Poster: Attack the Dedicated Short-Range Communication for Connected Vehicles

Tu Le, Ingy ElSayed-Aly, Weizhao Jin, Seunghan Ryu, Guy Verrier, Tamjid Al Rahat, B. Brian Park, Yuan Tian
University of Virginia
{tnl6wk, ie3ne, wj6ef, sr5ae, gjv7qw, tr9wr, bp6v, yt2e}@virginia.edu

***Abstract*—In the near future, autonomous vehicles will be able to operate without human drivers, making them safety-critical systems. Connected vehicles will make use of wireless communication technology to exchange information about their surrounding environment with each other and roadside infrastructure. It is essential to study these systems extensively before deployment to ensure the security and safety of passengers and pedestrians. Dedicated Short-Range Communication (DSRC) is a popular low-latency protocol designed for wireless communication between connected vehicles and infrastructure (V2I), and among connected vehicles (V2V). In this work, we evaluate the robustness of the DSRC protocol by presenting three real-world attacks on the communication layer of DSRC-connected vehicles. Such attacks can be cost-effectively deployed by adversaries without significant resources. We also discuss appropriate countermeasures against these attacks.**

***Index Terms*—DSRC, connected vehicles, safety**

I. Introduction

With the proliferation of smarter vehicles, our roadways are becoming more and more connected. An increasing proportion of vehicles on the road include features such as lane departure warning, obstacle avoidance, autonomous driving, vehicle-to-vehicle (V2V) communication and vehicle-to-infrastructure (V2I) communication. V2V and V2I are new concepts indispensable for autonomous driving and have great potential to change human and cargo transport.

Researches have outlined 5 levels of autonomous driving; the higher the level, the less human involvement is needed [2], [3]. We are currently on the way towards achieving fully automated safety features by 2025 [2]. As V2V and autonomous driving technologies advance, the need for communication security will grow. As vehicles assume larger roles in driving mechanics and roadway navigation, the risks associated with abuse of and tampering with communication systems becomes greater still. At level 5 of automation, vehicles are expected to be fully autonomous and humans will only assume the role of passengers. Without driver control, automated driving systems will increasingly rely on communication systems to make critical decisions every step of the drive.

While still a nascent technology, connected vehicle technology is growing in popularity and use. Currently, one popular communication protocol being adopted in connected vehicles is Dedicated Short-Range Communication (DSRC). DSRC is a low-latency wireless communication architecture for node-to-node communication among hardware-enabled vehicles and roadside equipment. DSRC typically includes Road Side Units (RSUs - roadside infrastructures) and On-board Units (OBUs - travelling vehicles) with transceivers and transponders. DSRC over different radio bands is already being used in North America, Europe, and Japan for transportation applications such as electronic toll collection [5].

Due to growing popularity of DSRC, and increasingly automated vehicular systems for which it will be used, it is expected that one of the greatest security threats to future automotive systems is DSRC itself. In this work, we study the security of DSRC communication and seek to determine how secure the protocol is in practice.

II. Technical Approach

DSRC is a network protocol which runs on 5.9 GHz (varies by region) and defines several sets of messages and fields for each message which can be customized for V2X applications [1]. DSRC aims to provide a low latency protocol for Vehicular Ad-Hoc Networks (VANETs) and V2X communication [6]. The main goals for the protocol are reliability and safety for both passengers and pedestrians. However, in this work, we show that DSRC protocol design has resulted in reliability and safety inadequate for real-world use. This section describes our approach to evaluate the robustness of the DSRC protocol using two Arada Locomate Mini 2 as the OBUs and an Arada Locomate Classic as a RSU.

Threat Model. In our attack model, the attacker has access to a vehicle with an OBU or to an RSU. It is reasonable to assume that the attacker has a vehicle or device with DSRC capability like a normal user. Basically, any user can act maliciously. The goal of the attacker is to disrupt 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. Our attacker may also position himself/herself to intercept communication and relay between two victims giving the impression that two units are in range. We inspect three different types of attacks targeting communication layer as follows.

Communication Jamming. We explore how a malicious RSU can jam the communications between two OBUs (see Figure 1). This could have very serious implications in the case where one OBU is transmitting a safety critical message and the other OBU cannot receive it.

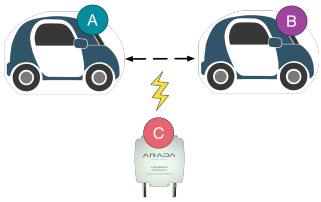

Fig. 1. Communication Jamming Attack Scenario

Man-in-the-middle (MITM) Forwarding. We look at how a malicious RSU can trick two OBUs into thinking they are in range by forwarding the messages (see Figure 2). This attack would be very dangerous to smart transportation systems such as platooning, which uses distance as a safety measure; as such, manipulating distance estimation could result in physical harm or loss of life.

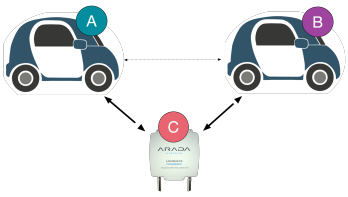

Fig. 2. Man-in-the-middle Forwarding Attack Scenario

False Alert. We show that a malicious OBU that decides to spread false information is as dangerous as a malicious RSU. In this case, the malicious OBU could cause traffic to reroute by sending messages announcing a collision (see Figure 3). The ability to control where traffic is rerouted can be dangerous for passengers when they are rerouted through areas that are less safe. 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) proof-of-concept [4].

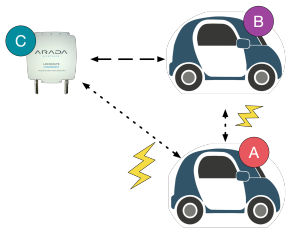

Fig. 3. False Alert Attack Scenario

III. Discussion

There are different types of messages used in DSRC such as Intersection Collision Alert (ICA), Probe Vehicle Date (PVD), Basic Safety Message (BSM), and Road Side Alert (RSA). If the communication protocol is not secure, these messages can be easily manipulated by adversaries to compromise the communications of connected vehicles.

To counter the first attack, there are two solutions we suggest to prevent these DOS-style attacks. The first is to set hardware constraints so that legitimate RSU and OBU devices cannot be exploited for this attack. The second method is to monitor network traffic to detect anomalies and prevent flooding of the queue. A primary limitation of this defense is that it can increase latency and does not prevent distributed attacks. Our recommendation is that both defense mechanisms are combined.

To prevent the second and third attacks, integrity checks in defense mechanisms such as the SCMS will be useful to provide a way of ensuring that the messages are not modified in transit; however, it will neither prevent the attacker from relaying the messages to an unexpected destination nor prevent the attacker from sending original malicious messages. Another method to prevent the second attack is to measure the time it takes to transmit a message at maximum range. If the difference between the sent time and the received time is too great then that message should be marked as malicious. This is called distance bounding. To prevent the third attack, a system needs to a way of detecting malicious behavior. Once the malicious behavior is detected, the sender of the malicious traffic should have their certificate suspended, mitigating the possibility of future attacks. Finally, all vehicles should maintain a list of revoked users in case a malicious user tries to contact them.

IV. Conclusion

Wireless communications of connected vehicles still have a lot of room for improvement before real-world deployment. In this work, we show that DSRC is vulnerable to three different communication layer attacks: jamming, MITM forwarding, and false alert. It is possible that there are other types of security attacks which can further break the protocol. With the rapid development of technology, connected and fully autonomous vehicles will soon replace the traditional vehicles. As such, more attack surfaces unfortunately lead to more types of attacks and the need for more effective defenses will inevitably be necessary to secure the roadways of the future.

References

[1] "Astm e2158-01 - 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, accessed: 2018-12-02.

[2] "Automated vehicles for safety," https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety, accessed: 2018-12-01.

[3] "The path to autonomous driving," https://www.bmw.com/en/automotive-life/autonomous-driving.html, accessed: 2018-12-01.

[4] "Security credential management system (scms)," https://www.its.dot.gov/resources/scms.htm, accessed: 2018-12-02.

[5] K. Abboud, H. A. Omar, and W. Zhuang, "Interworking of dsrc and cellular network technologies for v2x communications: A survey," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 12, pp. 9457–9470, Dec 2016.

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