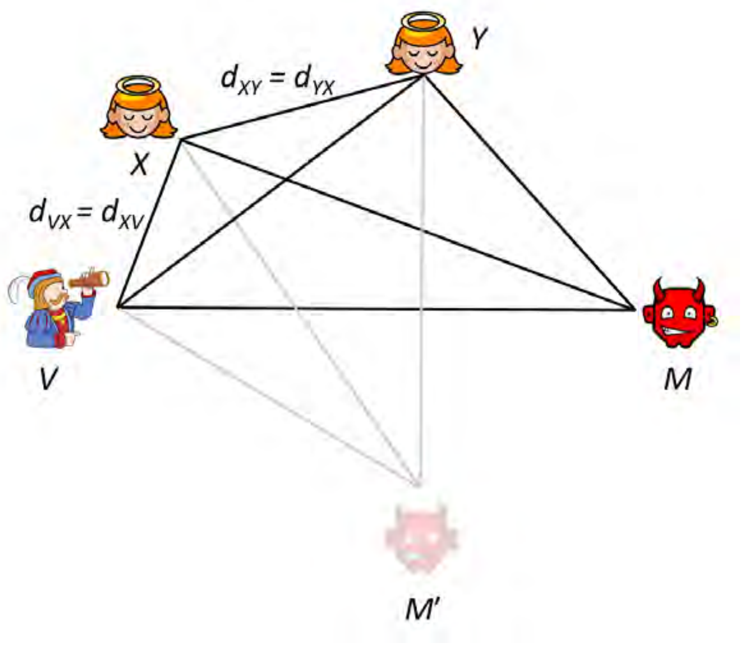


Figure 3.2: Example of Effect of a Fake Position Announcement by M

Figure 3.2 shows an example scenario of a typical NPV problem. M is an attacker announcing a false location M' to cause some damage to the vehicles in the CV network. The false location claim alters the distance between pairs of nodes in the neighborhood. This is clear from the different lengths of black and grey links between M and the surrounding nodes. The verification tests look for discrepancies in the node distance information to identify false location claims. Only the nodes that pass all of the above tests are categorized as *Accepted*. This protocol incorrectly categorizes an adversary as *Accepted* only if there are at least as many colluding adversaries as the number of legitimate nodes in the neighborhood. However, if a verifier has fewer than three neighbors at any time this protocol categorizes every neighbor as *Unverifiable*.

3.4 Open Problems

Despite the security measures implemented in the DSRC standards and the ongoing research outlined above, multiple security issues are still open and need to be addressed before mass market adoption of connected vehicles.

3.4.1 Limited Defense against Internal Attacks

Although Fiore *et al.* [70] make a good attempt at defending against internal adversaries, there are some important scenarios in which this protocol would fail. Consequently, dealing with internal attacks is still largely an open problem. As mentioned in [70], the protocol is unable to verify location claims if there are fewer than three neighbors. This is troublesome because it is common to have fewer than three vehicles in 1-hop communication range when traveling on a rural road.

To make this security threat more concrete, consider the following one-verifier-one-attacker scenario. Upon receiving a claim, the verifier wishes to verify the claimed location. Note that such verification is not possible using ToF techniques proposed in the literature. At best, the verifier can obtain a lower bound on the claimed range using distance-bounding techniques. Hence, the verifier must consider the claimant as *Unverifiable* even if the claimant was honest in reality. This implies that if better verification methods are not developed then CV technology will be ineffective on rural roads when less than three vehicles are in the neighborhood. On the other hand, passing on rural roads is one of the most important safety requirement that CVs must fulfill. In the worst but rare case, the verifier might incorrectly trust an internal attacker if more than two colluding attackers are present on a rural road.

Hence, despite many efforts in this area, defending internal attacks is still an open research problem that must be solved before deployment of CVs.

3.4.2 MITM Attacks on NPV

It was mentioned earlier that DSRC standards resolve the problem of MITM attacks by embedding transmit time-stamps in DSRC messages. However, as mentioned before, if the delay introduced by the MITM is on the order of a few microseconds then the claim cannot be rejected on the basis of time elapsed.

Recall that under the NPV schemes proposed in the literature, verifiers attempt to verify location claims using ToF of RF signals. If a MITM were to introduce a delay in the exchanged signals, then such verification schemes would fail since the claimed range would not match the ToF of the signal. The verifier would mark the claimant node as *Rejected* even though it is legitimate. Such an action would eventually lead to the claimant's credential revocation. This attack makes the NPV protocol ineffectual and counter-productive.

One of the arguments against such an attack might be that if the verifier receives two consecutive claims from the same claimant, then it can reject the one that arrives later. However, in many scenarios it is possible that the MITM can communicate with both the verifier and the claimant, but they cannot communicate with each other. This would be the case if the claimant and the verifier are separated by buildings and the MITM is positioned at the intersection. Even multipath signals could lead to such failure of proposed NPV techniques.

3.4.3 Inefficient Pseudonym Revocation

In order to protect the privacy of CV owners, the DSRC standard recommends that CVs must acquire short-lived pseudonyms using their LTC in order to prevent straightforward tracking of CVs. However, acquiring these pseudonyms too often would make the wireless communication network inefficient. Thus, it has been recommended in the standard that a large set of pseudonyms be made available to the CVs in a single transaction. These pseudonyms would be valid for many months before a new set must be acquired again using the LTC.

On the other hand, issuing a large number of pseudonyms at once is troublesome when the CA tries to revoke a misbehaving node. For example, in the European system for credential management, the Certificate Revocation List (CRL) must contain a large list of revoked pseudonyms along with the revoked LTC. Also, at the verifier, the receiver must check every received signature against a long list of revoked pseudonyms. In view of this overhead, the European standards recommended that only the LTC be revoked.

It is clear that this poses a security threat since a rogue vehicle could use its acquired set of pseudonyms for multiple months before it is unable to get new pseudonyms due to revocation of LTC. This issue has been addressed in the SCMS system that is the leading candidate for deployment in the US. Nonetheless, these shortcomings are presented here to prevent the mistakes made in the European system.

Chapter 4

Case Study: CV-enabled Variable Speed Limit

In this chapter, we present a case study on traffic management using CV-enabled variable speed advisory. The purpose of this case study is to compare connected-vehicle-enabled variable speed advisory with the existing approach using variable speed display signs or variable matrix signs.

It must be noted that while connected vehicles enable many other applications with possibly greater impact, we chose the case of variable speed advisory in this chapter keeping in mind the following considerations:

- Variable speed advisory enables traffic management on major freeways in Texas such as I-35 and Mopac.
- Autonomous or semi-autonomous vehicles are not a pre-requisite for successful deployment of variable speed advisory.
- Variable speed advisory can be implemented with modest CVs penetration.
- Variable speed advisory is amenable to incremental roll-out by TxDOT.

The analysis in this case study focuses on scenarios circa 2030. It is assumed that all new light vehicles will be mandated to have CV technology beginning 2021 (the exact date of this mandate is uncertain at the time of writing) and median age of passenger cars is 10 years. With these assumptions, it can be computed that the CV penetration would be about 50% by year 2030.

4.1 Background

VSLs are speed limits that change dynamically based on the latest information about traffic, weather, and road conditions. Variable speed advisory offers benefits in traffic flow, increases roadway capacity, and improves safety. VSLs are usually displayed using overhead or roadside variable message signs.

Variable speed advisory smooths traffic flow and prevents start-stop congestion. This reduces the speed variance of traffic and leads to speed harmonization [75, 76], which mitigates capacity drop on freeways. The smoothing effect of variable speed advisory also reduces the risk of an abrupt speed change, which is a cause of secondary crashes. Thus, variable speed advisory can lead to a significant reduction in rear-end collisions in stop-and-go traffic. Even when these collisions occur, their severity is significantly reduced due to speed harmonization. Moreover, it has been shown that judicious implementation of VSLs can reduce travel time [77, 78, 79].

Variable speed limiting has been implemented extensively in Europe, and has been tested successfully in many parts of the United States [80]. Germany has led the way in validating the benefits of variable speed limiting from as early as the 1970s. The German Ministry of Transportation has reported a 20-30% reduction in crashes on freeways with VSLs [75]. As of 2010, Germany had implemented variable speed limits on nearly 1000 miles of its freeways. Similar implementations in the Netherlands has shown that severity of shockwaves in traffic were reduced significantly as a result of VSLs [80]. For the particular case of I-35, [81] reports that speed harmonization and variable speed limiting have the potential to reduce collisions.

It has also been reported that drivers are more likely to follow a variable speed advisory since it is dynamic and reflects the current conditions faced by the vehicle. In contrast, drivers do not tend to trust static speed limits largely because drivers trust their own judgement over a universal speed limit that is applicable in all driving conditions.

We compare two strategies that can be adopted for implementation of variable speed advisory on Texas freeways:

- *Variable Speed Display Signs*: Traditionally, variable speed advisory has been implemented using electronic variable speed display signs or variable message signs. These are sometimes also referred to as variable matrix signs. The system uses detectors and sensors that collect information about traffic density, traffic flow, and possibly road conditions. These inputs are fed to a controller that computes the optimal speed limit under the given conditions. Finally, these speed limits are displayed on the variable speed display signs. Figure 4.1 shows an example of such a speed limit sign.

- *DSRC Beacons*: Here we propose that variable speed limiting can also be achieved using DSRC RSUs. Such a system retains the detectors, sensors, and controller, but replaces the visual speed display sign with a wireless radio device. The objective of this case study is to compare the efficiency and cost of each of these two methods. Here, it must be noted that a similar CV-enabled speed advisory system may also be implemented using LTE. This chapter focuses on DSRC as a special case.

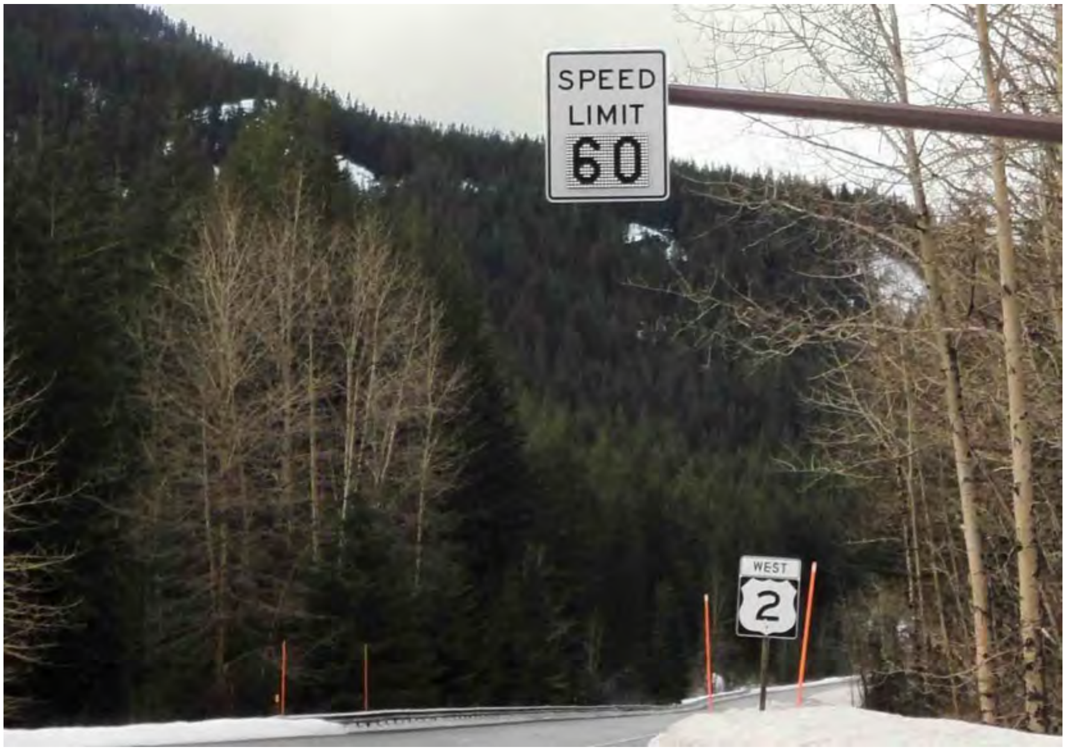


Figure 4.1: An Electronic Variable Speed Display Sign

4.2 Comparison with Existing Approach

This subsection outlines the major contrasts between the two approaches mentioned above. First, the advantages and disadvantages of each approach are summarized. Then, a brief comparison of costs of implementing the two systems is presented. In Section 4.5, we make recommendations on the path that TxDOT should take for the implementation of variable speed advisory systems.

The major contrasts between the two approaches to variable speed advisory are outlined below. These contrasts are arranged in decreasing order of favorability to the traditional approach.

- *CV Penetration*:
  - It is clear that variable speed advisory using variable speed display signs does not need any CV penetration. In case of DSRC beacons, however, the only vehicles that will get information on variable speed advisory will be CVs.
  - The concept of speed harmonization has been shown to work well even if 20% of the vehicles comply with the posted speed advisory [**?**]. Thus, it is not necessary for all vehicles to be connected in order to realize the benefits of variable speed advisory using DSRC beacons. As explained earlier in this chapter, 50% of the vehicles of Texas roads are expected to be connected by 2030. Thus, variable speed advisory can be expected to provide appreciable benefits even if a fraction of connected vehicles comply with the speed advisory. Nonetheless, variable speed advisory using variable signs has the advantage in this case. Another disadvantage of using connected vehicle technology for variable speed advisory is that it can cause confusion among the drivers who do not have access to the variable speed advisory. In particular, if the variable speed advisory is different than the posted static speed limit, then the drivers without access to connected vehicle technology might get impatient with the compliant drivers.
- *Range*:
  - The speed limit signs installed overhead have a maximum viewing distance in the range of 1100 feet (about a quarter mile) [82].
  - As discussed in Chapter 2, both DSRC and LTE are able to achieve such range. Thus, the wireless range of DSRC and visual range of variable speed display signs is comparable.
- *Ease of Installation*:
  - In case of VSL signs, it is critical to install these signs such that they are easily visible to motorists in all lanes. In fact, one of the reasons for limited success of variable speed advisory experiment by Virginia DOT on a 7.5-mile section of I-495 in Virginia between the Springfield Interchange and the Woodrow Wilson

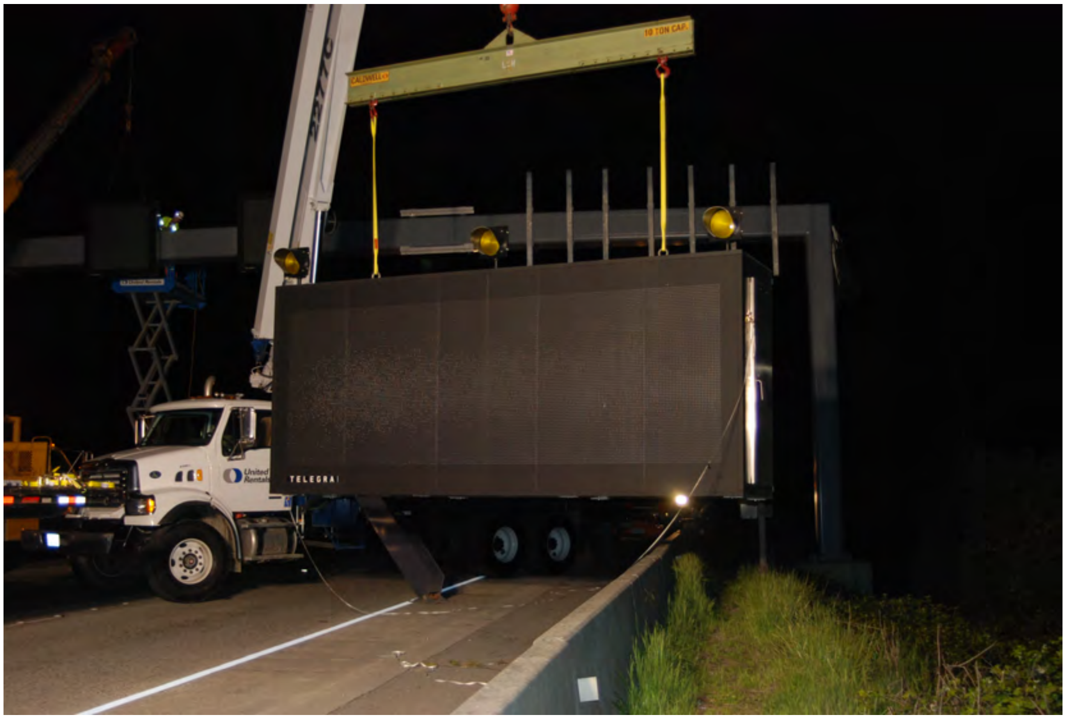


Figure 4.2: Installation of Variable Message Sign Requires Heavy Equipment

Bridge is believed to be improper placement of speed limit signs [?]. For multilane roadways, it would be preferable to install these signs overhead as shown in Figure 4.1 instead of installing them on the roadside. Such installation is expensive and inconvenient, as is evident from Figure 4.2. This is a picture of a variable message sign being installed by Washington State DOT (WSDOT) in 2010 on northbound I-5 in south Seattle, and on I-90 and SR 520 between Seattle and Bellevue.

- By contrast, DSRC beacons do not need to be visible to the motorists, and can be conveniently placed on the roadside. DSRC beacons have an advantage in this category. Another important consideration is that with speed limit signs, it is necessary that the driver sees the sign before he drives past it. With DSRC-based advisory, the optimum speed can be displayed continuously as an embedded *green* zone on the speedometer.

- *Scalability to Multiple Lanes*:
  - In order to advise different speed limits in different lanes, one variable speed display sign must be installed for each lane. This is shown in Figure 4.3.
  - However, with DSRC beacons it is possible to communicate the speed advisory

for all lanes and the on-board DSRC computer can display the advisory that is valid for the lane that the vehicle is occupying. DSRC-based speed advisory is attractive in this case because a single DSRC beacon can perform the function of six VSL signs on a six-lane highway.

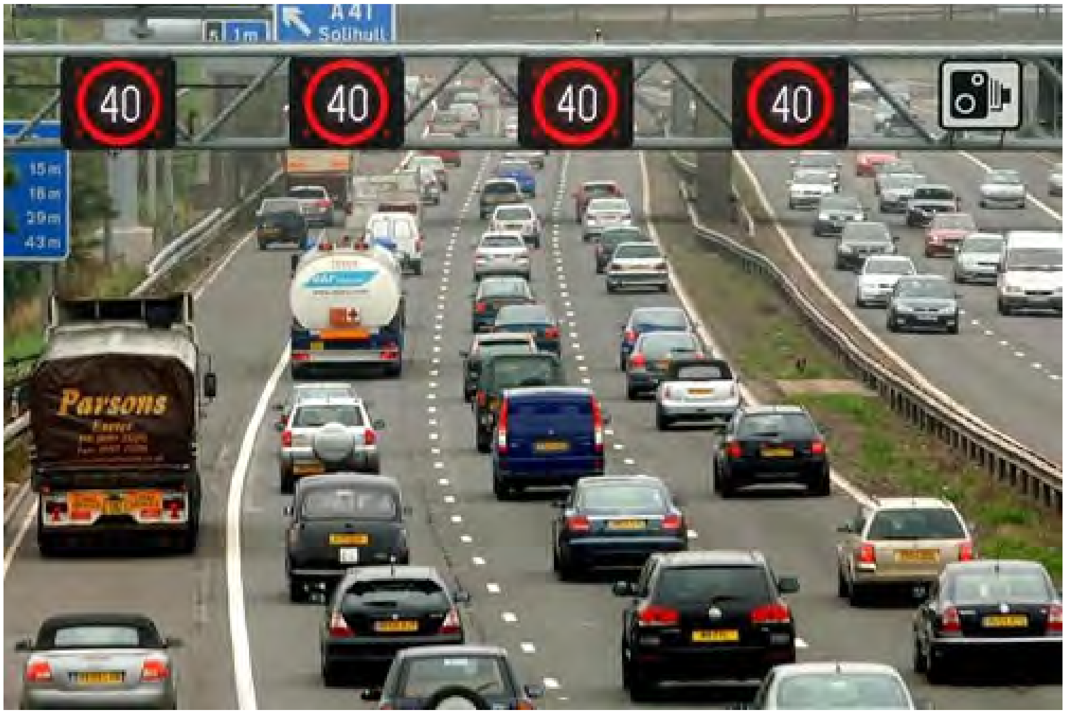


Figure 4.3: Variable Speed Advisory on Multiple Lanes. (The Red Circle Around the Speed Limit Denotes whether the Speed Limit is Advised or Enforced.)

- *Separation between Consecutive Signs*:
  - The separation between consecutive speed advisory displays is different in different implementations. In Germany, a separation to 1.5 to 2 km (1 to 1.25 miles) has been adopted. In the US, WSDOT adopted a separation of half a mile.
  - One of the advantages of using CV based speed advisory is that the on-board computer can easily handle multiple speed instructions. Specifically, the optimal speed controller can generate a speed advisory for many miles ahead. For example, the controller can advise a speed of 45 mph for the next mile, and 50 mph for the subsequent 2 miles. The on-board computer can then display this information to the motorist one at a time. However, this cannot be achieved in case of variable speed displays because humans are less proficient at following

such complex instructions. Thus, the separation between consecutive CV RSUs can be as large as 5 miles.

4.3 Cost Analysis of Variable Speed Display Signs and DSRC Beacons

According to the USDOT-maintained ITS Costs Database, the cost of DSRC RSU equipment is highly variable, primarily because this variability is that the cost of these units is dropping quickly and has not stabilized yet. For example, the Michigan DOT reports that each RSU cost them $3,750, whereas the Arizona DOT estimates this cost to be only $1,000 [41]. The RSU device for DSRC has the same functionality as the DSRC OBU, except for the RSU's requisite weather-proof casing. The OBU costs about $291 according to the USDOT database [83], and so we expect that the cost of DSRC RSUs would also settle near the $500 mark. Nonetheless, in this cost analysis we assume a cost of $1,000 per RSU. The cost of a variable speed display sign such as the one shown in Figure 4.1 is $3,700. This is the most basic display and can only be used for displaying digits between 0 and 99. A better display, such as the ones shown in Figure 4.3, costs at least 10 times more than the basic speed display. This variable *message* display can be used to indicate lane closure or display other text. As a conservative analysis, this section assumes that the cheapest alternative is chosen for traditional implementation of variable speed advisory.

Note that infrastructure, such as inductive loop sensors, power supply connections, and backhaul connections, are common for both approaches to variable speed advisory. Thus, these costs are not included in the cost analysis. Another factor that must be considered in this cost analysis is the power consumption of these devices. The basic speed display in Figure 4.1 typically consumes 145 watts of power, with a maximum consumption of 197 watts [82]. As a contrast, a commercial DSRC beacon with positioning hardware consumes a maximum power of 4 watts [84]. Moreover, inconvenient installation of variable speed displays is expected to be more expensive for TxDOT than installation of DSRC RSU beacons.

As a concrete example, consider a 30-mile stretch of a six-lane freeway on which TxDOT wishes to implement variable speed advisory. Also, assume that a variable speed display sign or DSRC beacon must be installed at every 1 mile. As discussed before, one variable speed display must be installed for each lane. This implies that a total of 180 variable speed displays must be installed. This would cost TxDOT $666,000 to install the basic display shown in Figure 4.1. Installation of overhead signage is very expensive. It costs a minimum of about $50,000 to install each overhead sign bridge, including cost of installation truck and overtime hourly wages of workers. Assuming that installing three variable speed displays over a one-way three-lane freeway is considered as a single operation, TxDOT would have to pay for 60 such installations at a total cost of $3,000,000. Thus, implementing variable speed advisory on this 30-mile stretch would incur TxDOT a one-time cost of roughly $3,666,000. Installation of better displays such as variable message sign boards would cost at least three times this estimate. Additionally, assuming 24-hour operation, variable displays consume power for 8,760 hours per year. This translates to 1270.2 kWh of typical annual energy consumption per unit. Assuming an electricity price of 12 cents per kWh, TxDOT would incur an annual electricity cost of $27,450 for the 180 units.

Since a single DSRC beacon can provide speed advisory to vehicles in all six lanes, only 30 such units would be required to implement variable speed advisory on a 30-mile stretch. Considering an installation cost of $2,475 per unit [41], the total one-time cost per unit is $3,475. TxDOT would incur a one-time cost of $104,250 if this alternative is chosen. It must be pointed out that in this case the CV consumers must also incur a one-time cost of $291 per vehicle. In light of the impending CV mandate, this might not be an issue of concern. Once again, assuming 24-hour operation, DSRC beacons would consume 35 kWh of energy annually. This would lead to an annual electricity expense of $126 for all the 30 units.

In summary, choosing the DSRC beacon approach in this scenario provides 35 times the savings to TxDOT on one-time investments, and 220 times the savings on annual electricity expense (neglecting the costs common to both approaches). Clearly, CV-enabled variable speed advisory is much more economical to TxDOT. In view of the impending CV mandate, installing variable speed displays approach is not recommended.

4.4 Security Considerations

In the last chapter we reviewed the security issues in DSRC and outlined the various attacks against CVs. Some of those attacks were mitigated using the IEEE 1609.2 standard for message security and authentication, while others were still open problems. In this section, these security issues are analyzed for the special case of variable speed advisory.

Recall that in this application, the CVs only receive advisory from the infrastructure RSUs. Only the RSUs must generate and transmit advisory messages. This is an important distinction from the case in which all CVs transmit their position and velocity to neighboring vehicles. As a result of this special setup, advisory applications are immune to the types of attacks that are in general possible against CVs.

As mentioned in the last chapter, counterfeit message generation, message tampering, and MITM attacks are precluded using authentication, encryption, and time-stamping. Moreover, connected infrastructure beacons are not concerned about their privacy. One possible attack against these systems is the masquerading attack where an internal attacker attempts to act as an advisory node and transmits malicious advisory messages. These attacks can be easily prevented by embedding information about the privileges of the V2X node in its authentication key. In other words, the authentication key possessed by a V2X node reflects the type of messages it is permitted to broadcast. This defense ensures that advisory messages cannot be successfully transmitted by nodes that are not a part of the installed infrastructure units. Such defenses have already been proposed in the DSRC standard. It must be noted that it is assumed that an attacker would not be able to physically or electronically hack the infrastructure RSUs.

Thus, it can be concluded that while CVs in general are susceptible to spoofing and internal attacks, these advisory applications are immune to such attacks so long as the RSUs are not accessible to malicious hackers.

4.5 Recommendations

As outlined in Section 4.1, variable speed advisory has been proven to be effective in aiding speed harmonization and making roadways safer. As a result, we recommend that TxDOT should incrementally implement variable speed advisory on Texas freeways. This subsection provides guidelines on gradual roll out of variable speed advisory using connected infrastructure beacons approach. Further research needs to be done to assess the confusion due to DSRC-based variable speed advisory for the drivers who are not equipped with connected vehicle technology.

4.5.1 Low Connected Vehicle Penetration Scenario

CV penetration is minimal at the time of writing this report. As a result, investing in CV-infrastructure-dependent variable speed advisory will not yield significant immediate rewards. We recommend that TxDOT should begin testing and experimentation of variable speed advisory using portable RSUs.

Non-recurrent congestion accounts for about 50% of all traffic congestion [85]. The main causes for non-recurrent congestion are traffic incidents such as flat tires and disabled vehicles, special events, work zones, and weather. We claim that variable speed advisory in such situations can be implemented using portable DSRC beacons. For example, in case of a collision, the relevant response team can carry a portable DSRC RSU and set it up at the incident site. Any CV approaching the incident site is made aware of the optimum speed in the approaching accident zone about half a mile in advance. This prevents panic braking and related rear-end collisions. As explained earlier, even if 20% of the vehicles were to comply with this advisory, speed harmonization can be achieved and non-recurrent congestion can be mitigated.

It should be noted that similar techniques are currently employed near work zones where portable variable matrix signs are placed to warn motorists about work zone and advise lane changing or merging. However, it is not convenient to transport this variable matrix sign to traffic incident sites. A portable DSRC RSU is a better alternative.

This approach is attractive because it does not need any fixed infrastructure, and thus TxDOT's investment is minimal. As mentioned before, the cost of a DSRC RSU would be less than $500 per unit. As CV penetration increases, this technique will become more efficient. Moreover, this approach also gives TxDOT an opportunity to validate the benefits of variable speed advisory using DSRC beacons with minimal investment.

4.5.2 High Connected Vehicle Penetration Scenario

If the performance benefits observed using portable RSUs are encouraging, then TxDOT should start deploying fixed connected infrastructure beacons on freeway areas that experience recurrent congestion. Ideally, this deployment should be undertaken when more than 50% of the vehicles are connected. Under such a scenario, immediate reduction of recurrent congestion and related collisions will be observed. Although many such experiments have already been performed worldwide using variable message and variable speed display signs, TxDOT could pioneer the implementation of economical and efficient speed advisory using connected infrastructure.

Chapter 5

Recommendations

5.1 Information Flow Quality Recommendations

5.1.1 Promote Industry Cooperation on LTE

LTE networks use licensed spectrum obtained at great cost by network operators (e.g. AT&T, Verizon, Sprint). These companies have invested a considerable amount of money to establish the current high-speed cellular network. One issue network operators are facing today is that the number of mobile devices keep increasing while the available spectrum is limited. The operating CV on the cellular networks would seemingly largely be left to the whims of this small handful of large corporations.

One possible way of incentivizing those large companies to allow CVs on their networks would be to give those corporations access to the DSRC spectrum in the exchange for enabling CV safety applications. The LTE networks enable safety applications by delivering BSMs between vehicles and RSUs. Partnerships between government agencies and network operators could be arranged, assuming the agreement fulfills the mutual interests of parties. Private companies will use the DSRC spectrum willingly to support their infotainment demands; government agencies would like to enable safety applications without investing huge amounts of money in order to deploy CVs the network.

5.1.2 Consider Longevity of Communication Standards

Most wireless communication standards, including 802.11-based standards and LTE, have relatively short life cycles when compared to that of automobiles. For example, a new Wi-Fi standard has emerged every few years. The 3GPP standards have also been evolving, from 3G UMTS to 4G LTE, and then to 5G mmWave (possibly). The life cycle of these technologies is at most 10 years, after which time they are retired completely. Since personal communication devices like smart phones typically last only 3 to 5 years at most, this has not posed a major problem. However, vehicles routinely stay on the road for 15 to 20 years. Thus, the compatibility and longevity of communication technologies and devices is a critical issue in the effective implementation of CV applications. Implementing easily replaceable communication equipment on vehicles would be a viable solution to ensure compatibility. In particular, the approach is excellent for 4G LTE which requires only small devices or models for reliable communications.

5.2 Information Flow Security Recommendations

This section presents some security recommendations that must be considered by TxDOT before deployment of CVs in Texas. These recommendations augment the current research efforts reviewed earlier in this report.

5.2.1 Require Dual-Antenna GNSS to Secure Own-Vehicle Positioning

Reliable own-vehicle positioning is the first step towards secure CVs. Also, CVs require lane-level accurate estimates of their own position to make safe decisions in high-speed driving applications. To this end, the two-antenna Real Time Kinematic (RTK) system with RPM monitoring for defending against GNSS spoofing [69] is recommended. As mentioned in Section 3.3.1, the two-antenna method estimates the direction of arrival of GNSS signals to detect a spoofing attack. RTK systems should be considered as a required component for CVs. This system also allows for robust centimeter-accurate positioning, multipath mitigation, and attitude determination of nodes in a CV network. A demonstration of such a system was carried out as a part of this project.

Our research indicted that if RTK systems are not incorporated, CV operations would be unsafe for certain applications. For example, using commercial-grade GNSS receivers with an accuracy of 2-3 meters in CVs would render all applications that require lane-level position information unsafe to operate.

5.2.2 Move towards a DSRC Sensor Paradigm

As discussed earlier, the position and velocity claims in a CV network cannot be trusted without verification. Hence, DSRC on its own is an insecure system. In this subsection we propose that DSRC and other CV technology be treated as one among many sensors in a modern car. DSRC must be integrated with other sensors such as radar, ultrasonic sensor, LiDAR, and optical camera to symbiotically enhance the security of all sensors. In an ideal setup, a modern car should not be vulnerable to compromise unless all of its sensors are spoofed simultaneously in a consistent manner.

Use of multiple sensors for robust sensing is a common practice. For example, positioning based on feature matching is usually aided with precise GNSS. Feature matching based positioning works better in urban areas where GNSS availability is limited. In inclement weather, obtaining visual features is a challenge for optical sensors, but GNSS signals are unaffected by weather elements. We recommend similar fusion of DSRC with other vehicular sensors.

DSRC-Radar Fusion The fusion of DSRC and radar makes a formidable composite system [86, 87]. DSRC requires all neighbors to actively engage and act honestly in order to function safely. Radar, on the other hand, does not require active participation of the neighboring vehicles. However, radar signals are not authenticated or encrypted and no signal verification is performed. These failure modes of radar and DSRC are complementary.

DSRC-based location verification fails in absence of multiple neighbors. In contrast, radar is inadequate in high density traffic and cannot detect vehicles shadowed by other vehicles. Once again, these limitations are complementary and the two systems compensate for each other's flaws.

Consider a spoofing scenario in which the attacker attempts to spoof radar signals using a signal generator. Such an attack can be detected using DSRC messages and associated verification as long as the attacker does not spoof both systems simultaneously. Similarly, if an attacker is close to the verifier but claims a farther location in its DSRC messages, it can be detected using radar.

We recommend integration of such composite systems before mass market deployment of CVs. The radar-DSRC combination provides promising security advantages.

5.2.3 Deploy Secure Credential Management System

The PKI credential management guidelines are under development. As discussed earlier, the DSRC standards in Europe only recommend revocation of the LTC of a misbehaving node, and do not deal with the pseudonyms already possessed by the attacker. Such an implementation is insecure.

There has been considerable research on efficient distribution of CRLs, and SCMS has emerged as a leading candidate for deployment in the US [55]. This report backs the implementation of SCMS in the US CV network. The most important contribution of this system is that it presents an efficient technique to revoke all pseudonyms of a vehicle using *linkage values*.

Furthermore, current standards and the literature do not consider the problem of a MITM attacker or multipath sources tarnishing the reputation of an honest node. Revocation of certificates under such circumstances would be troublesome for the users of connected vehicles. Thus, special care must be taken in deployment of a secure credential management system.

5.3 Industry Partnership

Emerging technologies in the cellular industry are leading to a proliferation of base stations deployed by cellular service providers. In addition to the traditional *macrocells*, cellular providers are deploying *small cell* radio access nodes to cope with the increasing data demand indoors over the cellular channel [88, 89]. Small cells are low-power radio nodes with a relatively small range, typically less than a kilometer. These nodes have a small form factor and can be deployed easily on poles and other such infrastructure. The use of small cells has been proven to be effective in East Asian regions.

Due to their limited range, small cell nodes must be deployed as a dense network. Although the dense deployment of small cell nodes is inconvenient, industry cellular providers are eager to take up this challenge because of the many potential benefits of small cells such as improved coverage, location-based services, etc. [88]. Illumination poles, traffic light signal poles, tubular piped gantries, etc., are ideal infrastructure for mounting small cells, and thus the industry cellular providers have great interest in using TxDOT's infrastructure for this purpose. Figure 5.1 demonstrates the non-intrusive nature of small cell deployment.

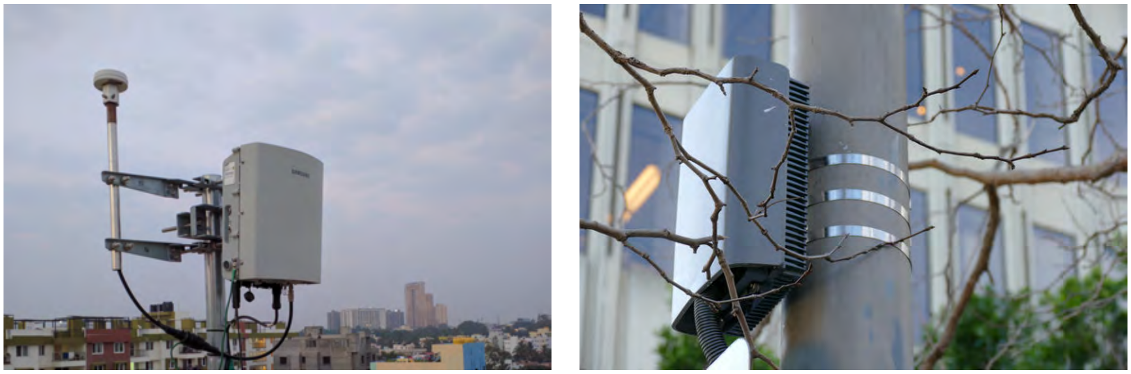


Figure 5.1: Two Examples of Small Cell Deployment

We recommend that TxDOT should consider building public-private partnerships with industry cellular providers to leverage TxDOT's right-of-way in exchange for free-of-cost safety-related CV communication over cellular networks. In particular, TxDOT should strike a deal in which the cellular providers relay the BSMs between connected vehicles without charging any subscription fee to the vehicle owners. In exchange the cellular providers may install non-intrusive small cell cellular nodes on TxDOT infrastructure such as highway gantries and guard rails or on local city government infrastructure such as traffic light signal poles and illumination poles.

As the cellular industry transitions from 4G LTE to 5G, the industry service providers would be even more interested in such a deal. With the onset of 5G technology, many factors will strengthen TxDOT's position in this public-private partnership. The 5G cellular technology is being developed keeping in mind that CVs will be one of the end-users. Furthermore, 5G requires a very dense network of small base stations that must be in the line-of-sight of the user equipment – in this case the vehicles [90]. It is clear that the optimal location to mount this infrastructure for CVs would be on TxDOT's roadway infrastructure. Thus, TxDOT is in a good position to negotiate free-of-cost roadway safety services from cellular providers. Through their contacts in cellular industry and cellular real-estate companies, the WNCG and CTR can assist TxDOT in bringing such a deal to fruition.

Chapter 6

Conclusions

Connected vehicles (CVs) are the future of transportation. CV technology utilizes wireless communication to realize real-time information exchange among vehicles, transportation infrastructure, and personal communication devices. The CV technology underpins many potential applications in safety, mobility, and infotainment. Looking to effectively and securely deploy these applications, industry and academia have paid considerable attention to making connections between vehicles as secure as possible while maintaining efficient wireless network use and protecting the privacy of users of CV technology. The goal of this project was to provide an up-to-date understanding of information flow quality and security issues in CV environments, as well as a preliminary guideline for optimizing information flow in Texas.

In terms of information flow quality, the objective was to compare and evaluate existing and emerging VANET (vehicular ad-hoc network) technologies in CV environments, including, but not limited to, the architecture, routing protocols, and hardware of vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications. This project focused on two major communication standards: dedicated short-range communications (DSRC) and Long-Term Evolution (LTE). In the area of information flow security, the team identified the open problems through a critical review of current security measures and potential issues. Extensive studies have shown that the security measures in existing standards are deficient and must be augmented for safe operation of CVs. The team reviewed these security issues and proposed potential solutions to address the security gaps. Based on analysis of the information flow quality and security issues, the team developed preliminary guidelines and analyzed two examples of CV-enabled applications for traffic management.

To achieve the above goals, the team conducted the following research activities:

- Provided a critical review of key candidate technologies (including DSRC and LTE) enabling CV applications, along with a baseline analysis on the tradeoffs and challenges presented by different current and future approaches to CVs.

- Conducted an extensive simulation study to evaluate VANETs with DSRC protocol (which uses the IEEE 802.11p standard), under a variety of performance metrics, including packet delivery ratio, throughput, and end-to-end delay. The performance of DSRC was compared with LTE.
- Analyzed DSRC and LTE costs and developed a customizable Excel spreadsheet tool to perform calculations.
- Provided a critical review of security issues in CV environments and identified the open problems and major threats.
- Recommended and demonstrated a Real-Time Kinematic GNSS positioning system towards addressing GNSS spoofing. Secure own-vehicle positioning is a necessary pre-requisite for secure CVs. This secure centimeter-accurate positioning system is a must-have for all CVs.
- Developed a preliminary guideline on networking information flow optimization and conducted case studies on two CV-enabled transportation applications in hypothetical scenarios.

The major findings include the following:

- Comparing the performance of DSRC with requirements and the demonstrated performance for the current state-of-the-art cellular standard, LTE, we concluded that VANETs are at a severe disadvantage except for extremely short range one-hop communication between slowly moving vehicles. We tentatively concluded that the DSRC may find limited use for certain short-range applications.
- The preliminary cost analysis indicates that the cost arguments in favor of DSRC are also unpersuasive at this time.
- To achieve a reliably and widely connected vehicular network, leveraging the cellular providers superior technology and network infrastructure appears to be the most plausible course of action.
- We established the position and velocity accuracy requirements for safe operation of CVs. A vehicles own position must be estimated with decimeter-level accuracy for

lane-keeping, and it must be able to verify a neighbors position to within a meter to disambiguate the lane that the neighboring vehicle occupies.

Two important implications may be drawn from the above findings:

- **DSRC vs. LTE**: The 3GPP standard body (which developed LTE) has been working on machine-to-machine communication supported by the cellular base stations and is paying increasing attention to vehicular applications in their future releases. Given the limitations of the DSRC standard and as compared to the capabilities and expected future evolution of the cellular infrastructure, we suggest TxDOT take a skeptical view as to what can be achieved with DSRC in the near future.
- **CV Security**: Infrastructural control is critical to establish secure vehicular communication, and LTE-based cellular networks provide such infrastructure. We suggest that DSRC, or any alternative communication technology for CVs, be combined with other modern vehicle sensors such as radar or optical cameras to enhance the security of neighbor position verification protocols. Finally, this projects analysis suggests that standards for credential revocation in CVs be revamped to defend CV networks against attacks.

Appendices

Appendix A

Accuracy Requirements for Connected Vehicles

It is important to lay down the position and velocity accuracy requirements for connected vehicles because these requirements determine the success of a security scheme. In other words, a scheme is only considered to be secure if it guarantees that the vehicle's reported position and velocity satisfy the accuracy requirements with the required probability.

In order to lay down these requirements, this report borrows the following definitions from aviation standards and adapts them to ground transportation:

- *Accuracy*: Accuracy in a given plane or direction is defined as the 95% error bound in that plane or direction. For example, 1 meter position accuracy in the lateral direction implies that the lateral error in position is less than 1 meter in 95% of all navigation solutions.

- *Alert Limit*: Maximum permissible error between the reported and true location without issuing an alert is defined as the Alert Limit (AL). For example, a lateral position AL of 1 meter implies that it is unsafe to operate the system if the lateral error in position exceeds 1 meter and an alert is not issued.

- *Integrity Risk*: The probability of true error being larger than the AL is defined as the Integrity Risk (IR). IR is usually specified as a constant and must be met for safe operation. Note that it is not possible to determine the true error during normal operations.

These definitions are visually represented in Figure A.1.

This report makes two claims:

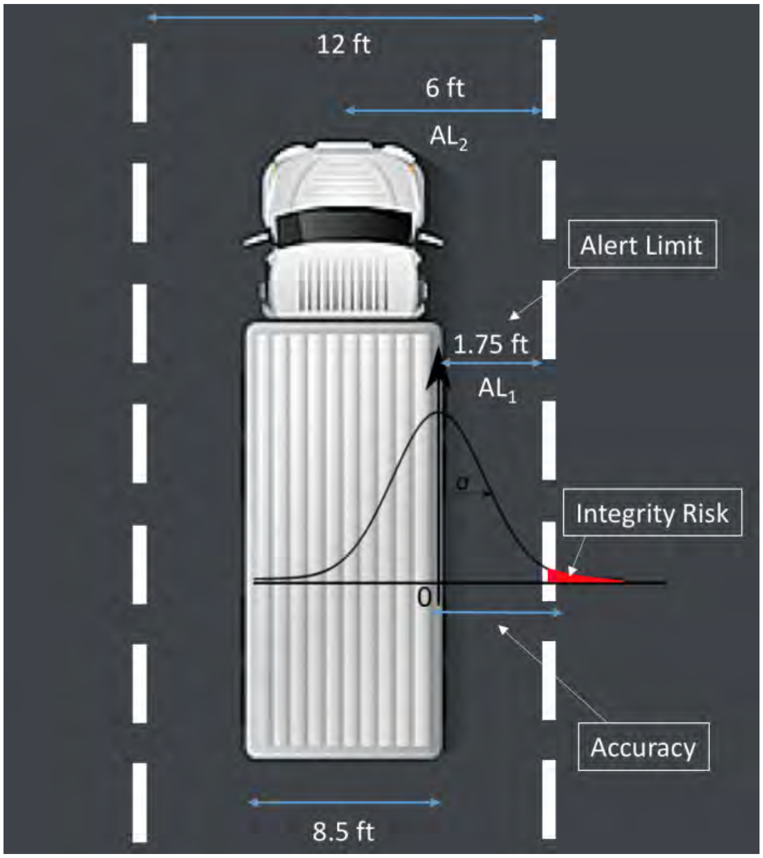


Figure A.1: Definitions of Accuracy, Alert Limit, and Integrity Risk adapted to ground transportation. AL_1 represents the AL for own-vehicle positioning; AL_2 represents the AL for neighbor-vehicle positioning.

1. The accuracy requirements are more stringent in the direction lateral to car's movement, where it is assumed that the car is moving parallel to the lane markings (longitudinal direction). This is because the separation between a vehicle and the lane markings is almost always less than the separation between two vehicles in a lane. This claim implies that it is sufficient to only compute the lateral requirements and safely assume the same requirements in the longitudinal direction.

2. The accuracy requirements for a vehicle's own position and velocity are different than the accuracy requirements for the position and velocity information it receives from its neighbors. The reason for this difference is that the applications that rely on own position and velocity need higher accuracy than those that depend on neighbor's position and velocity. For example, for safe operation a given vehicle must not drift out of its designated lane. This is enabled by the vehicle knowing its own lateral position accurately to within a small fraction of the total lane width. However, other

maneuvers such as passing or merging depend on which lane the other vehicles are in. This lane disambiguation can be performed with less accurate neighbor position information and allows a lateral error of about half a lane width.

The following subsections compute these lateral accuracy requirements for own-vehicle and neighboring vehicles separately.

A.1 Own-Vehicle Accuracy Requirements

The minimum lane width on US highways is specified to be 12 feet, and the maximum width of tractor trailer is specified to be 8.5 feet. Consider such a tractor trailer that wishes to stay in its lane for safe operation. From Figure A.1 it is observed that in this scenario the lateral position AL is 1.75 feet, or 53.34 cm. Consider a typical IR of 10^{-6}. In a Gaussian distribution, satisfying this IR entails that the AL must fall within 4.89σ of the error distribution, where σ is the standard deviation of lateral position errors. This translates into lateral position error standard deviation of σ =10.9 cm. Since accuracy is defined as 95% (or equivalently, 2σ) error bound, the own-vehicle position accuracy requirement for safe connected vehicle operations is 21.8 cm. As claimed above, this can safely be assumed to be the longitudinal position accuracy requirement too.

The instantaneous lateral velocity is, by definition, equal to zero when the vehicle is not changing a lane. The requirement for longitudinal velocity accuracy is a function of the trajectory of the road ahead, as well as the distances to the vehicles in front and behind. Assuming that the vehicle updates its position and velocity at a rate of 10 Hz, a velocity error standard deviation requirement of 10 cm per second is reasonable.

A.2 Neighbor-Vehicle Accuracy Requirements

Consider a minimum lane width of 12 feet, and a vehicle A moving in a lane. Consider another connected vehicle that wishes to know which lane A is in. If the second vehicle knows the lateral position of A to within half a lane's width, then it can disambiguate which lane A is occupying (assuming that A is not switching lanes). This implies that a lateral position error of 6 feet is permissible. Thus, in this scenario the lateral AL is 6 feet, or 182.88 cm. Assuming a typical IR of 10^{-6} and Gaussian-distributed errors, this AL corresponds to approximately 4.89σ, where σ is the standard deviation of lateral positajectory of the road ahead, as well as the distances to the vehicles ation of σ =37.4 cm. Since accuracy is defined as 95% (or equivalently, 2σ) error bound, the neighbor-vehicle position accuracy requirement for safe connected vehicle operations is 74.8 cm. As claimed above, this can also safely be assumed to be the longitudinal position accuracy requirement for neighboring vehicles.

If it is assumed that A is not switching lanes, that is, it is moving parallel to the lane markings, then the velocity accuracy requirements can be relaxed. However, if it is not known whether A is switching lanes, then it becomes important to know A's lateral velocity to about 10 cm per second. Once again, this velocity requirement depends on multiple factors. The 10 cm per second value is a reasonably conservative requirement.

Appendix B

Two-Antenna Spoofing Detection Demonstration

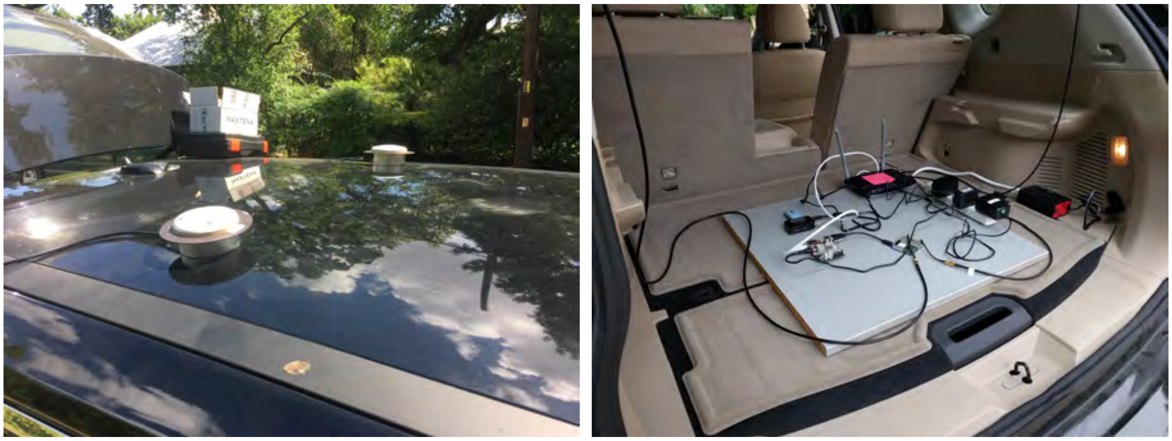
An implementation of the two-antenna spoofing detection mechanism was demonstrated on the University of Texas at Austin campus. This demonstration serves as a proof-of-concept for the corresponding recommendation made in Chapter 5.

The demonstration vehicle was outfitted with two GNSS antennas mounted with magnetic bases onto the vehicle roof. These antennas were be located towards the rear of the passenger cabin and oriented side-by-side. This set up is shown in Figure B.1. One of these antennas, designated *rov0*, was operated as the *rover antenna* in a single-baseline precise positioning solution against the master reference station of the Longhorn Dense Reference Network (LDRN) [91]. The LDRN is a network of GNSS reference stations deployed in Austin, TX by the UT Radionavigation Lab. The LDRN master reference station is located on the rooftop of the Aerospace Engineering building on the UT-Austin campus. The single-baseline solution between *rov0* and LDRN master reference station provides a georeferenced precise vehicle position. The second antenna, designated *rov1*, participates in a fixed-baseline two-dimensional attitude solution with *rov0* to provide vehicle heading. A basic visualization of this configuration is shown in Figure B.2.

The two GNSS antennas on the roof of the demonstration vehicle were connected to a software-defined receiver (SDR) running on a smartphone applications processor located in the trunk of the vehicle. A cellular data connection relayed real-time measurements from the master reference station to the SDR.

The RTK solution developed in this demonstration was constrained by the known separation between the *rov0* and *rov1* antennas. If the same spoofed GNSS signals were to be received by these two antennas, then the solution would collapse and become unavailable as a result of this constraint. Note that such unavailability could also occur due to other phenomenon like blockage of signals, so it is not a definitive indication of a spoofing attack. However, it is assured that no navigation solution would be generated if spoofed GNSS signals were received.

This two-antenna set up can be extended to perform the detection test proposed in [69]. When coupled with an RPM spoofing detector [62], this is a very capable solution and makes the connected vehicle network highly robust against GNSS spoofing.



(a) Two-antenna set up on roof of the demonstration vehicle for two-antenna RTK and spoofing detection.

(b) Electronics hub in demonstration vehicle trunk. Includes CDGNSS receiver, smartphone processor, and WiFi router.

Figure B.1: Demonstration vehicle two-antenna set up and processing hub.

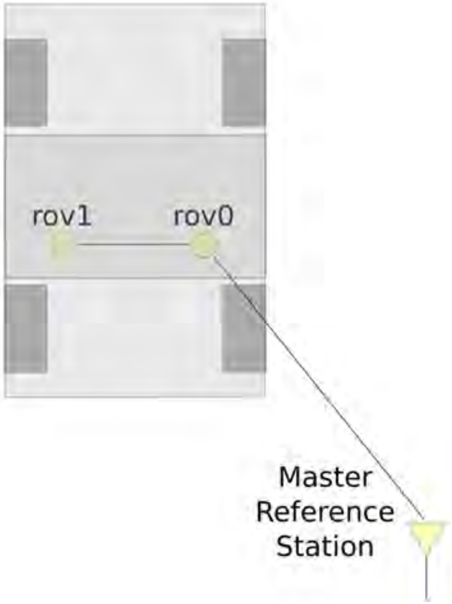


Figure B.2: Basic visualization of GNSS antenna configuration. A single-baseline precise position solution between *rov0* and the master reference station provides precise vehicle position. A fixed-baseline 2D attitude solution between *rov0* and *rov1* provides vehicle heading.

Appendix C

Security Issues in LTE

This appendix presents some of the shortcomings of the existing LTE standards for use in connected vehicles. Note that in addition to these security issues, LTE is vulnerable to all attacks that were effective against DSRC. In other words, LTE is vulnerable to internal attacks and GNSS spoofing, just like DSRC, but is also vulnerable to some other security issues.

LTE has made significant improvements over its predecessors (3G, CDMA, GPRS, etc.) in terms of security. The User Equipment (UE) performs bidirectional authentication with the cellular network, that is, UE authenticates the cellular network it is connecting to and the cellular network authenticates UE as a legitimate LTE user. This is followed by symmetric key encryption schemes such as AES or SNOW 3G to encrypt the data exchanged between the user and base stations.

However, recent research has shown that LTE is vulnerable to denial-of-service (DoS) attacks. These attacks exploit the unauthenticated and unencrypted information exchange between the UE and base station in the initial Attach phase. Similar vulnerabilities lead to abuse of privacy of the UE by fake base stations. These attacks are briefly described below.

It has been shown in [92] that it is straightforward to set up a malicious LTE eNodeB (base station) with commercially available hardware. The UE can be persuaded to connect to the malicious eNodeB by using high transmit power or by locating the malicious eNodeB very close to the physical location of the UE. During the initial *Attach* phase, the malicious eNodeB can disallow the use of LTE to its subscribers. No encryption or authentication keys are needed on the part of the eNodeB to disallow LTE service. This forces the UE to downgrade to older generations of cellular connectivity such as 3G or GSM, if available. These standards have much weaker security mechanisms. This downgrade opens the door for other attacks relevant to older generations of cellular protocols.

A passive or semi-passive [92] LTE attacker has been shown to be able to learn the coarse location of a UE by sniffing *paging* messages issued by the cellular network. Furthermore, an active eNodeB attacker can exploit vulnerabilities in the specification and implementation of LTE Radio Resource Control (RRC) protocol to accurately pinpoint the UE via GPS coordinates or multilateration using base station signal strengths as observed by that UE. All LTE devices currently deployed are vulnerable to such attacks. This is in contrast with the DSRC standards that use short-lived pseudonyms to prevent temporal tracking of vehicles.

In conclusion, even though the current LTE security mechanisms are an upgrade to previous generations of cellular protocols, a few modifications are required for adoption in safety-of-life applications such as connected vehicles.

Bibliography

[1] J. Kenney, "Dedicated short-range communications (DSRC) standards in the united states," *Proceedings of the IEEE*, vol. 99, no. 7, pp. 1162–1182, 2011.

[2] "IEEE Standard for Wireless Access in Vehicular Environments–Security Services for Applications and Management Messages," *IEEE Std 1609.2-2016 (Revision of IEEE Std 1609.2-2013)*, pp. 1–240, March 2016.

[3] "IEEE Standard for Information technology– Local and metropolitan area networks– Specific requirements– Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments," *IEEE Std 802.11p-2010 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008, IEEE Std 802.11r-2008, IEEE Std 802.11y-2008, IEEE Std 802.11n-2009, and IEEE Std 802.11w-2009)*, pp. 1–51, Jul. 2010.

[4] "IEEE Standard for Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: High Speed Physical Layer in the 5 GHz band," *IEEE Std 802.11a-1999*, pp. 1–102, Dec 1999.

[5] "IEEE Standard for Wireless Access in Vehicular Environments (WAVE)–Multi-channel Operation," *IEEE Std 1609.4-2010 (Revision of IEEE Std 1609.4-2006)*, pp. 1–89, Feb. 2011.

[6] "IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services," *IEEE Std 1609.3-2010 (Revision of IEEE Std 1609.3-2007)*, pp. 1–144, Dec. 2010.

[7] C. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers," in *Proc. 1994 ACM SIGCOMM*, vol. 24, pp. 234–244, ACM, 1994.

[8] T. Clausen and P. Jacquet, “Optimized link state routing protocol (OLSR),” tech. rep., 2003.

[9] R. Ogier, F. Templin, and M. Lewis, “Topology dissemination based on reverse-path forwarding (TBRPF),” tech. rep., 2004.

[10] C. Perkins, E. Belding-Royer, and S. Das, “Ad hoc on-demand distance vector (AODV) routing,” tech. rep., RFC 3561. 2003., 2003.

[11] Z. Haas, “A new routing protocol for the reconfigurable wireless networks,” in *Proc. IEEE Int. Conf. on Universal Personal Commun. Record*, vol. 2, pp. 562–566, Oct. 1997.

[12] B. Karp and H.-T. Kung, “GPSR: Greedy perimeter stateless routing for wireless networks,” in *Proc. Int. Conf. on Mobile Compu. and networking*, pp. 243–254, ACM, 2000.

[13] C. Lochert, H. Hartenstein, J. Tian, H. Fussler, D. Hermann, and M. Mauve, “A routing strategy for vehicular ad hoc networks in city environments,” in *Proc. IEEE IVS*, pp. 156–161, 2003.

[14] C. Lochert, M. Mauve, H. Füßler, and H. Hartenstein, “Geographic routing in city scenarios,” *ACM SIGMOBILE Mobile Comput. and Commun. Review*, vol. 9, no. 1, pp. 69–72, 2005.

[15] K. Lee, J. O. Häerri, U. Lee, and M. Gerl, “Enhanced perimeter routing for geographic forwarding protocols in urban vehicular scenarios,” in *IEEE Globecom Workshops*, pp. 1–10, 2007.

[16] K. Lee, M. Le, J. Härri, and M. Gerla, “LOUVRE: Landmark overlays for urban vehicular routing environments,” in *Proc. IEEE VTC*, pp. 1–5, 2008.

[17] V. Naumov and T. R. Gross, “Connectivity-aware routing (CAR) in vehicular ad-hoc networks,” in *Proc. IEEE INFOCOM*, pp. 1919–1927, 2007.

[18] J. Zhao and G. Cao, “VADD: Vehicle-assisted data delivery in vehicular ad hoc networks,” *IEEE Trans. Veh. Technol.*, vol. 57, pp. 1910–1922, May 2008.

[19] A. Skordylis and N. Trigoni, “Delay-bounded routing in vehicular ad-hoc networks,” in *Proc. ACM Intl Symp. on Mobile ad hoc networking and computing*, pp. 341–350, 2008.

[20] Y. Ding and L. Xiao, “SADV: static-node-assisted adaptive data dissemination in vehicular networks,” *IEEE Trans. Veh. Technol.*, vol. 59, pp. 2445–2455, Jun.

[21] Y. Luo, W. Zhang, and Y. Hu, “A new cluster based routing protocol for vanet,” in *Pro. IEEE Int. Conf. on NSWCTC*, vol. 1, pp. 176–180, 2010.

[22] T. Song, W. W. Xia, T. Song, and L. Shen, “A cluster-based directional routing protocol in VANET,” in *Proc. IEEE ICCT*, pp. 1172–1175, 2010.

[23] R. A. Santos, A. Edwards, R. Edwards, and N. L. Seed, “Performance evaluation of routing protocols in vehicular ad-hoc networks,” *Intl J. of Ad Hoc and Ubiquitous Computing*, vol. 1, pp. 80–91, Nov. 2005.

[24] M. Durresi, A. Durresi, and L. Barolli, “Emergency broadcast protocol for inter-vehicle communications,” in *Proc. Int. Conf. on Parallel and Distributed Systems*, vol. 2, pp. 402–406, Jul. 2005.

[25] G. Korkmaz, E. Ekici, F. Özgüner, and Ü. Özgüner, “Urban multi-hop broadcast protocol for inter-vehicle communication systems,” in *Proc. ACM Int. workshop on Veh. ad hoc networks*, pp. 76–85, 2004.

[26] W. Viriyasitavat, F. Bai, and O. K. Tonguz, “UV-CAST: an urban vehicular broadcast protocol,” in *Proc. IEEE VNC*, pp. 25–32, 2010.

[27] E. Fasolo, A. Zanella, and M. Zorzi, “An effective broadcast scheme for alert message propagation in vehicular ad hoc networks,” in *Proc. IEEE ICC*, pp. 3960–3965, 2006.

[28] 3GPP, “Evolved Universal Terrestrial Radio Access (E-UTRA); medium access control (MAC)protocol specification,” Tech. Rep. 3GPP TS 36.321.

[29] A. Vinel, “3GPP LTE versus IEEE 802.11p/wave: which technology is able to support cooperative vehicular safety applications?,” *IEEE Wireless Commun. Lett.*, vol. 1, pp. 125–128, Apr. 2012.

[30] Z. H. Mir and F. Filali, “LTE and IEEE 802.11p for vehicular networking: a performance evaluation,” *EURASIP J. on Wireless Commun. and Networking*, vol. 2014, no. 1, pp. 1–15, 2014.

[31] A. Moller, J. Nuckelt, D. M. Rose, and T. Kurner, “Physical layer performance comparison of LTE and IEEE 802.11p for vehicular communication in an urban NLOS scenario,” in *Proc. IEEE VTC*, pp. 1–5, 2014.

[32] A. Vinel, B. Bellalta, N. Chilamkurti, and Y. Koucheryavy, "Scalability analysis of infrastructure networks for vehicular safety applications," in *Proc. IEEE ICCVE*, pp. 124–127, 2012.

[33] K. Trichias, v. d. J. Berg, G. Heijenk, d. J. Jongh, and R. Litjens, "Modeling and evaluation of LTE in intelligent transportation systems," 2012.

[34] G. Araniti, C. Campolo, M. Condoluci, A. Iera, and A. Molinaro, "LTE for vehicular networking: a survey," *IEEE Commun. Mag.*, vol. 51, pp. 148–157, May 2013.

[35] 3GPP, "Policy and charging control architecture," Tech. Rep. 3GPP TS 23.203.

[36] M. Kihl, K. Bur, P. Mahanta, and E. Coelingh, "3GPP LTE downlink scheduling strategies in vehicle-to-infrastructure communications for traffic safety applications," in *Proc. IEEE ISCC*, pp. 448–453, Jul. 2012.

[37] A. Ghosh, J. Zhang, J. Andrews, and R. Muhamed, *Fundamentals of LTE*. Pearson Education, 2010.

[38] 3GPP, "Introduction of the multimedia broadcast multicast service (MBMS) in the radio access network (RAN)," Tech. Rep. 3GPP TS 25.346.

[39] A. Festag, M. Wiecker, and N. Zahariev, "Safety and traffic efficiency applications for GeoMessaging over cellular mobile networks," in *Proc. of the 19th ITS World Congress*, Oct. 2012.

[40] 3GPP, "Technical specification group services and system aspects; feasibility study for proximity services (ProSe)," Tech. Rep. 3GPP TR 22.803.

[41] J. Wright, K. Garrett, C. Hill, G. Krueger, J. Evans, S. Andrews, C. Wilson, R. Rajbhandari, and B. Burkhard, "National connected vehicle field infrastructure footprint analysis," tech. rep., 2014.

[42] D. Meyer, "AT&T speeds up connected car business," *RCR Wireless*, Feb 2016.

[43] K. Wesson, *Secure navigation and timing without local storage of secret keys*. PhD thesis.

[44] D. Magazu III, "Exploiting the automatic dependent surveillance-broadcast system via false target injection," tech. rep., DTIC Document, 2012.

[45] D. L. McCallie, “Exploring potential ads-b vulnerabilites in the faa’s nextgen air transportation system,” tech. rep., DTIC Document, 2011.

[46] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, “Secure vehicular communication systems: design and architecture,” *IEEE Communications Magazine*, vol. 46, no. 11, pp. 100–109, 2008.

[47] P. Papadimitratos, A. La Fortelle, K. Evenssen, R. Brignolo, and S. Cosenza, “Vehicular communication systems: Enabling technologies, applications, and future outlook on intelligent transportation,” *IEEE Comm. Mag.*, vol. 47, no. 11, pp. 84–95, 2009.

[48] P. Papadimitratos, M. Poturalski, P. Schaller, P. Lafourcade, D. Basin, S. Capkun, and J.-P. Hubaux, “Secure neighborhood discovery: a fundamental element for mobile ad hoc networking,” *IEEE Communications Magazine*, vol. 46, no. 2, pp. 132–139, 2008.

[49] M. Khodaei, H. Jin, and P. Papadimitratos, “Towards deploying a scalable & robust vehicular identity and credential management infrastructure,” in *2014 IEEE Vehicular Networking Conference (VNC)*, pp. 33–40, IEEE, 2014.

[50] M. Khodaei and P. Papadimitratos, “The Key to Intelligent Transportation: Identity and Credential Management in Vehicular Communication Systems,” *IEEE Vehicular Technology Magazine*, vol. 10, no. 4, pp. 63–69, 2015.

[51] Y. Sinelschikova, “Why is the Kremlin ’transporting’ GPS users to Vnukovo airport?,” 2016.

[52] ETSI, “Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions,” *ETSI Tech. Rep TR-102-638*, 2009.

[53] N. Bißmeyer, H. Stübing, E. Schoch, S. Götz, J. P. Stotz, and B. Lonc, “A generic public key infrastructure for securing Car-to-X communication,” in *18th ITS World Congress, Orlando, USA*, vol. 14, 2011.

[54] Y. Liang, V. Poor, *et al.*, “Information theoretic security,” *Foundations and Trends in Communications and Information Theory*, vol. 5, no. 4–5, pp. 355–580, 2009.

[55] W. Whyte, A. Weimerskirch, V. Kumar, and T. Hehn, “A security credential management system for v2v communications,” in *2013 IEEE Vehicular Networking Conference*, pp. 1–8, IEEE, 2013.

[56] M. Psiaki and T. Humphreys, “GNSS Spoofing and Detection,” *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1258–1270, 2016.

[57] B. W. O’Hanlon, M. L. Psiaki, J. A. Bhatti, D. P. Shepard, and T. E. Humphreys, “Real-time GPS spoofing detection via correlation of encrypted signals,” *Navigation*, vol. 60, no. 4, pp. 267–278, 2013.

[58] A. Kerns, K. Wesson, and T. Humphreys, “A blueprint for civil GPS navigation message authentication,” in *2014 IEEE/ION Position, Location and Navigation Symposium-PLANS 2014*, pp. 262–269, IEEE, 2014.

[59] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, “GPS vulnerability to spoofing threats and a review of antispoofing techniques,” *International Journal of Navigation and Observation*, vol. 2012, 2012.

[60] C. Günther, “A survey of spoofing and counter-measures,” *Navigation*, vol. 61, no. 3, pp. 159–177, 2014.

[61] C. Tanıl, S. Khanafseh, and B. Pervan, “Gnss spoofing attack detection using aircraft autopilot response to deceptive trajectory,” 2015.

[62] D. Akos, “Who’s afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control (AGC),” *Navigation*, vol. 59, no. 4, pp. 281–290, 2012.

[63] T. Humphreys, B. Ledvina, M. Psiaki, B. OHanlon, and P. Kintner Jr, “Assessing the spoofing threat: Development of a portable GPS civilian spoofer,” in *Proceedings of the ION GNSS international technical meeting of the satellite division*, vol. 55, p. 56, 2008.

[64] J. Volpe, “Vulnerability assessment of the transportation infrastructure relying on the global positioning system,” 2001.

[65] P. Montgomery, T. Humphreys, and B. Ledvina, “Receiver-autonomous spoofing detection: Experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer,” in *Proceedings of the ION International Technical Meeting*, pp. 124–130, 2009.

[66] A. Kerns, D. Shepard, J. Bhatti, and T. Humphreys, “Unmanned aircraft capture and control via GPS spoofing,” *Journal of Field Robotics*, vol. 31, no. 4, pp. 617–636, 2014.

[67] T. Humphreys, J. Bhatti, D. Shepard, and K. Wesson, "The Texas Spoofing Test Battery: Toward a standard for evaluating GNSS signal authentication techniques," in *Proceedings of the ION GNSS Meeting*, 2012.

[68] E. Manfredini, B. Motella, and F. Dovis, "Signal quality monitoring for discrimination between spoofing and environmental effects, based on multidimensional ratio metric tests," *Proc. ION GNSS+, Tampa, FL*, 2015.

[69] M. Psiaki, B. O'Hanlon, S. Powell, J. Bhatti, K. Wesson, T. Humphreys, and A. Schofield, "GNSS spoofing detection using two-antenna differential carrier phase," *Proceedings of the ION GNSS+ Meeting, (Tampa, FL)*, 2014.

[70] M. Fiore, C. E. Casetti, C.-F. Chiasserini, and P. Papadimitratos, "Discovery and verification of neighbor positions in mobile ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 12, no. 2, pp. 289–303, 2013.

[71] N. Chandran, V. Goyal, R. Moriarty, and R. Ostrovsky, "Position based cryptography," in *Advances in Cryptology-CRYPTO 2009*, pp. 391–407, Springer, 2009.

[72] N. Chandran, S. Fehr, R. Gelles, V. Goyal, and R. Ostrovsky, "Position-based quantum cryptography," *arXiv preprint arXiv:1005.1750*, 2010.

[73] H. Buhrman, N. Chandran, S. Fehr, R. Gelles, V. Goyal, R. Ostrovsky, and C. Schaffner, "Position-based quantum cryptography: Impossibility and constructions," *SIAM Journal on Computing*, vol. 43, no. 1, pp. 150–178, 2014.

[74] H.-K. Lau and H.-K. Lo, "Insecurity of position-based quantum-cryptography protocols against entanglement attacks," *Physical Review A*, vol. 83, no. 1, p. 012322, 2011.

[75] M. Mirshahi, J. T. Obenberger, C. A. Fuhs, C. E. Howard, R. A. Krammes, B. T. Kuhn, R. M. Mayhew, M. A. Moore, K. Sahebjam, C. J. Stone, *et al.*, "Active traffic management: the next step in congestion management," Tech. Rep. FHWA-PL-07-012, Federal Highway Administration, July 2007.

[76] X.-Y. Lu, J. Lee, D. Chen, J. Bared, D. Dailey, and S. E. Shladover, "Freeway microsimulation calibration: case study using aimsun and vissim with detailed field data," in *93rd Annual Meeting of the Transportation Research Board, Washington, DC*, 2014.

[77] A. Hegyi, B. De Schutter, and J. Hellendoorn, “Optimal coordination of variable speed limits to suppress shock waves,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 6, no. 1, pp. 102–112, 2005.

[78] M. Papageorgiou, E. Kosmatopoulos, and I. Papamichail, “Effects of variable speed limits on motorway traffic flow,” *Transportation Research Record: Journal of the Transportation Research Board*, no. 2047, pp. 37–48, 2008.

[79] G.-L. Chang, S. Park, and J. Paracha, “Intelligent transportation system field demonstration: integration of variable speed limit control and travel time estimation for a recurrently congested highway,” *Transportation Research Record: Journal of the Transportation Research Board*, no. 2243, pp. 55–66, 2011.

[80] M. Robinson, “Examples of variable speed limit applications,” 2000.

[81] J. K. Markt, “Evaluation of the safety and mobility impacts of a proposed speed harmonization system: the interstate 35 case study,” 2012.

[82] Daktronics, *Vanguard VS-5220-2-18-W Variable Speed Limit Sign*.

[83] J. Harding, G. Powell, R. Yoon, J. Fikentscher, C. Doyle, D. Sade, M. Lukuc, J. Simons, and J. Wang, “Vehicle-to-vehicle communications: Readiness of v2v technology for application,” tech. rep., 2014.

[84] Cohda Wireless, *CohdaMobility MK5 Module Datasheet*.

[85] J. McGroarty, “Recurring and non-recurring congestion: Causes, impacts, and solutions,” 2010.

[86] E. Yeh, J. Choi, N. G. Prelcic, C. Bhat, and R. Heath, “Security in automotive radar and vehicular networks,” *Microwave Journal*, Upcoming.

[87] Q. Chen, T. Roth, T. Yuan, J. Breu, F. Kuhnt, M. Zöllner, M. Bogdanovic, C. Weiss, J. Hillenbrand, and A. Gern, “DSRC and radar object matching for cooperative driver assistance systems,” in *2015 IEEE Intelligent Vehicles Symposium (IV)*, pp. 1348–1354, IEEE, 2015.

[88] J. Andrews, H. Claussen, M. Dohler, S. Rangan, and M. C. Reed, “Femtocells: Past, present, and future,” *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 3, pp. 497–508, 2012.

[89] M. Bennis, M. Simsek, A. Czylwik, W. Saad, S. Valentin, and M. Debbah, “When cellular meets wifi in wireless small cell networks,” *IEEE Communications Magazine*, vol. 51, no. 6, pp. 44–50, 2013.

[90] F. Boccardi, R. Heath, A. Lozano, T. L. Marzetta, and P. Popovski, “Five disruptive technology directions for 5G,” *IEEE Communications Magazine*, vol. 52, no. 2, pp. 74–80, 2014.

[91] M. J. Murrian, C. W. Gonzalez, T. E. Humphreys, and T. D. Novlan, “A dense reference network for mass-market centimeter-accurate positioning,” in *2016 IEEE/ION Position, Location and Navigation Symposium (PLANS)*, pp. 243–254, IEEE, 2016.

[92] A. Shaik, R. Borgaonkar, N. Asokan, V. Niemi, and J.-P. Seifert, “Practical attacks against privacy and availability in 4g/LTE mobile communication systems,” *arXiv preprint arXiv:1510.07563*, 2015.