Evaluating the Dedicated Short-range Communication for Connected Vehicles against Network Security Attacks

Conference Paper · January 2020

DOI: 10.5220/0009355500002550

8 authors, including:

Tu Le
University of Virginia
9 PUBLICATIONS **11** CITATIONS
SEE PROFILE

Weizhao Jin
University of Virginia
2 PUBLICATIONS **0** CITATIONS
SEE PROFILE

Seunghan Ryu
University of Virginia
8 PUBLICATIONS **135** CITATIONS
SEE PROFILE

Tamjid Al Rahat
University of California, Los Angeles
6 PUBLICATIONS **12** CITATIONS
SEE PROFILE

Evaluating the Dedicated Short-range Communication for Connected Vehicles against Network Security Attacks

Tu Le, Ingy Elsayed-Aly, Weizhao Jin, Seunghan Ryu, Guy Verrier, Tamjid Al Rahat, B. Brian Park and Yuan Tian

School of Engineering and Applied Science, University of Virginia, Charlottesville, Virginia, U.S.A.

Keywords: Cybersecurity, Network, DSRC, Connected Vehicles, VANET.

Abstract: According to the National Highway Traffic Safety Administration, there are more than 5 million road crashes every year in the U.S. More than 90 people die in car crashes every day. Even though the number of people surviving crashes has increased significantly thanks to safety features, such as airbags and anti-lock brakes, many people experience permanent injuries. The U.S. Department of Transportation introduced connected vehicle technologies, which enables vehicles to "talk" to each other and exchange important data on the roads, with the goal of preventing crashes from happening in the first place. With the rapid development of autonomous driving technology, vehicles in the near future will be able to operate completely without human drivers, increasing the need of reliable connected vehicle technologies. Due to the safety-critical characteristics of autonomous vehicles, it is important to evaluate the technologies extensively prior to deployment to ensure the safety of drivers, passengers, and pedestrians. In this paper, we evaluate the safety of Dedicated Short-Range Communication (DSRC), which is a popular low-latency wireless communication technology specifically designed for connected vehicles. We present three real-world network security attacks and conduct experiments on real DSRC-supported modules. Our results show that DSRC is vulnerable to these dangerous attacks and such attacks can be easily implemented by adversaries without significant resources. Based on our evaluation, we also discuss potential countermeasures to better improve the security and safety of DSRC and connected vehicles.

1 INTRODUCTION

With utilization of cutting-edge technologies in transportation, communication, and control, roadways are becoming connected. The connections among vehicles and infrastructure enable the urban transportation system to play a vital role in addressing mobility and sustainability concerns. Those connections have been introduced as vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication. In addition, smart vehicle's features such as lane departure warning, obstacle avoidance, and autonomous driving support the role of the urban transportation system to improve its performance.

Autonomous driving contains five levels based on their degree of autonomy. Higher level of autonomous driving requires less human involvement (BMW, 2019; NHTSA, 2020). For example, level 5 represents fully autonomous without human controls (NHTSA, 2020). The automated driving system overcomes distractions of human drivers; however, communication security becomes more important. As drivers' control will decrease along with the level of autonomy, the automated driving system will heavily rely on communication system.

Dedicated Short-Range Communication (DSRC) has been adopted in smart vehicles as the most popular communication protocol. It is a low-latency wireless communication architecture for node-to-node communication among hardware-enabled vehicles and roadside equipment. DSRC includes Road Side Units (RSUs; roadside infrastructure) and On-Board Units (OBUs; travelling vehicles) with transceivers and transponders. DSRC over different radio spectrum bands is already being used in North America, Europe, and Japan for several applications such as electronic toll collection (Abboud et al., 2016).

It is expected that DSRC will be more widely used in the smart vehicles due to its growing popularity. However, it is important to carefully investigate the DSRC because one of the greatest security threats to future automotive systems is DSRC itself. Therefore, this paper studies the security of DSRC communication and seeks to determine how secure the protocol

Le, T., Elsayed-Aly, I., Jin, W., Ryu, S., Verrier, G., Al Rahat, T., Park, B. and Tian, Y.
Evaluating the Dedicated Short-range Communication for Connected Vehicles against Network Security Attacks.
DOI: 10.5220/0009355500370044
In *Proceedings of the 6th International Conference on Vehicle Technology and Intelligent Transport Systems (VEHITS 2020)*, pages 37-44
ISBN: 978-989-758-419-0

is against network security attacks in practice.

In this paper, our main contributions are summarized as follows:

- We present three potential security attacks targeting the V2V and V2I communications: communication jamming, man-in-the-middle forwarding, and false alert.
- We evaluate the robustness of the DSRC protocol for connected vehicles against these attacks.
- We introduce some countermeasures to better protect DSRC against these network security attacks.

The remainder of this paper is organized as follows. Section 2 describes our literature review of related research. Section 3 presents the threat model and the network security attacks we implement to evaluate the DSRC protocol. Section 4 reports our evaluation of the proposed attacks on DSRC-supported devices. Section 5 evaluates our approach, suggests possible countermeasures, and outlines some future research directions. Finally, Section 6 concludes this paper.

2 LITERATURE REVIEW

Throughout the transportation community, cybersecurity vulnerabilities are a key concern for connected vehicle (CV) applications. Bertini et al. (Bertini et al., 2016) presented a survey result regarding the perception of connected and automated vehicle systems by the Oregon Department of Transportation. Over a hundred respondents were asked for potentials and concerns about CV deployment in the survey. As a result, 79% of responses were concerned about cybersecurity risks where 50% of them inferred the system is too premature to be implemented yet. The paper concluded that CV applications may be beneficial given that safe communication is guaranteed. Kaur et al. (Kaur et al., 2016) described potential security attacks on CV technology and classified the attacks based on the impacts of their outcomes. They also provided a comprehensive view of security practices and theoretical risk assessment for the attacks.

With increasing interests in cybersecurity, researchers attempted to investigate an impact of cyber-attacks and communication errors through simulation platform. Bhavsar et al. (Bhavsar et al., 2017) investigated the risk of communication threat to the mixed traffic stream. The communication threat in this paper were identified through fault tree model for both vehicular component and infrastructure component. Risk analysis was conducted through simulation; however, the paper defined the threat as communication failure probability from reviewing the literature. Cui et al. (Cui et al., 2018) proposed a simulation platform for Cooperative Adaptive Cruise Control (CACC) vehicles. The platform improved the quality of simulation considering vehicle dynamics, communication uncertainty, quantifying crash severity and CACC stability, and so on. Cyber-attack in this paper was defined as randomly varying radar and GPS sensor errors. Through sensitivity analysis, the authors resulted GPS and radar sensor errors may create a collision when the errors happened to be the same direction (e.g., sensor error of positive or negative value) and GPS jamming is the most dangerous cyber-attack. Heijden et al. (van der Heijden et al., 2017) analyzed security attacks on CACC and their impacts using simulation, suggesting the necessity of mis-behavior detection along with resilient controllers with graceful degradation.

When it comes to urban traffic, cybersecurity plays an even more critical role in road safety since street intersections are where most vehicle collisions happen. Ernst and Michaels (Ernst and Michaels, 2017) studied the severity of cyber vulnerability on signalized intersections. They investigated possible threats to the traffic controller (e.g., changes on signal phase and timing). Traffic simulation was conducted to measure the increase in travel time along with the threat level. Feng et al. (Feng et al., 2018) investigated vulnerabilities of traffic control system under cyber-attacks based on falsified data. They assumed the attacker's goal is to maximize the system delay on actuated and adaptive signal intersections. One of the achievements was identifying the critical intersection with the highest potential for heavy congestions.

In order to improve the security but not to compromise the low-latency feature of DSRC, the US Department of Transportation (USDOT) introduced their Security Credential Management System (SCMS). The Security Credential Management System (SCMS) is a proof-of-concept (PoC) message security solution for vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication (USDOT, 2020b). This PoC uses a Public Key Infrastructure (PKI) approach that issues digital certificates to authorized system participants to facilitate trusted communication. This ensures the messages originate from a legitimate source and guarantees the integrity of the messages communicated. Amoozadeh et al. (Amoozadeh et al., 2015) analyzed security vulnerabilities of connected vehicles in the context of multiple attacks whose impact was observed through simulation using VENTOS. They presented various types of attacks including message falsification in which the adversary listens to the wireless communication between vehicles and manipulates the contents of the messages. However, due to the fact that the messages are modified by the adversary, the attack is subjected to integrity checks from defense mechanisms such as SCMS. Laurendeau et al. (Laurendeau and Barbeau, 2006) performed an analysis on DSRC/WAVE architecture and implied that DSRC is potentially vulnerable towards cyber-attacks such as replay attacks where the adversary intercepts and retransmits malicious messages. Recent work (Le et al., 2019) presented some attacks that adversaries can cost-effectively launch on DSRC. However, they did not conduct experiments to evaluate the attacks on the DSRC protocol. Motro et al. (Motro et al., 2016) evaluated the effectiveness of the DSRC-based V2V communication system in VANET simulation environment. Various DSRC characteristics including power settings, communication range, packet errors, sensor errors, and estimation inaccuracy were tested to detect collision on highway. Throughout the simulation, the authors concluded that the primary factor to be considered is communication range. The majority of communication failures were caused by the vehicle being out of the range for the power settings. The research provided a promising result that packet errors at a rate of up to 50% did not have a significant impact on collision detection. However, this research is based on a strong assumption that their network is secured.

State-of-the-art research studied the impacts of cyber-attacks on transportation performance; however, their arguments are based on measurements obtained through simulation platforms or probabilities from literatures. In this paper, all experiments are conducted with real On-Board Units (OBU) and a Road Side Unit (RSU). Three possible cyber-attack scenarios are presented and evaluated.

3 METHODOLOGY

DSRC is a wireless communication technology specifically designed for high data transmission among vehicles and infrastructures. DSRC defines several sets of messages and fields for each message which can be customized for V2X applications (USDOT, 2009). DSRC bandwidth vary by region. In the U.S., the Federal Communications Commission (FCC) allocated 75 MHz of spectrum in the 5.9 GHz band for DSRC (FCC, 2019). Japan reserved 760 MHz of spectrum in the 5.8 GHz band for intelligent transportation systems, in particular for DSRC (Tachikawa, 2003). The European Union assigned 30 MHz of spectrum at 5.875 – 5.905 GHz for safety-related applications and 20 MHz at 5.855 – 5.875 GHz for other applications (ACEA, 2018). DSRC aims at providing a low latency protocol for Vehicular Ad-Hoc Networks (VANETs) and V2X communication (Torabi and Ghahfarokhi, 2014). The main goals for the protocol are to be reliable, fast, and safe for both passengers and pedestrians. However, in this work, we show that the DSRC protocol design has not met the reliability and safety goals to be deployed in real-world use. This section describes our approach to evaluate the robustness of the DSRC protocol.

Threat Model. In our attack model, the adversary has access to a vehicle with an On-Board Unit (OBU) or to a Road Side Unit (RSU). It is reasonable to assume that the adversary can have his/her vehicles or devices with DSRC capabilities like a legitimate user and exploit the vulnerabilities to attack others. Basically, any user can act maliciously. The goal of the adversary is to jam the communication channels or target other OBUs/RSUs to spread false information among the vehicles, which will then lead to physical damage and/or prevent other vehicles from communicating as a form of Denial-of-Service (DOS) attack. The adversary may also position himself/herself to intercept communication and relaying it giving the impression that two units are in range. In this paper, we inspect three different types of attacks targeting communication layer as follows.

Communication Jamming. We explore how a malicious RSU can jam the communication between two OBUs (see Figure 1). In this scenario, the adversary aims to disrupt communications between the victims by decreasing the signal-to-noise ratio. This could have very serious implications in the case where one OBU is trying to transmit a safety critical message and the other OBU cannot receive it properly.

Man-In-The-Middle (MITM) Forwarding. We look into the case that a malicious RSU can trick two OBUs into thinking they are within range of each other by forwarding the messages (see Figure 2). This attack would be dangerous to transportation operations such as platooning, which uses distance as a safety measure.

False Alert. A malicious OBU that decides to spread false information is just as dangerous as a malicious RSU. In this case, the malicious OBU could cause traffic to reroute by sending messages announcing a collision alert (see Figure 3). The ability to control how traffic is rerouted is dangerous because the

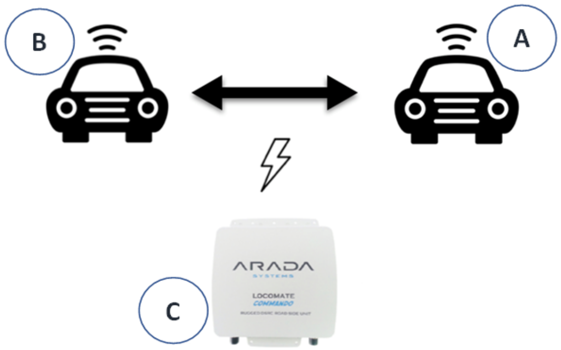


Figure 1: Communication Jamming Attack Scenario.

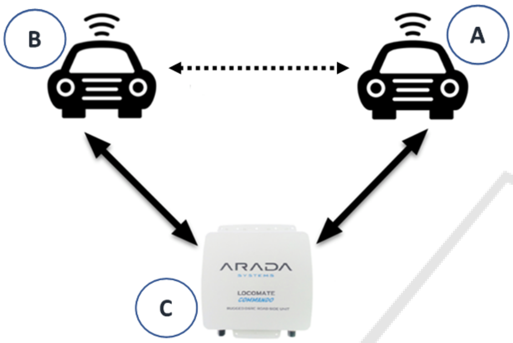


Figure 2: Man in the Middle Forwarding Attack Scenario.

victims could be rerouted through areas that are unsafe. It is important to note that this attack considers a malicious user sending messages instead of an attacker spoofing other users' messages. The original messages are not modified between source and destination, thus bypassing integrity checks of defense mechanisms such as the Security Credential Management System (SCMS) (USDOT, 2020b).

4 EVALUATION

In this section, we describe our evaluation of the proposed attacks on DSRC. We used LocoMate products made by Arada Systems, which was a leading automotive technology recently acquired by Lear Corporation (Lear, 2015). In order to experiment the proposed attacks, we use two LocoMate Mini 2 devices as the OBUs and a Locomate Classic device as an RSU. We control the RSU via Ethernet connection and control the OBUs via Bluetooth connection. Figure 4 shows an overview of our setup.

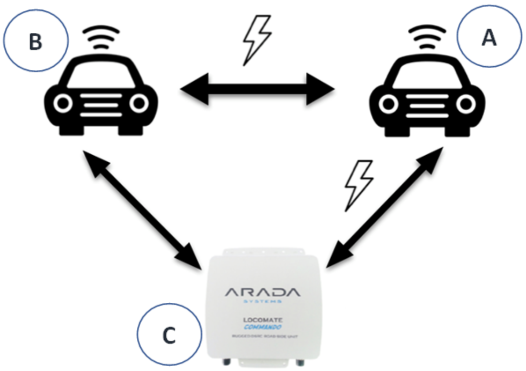


Figure 3: False Alert Attack Scenario.

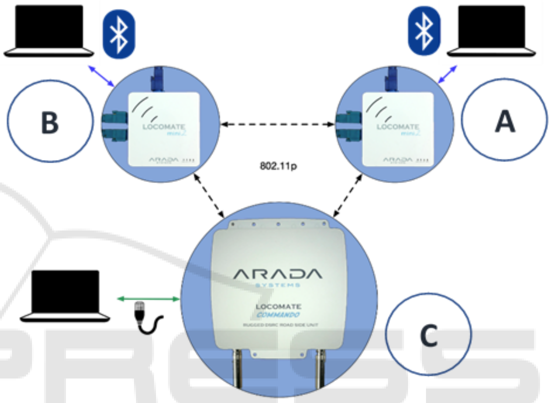


Figure 4: Experiment Setup to Evaluate Proposed Attacks on DSRC Protocol.

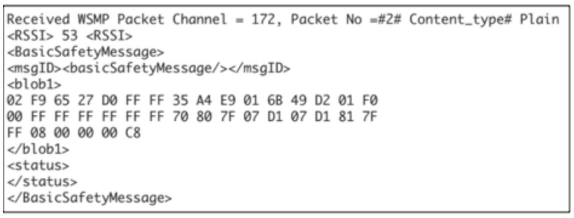
4.1 Communication Jamming

In this attack, the goal is to prevent messages sent by one OBU from reaching the other OBU (see Figure 1). The idea is that strategically placed malicious RSUs could create issues by flooding the communication channels (in our case the control channel).

We used the RSU as a jammer to try to block the messages going from the OBU A (Unit A) to the OBU B (Unit B). The two OBUs were placed within 2 meters from each other. At first, we attempted to manipulate the power of the transmissions in order to make the signal transmissions of the RSU much stronger than the others but that had no effect on the drop rate of the messages from Unit A to Unit B. Thus, we tried increasing significantly the number of messages being sent by the RSU in an amount of time. The default delay between each message was 100ms. We modified the RSU's transmission interval to 1ms, allowing it to transmit 100 times more messages in the same amount of time.

In our experiment, we also configured so that Unit A and Unit C are both sending Basic Safety Message

(BSM) but with different vehicle length information in order to differentiate them. More specifically, the messages being sent from Unit A to Unit B will include an additional byte C8 as shown in Figure 5.



```
Received WSMP Packet Channel = 172, Packet No =#2# Content_type# Plain
<RSSI> 53 <RSSI>
<BasicSafetyMessage>
<msgID><basicSafetyMessage/></msgID>
<blob1>
02 F9 65 27 D0 FF FF 35 A4 E9 01 6B 49 D2 01 F0
00 FF FF FF FF FF FF 70 80 7F 07 D1 07 D1 81 7F
FF 08 00 00 00 C8
</blob1>
<status>
</status>
</BasicSafetyMessage>
```

Figure 5: Basic Safety Message Sent by Unit a with the Additional Byte C8 in the End.

Before deploying the jamming attack (i.e., making the modification to the transmission interval), we calculated the message loss percentage (i.e., number of messages that are not received out of the total of sent messages) from Unit A to Unit B and found it to be 19%. We first found that the change in the transmission interval of the malicious RSU dramatically increased the message loss between OBU A and B to more than 50% when launching the attack (as can be seen in Table 1) indicating that the RSU (i.e., the jammer) can prevent a large proportion of the messages from reaching Unit B. We further observed the message reception rate of Unit B. The attack reduced the reception rate (from Unit A to B) by about a factor of 10 (10.4 msg/sec and 1.1 msg/sec respectively). In Table 2, we show the average number of messages per second that Unit B received from both message sources (i.e., from Unit A and the jammer) before and after launching the jamming attack.

4.2 Man In The Middle (MITM) Forwarding

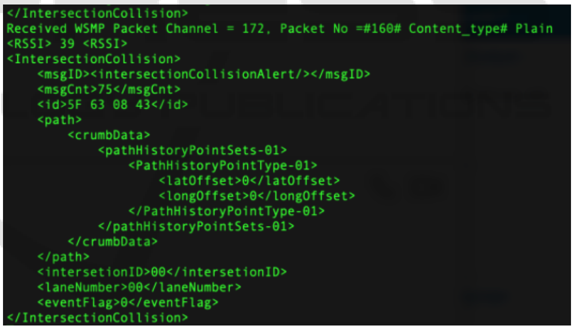
In this attack, the goal is to make two OBUs (Unit A and Unit B) believe that they are within range of each other and communicate through a malicious RSU (Unit C) which can eavesdrop on the messages, vehicle information and/or cause misinformation (see Figure 2).

We first measured the maximum range in which our two OBUs could communicate with each other. This range is estimated to be 20 feet without line of sight. For the experiment, we placed the two OBUs out of their range. We then used the RSU as the "middle man" to forward the messages from one OBU to the other. We found that the RSU was able to relay the messages and tamper with them as they were not encrypted or signed with security credentials. This attack shows that it is possible to interfere with vehicular applications such as platoon. In particular, this attack can lead to unexpected merging or changes in speed of the vehicles on the road, thus causing traffic chaos.

4.3 False Alert

In this attack, the attacker's goal is to exploit an OBU (unit A) to spread false information to the other OBU (Unit B) and the RSU (Unit C) (see Figure 3). The success of this attack means that a malicious OBU could reroute traffic or cause another vehicle brake unexpectedly.

We found that a malicious actor could send messages containing false information to other units and change the contents of the alerts and fields to arbitrary values. In Figure 6, we show an Intersection Collision Alert (ICA) message being received by the RSU (identical message received by the other OBU). Similar to the BSM shown in Figure 5, this message can be modified. There are also other types of messages used for critical alerts that can be sent. Those available message types that can be exploited for a false alert/information attack are: Intersection Collision Alert (ICA), Probe Vehicle Date (PVD), Basic Safety Message (BSM), and Road Side Alert (RSA).



```
</IntersectionCollision>
Received WSMP Packet Channel = 172, Packet No =#160# Content_type# Plain
<RSSI> 39 <RSSI>
<IntersectionCollision>
    <msgID><intersectionCollisionAlert/></msgID>
    <msgCnt>75</msgCnt>
    <id>5F 63 08 43</id>
    <path>
        <crumbData>
            <pathHistoryPointSets-01>
                <PathHistoryPointType-01>
                    <latOffset>0</latOffset>
                    <longOffset>0</longOffset>
                </PathHistoryPointType-01>
            </pathHistoryPointSets-01>
        </crumbData>
    </path>
    <intersetionID>00</intersetionID>
    <laneNumber>00</laneNumber>
    <eventFlag>0</eventFlag>
</IntersectionCollision>
```

Figure 6: Intersection Collision Alert Message.

Depending on the way the connected vehicles handle the reception of these alerts, the attack can be very effective or less effective. For example, it is reasonable to assume that when an ICA message is received, the vehicle would certainly brake to prevent the collision. Obviously, this critical message must be sent and received with the smallest latency possible (thus the possibility of sending it without registration to an application). Therefore, being able to manually send this type of message or modify it arbitrarily is dangerous. For example, someone who would like their route to be less congested could issue alerts to reroute the other vehicles to alternative routes resulting in unbalanced traffic and congestion. Although sensors attached to the vehicle (e.g., radar) may help with iden-

Table 1: Message Loss in Normal Operation and in Presence of Jamming Attack.

	Messages Sent by Unit A	Message Received by Unit B	Message Loss
Normal Operation	393	318	19.0%
Jamming Attack	193	106	54.4%

Table 2: Message Reception Rate of Unit B before and after Jamming.

Message Source	Unit B's Reception Rate (messages/second)	
	Before Jamming	After Jamming
From Unit A	10.40	1.10
From The Jammer	0	12.81

tifying false alerts, researchers have shown that sensors are vulnerable to spoofing attacks in which the adversary can easily manipulate outputs of the sensors (Fu and Xu, 2018).

5 DISCUSSION

We have shown that DSRC is vulnerable to the three network security attacks. In this section, we discuss some limitations of our work. We also describe potential defenses that can be adopted to enhance the security of DSRC. Finally, we outline some future research directions to extend our work.

5.1 Limitation

5.1.1 Scalability

The scalability of our attacks needs to be further researched. Our experiments were conducted using LocoMate devices (as described in Section 4). There can be other different manufacturers producing DSRC infrastructures and devices, which may introduce different variants of DSRC-supported hardware. Although these variants may vary in capabilities, we focus on evaluating DSRC rather than other capabilities. Besides, in our attack experiments, we use stationary hardware setup due to testing environment constraints. Hence, some attacks may produce different outcomes when it comes to real vehicles in motion. However, we believe that this does not undermine our overall findings and insights in this paper.

5.1.2 Security Credential Management System

Our proposed attacks reasonably assumed that SCMS was not in use because of the following reasons. First, SCMS is still a new technology under research and development. We tried to send an enrollment request to the USDOT. However, the access to enroll in the SCMS was limited to research deployment sites that receive funding from the USDOT (USDOT, 2020b). In addition, it is important to note that although security credentials issued by defense mechanisms such as SCMS may protect the authenticity and integrity of the messages, it can be difficult to defend against malicious users who possess several legitimate credentials and exploit their own credentials to launch attacks. In fact, assuming that units A, B, and C have valid credentials, all the aforementioned attacks are still possible. SCMS does not prevent users from changing message transfer rate, relaying messages, or sending messages that are not consistent with reality. Although, in the case of the MITM forwarding attack, SCMS might be able to prevent the malicious unit C from modifying the messages in between the source and the destination.

5.1.3 Testing on Real Vehicles

There are few vehicles actually equipped with DSRC. Many have hardware support for it but it is not necessarily supported by the car's manufacturer software yet. However, the USDOT has already equipped some trucks and infrastructure elements in order to test DSRC via pilot programs in Wyoming, Florida, and New York (USDOT, 2020a). Also, testing security attacks on a real vehicle in motion could be very dangerous if the vehicle has some of the basic responses to DSRC messages and alerts implemented (e.g., hard stop while in high speed motion due to a collision alert). For this reason, we decided to conduct our experiments with stationary hardware setup instead.

5.2 Potential Countermeasures

There are two solutions we suggest to prevent network congestion-based types of attack. The first would be to set a limit for the message transmission interval so that legitimate RSU and OBU devices cannot be exploited for spamming messages. The second solution is to monitor the network traffic to detect anomaly and prevent attackers from flooding the message queue. The limitation of this defense is that it may increase latency and it is not effective against distributed attacks which use a large number of exploited devices. In practice, both defense mechanisms should be combined to increase the coverage against different types of attack.

Integrity check in defense mechanisms such as the SCMS will be useful in providing a way of ensuring that the messages are not modified on the way; however, it will neither prevent the attacker from relaying the messages to an unexpected destination nor prevent the attacker from sending originally malicious messages. One solution to prevent the MITM forwarding attack is to measure the time it takes at maximum range to transmit a message. If the difference between the sent time and the received time is too great then that message should be marked as malicious item (i.e., distance bounding).

In order to prevent the false alert attack, anomaly detection is again a great method. Once malicious behaviors are detected, the adversary's credential must be suspended. As part of the system, all vehicles need to maintain a list of revoked credentials to avoid adversaries. However, there might be a tradeoff between security and user experience since the accuracy of the anomaly detection algorithm matters. It is important to have an accurate detection system to avoid losing too much user experience.

5.3 Future Work

5.3.1 DSRC Integrated with Visual Classification

Autonomous vehicles now are implemented with visual classification technology in the system to recognize road signs and traffic lights. Methods like deep neural networks (DNNs) are capable of doing that with the help of sensors such as camera and lidar. Visual classification based on DNNs has been proven to be vulnerable to adversarial machine learning examples, which would lead to dangerous attacks such as tricking a vehicle to mistake a stop sign as a speed limit sign. However, integrating data and the decisions based on DSRC and visual classification could help detect the adversaries and mitigate the threats. It would be much harder for the attacker to successfully spoof on both channels. Designing this type of integrated mechanisms and testing against attacks will be meaningful.

5.3.2 DSRC with Security Certificates Deployed

With security certificates implemented along with DSRC, our intuition is that the jamming and the false alert attacks can still be possible. However, after the incident happens, it might be easier to identify the culprit thanks to the certificates attached to the malicious messages. In the MITM forwarding attack the malicious actor will be able to forward the message, but not modify its content. In this case, the certificates will not prevent the incident but will be useful to trace the adversary after the attack happens. In the false alert attack, the attacker will still be able to create custom messages but will need to sign the message with a valid certificate.

5.3.3 Defense Evaluation

Our proposed defenses need to be further evaluated for each attack to validate their performance against the attack scenarios discussed in this paper. It is also important to evaluate the feasibility of our defenses, considering possible interference with other critical aspects of the protocol implementation such as latency.

5.3.4 Attack Implementation in Simulation

Simulation allows us to evaluate the attacks in a better controlled environment. In addition, we can compare the results between real hardware and simulation testing. A simulated environment also enables attack implementations without worrying about some physical limitations, for example, we had the constraints on power supply for the RSU when setting up the experiments. Moreover, a simulated environment may give us an opportunity to study the performance of the attacks without having to worry about hardware compatibility issues. Furthermore, a comprehensive simulator that enables modifications to the DSRC implementation may help us better evaluate our proposed countermeasures.

6 CONCLUSION

With the active growth of autonomous vehicles and the goal of improving automotive safety, a robust wireless communication technology used for connected vehicles is very important. Due to its safety-critical use case, this technology needs to be carefully evaluated and tested prior to deployment for real-world use. In this paper, we have shown that DSRC, which is a popular wireless communication technology designed for connected vehicles, is vulnerable to three network security attacks: jamming, MITM forwarding, and false alert. In the near future, connected and fully autonomous vehicles will soon replace traditional vehicles. As such, more attack surfaces will lead to more safety issues. Therefore, it is important to ensure that we have effective defense mechanisms in the first place.

REFERENCES

Abboud, K., Omar, H. A., and Zhuang, W. (2016). Interworking of dsrc and cellular network technologies for v2x communications: A survey. *IEEE transactions on vehicular technology*, 65(12):9457–9470.

ACEA (2018). Frequency bands for v2x. https://www.acea.be/uploads/publications/ACEA_position_paper-Frequency_bands_for_V2X.pdf.

Amoozadeh, M., Raghuramu, A., Chuah, C.-N., Ghosal, D., Zhang, H. M., Rowe, J., and Levitt, K. (2015). Security vulnerabilities of connected vehicle streams and their impact on cooperative driving. *IEEE Communications Magazine*, 53(6):126–132.

Bertini, R. L., Wang, H., Knudson, T., Carstens, K., and Rios, E. (2016). Assessing state department of transportation readiness for connected vehicle–cooperative systems deployment: Oregon case study. *Transportation Research Record*, 2559(1):24–34.

Bhavsar, P., Das, P., Paugh, M., Dey, K., and Chowdhury, M. (2017). Risk analysis of autonomous vehicles in mixed traffic streams. *Transportation Research Record*, 2625(1):51–61.

BMW (2019). The path to autonomous driving. https://www.bmw.com/en/automotive-life/autonomous-driving.html.

Cui, L., Hu, J., Park, B. B., and Bujanovic, P. (2018). Development of a simulation platform for safety impact analysis considering vehicle dynamics, sensor errors, and communication latencies: assessing cooperative adaptive cruise control under cyber attack. *Transportation research part C: emerging technologies*, 97:1–22.

Ernst, J. M. and Michaels, A. J. (2017). Framework for evaluating the severity of cybervulnerability of a traffic cabinet. *Transportation Research Record*, 2619(1):55–63.

FCC (2019). Dedicated short range communications (dsrc) service. https://www.fcc.gov/wireless/bureau-divisions/mobility-division/dedicated-short-range-communications-dsrc-service.

Feng, Y., Huang, S., Chen, Q. A., Liu, H. X., and Mao, Z. M. (2018). Vulnerability of traffic control system under cyber-attacks using falsified data. In *97th Annual Meeting of the Transportation Research Board*.

Fu, K. and Xu, W. (2018). Risks of trusting the physics of sensors. *Communications of the ACM*, 61(2):20–23.

Kaur, M., Martin, J., and Hu, H. (2016). Comprehensive view of security practices in vehicular networks. In *2016 International Conference on Connected Vehicles and Expo (ICCVE)*, pages 19–26.

Laurendeau, C. and Barbeau, M. (2006). Threats to security in dsrc/wave. In *International Conference on Ad-Hoc Networks and Wireless*, pages 266–279. Springer.

Le, T., ElSayed-Aly, I., Jin, W., Ryu, S., Verrier, G., Al Rahat, T., Park, B. B., and Tian, Y. (2019). Poster: Attack the dedicated short-range communication for connected vehicles. Poster presented at the 40th IEEE Symposium on Security and Privacy.

Lear (2015). Lear acquires arada systems, a leading automotive technology company that specializes in vehicle-to-vehicle and vehicle-to-infrastructure communications. https://www.lear.com/Press-Room/4279/lear-acquires-arada-systems-a-leading-automotive-technology-company-that-special.aspx.

Motro, M., Chu, A., Choi, J., Lavieri, P. S., Pinjari, A. R., Bhat, C. R., Ghosh, J., and Heath, R. W. (2016). Vehicular ad-hoc network simulations of overtaking maneuvers on two-lane rural highways. *Transportation Research Part C: Emerging Technologies*, 72:60–76.

NHTSA (2020). Automated vehicles for safety. https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety.

Tachikawa, K. (2003). Global standards on its radio communications. https://itsforum.gr.jp/Public/E4Meetings/P01/tachikawa5_5_3.pdf.

Torabi, N. and Ghahfarokhi, B. S. (2014). Implementation of the ieee 802.11 p/1609.4 dsrc/wave in ns-2. In *2014 4th International Conference on Computer and Knowledge Engineering (ICCKE)*, pages 519–524. IEEE.

USDOT (2009). Standard specification for dedicated short range communication (dsrc) physical layer using microwave in the 902-928 mhz band. https://www.standards.its.dot.gov/Factsheets/Factsheet/5.

USDOT (2020a). Connected vehicle pilot deployment program. https://www.its.dot.gov/pilots.

USDOT (2020b). Security credential management system. https://www.its.dot.gov/resources/scms.htm.

van der Heijden, R., Lukaseder, T., and Kargl, F. (2017). Analyzing attacks on cooperative adaptive cruise control (cacc). In *2017 IEEE Vehicular Networking Conference (VNC)*, pages 45–52. IEEE.