Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

A survey on security attacks and defense techniques for connected and autonomous vehicles

Minh Pham[a,*], Kaiqi Xiong[b]

[a] Department of Computer Science and Engineering, University of South Florida, United States
[b] Intelligent Computer Networking and Security Laboratory, Florida Center for Cybersecurity, Department of Mathematics and Statistics, Department of Electrical Engineering, University of South Florida, United States

ARTICLE INFO

Article history:
Received 16 July 2020
Revised 23 February 2021
Accepted 4 March 2021
Available online 17 June 2021

Keywords:
Connected and autonomous vehicles
Intelligent transportation system
Cybersecurity
Traffic engineering

ABSTRACT

Autonomous Vehicle has been transforming intelligent transportation systems. As telecommunication technology improves, autonomous vehicles are getting connected to each other and to infrastructures, forming Connected and Autonomous Vehicles (CAVs). CAVs will help humans achieve safe, efficient, and autonomous transportation systems. However, CAVs will face significant security challenges because many of their components are vulnerable to attacks, and a successful attack on a CAV may have significant impacts on other CAVs and infrastructures due to their interconnectivity. In this paper, we conduct a survey on 189 papers from 2000 to 2020 to understand state-of-the-art CAV attacks and defense techniques. Of those 189 papers, 131 were directly concerned with attack models or defense strategies for CAVs. This survey first presents a comprehensive overview of security attacks and their corresponding countermeasures on CAVs. We then discuss the details of attack models based on the targeted CAV components of attacks, access requirements, and attack motives. Finally, we identify some current research challenges and trends from the perspectives of both academic research and industrial development. Based on our studies of academic literature and industrial publications, we have not found any strong connection between academic research and industry's implementation of CAV-related security issues. While efforts from CAV manufacturers to secure CAVs have been reported, there is no evidence to show that CAVs on the market can defend against some novel attack models that the research community has recently found. This survey may give researchers and engineers a better understanding of the current status and trend of CAV security for CAV's future improvement.

1. Introduction

Autonomous Vehicle (AV) has been a fascinating and impactful application of modern technology and it has been transforming human's intelligent transportation systems (Becker and Simon, 2000; Figueiredo et al., 2001). As telecommunication technology improves, the concept of Connected Vehicles (CVs), which is the idea to connect vehicles and to communicate with road infrastructures and the Internet, has been realized and often implemented together with AVs (Bansal and Kockelman, 2017; Uhlemann, 2015). Many research stud-

[*] Corresponding author.
E-mail addresses: minhpham@usf.edu (M. Pham), xiongk@usf.edu (K. Xiong).

https://doi.org/10.1016/j.cose.2021.102269

ies in academia and industry have advanced Connected and Autonomous Vehicles (CAVs), aiming toward a safe, driverless, and efficient transportation system. These advancements have led to prominent public demonstrations of CAVs in North America, Japan, and Europe (Benmimoun et al., 2009; van Nunen et al., 2012; Suzuki et al., 2010; Williams, 1988). There are various levels of CAV automation, ranging from non-automated to fully automated. In 2018, the Society of Automobile Engineers updated the official reference that specifically described the five levels of vehicle automation (SAE International, 2018). These five levels include Level 0-no automation, Level 1-driver assistance, Level 2-partial automation, Level 3-conditional automation, Level 4-high automation, and Level 5-full automation. In this paper, we consider automation levels 2, 3, 4, and 5, which are described by the official document (SAE International, 2018) that humans are not fully involved when the automated driving features are engaged (such as being hands-off).

A CAV consists of many sensing components such as laser, radar, camera, Global Positioning System (GPS), and light detection and ranging (LiDAR) (Wyglinski et al., 2013), as well as their connection mechanisms such as cellular connection, Bluetooth, IEEE 802.11p Wireless Access in Vehicular Environments (WAVE) (IEEE Standards Association, 2010), and Wi-Fi. The sensing components enable a CAV to navigate in an environment with unknown obstacles. Using data from these sensors, the surrounding environment and the vehicle's location are computed by a system in a process known as Simultaneous Localization and Mapping (SLAM) (Bailey and Durrant-Whyte, 2006; Durrant-Whyte and Bailey, 2006). Connection mechanisms improve the driving experience or enhance an autonomous driving system by providing advanced knowledge and a bigger picture of the environment. Applications that utilize connection mechanisms include Intelligent Driver-Assistance Systems (IDAS) (Pilipovic et al., 2014), safety features through Vehicle-to-Infrastructure communications (Bohm and Jonsson, 2008), and safety features through Vehicle-to-Vehicle communications (Biswas et al., 2006; Xu et al., 2004). While the sensing components and connection mechanisms have offered significant improvements in safety, cost, and fuel efficiency, they have also created more opportunities for cyberattacks.

Attempts to deploy and test CAVs have been carried out in many places, and they are supported by governments and corporations. In September 2016, the United States Department of Transportation started the Connected Vehicle Pilot Deployment Program (Gopalakrishna et al., 2015; Kitchener et al., 2017), providing over 45 million USD to Wyoming (2021), New York City (2021), and Tampa (2021) to begin building connected vehicle programs. In the United Kingdom, the Centre for Connected and Autonomous Vehicles has invested 120 million GBP to support over 70 CAVs projects, with a further 68 million GBP coming from industry contributions (Centre for Connected and Autonomous Vehicles, 2021). In China, industry officials estimated that by 2035, there will be around 8.6 million autonomous vehicles on the road, of which 5.2 million are semi-autonomous (SAE levels 3 and 4) and 3.4 million are fully autonomous (SAE level 5) (West, 2016). In Japan, prime minister Shinzo Abe claimed to grow a fleet of thousands of autonomous vehicles to serve in Tokyo Olympics 2020 (West, 2016). In South Korea, two competitions were sponsored by Hyundai Motor Group to stimulate the development of CAVs (Jo et al., 2015). These two competitions were held in 2010 and 2012, respectively. The development of CAVs is gaining significant public attention. The unfortunate side effect of this public attention is that CAVs will probably become attractive targets for cyberattacks.

Furthermore, CAV engineers and manufacturers need to have a systematic understanding of the cybersecurity implications of CAVs. Even though no significant cyberattack has occurred to the publicly deployed CAV programs, there are potential security threats to CAVs that have been discovered largely by the academic research community (Petit and Shladover, 2014). These potential security attacks will be more harmful than attacks on non-automated transportation systems because drivers may not be mentally or physically available to take over the driving, and engineers and technicians may not be available immediately to recover a compromised system.

Considerable research efforts have been carried out for identifying vulnerabilities in CAVs, recommending potential mitigation techniques, and highlighting the potential impacts of cyberattacks on CAVs and related infrastructures (Checkoway et al., 2011; Koscher et al., 2010; Petit et al., 2015; Yadav et al., 2016). Researchers have identified many vulnerabilities associated with sensors, electronic control units, and connection mechanisms. Some even demonstrated successful cyberattacks on CAVs and their components that are currently being sold and operated (Cao et al., 2019; Regulus Cyber LTD, 2020; Yan et al., 2016). Since detailed and security-focused studies for CAVs are fairly new in the literature (the majority of technical and in-depth papers discussed in this survey are published after 2011), there is an absence of a comprehensive survey paper that utilizes the current literature to build a taxonomy and to suggest significant gaps and challenges. For example, Miller and Valasek (2014) published a survey paper on attack surfaces but did not have much cover on defense strategies. Thing and Wu (2016) proposed a taxonomy of attacks and defenses but failed to point out specific examples in the literature with only 16 references (Thing and Wu, 2016). In this paper, we present a similar attack taxonomy to Thing and Wu's one, which is based on attack targets, access requirements, and attack motivation. However, we provide much more details on each class of the attack taxonomy and point out their specific references in the literature. On the other hand, our defense taxonomy differs significantly from Thing and Wu's one in that our taxonomy is based on the high-level ideas on defense techniques including anomaly-based intrusion detection, an abundance of information, and encryption methods, whereas Thing and Wu's one is based on the timing of the techniques including preventive, passive, and active. Some other survey papers are dedicated to specific components of CAVs (Haider and Khalid, 2016; van der Heijden et al., 2018; Tomlinson et al., 2018). To our knowledge, (Parkinson et al., 2017) is a state-of-the-art survey paper on this topic. Parkinson et al.'s paper reviewed 89 publicly accessible publications and identified knowledge gaps in the literature. However, we found that the authors missed interesting and important papers on some attack models and defense strategies, such as ones that we will cover in the GPS spoofing attacks (O'Hanlon et al., 2013;

Table 1 – A comparison of the survey papers on CAVs.

Survey paper	Year published	Reference count	Year of latest references	Focused topic	High-level taxonomy	Outline of open issues
Miller and Valasek (2014)	2014	12	2012	Security of CAVs	No	No
Thing and Wu (2016)	2016	16	2016	Security of CAVs	Yes	No
Haider and Khalid (2016)	2016	10	2015	Security of Global Positioning System	No	No
Parkinson et al. (2017)	2017	91	2016	Security of CAVs	No	Yes
Tomlinson et al. (2018)	2018	43	2018	Security of Controller Area Network	Yes	Yes
van der Heijden et al. (2018)	2018	126	2018	Misbehavior detection in communication between CAVs	No	Yes
This paper	2021	189	2020	Security of CAVs at component level	Yes, taxonomy is organized according to access requirements and attack motives	Yes

Yang and Xu, 2016) (Section 3.6), defense against LiDAR spoofing (Nouri et al., 2017; Wang et al., 2015) (Section 3.4), and adversarial input attack on cameras (Man et al., 2019; Sitawarin et al., 2018) (Section 3.7). Meanwhile, Parkinson et al. (2017) did not include any literature published after 2017. We tried our best to explore and present such technical papers, which are experimented not only on CAVs but also on related cyber-physical systems (e.g., unmanned aerial vehicles). Besides, our survey paper covers the recent developments of attacks and defenses on CAVs, including three ethical hacking studies on Tesla and Baidu autonomous vehicles in 2019. A comparison of the survey papers can be found in Table 1.

This survey paper makes the following contributions:

- This paper provides the foundation of knowledge on the topic of security for CAVs. We present a comprehensive view of vulnerable CAV components and their exploitation by attackers.
- This paper adopts the taxonomies of attack models and defense strategies. There are a wide variety of attack models on CAVs, but many of them share similarities in terms of attack motives and access requirements. Our taxonomy of attack models will be useful for developing defense strategies for a wide range of attack models that share some similarities in access requirements to launch attacks or attack motives.
- We summarize and discuss the state-of-the-art attack models and defense strategies for each CAV component. We have surveyed 189 papers from 2000 to 2020 about CAVs and CAV components, in which 131 papers are directly concerned with attack models and/or defense strategies. We present in chronological order the attack models and defense strategies for each CAV component and highlight those that are considered state-of-the-art. The technical details of each attack model and defense strategies are also summarized in Table 3.
- Finally, we outline the research trends, challenges, and open issues that would enhance the security of CAVs against recently reported attack models.

We aim to summarize the findings and conclusions from previous studies, provide the foundation of knowledge on this topic, highlight important contributions and findings in the field, and point out research gaps and trends. We do not try to prove or disprove previous studies nor to present new knowledge. We hope that our work can inform current and aspiring researchers and engineers of the security issues of CAVs as well as state-of-the-art defense and mitigation techniques. We further hope that our work can motivate other researchers to address cybersecurity challenges facing the development of CAVs. We acknowledge that research in this area is growing at a rapid rate and that some achievements from academia and industry might have been overlooked or not yet published. As a result, we observe that many vulnerabilities do not have enough tested solutions. Given the vast investment and rapid changes in the CAV industry, many individuals and corporations may not agree with our observations in this article, but

Table 2 – Classification of CAV attack models.

Sub-section in Section 3	Targeted CAV component	Access requirement	Attack motives
Malicious OBD Devices (Section 3.1)	OBD	Physical	Interrupting operations, Gaining Control over CAVs, Stealing Information
CAN Attacks through OBD (Section 3.2)	CAN	Physical	Interrupting operations, Gaining Control over CAVs, Stealing Information
CAN Attacks through Telematics ECUs (Section 3.2)	CAN	Remote	Interrupting operations, Gaining Control over CAVs, Stealing Information
ECU Attacks through CAN (Section 3.3)	ECU	Physical	Interrupting operations, Gaining Control over CAVs, Stealing Information
Attacks on Telematics ECUs (Section 3.3)	ECU	Remote	Interrupting operations, Gaining Control over CAVs, Stealing Information
LiDAR Spoofing (Section 3.4)	LiDAR	Remote	Gaining Control over CAVs
LiDAR Jamming (Section 3.4)	LiDAR	Remote	Interrupting operations
Radar Spoofing (Section 3.5)	Radar	Remote	Gaining Control over CAVs
Radar Jamming (Section 3.5)	Radar	Remote	Interrupting operations
GPS Spoofing (Section 3.6)	GPS	Remote	Gaining Control over CAVs
GPS Jamming (Section 3.6)	GPS	Remote	Interrupting operations
Camera Blinding (Section 3.7)	Camera	Remote	Gaining Control over CAVs
Adversarial Images (Section 3.7)	Camera	Remote	Interrupting operations
Falsified Information on Network (Section 3.8)	Connection Mechanism	Remote	Interrupting operations
Network Denial of Service (Section 3.8)	Connection Mechanism	Remote	Gaining Control over CAVs

any debate and criticism would be welcomed and appreciated for the growth of the community.

Since CAVs not only have highly connected internal components but also are highly connected to their external environments via communication networks, in this survey paper, we focus on the majority of the attack models that can be performed at a distance from a CAV (from the roadside or from other vehicles), as well as the most easily targeted components including sensors, cameras, and communication mechanisms. Furthermore, the current trend in developing new defense strategies is to utilize machine learning and anomaly-based intrusion detection systems because of their low expense and lower modification requirements on CAVs' system. Moreover, a decentralized public key infrastructure will be very helpful to improve the authentication process on vehicle-to-vehicle and vehicle-to-infrastructure communications. One of the most important research challenges is to find countermeasures for recently developed attack models that could pose serious threats to CAVs.

The remainder of this paper is organized as follows. Section 2 describes the taxonomies of attack and defense according to the components of CAVs, where those components are also explained in detail. This section would provide readers a brief overview of the attack and defense techniques that appeared in the existing literature so that readers without technical experience can have a high-level understand-

Table 3 – Summary of the existing attack models and defense strategies with challenges.

Subsection	Attack model	Attack model strategies	Existing defense strategies	Challenges
3.1	Malicious OBD Devices	With physical access to OBD port, attackers can intercept data transfer, collect information, and transmit malicious data frame (Koscher et al., 2010; Miller and Valasek, 2013; Woo et al., 2014).	Fowler et al. (2017) proposed using hardware-in-the-loop (HIL) equipment to collect and simulate data on attacks through an OBD port.	It is difficult to distinguish legitimate from malicious OBD devices.
3.2	CAN Attacks through OBD	Through access from OBD port, attackers can observe CAN message, replay messages, and transmit messages (Lin and Sangiovanni-Vincentelli, 2012; Matsumoto et al., 2012).	Ensure authenticity and confidentiality of CAN messages (Cho and Shin, 2016; Gmiden et al., 2016; Halabi and Artail, 2018; Nilsson et al., 2008c; Shin and Cho, 2017; Siddiqui et al., 2017; Tomlinson et al., 2018; Van Herrewege et al., 2011; Wolf et al., 2006).	There are criticisms to most defense strategies and CAN standards may carry legacy and may not have the capacity to accommodate the computing demand.
	CAN Attacks through Telematics ECUs	Some ECUs could be compromised through their connection mechanisms such as Bluetooth and cellular networking (Matsumoto et al., 2012; Miller and Valasek, 2013).	IDS-based approaches may be able to detect abnormal messages from the compromised ECUs (Mulliner and Michéle, 2012; Müter and Asaj, 2011; Tyree et al., 2018).	It is still unclear how effective these approaches will be and how difficult they are to be implemented.
3.3	ECU Attacks through CAN	Attackers compromise ECUs through their access to CAN (Chattopadhyay and Lam, 2017; Checkoway et al., 2011; Jungk and Bhasin, 2017; Mahmud et al., 2005; Nilsson and Larson, 2008; Nilsson et al., 2008a; 2008c).	To secure OBD port and CAN messages.	Difficulty in securing OBD port and CAN messages.
	Attacks on Telematics ECUs	Attackers compromise telematics ECUs through their connection mechanisms (Chattopadhyay and Lam, 2017; Checkoway et al., 2011; Jungk and Bhasin, 2017; Mulliner and Michéle, 2012; Nilsson et al., 2008a).	Robust firmware update protocols for ECUs are necessary (Checkoway et al., 2011; Seshadri et al., 2006).	A study to validate these defense frameworks in a realistic CAV environment is needed.
3.4	LiDAR Spoofing	Attackers create counterfeit signals that represent an object and inject the counterfeit signals into a LiDAR sensor (Cao et al., 2019; Petit and Shladover, 2014; Shin et al., 2017).	Defense strategies include using multiple sensors having overlapping views, reducing the signal-receiving angle, transmitting pulses in random directions, and randomizing the pulses' waveforms (Cao et al., 2019; Davidson et al., 2016; Matsumura et al., 2018; Pace, 2009; Shin et al., 2017).	Cao's attack model (Cao et al., 2019) may be considered state-of-the-art for its newness and effectiveness. Defense strategies need to be tested against this attack model.
	LiDAR Jamming	Attackers send light beams with the same wavelength but with higher intensity and effectively preventing the sensor from acquiring the legitimate light wave (Stottelaar, 2015).	Defense strategies include changeing the wavelength frequently, using multiple sensors, and shortening the ping period (Stottelaar, 2015). Wang et al. (2015) proposed pseudo-random modulation (PMQSL) quantum secured LiDAR (Wang et al., 2015).	These defense strategies need to be tested because they were not specifically developed for CAVs.

(continued on next page)

Table 3 (*continued*)

3.5	Radar Spoofing	Attackers replicate and rebroadcast radar signals to inject distorted data to the sensor. Chauhan (2014); Roome (1990); Yan et al. (2016).	Various approaches have been proposed (Dutta et al., 2017; Kapoor et al., 2018; Shoukry et al., 2015). The main ideas are using challenging signals and detecting abnormalities.	Kapoor et al.'s defense method (Kapoor et al., 2018) is the state-of-the-art technique. These defense techniques still need to be validated.
	Radar Jamming	Attackers modify frequency and amplitude of the stored signals before rebroadcasting to the radar sensors so that radar sensors fail to detect objects (Buehler et al., 2014; Lothes et al., 1990; Stott, 1994).	Defense strategies are widely studied for UAVs (Greco et al., 2005; 2008; Lu et al., 2010; Nouri et al., 2017), but none has been discussed for CAVs. The main idea is to separate the legitimate signals from the counterfeit signals.	These defense techniques were proposed for UAVs and thus need to be validated on CAVs.
3.6	GPS Spoofing	An attacker broadcasts incorrect, but realistic GPS signals to mislead GPS receivers on CAVs (El-Sheimy et al., 2006; Krasner, 2000; Meng et al., 2019a; Narain et al., 2019; Petovello et al., 2001; Psiaki et al., 2014; Shepard et al., 2012; Tippenhauer et al., 2011; Zeng et al., 2018).	Defense strategies include monitoring GPS signal strength, monitoring satellite signals, and checking time intervals from signals (Blanch et al., 2012; Brown, 1996; Choi et al., 2011; Hewitson and Wang, 2006; Loh and Fernow, 1994; Meng et al., 2019a; Narain et al., 2019; Qian et al., 2019; Van Dyke, 1992; Warner and Johnston, 2003; Yang and Xu, 2016).	Even though several countermeasures have been proposed in the literature, their effectiveness against newer attack strategies, such as (Meng et al., 2019a; Narain et al., 2019), is unknown.
	GPS Jamming	Attackers broadcast strong signals that overwhelm GPS receiver, so that the legitimate signals can not be detected (Coffed, 2014; Helfrick, 2014; Hu and Wei, 2009).	To calculate the probability of intentional GPS jamming attack just by using information from GPS receivers (Coffed, 2014; Hunkeler et al., 2012; Mukhopadhyay et al., 2007; Pattinson et al., 2017; Purwar et al., 2016; Sun and Amin, 2005; Zhang and Amin, 2012).	The state-of-the-art countermeasure was published by Purwar et al. (2016), but it requires modification to the GPS satellites and is only effective if the jamming signals are not too strong.
3.7	Camera Blinding	Cameras may be blinded by a quick burst of extra light (Petit et al., 2015; Yan et al., 2016).	To install extra cameras or to integrate a removable near-infrared-cut filter into a camera (Petit et al., 2015), or to predict the future frames (Sharath Yadav and Ansari, 2020).	DH and Ansari's solution (Sharath Yadav and Ansari, 2020) has the potential to be a generalized solution and may be implemented easily, but needs further validations due to its newness.
	Adversarial Images	Adversaries make small perturbations on the images that cameras observe and cause the AI algorithms to generate incorrect predictions (Brown et al., 2018; Eykholt et al., 2018; Goodfellow et al., 2014; Kelarestaghi et al., 2019; Kos et al., 2018; Lu et al., 2017; Moosavi-Dezfooli et al., 2017; Sitawarin et al., 2018).	To train machine learning models to be more resistant to adversarial images (Dziugaite et al., 2016; Guo et al., 2017; Jiang et al., 2020; Miyato et al., 2015; Nicolae et al., 2018; Szegedy et al., 2013; Xu et al., 2017; Zantedeschi et al., 2017), or to detect abnormal inputs (Buckman et al., 2018).	A validation and comparison study is needed for these defense techniques.
3.8	Falsified Information on Network	Attackers send falsified information through the V2V and V2I communications to disrupt CAVs' operation and traffic flow Amoozadeh et al. (2015); Chim et al. (2009); Rawat et al. (2012).	Use secured authentication schemes for the networks (Alimohammadi and Pouyan, 2015; 2015; Chim et al., 2009; Grover et al., 2011; Whyte et al., 2013; 2013; Zhao et al., 2020)	Strong authentication methods that are based on public-key encryption would require expensive public key infrastructures.

(*continued on next page*)

Table 3 (*continued*)

	Network Denial of Service	Attackers perform Denial-of-Service (DoS) attack and Distributed Denial-of-Service (DDoS) attack on the communication mechanisms (Blum and Eskandarian, 2006; Douligeris and Mitrokotsa, 2004; Ekedebe et al., 2015; Hasbullah et al., 2010; Leinmuller et al., 2006; Pathre, 2013; Pathre et al., 2013).	Various techniques include intrusion prevention, intrusion detection, intrusion response, and intrusion tolerance (Blum and Eskandarian, 2006; Douligeris and Mitrokotsa, 2004; Hubaux et al., 2004; Plossl et al., 2006; Singh et al., 2018).	Defending against DoS and DDoS attacks on V2I and V2V network requires a secured V2I or V2V network architecture and protocols (Blum and Eskandarian, 2006; Douligeris and Mitrokotsa, 2004; Plossl et al., 2006).

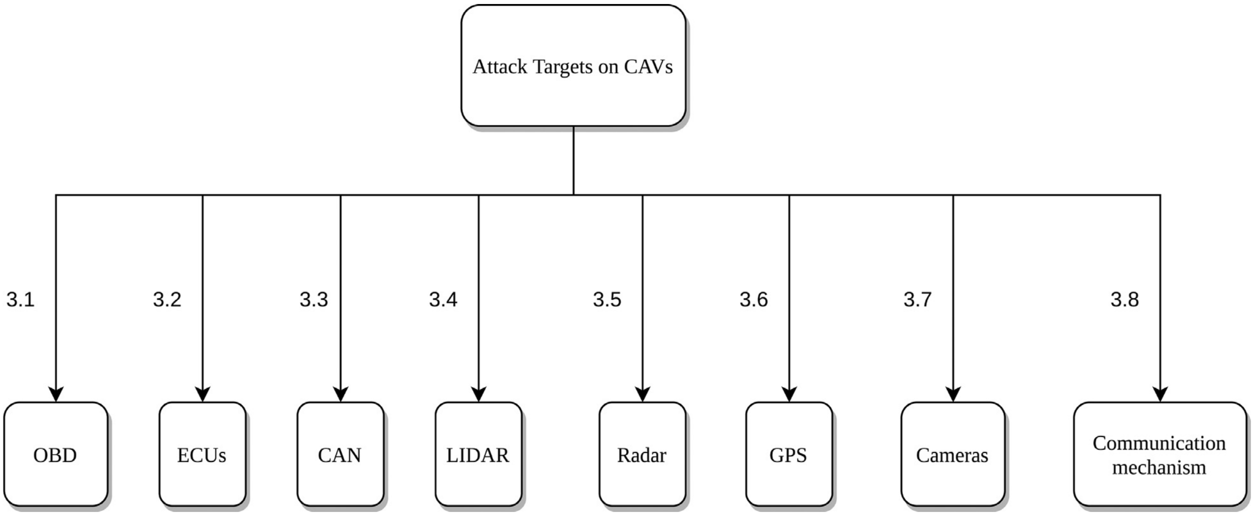

Fig. 1 – Possible attack targets on CAVs.

ing of those attacks and defenses. Section 3 discusses the attack techniques, their corresponding mitigation/defense techniques, and the challenges in defense and the gaps between attack models and defense techniques. In Section 4, we identify the trends, challenges, and open issues in academic research and industry developments.

2. Taxonomy of attacks and defenses

The purpose of this section is to provide a high-level overview of the types of attacks and defenses that have been discussed for CAVs. In this section, we attempt to classify attack models and defense strategies based on their characteristics but do not provide technical details. Instead, technical details of attack models and defense strategies with their corresponding references are presented in Section 3. Figs. 3 and 4, which are presented in Section 2 to point readers to related parts in Section 3, may help readers navigate easily between the two sections.

2.1. *Taxonomy of attacks*

In this section, we discuss the CAV components whose vulnerabilities have been found in the literature and provide a high-level overview of the attack models.

2.1.1. *Attack targets*

As discussed in Section 1, a good CAV system consists of many sensor components and connection mechanisms. They work together and contribute to CAVs' functioning. Compromising or tampering with any of these components may destabilize a CAV and serve the attacker's goal, such as stealing information and causing property damage and bodily injury. In this subsection, we describe CAV components that have been targeted by cyber attackers in the literature. Some attack models have been demonstrated as realistic threats while the others have only been discussed theoretically. While Section 2 presents the classification of attacks and defense, Section 3 gives a detailed discussion of attack models and defense strategies with their citations. Fig. 1 summarizes the attack targets along with their corresponding subsections in Section 3, where readers can find detailed discussions of the attack models and the mitigation techniques along with their references.

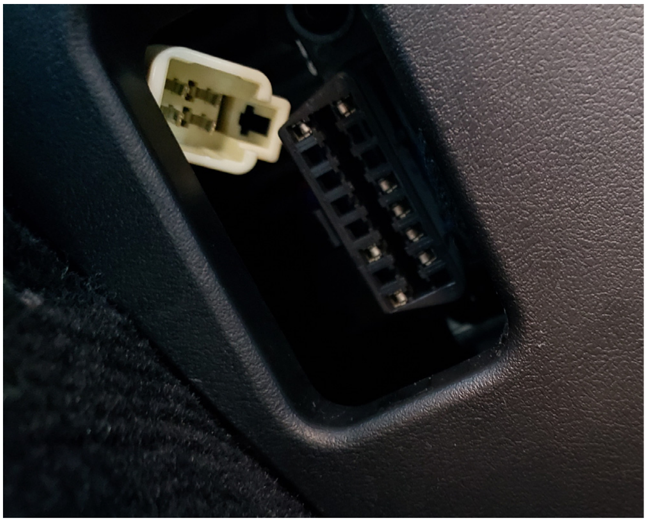

Fig. 2 – OBD port on Tesla Model X.

On-board diagnostic port (OBD) is a connection port that anyone can use to collect information about a vehicle's emissions, mileage, speed, and data on a vehicle's components. There are two OBD standards, namely OBD-I and OBD-II. OBD-I was introduced in 1987 but had many flaws, so it was replaced by OBD-II introduced in 1996 (Kalmeshwar and Prasad, 2017). OBD-II port should be found in almost any modern vehicle, and CAVs are not exceptions. Fig. 2 shows the OBD port on a Tesla Model X (SAE level 2). Modern OBD ports can provide real-time data (Lin et al., 2005). OBD also provides a pathway to acquire data from CAV's Electronic Control Units and possibly to modify the software embedded in those control units. Many manufacturers also use OBD ports to perform firmware updates (Checkoway et al., 2011). Attack models on OBD ports and their corresponding mitigation techniques are discussed in Section 3.1.

Electronic control units (ECUs) are embedded electronic systems that control other subsystems in a vehicle. All modern vehicles use ECUs to control vehicular functionalities by acquiring electronic signals from other components, as well as processing and sending control signals. Some important ECUs are the Brake Control Module, Engine Control Module, Tire-pressure Monitor Systems, and Inertial Measurement Units. Their functionalities are as follows. The Brake Control Module collects data from wheel-speed sensors and the brake system, as well as processes the data to determine whether or not to release braking pressure in real-time (Kassakian et al., 1996). The Engine Control Module controls fuel, air, and spark, as well as collects data from many sensors around the vehicle to ensure that all components are within a normal operating range (Kassakian et al., 1996). The Tire-pressure Monitor Systems collect data from sensors within tires and determine if the tire pressures are at ideal levels. The United States has legally required all vehicles to be equipped with Tire-pressure Monitor Systems since 2007 (Singh et al., 2009), and the European Union issued the same regulation in 2012 (European Parliament, 2009). The Inertial Measurement Units collect data from accelerometers, magnetometers, and gyroscopes and calculate the vehicle's velocity, acceleration, angular rate, and orientation. These calculations are pivotal for CAVs because they serve as inputs for running a safe automated driving system (Jitpakdee and Maneewarn, 2008). For example, a change in road gradient would change a CAV's angular rate and orientation, and the automated driving system may issue an adjustment in a vehicle's speed to maintain safe operations. CAVs involve a larger number of ECUs than a non-automated vehicle (SAE level 2 and below) because they possess many more sensors and require many more calculations to make autonomous decisions in driving. Readers may think of ECUs in CAVs as mini-computers, each carries out a specific role and collaborates with others to perform autonomous driving. It is common to see complex collaborations between ECUs (Koscher et al., 2010). Attack models and defense strategies on ECUs are discussed in Section 3.1. Communications between ECUs happen on Controller Area Networks, which will be discussed as follows.

Controller area network (CAN). ECUs are typically connected through a CAN. In a vehicle, the CAN is a central network to connect ECUs so that they can communicate with each other. A CAN bus is typically structured as a two-wire and half-duplex network system that can support high-speed communication (Corrigan, 2002). The greatest benefits of CANs are the low amount of wiring and the ingenious prevention of message loss and message collision (Corrigan, 2002). In CAVs, network packets are transmitted to all the nodes in the CAV network, and the packets do not contain an authentication field or source identification field (Thing and Wu, 2016). Therefore, a compromised node can collect all data being transferred through the network and broadcast malicious data to other nodes, making the entire CAN vulnerable to cyberattacks. Attack models and defense strategies on CANs are discussed in Section 3.2.

Sensors. The following sensors are crucial to CAVs and are often found in most CAVs. All of the sensors discussed below will have their vulnerabilities discussed in Section 3.

- **Light Detection And Ranging (LiDAR)** are sensors that use light to measure the distance to surrounding objects. LiDAR sensors operate by sending light waves to probe the surrounding environment and make measurements based on reflected signals (Wandinger, 2005). The light beam's wavelength varies to suit the purpose and ranges from 10 micrometers (infrared light) to approximately 250 nanometers (ultraviolet light) (Wandinger, 2005). In CAVs, LiDAR is often used for obstacle detection to navigate safely through environments and is often implemented by rotating laser beams (Hecht, 2018). Data from LiDAR can be used by software embedded in ECUs to determine whether there are obstacles in the environment, as well as by autonomous emergency braking systems (Hulshof et al., 2013). Attacks and defense techniques on LiDAR are described in Section 3.4.
- **Radio Detection and Ranging (Radar)** are sensors that send out electromagnetic waves in the radio or microwave domain to detect objects and measure their distance and speed by sensing the reflected signals. In CAVs, radars are useful in many applications. For example, short-range radars enable blind-spot monitoring

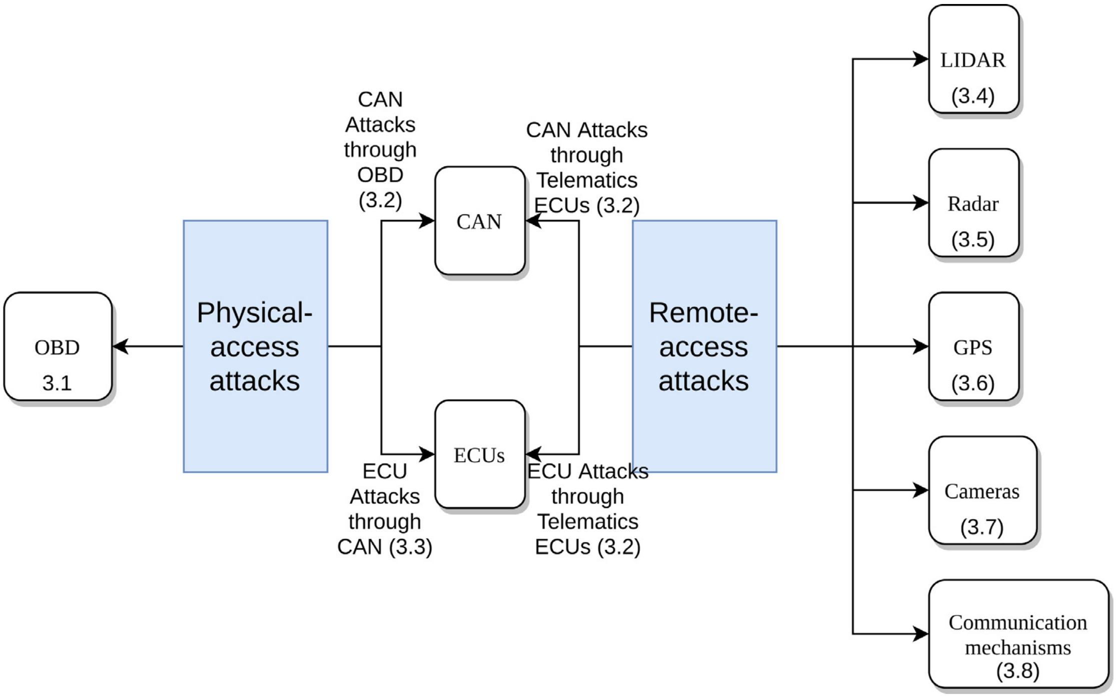
OBD
3.1
Physical-access attacks
CAN Attacks through OBD (3.2)
CAN
ECU Attacks through CAN (3.3)
ECUs
CAN Attacks through Telematics ECUs (3.2)
ECU Attacks through Telematics ECUs (3.2)
Remote-access attacks
LIDAR (3.4)
Radar (3.5)
GPS (3.6)
Cameras (3.7)
Communication mechanisms (3.8)

Fig. 3 – Access requirements to attack some CAV components.

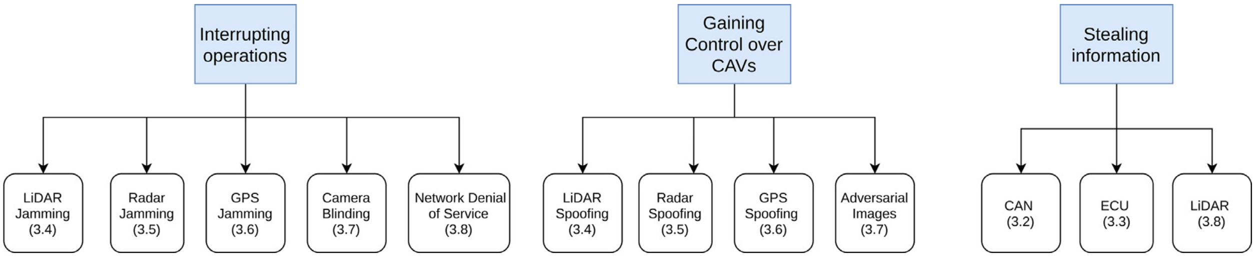

Fig. 4 – Attack motives.

(Uselmann and Uselmann, 2004), lane-keeping assistance (Ishida and Gayko, 2004), and parking aids (Reed, 2003). Long-range radars assist in automatic distance control (Chi, 1992) and brake assistance (Breuer et al., 2007). Attacks and defense techniques on radars are described in Section 3.5.

- **Global Positioning System (GPS)** is a satellite-based navigation system that is funded and owned by the United States government, is operated and maintained by the United States Air Force (William J. Hughes Technical Center, 2014). It is a global navigation system that operates based on the satellites in the Earth's orbit that transmit high-frequency radio signals. The radio signals may be sensed by many devices such as smartphones and GPS receivers in CAVs. When GPS receivers find signals from three or more satellites, they can compute their locations. Since finding a route between two locations is necessary for autonomous driving, GPS signals are critical to CAVs. GPS receivers can operate without any communication channel such as wireless networks, but data from wireless networks can often enhance GPS receivers' accuracy (Twitchell and Taylor, 2001). Since GPS signals do not contain any data that can directly authenticate the source of signals, GPS receivers are vulnerable to jamming and spoofing attacks. These attacks and mitigation techniques are described in section3.6.
- **Cameras (image sensors)** are widely applied in CAVs. Autonomous and semi-autonomous vehicles (SAE level 2 and above) rely on cameras placed in many positions to acquire a 360-degree view around the vehicle. Cameras provide information for important autonomous tasks such as traffic sign recognition (Fairfield and Urmson, 2011; Levinson et al., 2011; Omachi and Omachi, 2009) and lane detection (Hillel et al., 2014; Sun et al., 2013). Cameras can also be used to replace LiDAR for the task of object detection and for measuring distance at a lower cost, but they have poor performance under specific situations such as rain, fog, or snow (Wang et al., 2019). Together with LiDAR and radars, cameras provide abundant and diverse data for autonomous driving. Attack models on cameras and mitigation techniques are described in Section 3.7.

Connection mechanisms in CAVs can be divided into vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) networking. V2V communications help exchange data between nearby vehicles and can quickly provide additional information to the data already collected by a CAV regarding its surrounding environment. This additional data can lead to safer and more efficient autonomous driving. V2I communications help exchange data between CAVs and road infrastructures, which provide data about the bigger picture of the transportation system, such as smart traffic signs (without the need to do image recognition) and safety warnings in a large region (Chang et al., 2015). Joy and Gerla (2017) described several important applications that leverage V2I communication, such as safe and efficient routing, crash prevention, platoon stability, and sensor data gathering. Joy and Gerla also proposed the Haystack Privacy mechanism for strengthening privacy and maintaining accuracy in a V2I network with a large number of participants. V2V communications often follow the Vehicular Ad-hoc NETworks (VANET) paradigm, where each vehicle acts as a network node and can independently interact with other nodes through a wireless connection (Watfa, 2010). The wireless connections used are often dedicated short-range communications (DSRC) and cellular networks (Abboud et al., 2016). A well-known example of DSRC is the IEEE 802.11p Wireless Access in Vehicular Environments (WAVE) (Baccelli et al., 2010; IEEE Standards Association, 2010). WAVE is described in detail by Kenney (2011). V2I communications are often achieved by using cellular networks, where Long-Term Evolution (LTE) is the current standard (Abboud et al., 2016). Attack models on V2V and V2I networks and defense techniques are discussed in Section 3.8.

2.1.2. *Classifications of attack models*

We can categorize the attack models, described in detail in Section 3, by their access requirements and by their motives.

Access requirement: attack models can be performed remotely (remote-access attacks) or can only be performed with physical access to CAV components (physical-access attacks).

- **Remote-access attacks:** Attackers do not need to physically modify parts on CAVs or attach instruments to CAVs. Attacks can be launched from a distance, such as from another vehicle. This type of attack is a lot more common than physical-access attacks and is increasing in number due to the large amount of information transferred to and from CAVs. Any component on CAVs that communicate and interact with the surrounding environment is vulnerable to be exploited from distance. Three common patterns for remote-access attacks are sending counterfeit data, blocking signals, and collecting confidential data:
  - Sending counterfeit data aims to trick the CAV system in order to gain significant control over the system's behavior. Examples of sending counterfeit data are LiDAR spoofing (Section 3.4), radar spoofing (Section 3.5), GPS spoofing (Section 3.6), and adversarial image attacks (Section 3.7).
  - Attackers' blocking signals aims to prevent CAVs from receiving such information that ensures them to function properly. Examples of these attacks are LiDAR Jamming (Section 3.4), Radar Jamming (Section 3.5), GPS Jamming (Section 3.6), Camera Blinding (Section 3.7), and Network Denial of Service (Section 3.8).
  - Attackers may also aim to collect confidential data to serve further attacks. Several examples of such attacks are described in the Falsified Information attack model in Section 3.8.
- **Physical-access attacks:** Attackers need to physically modify components on CAVs or attach instruments to CAVs. Examples of these attacks are reprogramming ECU (Sections 3.1 and 3.2) and falsifying input data (Section 3.3). Physical-access attacks are more difficult to carry out because attackers may be detected when tampering with CAVs.

For easier navigation through this paper, a summary of access requirements to perform attacks on the aforementioned CAV components is presented in Fig. 3, annotated with the corresponding parts in Section 3 for more details. CAN and ECUs can be targets for both remote-access and physical-access attacks.

Attack motivations: Three common attack motivations are to interrupt (but without control) CAVs' operation, to control CAVs as attackers' wishes, or to steal information.

- **Interrupting operations:** attackers aim to corrupt CAV components that are important for autonomous driving, thus making the autonomous driving mode unavailable on CAVs. These attacks are analogous to Denial-of-Service attacks on networks. Examples can be found in Section 3.4-LiDAR Jamming, Section 3.5-Radar Jamming, Section 3.6-GPS Jamming, Section 3.7-Camera Blinding, and Section 3.8-Network Denial of Service.
- **Gaining control over CAVs:** attackers gain sufficient control over CAVs so that they can alter the vehicles' movements, such as changing the vehicle's route, forcing emergency brake, and changing vehicle speed. Examples of these attacks can be found in Section 3.4-LiDAR Spoofing, Section 3.5-Radar Spoofing, Section 3.6-GPS Spoofing, and Section 3.7-Adversarial Images.
- **Stealing information:** attackers' goal is to collect important and/or confidential information from CAVs. Collected information may be used for further attacks. Examples of this type of attack can be found in Sections 3.2, 3.3, and 3.8-Falsifying Information.

For easier navigation through this paper, a summary of attack motives is presented in Fig. 4, annotated with the corresponding parts in Section 3 for more details.

Finally, for each attack model described in Section 3, we show its targeted CAV component, access requirement, and attack motives in Table 2.

2.2. *Taxonomy of defenses*

In this section, we attempt to organize the defense techniques into categories that have certain patterns. Some defense categories are generally effective against certain types of attacks, but we suggest that readers study defense techniques for attacks on a case-by-case basis. For example, attacks that prevent sensors from receiving legitimate signals can usually be mitigated by the abundance of information, through planting multiple sensors or through acquiring additional information from V2V or v2I connections, but this does not hold for the case of GPS Jamming (Section 3.6).

The categories for defense techniques are as follows.

- **Anomaly-based Intrusion Detection System (IDS)** is a method that is designed to detect unauthorized access or counterfeit data. IDS methods generally look to detect abnormal data from the signals or side-channel information. For example, Cho and Shin (2016) proposed Clock-based IDS (CIDS), which measures the clock skew of ECUs (the phenomenon in which the clock signal arrives at different ECU at slightly different times) and uses this information to fingerprint the ECUs. The fingerprints are then used to detect intrusions by checking for any abnormal shifts in the clock skews. IDS methods are generally applicable in attack models that rely on sending counterfeit signals, such as CAN attacks (Section 3.2), LiDAR spoofing (Section 3.4), Radar Spoofing (Section 3.5), and GPS spoofing (Section 3.6). However, they are not effective to defend against Adversarial Images attacks on cameras (Section 3.7).
- **The abundance of information** can be achieved by getting information from other CAVs and infrastructures or by setting up abundant information within a CAV. This is good not only for defending against cyberattacks but also for increasing confidence in autonomous driving. This category of defense strategy is generally effective against Denial-of-Service types of attacks, such as LiDAR Jamming (Section 3.4), Radar Jamming (Section 3.5), and Camera Blinding (Section 3.7). For example, by using multiple LiDAR sensors with different wavelengths, a CAV is protected from attackers who send high-power light beams to blind LiDAR sensors. However, this method is not effective against GPS Jamming (Section 3.6). A major drawback of this defense category is that placing abundant components on CAVs is expensive.
- **Encryption methods** can be applied to defend against attacks that abuse components that lack authentication methods, such as CANs and signals for sensors. Many encryption methods have been published to secure CAN and sensor signals, such as those in Halabi and Artail (2018); Lin and Sangiovanni-Vincentelli (2012); Nilsson et al. (2008c); Van Herrewege et al. (2011) (they will be discussed in detail in Section 3). However, an encryption method is not applicable for GPS receivers because it is too expensive to modify the satellites so that they can send encrypted radio signals. This makes defending against GPS Jamming attacks a difficult task (Section 3.6).

Some defense techniques are unique and do not fall into any of these categories, which is why we suggest that readers study defense techniques on a case-by-case basis.

3. Existing attacks and their countermeasures

One compromised component of CAVs may allow attackers to compromise other components, other CAVs, and infrastructures, thus forming a sequence of attacks. From our reading of the literature, we have come up with possible attack sequences that attackers may perform and present them in Fig. 5. The attack sequences plotted in Fig. 5 are:

- Sequence with the label (1): Attackers gain physical access to OBD ports, which gives them access to CANs and subsequently access to ECUs.
- Sequence with the label (2): Attackers compromise LiDAR, radar, GPS, or cameras and send adversarial information to ECUs.
- Sequence with the label (3): Attackers compromise telematics ECUs (ones that have access to communication channels such as VANET, Bluetooth, and DSRC). Attackers can then send adversarial information through the CAN to other ECUs.
- Sequence with the label (4): Attackers can send adversarial information from their CAVs or CAVs that have been compromised.

The possibility that attackers may compromise one CAV component after another means that in order to enhance the security of CAVs, manufacturers should enhance the security of all CAV components.

Each of the following subsections describes attack model(s) for a specific CAV component. In each subsection, we describe the attack models, the security requirements for defense techniques against the attack models, existing defense techniques in the literature and whether they meet the security requirements, and challenges for defending against the attack models. Table 3 summarizes each subsection in this Section 3, which includes the summary of attack and defense strategies, challenges, and literature references.

3.1. *Attacks on OBD*

Attack model - malicious OBD devices The OBD port is an open gateway for many attacks to other CAV components because the port usually does not encrypt data or control access. Since the OBD port itself has no capability of remote connection, attackers would need physical access to the OBD port to perform these attacks. Some devices that are plugged into the OBD port can transfer data to a computer through wired or wireless connections. Some of these devices were made by car manufacturers for diagnostic purposes and firmware updates. Some examples of these devices are Honda's HDS, Toyota's TIS, Nissan's Consult 3, and Ford's VCM (Checkoway et al., 2011). Some other devices are developed by third-party companies to connect vehicles to smartphones (i.e. self-diagnostic purpose), such as Telia Sense (Uhlir et al., 2017) and AutoPi (Zamfir and Drosescu, 2019). Studies have been done to assess the feasibility of using these third-party devices to perform a meaningful attack. Marstorp and Lindström (2017) found that Telia Sense is a well-secured system whereas Christensen and Dannberg (2019) successfully performed a man-in-the-middle attack, where they intercepted data to and from the AutoPi Cloud interface. After gaining access to the OBD port, attackers can interrogate information about the CAV, controlling key components (such as warning light Ishtiaq Roufa et al., 2010, windows lift, airbag control system,

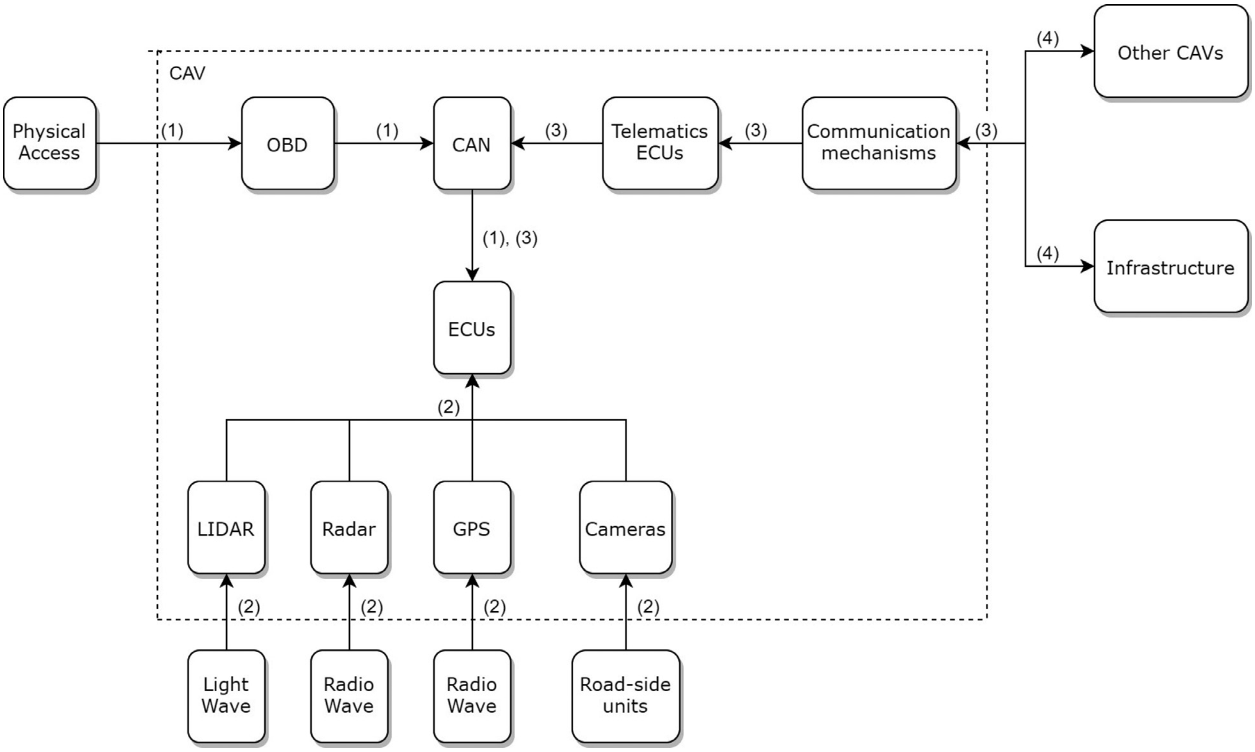

Fig. 5 – Possible attack sequences on the components of CAVs.

horn Koscher et al., 2010), and injecting codes to ECUs (Miller and Valasek, 2013). Koscher et al. (2010) successfully performed one such attack on a running vehicle by using a self-written program named CARSHARK to compromise many components on the vehicle. in Woo et al. (2014), it was shown that if attackers can trick drivers into downloading a malicious self-diagnostic application on their smartphones, attackers can transmit an ECU-controlling data frame through the OBD device to the vehicle's ECUs.

Criteria for defense strategies Defense may take place at the OBD level, or at CAN and ECUs level. Criteria for defense strategies at CAN and ECUs are discussed in their respective subsections (3.2 and 3.3). Here, we discuss the criteria for securing the OBD port. Based on our understanding of the attack model and study on the defense techniques, we suggest the following criteria.

- Authenticity of OBD devices: before being granted access to a CAV's data, OBD devices must come from a trusted manufacturer
- Integrity of OBD devices: they must be provable that they have not been compromised or corrupted after their creation.
- Privacy of OBD devices: any information gained from the OBD port is intelligible only to the device's intended party.
- The authentication process of OBD devices should be efficient to not cause significant delay to users.

Existing defense strategies Unfortunately, we have not found any significant method in the literature to secure the OBD port and to detect malicious devices. However, defense strategies for CAN and ECUs are abundant. Defense strategies to detect abnormal activities from OBD ports can be implemented in CANs and ECUs and are described in their respective subsections. Fowler et al. (2017) proposed using hardware-in-the-loop (HIL) equipment to collect and simulate data on attacks through an OBD port. The HIL technique is not a defense layer on OBD ports but provides a virtual environment for further testing attack and defense mechanisms for the OBD port.

Challenges for defending against this attack model Because OBD ports are commonly used by car manufacturers for diagnostics and firmware updates, and by other companies for data collection purposes, it is difficult to distinguish legitimate from malicious OBD devices. No study has proposed putting a layer of defense in the OBD port and this remains a challenging problem.

3.2. *Attacks on CAN*

Attack model - CAN attacks through OBD Since CAN protocols generally do not support encrypting messages for authentication and confidentiality (Matsumoto et al., 2012), attackers can perform three types of attack as follows.

- Eavesdrop: CAN messages can be observed from the OBD port (Matsumoto et al., 2012).
- Replay attack and unauthorized data transmission (Lin and Sangiovanni-Vincentelli, 2012): Once attackers have observed all messages transmitted on the CAN bus, they can easily impersonate an ECU and transmit counterfeit messages through OBD ports.

- Denial of Service attack (Matsumoto et al., 2012). Attackers can send many messages with high priority through OBD ports and prevent CAN from processing other messages on the CAN bus.

It is important to note that all of these attacks require physical access to the OBD port.

Criteria for defense strategies against CAN attacks through OBD Based on our understanding of the attack model and study on the defense techniques, we suggest the following criteria.

- Confidentiality/privacy of CAN messages: CAN messages should be readable by only the intended receiving ECUs. A message sent through CAN is received by all ECUs connected to that CAN and each ECU decides whether to use it by checking the identifier of the message (Hoppe et al., 2008). This may allow attackers to conclude private information such as driving behavior or the state of the vehicle.
- Authenticity of CAN messages: CAN messages should only be sent from verified ECUs connect to that CAN to prevent unauthorized data transmission and Denial of Service attacks.
- Low requirement for computing resources: the authentication and verification process of CAN messages should be done efficiently to ensure real-time performance of the entire CAV system.

Existing defense strategies against CAN attacks through OBD Wolf et al. (2006) proposed a secure CAN protocol that achieved authenticity and confidentiality by using Symmetric Key Encryption and Public Key Encryption. Lin and Sangiovanni-Vincentelli (2012) and Nilsson et al. (2008b) also proposed to achieve authenticity by using the Message Authentication Code (MAC) method. Van Herrewege et al. (2011) proposed an authentication protocol named CANAuth, which also uses MAC for authentication but utilizes an out-of-band channel to send more authentication data in a real-time environment. Even with the out-of-band channel, Herrewege et al. acknowledge that public-key cryptography is not viable due to its large key size requirement. Matsumoto et al. (2012) criticized that the aforementioned cryptographic methods suffer from key management issues (e.g. leakage of secret keys) and may not be fast enough to achieve real-time response in a moving vehicle. Halabi and Artail (2018) aimed to solve these problems by proposing lightweight symmetrical encryption where the keys are generated based on a CAN frame's payload and the previous key.

IDS-based defense techniques are popular. Müter and Asaj (2011) proposed calculating the entropy of a CAN bus during normal activities; significant deviations in entropy are then used to detect attacks. Similarly, Miller and Valasek (2014) proposed using a small device that connects to the OBD port, collects traffic data, and detects abnormal traffic patterns with machine learning. When the device detects an attack, it stops the circuit on the CAN bus and disables all CAN messages. Matsumoto et al. (2012) proposed a solution where all ECUs attempt to detect unauthorized messages by monitoring all messages being transmitted on the CAN bus. For each ECU, a flag is implemented within the CAN controller that would indicate whether the ECU is trying to send a message. Then, the timing of the flag being switched is measured to detect unauthorized messages. Cho and Shin (2016); Shin and Cho (2017) proposed a similar method, where they measured the intervals of periodic CAN messages and used these measurements to detect abnormal messages. Gmiden et al. (2016) criticized that Matsumoto's method requires modifications to each ECU and thus is an expensive solution. Gmiden et al. then proposed an IDS that checks the identity of each ECU that sends CAN messages and calculates the time since the last message from the same ECU was observed. If the new time interval is significantly shorter than the previous time intervals from the same CAN ID, an alert of attack is raised. Tyree et al. (2018) proposed an IDS that uses the correlations between ECU messages to estimate the state of the vehicle. A sudden change to an ECU's messages would raise an alert that the ECU is compromised. If an attacker successfully compromises many ECUs, the sudden change in the state of the vehicle is used to detect the attack. Many more types of IDS for CAN can be found in Tomlinson's survey paper about this topic Tomlinson et al. (2018). Siddiqui et al. (2017) proposed a hardware-based framework that implements mutual authentication and encryption over the CAN Bus.

Challenges for defending against CAN attacks through OBD Requirements for a good defense method against this attack model are real-time response, accuracy, and low degree of modification needed on the vehicle. Even though many defense mechanisms have been proposed in the literature (Tomlinson et al., 2018), there also exist criticisms to most of them as discussed in the previous two paragraphs. It is difficult to determine the best defense strategies to implement in an operating CAV. Therefore, there is a need for comparative studies that are performed on moving vehicles to serve as recommendations for CAV manufacturers. Besides, CAN standards may carry legacies and thus may not have the capacity to accommodate the computing demand and communication constraints to these innovative solutions.

Attack model - CAN attacks through telematics ECUs One may attack a CAN by compromising a member ECU first. Some ECUs could be compromised without access to the CAN because they have other access points through connection mechanisms such as Bluetooth and cellular networking. The compromised ECU can then send authenticated messages that can bypass the cryptographic and IDS-based defense mechanisms discussed in CAN Attacks through OBD. More details about how telematics ECUs are compromised and studies that have implemented this attack model are presented in Section 3.3.

Criteria for defense strategies against CAN attacks through telematics ECUs Defense strategies may be implemented on the CAN to detect abnormal ECU behaviors or may be implemented on telematics ECUs to prevent compromise. Here, we discuss the second approach and leave the first approach for Section 3.3. The criteria for a defense strategy to be implemented on CAN are:

- Enforce integrity of messages sent through CAN under the possibility that a connected ECU is compromised (and thus any authenticity test is invalid).

- Efficient verification process to not interrupt system-wide service.

Existing defense strategies against CAN attacks through telematics ECUs When attackers have successfully compromised an ECU, they may be able to send encrypted and authenticated messages through the CAN. Therefore, cryptographic methods discussed in CAN Attacks through OBD such as Symmetric Key Encryption, Public Key Encryption, and MAC may not be able to detect the attack. Some IDS-based defense techniques would not be useful either. For example, Matsumoto's method (Matsumoto et al., 2012) and Gmiden's method (Gmiden et al., 2016) may not work because messages being sent from the compromised ECU would not create any timing abnormality. Other IDS-based approaches, such as Müter's (Müter and Asaj, 2011), Miller's (Miller and Valasek, 2014), and Tyree's (Tyree et al., 2018), may work because they attempt to model the traffic patterns and state of the vehicles, thus we speculate that they may acquire essential information to detect abnormal messages from the compromised ECU. A probably better strategy of defense is to secure the telematics ECUs. Securing telematics ECUs are discussed in the next subsection about ECUs.

Challenges for defending against CAN attacks through Telematics ECUs As previously discussed, there are two approaches to defend against this attack model: securing telematics ECUs (Nilsson et al., 2008c; Seshadri et al., 2006) and using IDS-based algorithms to detect abnormal traffic patterns from the compromised telematics ECUs (Miller and Valasek, 2014; Müter and Asaj, 2011; Tyree et al., 2018). Implementing both approaches in a CAV would increase the security against this attack model. However, it is still unclear how effective these approaches will be and how difficult they are to be implemented.

3.3. *Attacks on electronic control units*

Attack model - ECU attacks through CAN Attackers compromise ECUs through their access to CAN. As previously discussed, after gaining access to CAN through the OBD port or telematics ECUs, attackers may compromise other ECUs on the CAN. Examples of attack techniques are falsifying input data (Koscher et al., 2010), code injection and reprogramming ECUs (Hoppe et al., 2008; Prathap and Rachumallu, 2013).

Existing defense strategies against ECU attacks through CAN have been discussed in sections regarding OBD and CAN (3.1 and 3.2).

Attack model - attacks on telematics ECUs Attackers compromise telematics ECUs through their connection mechanisms. We have found two examples of this attack model in the literature. First, Checkoway et al. (2011) were able to get remote code executions on a telematics unit of a vehicle through Bluetooth and long-range wireless connection (chapters 4.3 and 4.4 on the cited paper, respectively). The authors achieved this result by extracting the ECUs' firmware and using disassembly (a computer program that decompiles machine code into assembly language) to reverse-engineer the code. After assessing the firmware of the ECU that is responsible for Bluetooth connections, the authors hypothesized that if attackers can pair their smartphones with the Bluetooth ECU, they can compromise the ECU by sending malicious code through their smartphones. For example, after re-engineering the operating system of the ECU that is responsible for handling Bluetooth connections, Checkoway et al. found over 20 insecure calls to *strcpy*, one of which would allow them to copy data to the stack and thus to execute any code on the ECU. Second, Nilsson et al. (2008c) described another pathway for attacking telematics ECUs as follows. Many CAV manufacturers are performing firmware updates over the air (FOTA) for ECUs (Nilsson et al., 2008a). The FOTA process works as follows. The firmware is first downloaded over a wireless network connection to a trusted station, then transferred to the vehicle, and finally transferred to the ECUs. The firmware transferring process can be secured by using protocols described in Mahmud et al. (2005); Nilsson and Larson (2008), but the installation process is not secured. Therefore, the downloaded firmware is vulnerable to susceptible to adversarial modification by a time-of-check-to-time-of-use attack (TOCTTOU), as described in Mulliner and Michéle (2012). The TOCTTOU attack works as follows. Given the benign firmware update *File B* that is expected by the check-install code. The attacker also prepares malicious *File M* and constructs a storage device that can observe the read requests to *File B*. For the first access to *File B*, the mass storage device serves the legitimate *File B*. This first access is likely to serve the purpose of calculating and comparing the cryptographic hashes. After the verification process succeeds, the storage device serves the malicious *File M* for the installation phase. The attack succeeds if the check code verifies the benign file *File B* and then install the malicious *File M* for the ECU's firmware update. Also regarding firmware updates for ECUs, Chattopadhyay and Lam (2017) Chattopadhyay and Lam (2017) raised a security concern over the use of the stream cipher ChaCha20 and the MAC function Poly1305 for high-speed secure boot for ECUs. The reason is that these two techniques were shown to be susceptible to power and electromagnetic side-channel analysis (Jungk and Bhasin, 2017). We have not found any study that discusses how the information obtained from the side-channel analysis may translate into meaningful attacks and thus this may be an interesting direction of research.

Criteria for defense strategies against ECU access through connection mechanisms 2 Based on our understanding of the attack model and study on the defense techniques, we suggest the following criteria.

- Robust code on ECUs' firmware to avoid code injection.
- Restrict access to connect to telematics ECUs, i.e., only accept connections from trusted and authenticated sources.
- Robust firmware update protocols for ECUs that assure the integrity and authenticity of the firmware updates.

Existing defense strategies against ECU attacks through connection mechanisms Checkoway et al. (2011) did not discuss specific defense strategy against their attack model through Bluetooth and wireless connection, but did mention that robust code and firmware update protocols for ECUs are necessary. Seshadri et al. (2006) and Nilsson et al. (2008c) proposed a protocol to secure the ECUs' FOTA. in Nilsson et al. (2008c), the secure protocol can be summarized as follows. First, the trusted station generates a random value and combines it with fragments of the firmware update to create a chain. The chain is then hashed repeatedly and the final hash value serves as the verification code. Next, the firmware, the random value, and the verification code are transferred to the vehicle over a secure channel and the hashing process is performed again to validate the integrity of the firmware. in Seshadri et al. (2006), the authors proposed Indisputable Code Execution (ICE), which is a protocol to securely execute codes on a network node from a trusted station. ICE consists of three steps: checking the integrity of the firmware update code, setting up an environment in which once the firmware update is executed, no other code is allowed to be executed, and executing the firmware update within the safe environment.

Challenges for defending against ECU attacks through connection mechanisms We have not found any study that implements the frameworks described in Nilsson et al. (2008c) and Seshadri et al. (2006) to secure FOTA. A study to validate these frameworks in a realistic CAV environment is still needed as these publications only presented theoretical frameworks.

3.4. *Attacks on LiDAR*

Attack model - LiDAR spoofing An attacker can record legitimate signals sent from a LiDAR sensor and relay the signals to another LiDAR sensor of the same CAV to make real objects appear closer or further than their actual locations. Another variation of this attack model is when an attacker creates counterfeit signals that represent an object and inject the counterfeit signals into a LiDAR sensor. Both of these variations have been successfully demonstrated by Petit et al. (2015) at a low financial cost. The authors performed the spoofing attack as follows. The attacker uses two transceivers *B* and *C*. The output of *B* is a voltage signal that corresponds to the intensity of the pulse sent by the LiDAR device being attacked. The output of *B* is sent to *C*, which in turn emits a pulse to the LiDAR device. The total cost of these two transceivers was 49.9 US Dollars! Despite the low cost, the authors managed to make the vehicle's ECU (one that receives input from a LiDAR sensor) think that it is approaching a large object and initiate emergency brakes. The second attack variation was more difficult to perform, as it requires the attacker to send the counterfeit signals within a small window after a LiDAR sensor sends its signal. Shin et al. (2017) performed this attack variation on a standalone LiDAR sensor, Velodyne's VLP-16. Cao et al. (2019) concluded from their experiments that the machine learning-based object detection process made it difficult to perform a LiDAR spoofing attack. Nevertheless, the authors formulated an optimization model for the process of generating counterfeit inputs. They performed a case study on the Baidu Apollo's software module and was able to force an emergency brake, reducing the vehicle's speeding from 43 km/h to 0 in a second. The authors claimed that their attack model can have a success rate of 75%.

Criteria for defense strategies against LiDAR spoofing Based on our understanding of the attack model and study on the defense techniques, we suggest the following criteria.

- Low cost: A trivial solution for defending against this attack model is to have redundant LiDAR devices on the vehicle to make it more difficult for attackers to spoof all devices simultaneously. However, the cost for this solution is proportional to the number of redundant LiDAR devices and thus this solution may not be appealing for manufacturers.
- High immediacy: The solution should not take too long to detect a spoofing attack. This also implies that the solution should be computationally efficient.
- Signal filter: a solution that can detect spoofing attacks may be sufficient, but a solution that can filter out legitimate signals among adversarial signals would be even more appealing.

Existing defense strategies against LiDAR spoofing Shin et al. (2017) proposed a few defense strategies such as using multiple sensors having overlapping views, reducing the signal-receiving angle, transmitting pulses in random directions, and randomizing the pulses' waveforms. Nevertheless, the authors also pointed out that these defense strategies do not match all the aforementioned criteria. Using multiple sensors is expensive. Reducing the signal-receiving angle is also expensive because it requires more LiDAR devices to cover the entire space around the vehicle. Transmitting pulses in random directions is feasible and inexpensive, but does not have good immediacy because the LiDAR device would have to send many unused pulses. Randomizing the pulses' waveforms and rejecting pulses different from the transmitted one is probably the most appealing solution thanks to its low cost and high immediacy. Approaches of this type have also been studied intensively and applied for military radars (Pace, 2009). In a 2016 study on LiDAR spoofing on Unmanned Aerial Vehicle (UAV), Davidson et al. (2016) proposed using LiDAR data in previous frames to formulate a momentum model that aims to detect adversarial inputs. The model utilizes the random sample consensus (RANSAC) method and works as follows. Let $v_{diff} = (dx_1, dy_1), (dx_2, dy_2), \ldots$ be the vector of motion that contain features from LiDAR object detection. RANSAC randomly samples k features and forms a hypothesis for each of them. The hypothesis h_j for vector (dx_j, dy_j) is the ground truth motion for vector (dx_j, dy_j). Then, we let all other features vote for each of these k hypotheses. For a feature motion (dx_j, dy_j) to vote for a hypothesis h_j, the two motion vectors need to be similar such that $|(dx_i - dx_j, dy_i - dy_j)|_1 < threshold$. The RANSAC method performs many realizations of this process and then picks the hypothesis with the highest vote to be the final hypothesis for the frame, and the corresponding features to be the ground truth of the frame. The shortcoming of this solution, which the authors also acknowledged in the paper, is that it would take some time to build up the weights for the model and would require high computational power. Thus, the solution is not immediate. In 2018, Matsumura et al. (2018) proposed a mitigation technique that embeds the authentication data onto the light wave itself. The fingerprinting is obtained by modulating LiDAR's laser light with information from a cryptographic device, such as an AES encryption circuit. This defense strategy is interesting because it is cost-effective to implement and the authors claimed that attackers cannot make a distance-decreasing attack larger than 30 cm. It is important to note that Cao's study (2019) Cao et al. (2019) on an attack model was published after Matsumura's defense strategy (2018) Matsumura et al. (2018) but did not discuss this defense strategy any other countermeasure. In 2020, Porter et al. proposed adding dynamic watermarking to LiDAR signals to validate measurements. This solution has the potential to satisfy all the three aforementioned criteria.

Challenges for defending against LiDAR spoofing Cao's attack model may be considered state-of-the-art for its newness and effectiveness. Matsumura's countermeasure is also novel and recent (Matsumura et al., 2018). It will be an interesting study to implement Matsumura's strategy against Cao's attack model (Cao et al., 2019). Davidson's proposed method for UAV (Davidson et al., 2016) may also be worth an experiment on CAVs. Porter et al.'s solution shows good potential and will be interesting for the community to discuss.

Attack model - LiDAR jamming Attackers aim to perform a Denial-of-Service attack by sending out light with the same wavelength but with higher intensity and effectively preventing the sensor from acquiring the legitimate light wave. This technique has been used by civilians who aim to avoid speeding tickets by jamming police's speed gun (a LiDAR device) (Fox News, 2020). In the context of CAV attacks, Stottelaar (2015) successfully performed a jamming attack on a LiDAR sensor (Ibeo Lux3) and argued that such an attack on a CAV's LiDAR sensor is possible. We have not found any other study or experiment on LiDAR jamming in the literature. Nevertheless, the attack process, as described in detail in Stottelaar (2015), is relatively straightforward and should not require much training to replicate.

Criteria for defense strategies against LiDAR jamming Based on our understanding of the attack model and study on the defense techniques, we suggest the following criteria.

- Low cost: The solution should not require expensive modification to the vehicle
- High immediacy: The solution should not take too long to detect a jamming attack.
- Signal filter: a solution should be able to filter out legitimate signals among jamming signals.

Existing defense strategies against LiDAR jamming Stottelaar (2015) suggested several countermeasures such as using V2V communications to gather additional information, changing the wavelength frequently, using multiple LiDAR sensors with different wavelengths, and shortening the ping period (the time window that a sensor waits for the signal to come back). However, these countermeasures all have disadvantages. Vehicle-to-vehicle communication may not always be available. Using multiple LiDAR devices is expensive. The shortened ping period makes a device prone to errors. Changing wavelength frequently may not be effective against attackers who can follow a CAV for a while, as acknowledged by the author. Wang et al. (2015) proposed a novel LiDAR scheme called pseudo-random modulation (PMQSL) quantum secured LiDAR (Wang et al., 2015). The PMQSL scheme is based on the random modulation technique. Random modulation is a technique in the time domain, which is a typical way to recover the weak signal buried in random noise. The transmitting signal is modulated by the digital pulse codes, usually consisting of on and off. The n^{th} order M-sequence a_i with elements 1 or 0 is generated by a set of n-stage shift registers. The laser is pulse-position modulated by an electro-optic modulator. These pulses are further randomly modulated to create the horizontal, diagonal, vertical, and anti-diagonal polarization states of the photon through a polarization modulated model. When there is no jamming attack, four different distances corresponding to the four measured polarizations have very small error rates. In the presence of jamming attacks, the four distances have considerable errors in the received polarization. The increase in error allows the system to determine that the LiDAR device was being jammed. The authors claimed that this LiDAR scheme can efficiently detect a jamming attack, but cannot filter out legitimate signals among jamming signals.

Challenges for defending against LiDAR jamming We have not found any study or experiment that demonstrates LiDAR jamming on a moving autonomous vehicle, as in LiDAR Spoofing. Such a study will be interesting since we can observe the real effectiveness of LiDAR Jamming. Besides, defense strategies proposed in Wang et al. (2015) and Nouri et al. (2017) need to be tested for CAVs because they were not specifically developed for CAVs.

3.5. *Attacks on radar*

Attack model - radar spoofing Attackers replicate and rebroadcast radar signals to inject distorted data to the sensor. A common tool to perform this attack model is Digital radio frequency memory (DRFM), which is an electronic method to store radio frequency and microwave signals by using high-speed sampling and digital memory (Roome, 1990). The phase of stored signals can then be modified and the signals are then re-broadcasted to the radar sensor. The falsified signals can then cause incorrect calculations of distance to surrounding objects. Chauhan (2014) Chauhan (2014) experimented with this attack model on a radar device (Ettus Research USRP N210) and managed to make an object from a 121-meter distance appear at a 15-meter distance. Yan et al. (2016) discussed the same idea of the attack but unfortunately, they did not have the resource to implement the attack. Instead, they attempted to inject counterfeit signals to a radar sensor on a Tesla Model S. The attempt was not successful because the sensor has a low ratio of working time over idle time, which makes it difficult to inject signals at the precise time slot.

Criteria for defense strategies against radar spoofing Based on our understanding of the attack model and study on the defense techniques, we suggest the following criteria.

- Attack Detection: The solution should be able to detect a radar spoofing attack in a timely manner.
- Signal Filter: The solution should be able to filter out the attack signals and derives accurate distance measurements.
- Consistency: The solution should be able to achieve the previous two criteria under many circumstances and over a long period of time.
- Non-disruptivity: The solution should not affect other services of a vehicle.

Existing defense strategies against radar spoofing A novel approach, called physical challenge-response authentication (PyCRA) (2015) Shoukry et al. (2015), inspects the surrounding environment by sending randomized probing signals, called challenging signals. PyCRA shuts down the actual sensing signals at random times and assumes that attackers cannot detect challenging signals immediately. Under that assumption, PyCRA can detect malicious signals by determining if they are higher than a noise threshold during a period with the Chi-square test. Kapoor et al. (2018) criticized PyCRA that PyCRA may severely affect the safety-critical CAV components, such as adaptive cruise control and collision warning because they are shut down at random times. Another shortcoming of PyCRA is that after the first 30 seconds following an attack, The derived distance is continuously longer than the actual distance (Kapoor et al., 2018), thus PyCRA falls short of the Consistency criteria. Dutta et al. (2017) attempted to address PyCRA's problems with consistency and non-disruptivity by introducing the Challenge Response Authentication method (CRA). CRA works by applying the recursive least square method to provide the estimated distance by minimizing the sum of square of errors, which is defined as the difference between the predicted distance and the actual distance. According to Dutta et al., CRA may satisfy all four aforementioned criteria. However, Kapoor et al. criticized that CRA may not be effective in practice because it relies on the assumption that the actual distance is known (Kapoor et al., 2018). Kapoor et al. proposed a new method called Spatio-Temporal Challenge-Response (STCR). STCR uses the same idea as PyCRA, but instead of shutting down sensing signals, it transmits challenging signals in randomized directions. Reflected challenging signals can be used to identify directions that reflect malicious signals, then excludes the untrustworthy directions when measuring the surrounding environment. According to Kapoor et al. (2018), STCR is able to detect attacks and measure the actual distance consistently and in a timely manner.

Challenges for defending against radar spoofing Yan et al. (2016) failed to apply the DRFM technique to inject counterfeit signals to a radar sensor because the sensor has a low ratio of working time over idle time. However, it was unclear from their publication whether this is the characteristic that all CAVs' radar sensors share, and whether an attacker can find a way to overcome this problem. Further experiments are needed to answer this question. Besides, Kapoor et al.'s defense method (Kapoor et al., 2018) is a state-of-the-art technique but has not been validated in an experiment.

Attack model - radar jamming This attack model can also be carried out by using DRFM, but instead of modifying the phase, attackers can modify the frequency and the amplitude of the stored signals before rebroadcasting to the radar sensors. The falsified signals can make the radar sensors fail to detect the object, at which the jamming device is located. We have not found any publication that experimented with this attack model on CAVs. However, this attack model is widely used by manned and unmanned aerial vehicles (UAV) to hide from radar detection (Buehler et al., 2014; Lothes et al., 1990; Stott, 1994). Since these attacks have only been applied to UAVs and not CAVs, we are not certain about their feasibility on CAVs and thus cannot make claims about criteria for defense strategies.

Existing defense strategies against radar jamming Similar to the attack model, defense strategies are widely studied for UAVs, but none has been discussed for CAVs. To defend against this attack model, one can attempt to separate the legitimate signals from the counterfeit signals. The specific methods are described in Greco et al. (2005, 2008); Lu et al. (2010); Nouri et al. (2017).

Challenges for defending against radar jamming Further studies on both attacks and defense techniques are needed to investigate whether the attacks are feasible on CAVs and whether the defense techniques are also effective on CAVs.

3.6. *Attacks on GPS*

Attack model - GPS spoofing An attacker broadcasts incorrect, but realistic GPS signals to mislead GPS receivers on CAVs. This is also known as a GPS Spoofing attack. In this attack model, attackers begin by broadcasting signals that are identical to the satellites' legitimate signals. The attackers then gradually increase the power of their signals and gradually deviate their GPS signals from the target's true location. GPS receivers are often configured to make use of signals with the strongest magnitudes (Krasner, 2000). Therefore, once the counterfeit signal is stronger than the legitimate satellite signal, GPS devices would choose to process the counterfeit signal. Tippenhauer et al. (2011) described in detail how to perform a GPS Spoofing attack and the requirements for a successful attack (Tippenhauer et al., 2011). They found that an attacker must be able to calculate the distance from himself to the victim with an error of at most 22.5 meters. Whether this condition could be met on a moving CAV is still unclear. We have not found any successful GPS spoofing attack on CAV published in the literature. However, attacks on other transportation means are available. For instance, in 2014, Psiaki et al. (2014) successfully spoofed GPS signals to a superyacht's and reported counterfeit locations to the crew. The crew then attempted to correct the course, only to deviate from the correct course. Shepard et al. (2012) used a civilian GPS spoofer to successfully create a significant timing error in a phasor measurement unit, which is a component of GPS devices responsible for estimating the magnitude and phase angle of GPS signals. Zeng et al. (2018) assembled a small device from popular components with a total cost of 223 US Dollars and used it to trigger fake turn-by-turn navigation to guide victims to a wrong destination without being noticed. The authors demonstrated the attacks on real cars with 40 participants and were able to guide 38 participants to the authors' predetermined locations (95% success rate). Zeng et al. discussed one of the limitations of their study is that it is not effective if a driver is familiar with the area. However, this may not be the case for CAVs and thus Zeng et al.'s attack model would pose a significant threat to CAVs. Recently, Regulus Cyber LTD. tested GPS spoofing on a Tesla 3 and successfully made the car's GPS display false positions on the map, and hence any attempt to find a route to a destination resulted in bad navigation Regulus Cyber LTD (2020). The total equipment cost to perform this attack was 550 US Dollars and the report also stated that "this dangerous technology is everywhere". Unfortunately for those who are curious, the researchers did not perform an attack when the car was on autopilot mode. Narain et al. (2019) proposed an interesting approach for attackers. They first looked for data on regular patterns that exist in many cities' road networks. Then, they used an algorithm to exploit the regular patterns and identify navigation paths that are similar to the original route (assuming that the attackers know the victim's route). Finally, the identified paths can be forced onto a target CAV through spoofed GPS signals. This attack model allows attackers to possibly bypass some defense mechanisms, such as the Inertial Navigation System (INS), which helps GPS receivers to get positions and angle updates at a quicker rate (El-Sheimy et al., 2006; Petovello et al., 2001). The inconsistencies between the spoofed path and the original path may be negligible and the attack can be successfully executed. Also in 2019, Meng et al published an open-source GPS-spoofing generator using Software-Defined Receiver (Meng et al., 2019a). The authors claimed that their spoofing generator can cover all open-sky satellites while providing high-quality concealment, thus it can block all the legitimate signals. This would make the spoofing signals closely similar to that of the legitimate signal. Therefore, it would be difficult to detect this attack based on only the differences with surrounding GPS receivers or the signal consistency. The threat of this spoofing model to CAVs is very serious once all signals from the visible GPS satellites are spoofed (Meng et al., 2019a).

Criteria for defense strategies against GPS spoofing Haider and Khalid (2016) proposed the following criteria for effective defense strategies:

- Quick Implementation: The solution can be implemented easily.
- Cost Effective: The solution should be affordable on either a small scale or a large scale.
- Prevent Simple Attack: the ability to detect simple attacks.
- Prevent Intermediate Attacks: the ability to detect intermediate types of attack.
- Prevent Sophisticated Attacks: the ability to detect sophisticated and advanced types of attacks, such as (Meng et al., 2019a; Narain et al., 2019).
- No Requirements to modify satellite transmitters: the solution does not require changes to be made on the satellite transmitters.
- Validation: the solution is easy to test.
- Interoperability: The solution works on many types of machines (however, we are only concerned about CAVs in this context).

Existing defense strategies against GPS spoofing In 2003, the United States Department of Energy suggested seven simple countermeasures to detect GPS spoofing attacks (Warner and Johnston, 2003). The seven countermeasures are:

- Monitor the absolute GPS signal strength: by recording and monitoring the average signal strength, a system may detect a GPS spoofing attack by observing that signal strengths are many orders of magnitude larger than normal signals from GPS satellites.
- Monitor the relative GPS signal strength: the receiver software could be programmed to record and compare signals in consecutive time frames. A large change in relative signal strength would be an indication of a spoofing attack.
- Monitor the signal strength of each received satellite signal: the relative and absolute signal strengths are recorded and monitored individually for each of the GPS satellites.
- Monitor satellite identification codes and the number of satellite signals received: GPS spoofers typically transmit signals that contain tens of identification code, whereas legitimate GPS signals on the field often come from a few satellites. Keeping track of the number of satellite signals received and the satellite identification codes may help determine a spoofing attack.
- Check the time intervals: with most GPS spoofers, the time between signals is constant. This is not the case with real satellites. Keeping track of the time intervals between signals may be useful in detecting spoofing attacks.
- Do a time comparison: Many GPS receivers do not have an accurate clock. By using timing data from an accurate clock to compare to the time derived from the GPS signals, we can check the veracity of the received GPS signals.
- Perform a sanity check: by using an accelerometer and a compass, a system can independently monitor and double-check the position reported by the GPS receiver.

All of the above seven countermeasures are simple and inexpensive to implement, may prevent simple attacks, do not require modification to satellite transmitters, and are inter-operable. However, they may fall short when dealing with sophisticated attacks such as Meng et al. (2019a); Narain et al. (2019).

Defense strategies against GPS spoofing attacks have also been studied extensively in the academic literature. Since GPS signals do not contain any information that can verify their integrity, a natural way to defend against GPS Spoofing is to use redundant information to verify the integrity of GPS signals. One example of such a method is the Receiver autonomous integrity monitoring (RAIM), a technology that uses redundant signals from multiple GPS satellites to produce several GPS position fixes and compare them (Brown, 1996; Hewitson and Wang, 2006). A RAIM system is considered available if it can receive signals from 24 or more GPS satellites (Loh and Fernow, 1994; Van Dyke, 1992). RAIM statistically determines whether GPS signals are faulty or malicious by using the pseudo-range measurement residual, which is the difference between the observed measurement and the expected measurement (Yang and Xu, 2016). Advanced Receiver Autonomous Integrity Monitoring (ARAIM) is a concept that extends RAIM to other constellations beyond GPS, such as GLObal NAvigation Satellite System (GLONASS), Galileo, and compass (Blanch et al., 2012; Choi et al., 2011). One criticism with ARAIM is that its availability is inconsistent if one or more satellites are not reachable (Qian et al., 2019; Van Dyke, 1992). Meng et al. (2019b) proposed solutions for this problem and improved ARAIM availability up to 98.75% (Meng et al., 2019b; Qian et al., 2019). There are many other validation mechanisms, which all make use of additional satellites or side-channel information. For example, O'Hanlon et al. described how to estimate the expected GPS signal strength and compared it against the observed signal strength to validate GPS signals (O'Hanlon et al., 2013). Furthermore, a defense system can monitor GPS signals to ensure that the rate of change is within a threshold. Montgomery proposed a defense approach that uses a dual antenna receiver that employs a receiver-autonomous angle-of-arrival spoofing countermeasure (Montgomery, 2011). The main idea is to measure the difference in the signal's phase between multiple antennas referenced to a common oscillator. Other examples of countermeasures can be found in the survey paper by Haider and Khalid (2016).

Challenges for defending against GPS spoofing Even though several countermeasures have been proposed in the literature, their effectiveness against newer attack strategies, such as Meng et al. (2019a); Narain et al. (2019), is unknown. The attack strategy in Meng et al. (2019a) is especially dangerous for CAVs. Therefore, finding effective countermeasures for these 2019-born attack models is a current research challenge.

Attack model - GPS jamming: Since radio signals from the satellites are generally weak, jamming can be achieved by firing strong signals that overwhelm the GPS receiver so that the legitimate signals can not be detected (Hu and Wei, 2009). Examples that highlight the risks of GPS jamming have been reported. In 2013, a New Jersey man was arrested for using a $100 GPS jamming device plugged into the cigarette lighter in his company truck (Helfrick, 2014). The man's motive was to jam his company truck's GPS signal to hide from his employer. However, the device was reported to be powerful enough to interfere with GPS signals at the nearby Newark airport. Even though GPS jamming devices are illegal for civilian use, they can easily be found on online retailers such as eBay (Coffed, 2014). GPS jamming is less dangerous than GPS spoofing in the sense that attackers have higher control over GPS receivers with a spoofing attack. However, GPS jamming attacks can cause disruptions of service and is essentially a Denial-of-Service attack.

Criteria for defense strategies against GPS jamming Based on our understanding of the attack model and study on the defense techniques, we suggest the following criteria.

- Attack Detection: The solution should be able to detect a jamming attack in a timely manner to ensure the safety of CAVs.
- Signal Filter: The solution should be able to filter out the attack signals so that the vehicle can still operate under certain attack scenarios and avoid disruption of service.

Existing defense strategies against GPS jamming Many GPS receiver modules have implemented anti-jamming measures that target unintentional interference from every-day electronic devices. However, Hunkeler et al. (2012) have shown that these countermeasures are ineffective against intentional attacks. For example, the NEO-6 GPS receiver has an integrated anti-jamming module that provides data to assess the likelihood that a jamming attack is ongoing. Hunkeler et al. showed that the parasitic signal from the GPS jammer interfered with the NEO-6 receiver in such a way that the receiver could not function while the anti-jamming module reported a very low probability for a jamming attack. Several studies have demonstrated how to calculate the probability of intentional GPS jamming attack just by using information from GPS receivers (Hunkeler et al., 2012; Sun and Amin, 2005; Zhang and Amin, 2012). Unfortunately, detection of GPS jamming does not prevent disruption of service, which is the main objective of a GPS jamming attack. L3Harris Technologies, Inc. developed a technology, Excelis Sentry 1000, that can detect sources of interference to support timely and effective actionable intelligence (Pattinson et al., 2017). The Excelis Sentry 1000 systems can be strategically placed around high-risk areas to instantaneously sense and triangulate the location of jamming sources (Coffed, 2014). However, this defense strategy may not be effective for CAVs, whose operating location is not predictable.

Mukhopadhyay et al. (2007) and Purwar et al. (2016) proposed methods to reduce the jamming signals and estimate the legitimate GPS signals. Mukhopadhyay used the Adaptive Array Antenna technology and the Least Mean Squared (LMS) algorithm to maximize the chance of collecting the desired signals and the chance of rejecting jamming signals. The Adaptive Array Antenna technology is antenna arrays that have integrated signal processing algorithms that can identify spatial signal signatures such as the direction of arrival (DOA) of the signal, and use them to calculate beamforming vectors to track and locate the antenna beam. Mukhopadhyay used the LMS algorithm, which is a member of a family of stochastic gradient algorithms, to further accurately calculate the DOA. The DOA information would then contribute to determining the signals being rejected or accepted. Purwar et al. (2016) proposed the Turbo Coding method for counter jamming. In Turbo Coding, The Turbo encoder at the GPS satellites that send the original GPS data is encoded, then modulated, and passed over a noisy channel. Then, the encoded data arrives at the GPS receivers along with noise and jamming signals. The receiver demodulates the distorted GPS signals and then the Turbo Decoder decodes demodulated signals to retrieve the original GPS signals. This technique has two major weaknesses. First, the results in Purwar et al. (2016) demonstrated that as the strength of jamming signals increases, their method becomes less effective. Specifically, when the jamming signals is about 14 times stronger than the legitimate signals, the method cannot recover the legitimate signals. Second, this method requires modification to the GPS satellites.

Challenges for defending against GPS jamming: The state-of-the-art countermeasure was published by Purwar et al. (2016). It has two major weaknesses that would be problematic to be implemented for CAVs. The method requires modification to the GPS satellites and is only effective if the jamming signals are not too strong.

3.7. *Attacks on cameras*

Attack model - camera blinding On CAVs, cameras commonly provide inputs for deep learning models for the task of object detection. Attackers aim for a denial of this service by blinding a camera with extra light. Petit et al. (2015) experimented with a blinding attack on a MobilEye C2-270 camera installed on a non-automated car's windshield. The researchers showed that a quick burst of 650 nm laser was able to almost fully blind the camera and the camera never recovered from the blindness. The 940 nm 5 × 5 LED matrix and 850 nm LED spot also achieved the same result, but the camera was able to recover after more than 5 s. It is important to note that the MobilEye C2-270 camera is not used for full vehicle automation (SAE Level 5) but function-specific automation (SAE Level 1 to 3). Yan et al. (2016) experimented with similar attacks and was also able to blind a camera permanently (the authors did not specify the camera). This paper also pointed out that LED and Laser beam could blind a camera but Infrared LED could not because of the narrow frequency band filters. We have not found any other study on this attack model.

Criteria for defense strategies against camera blinding Based on our understanding of the attack model and study on the defense techniques, we suggest the following criteria.

- Low cost: The solution should not require expensive modification to the vehicle
- Generalization: The solution should work on as many attack wavelengths as possible. Petit et al. and Yan et al. showed that this attack model is possible for laser and LED with different wavelengths. A solution that works for all attack wavelengths would be ideal.

Existing defense strategies against camera blinding Petit et al. (2015) also suggested two countermeasures in their study. The first countermeasure is to use redundancy by installing multiple cameras that have overlapping coverage. This is effective because laser and LED spot have small beam widths, making it difficult to attack multiple cameras spontaneously. This defense strategy cannot mitigate the risk of Camera Blinding completely, but it makes attackers spend more effort on a successful attack. Nevertheless, the cost to implement this solution grows in direct proportion to the number of extra cameras. The second countermeasure is to integrate a removable near-infrared-cut filter into a camera. This is a technology that is available on security cameras and can filter near-infrared light on request. This solution can potentially satisfy both criteria but would need implementation and experiments to be verified. In 2020, DH and Ansari proposed a detection method by using predictive analytics to predict the future next frames captured by the cameras and then compare the received frames with the predicted frames (Sharath Yadav and Ansari, 2020). DH and Ansari's solution has the potential to satisfy both the criteria we mentioned.

Challenges for defending against camera blinding Petit et al.'s suggested countermeasures are the only ones that we found in the literature. Yan et al. (2016) did not discuss any countermeasure in their experiment. Petit et al.'s proposed strategy of using a near-infrared-cut filter into cameras has high potential but needs further experiments and validations. Similarly, DH and Ansari's solution has the potential to be a generalized solution and may be implemented easily, but need further validations due to its newness.

Attack model - adversarial images An adversary may carefully make small perturbations on the images that cameras observe and cause the artificial-intelligence algorithms (used for CAV's vision) to generate incorrect predictions. Even though the ultimate targets of this type of attack are the deep learning models that reside in ECUs, cameras are convenient channels for attackers to inject adversarial images. In 2017, Google researchers were able to create stickers called adversarial patch (Brown et al., 2018) with patterns that can deceive artificial intelligence algorithms. These stickers may be printed out and attached to important transportation objects, such as road signs. Lu et al. (2017) experimented with such an attack by taking 180 photos of compromised stop signs with an iPhone 7 from a moving vehicle. They found that a trained neural network classified most of the pictures correctly, which meant that the attack model was not effective. In contrast, Eykholt et al. (2018) were a lot more successful with their experiments. They experimented with a camera in a lab setting and a camera on a moving vehicle (non-CAV). By decorating stop signs with small black-and-white stickers, the authors made a state-of-the-art algorithm fail to recognize the stop signs 100% of the time in a lab setting and 84.8% on a moving vehicle. Kelarestaghi et al. (2019) experimented with the same type of attack by using electromagnetic interference in a remote manner and without physical modification to the stop signs, which makes the attack easier to launch and harder to detect. We have not found any experiment on CAVs, but this attack model, as demonstrated in a moving vehicle setting (Eykholt et al., 2018), should also apply to CAVs. There are several methods that attackers can use to know how to tamper with objects such as road signs. These methods are called universal adversarial perturbations and are described in Goodfellow et al. (2014); Kos et al. (2018); Moosavi-Dezfooli et al. (2017); Sitawarin et al. (2018). Recently, an IBM research group released an open-source Python library, called Adversarial Robustness 360 Toolbox, for generating and defending against adversarial images (Nicolae et al., 2018). This attack model is especially dangerous because it may make CAVs ignore alerts or read the wrong speed limits from road signs.

Criteria for defense strategies against adversarial images Based on our understanding of the attack model and study on the defense techniques, we suggest the following criteria.

- Low cost and easy implementation: The solution should not require expensive modification to the vehicle
- Generalization: The solution should work on many types of image perturbations.
- Computationally efficient: The solution should be calculated efficiently to serve real-time object-detection purposes.

Existing defense strategies against adversarial images Securing Machine Learning models against adversarial images have been discussed extensively. This can be achieved by several techniques such as pre-processing inputs (Dziugaite et al., 2016; Guo et al., 2017; Xu et al., 2017; Zantedeschi et al., 2017), adding adversarial samples to training data (Jiang et al., 2020; Miyato et al., 2015; Szegedy et al., 2013), and utilizing run-time information to detect abnormal inputs (Buckman et al., 2018). All of these methods are algorithm-based and can probably be integrated into the codes on the ECUs that handle object-detection from camera data. To our knowledge, no research has studied the extent of generalization of these algorithms, as well as their theoretical and practical computational complexity. Such a comparison study for these defense techniques should be performed for further discussions on this topic.

Challenges for defending against adversarial images The attack and defense of Adversarial Images have been studied extensively in terms of methodologies and have been tested with general images. A comparison study for these defense techniques in terms of generalization and computational efficiency should be performed to serve further discussions on this topic.

3.8. Attacks on communication mechanisms

Attack model - falsified information on network Attackers aim to send falsified information through the V2V and V2I communications to disrupt CAVs' operation and traffic flow. This can be achieved by impersonation or Sybil attacks. In an impersonation attack, attackers steal the identity of legitimate CAVs and broadcast falsified information. This could be achieved if the connection protocol lacks a strong authentication method. Chim et al. (2009) described in detail one way to impersonate another CAV's identity in section IV of their paper. In a Sybil attack, attackers create a large number of identities and use them to send falsified information over a network and make the falsified information appear to be popular and legitimate. For example, Rawat et al. (2012) described a scenario in a VANET network, where fake identities are made to look like they surround a target vehicle, making the target vehicle think that there is a traffic jam. Amoozadeh et al. (2015) performed a simulated study to attack a stream of cooperative driving CAVs by assuming that the adversary is a trusted insider such as a compromised vehicle with a valid certificate. From the trusted vehicle, falsified messages were sent to the whole crew and successfully disturbed the speeds of member vehicle and caused a significant increase in the gap between vehicles.

Criteria for defense strategies against falsified information on network This attack model can be mitigated by implementing strong authentication methods that may be specified in the V2V and V2I network protocols. Based on our understanding of the attack model and study on the defense techniques, we suggest the following criteria.

- Low cost and easy implementation: Solutions that are easier to implement and cost less are preferable.
- Computationally efficient: The solution should be calculated efficiently to serve real-time authentication.

Existing defense strategies against falsified information on network Several authentication methods have been proposed, such as Alimohammadi and Pouyan (2015); Grover et al. (2011); Whyte et al. (2013). Grover et al. (2011) proposed an authentication scheme that uses neighboring vehicles in VANET. There are four phases:

- Periodic Communication: each vehicle on the road periodically broadcasts and receives beacon packets. This phase is to announce a vehicle's presence to all vehicles on the road.
- Group construction of neighboring nodes: when a vehicle collects enough beacon messages from other vehicles, it makes a record of neighboring nodes in the form of groups at regular intervals of time.
- Exchange groups with other nodes in vicinity: after a significant duration of time, these vehicles exchange their neighboring nodes record with each other in vicinity.
- Identify the vehicles comprising similar neighboring nodes: after receiving the records from other vehicles, each vehicle may detect malicious vehicles by observing that the abnormal vehicles exist in neighboring nodes for a duration greater than a threshold.

Grover's approach may satisfy both of the aforementioned criteria but may fall short when there are not enough vehicles on the road to exchange information. Whyte et al. (2013) proposed the Security Credential Management System (SCMS) that implements a public-key infrastructure (PKI) with some features for providing privacy. The PKI is used to authenticate vehicles through V2I connections. Two major drawbacks of this approach are that PKIs are expensive to implement and that V2I communication may add significant delays to the authentication process. Alimohammadi and Pouyan (2015) proposed a secure protocol based on a lightweight group signature scheme. For a short time and secure group communication, the Boneh–Shacham algorithm is used for short group signature schemes and batch verification. Hubaux et al. (2004) suggested that all vehicles use electronic license plates to allow the wireless authentication of CAVs. Zhang et al. (2008) proposed an authentication scheme that would efficiently authenticate CAVs by using some roadside infrastructures. However, Chim et al. (2009) claimed that their attack model would penetrate Zhang et al.'s method. In 2020, Zhao et al. (2020) proposed a protection mechanism that consists of an offline phase and an online phase. The offline phase establishes matrices and parameters to support attack detection and decision making during the online phase. All the methods that require PKI and roadside infrastructures are costly and difficult to implement.

Challenges for defending against falsified information Strong authentication methods that are based on public-key encryption would require a public key infrastructure. However, as van der Heijden et al. (2018) discussed van der Heijden et al. (2018), PKIs suffer from problems such as being expensive to implement in a large region and may not provide real-time authentication. Furthermore, Chim et al. (2009) pointed out that the processing units on CAVs may not be able to process the authenticating messages in real-time.

Attack model - network denial of service Attackers perform Denial-of-Service (DoS) attack and Distributed Denial-of-Service (DDoS) attack on the communication mechanisms. Several studies have demonstrated how VANETS and V2I networks are vulnerable to DoS and DDoS attacks (Douligeris and Mitrokotsa, 2004; Hasbullah et al., 2010; Pathre, 2013; Pathre et al., 2013). All of these attacks are intended to confuse CAVs' operations and disrupt traffic flows. DDoS attacks on V2I networks are likely to disrupt transportation in a large region, especially if the infrastructure provides critical information to control traffic flows. Ekedebe et al. (2015) experimented with DoS attacks on V2I networks by using a simulated environment and showed that DoS attacks can prevent all messages from being sent to vehicles in the network. V2V networks are also possible targets for DoS and DDoS attacks because they have limited connection bandwidth. For example, the DSRC standard specifies that a node must wait to transmit signals until the DSRC channel is idle (Blum and Eskandarian, 2006). To exploit this limitation, attackers may constantly transmit noises through the DSRC channel to keep it always busy and thus to prevent legitimate signals from being delivered. Leinmuller et al. (2006) described another variation of DoS attacks on V2V networks, where an adversarial vehicle in a VANET network can falsify its position information to intercept message packets between other vehicles in the network.

Existing defense strategies against network denial of service Defending against DoS and DDoS attacks on V2I and V2V network requires a secured V2I or V2V network architecture and protocols. Just like DoS attacks on V2I networks resemble those on a traditional centralized network, defending strategies for a traditional centralized network can be applied to defend V2I networks. The defense strategies for a general centralized network can be found in Douligeris's survey paper (2004) Douligeris and Mitrokotsa (2004), which include intrusion prevention, intrusion detection, intrusion response, and intrusion tolerance techniques. Singh et al. (2018) discussed a machine-learning based approach to detect DDoS attacks on V2I networks. Besides this study, We have not found any other study that is specific to V2I networks. To secure V2V networks, several papers have proposed secured architecture. For example, Blum and Eskandarian (2006) proposed the CARAVAN architecture, Plossl et al. (2006) proposed an architecture that uses a certified GALILEO receiver to achieve reliable time and position information, Hubaux et al. (2004) suggested using electronic license plates to authenticate CAVs.

Challenges for defending against network denial of service All the aforementioned studies are based on theoretical frameworks and have not been tested in a realistic CAV environment. An experimental study, even if performed on simulated but realistic data, would be valuable to determine suitable methods to defend against DoS and DDoS attacks on V2V and V2I networks.

4. Research challenges, trends, and open issues

In this section, we first highlight the challenges and research trends that we have observed and discussed in Sections 2 and 3. These observations all came from academic research. Next, we present official publications and reports from the industry that are related to the cybersecurity of CAVs. We searched for publications and reports from corporations that are involved in the developments of CAVs.

4.1. *Academic research*

Research trends We have observed the following research trends happening on the topic of security of CAVs.

- The trend in developing new attack models largely follows the remote attack pattern by targeting sensors, cameras, and communication mechanisms. We have observed that most of the recently developed attacks can be performed from a remote distance, either from the roadside or from other vehicles. Examples of such attack can be found in Meng et al. (2019a); Narain et al. (2019); Pathre (2013); Petit et al. (2015).
- The trend in developing new defense strategies is to utilize machine learning and anomaly-based intrusion detection systems. The requirements for new defense strategies often include the capability of real-time response, low expense, and less modification to CAVs' architecture.
- There is an obvious need to develop secured mechanisms to update the software on ECUs. All the current updating mechanisms are easily abused by attackers to compromise CAVs, such as those attack models mentioned in Mulliner and Michéle (2012); Nilsson et al. (2008a).
- A decentralized public key infrastructure (PKI) will be necessary to improve the security of V2V and V2I communications van der Heijden et al. (2018); University of Warwick (2020). While operating, a CAV may meet many other CAVs in a short time and may need to exchange information through V2V communications. To mitigate the Falsified Information attack model discussed in Section 3.8, authentication based on public-key encryption is necessary. To achieve this, a CAV will need to request the public key of other CAVS from a PKI. Decentralizing PKI is necessary to reduce the latency before the vehicle receives the necessary keys to achieve real-time authentication.

Research challenges From the research challenges discussed in Section 3, we organize three categories for the open security issues on CAVs. The specific challenges and their related publications are presented in Table 4.

- **Unsolved attack models:** there are several attack models in the literature that we have not found a corresponding defense strategy in the literature. Some of these attack models pose significant and realistic threats to CAVs, such as the GPS Spoofing methods discussed inMeng et al. (2019a) and (Narain et al., 2019), both published in 2019. These challenges are presented in the first column of Table 4.
- **Attack models needing further experiments**: there are recently developed attack models that we are unable to assess the level of threat and effectiveness in a realistic environment of CAVs. Further experiments under a realistic environment will provide the community with a better understanding of the impact of these attack models and incentivize research for defense strategies. These challenges are presented in the second column of Table 4.
- **Defense strategies needing further experiments**: there are many defense strategies proposed only theoretically or have only been tested under unrealistically simulated environments. Further experiments under realistic environments will help validate these strategies and identify the most suitable ones. These challenges are presented in the third column of Table 4.

4.2. *Industrial development*

In July 2019, a coalition of 11 companies that are involved in the development of CAVs published a whitepaper titled "Safety First For Automated Driving“ (Wood et al., 2020). The 11 companies include Audi, Intel, Volkswagen, Baidu, BMW, Aptiv, Fiat Chrysler Automobiles, Daimler, Continental, Infineon, and HERE. The whitepaper describes a thorough approach to make CAVs operate safer, of which security is a subtopic. With this publication, the authors aimed to build a guideline for the development of safer and more secure CAVs. The authors claimed to continuously update this whitepaper

Table 4 – Summary of unsolved attack models with research challenges.

Unsolved attack models	Attack models needing further experiments	Defense strategies needing further experiments
• No study have proposed a defense layer to secure the OBD port that aims to distinguish legitimate from malicious OBD devices.	• The LiDAR jamming attack model discussed in Stottelaar (2015) has not been experimented in a CAV environment.	• Many defense strategies have been proposed for defending against CAN attack through the OBD port, but most of them receive criticisms (Cho and Shin, 2016; Gmiden et al., 2016; Shin and Cho, 2017; Tomlinson et al., 2018; Tyree et al., 2018). A comparison study is needed in this topic.
• Recently developed GPS Spoofing techniques (Meng et al., 2019a; Narain et al., 2019) still lack an effective countermeasure	• Yan et al. (2016) failed to apply the DRFM technique to inject counterfeit signals to a radar sensor on a Tesla Model S. Further experiments are needed to determine whether this is also the case for other CAVs and whether the challenges in this attack model can be overcome.	• Several IDS-based algorithms have been proposed to detect abnormal CAN network packets that are sent from compromised ECUs (Miller and Valasek, 2014; Müter and Asaj, 2011; Tyree et al., 2018). However, it is still unclear how effective these approaches are under a realistic CAV environment.
• Several efficient methods to detect GPS jamming are described in Hunkeler et al. (2012); Sun and Amin (2005); Zhang and Amin (2012), but none of them could filter out the jamming signals to obtain legitimate signals. Maintaining GPS service under GPS jamming attacks remains a challenge.	• Radar jamming attacks have been widely studied for manned and unmanned aerial vehicles (Buehler et al., 2014; Lothes et al., 1990; Stott, 1994), but have not been experimented on CAVs.	• Two frameworks are proposed in Seshadri et al. (2006) and Nilsson et al. (2008c) that aim to secure firmware updates over the air (FOTA). They still need further testings and experiments.
• A strong and efficient authentication method is necessary to defend V2V and V2I networks from Sybil and impersonation attacks. Public-key encryption can provide authenticity but is difficult to implement on V2V and V2I due to the reasons presented in van der Heijden et al. (2018). Further studies are needed to find an adequate solution that overcomes all the issues discussed in van der Heijden et al. (2018).	• Although the experiments on GPS jamming have been demonstrated in Helfrick (2014); Hu and Wei (2009) and the jamming devices can be obtained with relative ease, the potential and threat level of such an attack on CAVs have not been studied. • Regarding firmware updates for ECUs, Chattopadhyay and Lam (2017) Chattopadhyay and Lam (2017) raised a security concern over the use of the stream cipher ChaCha20 and the MAC function Poly1305 for high-speed secure boot for ECUs. These techniques were shown to be susceptible to power and electromagnetic side-channel analysis (Jungk and Bhasin, 2017). It will be useful to study how information obtained from the side-channel analysis may translate into meaningful attacks.	• Recently proposed defense strategies against LiDAR Spoofing (Davidson et al., 2016; Matsumura et al., 2018) need further experiments.
		• Camera blinding attacks have been successfully demonstrated on CAVS (Petit et al., 2015; Yan et al., 2016). Petit et al.'s countermeasures (Petit et al., 2015) are the only current countermeasures against this attack model. Further studies to validate this defense strategy is needed. • Adversarial image attacks, as experimented in Eykholt et al. (2018); Kelarestaghi et al. (2019), have many proposed countermeasures in the literature, which can be found in Nicolae et al. (2018). Implementations of these countermeasures need to be validated. • There exists countermeasures against DDoS attacks on V2V networks (Blum and Eskandarian, 2006; Hubaux et al., 2004; Plossl et al., 2006). However, they are all based on theoretical frameworks and need validation in a realistic CAV environment.

by including detailed solutions for defined problems in the future. They hope that the whitepaper will become an international standard for the development of CAVs. Regarding security issues, the whitepaper (Wood et al., 2020) recommends two approaches:

- Using Secure Development Lifecycle (SDL), which is a process for integrating security into the product development and product maintenance processes. SDL practices are divided into preliminaries, development, and sustainment. Regarding preliminaries, a CAV development team is required to be sufficiently trained with knowledge of security issues, policies, procedures, and guidelines. Development includes security practices in software engineering, such as code review, penetration testing, and threat modeling. Sustainment practices ensure that CAVs continue to operate safely after release by having an effective incident response system and continuous updates.
- Regarding the machine learning models embedded in CAVs, the authors conducted a brief survey on the challenges of building safety-ensured machine learning models and suggested many guidelines. This section is presented in Appendix B of the whitepaper (Wood et al., 2020). In short, the guidelines involve the processes of selecting data for model training and testing, architecture design of models, model evaluation, and deployment and monitoring. Interestingly, we think that building defense mechanisms against the Adversarial Image attack model (section 3G) fits into the paradigm of data selection and model validation that the whitepaper describes.

Another coalition of Ford, Lyft, Uber, Volvo, and Waymo, named the Self-Driving Coalition for Safer Streets also presented several publications related to CAV's security on their website (Self-Driving Coalition, 2020). Most notable is Waymo's safety report titled "On the Road to Fully Self-Driving" Waymo (2020). The report claimed that Waymo applied approaches such as building redundant security measures for critical systems and limiting communication between critical systems. However, the specific implementation of these approaches was not described. We have not found related safety reports from other members of this coalition.

Regarding secure communication for CAN Bus, Guardknox Cyber Technologies Ltd. developed a patented security approach, named Communication Lockdown, to enforce a formally verified and deterministic configuration of communication among the CAN Bus Guardknox Cyber Technologies Ltd (2021). Guardknox Cyber Technologies Ltd. claims that this technology can provide zero false positives with minimal integration and no vehicular hardware modification.

From our observations, research and implementation of security issues are in the early stage of development among the CAV corporations. We have not found any strong connection between academic research and the industry's implementation of CAV-related security issues. There is no evidence to show that CAVs on the market have been updated to defend against the novel attack models that the research community has found.

5. Conclusion

Modern innovations of Connected and Autonomous Vehicles (CAVs) are transforming transportation and gaining a lot of public attention. While CAVs have enormous potentials to change human life, they pose significant security concerns and are vulnerable targets for attackers. Therefore, interest in the security of CAVs has been increasing rapidly. During the last decade, many attack models and defense strategies for CAVs have been discussed and experimented with. In this paper, we studied 189 papers from 2000 to 2020 to understand state-of-the-art security issues with CAVs, 131 of which directly discussed attack models and defense strategies. CAVs are prone to attacks on many of their components. These attacks can render CAVs out of service or give attackers control over CAVs. Some attack models are published recently and are seriously threatening to CAVs. We have presented readers with a comprehensive review of the security challenges of CAVs and corresponding state-of-the-art countermeasures. Furthermore, we organized the attack models based on their target components, access requirements, and attack motives. Finally, we have identified some research challenges and future directions that researchers can contribute to so that CAVs become secure and trustworthy to the general public.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

REFERENCES

Abboud K, Omar HA, Zhuang W. Interworking of DSRC and cellular network technologies for V2X communications: a survey. IEEE Trans. Veh. Technol. 2016;65(12):9457–70.

Alimohammadi M, Pouyan AA. Sybil attack detection using a low cost short group signature in VANET. In: 12th International Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC). IEEE; 2015. p. 23–8.

Amoozadeh M, Raghuramu A, Chuah CN, Ghosal D, Zhang HM, Rowe J, Levitt K. Security vulnerabilities of connected vehicle streams and their impact on cooperative driving. IEEE Commun. Mag. 2015;53(6):126–32.

Baccelli E, Clausen T, Wakikawa R. IPv6 operation for WAVE-Wireless access in vehicular environments. In: IEEE Vehicular Networking Conference. IEEE; 2010. p. 160–5.

Bailey T, Durrant-Whyte H. Simultaneous localization and mapping (SLAM): part II. IEEE Robot. Autom. Mag. 2006;13(3):108–17.

Bansal P, Kockelman KM. Forecasting americans' long-term adoption of connected and autonomous vehicle technologies. Transp. Res. Part A 2017;95:49–63.

Becker JC, Simon A. Sensor and navigation data fusion for an autonomous vehicle. In: Proceedings of the IEEE Intelligent Vehicles Symposium (Cat. No. 00TH8511). IEEE; 2000. p. 156–61.

Benmimoun A, Lowson M, Marques A, Giustiniani G, Parent M. Demonstration of advanced transport applications in citymobil project. Transp. Res. Rec. 2009;2110(1):9–17.

Biswas S, Tatchikou R, Dion F. Vehicle-to-vehicle wireless communication protocols for enhancing highway traffic safety. IEEE Commun. Mag. 2006;44(1):74–82.

Blanch J, Walter T, Enge P, Lee Y, Pervan B, Rippl M, Spletter A. Advanced RAIM user algorithm description: integrity support message processing, fault detection, exclusion, and protection level calculation. In: Proceedings of the 25th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2012); 2012. p. 2828–49.

Blum JJ, Eskandarian A. Fast, robust message forwarding for inter-vehicle communication networks. In: IEEE Intelligent Transportation Systems Conference. IEEE; 2006. p. 1418–23.

Bohm A, Jonsson M. Supporting real-time data traffic in safety-critical vehicle-to-infrastructure communication. In: 33rd IEEE Conference on Local Computer Networks (LCN). IEEE; 2008. p. 614–21.

Breuer JJ, Faulhaber A, Frank P, Gleissner S. Real world safety benefits of brake assistance systems. 20th International Technical Conference on the Enhanced Safety of Vehicles (ESV), 2007.

Brown RG. Receiver autonomous integrity monitoring. Global Position. Syst. 1996;2:143–65.

Brown TB, Mané D, Roy A, Abadi M, Gilmer J. Adversarial patch arXivpreprint arXiv:1712.09665.

Buckman J, Roy A, Raffel C, Goodfellow I. Thermometer encoding: one hot way to resist adversarial examples. 6th International Conference on Learning Representations, ICLR, 2018.

Buehler W.E., Whitson R.M., Lewis M.J.. Airborne radar jamming system. 2014. US Patent 8,830,112.

Cao Y, Xiao C, Cyr B, Zhou Y, Park W, Rampazzi S, Chen QA, Fu K, Mao ZM. Adversarial sensor attack on LiDAR-based perception in autonomous driving. In: ACM SIGSAC Conference on Computer and Communications Security. ACM; 2019. p. 2267–81.

Chang J, Hatcher G, Hicks D, Schneeberger J, Staples B, Sundarajan S, Vasudevan M, Wang P, Wunderlich K, et al. In: Technical Report. Estimated Benefits of Connected Vehicle Applications: Dynamic Mobility Applications, AERIS, V2I safety, and Road Weather Management Applications. United States Department of Transportation; 2015.

Chattopadhyay A, Lam KY. Security of autonomous vehicle as a cyber-physical system. In: 2017 7th International Symposium on Embedded Computing and System Design (ISED). IEEE; 2017. p. 1–6.

Chauhan R.. A Platform for False Data Injection in Frequency Modulated Continuous Wave Radar. Master's thesis; Utah State University; 2014.

Checkoway S, McCoy D, Kantor B, Anderson D, Shacham H, Savage S, Koscher K, Czeskis A, Roesner F, Kohno T, et al. Comprehensive experimental analyses of automotive attack surfaces, 4; 2011. p. 447–62.

Chi C.Y.. Automatic safety driving distance control device for a vehicle. 1992. US Patent 5,165,497.

Chim TW, Yiu SM, Hui LCK, Li VOK. Security and privacy issues for inter-vehicle communications in VANETs. In: 6th IEEE Annual Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks Workshops. IEEE; 2009. p. 1–3.

Cho KT, Shin KG. Fingerprinting electronic control units for vehicle intrusion detection. In: 25th USENIX Security Symposium; 2016. p. 911–27.

Choi M, Blanch J, Walter T, Enge P. Advanced RAIM demonstration using four months of ground data. In: Proceedings of the 2011 International Technical Meeting of The Institute of Navigation; 2011. p. 279–84.

Christensen L., Dannberg D.. Ethical hacking of IoT devices: OBD-II dongles. http://www.diva-portal.org/smash/get/diva2:1333813/FULLTEXT01.pdf; 2019.

Coffed J. In: Technical Report. The Threat of GPS Jamming: The Risk to an Information Utility. Harris Corporation; 2014.

Centre for Connected and Autonomous Vehicles. UK Connected & Autonomous Vehicle Research & Development Projects 2018. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/737778/ccav-research-and-development-projects.pdf.

Corrigan S. In: Technical Report. Introduction to the Controller Area Network (CAN). Texas Instruments; 2002.

Davidson D, Wu H, Jellinek R, Singh V, Ristenpart T. In: 10th USENIX Workshop on Offensive Technologies (WOOT 16). Controlling UAVs with sensor input spoofing attacks; 2016.

Douligeris C, Mitrokotsa A. DDoS attacks and defense mechanisms: classification and state-of-the-art. Comput. Netw. 2004;44(5):643–66.

Durrant-Whyte H, Bailey T. Simultaneous localization and mapping: part I. IEEE Robot. Autom. Mag. 2006;13(2):99–110.

Dutta RG, Guo X, Zhang T, Kwiat K, Kamhoua C, Njilla L, Jin Y. Estimation of safe sensor measurements of autonomous system under attack. In: Proceedings of the 54th Annual Design Automation Conference 2017; 2017. p. 1–6.

Dziugaite G.K., Ghahramani Z., Roy D.M.. A study of the effect of JPG compression on adversarial images. arXiv preprint arXiv:1608.00853

Ekedebe N, Yu W, Song H, Lu C. On a simulation study of cyber attacks on vehicle-to-infrastructure communication (V2I) in Intelligent Transportation System (ITS). In: International Society for Optics and Photonics, 9497. SPIE; 2015. p. 96–107. doi:101117/122177465.

El-Sheimy N, Shin EH, Niu X. Kalman filter face-off: extended vs. unscented Kalman filters for integrated GPS and MEMS inertial. Inside GNSS 2006;1(2):48–54.

European Parliament, Council of the European Union. Regulation (EC) No 661/2009 of the European Parliament and of the Council of 13 July 2009 concerning type-approval requirements for the general safety of motor vehicles, their trailers and systems, components and separate technical units intended therefor. Official Journal of the European Union; 2009.

Eykholt K, Evtimov I, Fernandes E, Li B, Rahmati A, Xiao C, Prakash A, Kohno T, Song D. Robust physical-world attacks on deep learning visual classification. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition; 2018. p. 1625–34.

Fairfield N, Urmson C. Traffic light mapping and detection. In: IEEE International Conference on Robotics and Automation. IEEE; 2011. p. 5421–6.

Figueiredo L, Jesus I, Machado JAT, Ferreira JR, De Carvalho JLM. Towards the development of intelligent transportation systems. In: IEEE Intelligent Transportation Systems (ITSC) (Cat. No. 01TH8585). IEEE; 2001. p. 1206–11.

Fowler DS, Cheah M, Shaikh SA, Bryans J. Towards a testbed for automotive cybersecurity. In: IEEE International Conference on Software Testing, Verification and Validation (ICST). IEEE; 2017. p. 540–1.

Fox News. Zapped: driver fined thousands for using laser jammer. [Online]. Available: https://www.foxnews.com/auto/zapped-driver-fined-thousands-for-using-laser-jammer. Accessed: July 11.

Gmiden M, Gmiden MH, Trabelsi H. An intrusion detection method for securing in-vehicle CAN bus. In: 17th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA). IEEE; 2016. p. 176–80.

Goodfellow I.J., Shlens J., Szegedy C.. Explaining and harnessing adversarial examples. arXiv preprint arXiv:1412.6572

Gopalakrishna D, Garcia V, Ragan A, English T, Zumpf S, Young R, Ahmed M, Kitchener F, Serulle NU, Hsu E, et al. In: Technical Report. Connected Vehicle Pilot Deployment Program Phase 1, Concept of Operations (ConOps), ICF/Wyoming. United States Department of Transportation, Intelligent Transportation Systems Joint Program Office; 2015.

Greco M, Gini F, Farina A. Combined effect of phase and RGPO delay quantization on jamming signal spectrum. In: IEEE International Radar Conference. IEEE; 2005. p. 37–42.

Greco M, Gini F, Farina A. Radar detection and classification of jamming signals belonging to a cone class. IEEE Trans. Signal Process. 2008;56(5):1984–93.

Grover J, Gaur MS, Laxmi V, Prajapati NK. A sybil attack detection approach using neighboring vehicles in VANET. In: Proceedings of the 4th International Conference on Security of Information and Networks. ACM; 2011. p. 151–8.

Guo C., Rana M., Cisse M., Van Der Maaten L.. Countering adversarial images using input transformations. arXiv preprint arXiv:1711.00117

Guardknox Cyber Technologies Ltd. The Communication Lockdown Methodology: Fighter Jet Cybersecurity for Connected Vehicles. https://learn.guardknox.com/communication-lockdown-whitepaper.

Haider Z, Khalid S. Survey on effective GPS spoofing countermeasures. In: Sixth International Conference on Innovative Computing Technology (INTECH). IEEE; 2016. p. 573–7.

Halabi J, Artail H. A lightweight synchronous cryptographic hash chain solution to securing the vehicle CAN bus. In: IEEE International Multidisciplinary Conference on Engineering Technology (IMCET). IEEE; 2018. p. 1–6.

Hasbullah H, Soomro IA, et al. Denial of service (DOS) attack and its possible solutions in VANET. Int. J. Electron. Commun. Eng. 2010;4(5):813–17.

Hecht J. Lidar for self-driving cars. Opt. Photonics News 2018;29(1):26–33.

van der Heijden RW, Dietzel S, Leinmüller T, Kargl F. Survey on misbehavior detection in cooperative intelligent transportation systems. IEEE Commun. Surv. Tutor. 2018;21(1):779–811.

Helfrick A. Question: alternate position, navigation timing, APNT? Answer: ELORAN. IEEE/AIAA 33rd Digital Avionics Systems Conference (DASC). IEEE, 2014. 3C3-1–3C3-9

Hewitson S, Wang J. GNSS receiver autonomous integrity monitoring (RAIM) performance analysis. GPS Solut. 2006;10(3):155–70.

Hillel AB, Lerner R, Levi D, Raz G. Recent progress in road and lane detection: a survey. Mach. Vis. Appl. 2014;25(3):727–45.

Hoppe T, Kiltz S, Dittmann J. Security threats to automotive CAN networks–practical examples and selected short-term countermeasures. In: International Conference on Computer Safety, Reliability, and Security. Springer; 2008. p. 235–48.

Hu H, Wei N. A study of GPS jamming and anti-jamming, 1. IEEE; 2009. p. 388–91.

Hubaux JP, Capkun S, Luo J. The security and privacy of smart vehicles. IEEE Secur. Priv. 2004(3):49–55.

Hulshof W, Knight I, Edwards A, Avery M, Grover C. Autonomous emergency braking test results. In: Proceedings of the 23rd International Technical Conference on the Enhanced Safety of Vehicles (ESV); 2013. p. 1–13.

Hunkeler U, Colli-Vignarelli J, Dehollain C. Effectiveness of GPS-jamming and counter-measures. In: International Conference on Localization and GNSS. IEEE; 2012. p. 1–4.

IEEE Standards Association. 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 80211-2016 (Revision of IEEE Std 80211-2012)2010.

Ishida S, Gayko JE. Development, evaluation and introduction of a lane keeping assistance system. In: IEEE Intelligent Vehicles Symposium. IEEE; 2004. p. 943–4.

Ishtiaq Roufa RM, Mustafaa H, Travis Taylora SO, Xua W, Gruteserb M, Trappeb W, Seskarb I. Security and privacy vulnerabilities of in-car wireless networks: a tire pressure monitoring system case study. In: 19th USENIX Security Symposium; 2010. p. 11–13.

Jiang W, Li H, Liu S, Luo X, Lu R. Poisoning and evasion attacks against deep learning algorithms in autonomous vehicles. IEEE Trans. Veh. Technol. 2020;69(4):4439–49.

Jitpakdee R, Maneewarn T. Neural networks terrain classification using inertial measurement unit for an autonomous vehicle. In: SICE Annual Conference. IEEE; 2008. p. 554–8.

Jo K, Kim J, Kim D, Jang C, Sunwoo M. Development of autonomous car—Part II: a case study on the implementation of an autonomous driving system based on distributed architecture. IEEE Trans. Ind. Electron. 2015;62(8):5119–32.

Joy J, Gerla M. Internet of vehicles and autonomous connected car-privacy and security issues. In: 2017 26th International Conference on Computer Communication and Networks (ICCCN). IEEE; 2017. p. 1–9.

Jungk B, Bhasin S. Don't fall into a trap: physical side-channel analysis of chacha20-poly1305. In: Design, Automation & Test in Europe Conference & Exhibition (DATE), 2017. IEEE; 2017. p. 1110–15.

Kalmeshwar M, Prasad KSN. Development of on-board diagnostics for car and it's integration with android mobile. In: 2nd International Conference on Computational Systems and Information Technology for Sustainable Solution (CSITSS). IEEE; 2017. p. 1–6.

Kapoor P, Vora A, Kang KD. Detecting and mitigating spoofing attack against an automotive radar. In: IEEE 88th Vehicular Technology Conference (VTC-Fall). IEEE; 2018. p. 1–6.

Kassakian JG, Wolf HC, Miller JM, Hurton CJ. Automotive electrical systems circa 2005. IEEE Spectr. 1996;33(8):22–7.

Kelarestaghi KB, Foruhandeh M, Heaslip K, Gerdes R. Intelligent transportation system security: Impact-oriented risk assessment of in-vehicle networks. IEEE Intell. Transp. Syst. Mag. 2019;13(2):1.

Kenney JB. Dedicated short-range communications (DSRC) standards in the United States. Proc. IEEE 2011;99(7):1162–82.

Kitchener F, English T, Gopalakrishna D, Garcia V, Ragan A, Young R, Ahmed M, Stephens D, Serulle NU, et al. In: Technical Report. Connected Vehicle Pilot Deployment Program Phase 2, Data Management Plan-Wyoming. United States Department of Transportation, Intelligent Transportation Systems Joint Program Office; 2017.

Kos J, Fischer I, Song D. Adversarial examples for generative models. In: IEEE Security and Privacy Workshops (SPW). IEEE; 2018. p. 36–42.

Koscher K, Czeskis A, Roesner F, Patel S, Kohno T, Checkoway S, McCoy D, Kantor B, Anderson D, Shacham H, et al. Experimental security analysis of a modern automobile. In: IEEE Symposium on Security and Privacy. IEEE; 2010. p. 447–62.

Krasner N.F.. Method and apparatus for adaptively processing GPS signals in a GPS receiver. 2000. US Patent 6,133,873.

Leinmuller T, Schoch E, Kargl F. Position verification approaches for vehicular ad hoc networks. IEEE Wirel. Commun. 2006;13(5):16–21.

Levinson J, Askeland J, Dolson J, Thrun S. Traffic light mapping, localization, and state detection for autonomous vehicles. In: IEEE International Conference on Robotics and Automation. IEEE; 2011. p. 5784–91.

Lin CE, Li CC, Yang SH, Lin Sh, Lin Cy. Development of on-line diagnostics and real time early warning system for vehicles. In: Sensors for Industry Conference. IEEE; 2005. p. 45–51.

Lin CW, Sangiovanni-Vincentelli A. Cyber-security for the controller area network (CAN) communication protocol. In: International Conference on Cyber Security. IEEE; 2012. p. 1–7.

Loh R, Fernow JP. Integrity monitoring requirements for FAA's GPS wide-area augmentation system (WAAS). In: IEEE Position, Location and Navigation Symposium. IEEE; 1994. p. 629–36.

Lothes RN, Szymanski MB, Wiley RG. Radar Vulnerability to Jamming. Artech House; 1990.

Lu G, Zeng D, Tang B. Anti-jamming filtering for DRFM repeat jammer based on stretch processing, 1. IEEE; 2010. p. V1–78.

Lu J., Sibai H., Fabry E., Forsyth D.. No need to worry about adversarial examples in object detection in autonomous vehicles. arXiv preprint arXiv:1707.03501

Mahmud SM, Shanker S, Hossain I. Secure software upload in an intelligent vehicle via wireless communication links. In: IEEE Proceedings. Intelligent Vehicles Symposium. IEEE; 2005. p. 588–93.

Man Y, Li M, Gerdes R. In: IEEE Symposium on Security and Privacy. Poster: perceived adversarial examples; 2019.

Marstorp G., Lindström H.. Security Testing of an OBD-II Connected IoT Device. http://autosec.se/wp-content/uploads/2018/05/Marstorp-Lindstrom-Security-Testing-of-an-OBD-II-Connected-IoT-Device.pdf; 2017.

Matsumoto T, Hata M, Tanabe M, Yoshioka K, Oishi K. A method of preventing unauthorized data transmission in controller area network. In: IEEE 75th Vehicular Technology Conference (VTC Spring). IEEE; 2012. p. 1–5.

Matsumura R, Sugawara T, Sakiyama K. A secure LiDAR with AES-based side-channel fingerprinting. In: Sixth International Symposium on Computing and Networking Workshops (CANDARW). IEEE; 2018. p. 479–82.

Meng Q, Hsu LT, Xu B, Luo X, El-Mowafy A. A gps spoofing generator using an open sourced vector tracking-based receiver. Sensors 2019a;19(18):3993.

Meng Q, Liu J, Zeng Q, Feng S, Xu R. Improved ARAIM fault modes determination scheme based on feedback structure with probability accumulation. GPS Solut. 2019b;23(1):16.

Miller C, Valasek C. Adventures in automotive networks and control units. In: Def Con 21 Archive; 2013. p. 260–4.

Miller C, Valasek C. A survey of remote automotive attack surfaces. In: Black Hat USA; 2014. p. 94.

Miyato T., Maeda S., Koyama M., Nakae K., Ishii S.. Distributional smoothing with virtual adversarial training. arXiv preprint arXiv:1507.00677

Montgomery PY. Receiver-autonomous spoofing detection: experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer. Radionavigation Laboratory Conference Proceedings, 2011.

Moosavi-Dezfooli SM, Fawzi A, Fawzi O, Frossard P. Universal adversarial perturbations. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition; 2017. p. 1765–73.

Mukhopadhyay M, Sarkar BK, Chakraborty A. Augmentation of anti-jam GPS system using smart antenna with a simple DOA estimation algorithm. Prog. Electromagn. Res. 2007;67:231–49.

Mulliner C, Michéle B. Read it twice! a mass-storage-based TOCTTOU attack. In: 6th USENIX Workshop on Offensive Technologies (WOOT 12); 2012. p. 105–12.

Müter M, Asaj N. Entropy-based anomaly detection for in-vehicle networks. In: IEEE Intelligent Vehicles Symposium (IV). IEEE; 2011. p. 1110–15.

Narain S, Ranganathan A, Noubir G. Security of GPS/INS based on-road location tracking systems. In: IEEE Symposium on Security and Privacy (SP). IEEE; 2019. p. 587–601.

New York City Department of Transportation. NYC Connected Vehicle Project For Safer Transportation. https://cvp.nyc/; a.

Nicolae MI, Sinn M, Tran MN, Buesser B, Rawat A, Wistuba M, Zantedeschi V, Baracaldo N, Chen B, Ludwig H, Molloy I, Edwards B. Adversarial robustness toolbox v1.0.1. Comput. Res. Repos. (CoRR) 2018 arXiv:1807.01069.

Nilsson DK, Larson UE. Secure firmware updates over the air in intelligent vehicles. In: ICC Workshops - IEEE International Conference on Communications Workshops. IEEE; 2008. p. 380–4.

Nilsson DK, Larson UE, Jonsson E. Creating a secure infrastructure for wireless diagnostics and software updates in vehicles. In: International Conference on Computer Safety, Reliability, and Security. Springer; 2008a. p. 207–20.

Nilsson DK, Larson UE, Jonsson E. Efficient in-vehicle delayed data authentication based on compound message authentication codes. In: IEEE 68th Vehicular Technology Conference. IEEE; 2008b. p. 1–5.

Nilsson DK, Sun L, Nakajima T. A framework for self-verification of firmware updates over the air in vehicle ECUs. In: IEEE Globecom Workshops. IEEE; 2008c. p. 1–5.

Nouri M, Mivehchy M, Sabahi MF. Target recognition based on phase noise of received laser signal in LiDAR jammer. Chin. Opt. Lett. 2017;15(10):100302.

van Nunen E, Kwakkernaat MR, Ploeg J, Netten BD. Cooperative competition for future mobility. IEEE Trans. Intell. Transp. Syst. 2012;13(3):1018–25.

O'Hanlon BW, Psiaki ML, Bhatti JA, Shepard DP, Humphreys TE. Real-time GPS spoofing detection via correlation of encrypted signals. Navigation 2013;60(4):267–78.

Omachi M, Omachi S. Traffic light detection with color and edge information. In: 2nd IEEE International Conference on Computer Science and Information Technology. IEEE; 2009. p. 284–7.

Pace PE. Detecting and Classifying low Probability of Intercept Radar. Artech House; 2009.

Parkinson S, Ward P, Wilson K, Miller J. Cyber threats facing autonomous and connected vehicles: Future challenges. IEEE Trans. Intell. Transp. Syst. 2017;18(11):2898–915.

Pathre A. Identification of malicious vehicle in VANET environment from DDoS attack. J. Global Res. Comput. Sci. 2013;4(6):30–4.

Pathre A, Agrawal C, Jain A. A novel defense scheme against DDOS attack in VANET. In: Tenth International Conference on Wireless and Optical Communications Networks (WOCN). IEEE; 2013. p. 1–5.

Pattinson M, Dumville M, Ying Y, Fryganiotis D, Bhuiyan MZH, Thombre S, Kuusniemi H, Waern A, Eliardsson P, Hill S, Manikundalam V, Lee S, Gonzalez J. Standardization of GNSS threat reporting and receiver testing through international knowledge exchange, experimentation and exploitation [STRIKE3] - draft standards for receiver testing. Eur. J. Navig. 2017;15:4–8.

Petit J, Shladover SE. Potential cyberattacks on automated vehicles. IEEE Trans. Intell. Transp. Syst. 2014;16(2):546–56.

Petit J, Stottelaar B, Feiri M, Kargl F. Remote attacks on automated vehicles sensors: experiments on camera and LiDAR, 11; 2015.

Petovello MG, Cannon ME, Lachapelle G, Wang J, Wilson C, Salychev OS, Voronov VV. Development and testing of a real-time GPS/INS reference system for autonomous automobile navigation, 1; 2001. p. 2634–41.

Pilipovic M, Spasojevic D, Velikic I, Teslic N. Toward intelligent driver-assist technologies and piloted driving: overview, motivation and challenges. Proceedings of the X International Symposium on Industrial Electronics (INDEL 14), 2014.

Plossl K, Nowey T, Mletzko C. Towards a security architecture for vehicular ad hoc networks. In: First International Conference on Availability, Reliability and Security (ARES'06). IEEE; 2006. p. 8.

Prathap V., Rachumallu A.. Penetration Testing of Vehicle ECUs. Master's thesis; Chalmers University of Technology; 2013.

Psiaki ML, O'hanlon BW, Powell SP, Bhatti JA, Wesson KD, Humphreys TE. Gnss spoofing detection using two-antenna differential carrier phase. Radionavigation Laboratory Conference Proceedings, 2014.

Purwar A, Joshi D, Chaubey VK. GPS signal jamming and anti-jamming strategy atheoretical analysis. In: IEEE Annual India Conference (INDICON). IEEE; 2016. p. 1–6.

Qian M, Jianye L, Qinghua Z, Shaojun F, Rui XU. Impact of one satellite outage on ARAIM depleted constellation configurations. Chin. J. Aeronaut. 2019;32(4):967–77.

Rawat A, Sharma S, Sushil R. VANET: Security attacks and its possible solutions. J. Inf. Oper. Manag. 2012;3(1):301.

Regulus Cyber LTD. Tesla model 3 spoofed off the highway regulus navigation system hack causes car to turn on its own. [Online]. Available: https://www.regulus.com/blog/tesla-model-3-spoofed-off-the-highway-regulus-researches-hack-navigation-system-causing-car-to-steer-off-road/. Accessed: July 11, 2020.

Reed J.C.. Vehicle back-up and parking aid radar system. 2003. US Patent 6,583,753.

Roome SJ. Digital radio frequency memory. Electron. Commun. Eng. J. 1990;2(4):147–53.

SAE International. Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles. https://www.sae.org/standards/content/j3016_201806/; 2018.

Seshadri A, Luk M, Perrig A, van Doorn L, Khosla P. SCUBA: secure code update by attestation in sensor networks. In: Proceedings of the 5th ACM Workshop on Wireless Security. ACM; 2006. p. 85–94.

Self-Driving Coalition. Research Publications. https://www.selfdrivingcoalition.org/resources/research;. Accessed June 2020.

Sharath Yadav DH, Ansari A. In: Technical Report. Autonomous Vehicles Camera Blinding Attack Detection Using Sequence Modelling and Predictive Analytics. SAE International. Available at; 2020. doi:10.4271/2020-01-0719.

Shepard DP, Humphreys TE, Fansler AA. Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks. Int. J. Crit. Infrastruct. Prot. 2012;5(3-4):146–53.

Shin H, Kim D, Kwon Y, Kim Y. Illusion and dazzle: adversarial optical channel exploits against LiDARs for automotive applications. In: International Conference on Cryptographic Hardware and Embedded Systems. Springer; 2017. p. 445–67.

Shin K.G., Cho K.T.. Fingerprinting electronic control units for vehicle intrusion detection. 2017. US Patent App. 15/472,861.

Shoukry Y, Martin P, Yona Y, Diggavi S, Srivastava M. PyCRA: physical challenge-response authentication for active sensors under spoofing attacks. In: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. ACM; 2015. p. 1004–15.

Siddiqui AS, Gui Y, Plusquellic J, Saqib F. Secure communication over CANBus. In: 2017 IEEE 60th International Midwest Symposium on Circuits and Systems (MWSCAS). IEEE; 2017. p. 1264–7.

Singh PK, Jha SK, Nandi SK, Nandi S. ML-based approach to detect DDoS attack in V2I communication under SDN architecture. In: TENCON IEEE Region 10 Conference. IEEE; 2018. p. 0144–9.

Singh S, Kingsley K, Chen CL. In: Technical Report. Tire Pressure Maintenance—A Statistical Investigation. National Highway Traffic Safety Administration; 2009.

Sitawarin C., Bhagoji A.N., Mosenia A., Chiang M., Mittal P.. DARTS: Deceiving Autonomous Cars with Toxic Signs. arXiv preprint arXiv:1802.06430

Stott GF. In: IEE Colloquium on Signal Processing in Electronic Warfare. Digital modulation for radar jamming. IET; 1994. 1–1

Stottelaar B.G.B.. Practical Cyber-Attacks on Autonomous Vehicles. Master's thesis; University of Twente; 2015.

Sun T, Tang S, Wang J, Zhang W. A robust lane detection method for autonomous car-like robot. In: Fourth International Conference on Intelligent Control and Information Processing (ICICIP). IEEE; 2013. p. 373–8.

Sun W, Amin MG. A self-coherence anti-jamming GPS receiver. IEEE Trans. Signal Process. 2005;53(10):3910–15.

Suzuki Y, Hori T, Kitazumi T, Aoki K, Fukao T, Sugimachi T. In: 7th IFAC Symposium on Advances in Automotive Control. Development of automated platooning system based on heavy duty trucks; 2010.

Szegedy C., Zaremba W., Sutskever I., Bruna J., Erhan D., Goodfellow I., Fergus R.. Intriguing properties of neural networks. arXiv preprint arXiv:1312.6199

Tampa Hillsborough Expressway Authority. THEA Connected Vehicle Pilot. https://www.tampacvpilot.com/.

Thing VLL, Wu J. Autonomous vehicle security: a taxonomy of attacks and defences. In: IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE; 2016. p. 164–70.

Tippenhauer NO, Pöpper C, Rasmussen KB, Capkun S. On the requirements for successful GPS spoofing attacks. In: 18th ACM Conference on Computer and Communications Security. ACM; 2011. p. 75–86.

Tomlinson A, Bryans J, Shaikh SA. In: 2nd ACM Computer Science in Cars Symposium. Towards viable intrusion detection methods for the automotive controller area network; 2018.

Twitchell R.W., Taylor A.. GPS location for mobile phones using the internet. 2001. US Patent 6,222,483.

Tyree Z, Bridges RA, Combs FL, Moore MR. Exploiting the shape of CAN data for in-vehicle intrusion detection. In: IEEE 88th Vehicular Technology Conference (VTC-Fall). IEEE; 2018. p. 1–5.

Uhlemann E. Autonomous vehicles are connecting...[connected vehicles]. IEEE Veh. Technol. Mag. 2015;10(2):22–5.

Uhlir D, Sedlacek P, Hosek J. Practial overview of commercial connected cars systems in Europe. In: 9th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT). IEEE; 2017. p. 436–44.

Uselmann D.J., Uselmann L.M.. Sonic blind spot monitoring system. 2004. US Patent 6,727,808.

University of Warwick. Cyber security of connected autonomous vehicles trialled. [Online]. Available: https://techxplore.com/news/2019-09-cyber-autonomous-vehicles-trialled.html. Accessed: July 11.

Van Dyke KL. RAIM availability for supplemental GPS navigation. Navigation 1992;39(4):429–43.

Van Herrewege A, Singelee D, Verbauwhede I. In: ECRYPT Workshop on Lightweight Cryptography. CANAuth-a simple, backward compatible broadcast authentication protocol for CAN bus; 2011.

Waymo LLC. Waymo safety report - on the road to fully self-driving. [Online]. Available: https://storage.googleapis.com/sdc-prod/v1/safety-report/Safety%20Report%202018.pdf. Accessed: July 11, 2020.

Wandinger U. Introduction to LiDAR. In: Weitkamp C, editor. In: LiDAR: Range-Resolved Optical Remote Sensing of the Atmosphere. Springer; 2005. p. 1–18.

Wang Q, Zhang Y, Xu Y, Hao L, Zhang Z, Qiao T, Zhao Y. Pseudorandom modulation quantum secured LiDAR. Optik 2015;126(22):3344–8.

Wang Y, Chao WL, Garg D, Hariharan B, Campbell M, Weinberger KQ. Pseudo-LiDAR from visual depth estimation: bridging the gap in 3d object detection for autonomous driving. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition; 2019. p. 8445–53.

Warner JS, Johnston RG. GPS spoofing countermeasures. Homel. Secur. J. 2003;25(2):19–27.

Watfa M. Advances in Vehicular Ad-Hoc Networks: Developments and Challenges: Developments and Challenges. IGI Global; 2010.

West DM. Moving Forward: Self-Driving Vehicles in China, Europe, Japan, Korea, and the United States. Center for Technology Innovation at Brookings; 2016.

Whyte W, Weimerskirch A, Kumar V, Hehn T. A security credential management system for V2V communications. In: IEEE Vehicular Networking Conference. IEEE; 2013. p. 1–8.

Williams M. In: IEE Colloquium on Driver Information. Prometheus-the european research programme for optimising the road transport system in europe. IET; 1988. 1–1

William J. Hughes Technical Center. In: Technical Report. Global Positioning System (GPS) Standard Positioning service (SPS) Performance Analysis Report. Federal Aviation Administration; 2014.

Wolf M, Weimerskirch A, Paar C. Secure in-vehicle communication. In: Embedded Security in Cars. Springer; 2006. p. 95–109.

Woo S, Jo HJ, Lee DH. A practical wireless attack on the connected car and security protocol for in-vehicle CAN. IEEE Trans. Intell. Transp. Syst. 2014;16(2):993–1006.

Wood M., Robbel P., Maass M., Tebbens R.D., Meijs M., Harb M., Schlicht P.. Safety first for automated driving. [Online]. Available: https://newsroom.intel.com/wp-content/uploads/sites/11/2019/07/Intel-Safety-First-for-Automated-Driving.pdf, July 11.

Wyglinski AM, Huang X, Padir T, Lai L, Eisenbarth TR, Venkatasubramanian K. Security of autonomous systems employing embedded computing and sensors. IEEE Micro 2013;33(1):80–6.

Wyoming Department of Transportation. Wyoming DOT Connected Vehicle Pilot. https://wydotcvp.wyoroad.info/; b.

Xu Q, Mak T, Ko J, Sengupta R. Vehicle-to-vehicle safety messaging in DSRC. In: Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks. ACM; 2004. p. 19–28.

Xu W., Evans D., Qi Y.. Feature squeezing: Detecting adversarial examples in deep neural networks. arXiv preprint arXiv:1704.01155

Yadav A, Bose G, Bhange R, Kapoor K, Iyengar NC, Caytiles RD. Security, vulnerability and protection of vehicular on-board diagnostics. Int. J. Secur. Appl. 2016;10(4):405–22.

Yan C, Xu W, Liu J. In: DEF CON 24. Can you trust autonomous vehicles: contactless attacks against sensors of self-driving vehicle; 2016.

Yang Y, Xu J. GNSS receiver autonomous integrity monitoring (RAIM) algorithm based on robust estimation. Geodesy Geodyn. 2016;7(2):117–23.

Zamfir S, Drosescu R. Automotive black box and development platform used for traffic risks evaluation and mitigation. In: SIAR International Congress of Automotive and Transport Engineering: Science and Management of Automotive and Transportation Engineering. Springer; 2019. p. 426–38.

Zantedeschi V, Nicolae MI, Rawat A. Efficient defenses against adversarial attacks. In: Proceedings of the 10th ACM Workshop on Artificial Intelligence and Security. ACM; 2017. p. 39–49.

Zeng KC, Liu S, Shu Y, Wang D, Li H, Dou Y, Wang G, Yang Y. All your GPS are belong to us: towards stealthy manipulation of road navigation systems. In: 27th USENIX Security Symposium (USENIX Security 18); 2018. p. 1527–44.

Zhang C, Lu R, Lin X, Ho PH, Shen X. An efficient identity-based batch verification scheme for vehicular sensor networks. In: 27th Conference on Computer Communications. IEEE; 2008. p. 246–50.

Zhang YD, Amin MG. Anti-jamming GPS receiver with reduced phase distortions. IEEE Signal Process. Lett. 2012;19(10):635–8.

Zhao M, Qin D, Guo R, Xu G. Efficient protection mechanism based on self-adaptive decision for communication networks of autonomous vehicles. Mob. Inf. Syst. 2020.

Minh Pham is a second-year Ph.D student at the department of Computer Science and Engineering, University of South Florida. Minh received a Master's degree in Statistics from the University of South Florida in 2018 and worked at the Center for Urban Transportation Research as a Research Associate before joining the Ph.D. program. He has published several articles about information systems in transportation.

Dr. Kaiqi Xiong is a Professor at the University of South Florida, affiliated with the Florida Center for Cybersecurity, the Department of Mathematics and Statistics, and the Department of Electrical Engineering. He received my Ph.D. degree in Computer Science from Department of Computer Science and his M.S. degree in Computer Engineering from Department of Electrical and Computer Engineering at the North Carolina State University, respectively. His Ph.D. thesis in Computer Science is ”Resource Optimization and Security in Distributed Computing” under the direction of Dr. Harry Perros. He also received a Ph.D. degree in Mathematics from Claremont Graduate School. He has published referred papers in leading journals and conferences, such as ACM Transactions on Sensor Networks, IEEE Transactions on Systems, Man, and Cybernetics, IEEE Transactions on Automatic Control, Journal of Parallel and Distributed Computing, Automatica, International Journal of Control, and Journal of Mathematics Analysis and Its Applications.