JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 39, 1265-1303 (2023)
DOI: 10.6688/JISE.202311_39(6).0003

Intelligent Connected Vehicle Security: Threats, Attacks and Defenses*

XIFENG WANG[1], LIMIN SUN[1], CHAO WANG[1], HONGSONG ZHU[1], LIAN ZHAO[2], SHUJIE YANG[1] AND CHANGQIAO XU[1,+]
[1]*State Key Laboratory of Networking and Switching Technology*
Beijing University of Posts and Telecommunications
Beijing, 10086 P.R. China
E-mail: {xifengwang; sjyang; cqxu}@bupt.edu.cn; {sunlimin; zhuhongsong}@iie.ac.cn; wangchao.andy@gmail.com
[2]*Department of Electrical, Computer, and Biomedical Engineering*
Ryerson University
Toronto, ON M5B 2K3, Canada
E-mail: l5zhao@ryerson.ca

The driving experience has improved significantly due to the advancement of automotive information and electronic technologies. Vehicles are becoming intelligent and connected, which are named Intelligent Connected Vehicles (ICVs). However, the security problems of ICVs have emerged, and the cyber security of ICVs has become one of the most popular research fields to avoid ICVs being invaded. To mitigate the security threats of ICVs and enhance their defense ability, we investigate ICV security from the aspects of vehicle attacks and defenses. We classify the attack and defense technologies in terms of the functions of various information subsystems in the ICV, *i.e.*, the ICV information perception system, in-vehicle communication system, control system, and V2X communication systems. We further highlight the security challenges and potential research directions to facilitate the development of better security mechanisms for ICV security.

Keywords: intelligent connected vehicle (ICV), vehicle attacks, vehicular security mechanisms, in-vehicle network, vehicle-to-everything

1. INTRODUCTION

The development of automobiles has dramatically improved people's lives, expanded the scope of people's activities, and enabled the normal operations of modern cities. In particular, when ICVs are widely spread, many new cyber-physical features are introduced into automotive systems. Since ICVs are configured with multiple communication technologies (*e.g.* vehicle-to-everything (V2X) communications), several information systems (*e.g.* Advanced Driver Assistant System (ADAS)) and several electronic devices (*e.g.* sensors and Electronic Control Units (ECUs)), many computerized systems can directly or indirectly connect to them via wireless channels or other interfaces, which

Received August 17, 2022; revised October 1, 2022, accepted October 20, 2022.
Communicated by Xiaohong Jiang.
+ Corresponding author.
* This work is supported by the National Natural Science Foundation of China under Grant Nos. 62225105, 61871048 and 61872253.

significantly enhance the automobile's intelligence and connectivity [1–3]. For instance, Tesla empowers its clients to control their car doors, air conditioners, and other functions remotely by using smartphones when the car is connected to the Internet.

Although integrating these new features into automobiles significantly improves the driving experience, information technologies also bring various security threats into the systems. Especially, the growing number of communication interfaces greatly increases the attack surfaces. Integrated smart systems also increase the number of codes and thus increase security vulnerabilities. If adversaries exploit one of these attack surfaces or vulnerabilities, the owner's privacy and life would be compromised.

Several cyber attack incidents on modern vehicles have happened recently. For example, hackers unlocked the Subaru Outback using short messages in Def Con 2011. In 2013 [4], Miller and Valasek, the famous white hats, attacked a Toyota Prius at high speed, disabling its braking system and controlling the steering. After the attack, they published a white paper about the details of the attack process. This white paper greatly arose the attention of cyber security researchers and vehicle manufacturers to vehicle cyber security. In Black Hat 2014 [5], Miller and Valasek announced another research report again, which contained the cyber security analysis of 20 vehicle models. And they took the in-vehicle infotainment system as an attack vector and launched an attack remotely on a Jeep Cherokee in the second year [6]. After that, vehicle cyber attacks increased year by year, and modern vehicles have become popular targets of hackers for various purposes.

Researchers have made great efforts to facilitate the research of vehicle security [7, 8]. For instance, Jia *et al*. [9] provided a survey on Social Internet of Vehicles (SIoV) location privacy preservation. Wu *et al*. [10] gave a deep discussion about vehicle intrusion detection and provided the design requirements and the drawbacks of the existing works. Zhao *et al*. [11] outlined the major attack entrances of ICV's cybersecurity and listed the corresponding six kinds of key protection strategies. Pham *et al*. [12] reviewed the security attacks and the corresponding countermeasures of CAN buses on ICVs.

A comparison between the existing survey papers and our work is shown in Table 1. Our work provides a comprehensive and systematic description and analysis of security issues from the perspectives of the components in ICVs, which is quite different from the existing work listed in Table 1. Moreover, we particularly provide an in-depth discussion about future research on security challenges and possible countermeasures in the ICV area. This survey aims to provide some basic guidance to new researchers in the ICV security area. At the same time, we try to conclude and analyze the current work to provide the details of vehicle attacks and defenses that are not shown in the previous papers. As far as we know, this is the first survey to discuss the security issues on ICVs referred to in the future Space-Air-Ground Integrated Network (SAGIN) from the perspective of attacks and defenses.

The survey is organized as follows, Section 2 summaries the in-vehicle perception system security and Section 3 in-vehicle network security is discussed. The control system security is presented in Section 4 to emphasize the security of in-vehicle important components. Section 5 describes the security of V2X communication systems. Section 6 suggests potential directions for future research, while Section 7 concludes the entire paper.

Table 1. Comparison of the existing surveys and ours.

Survey	Year	Focus	Our difference
[13]	2017	Details of the security and privacy issues of vehicular fog platform.	Systematic discussion of ICV attacks and defenses.
[14]	2017	The possible vulnerabilities of ICVs and their recommended protective mechanisms.	We provided additional discussion of vehicular control systems security.
[15]	2017	Key enabling technologies,opportunities and challenges of ICVs	A deeper discussion of ICV security issues rather than its enabling technology features
[16]	2020	Security issues with the ML-based applications in vehicular networks	Not only the ML related security issues of ICVs, including more enabling technology
[17]	2020	Discuss the recent attacks and possible mitigation approaches on self-driving cars.	We consider the security issues of ICVs in more depth through different taxonomies.
[16]	2020	Present an in-depth overview of the various challenges associated with the ML-based applications in vehicular networks.	We discuss more security topics of ICVs including the application of ML technology.
[18]	2020	Formulate a paper database with character clustering to guide the future research in ICV security area	Details of the security issues rather than the statistic characters
[12]	2021	Focus on the security of ICVs at component level.	We discuss more security topics of ICVs, *e.g*. ECU security.
[19]	2021	Focus on the security of CAN, including attacks and several state-of-art countermeasures	Not only CAN security issues but also other in-vehicle network protocols
[20]	2022	Present a survey on security and privacy issues by classifying them from a layer-based perspective inspired by the TCP/IP network model.	We use a different classifying method.

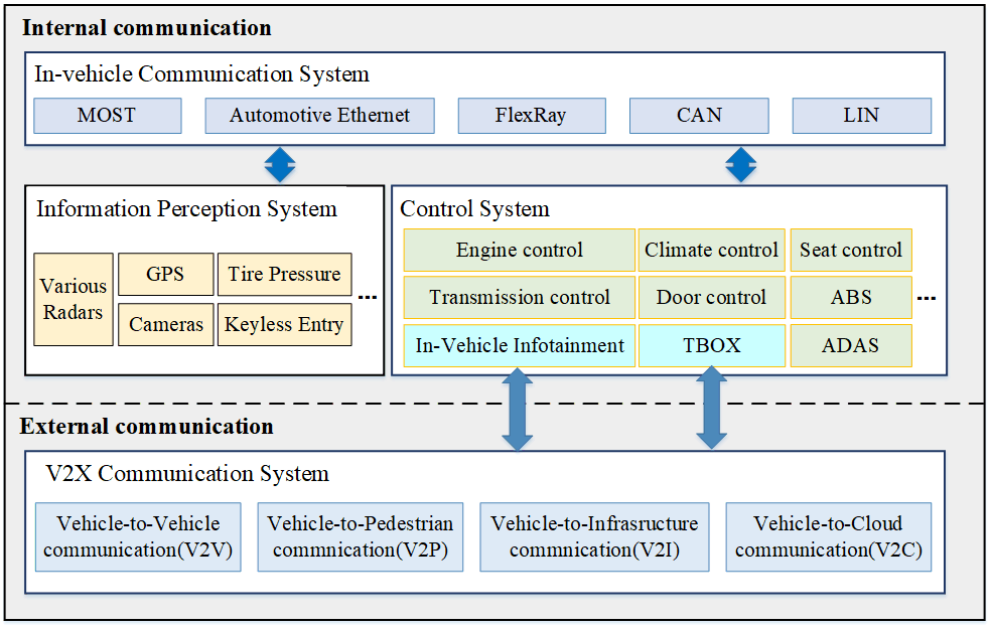

Fig. 1. ICV information system architecture.

2. SECURITY OF INFORMATION PERCEPTION SYSTEMS

The safe and convenient driving process of ICVs highly depends on the precise perception of environmental conditions. In particular, when the ICVs are in automatic cruising mode, it is vital to precisely sense the surroundings. In this paper, we uniformly call these onboard sensors information perception systems, which are the ”eyes” of ICVs. Once these information perception systems were blinded or maliciously controlled, the consequences could be disastrous. In this section, we discuss various attacks and defense strategies against information perception systems.

2.1 Security of Radar

Radar Systems are used to perceive the surrounding environment [21]. For example, mmWave radars are equipped onto ICVs to help with Adaptive Cruise Control (ACC), Blind Spot Detection (BSD) and Rear Collision Warning (RCW). Most automotive radars are designed without security considerations. Thus, they are the superior attack targets Although the attacks on vehicle radars are not common, considerable research and development efforts are necessary to defend against jamming and spoofing attacks in the future.

2.1.1 Attack analysis

- Radar Jamming: Attackers can launch radar jamming attacks by altering the frequency and amplitude of radio signals using signal generators before replaying,

which could blind the radar to the obstacles and cause a collision [22]. In DEF CON 2016, Yan *et al*. [23] launched practical jamming attacks against Tesla Model S by replaying the same waveform signals to the mmWave radar. However, It is difficult for malicious attackers to jam the automotive mmWave radars stealthily due to the fast movement of vehicles. And till now, we haven't found another publication about this kind of attack.

- Radar Spoofing: In contrast to jamming, the attackers launch radar spoofing attacks by altering the phase of the stored signals before they are rebroadcasted to the radar sensor. The purpose of this kind of attack is to confuse the distance to the surrounding objects. Besides the jamming attack, Yan *et al*. [23] also implement spoofing attacks by injecting bogus signals into a radar sensor on a Tesla Model S. Noriyuki *et al*. [24] propose a low-cost distance-spoofing attack on mmWave radars with a replica radar chipset and a single compact micro-controller board to tamper distance measured at the target radar.

2.1.2 Defense methods

- Defense for Radar Jamming: There are few types of research on the attack and defense methods of vehicle radar jamming except [23, 25]. And they consider that the jamming attack could be easily discovered by directly signal detection. Thus, this research direction is unlikely to become a research focus and hot spot in the area of ICVs.

- Defense for Radar Spoofing: The defense strategies against spoofing attacks should be timely detectable, malicious-signal-filtering and non-disruptive under most circumstances. Shoukry *et al*. [26] propose a challenge-response authentication to detect bogus signals. They suppose that adversaries cannot detect challenging signals in time and stop sending signals randomly. They determine whether there are malicious signals or not in terms of the noise threshold during a period with the Chi-square test. However, their work may cause safety problems such as adaptive cruise control and collision warning for random stopping. Meanwhile, it lacks experiments to be validated. And Kapoor *et al*. [27] discussed the detailed shortcomings of the above method. Yan *et al*. [23] suggest introducing randomness into the radio signals. They also propose to use several sensors reading to correct the measure values.

2.2 Security of GPS

GPS receivers and antennas are integrated in-vehicle navigation systems to provide position, velocity measurement, and high precise standard time information [28, 29]. This information is significant to realize vehicle positioning, tracking, navigating and timing (PNT) services. There is almost no theory difference between vehicular GPS and mobile GPS but some performance differences such as accuracy and speed. However, GPS signals are easy to be blocked, jammed, recorded and replayed with some radio transceivers just like other wireless communication technologies [30]. Due to the significance of the vehicle navigation system, it will be a disaster once the information tampers or the system is disabled.

2.2.1 Attack analysis

- GPS Jamming: Generally speaking, GPS jamming can be realized by strong radio signals which can confuse the GPS receiver to detect the legitimate signals. In addition, GPS jamming devices are easy to buy online. Although there are much work on GPS jamming attacks, there is scarcely anyone special for vehicles.

- GPS Spoofing: The spoofing attacks can be launched easily by using software defined radios (SDR) or hardware GPS simulators [29,31–33]. The adversaries firstly broadcast the same signals as the satellites' legitimate signals and then increase their power. Then, they broadcast the bogus GPS signals to overwhelm the legitimate signals to supply wrong position information to the vehicle [34, 35]. Further, the adversary can make a GPS simulator using USRP, BladeRF and HackRF to generate malicious GPS signals, which can be used to launch spoofing attacks.

2.2.2 Defense methods

- Defense for GPS Jamming: Similarly, there is rarely research special for defending automotive GPS jamming attacks. According to the existing GPS jamming defense methods, they should have the ability to detect and filter jamming signals timely to avoid disruption of service. Many GPS receivers have the function of anti-jamming measures to handle unintentional interference but not effective for intentional attacks [36]. Purwar *et al*. [28] used the Turbo Coding method to encode the GPS data. The receiver receives them along with the noise and jamming signals. However, because this method needs to modify the GPS satellites, it is not applicable to ICVs.

- Defense for GPS Spoofing: Receiver Autonomous Integrity Monitoring (RAIM) and spatial processing methods are effective defense methods against spoofing attacks [37, 38]. A secure countermeasure was proposed by Psiaki's team to discover the spoofing attacks and notify the corresponding defender [39]. The proposed method could detect the spoofing attacks since it traced the public known signals in a secure reference receiver and a defender receiver [40]. The spoofing attacks could also be detected by tracking modifications on power and time-related parameters [39, 41]. Deep learning methods were used to defend the GPS spoofing in recent years [42, 43]. However, there is not too much research on how to recover accurate navigation once an attack on GPS is discovered.

3. SECURITY OF IN-VEHICLE NETWORKS

In-vehicle networks connect various automotive systems or subsystems to provide drivers and passengers with entertainment, comfort, and safety. There are several types of in-vehicle networks, including CAN, LIN, FlexRay, MOST, and the emerging Automotive Ethernet. Fig. 2 shows an example of their technologies implemented in a vehicle. Different in-vehicle networks have different bitrates, deciding the data types transmitted and the applied scenarios in vehicles, which are detailed in [44, 45]. These in-vehicle networks not only facilitate ECUs cooperating with each other but also make it easier

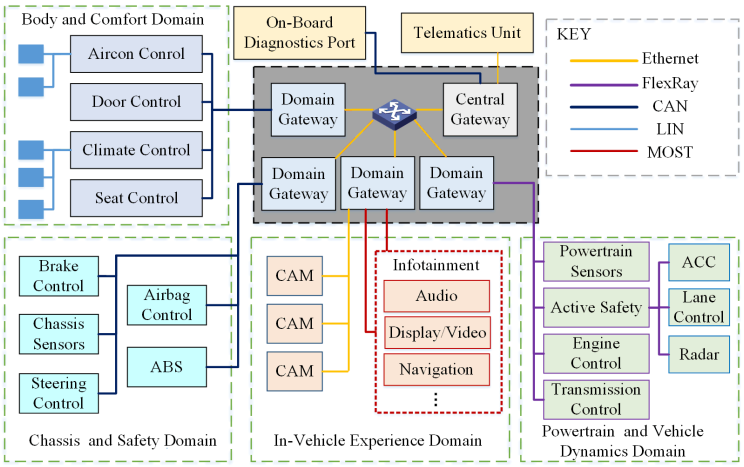

Fig. 2. Example of in-vehicle network topology.

to maintain the normal operation of in-vehicle systems. However, with the introduction of these networks, any ECUs can send commands to the other ECUs [8, 46–48]. Therefore, significant automotive components (such as engines, brakes, airbags, *etc.*) can be accessed by external adversaries, which breaks the physical isolation between a vehicle and the Internet. Any ECUs, which are subjected to a bus attack, will make a substantial contribution to the entire vehicle communication network threats. For example, Charlie Miller and Chris Valasek disclosed the details of an attack on a "Jeep Cherokee" car at the Black Hat Conference [49] in 2015. They chose the Uconnect entertainment system connected to the CAN bus as the breakthrough point [50]. If the Uconnect system was cracked, they can send any command to the CAN bus. The attacking process is showed in Fig. 3.

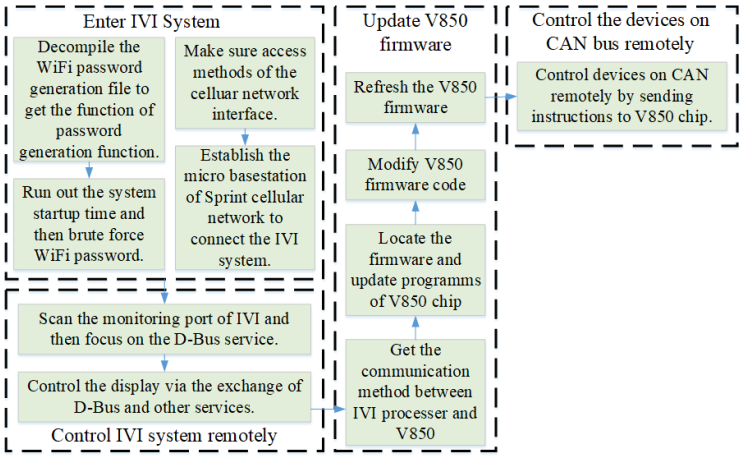

Fig. 3. Attack JEEP Cherokee.

Nowadays, scholars in interdisciplinary fields have separately studied the challenges, threats, attacks, and protection of these in-vehicle networks, and have a good accumulation of technologies [45, 51]. In the following subsections, we respectively provide the corresponding security analysis, attack analysis and defense methods with each in-vehicle network technology.

3.1 Security of CAN

CAN is a message ID-based broadcast communication protocol [52]. The characteristics of CAN such as its high efficiency and low latency make it still a charming and competitive protocols for ICVs [53, 54]. CAN has been in charge with the safety-related communications and thus, its security plays a vital role in the whole security of ICVs. However, CAN was designed focusing on its reliability and low cost with no intentions in security mechanisms, which was consistent with the closed cyber physical systems of traditional vehicles.

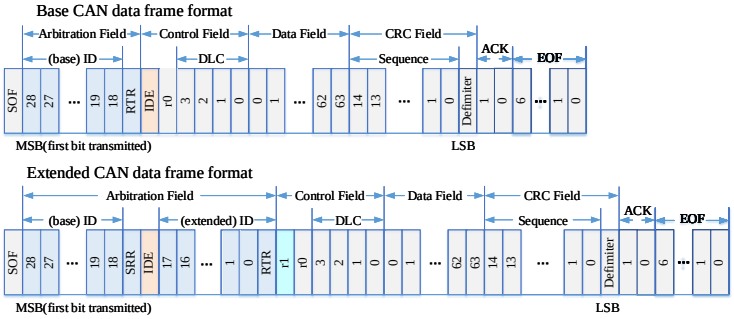

Fig. 4. Frame structures of different versions of CAN.

Fig. 4 shows the CAN data frame structures. Its simple communication mechanisms, especially its broadcast transmission, available interfaces, no authentication, no encryption and ID-based priority scheme, make it naturally vulnerable to cyber attacks in the open scenarios, which is a disaster for ICVs. First, any nodes can broadcast their frames to all other nodes connected to the same CAN bus when they need to transmit messages. Besides, every node on the bus can receive the frames and take actions after identifying the frame ID. This makes it convenient for malicious nodes to launch eavesdropping attacks. Second, there are several attack surfaces can be used to access CAN bus, such as the OBD port and telematic systems. The OBD port can be used not only diagnose CAN buses, but also transmit and receive messages to/from CAN buses. The wireless communication functions, such as cellular networks and WiFi, of telematic systems can be used by the hackers to launch remotely attacks. Third, the CAN protocol lacks of authentication and encryption mechanisms due to its limited data-field of CAN frames (64 bits). Malicious nodes can easily obtain and analyze all the messages transmitted on the bus without identification. Besides, the receivers cannot verify whether the received frames are valid. Finally, CAN adopts the ID-based Priority Scheme, *i.e.* the higher the message priority corresponding to the smaller message ID. Malicious nodes can send fake messages with higher priority to interrupt the transmission of normal messages with a lower priority. In summary, hackers can utilize all the above characteristics to obtain in-vehicle

messages from CAN buses or send CAN buses the malicious frames.

3.1.1 Attack analysis

Due to the above security issues, the major attack target in vehicles is the CAN bus. The studies on how to attack CAN buses also occupy the largest parts of the study on the vehicle attacks [55–57]. Initially, Koscher *et al*. [55] demonstrate that attackers can leverage the CAN designing flaws to completely attack many in-vehicle systems, including disabling the brakes and stopping the engine. However, there are some limitations to the attack. For example, steering and acceleration systems cannot be controlled. Then, Stephen Checkoway *et al*. [56] break the limitations and extend the attack range from the local area to the remote side by analyzing the attack surfaces and their corresponding attack vectors in experiments, which include physical accesses via the OBD-II interface, short-range wireless accesses using BlueTooth and remote accesses via 4G/5G or WiFi. Samuel Woo *et al*. [57] showed that the attackers could launch remote attacks on ICVs in the real world when the vehicles were connected to the network.

The possible attacks on the CAN bus are presented as follows:

- DoS attack. Attackers may exploit any vulnerability of vehicular services to stop the CAN bus and nodes linked to it from working properly. Kyong-Tak Cho *et al*. [58] unveiled a new significant vulnerability that appeared in several in-vehicle networks. They proposed a new type of DoS attack, *i.e*. bus-off attack, which exploited the error-handling scheme of CAN protocol to isolate the normal working ECUs from bus communication. The proposed attack is easy to implement on safety-critical ECUs, but difficult to prevent. Kyong-Tak Cho *et al*. [59] showed two new practical and important attacks: battery drain and Denial-of-Body-control (DoB). It proved that defenses are required at any time, not only when the vehicle's ignition is turned on.

- Spoofing attack. Attackers can inject malicious messages into CAN buses by disguising themselves as a legitimate ECU. Hazuki Iehira *et al*. [60] proposed a new spoofing attack method, which combines the advantages of bus-off attacks and spoofing attacks. The proposed attack method was a potential threat to the vehicle due to its imperceptibility.

3.1.2 Defense Methods

To mitigate these attacks of CAN, researchers mainly proposed two types of countermeasures, encryption and authentication [61], and anomaly detection, in terms of whether modifying CAN protocol.

- Authentication

Naturally, the CAN has no built-in security mechanisms to defend against malicious attacks. CRCs can only find the random transmission errors in CAN communications. The safe and reliable driving of ICVs requires CAN bus to ensure the message integrity and confidentiality. Authentication is a basic but effective countermeasure to provide proactive security for CAN. However, the limited data-field length (*i.e*. 64 bits) of the message frame makes it difficult to design a practical one for implementation.

For example, Wolf [62] and Schweppe [48] developed a security module using symmetric keys called hardware security module (HSM) to improve communication confidentiality. In [57], Woo *et al*. proposed a CAN security protocol to improve the CAN security level, which could meet the requirements of low delayed data encryption and authentication as well as message authentication code (MAC) applicable to limited CAN frame payload. Other typical methods are elaborated in Table 2.

- Anomaly Detection

Anomaly detection systems are widely applied in various traditional computer networks to detect whether the networks are under cyber attacks. However, these existing anomaly detection methods, which are mostly high-cost in time, computing and energy, can not satisfy the real-time and lightweight detection requirements of in-vehicle communications. Since anomaly detection systems are the most external security line, many researchers are working to develop anomaly detection algorithms for emerging vehicles. At present, the mainstream anomaly detection algorithms are divided into two categories, one is signature-based detection, and the other is anomaly-based detection. The signature-based anomaly detection methods summarize the signatures of the existing types of attacks and then justify whether the vehicles are suffering cyber-attacks based on these signatures. Meanwhile, anomaly-based detections refer to the statistical characteristics of the valid CAN frame transmission to justify the vehicle status. They use statistical features to identify the abnormal traffic on the bus, no matter whether the attacks are known or unknown. Thus, abnormal detection is more suitable with modern vehicles, and has attracted much research attention for many years.

Larson *et al*., [71] studied the applicability of a specification-based method to detect network intrusions. The authors made security specifications of communication and ECU behaviors used to verify whether the in-vehicle network was healthy at the time. In [72], the researchers proposed a dynamic anomaly detection algorithm for Mobile Ad hoc Networks (MANETs). In this scheme, the training set could be updated at a certain frequency. The updating depended on the dynamic learning process which is related to the projection distance calculation. The dynamic training set made the proposed algorithm outperform the anomaly detection algorithms using a static initial training set according to the average false positive rate. Schweppe *et al*. [47] used a binary function for marking in order to track malicious system intrusions. The time interval of CAN messages was an important feature to detect the CAN bus security. Several researchers used this feature to design anomaly or intrusion detection algorithms. Song *et al*. [73] proposed a hybrid intrusion detection system (IDS) supporting both known attack patterns and anomaly invasions. The proposed IDS could provide light-weight intrusion detection in terms of the CAN message rate, and test the validity by injecting three types of CAN frames, *i.e*. specific message injection for precise vehicle control, random or pre-ordered message sequences injection for system operation chaos and massive messages injection for communication disruption. However, The sequence analysis could cost much computing power and the implementation needed the CAN design information of original equipment manufacturers (OEMs). Researchers introduced deep neural network (DNN) into intrusion detection mechanisms in order to improve its performances [74]. The authors trained a DNN and obtained the low-dimensional features of the CAN message flows. The advantages were the obtained many features without the pre-knowledge of CAN payloads, while the

Table 2. Summary of encryption and authentication on CAN.

Author	Years	Description	Advantages	Disadvantages
Oguma *et al*. [63]	2008	An attestation-based security architecture for automobiles.	Lower overhead and latency compared with the RSA-based methods.	Require ECUs with rich resources to work as verification servers. Need to modify the communication protocol.
Van *et al*. [64]	2011	A message authentication protocol of CAN+, an high speed version.	Satisfy the requirements such as hard real-time and message length requirements. Strong security level	No implementation of CAN+ exists. Backward-incompatible. Need to modify the physical layer of CAN.
Hazem *et al*. [65]	2012	Lightweight message authentication protocol LCAP.	Small overhead to exchange authentication codes. No requirements on hardware modifications. Avoid modifying any existing CAN message.	Require larger address space due to the introduction of the new IDs in network configuration. Larger bandwidth cost. Larger time cost for session key distribution.
Groza *et al*. [66]	2013	A broadcast authentication protocol based on the key-chains and time synchronization.	Use cryptographic authentication in CAN networks. Use symmetric primitives without sharing keys during broadcast.	Have delay and restrictions for some applications.
Wang *et al*. [67]	2014	A security framework named VeCure, authenticating every message via an extra message.	Backward-compatible Defend against replay attacks. Little communication overhead. Have implementation details	High computation cost. High storage requirement of ECUs for maintaining the message counters.
Ueda *et al*. [68]	2015	A centralized authentication system with improved controllers.	High efficiency. Low latency.	Need to modify the CAN controller. High communication and computation overhead.
Hyo Jin Jo *et al*. [69]	2020	Propose the MAuth-CAN protocol	Defense masquerade attacks and bus-off attacks. NO hardware modifications of CAN-controllers	High Delay.
Franco *et al*. [70]	2022	Propose CAN Multiplexed MAC (CAN-MM), a new authentication protocol.	Exploit frequency modulation to multiplex MAC data with standard CAN communication. Compatibility with all CAN versions.	When the CAN-MM carrier and the external noise are at the same frequency, MAC bit stream demodulation could fail for some frames in a sporadic case.

disadvantages were the natural limitations of DNN, *i.e.* vanishing gradient problem and slow convergent speed. The authors utilized the pre-trained initial parameters to address the problems. Zhang *et al*. [75] proposed a detection method based on cooccurrence matrixes, which used the correlation property of audit to profile the valid user's normal behaviors. It can be suitable for real-time masquerade detection. The detailed anomaly detection methods are described and analyzed in Table 3.

3.2 Security of Automotive Ethernet

Automotive Ethernet is an emerging automotive protocol, which is mainly used for Diagnostics over IP (DoIP), IVI systems, and core network backbones. The excellent performances of Automobile Ethernet, *i.e.* high bandwidth (generally 100 Mbps), low cost, high compatibility and strong scalability of networking, make it a substitute for the existing bus networks such as CAN, MOST and FlexRay [84], which can provide better support for advanced automotive applications such as Advanced Driver Assistance Systems (ADAS).

Although Automotive Ethernet introduces so many advantages to automobiles, new security challenges also appear [85]. First, the number of potential attackers increases since more and more people are familiar with Ethernet technology, which means that the technical barrier and device cost to exploit it are rather low. Second, due to the limited computing, power and memory cost, Automotive Ethernet cannot be equipped with conventional security mechanisms directly such as intrusion detection systems (IDS) or high-performance traffic inspection systems [86]. Finally, the new physical switch network architecture and virtual segmentation of Automotive Ethernet can arise the security challenges such as drop or redirection of malicious signals and rogue messages.

3.2.1 Attack analysis

Due to the above security issues, Automotive Ethernet may suffer from several attacks as follows:

- Frame padding: Usually, when the payloads of frames are too short, the manufacturers will not pad enough bits of zeros as the protocol standard sets. Thus, the attackers have the possibility to obtain valuable memory information through multiple ICMP echo requests.
- DoS attacks: The attackers can launch TCP DoS attacks to hinder the flashing process of ECUs.
- IP spoofing: The attackers can send forged packets from their PCs to spoof the targeted ECUs.
- ARP cache poisoning: The attackers can send forged ARP requests to damage the ARP cache of the targets. They can bind a legal IP address and their own MAC addresses together to get all data of legal hosts, and then filter or stop forwarding these data to the targets.
- TCP hijacking: The attackers can sniff the current communication traffic and get their sequence numbers of them. After that, they insert their elaborate spoofed

Table 3. Summary of CAN anomaly detection.

Author	Years	Description	Advantages	Disadvantages
Muter *et al*. [76]	2010	An feature-based anomaly detection systems to recognize attacks.	The ability to identify some different threats. Provide a rational basic level for anomaly detection.	Attacks similar to the normal behaviors of CAN communication cannot be detected.
Muter *et al*. [77]	2011	Propose an entropy-based attack detection algorithm for in-vehicle networks.	Easy adaptive.	Difficult with identifying small-scale attacks.
Murvay *et al*. [78]	2014	Authentication using the physical characteristics of frames, *i.e*. voltage values.	High valid when transmitting the IDs of CAN message.	Limited valid time and only suiting with low speed bus.
Song *et al*. [73]	2016	An deep neural network (DNN) based intrusion detection system (IDS).	Real-time. High accuracy.	The training dataset can affect the system performance.
Cho *et al*. [79]	2016	An IDS called CIDS to fingerprints the transmitter ECUs.	High accuracy. Large capability of discovering the attack sources.	Attack identification working normally on periodical injecting attacks.
Cho *et al*. [80]	2017	An ECU fingerprinting method, called Viden (Voltage-based attacker identification)	High adaptability. Low sampling rate without strict restrictions on the type and speed of CAN message.	The existing sampling offset is difficult to be balanced.
Kuwahara *et al*. [81]	2018	A statistical anomaly detection method focusing on the number of messages observed in a fixed time window.	Robust even when the normal sequences are diverse.	High computing cost. Low sensibility.
Groza *et al*. [82]	2019	An intrusion detection mechanism that takes advantage of Bloom filtering to test frame periodicity.	Efficient time-memory tradeoff which is beneficial for the constrained resources of CAN.	The abnormal ECUs cannot be located.
Xinghua *et al*. [83]	2022	A car networking message classification mechanism with two improved SVDD schemes.	Higher accuracy, recall rate, and fewer computation overhead.	There are many learning method to be selected and improved.

packets into the session. Then, they can replace the legitimate hosts to continue communicating.

3.2.2 Defense methods

The implementation of Automotive Ethernet makes the automotive network architecture change into a switching network, which is more complex than the traditional bus system. Although the existed vehicle attacks are unsuitable with the new networks, specific security defense methods are required to protect the vehicle from the new security threats. The possible defense methods are presented as follows,

- Enhancing network management: The automotive switching networks deploy the gateways to forward packets. Thus, it is positive to deploy access control lists (ACL), and virtual local area networks (VLAN) on gateways to enhance security.

- Encryption and Signatures: Using MAC security (*i.e*. 802.1AE), IPsec and SSL/TLS encryption can greatly increase communication confidentiality and data privacy.

- Static configuration: Although the Automotive Ethernet may apply the traditional protocols, it can cut down the original functions of protocols by static configurations. For example, ICMP implements the ECHO requests and responses only, which avoids many inherent vulnerabilities of this protocol. In addition, the ARP cache can be configured static to defend against many attacks such as ARP cache poisoning.

- Intrusion detection: IDSs are also used to detect cyber attacks on autonomous Ethernet. For example, [87] compared the performance of different unsupervised ML-based anomaly detection algorithms for real-time anomaly detection over the Audio Video Transport Protocol (AVTP), which is an application layer protocol implemented in the automotive Ethernet. [88] proposed an offline intrusion detection sequence model based on deep learning. They labeled a dataset with several classes representing real-world intrusions and one common class, and applied the proposed RNN-based sequence model to it. [89] present an intrusion detection method for detecting Audio-Video Transport Protocol (AVTP) stream injection attacks in automotive Ethernet-based networks. The proposed intrusion detection model is based on feature generation and convolutional neural network (CNN).

3.3 Security of FlexRay

FlexRay [90,91] is an in-vehicle communication protocol designed for safety-critical and time-critical data transmission by providing two parallel channels both up to 10 Mbit/s. It can satisfy the requirements of high data rates, high fault tolerance and high reliability at a high price compared with CAN [92]. Nilsson *et al*. [93] analyzed the security threats of FlexRay Protocol specification and found that it lacked sufficient protection against some general attacks such as spoofing. However, security research in this field still deal with the initial stages.

3.3.1 Attack analysis

The study about the attack methods of FlexRay is scary. We haven't found any examples of real-world attacks on FlexRay in published articles or reports. Nilsson *et al*. [93] monitored and spoofed FlexRay in the simulated FlexRay network to turn on the braking lights without pushing the braking pedal. And this is the only publication we have found about the FlexRay attacks.

3.3.2 Defense methods

Similarly, there is seldom security research against FlexRay attacks. The first attempt to secure FlexRay protocol was published in 2019 [94]. The authors proposed to introduce key management into FlexRay communications. They suggested associating cryptography keys with FlexRay time slots to obtain well scalability in the number of nodes and message types. They also computed MACs to provide data authenticity. Some researchers [95, 96] proposed a FlexRay/Ethernet gateway design to adapt the development and security of embedded systems and vehicle networking. They used the Field Programmable Gate Array (FPGA) system as the platform to evaluate the performance of the proposed mechanism such as running time and overhead. Moreover, they integrated the security functions with the gateway with low latency and power consumption. Other researchers [97] proposed some FlexRay-related defense techniques against message spoofing attacks using the slot-based and channel-based FlexRay communication features to ensure the authenticity of safety-critical in-vehicle data transmission. In particular, they suggest splitting authentication tags across two physical independent channels, allowing for their concurrent transmission. However, Automotive Ethernet could be a future replacement for FlexRay. Whether to make a further study on FlexRay protocol is still confusing.

3.4 Security of Media Oriented System Transport

Media Oriented System Transport (MOST) [98, 99] is a high-bandwidth and high-speed network protocol used to transmit audio, video, and control data in modern automotive multimedia networks via fiber optic cables. It is a point-to-multipoint data transmission network supporting up to 64 MOST devices. The features of immunizing electromagnetic interference and high data rate make it to be an ideal solution for ADAS and popular among automakers. However, the high cost, restricted access to hardware, reliance on heavy coax cable and easily damaged optical fiber make MOST inferior to the emerging automotive network in the new generation of vehicles. Besides, MOST has security issues in data transmission. First, MOST transmits audio and video streams via the synchronous channel and data packets (*e.g*. navigation information) via the asynchronous channel. Attacking the transmission process of streaming data and packets can lead the audio or video information to be damaged and navigation information to be lost. Second, MOST can suffer from the single-point failure problem due to the cyclic structure. Once a node in the loop doesn't work, the communication stops immediately. Finally, MOST150, the last version of MOST introduced in 2007 [45], can transmit original IP data packets, which may increase the risk of infection with computer viruses and worms.

3.4.1 Attack analysis

Due to the characteristics of uncommon deployment and the high cost of MOST, the attacks on in-vehicle MOST networks have not been reported yet. However, MOST can suffer from cyber-attacks as well. Especially, a compromised MOST node can stop the operation of the complete network. For example, attackers can compromise a MOST node to continuously send malicious timing frames to disrupt the MOST synchronization mechanism. Attackers can also send continuous bogus channel requests, to exhaust bandwidth and launch a jamming attack on the MOST bus. Moreover, the use of CSMA/CD in asynchronous and control channels makes the MOST vulnerable to jamming attacks like CAN.

3.4.2 Defense methods

Possible defense methods to enhance MOST security can be listed as follows,

- Data encryption: Encrypting the synchronous data and asynchronous packed data can increase data security. MAC or Central gateway encryption can also be used to reduce the security risks.

- Structure redundancy: Since MOST can suffer from single-point attacks, bi-cyclic MOST can provide effective redundancy to ensure stability.

- Abnormality monitoring: MOST adopts the polling mechanism in the process of network startup to establish a central registry. When a device node is added to the MOST bus, detecting the transmission content can be used to detect whether the newly added node is trying to occupy a large amount of bandwidth to transfer data on the annular network.

3.5 Security of LIN

Local Interconnect Network (LIN) is a low-cost serial communication network specially designed for automobiles to realize distributed control in automobile electronic systems [100]. It is commonly applied to low-speed communication where real-time operation is not required. For example, LIN is usually used for connecting non-safety-related systems such as automatic door locking mechanisms, power windows and mirrors, and so on [101].

The security of LIN has been briefly introduced in [102]. In addition, researchers have analyzed the security threats in [103]. Although LIN may suffer from significant threats when the attackers have the ability to control the LIN communications, implementing these malicious behaviors is difficult. On one hand, the method of injecting false responses into LIN depends on the types of data. Because simply injecting false responses may collide with the following correct response after the transmission of the header. On the other hand, It is difficult to modify the time scheduling to control the timing of the sequence of the messages. To manipulate the time schedule, attackers need to physically access and tamper with the master node, which needs the details of the implementation of the master node. However, it's impossible in general.

3.5.1 Attack analysis

The hacking techniques [55] make it easier to access the LIN bus via CAN nodes. The possible attack methods are listed as follows,

- Master node attacks: Because the operations of LIN slave nodes depend on their corresponding LIN masters, the major promising attacking approaches are to attack the master nodes.
- Injecting attacks: Attackers can inject malicious sleep frames into LIN networks to deactivate the corresponding bus communications completely until a wake-up frame recovers it to the proper states again.
- Synchronization attacks: Sending frames with bogus synchronization bytes can make LIN inefficient.

3.5.2 Defense methods

Typically, the defense methods can be listed as follows,

- Byte Assignment in Response: The first byte of the response in a collision has great difficulty to be changed. Thus, setting the first byte of the response with significant data can protect the important values from falsifying.
- Message Authentication Code (MAC): Similar to CAN, MAC can reduce the possibility that the slave nodes receive a false response as a corrected one [104].
- Abnormality warning: When a slave node finds an abnormality by comparing the bus level with the sent response, it sends an abnormal signal to notify the network status and then all nodes will change to safe mode.

4. SECURITY OF CONTROL SYSTEM

The functions of modern vehicle control systems are mainly accomplished by the cooperation of various ECUs, which are the main in-vehicle components. These ECUs play important roles in the vehicle and exchange messages through vehicle buses to control vehicles such as ignition, speed changing, lighting, and braking. A typical ECU structure is shown in Fig. 5.

Initially, ECUs were designed to improve the response speed and data processing capability of the control system. However, anyone could access the system via its interfaces due to the lack of hierarchy and authentication mechanisms. If one of the in-vehicle ECUs was compromised, the entire vehicle system would be subjected to significant security threats. Besides, the remote communication capabilities of Infotainment ECU and Telematics increase the security threats of the in-vehicle control systems. Thus, ECU threat analysis and related protections should be an indispensable research point for vehicle manufacturers. Table 4 shows the detailed security threats and countermeasures of ECUs.

Table 4. Summary of ECU attacks and defense.

Attack type	Access level	Attack potential	Benefits	Attack likelihood	Application method	Attack method	Defend method
Communication	External interfaces (remote)	Low	Large	High	Protocol analysis, *etc*.	Blocking; Replaying; Insertion; Flooding.	Encryption;Authentication;Freshness values;Rate limitation; Network IDS.
Exposed Functions	External interfaces (remote)	Low	Large	High	Pen test, fuzzing, *etc*.	Software bugs;Resource exhaustion;Rowhammer;Design flaws	Code analysis; Host IDS; DPI; Firewalls.
Non-invasive Attacks	ECU PCB IC (local)	Medium	Large	Medium	Side Channel Analysis	Time analysis; Static and dynamic power analysis; Photo emission analysis.	Constant-time execution; Constant-power execution; Execution jitter.
Semi-invasive Attacks	ECU PCB IC (local)	High	varying by the target.	Low	Temporarily physical tampering	Local light attacks; Spike/signal injection; Aplha Particle penetration.	Light sensor; Sensors on supply/signals; Information redundancy.
Invasive Attacks	ECU PCB IC (local)	High	varying by the target.	Low	Permanently physical tampering	Delaying; Micro probing; IC modification using FIB.	Camouflage logic; Shield; Masking; Tamper detect Pins.

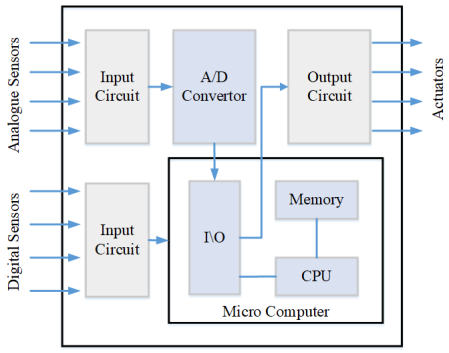

Fig. 5. Example of a typical ECU structure.

4.1 Software Security

ECU software security mainly refers to communication, software vulnerabilities and firmware updating mechanisms, corresponding to the first two rows of Table 4. First, some ECUs can be directly accessed from the external networks via cellular networks or Wifi. When ECU applications have security vulnerabilities, they can be exploited to inject and execute malicious codes or disable significant functions. Second, ECU firmware updates can improve ECU performance, but it lacks digital signatures and verification mechanisms, which can result in serious security threats such as system firmware overwritten, system logic modifying or reserving system back doors.

4.1.1 Attack analysis

Most attacks can be achieved by the following methods with some subsequent targets such as buffer overflow, resource exhaustion, and so on.

- Blocking: Attackers can block the transmission of the messages by flooding a lot of attack messages to disable the normal functions of vehicles.

- Injecting: Most ECUs connected by CAN buses can be accessed through the OBD-II interface for both diagnostic and reprogramming [105]. Theoretically, the OBD-II adapter can be directly connected to the OBD-II interface and hackers can attack the vehicle through the interface in real-time. [106]. Due to the broadcast mechanism and lack of authentication on CAN, attackers can eavesdrop on the messages, and resend them directly to the bus with or without some modifications. The corresponding ECU actuators respond to repetitive commands, which can be harmful to the vehicle.

- Tampering: The ISO 14229 electrical industry standard specifies the relationship between packet IDs and ECUs [107]. Each message has an ID which represents that it is sent by a specific ECU. By modifying the packet ID, sending the wrong instruction to the designated ECU can lead to abnormal operations such as braking, locking, and sharp turns. It can also change the content of a message to make the corresponding parameters on vehicle meters display incorrectly. Further, By

modifying the central controller to unlock message information sent by the ECU, the driving vehicle can be forcibly unlocked [108].

4.1.2 Defense methods

Several types of defense methods can be used to protect ECU software from cyber attacks. For wireless communications, encryption and authentication technologies are good choices to protect the target from data tampering [109, 110]. For software vulnerabilities, programming checksum, code analysis, secure updating and IDS can be used to defend against malicious instruction injecting [111–113].

4.2 Hardware Security

ECU hardware mainly refers to three parts, including Printed Circuit Board (PCB), Integrated Circuit (IC) and Central Processing Unit (CPU) [62, 114]. It has the security issues of traditional hardware as well as special security challenges due to the features of the in-vehicle networks. The last three rows in Table 4 describe the corresponding security threats and possible countermeasures.

4.2.1 Attack analysis

The ECU hardware can suffer from three types of attack, *i.e.* non-invasive attacks, semi-invasive attacks and invasive attacks.

- Non-invasive attacks: For non-invasive attacks, side-channel analysis (SCA) is the most popular attack method, which is widely used to crack the inset cryptography methods [115]. SCA can exploit physical signals leaking from ECU's cryptographic implementation to get various information using corresponding methods such as timing analysis, static power analysis, dynamic power analysis, and electromagnetic analysis [115]. For example, in [116], the clock glitch attack is described in detail. Since the vehicle's ECUs rely on the internal clock to perform instructions, if the clock pulses get into a mess, the current instruction will be skipped and the next will be executed.
- Semi-invasive attacks: For semi-invasive attacks, the attackers may temporarily physically tamper with ECUs or their components. For example, the attacker may introduce an additional charge to an IC by using flashlight to launch light attacks, which leads to bit changing from 0 to 1.
- Invasive attacks: The last class is invasive attacks, which can change the hardware system permanently. For example, attackers can change the interconnects on a PCB or even an IC by a Focused Ion Bin (FIB).

4.2.2 Defense methods

Currently, the main hardware protection measures are secure boot, secure debugging, secure communication, secure storage, integrity monitoring, channel protection, hardware fast encryption, device identification, message authentication, and execution isolation. The current popular designs for automotive security chips are Secure Hardware Extension (SHE) [117] and E-safety Vehicle Intrusion protected Applications (EVITA) [118, 119]. SHE mainly provides AES-128 cryptographic calculations. In the EVITA architecture,

cryptographic coprocessor HSMs are deployed in the ECU's CPU to perform all cryptographic calculations, including encryption and decryption, integrity verification, and digital signatures. The HSM based on the EVITA architecture enables secure boot, authentication, and encryption. These measures can effectively strengthen ECUs' security. However, the cost of hardware security deployment is high and thus it is not widely used at present.

5. SECURITY OF V2X COMMUNICATION SYSTEMS

V2X communication systems, which are responsible for vehicular external communications with other vehicles, user equipments (UEs) and various infrastructures, have been playing a significant role for the numerous emerging functions of ICVs such as cooperative driving, navigation, automatic parking and *etc*. In recent years, research and standardization efforts to V2X technology have been carried out and important breakthroughs have been made [120]. Dedicated Short-Range Communication (DSRC) and cellular V2X (C-V2X) are the two main technology directions with their unique set of pros and cons for application in this area. The 802.11-based DSRC can provide reliable and ultra-low latency communication with low overhead for medium-sized VANETs in LOS conditions thanks to its independence from infrastructure and no requirement of transmission and process latency in core network. However, the connectivity availability, channel utilization and security cannot be ensured, and the situation can even be worse in congestion conditions. In addition, the full deployment of DSRC requires mass construction and operation of roadside units and VPKI infrastructures, which would be a big cost. On the other hand, C-V2X technology is different from DSRC in several aspects, generally including larger scale communication, more efficient but simpler security mechanisms as well as lower construction costs benefiting from the existing mobile network deployments.

With the performance requirements of low delay, high reliability, high bandwidth and large capacity for mobile communications, both DSRC and C-V2X must pay attention to security issues. The 802.11-based DSRC must maintain a tight grip on secure, verified and authenticated messages while meeting privacy restrictions, because inaccurate sensor data or malicious spoofing data can cause communication congestion, energy consumption, and even endanger people's lives. However, it's difficult for DSRC to prevent the spoofing or tampering attacks completely by low extent detection and stemming. For C-V2X, the 5G-V2X which are deploying in the real world can handle the existing security threats in LTE-V2X, such as identity theft, anonymity, sniffing, authentication, message protection, and so on [121–123]. However, there are still few concurrent studies about the special security issues from 5G-V2X perspectives.

In conclusion, no matter DSRC or C-V2X, the nature of ad-hoc and wireless communications makes the V2X communication systems vulnerable to a number of potential attacks such as vehicular worms and wormhole attacks. To defend against them, various security mechanisms have been proposed respectively [124–126].

5.1 Attack Analysis

Possible attacks to V2X communications are listed as follow:

- Eavesdropping. Adversaries may monitor the wireless channels to collect vehicle-specific information.
- Bogus information. Bogus information can be injected into the targeted vehicle in order to mislead the drivers to make wrong decisions. Sybil attack is a typical example, which cheats the driver that there are one hundred vehicles and makes him believe there is a traffic jam ahead while there is only one.
- Impersonating. The adversaries can obtain the identities of the legitimate nodes by illegal means and then infuse malicious information into the network by impersonating the node.
- Denial of service. The adversaries can exhaust the computing and storage of the targeted nodes by sending a mass of irrelevant messages which can overwhelm the normal messages transmission [127].
- Message suspension. Adversaries may selectively block some packets of messages important to the intended nodes [128,129]. Then these messages are used for some purposes in the future, such as preventing the roadside units from obtaining the collision reports of vehicles.
- Hardware tampering. The hardware of ECUs or other on board devices in vehicles may suffer tampering, which can impact the motoring condition and cause the serious traffic accidents.

5.2 Defense Methods

The defense methods of V2X communication systems can be classified into three categories: cryptography-based methods, behavior-based methods and identity-based methods [124].

- Cryptography-based methods. Cryptography-based methods include encryption, key management and authentication. Encryption can transform the data to another form to protect data from being eavesdropped and tampered. However, it increase the processing time and network overhead. Key management process handles the generation, exchange and storage of cryptographic keys. Authentication schemes are used to detect unauthorized nodes to defend against external attacks. Researchers have designed many authentication methods to avoid being exposed directly to attackers, such as RSU-aided message authentication schemes [130] and the PKI-based authentication schemes. All the above methods can be used to pretect privacy. For example, researchers have made considerable efforts to preserve the identity privacy [130] and location privacy [131,132] by designing novel anonymous authentication methods [133] or dynamic key management schemes [134].
- Behavior-based methods. Behavior-based methods complement the cryptography-based methods to detect internal attackers. These kinds of methods are used for trust management by considering weighted sum [135], rewarding [136], fuzzy logic [137] and so on. The weighted-sum methods assign different weights for every trust component and the total trust value is used to tell whether the node is malicious. The rewarding-based methods reward the neighboring node for behaving normally and cooperating with others actively to encourage nodes to participate in vehicle cooperation. The fuzzy logic methods are used to detect false or bogus messages using fuzzy logic models.

- Identity-based methods. The identity-based methods are used to defend the attacks such as Sybil attack which uses the identity maliciously, and protect privacy by using identity pseudonyms, geographic proximity techniques, and so on [138, 139].

6. FUTURE RESEARCH DISCUSSION

In the above, we have discussed various security issues and their corresponding defense methods, which are related to each core components of ICVs in a wide and deep way. Many researchers and organizations have proposed that the vehicle perception system such as GPS is one important direction, which has been discussed in Section 2 [8]. Since the artificial intelligence (AI) and SAGIN are two hot points in the future's automotive and communications industries, in this section, we focus on the future research directions from the perspectives of in-vehicle networks and its components (*i.e.* ECUs), as well as V2X communications in the new network environments.

6.1 Security Discussion of In-vehicle Networks and Its Components

As we all know, in-vehicle networks play an irreplaceable role in both traditional vehicles and ICVs. Whether they work normally and efficiently can greatly affect the development of vehicles and traffic safety and efficiency. Therefore, their security issues should be considered seriously. Section 3 has discussed the existed security threats, attacks and countermeasures related to the various in-vehicle buses such as CAN, LIN, FlexRay, and so on. We believe that the existing security threats come from the contradiction between the increasingly open vehicle network environment and the inherent lack of security mechanisms such as message authentication in the in-vehicle network protocol design. Thus, the vehicles could be easily penetrated by inner and external adversaries and lose their normal and safe status.

Nowadays, there have been a lot of related research about this topic, referring to both attacks and defenses. However, due to the rapid development of ICVs, especially self-driving vehicles, we still need to further study security issues on in-vehicle networks in the future. Firstly, the advancement of intelligence in ICVs means the tremendous increase of software codes equipped in ICVs, which can enlarge the attack surface. In addition, the self-driving technology and vehicle-road collaboration technology make it with greater risk to be attacked maliciously. Thus, the security risk identification of in-vehicle networks and components should be carried out all the time. In this paper, based on our knowledge of the attacks and protection methods of the in-vehicle network and components as reviewed in Sections 3 and 4, we present some open future research directions, just as follows:

- **Intelligent access control strategies:** Generally, ICV is considered equipping a number of wireless connections to support V2X communications. Therefore, an intelligent dynamic configured access control strategy is needed to adopt the various environmental conditions and vehicle states. Software-defined networking (SDN) could be a potential technique for next-generation in-vehicle networks as it offers greater flexibility.

- **New in-vehicle protocols design:** Existing in-vehicle protocols can not meet the bandwidth and design performance requirements of the next generation ICVs' in-vehicle networks, Especially when the sensor-based attacks to ICVs increase the security vulnerabilities such as incorrect information sharing and inaccurate vehicle control. The new in-vehicle network standard design should take the security mechanisms into consideration at the beginning. For example, the authentication mechanism and intrusion detection should be equipped in the protocol design.

- **Machine learning-based security mechanisms in ICVs:** Machine learning-based methods are applied generally in the intelligent function design of ICVs and achieve good results. These kinds of methods can also promote the advancement of in-vehicle anomaly or intrusion detection systems due to their unique advantages in anomaly identification. However, they also have two limitations, one is the large computing cost, and the other is the difficulty of obtaining effective trained data. Since these limitations can impact the accuracy and response time of detection, how to solve these problems is the main challenge in their deployments. Edge computing technology may be a good solution. However, the combination of edge computing and machine learning could pose other particular security problems.

- **Security gateways in ICVs:** The in-vehicle control systems are complex and heterogeneous. In addition, the emerging functions for vehicle-road collaboration and autonomous driving make it more complex to protect the security of in-vehicle components. Security gateways may be a good choice to segregate heterogeneous control systems to provide more efficient and safe control services. The gateway is the device that has the functions of routing, filtering, ID modification, repacking, splitting, translation and scheduling [140]. Considering the in-vehicle security, the gateway should make sure that the messages exchanged among different networks are integrated and undisclosed. Seriously, once the gateway is compromised, the messages passing by cannot be authenticated and the whole automobile cannot be controlled easily. Thus, the gateway protection and the heterogeneous messages authentication are both the focused points of ICV security [141].

- **Security of autonomous driving or collaborative driving decisions:** The intelligence of ICVs greatly benefited from the rapid development of machine learning technology. Almost all advanced functions are infiltrated by machine learning, which includes environment perceptions, behavior predictions, routing plans and driving decision making. However, machine learning models are also can suffer malicious attacks. Actually, ML-based methods are vulnerable to adversarial attacks. For example, the poisoning attacks can affect the training phase of the learning process by manipulating the training data, which are called adversarial examples [142]. Adversarial attacks on object detection from images have been studied broadly, however, there are little work on this kind of attacks to vehicular LiDAR and radar data [16].

6.2 Security Discussion of V2X Communications

We have discussed the V2X communication security issues in Section 5. We present that V2X communications play a significant role in the numerous emerging functions of

ICVs such as cooperative driving, automatic parking, and so on. We provided recent research about V2X technology and its security, including DSRC and C-V2X technology, as well as their comparisons. Although there are many researches about attacks and defenses of V2X communications, there are rarely security discussions about the new 5G-V2X security and the future SAGIN V2X security issues. Since the security of ICVs can be great affected by the surrounding networks, and the huge increase in vehicle intelligence and amount makes the demand for communication, computation, and storage resources arising largely, V2X communication security in new network environments should be considered seriously. For example, Space-Air-Ground integrated network (SAGIN), which integrates with satellite communications, UAV communications and terrestrial communications, can provide large scalability, large capability and low latency for vehicular communication and will have a great impact on the security of ICVs. The friendly collision of ICVs and SAGIN can bring both challenges and opportunities to ICV security. SAGIN can provide the ICVs with flexible relay nodes or management nodes such as UAVs or airships to reduce the communication delay and handovers when it is moving fleetly. However, SAGIN also increases the heterogeneity of Node and network and make the authentication design more complex. Besides, the privacy protection of ICVs in SAGIN would be a great issue due to the enlarged attack surfaces, *e.g.* the increased network nodes and wireless links. The existing privacy protection methods are seldom suited to these complex and heterogeneous networks.

In this paper, we provide some future research directions on V2X security that we think are interesting, just as follows:

- **SAGIN-enabled cross-layer V2X security mechanisms:** SAGIN is an important development direction of 6G communication in the future. It is also the main communication technology background of future Intelligent Transport Systems (ITSs). V2X is an indispensable and important part of the next-generation ITS. SAGIN-enabled V2X technology can improve the communication efficiency caused by current communication infrastructure deployment in remote areas and coverage limitations. However, limited to the inherent broadcasting nature and broad coverage, the satellite down-links in SAGIN-enabled V2X communications are vulnerable to security threats. Recently, the various V2X applications under SAGIN and the corresponding technique challenges are actively studied. For example, Yin *et al*. [143] have investigated the unmanned aerial vehicle (UAV) assisted physical layer security in multi-beam satellite-enabled V2X communications. In this work, they used the UAV as a relay to guarantee the security of the vehicle-to-satellite link. For the future, we consider designing not only the physical layer but also the cross-layer V2X security mechanism to defend the masses of cyber-attacks outside ICVs.

- **Decentralized V2X authentication mechanisms:** Although the research about V2X authentication mechanisms has been many years, there are still some challenges that existed to be solved. Most existing authentication protocols had no idea about avoiding single-point failures and reducing authentication latency at the same time. Particularly, when it is related to SAGIN vehicular network, new authentication protocols are needed, which should consider various use cases with different network elements such as vehicles, infrastructure units, pedestrians *etc*. Also,

safety-related applications must deal with low-latency requirements, which requires authentication mechanisms to be handled rapidly and flexibly. The most entertainment applications have lower requirements of the delay, but they need the assistance of edge computing. Recently, Yang *et al*. [144] proposed an edge-assisted decentralized mutual authentication protocol. This protocol can achieve efficient authentication with only one-round interaction. Blockchain can provide a neutral computational and communication platform for V2V and V2I communications. we consider that using emerging blockchain and edge computing technology to design more effective mutual authentication mechanisms is an important direction for future research.

- **Privacy preserving V2X communications:** Privacy protection is another inevitable challenge for V2X communications. Due to the open communication characteristics of V2X, privacy leakages are easy to happen when large amount of sensitive data is being transmitted. Once it happening, attackers can track and monitor vehicles and then get sensitive information of vehicle users. In addition, the current and future V2X communications are related to many cloud technology, lots of sensitive data are transmitted and stored in cloud servers, which need to enhance their security and privacy protections. Recently, researchers have proposed some privacy-preserving mechanisms for the new V2X applications. For example, Song *et al*. [145] proposed a task matching scheme with threshold similarity search through vehicular crowd-sourcing to protect privacy. Huang *et al*. [146] proposed a decentralized, accountable, and privacy-preserving architecture for car sharing services. In conclusion, it is important for ICVs to protect their data privacy and defend against cyber attacks such as message falsification, message eavesdropping, radio jamming, DoS and DDoS attacks and so on. Blockchain-based decentralized privacy preserving mechanisms may be a research direction for various V2X applications in the future SAGIN-based ITSs.

7. CONCLUSION

In this paper, we have investigated the security issues of ICV information systems from the perspective of their architecture. We analyze the security threats, including the attack motivations and the attack surfaces, and then discuss the detailed security issues and their countermeasures of the four different aspects of ICV information systems. Finally, we pointed out some important future research directions of ICVs for further study. We believe that future ICV security levels can be raised with the aid of cyberattack techniques and defense technology modeled after blockchain.

ACKNOWLEDGMENT

The authors would like to thank the editor and the anonymous reviewers for their constructive feedback.

REFERENCES

1. Q. Luo and J. Liu, "Wireless telematics systems in emerging intelligent and connected vehicles: Threats and solutions," *IEEE Wireless Communications*, Vol. 25, 2018, pp. 113-119.
2. J. Gao, M. Li, L. Zhao, and X. Shen, "Contention intensity based distributed coordination for V2V safety message broadcast," *IEEE Transactions on Vehicular Technology*, Vol. 67, 2018, pp. 12 288-12 301.
3. L. Kang and H. Shen, "Detection and mitigation of sensor and CAN bus attacks in vehicle anti-lock braking systems," *ACM Transactions on Cyber-Physical Systems*, Vol. 6, 2022, pp. 1-24.
4. C. Miller and C. Valasek, "Adventures in automotive networks and control units," in *DEF CON*, Vol. 21, 2013, pp. 15-31.
5. M. Charlie and V. Chris, "A survey of remote automotive attack surfaces," *Black Hat USA*, Vol. 2014, 2014, p. 94.
6. J. Zhang, G. Lu, H. Yu, Y. Wang, and C. Yang, "Effect of the uncertainty level of vehicle-position information on the stability and safety of the car-following process," *IEEE Transactions on Intelligent Transportation Systems*, Vol. 23, 2020, pp. 4944-4958.
7. M. H. Eiza and Q. Ni, "Driving with sharks: Rethinking connected vehicles with vehicle cybersecurity," *IEEE Vehicular Technology Magazine*, Vol. 12, 2017, pp. 45-51.
8. J. Petit and S. E. Shladover, "Potential cyberattacks on automated vehicles," *IEEE Transactions on Intelligent Transportation Systems*, Vol. 16, 2015, pp. 546-556.
9. X. Jia, L. Xing, J. Gao, and H. Wu, "A survey of location privacy preservation in social internet of vehicles," *IEEE Access*, Vol. 8, 2020, pp. 201 966-201 984.
10. W. Wu, R. Li, G. Xie, J. An, Y. Bai, J. Zhou, and K. Li, "A survey of intrusion detection for in-vehicle networks," *IEEE Transactions on Intelligent Transportation Systems*, Vol. 21, 2020, pp. 919-933.
11. Z. Wang, Y. Wang, Y. Zhang, Y. Liu, C. Ma, and H. Wang, "A brief survey on cyber security attack entrances and protection strategies of intelligent connected vehicle," in *SmartCom*, LNCS, Vol. 11910, 2019, pp. 73-82.
12. M. Pham and K. Xiong, "A survey on security attacks and defense techniques for connected and autonomous vehicles," *Computers and Security*, Vol. 109, 2021, p. 102269.
13. S. Parkinson, P. Ward, K. Wilson, and J. Miller, "Cyber threats facing autonomous and connected vehicles: Future challenges," *IEEE Transactions on Intelligent Transportation Systems*, Vol. 18, 2017, pp. 2898-2915.
14. A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-physical systems security – a survey," *IEEE Internet of Things Journal*, Vol. 4, 2017, pp. 1802-1831.
15. J. E. Siegel, D. C. Erb, and S. E. Sarma, "A survey of the connected vehicle landscape – architectures, enabling technologies, applications, and development areas," *IEEE Transactions on Intelligent Transportation Systems*, Vol. 19, 2017, pp. 2391-2406.

16. A. Qayyum, M. Usama, J. Qadir, and A. Al-Fuqaha, "Securing connected & autonomous vehicles: Challenges posed by adversarial machine learning and the way forward," *IEEE Communications Surveys & Tutorials*, Vol. 22, 2020, pp. 998-1026.
17. A. Chowdhury, G. Karmakar, J. Kamruzzaman, A. Jolfaei, and R. Das, "Attacks on self-driving cars and their countermeasures: A survey," *IEEE Access*, Vol. 8, 2020, pp. 207 308-207 342.
18. Z. Pethő, Á. Török, and Z. Szalay, "A survey of new orientations in the field of vehicular cybersecurity, applying artificial intelligence based methods," *Transactions on Emerging Telecommunications Technologies*, Vol. 32, 2021, p. e4325.
19. H. J. Jo and W. Choi, "A survey of attacks on controller area networks and corresponding countermeasures," *IEEE Transactions on Intelligent Transportation Systems*, Vol. 23, 2022, pp. 6123-6141.
20. M. Hataba, A. B. T. Sherif, M. Mahmoud, M. Abdallah, and W. Alasmary, "Security and privacy issues in autonomous vehicles: A layer-based survey," *IEEE Open Journal of the Communications Society*, Vol. 3, 2022, pp. 811-829.
21. A. Davies, "Turns out the hardware in self-driving cars is pretty cheap," *Wired Blog*, https://www.wired.com/2015/04/cost-of-sensors-autonomous-cars/, 2015.
22. E. B. Hamida, H. Noura, and W. Znaidi, "Security of cooperative intelligent transport systems: Standards, threats analysis and cryptographic countermeasures," *Electronics*, Vol. 4, 2015, pp. 380-423.
23. C. Yan, W. Xu, and J. Liu, "Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle," Vol. 24, 2016, p. 109.
24. N. Miura, T. Machida, K. Matsuda, M. Nagata, S. Nashimoto, and D. Suzuki, "A low-cost replica-based distance-spoofing attack on mmwave fmcw radar," in *Proceedings of the 3rd ACM Workshop on Attacks and Solutions in Hardware Security Workshop*, 2019, pp. 95-100.
25. N. Rastogi, S. Rampazzi, M. Clifford, M. Heller, M. Bishop, and K. Levitt, "Explaining RADAR features for detecting spoofing attacks in connected autonomous vehicles," *arXiv Preprint*, 2022, arXiv:2203.00150.
26. S. Tuohy, M. Glavin, C. Hughes, E. Jones, M. Trivedi, and L. Kilmartin, "Intra-vehicle networks: A review," *IEEE Transactions on Intelligent Transportation Systems*, Vol. 16, 2015, pp. 534-545.
27. P. Kapoor, A. Vora, and K. Kang, "Detecting and mitigating spoofing attack against an automotive radar," in *Proceedings of IEEE 88th Vehicular Technology Conference*, 2018, pp. 1-6.
28. P. Misra and P. Enge, *Global Positioning System: Signals, Measurements and Performance*, Ganga-Jamuna Press, MA, 2nd ed., Vol. 2, 2006, pp. 1-7.
29. S. Kiese, "Gotta Catch Em All - C Worldwide! (or how to spoof GPS to cheat at Pokmon GO)," in *INSINUATOR*, https://insinuator.net/2016/07/gotta-catch-em-all-worldwide-or-how-to-spoof-gps-to-cheat-at-pokemon-go/, 2018.
30. H. Hu and N. Wei, "A study of GPS jamming and anti-jamming," in *Proceedings of the 2nd International Conference on Power Electronics and Intelligent Transportation System*, Vol. 1, 2009, pp. 388-391.
31. L. Huang and Q. Yang, "Low-cost GPS simulator GPS spoofing by SDR," in *DEF CON 23*, 2015.

32. "Software-defined GPS signal simulator," https://github.com/osqzss/gps-sdr-sim, 2017.
33. I. G. Ferrão, S. A. da Silva, D. F. Pigatto, and K. R. Branco, "GPS spoofing: Detecting GPS fraud in unmanned aerial vehicles," in *Proceedings of IEEE Latin American Robotics Symposium, 2020 Brazilian Symposium on Robotics and 2020 Workshop on Robotics in Education*, 2020, pp. 1-6.
34. M. L. Psiaki and T. E. Humphreys, "GNSS spoofing and detection," *Proceedings of the IEEE*, Vol. 104, 2016, pp. 1258-1270.
35. L. Zhu, L. Yu, Z. Cai, X. Liu, and J. Zhang, "K-anonymous based anti-positioning security strategy in mobile networks." *Journal of Information Science and Engineering*, Vol. 38, 2022, pp. 121-138.
36. U. Hunkeler, J. Colli-Vignarelli, and C. Dehollain, "Effectiveness of GPS-jamming and countermeasures," in *Proceedings of International Conference on Localization and GNSS*, 2012, pp. 1-4.
37. P. Y. Montgomery, T. E. Humphreys, and B. M. Ledvina, "A multi-antenna defense: Receiver-autonomous GPS spoofing detection," *Inside GNSS*, Vol. 4, 2009, pp. 40-46.
38. M. Meurer, A. Konovaltsev, M. Cuntz, and C. Hättich, "Robust joint multi-antenna spoofing detection and attitude estimation using direction assisted multiple hypotheses RAIM," in *Proceedings of the 25th International Technical Meeting of the Satellite Division of the Institute of Navigation*, 2012, pp. 3007-3016.
39. J. S. Warner and R. G. Johnston, "GPS spoofing countermeasures," *Homeland Security Journal*, Vol. 25, 2003, pp. 19-27.
40. G. D. L. T. Parra, P. Rad, and K. R. Choo, "Driverless vehicle security: Challenges and future research opportunities," *Future Generation Computer Systems*, Vol. 108, 2020, pp. 1092-1111.
41. Z. Haider and S. Khalid, "Survey on effective GPS spoofing countermeasures," in *Proceedings of the 6th International Conference on Innovative Computing Technology*, 2016, pp. 573-577.
42. R. A. Agyapong, M. Nabil, A.-R. Nuhu, M. I. Rasul, and A. Homaifar, "Efficient detection of GPS spoofing attacks on unmanned aerial vehicles using deep learning," in *Proceedings of IEEE Symposium Series on Computational Intelligence*, 2021, pp. 01-08.
43. Y. Dang, C. Benzaid, B. Yang, and T. Taleb, "Deep learning for GPS spoofing detection in cellular enabled unmanned aerial vehicle systems," *arXiv Preprint*, 2022, arXiv:2201.00568.
44. M. Wolf, A. Weimerskirch, and C. Paar, "Security in automotive bus systems," in *Proceedings of Workshop on Embedded Security in Cars*, 2004.
45. W. Zeng, M. A. S. Khalid, and S. Chowdhury, "In-vehicle networks outlook: Achievements and challenges," *IEEE Communications Surveys Tutorials*, Vol. 18, 2016, pp. 1552-1571.
46. L. Yu, J. Deng, R. R. Brooks, and S. B. Yun, "Automobile ECU design to avoid data tampering," in *Proceedings of the 10th ACM Annual Cyber and Information Security Research Conference*, 2015, p. 10.

47. H. Schweppe and Y. Roudier, "Security and privacy for in-vehicle networks," in *IEEE 1st International Workshop on Vehicular Communications, Sensing, and Computing*, 2012, pp. 12-17.
48. H. Schweppe, Y. Roudier, B. Weyl, L. Apvrille, and D. Scheuermann, "Car2X communication: Securing the last meter – a cost-effective approach for ensuring trust in car2X applications using in-vehicle symmetric cryptography," in *IEEE Vehicular Technology Conference*, 2011, pp. 1-5.
49. C. Miller and C. Valasek, "Remote exploitation of an unaltered passenger vehicle," in *Black Hat USA*, Vol. 2015, 2015.
50. S. Mazloom, M. Rezaeirad, A. Hunter, and D. McCoy, "A security analysis of an in-vehicle infotainment and APP platform," in *Proceedings of the 10th USENIX Workshop on Offensive Technologies* https://www.usenix.org/conference/woot16/workshop-program/presentation/mazloom, 2016.
51. I. Studnia, V. Nicomette, E. Alata, Y. Deswarte, M. Kaaniche, and Y. Laarouchi, "Survey on security threats and protection mechanisms in embedded automotive networks," in *Proceedings of the 43rd Annual IEEE/IFIP Conference on Dependable Systems and Networks Workshop*, 2013, pp. 1-12.
52. O. I. de Normalización, *ISO 11898: Road Vehicles: Interchange of Digital Information: Controller Area Network (CAN) for High-speed Communication*, ISO, 1993.
53. Y. Zhang, M. Chen, N. Guizani, D. Wu, and V. C. M. Leung, "SOVCAN: Safety-oriented vehicular controller area network," *IEEE Communications Magazine*, Vol. 55, 2017, pp. 94-99.
54. E. Choi, S. Han, J. Lee, S. Lee, S. Kang, and J. Choi, "Compatibility analysis of the turbo controller area network (TURBO CAN)," *IEEE Transactions on Vehicular Technology*, Vol. 67, 2018, pp. 5146-5157.
55. K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, "Experimental security analysis of a modern automobile," in *IEEE Symposium on Security and Privacy*, 2010, pp. 447-462.
56. S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, T. Kohno *et al.*, "Comprehensive experimental analyses of automotive attack surfaces." in *Proceedings of USENIX Security Symposium*, 2011, pp. 77-92.
57. S. Woo, H. J. Jo, and D. H. Lee, "A practical wireless attack on the connected car and security protocol for in-vehicle CAN," *IEEE Transactions on Intelligent Transportation Systems*, Vol. 16, 2015, pp. 993-1006.
58. K.-T. Cho and K. G. Shin, "Error handling of in-vehicle networks makes them vulnerable," in *Proceedings of ACM SIGSAC Conference on Computer and Communications Security*, 2016, pp. 1044-1055.
59. K.-T. Cho, Y. Kim, and K. G. Shin, "Who killed my parked car?" *arXiv Preprint*, 2018, arXiv:1801.07741.
60. K. Iehira, H. Inoue, and K. Ishida, "Spoofing attack using bus-off attacks against a specific ECU of the CAN bus," in *Proceedings of the 15th IEEE Annual Consumer Communications Networking Conference*, 2018, pp. 1-4.
61. A. Wahaballa, Z. Qin, H. Abdalla, M. Abdellatief, and M. A. Elfaki, "Oblivious transfer with hidden access control and outsourced decryption from deterministic

finite automata-based functional encryption for an in-vehicle sensor database system," *Transactions on Emerging Telecommunications Technologies*, Vol. 33, 2022, p. e3870.
62. M. Wolf and T. Gendrullis, "Design, implementation, and evaluation of a vehicular hardware security module," in *Proceedings of International Conference on Information Security and Cryptology*, 2011, pp. 302-318.
63. H. Oguma, A. Yoshioka, M. Nishikawa, R. Shigetomi, A. Otsuka, and H. Imai, "New attestation based security architecture for in-vehicle communication," in *Proceedings of IEEE Global Telecommunications Conference*, 2008, pp. 1-6.
64. A. Van Herrewege, D. Singelee, and I. Verbauwhede, "CANAuth-a simple, backward compatible broadcast authentication protocol for CAN bus," in *Proceedings of ECRYPT Workshop on Lightweight Cryptography*, 2011, pp. 28-29.
65. A. Hazem and H. Fahmy, "LCAP-a lightweight CAN authentication protocol for securing in-vehicle networks," in *Proceedings of the 10th escar Embedded Security in Cars Conference*, Vol. 6, 2012, p. 172.
66. B. Groza and S. Murvay, "Efficient protocols for secure broadcast in controller area networks," *IEEE Transactions on Industrial Informatics*, Vol. 9, 2013, pp. 2034-2042.
67. Q. Wang and S. Sawhney, "VeCure: A practical security framework to protect the CAN bus of vehicles," in *Proceedings of International Conference on the Internet of Things (IoT)*, 2014, pp. 13-18.
68. H. Ueda, R. Kurachi, H. Takada, T. Mizutani, M. Inoue, and S. Horihata, "Security authentication system for in-vehicle network," *SEI Technical Review*, Vol. 81, 2015, pp. 5-9.
69. H. J. Jo, J. H. Kim, H. Choi, W. Choi, D. H. Lee, and I. Lee, "Mauth-can: Masquerade-attack-proof authentication for in-vehicle networks," *IEEE Transactions on Vehicular Technology*, Vol. 69, 2020, pp. 2204-2218.
70. F. Oberti, E. Sánchez, A. Savino, F. Parisi, and S. D. Carlo, "CAN-MM: multiplexed message authentication code for controller area network message authentication in road vehicles," *CoRR*, Vol. abs/2206.02603, https://doi.org/10.48550/arXiv.2206.02603, 2022.
71. U. E. Larson, D. K. Nilsson, and E. Jonsson, "An approach to specification-based attack detection for in-vehicle networks," in *Proceedings of IEEE Intelligent Vehicles Symposium*, 2008, pp. 220-225.
72. H. Nakayama, S. Kurosawa, A. Jamalipour, Y. Nemoto, and N. Kato, "A dynamic anomaly detection scheme for AODV-based mobile ad hoc networks," *IEEE Transactions on Vehicular Technology*, Vol. 58, 2009, pp. 2471-2481.
73. H. M. Song, H. R. Kim, and H. K. Kim, "Intrusion detection system based on the analysis of time intervals of CAN messages for in-vehicle network," in *Proceedings of International Conference on Information Networking*, 2016, pp. 63-68.
74. M. Kang and J. Kang, "A novel intrusion detection method using deep neural network for in-vehicle network security," in *Proceedings of IEEE 83rd Vehicular Technology Conference*, 2016, pp. 1-5.
75. B. Zhang, X. Xiao, W. Zhang, A. Kumar Sangaiah, Y. Zhou, and X. Liu, "A co-occurrence matrix-based masquerade detection method in in-vehicle network," *Transactions on Emerging Telecommunications Technologies*, Vol. 33, 2022, p. e3858.

76. M. Müter, A. Groll, and F. C. Freiling, "A structured approach to anomaly detection for in-vehicle networks," in *Proceedings of the 6th International Conference on Information Assurance and Security*, 2010, pp. 92-98.
77. M. Müter and N. Asaj, "Entropy-based anomaly detection for in-vehicle networks," in *Proceedings of IEEE Intelligent Vehicles Symposium*, 2011, pp. 1110-1115.
78. P. Murvay and B. Groza, "Source identification using signal characteristics in controller area networks," *IEEE Signal Processing Letters*, Vol. 21, 2014, pp. 395-399.
79. K.-T. Cho and K. G. Shin, "Fingerprinting electronic control units for vehicle intrusion detection," in *Proceedings of USENIX Security Symposium*, 2016, pp. 911-927.
80. K.-T. Cho and K. G. Shin, "Viden: Attacker identification on in-vehicle networks," in *Proceedings of ACM SIGSAC Conference on Computer and Communications Security*, 2017, pp. 1109-1123.
81. T. Kuwahara, Y. Baba, H. Kashima, T. Kishikawa, J. Tsurumi, T. Haga, Y. Ujiie, T. Sasaki, and H. Matsushima, "Supervised and unsupervised intrusion detection based on CAN message frequencies for in-vehicle network," *Journal of Information Processing*, Vol. 26, 2018, pp. 306-313.
82. B. Groza and P. Murvay, "Efficient intrusion detection with bloom filtering in controller area networks," *IEEE Transactions on Information Forensics and Security*, Vol. 14, 2019, pp. 1037-1051.
83. X. Li, H. Zhang, Y. Miao, S. Ma, J. Ma, X. Liu, and K. R. Choo, "CAN bus messages abnormal detection using improved SVDD in internet of vehicles," *IEEE Internet of Things Journal*, Vol. 9, 2022, pp. 3359-3371.
84. M. Postolache, G. Neamtu, and S. D. Trofin, "CAN – Ethernet gateway for automotive applications," in *Proceedings of the 17th International Conference on System Theory, Control and Computing*, 2013, pp. 422–427.
85. C. Corbett, E. Schoch, F. Kargl, and F. Preussner, "Automotive ethernet: security opportunity or challenge?" in *Sicherheit, Schutz und Zuverlassigkeit*, M. Meier, D. Reinhardt, and S. Wendzel, (eds.), Gesellschaft fur Informatik e.V., Bonn, 2016, pp. 45-54.
86. C. Corbett, T. Basic, T. Lukaseder, and F. Kargl, "A testing framework architecture for automotive intrusion detection systems," *Automotive-Safety & Security 2017-Sicherheit und Zuverlässigkeit für automobile Informationstechnik*, 2017.
87. N. Alkhatib, M. Mushtaq, H. Ghauch, and J.-L. Danger, "Unsupervised network intrusion detection system for avtp in automotive ethernet networks," in *Proceedings of IEEE Intelligent Vehicles Symposium*, 2022, pp. 1731-1738.
88. S. Jeong, B. Jeon, B. Chung, and H. K. Kim, "Convolutional neural network-based intrusion detection system for avtp streams in automotive ethernet-based networks," *Vehicular Communications*, Vol. 29, 2021, p. 100338.
89. N. Alkhatib, H. Ghauch, and J.-L. Danger, "Some/ip intrusion detection using deep learning-based sequential models in automotive ethernet networks," in *Proceedings of IEEE 12th Annual Information Technology, Electronics and Mobile Communication Conference*, 2021, pp. 0954-0962.
90. R. Makowitz and C. Temple, "FlexRay-a communication network for automotive control systems," in *Proceedings of IEEE International Workshop on Factory Communication Systems*, 2006, pp. 207-212.

91. ISO, "Road vehicles–flexray communications system–part 1: General information and use case definition," *International Organization for Standardization*, Vol. ISO 17458-1, 2013.
92. C. Bernardini, M. R. Asghar, and B. Crispo, "Security and privacy in vehicular communications: Challenges and opportunities," *Vehicular Communication*, Vol. 10, 2017, pp. 13-28.
93. D. K. Nilsson, U. Larson, F. Picasso, and E. Jonsson, "A first simulation of attacks in the automotive network communications protocol flexray," in *Proceedings of International Workshop on Computational Intelligence for Security in Information Systems*, Vol. 53, 2008, pp. 84-91.
94. D. Püllen, N. A. Anagnostopoulos, T. Arul, and S. Katzenbeisser, "Security and safety co-engineering of the flexray bus in vehicular networks," in *Proceedings of ACM International Conference Omni-Layer Intelligent Systems*, 2019, pp. 31-37.
95. T. Lee and R. Lin, and I. Liao, "Design of a flexray/ethernet gateway and security mechanism for in-vehicle networks," *Sensors*, Vol. 20, 2020, p. 641.
96. J. H. Kim, S.-H. Seo, N. T. Hai, B. M. Cheon, Y. S. Lee, and J. W. Jeon, "Gateway framework for in-vehicle networks based on can, flexray, and ethernet," *IEEE Transactions on Vehicular Technology*, Vol. 64, 2015, pp. 4472-4486.
97. D. Püllen, N. A. Anagnostopoulos, T. Arul, and S. Katzenbeisser, "Securing flexray-based in-vehicle networks," *Microprocessors and Microsystems*, Vol. 77, 2020, p. 103144.
98. MOST Cooperation, "Media oriented systems transport (most)," http://www. most-cooperation. com/.–Zugriffsdatum, 2011, pp. 01-06.
99. I. A. Grzemba, *MOST: the Automotive Multimedia Network*, Franzis Verlag, 2012.
100. H.-C. von der Wense, "Introduction to the local interconnect network (LIN) bus," SAE Technical Paper, No. 9733, http://www.ni.com/white-paper/9733/en/, 2000.
101. J. Stelzer, "LIN bus – an emerging standard for body control APPs," *EE Times Asia*, Vol. 12, 2004, pp. 24-26.
102. M. Wolf, A. Weimerskirch, and C. Paar, "Secure in-vehicle communication," *Embedded Security in Cars*, 2006, pp. 95-109.
103. J. Takahashi, Y. Aragane, T. Miyazawa, H. Fuji, H. Yamashita, K. Hayakawa, S. Ukai, and H. Hayakawa, "Automotive attacks and countermeasures on LIN-Bus," *Journal of Information Processing*, Vol. 25, 2017, pp. 220-228.
104. F. Oberti, E. Sanchez, A. Savino, F. Parisi, M. Brero, and S. Di Carlo, "Lin-mm: Multiplexed message authentication code for local interconnect network message authentication in road vehicles," *arXiv Preprint*, 2022, arXiv:2206.02602.
105. R. Rajamani, A. S. Howell, J. K. Hedrick, and M. Tomizuka, "A complete fault diagnostic system for automated vehicles operating in a platoon," *IEEE Transactions on Control Systems Technology*, Vol. 9, 2001, pp. 553-564.
106. T. Nguyen, B. M. Cheon, and J. W. Jeon, "CAN FD performance analysis for ECU re-programming using the CANoe," in *Proceedings of the 18th IEEE International Symposium on Consumer Electronics*, 2014, pp. 1-4.
107. A. X. A. Sim and B. Sitohang, "OBD-II standard car engine diagnostic software development," in *Proceedings of International Conference on Data and Software Engineering*, 2014, pp. 1-5.

108. R. Čech, P. Tomčík, and J. Kulhánek, "Setting of combustion engine ECU parameters with use of knocking detection," in *Proceedings of the 16th International Carpathian Control Conference*, 2015, pp. 69-72.
109. L. Yu, J. Deng, R. R. Brooks, and S. B. Yun, "Automobile ECU design to avoid data tampering," in *Proceedings of the 10th ACM Annual Cyber and Information Security Research Conference*, 2015, pp. 10:1-10:4.
110. M. S. U. Alam, S. Iqbal, M. Zulkernine, and C. Liem, "Securing vehicle ECU communications and stored data," in *Proceedings of IEEE International Conference on Communications*, 2019, pp. 1-6.
111. M. H. Sarwar, M. A. Shah, M. Umair, and S. H. Faraz, "Network of ECUs software update in future vehicles," in *Proceedings of IEEE 25th International Conference on Automation and Computing*, 2019, pp. 1-5.
112. P. Sharma and D. P. Möller, "Protecting ECUs and vehicles internal networks," in *Proceedings of IEEE International Conference on Electro/Information Technology*, 2018, pp. 0465-0470.
113. M. Tian, R. Jiang, C. Xing, H. Qu, Q. Lu, and X. Zhou, "Exploiting temperature-varied ecu fingerprints for source identification in in-vehicle network intrusion detection," in *Proceedings of IEEE 38th International Performance Computing and Communications Conference*, 2019, pp. 1-8.
114. S. Jafarnejad, L. Codeca, W. Bronzi, R. Frank, and T. Engel, "A car hacking experiment: When connectivity meets vulnerability," in *Proceedings of IEEE Globecom Workshops*, 2015, pp. 1-6.
115. Y. Zhou and D. Feng, "Side-channel attacks: Ten years after its publication and the impacts on cryptographic module security testing," *IACR Cryptology ePrint Archive*, Vol. 2005, 2005, p. 388.
116. C. Smith, *The Car Hacker's Handbook: A Guide for the Penetration Tester*, No Starch Press, 2016.
117. C. Corbett, M. Brunner, K. Schmidt, R. Schneider, and U. Dannebaum, "Leveraging hardware security to secure connected vehicles," in *SAE Technical Paper*, SAE International, 2018.
118. L. Apvrille, R. El Khayari, O. Henniger, Y. Roudier, H. Schweppe, H. Seudié, B. Weyl, and M. Wolf, "Secure automotive on-board electronics network architecture," in *Proceedings of FISITA World Automotive Congress*, Vol. 8, 2010, pp. 1-9.
119. "E-safety vehicle intrusion protected applications (EVITA) project," www.evita-project.org/, 2018.
120. Z. MacHardy, A. Khan, K. Obana, and S. Iwashina, "V2X access technologies: Regulation, research, and remaining challenges," *IEEE Communications Surveys Tutorials*, Vol. 20, 2018, pp. 1858-1877.
121. K. B. Kelarestaghi, M. Foruhandeh, K. Heaslip, and R. M. Gerdes, "Survey on vehicular ad hoc networks and its access technologies security vulnerabilities and countermeasures," *arXiv Preprint*, 2019, arXiv:1903.01541.
122. C. Lai, R. Lu, D. Zheng, and X. S. Shen, "Security and privacy challenges in 5g-enabled vehicular networks," *IEEE Network*, Vol. 34, 2020, pp. 37-45.

123. Y. Cao, S. Xu, J. Liu, and N. Kato, "Toward smart and secure v2x communication in 5g and beyond: A uav-enabled aerial intelligent reflecting surface solution," *IEEE Vehicular Technology Magazine*, Vol. 17, 2022, pp. 66-73.
124. A. Alnasser, H. Sun, and J. Jiang, "Cyber security challenges and solutions for V2X communications: A survey," *Computer Networks*, Vol. 151, 2019, pp. 52-67.
125. F. Qu, Z. Wu, F. Wang, and W. Cho, "A security and privacy review of VANETs," *IEEE Transactions on Intelligent Transportation Systems*, Vol. 16, 2015, pp. 2985-2996.
126. N. Sharma, N. Chauhan, N. Chand, and L. K. Awasthi, "Secure authentication and session key management scheme for internet of vehicles," *Transactions on Emerging Telecommunications Technologies*, 2022, p. e4451.
127. G. Twardokus and H. Rahbari, "Vehicle-to-nothing? securing C-V2X against protocol-aware dos attacks," in *Proceedings of IEEE INFOCOM Conference on Computer Communications*, 2022, pp. 1629-1638.
128. Y. Yoon and H. Kim, "An evasive scheduling enhancement against packet dropping attacks in c-v2x communication," *IEEE Communications Letters*, Vol. 25, 2020, pp. 392-396.
129. H. Bangui, M. Ge, B. Buhnova, and L. Hong Trang, "Towards faster big data analytics for anti-jamming applications in vehicular ad-hoc network," *Transactions on Emerging Telecommunications Technologies*, Vol. 32, 2021, p. e4280.
130. C. Zhang, X. Lin, R. Lu, P. Ho, and X. Shen, "An efficient message authentication scheme for vehicular communications," *IEEE Transactions on Vehicular Technology*, Vol. 57, 2008, pp. 3357-3368.
131. Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, "An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications," *IEEE Transactions on Vehicular Technology*, Vol. 59, 2010, pp. 3589-3603.
132. R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, "Pseudonym changing at social spots: An effective strategy for location privacy in VANETs," *IEEE Transactions on Vehicular Technology*, Vol. 61, 2012, pp. 86-96.
133. S. Chang, Y. Qi, H. Zhu, J. Zhao, and X. Shen, "Footprint: Detecting sybil attacks in urban vehicular networks," *IEEE Transactions on Parallel and Distributed Systems*, Vol. 23, 2012, pp. 1103-1114.
134. R. Lu, X. Lin, X. Liang, and X. Shen, "A dynamic privacy-preserving key management scheme for location-based services in VANETs," *IEEE Transactions on Intelligent Transportation Systems*, Vol. 13, 2012, pp. 127-139.
135. A. Ahmed, K. A. Bakar, M. I. Channa, K. Haseeb, and A. W. Khan, "TERP: A trust and energy aware routing protocol for wireless sensor network," *IEEE Sensors Journal*, Vol. 15, 2015, pp. 6962-6972.
136. N. Haddadou, A. Rachedi, and Y. Ghamri-Doudane, "A job market signaling scheme for incentive and trust management in vehicular ad hoc networks," *IEEE Transactions on Vehicular Technology*, Vol. 64, 2015, pp. 3657-3674.
137. N. Rafique, M. A. Khan, N. A. Saqib, F. Bashir, C. Beard, and Z. Li, "Black hole prevention in VANETs using trust management and fuzzy logic analyzer," *International Journal of Computer Science and Information Security*, Vol. 14, 2016, p. 1226.

138. J. Kang, R. Yu, X. Huang, M. Jonsson, H. Bogucka, S. Gjessing, and Y. Zhang, "Location privacy attacks and defenses in cloud-enabled internet of vehicles," *IEEE Wireless Communications*, Vol. 23, 2016, pp. 52-59.
139. O. Zhao, X. Liu, X. Li, P. Singh, and F. Wu, "Privacy-preserving data aggregation scheme for edge computing supported vehicular ad hoc networks," *Transactions on Emerging Telecommunications Technologies*, Vol. 33, 2022, p. e3952.
140. T. Zhang, H. Antunes, and S. Aggarwal, "Defending connected vehicles against malware: Challenges and a solution framework," *IEEE Internet of Things Journal*, Vol. 1, 2014, pp. 10–21.
141. S. Seifert and R. Obermaisser, "Secure automotive gateway – secure communication for future cars," in *Proceedings of the 12th IEEE International Conference on Industrial Informatics*, 2014, pp. 213-220.
142. G. Sun, Y. Cong, J. Dong, Q. Wang, L. Lyu, and J. Liu, "Data poisoning attacks on federated machine learning," *IEEE Internet Things Journal*, Vol. 9, 2022, pp. 11 365-11 375.
143. Z. Yin, M. Jia, N. Cheng, W. Wang, F. Lyu, Q. Guo, and X. Shen, "UAV-assisted physical layer security in multi-beam satellite-enabled vehicle communications," *IEEE Transactions on Intelligent Transportation Systems*, Vol. 23, 2022, pp. 2739-2751.
144. A. Yang, J. Weng, K. Yang, C. Huang, and X. Shen, "Delegating authentication to edge: A decentralized authentication architecture for vehicular networks," *IEEE Transactions on Intelligent Transportation Systems*, Vol. 23, 2022, pp. 1284-1298.
145. F. Song, Z. Qin, D. Liu, J. Zhang, X. Lin, and X. Shen, "Privacy-preserving task matching with threshold similarity search via vehicular crowdsourcing," *IEEE Transactions on Vehicular Technology*, Vol. 70, 2021, pp. 7161-7175.
146. C. Huang, R. Lu, J. Ni, and X. Shen, "DAPA: A decentralized, accountable, and privacy-preserving architecture for car sharing services," *IEEE Transactions on Vehicular Technology*, Vol. 69, 2020, pp. 4869-4882.

Xifeng Wang received the BS degree in Communication Engineering from Jilin University, Changchun, China, in 2016. She is currently pursuing the Ph.D. degree at the State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, China. She was a Visiting Ph.D. student at The University of Waterloo, Canada, from 2021 to 2022. Her research interests include security and privacy in the Internet of Vehicles and the Intelligent Connected vehicle.

Limin Sun received the BS and Ph.D. degrees from the National University of Defense Technology, Changsha, China, in 1988 and 1998, respectively. He is a Professor at the Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China. He is also with the School of Cyber Security, University of Chinese Academy of Sciences, Beijing. His research interests include mobile vehicle networks, Internet of Things security, and wireless sensor networks.

Chao Wang received the Ph.D. degree from the Beijing Institute of Technology. He was a Visiting Scholar with The George Washington University, from 2012 to 2014. He is currently a Faculty Member of the School of Information Science and Technology, North China University of Technology. He has published several research articles in refereed international conferences and premier journals. His research interests include security and privacy in cyber-physical systems and the Internet of Vehicles.

Hongsong Zhu received the Ph.D. degree from the Institute of Computing Technology, Chinese Academy of Sciences. He is currently a Professor with the Institute of Information Engineering, Chinese Academy of Sciences, and the University of Chinese Academy of Sciences. His main research interests include network measurement, Internet-of-Things (IoT) security, and defense against social engineering. He is also a Senior Member of the China Computer Federation and a member of the Select Committee of China Computer Federation Technical Commission on Sensor Network.

Lian Zhao received the Ph.D. degree from the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada, in 2002. She is currently a Professor at the Department of Electrical, Computer, and Biomedical Engineering, Ryerson University, Toronto, ON, Canada. Her research interests are in the areas of wireless communications, resource management, mobile edge computing, caching and communications, and vehicular ad hoc networks. She received the Best Land Transportation Paper Award from IEEE Vehicular Technology Society in 2016, the Top 15 Editor Award in 2016 for IEEE Transactions on Vehicular Technology, the Best Paper Award from the 2013 International Conference on Wireless Communications and Signal Processing (WCSP), and the Canada Foundation for Innovation (CFI) New Opportunity Research Award in 2005. She served as the Co-Chair for the Wireless Communication Symposium, IEEE Globecom 2020 and IEEE ICC 2018, the Local Arrangement Co-Chair for IEEE VTC Fall 2017 and IEEE Infocom 2014, and the Co-Chair for the Communication Theory Symposium, IEEE Globecom 2013. She has been serving as an Editor for IEEE Transactions on Wireless Communications, IEEE Internet of Things Journal, and IEEE Transactions on Vehicular Technology. She has been an IEEE Communication Society (ComSoc) Distinguished Lecturer (DL).

Shujie Yang received his Ph.D. degree from the Institute of Network Technology, Beijing University of Posts and Telecommunications, Beijing, China, in 2017, where he is currently a Lecturer with the State Key Laboratory of Networking and Switching Technology. His major research interests are in the areas of wireless communications and wireless networking.

Changqiao Xu received the Ph.D. degree from the Institute of Software, Chinese Academy of Sciences in January 2009. He was an Assistant Research Fellow and R&D Project Manager in ISCAS from 2002 to 2007. He was a researcher at Athlone Institute of Technology and Joint Training Ph.D. at Dublin City University, Ireland during 2007-2009. He joined Beijing University of Posts and Telecommunications, Beijing, China, in December 2009. Currently, he is a Professor with the State Key Laboratory of Networking and Switching Technology, and Director of the Network Architecture Research Center at BUPT. His research interests include Future Internet Technology, Mobile Networking, Multimedia Communications, and Network Security. He has edited two books and published over 200 technical papers in prestigious international journals and conferences, including IEEE/ACM ToN, IEEE TMC, IEEE INFOCOM, ACM Multimedia *etc*. He has served a number of international conferences and workshops as a Co-Chair and TPC member. He is currently serving as the Editor-in-Chief of Transactions on Emerging Telecommunications Technologies. He is a senior member of IEEE.