*Review*

# Security Issues and Solutions for Connected and Autonomous Vehicle in Sustainable City: A Survey

**Zhendong Wang [1]*, Haoran Wei [1]*, Jianda Wang [1], Xiaoming Zeng [1] and Yuchao Chang [2]**

[1] Department of ECE, University of Texas at Dallas; zhendong.wang@utdallas.edu(Z.W.), haoran.wei@utdallas.edu(H.W.), jianda.wang@utdallas.edu(J.W.), xiaoming.zeng@utdallas.edu(X.Z.)
[2] Shanghai Jiaotong University; yuchaoch@126.com
* Correspondence: zhendong.wang@utdallas.edu, wzhend@alumni.uml.edu (Z.W.), haoran.wei@utdallas.edu(H.W.)

**Abstract:** Connected and Autonomous Vehicle (CAV) combines technologies of autonomous vehicle (AV) and connected vehicles (CV) to develop quicker, more reliable and safer traffic. Artificial Intelligence (AI) based CAV solutions play significant roles in sustainable city. The convergence imposes stringent security requirements for CAV safety and reliability. In practice, vehicles are developed with increased automation and connectivity. Increased automation increases the reliance on the sensor-based technologies and decreases the reliance on driver; increased connectivity increases the exposures of vehicles vulnerability and increases the risk for an adversary to implement a cyber-attack. Much work has been dedicated to identifying the security vulnerabilities and recommending mitigation techniques associated with different sensors, controllers, and connection mechanisms, respectively. However, there is an absence of comprehensive and in-depth studies to identify how the cyber-attacks exploit the vehicles vulnerabilities to negatively impact the performance and operations of CAV. In this survey, we set out to thoroughly review the security issues introduced by AV and CV technologies, analyze how the cyber-attacks impact the performance of CAV, and summarize the solutions correspondingly. The impact of cyber-attacks on the performance of CAV is elaborated from both viewpoints of intra-vehicle system and inter-vehicle system. We pointed out that securing the perception and operations of CAV would be the top requirement to enable CAV to be applied safely and reliably in practice. Also, we suggested to utilize cloud and new AI methods to defend against smart cyber-attacks on CAV.

**Keywords:** artificial intelligence; autonomous vehicles; connected vehicles; CAV; security; cyber-attacks; Intra-/inter-vehicle system; cloud; sustainable city application

## 1. Introduction

CAV effectively combines technologies of sensor-based autonomous vehicles and communication-based connected vehicles, and it is anticipated that the convergence will greatly improve safety and reduce cost, emissions and energy consumption, and change the way they are operated today. Currently, vehicles are being developed with increasing levels of connectivity and automation. Many new vehicles and aftermarket systems are already at Level 2 and approaching Level 3 and provide partially-autonomous capability [1]. However, with the ascendance of CAV, drivers involve less control and management of the vehicle; increased automation exacerbates the security risk by increasing the possibilities for adversaries to implement a successful attack. Meanwhile, the increased connectivity of the vehicles increases the exposure of potential vulnerabilities and paves avenues for cyber-attacks. The development of CAV is inevitably facing great security threats and attacks risks.

In early stage, manual vehicle is not equipped with much connectivity to the outside, therefore, hackers must have physical access to the vehicle, which causes great difficulty for hackers to perform the attack. In [2] [3], researchers showed they could use wired connections to the vehicle to manipulate the vehicle, such as controlling the display

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 September 2022 doi:10.20944/preprints202209.0230.v1

dashboard, killing the engine, disturbing the steering, etc. However, the demonstrations do not attract much attention from the audience. In recent years, the advancement in AV technology allows a diverse type of sensors to be installed on the vehicle to assist humans driving. For example, Google's driverless car utilizes more than ten types of sensors to move autonomously on the road. However, sensors are easily affected by noise and fooled by malicious attacks, which can cause dangers and accidents [4] [5]. Due to people's concerns on the AV's reliance, many efforts have been dedicated to the studies of AV security and safety issues.

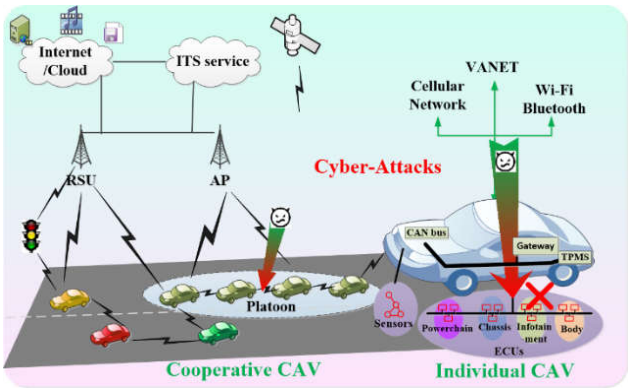


**Figure 1.** Overview of Connected and Autonomous Vehicle (CAV) and the cyber-attacks.

As AV has evolved, many types of wireless connectivity technologies are installed on the vehicle, such as Bluetooth, keyless remote entry, telematics connected to the internet, and VANET, etc. The increased connectivity not only provides more convenience and better safety for the driver, but also speeds up the development of subsequent automation. However, the expansion of vehicle connectivity exposes more vulnerabilities of the vehicle and increases the opportunities for attackers to implement cyber-attacks. [6] showed that a vehicle can be compromised through Bluetooth connection meters away from the vehicle. [3] showed that the attackers successfully hacked an unaltered Jeep Cherokee through cellular network and then controlled the vehicle critical functions remotely, such as disabling brakes and steering, etc. [4] investigated potential cybersecurity threats to both individual automated vehicle and cooperative automated vehicles. [5] surveyed cyber threats facing CAV from three aspects of vehicles, human, and connection infrastructure. Recently, with the flourishing and advancement of IoT and sensing networks, the CAV and even Internet of Vehicles are deeply involved in intelligent transportation and smart city development. Thus, [129] provided detailed analyses on characteristics, architecture, and challenges of intelligent transportation systems. [130] comprehensively investigated how the smart city development imposes precedented security and privacy challenges on intelligent transportation and intelligent infrastructures, such as smart parking, intelligent navigation and electrical vehicle charging, which illustrates the obstacles of widely deploying CAV.

Clearly, CAV faces great security risks. Although much effort has been dedicated to identifying security vulnerabilities and recommending potential mitigation techniques for AV and CV, respectively, there is still an absence of in-depth and comprehensive research to study how cyber-attacks can exploit the vulnerabilities of CAV to negatively impact the physical operation and performance of CAV. Therefore, the purposes of the work are to thoroughly investigate the potential vulnerabilities and security issues of CAV from the viewpoints of individual autonomous vehicle technologies (e.g., sensors, in-vehicle system) and connected vehicle technologies, and accordingly, to identify the negative impacts of cyber-attacks on the physical operation and performance of CAV from the perspectives of intra-vehicle system and inter-vehicles systems. The work aims to create a future roadmap for CAV development and deployment. Figure 1 shows the cyber-attacks on CAV. The main contribution of the paper are as follows,

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 September 2022 doi:10.20944/preprints202209.0230.v1

1) summarized the security issues and solutions for AV associated with different sensors, controllers and in-vehicle network.
2) investigated the connectivity technologies of CV and analyzed their advantages and applications in CAV, as well as identified the security issues of each type.
3) accordingly analyzed the impact of cyber-attacks on CAV: cyber-attacks on intra-vehicle system to impact the individual CAV, and cyber-attacks on vehicle connectivity to impact the cooperative CAV.
4) proposed future directions to enhance the CAV security.

The paper is organized as follows. As AV highly depends on the various sensors technologies and in-vehicle systems to perform perceptions and actions, these sensors and in-vehicle systems expose vulnerabilities to malicious agents. Thus, we first summarized the security issues and solutions of sensors and in-vehicle systems in section II. Then, besides the individual AV technologies, CAV also utilizes various communication and connection technologies to achieve autonomous driving and cooperative driving. Thus, we extended to investigating the main connectivity technologies in CV and analyzed the security issues exposed by these various types of connectivity technologies in Section III. With AV and CV technologies further converging and composing the entire CAV to constitute a vehicular cypher-physical system (VCPS), including intra-vehicle and inter-vehicles systems, we deep-analyzed cyber-attacks on VCPS in Section IV. Finally, in section V, we dis-cussed the future work and directions. Section VI concludes the work.

## 2. Security issues facing AV and solutions

For a manual vehicle, the driver perceives the environment and takes control actions, while an autonomous vehicle mainly relies on diverse types of sensors to perceive the environment. Specific types of sensors include cameras, lidar, radar, GPS, tire pressure measure sensor (TPMS), Inertial measurement units (IMU), engine control sensor, etc. Currently, some of these sensors have been installed on manual vehicles to assist drivers and achieve partially-autonomous driving. However, all these sensors have vulnerabilities and can be attacked by malicious adversaries. Due to the high reliance on sensors, AV faces great security threats. In addition, a vehicle used to be separated from the outside world, thus, almost no security mechanisms have been adopted on the in-vehicle system (i.e., in-vehicle networks and electronic control units (ECUs)). In this section, we mainly investigate the security issues facing an AV, including sensors, in-vehicle networks and ECUs and summarize existing workable solutions. Figure 2 presents the security issues facing an individual AV.

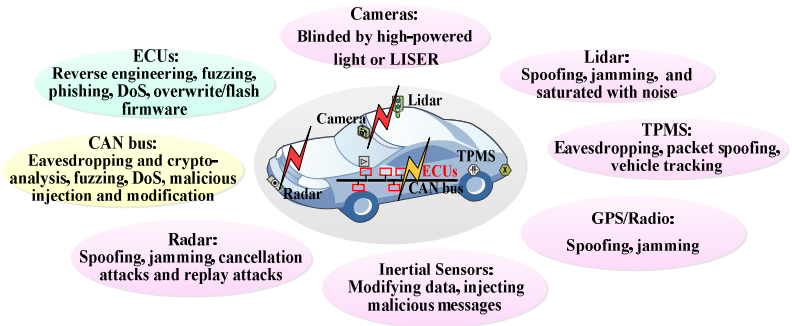


**Figure 2.** Security issues facing AV.

### *2.1. Sensors*

The type and functionality of a sensor determines the extent to which it could contribute to scoping out secure threats, as well as the extent to which it could inform potential implications should it be compromised [5]. Table 1 summarizes the applications, security issues and the corresponding solutions for common sensors mounted on AV.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 September 2022 doi:10.20944/preprints202209.0230.v1

For partially-autonomous vehicles, sensors only assist the driver to obtain some information and the vehicle is still monitored and controlled by the driver. Even for Google's driverless car that operates autonomously at most times, the driver will take over of control immediately if the automation system cannot process dangerous situations. Therefore, the impact of attacks on these sensors may be mitigated by the driver's surveillance or management. Even so, autonomous vehicles significantly depend on these various types of sensors to perceive the surroundings and the status of the vehicles to assist driving or automatically drive by itself. For example, [131] utilized multiple sensors such as radar, LIDAR and cameras to perform autonomous lane changing. [132] reviews vision based autonomous driving system. [133] proposes an effective empirical formula solution to help autonomous driving in GPS denied environment. [134] provide a survey on intelligent tires for tire-road interaction recognition. [135] proposed a localization system for autonomous driving using gyroscopes and accelerometer. In the future, fully-autonomous vehicle completely operates without driver's involvement. Thus, attacks on these sensors will cause serious results, and must call for more attentions.

**Table 1.** Security issues and solutions of sensors mounted on AV.

| Type | Application | Security issues | Solutions | References |
|---|---|---|---|---|
| Camera | Interpret objects/signs. An array of cameras to provide 360 views, while stereo-cameras can extract extra depth information. | Extra light from other sources may decrease the sensitivity of the sensors; intense light (e.g., Laser, IR LEDs) can directly blind/blaze the sensors. | 1) Camera filter to prevent blinding;<br>2) Installation of multi-cameras to improve the detection;<br>3) Fuse with other sensors to improve the accuracy of detection. | [4], [5], [7], [8], [ 9], [10],[131], [132] |
| Lidar, Radar and Ultrasonic | Lidar provides "3D" map of surrounding environment and depth perception. Radar detects obstacles and measure distances in bad weather conditions/ low light situations. Ultrasonic assists short-range detection. | Spoofing, jamming, saturation, cancellation attacks and replay attacks. | 1) Tunable wavelength emission and random probing to disturb the attacker;<br>2) Data fusion from other sources, like V2V communication, to correct the measure errors. | [4], [11], [5], [12], [13],[131] |
| GPS | Provide real-time position data of the vehicle through the connection with multiple satellites. | Spoofing, jamming. | 1) Validation to prevent spoofing.<br>2) Other types of sensors are integrated to correct the data or maintain reliable navigation service, such as IMU. | [14], [15], [133] |
| TPMS | Measuring the pressure of each tire and provide real-time information to vehicle system. | Eavesdropping, packet spoofing, vehicles tracking, message forgery. | 1) Encrypting packets to defend against eavesdropping and spoofing;<br>2) Reliable software design and detection mechanisms. | [16], [134] |
| Inertial measurement units | Including gyroscopes, accelerometers, etc., to provide velocity, acceleration and orientation data to the control system. | Data modification and injection attacks, DoS. Typically, attacks need physical access to the sensor to interfere with its readings, or alternatively to intercept communication between sensor and control unit. | 1) Using encrypted communication on vehicle's network.<br>2) Monitor signals within regular tolerance;<br>3) Using secondary sensor data to correct measures.<br>4) Implementation of cryptographic solution to ensure data integrity and its authenticity. | [2], [5], [11], [135] |
| Engine control sensor | Including temperature, air flow sensors, etc., to acquire performance data to adjust engine conditions. | | | |

 doi:10.20944/preprints202209.0230.v1

### 2.2. In-vehicle Network

In-vehicle networks are composed of diverse types of bus systems, mainly including CAN, LIN, FlexRay, and MOST. Due to the specific characteristics of each type of bus system, each type possesses distinct vulnerabilities [17]. These bus systems connect diverse types of ECUs together, therefore, any type of bus controller can send messages to any other existing ECU. Among these bus systems, CAN bus works as the backbone of the in-vehicle network to receive many control messages and deliver them to the corresponding ECU. Therefore, we analyze the security issues of CAN. Typically, CAN bus can be categorized into two types: CAN-C and CAN-HIS buses; each of them is designed with distinct functions. Due to the lack of encryption, authentication and authorization on CAN bus, all messages on the bus are transmitted in plaintext; neither source or destination address is included in the message format. Therefore, attacks on CAN bus include eavesdropping and traffic analysis, jamming and DoS, and malicious modification or injection. For attacks aimed at manipulating certain functions of a vehicle, such as steering, braking, the attacker needs access to CAN bus and modify messages on CAN bus or directly inject malicious messages into the bus. In the past, the in-vehicle system was sealed from the outside, the CAN bus can only be accessed on special occasions with the help of special tools; For example, the maintenance technician uses OBD-II scanner to diagnose the system. Recently, increased connectivity on vehicle increased the chances that the in-vehicle network is accessed, which exposed the CAN bus to more types of attacks. For example, the attack successfully accessed the CAN bus and sent messages on the bus remotely from the cellular connection [3].

Much work has been done to boost CAN bus security. Generally, these measures can be categorized into two types: 1) cryptography [17-20], which originated from a) controller authentication, b) message encryption; 2) firewall and physical separation.

1a) Authentication requires that only authorized controllers can communicate over the bus systems. A general way to ensure authentication combing unsymmetrical and symmetric keys is in [17]. 1b) Encryption of CAN message typically involves the data field [20]. The sender and receiver ECUs synchronously manage a sequence number. Sender can use the number and encryption algorithm, like AES-128, to generate cipher text. After receiving the message, the receiver can decrypt the message and verify the source. In practice, implementing a real-time cryptographic solution can cause overhead of extra computation and data transfer time. Thus, a clear trade-off between security, functionality, and efficiency should be taken into consideration.

2) Firewall and Physical separation. An effective way to prevent malicious attacks through OBD-II port is to set up a firewall on the central gateway to filter the outside communication between the port and inside network [56][43]. However, implementation of a firewall usually requires more cost, and results in communication overhead, which should be within the consideration of design. Physically separating the infotainment system from the main inside networks can prevent certain types of attacks. The messages as well as the multimedia interfaces should be forbidden from interfering with the main system during normal driving operation. However, considering that several functions and components cooperate with each other to implement a complicated module, concerns on separation exist that the complicated operations on vehicles will be impacted.

### 2.3. Electronic Control Unit (ECU)

ECU is a kind of embedded system in a vehicle to monitor the real-time state of the corresponding component and feedback the status parameters to the bus system. Meanwhile, ECU processes the information exchanged from the bus system and takes control of operations to adapt vehicle's behavior. The number of ECUs ranges from about 40 in compact cars to about 90 in luxury cars. According to their functions, ECUs are loosely categorized into four types: powertrain, chassis, infotainment, and body control [21]. There are some key ECUs, such as EBCM, playing a critical role in manipulating vehicle's behavior; compromising them will directly kill the vehicle and endanger driver's safety

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 September 2022 doi:10.20944/preprints202209.0230.v1

[22]. In practice, many ECUs are coupled with each other to achieve some complicated control functions [5]. Thus, attacking a single ECU has the potential to impact large control functionality of the vehicle.

Attacks on ECUs might result from compromising a vehicle's sensor network or exploiting the control module directly through diverse types of connectivity. As [23] provided, a comprehensive guide of ECUs vulnerabilities regarding different attack surfaces exist in many popular vehicles in U.S. Specific attacks on ECUs include fuzzing, phishing, DoS [5], etc. A fuzzing attack aims at finding vulnerabilities by sending random packets to ECU. Phishing attack involves masquerading a trusted entity to gain sensitive information and compromise the system. The driver might be tricked by the phisher into flashing the firmware, which will cause permanent damage. In most cases, a fuzzing attack is the first step in creating a phishing attack. Typically, ECUs are configured when a vehicle is manufactured, and have a long lifetime. Therefore, other exploits on ECUs involve overwriting firmware and flashing ECU [22]. The firmware can be modified or replaced by performing a physical and valid update via OBD port. Recently, an ECU update over the air (OTA) has been proposed [24, 25], which would expose more security risks. Table 2 also lists the security mitigations: a) The use of Message Authentication Codes (MAC) and other cryptography solutions are investigated in [6]. b) In practice, a dedicated hardware for encryption purposes, known as hardware secure module (HSM), can be used to perform sophisticated cryptography [21]. HSM usually cannot be tampered with or harmed by external attacks. Therefore, it can be adopted in each ECU to securely store confidential private keys, to trustworthily calculate the reputation of other ECUs, to perform digital signature generation and verification, or to manage the certificate. c) In the future, if updating ECUs over the air is widely adopted in various models, the mitigation of vulnerabilities in the process should be implemented in each step from update center, wireless transmission path, and target vehicle.

**Table 2.** Summary of the security issues and solutions for CAN bus and ECUs.

| Components | Application | Security issues | Solutions |
|---|---|---|---|
| CAN bus | 1) CAN-C: high-speed bus that connects the engine, brakes, airbags etc.;<br>2) CAN-HIS: low speed bus that connects the comfort systems and climate controls. | 1) Eavesdropping and traffic analysis;<br>2) Jamming and DoS;<br>3) Malicious modification and injection. | 1) Strong authentication between different entities, including exterior devices;<br>2) Message encryption. |
| ECUs | 1) Powertrain; 2) Chassis;<br>3) Infotainment; 4) Body control. | 1) Monitor the real-time state of the corresponding component;<br>2) Control the components | 1) fuzzing, phishing, DoS， etc.<br>2) Overwriting firmware and flashing ECU |

Table 2 summarizes the security issues and solutions for CAN bus and ECU. As we mentioned, either CAN bus or ECU is well sealed from the outside in the past. Attackers must have physical access to the in-vehicle system to implement the attacks, which is not an easy task. However, increased connectivity exposes the vulnerabilities of these components to remote cyber-attacks and impose severe security threats on the in-vehicle system.

### 3. Security issues facing CV and solutions

CV adopts wireless communications to allow vehicles, roadside units, and mobile devices to communicate with each other and exchange critical information. In essence, CV is a kind of distributed system and imposes severe security and privacy challenges. It is anticipated that vehicle connectivity coupled with AV will revolutionize transportation systems, improve safety, and reduce costs, emissions and energy consumption. In fact, the adoption of diverse types of vehicle connectivity on AV enables the exposure of potential vulnerabilities of the vehicle and results in a heightened risk of cyber-attacks on the CAV.

CV incorporates multiple specific types of wireless communication to provide the information needed to implement vehicle-to-everything (V2X) applications, such as

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 September 2022 doi:10.20944/preprints202209.0230.v1

vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), vehicle-to-pedestrian (V2P), vehicle-to-sensor (V2S), etc. Figure 3 shows the various communications of CV in the future. Vehicular Ad Hoc Network (VANET) adopts Dedicated Short Range Communication (DSRC) to enable V2V and V2I. Cellular-network is gradually standardized by 3GPP to support Cellular-V2X (C-V2X) services [26]. Bluetooth can be considered in V2P due to its energy-saving properties. Wi-Fi also satisfy some types of V2X communications with the advantages of low cost and the ease of deployment. However, all these communications have their own vulnerabilities and face some security issues. Therefore, in this subsection, we investigate the security issues facing these communications of CV and identify some open issues for these communications if any of them will be well applied in CAV.

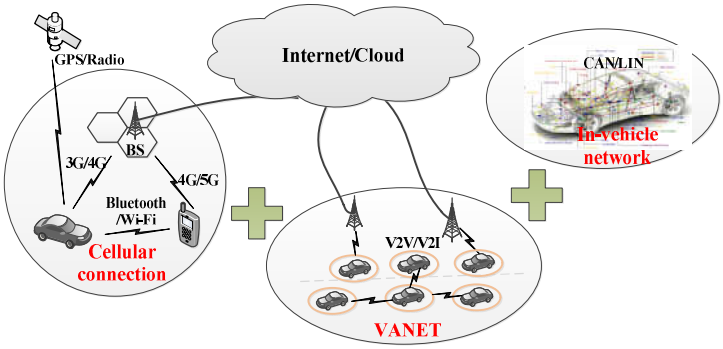


**Figure 3.** The wireless communications of CV.

*3.1. Bluetooth*

Bluetooth is a type of short-range communication (typically, tens of meters) and was proposed to be applicable for the communications of CV in some certain situations. For example, at a traffic intersection, Bluetooth can be used for connected vehicles' communication to avoid potential accidents [27]. Another scene is that Bluetooth may be applicable to V2P communication due to its low-energy-consumption. considering that pedestrian users in V2P usually have the limit on power saving of the device. However, Bluetooth is natively developed for short-range low-speed transmission, it would be challenging when it's applied in highly-mobile-vehicles' communication, which has the requirements of high transmission data.

In recent years, a few techniques have even been taken to enhance the security of Bluetooth communication, including frequency hopping, a pre-shared key for authentication and encryption [28]. Even so, some security risks cannot be avoided, yet, when Bluetooth is used in vehicles' connectivity. Table 1 lists the applications and potential security issues of Bluetooth. In nature, how to handle the native security risks caused by the frequent iteration, various versions of Bluetooth and pairing methods would be challenging. As a matter of fact, the reason why Bluetooth is so convenient to use in the first place is that it constantly broadcasts information such that nearby devices can be alerted to its presence. Thus, setting the Bluetooth device to "undiscoverable" mode would be a securer measure.

Bluetooth devices can form piconets, and multiple piconets through sharing the same devices can join to form a scatternet. If an entity is compromised, it's possibly going to infect other piconets or scatternet, which finally damage multiple entities in V2X connection. In addition, the MAC address of a Bluetooth device is usually unique and traceable, which may expose the vehicle to traceability attacks [6]. Even though Bluetooth PIN is used between the paired Bluetooth devices to implement authentication, it's vulnerable to brute-force decryption, interception and injection of a fake PIN [29]. What's worse, the compromised device can inject malicious messages into the paired vehicle and damage its functions. [30] shows how a user device connected to a vehicle through Bluetooth launch an attack on the vehicle. [31, 32] investigated how Bluetooth-enabled devices are extremely vulnerable within and beyond the vehicle domain.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 September 2022 doi:10.20944/preprints202209.0230.v1

### 3.2. Wi-Fi

As another type of short range communication, Wi-Fi satisfies some types of V2X communications with the advantages of low cost and the ease of deployment [33, 34]. In [35], Wi-Fi and WiMax provide viable solutions for V2V and V2I communications. Some researchers even suggested using Wi-Fi direct to facilitate the relaying of information from one vehicle to another [36, 37][38]. The built-in Wi-Fi module or Wi-Fi enabled mobile device in a vehicle allows the vehicle to approach the Internet when it's moving into the coverage of Wi-Fi hotspots, which is referred as the Drive-Through Internet. With the increasing deployment of the urban-scale WLAN (i.e., Google Wi-Fi in the city of Mountain View), the Drive-Through Internet would rapidly increase, which could provide a complementary solution to V2X with low cost. In actual design, some technologies are applied to enhance Wi-Fi capabilities to fit the high-speed and secure requirements of vehicular communications, like Multiple-Input Multiple-Output (MIMO). Recent advances in Passpoint/Hotspot 2.0 provide Wi-Fi with some secure connectivity [39], which makes Wi-Fi more competitive in V2X communications.

Even so, Wi-Fi is not originally designed for a high mobility environment; the stringent V2X service requirements impose some challenges on the reliability, robustness and security of Wi-Fi based V2X connectivity [40, 41]. Table 3 lists the applications and potential security issues of Wi-Fi. In terms of security, high vehicle mobility yields a very short connect time to the AP, while Wi-Fi communication usually takes a long establishing procedure. Time spent in Wi-Fi association, authentication, and IP configuration before actual data transmission cannot be negligible. For instance, if cryptography (i.e., Wi-Fi Protected Access, WPA) is applied in Wi-Fi communication, it will generate considerable delay up to 250ms, which is fatal to the safety-related application in VANET. In addition, Wi-Fi is typically set as the "discoverable" mode for users' search and connection as Bluetooth is, thus, it requires large bandwidth to guarantee the high transmission, which provides opportunities for attackers to launch such attacks as cracking, DoS, and karma attack [42]. Especially, with security-enhanced WAP2 being cracked recently [43], it must raise more attention and research efforts to enable Wi-Fi in connected vehicles' communication.

**Table 3.** Comparison of Bluetooth and Wi-Fi in connected vehicles.

| | Application | Attacks | Existing enhancement | Open issues |
|---|---|---|---|---|
| Bluetooth | V2P and specific scenarios with low density and low speed of vehicles (e.g., rural roads). | Pin interception; Injection of fake pin; Traceability attack; Infection attack. | Strong PIN authentication; frequency hopping; pre-shared key for authentication and encryption. | Security risks caused by frequent iterations of versions. Security risks caused by different pairing modes. |
| Wi-Fi | Built-in or brought-in. Scenarios: V2V, V2I, V2P, etc. | DoS, cracking, rekeying, karma attack, etc. | MIMO to improve transmission; Passpoint/Hotspot 2.0 provide Wi-Fi with security, WPA 2 | Long establishing time, including association, authentication, etc.; Unsecure mode (e.g., WPA 2 is cracked) |

### 3.3. Cellular Network

Cellular networks are considered a potential one that can guarantee the mobility and seamless connection in V2V and V2I. Existing solutions to connect vehicles together through widely deployed cellular infrastructure can be divided into: brought-in and built-in [41]. The brought-in connectivity refers to that users in a vehicle tether their own smart phone to the vehicle's infotainment system such that the vehicle gains immediate access to the Internet and some duplicate functions of a smartphone. Incidentally, built-in connectivity integrates cellular module into a vehicle's on-board infotainment system, and the Internet connection relies on a built-in module. C-V2X is a part of the overall 3GPP process to advance cellular systems from 4G to 5G technologies. Starting from Release 14 published by 3GPP, the LTE Direct and LTE broadcast laid the foundation for C-V2X,

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 September 2022 doi:10.20944/preprints202209.0230.v1

while after Release 16+, the 5G technology builds new capabilities for C-V2X networks and augments C-V2X direct communications overtime. [44, 45]. As Khanh, Quy Vu, et al. highlighted in [127], the power of 5G enables cellular and mobile communication networks to connect to hundreds of billions of devices with extreme-high throughput and extreme-low latency, including IoT, smart connected vehicles, smart cities, smart agriculture, smart retail, intelligent transportation systems. Built on many existing cellular infrastructures, C-V2X service covers large areas, and has a high penetration rate and low cost to potentially support the high-bandwidth demands and QoS-sensitive requirements of vehicular applications.

C-V2X defines multi-types of services, including V2V, V2P and V2I, and V2N, and two modes of transmission, including network-based communication and direct communication [46]. It's also designed for both in-coverage and out-of-coverage services. C-V2X direct communications can support active safety and enhance situational awareness by detecting and exchanging information using low-latency transmission in the 5.9-GHz ITS band for vehicle-to-vehicle (V2V) as well as V2I and V2P scenarios. In practice, C-V2X needs to address some technical challenges, such as high Doppler effect, resources scheduling, and synchronization [47].

Concerning security, C-V2X imposes some specific requirements on current cellular networks [48, 49]. Currently, the security key in cellular networks is priori-configured. Future direct communication between two vehicles should communicate without having to be provisioned with a shared key; D2D communications cannot rely on pre-shared pairwise keys. More importantly, pre-shared keys alone cannot provide a non-repudiation service. Therefore, the receiver needs a way to verify whether the received message was transmitted from a trusted entity. Secondly, no integrity protection on application layer messages is provided in current communication between user and network or D2D communication. Confidentiality for safety messages can be ignored, but strong integrity is paramount. Hence, none of the measures implemented in current cellular security are applicable. Thirdly, user privacy in C-V2X must be well considered. As cellular infrastructure and core networks are under different operators' domains, privacy from the network entities needs to arise attention. On one hand, the link between user and network is established based on its cellular subscriber identifier; on the other hand, the messages sent by vehicles devices usually contain application layer data, such as the exact geographical coordinates, the granularity of which is much finer than the cellular-site level device tracking presently. Therefore, it's possible that the operator can correlate the exact location with the vehicle's cellular subscriber identifier. Therefore, a solution that allows no network entity to be able to correlate the V2X messages with a vehicle is needed. Table 4 summarizes the C-V2X features and security issues.

**Table 4.** Features of LTE V2X communications and potential issues.

| | Services | Transmission mode | Advantages | Open issues |
|---|---|---|---|---|
| C-V2X | V2V, V2P, V2I, V2N | 1) Network-based communication,<br>2) Direct- communication | 1) Large Coverage and support for high mobility;<br>2) High Market penetration;<br>3) High capacity and bit rate. | 1) Direct secure communication without a priori configuration of keys by the network is needed;<br>2) Integrity protection on application layer messages;<br>3) Privacy protection of location. |

### *3.4. VANET*

VANET (Vehicular ad hoc network) is built on Wireless Access for Vehicle Environment (WAVE) and specifies 5.85~5.925 GHz frequency band dedicated for vehicle communication. VANET natively supports V2V and V2I communications in ad hoc mode, and enables efficient information exchange among vehicles, other end devices and public

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 September 2022 doi:10.20944/preprints202209.0230.v1

networks, and thus it plays a critical role in road safety and infotainment, self-driving systems, and intelligent transportation systems [128]. However, the drawbacks of VANET also include the prohibitive cost to construct new infrastructures, scalability issues, and the lack of deterministic quality of service guarantees, etc. Due to the high mobility of vehicles, there is a short communication time between a vehicle and the other entity. Therefore, VANET requires low communication delay and low tolerance for errors. Much work has been dedicated to the specific security vulnerabilities of VANET and possible solutions due to its importance to the improvement of traffic safety [50-52], which is shown in Figure 4. Thus, we will focus on issues remained.

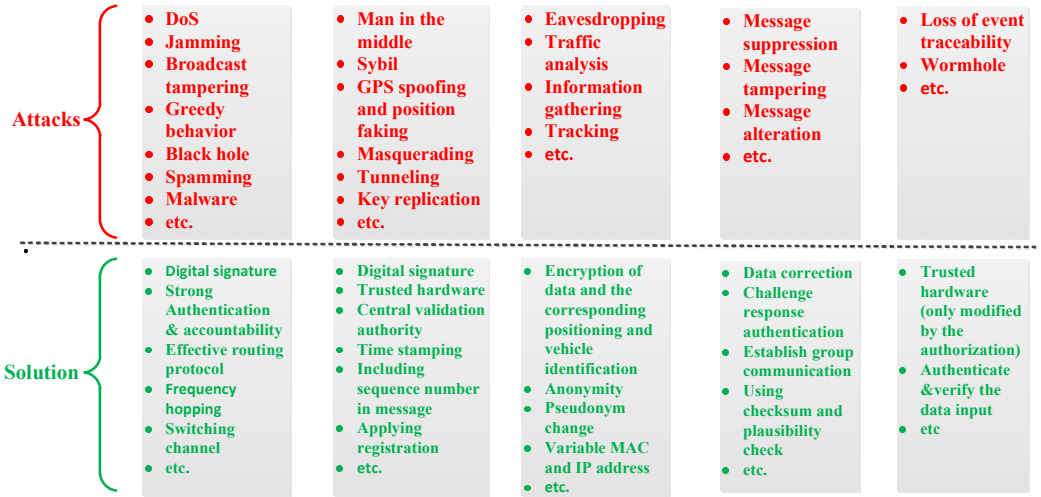


**Figure 4.** Attacks on VANET and the solutions.

3.4.1. Efficient authentication with privacy preservation and key management in group signature

Authentication is the primary step to ensure security in VANET, and much existing work proposed different techniques to provide authentication in VANET [53-56]. Usually, the symmetric key method is significantly faster than the digital signatures; however, the symmetric key method cannot provide non-repudiation [57]. Unsymmetrical key can provide authentication and non-repudiation, but it may cause computation complexity and communication overhead [58], as well as privacy exposure [59]. Therefore, efficient unsymmetrical authentication with privacy preservation is needed. In recent years, group signature has been applied in VAENT to protect a vehicle's anonymity besides authentication [60, 61]. The main limitation of this approach is the computation complexity and communication overhead to distribute group keys [61, 62]. In addition, a manager is needed to distribute the key to a new member when it joins the group or revoke the key when the member leaves. Invalid and malicious signers should be identified in time, while forward privacy should be protected at the same time [63, 64]. Therefore, how to manage the key in a group signature is still challenging.

3.4.2. Privacy protection and effective pseudonym change strategy

Privacy protection (e.g., vehicle's location and trajectory) has been a top challenge in VANET [65]. Many approaches have been proposed to implement effective strategies of pseudonym changing [66-70]. However, the simple changing of a pseudonym is not sufficient to defend against pseudonym linking attacks, especially semantic linking, which can predict the next position of a vehicle and link the vehicle's new pseudonym and the original one [71]. Currently, encryption or radio silence is suggested to defend against the semantic linking attack. However, encryption is ineffective against internal passive adversaries [66], and radio silence may negatively affect safety-related applications in VANET [72]. Therefore, highly effective and reliable pseudonym change strategy is still

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 September 2022 doi:10.20944/preprints202209.0230.v1

needed to protect vehicle's privacy from semantic linking attack. In addition, a unified framework and metric is needed to quantify the privacy protection level, which will contribute to evaluating new privacy protection mechanisms [73-75].

3.4.3. Trust management and enhancement

Trust usually works as a complementary defense to cryptography in some specific situations. Specifically, trust mainly deals with inside attackers (e.g., passive attacks) and has little negative impact on message treatment and transmission delays, and thus, can be applied in both delay-sensitive and delay-tolerant traffic [76, 77]. Even so, some issues should be considered when applying trust management in VANET security. Most exiting models assume the adversary has stable and continuous behavior. However, smart attacks (e.g., an insider user becomes malicious) may get aware of the trust rule and can alternate between legal and illegal behaviors. Therefore, new trust models should adaptively detect such kinds of 'unstable' dishonest behaviors or entities. On the other hand, how to handle the location and identities privacy while ensure efficient and reliable messages dissemination is still one of the open issues in existing models [76].

3.4.4. RSU assisted security and RSU power abuse

Within the communication range of a RSU, multiple vehicles nodes may communicate with its neighbors via V2V or via V2I through RSU. As a result, the nodes will contend for the radio resources of the single RSU. When traffic density and message dissemination increase, the RSU may become saturated. Therefore, it's critical to make the communication near the RSU both secure and scalable. In practice, a challenging scheduling problem arises when RSU serves as a centralized scheduler for all the nodes within its coverage. On the other hand, RSU will possess great power to allocate resources to different nodes. It registers much private and secure information of each node within its range. Therefore, valid measures should be taken to block the power abuse of RSU, to prevent RSU from unfairly allocating resources to a certain node, and to maliciously invade or disclose the privacy of a node within its range.

Either C-V2X or VANET represents a promising solution to support V2X communication. At the moment, VANET has the advantage. The 5.9 GHz band made available in U.S. more than a decade ago remains reserved for it, the EU also intended to make 802.11p the basis of the radio standard for safety-related messages between vehicles within ITS-G5. However, Qualcomm, which supports DSRC and offers second-generation 802.11p DSRC chips in the past, introduced its first C-V2X commercial solution in 2017; China appears ready to mandate C-V2X for C-ITS and safety-related services. No matter which one will become the standard to support V2X finally, the security issues in both types of networks should be well considered before they are widely developed to support CAV application.

Table 5 summarizes the features and security issues of C-V2X and VANET. As analyzed above, they possess different features and face different security issues accordingly. For example, as C-V2X potentially support direct V2V communication, the direct secure communication without a priori configuration of keys network is needed to benefit the network's security and efficiency. On the contrary, VANET natively supports V2V and V2I, but requires efficient authentication with privacy preservation and key management in group signature to achieve multi-vehicles' secure and efficient communications. Meanwhile, due to the risk of C-V2X being exposed to operators, the privacy protection (e.g., vehicle's location) and defense against operator power abuse will be indispensable. Accordingly, as VANET deep involves RSU or other infrastructures in its deployments, the security and power abuse of RSU or infrastructures need to be well considered. Besides, since vehicular connectivity significantly increases, VANET produces ever-increasing amount of data, it will impose significant challenges on the efficient, reliable and secure data transmissions and processing in VANET and calls for further attentions [128].

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 September 2022 doi:10.20944/preprints202209.0230.v1

**Table 5.** Comparisons of features and security issues between C-V2X and VANET.

| Feature | C-V2X | VANET |
|---|---|---|
| Capacity | High | Medium |
| Mobility | Very high (support speed up to 350 km/h) | Medium |
| Coverage | Ubiquitous | Medium |
| Delay | Goal is 100ms (C-plane) and 10ms round-trip and 5ms (U-plane) | Goal is 100ms (safety-critical application) and 500ms (non-safety-critical application) |
| V2I support | Native, due to the centralized architecture with enhancements | Yes, only intermittent and short-lived connectivity |
| V2V support | Potential, through D2D extension | Native, through extensions in MAC protocols |
| Network infrastructure | Adopting existing cellular infrastructure for V2I communications | Requiring high investment on network backbone devices |
| Security issues | 1) Direct secure communication without a priori configuration of keys by the network is needed;<br>2) Integrity protection on application layer messages;<br>3) Privacy protection of location, and operator power abuse. | 1) Efficient authentication with privacy preservation and key management in group signature;<br>2) Privacy protection and effective pseudonym change strategy;<br>3) Trust management and enhancement;<br>4) RSU assisted security and RSU power abuse |

## 4. Security issues and solutions for CAV

With the convergence of AV and CV technologies, the future CAV is essentially the most complex large-scale cyber physical system composing of advanced sensing, computing, communication and control systems. The security vulnerabilities and implications of both AV and CV technologies and their combination impose significant challenges in such a safety-critical system. Although the general security issues facing AV and CV have been relatively well studied in the previous two sections, there is still an absence of systematic analysis to indicate the impact of cyber-attacks on the physical performance and operations of CAV. In the subsection, we will focus on how cyber-attacks exploit the vulnerabilities of vehicles and impact the performance of CAV.

Cyber-attacks on CAV can be analyzed from two angles: the intra-vehicle and the inter-vehicle. Typically, intra-vehicle system focuses on individual vehicle and combines the in-vehicle networks with other components (e.g., actuators) into a tight system to improve the kinetic performance of the single vehicle, while the inter-vehicle involving multiple vehicles and the traffic flow are designed to optimize traffic dynamics and inter-vehicle networking performances based on their tight interaction with each other. For intra-vehicle system, increased connectivity exposes the inherent vulnerabilities of the system. Therefore, cyber-attacks can exploit the vulnerability to impact the operation of the vehicle. For example, cyber-attacks can inject malicious messages into in-vehicle network remotely to directly manipulate certain functions of the vehicle, such as braking, steering, which may directly threaten the vehicle's safety. For inter-vehicle system, the control

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 September 2022 doi:10.20944/preprints202209.0230.v1

performance and dynamics of the system highly depends on the communication performance. Cyber-attacks can impact cooperative vehicle dynamics and traffic flow by jamming or spoofing the inter-vehicle communication. Therefore, we will analyze these two types of cyber-attacks and their impact on the performance of CAV as well as identify some open issues in current research.

### *4.1. Cyber-attacks on intra-vehicle system*

#### 4.1.1. Models of the attacks

Cyber-attacks indicate that the attacks on the vehicle are launched through physical/wireless connection to vehicle. There exist some entry ports on vehicle to the intra-vehicle system to enable a wide range of services, including support for self-diagnostics, media play, etc. In early stage, attacks must have physical connectivity to the vehicle, such as using a USB stick or an OBD-II scanner [2, 6, 20], which limits the implementation of the attacks.

CV enables diverse types of wireless connectivity on intra-vehicle systems; thus, cyber-attacks can be implemented remotely. In [2], two vehicles are connected through the wireless communication of two laptops. In the victim vehicle, the laptop running CARSHARK is connected to the vehicle's CAN bus through an OBD-II port; in the attack vehicle, another laptop transmits commands to the victim vehicle to manipulate its body control module, engine control module, etc. Most modern vehicle provide Bluetooth ports or Wi-Fi hotspots to outside devices. Cyber attackers can directly pair with the vehicle or crack a device which has joined the Wi-Fi hotspot. Typically, the range of such cyber-attacks is quite short, approximately ten of meters. Due to the large covering areas and high penetration rate cellular networks, some researchers exploited the cellular networks to perform remote cyber-attacks. In [3], the researchers provided a "super-remote" connection (between Pittsburgh and St. Louis) to compromise an unaltered vehicle through a cellular network. Currently, vehicles are gradually installed with VANET communication modules, which allows vehicles to communicate with other vehicles or infrastructure even without a base station. This would provide much convenience for attackers to launch cyber-attacks on inter-vehicle systems in the future.

Figure 5 presents the general model of cyber-attacks on intra-vehicle systems. Essentially, cyber-attack on intra-vehicle systems involves manipulating messages on intra-vehicle networks, especially the CAN bus, to control the physical functions of the vehicle remotely. Therefore, the attacker needs to identify the address of the vehicle first and has access to a communication module on the system via physical/wireless connectivity. Then the attacker needs to compromise the communication module, typically by modifying the files on the module. For certain types of vehicles, the compromised communication module is connected to the CAN bus, which allows an attacker to manipulate a CAN message to affect the control functions of the vehicle. For some types of vehicles, the communication module doesn't connect to the CAN bus, which will take more efforts of the attacker to compromise another module which has the ability to send messages to the CAN bus. After all these things are achieved, attackers can launch a real cyber-attack on the intra-vehicle system. [23] investigated the remote attack surfaces, internal network structure and computer-controlled features of several popular vehicles' patterns on the market of U.S.

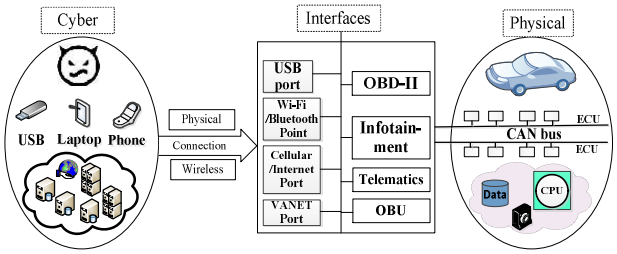


**Figure 5.** Model of cyber-attacks on intra-vehicle system.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 September 2022 doi:10.20944/preprints202209.0230.v1

4.1.2. Attack impacts on intra-vehicle system

It's typically the first step that cyber-attacks that remotely compromised a module of a vehicle. To successfully manipulate specific operation functions of the vehicle, attackers need to further figure out the proprietary nature of different messages on the network, which usually involves the reverse engineering of ECU firmware. This is also why attacks on intra-vehicle system can cause considerable damage to the vehicle. They directly tampered the control message on the system and manipulated the control modules (ECUs) of the system, which would quickly kill some functions of the vehicle. In [3, 20], researchers provided the packet analysis results and their effects on different control modules of the vehicle, which are partially presented in Table 6.

**Table 6.** Different packet of in-vehicle network and their effects on control module [20]

| Control Message Code | Controlled Function | Impacted Control Module |
|---|---|---|
| 07 AE ... 1F 87 | Continuously activates lock replay | Body control module |
| 07 AE ... CE 32 | Temporary RPM Increase | Engine Control Module |
| 07 AE ... 25 2B | Engages Front Left Brake | Electronic Brake Control |
| 00 00 ... 00 00 | Falsify Speedometer Reading | Other modules |

After attackers know well the nature of different communication packets on intra-vehicle system and their effects on the corresponding control modules, they can implement diverse types of attacks on the intra-vehicle system remotely. Specific attacks include a) Denial of Service (DoS) [78] and Fuzzing attack [79]; b) Code modification and injections [2]; c) Replay attack [6, 16]; d) Malware injection. Even though these types of attacks may be presented in the previous section, this section focuses on the direct impact of the attacks on intra-vehicle system. In addition, a type of smart attack, malware is considered considerably threatening in the future [80], because it can modify itself to look different each time it replicates, such as polymorphic and metamorphic malware. Many existing defense approaches become fragile and unresisting to polymorphic and metamorphic malware [80-82]. To effectively defend against smart malware, some intelligent analysis and detection methods are needed [54]. Table 7 summarizes the different interfaces and types of attacks on the intra-vehicle system.

**Table 7.** Cyber-attacks on intra-vehicle system and the defenses

| Type | Description | Attacks/ Consequences | Defenses |
|---|---|---|---|
| DoS | Introduce topmost priority nonsense message frequently to system. | 1) Cause flooding;<br>2) Hinder regular services;<br>3) Detect existing security loopholes of system. | 1) Identify security loopholes earlier;<br>2) Verify the fix/ update files;<br>3) Combination of authentication and integrity verification. |
| Fuzzing attack | Massive amounts of random data can be inputted to the system. | 1) Crash the system;<br>2) Exploit vulnerabilities for further attacks. | |
| Code modification and injections | Carry out malicious modifications of code; inject malicious messages to bus system. | 1) Override certain functions;<br>2) Compromise the system. | 1) Authorize connected devices;<br>2) Intrusion detection. |
| Replay attack | Retransmit eavesdropped packer to system. | 1) Activate/ Disactivate certain functions maliciously | 1) Encryption on messages;<br>2) Ensure the freshness and; validness of input data. |
| Malware injection | Malware codes can modify themselves to look different each time they replicate and deceive the system to download them into system. | 1) Execute damages;<br>2) Approach privacy information;<br>3) Eavesdrop communication. | 1) Intrusion Detection;<br>2) Network Separation;<br>3) Message Obfuscation;<br>4) Cloud-based defense. |

 doi:10.20944/preprints202209.0230.v1

4.1.3. Open issues of intra-vehicle system security

In practice, there are many limits to successfully launch a cyber-attack on CAV. For example, when the attacker tried to compromise the communication module, the attack needs to bypass the verification or integrity check of the system, which may activate the alarm. Besides, some patterns of vehicles don't allow outside devices to send a message to the bus system when the vehicle is moving. Even so, security must be built into the system before the manufacturing of a vehicle and the wide deployment of CAV.

On one hand, to maintain the various connectivity to vehicle systems without exposing vulnerabilities of the system, effective access control must be implemented on the system to guarantee secure information input. The system must grant selective access to its components. For example, when a vehicle is moving, the module which can send messages to the CAN bus should forbid any reboot. Furthermore, the system must ensure that only authorized devices can gain limited access to certain types of its components. Each time a new connectivity is created between the system and an outside device, integrity and verification must be implemented [20]. The principle of least privilege should be applied while providing access to the connected device. In addition, in terms of software design of the system, buffer overflow, string format vulnerabilities should be avoided to prevent connected devices from modifying the system when the situations occur.

On the other hand, network monitoring and intrusion detection should be implemented on intra-vehicle systems. Typically, attacks on the system last for several minutes or more, therefore, it's essential to monitor the network and to detect possible attacks as soon as possible. For the purpose, real-time intrusion detection and response on the system could be adopted on the system. Currently, most intrusion detection for the system is either based on misuse or based on anomaly detection. Compared the misuse detection, anomaly detection can not only identify specific attacks, but to identify some unknown attacks by discovering abnormal frames transmitted on the traffic [83]. To develop intrusion detection for intra-vehicle systems, some issues should be considered. Firstly, the detector should be appropriately deployed in the system. Usually, the detector could be host-based or network-based. Secondly, the detecting methodologies should be carefully considered. The abnormal detection may capture the abnormal patterns according to predefined ones [84], or analyze the unusual frequency or time interval [85]. In the last, the accuracy of detection matters a lot. Compared with existing methods, machine learning-based detection can well extract the features of intrusion and decrease the error rate [86]. However, due to the limited computing power, memory and communication capacities of current vehicles, it's impractical to implement sophisticated machine learning detection on individual vehicles. CAV essentially is a large scale distributed system composed of safety-critical individual vehicles that demand reliable real-time operations. Therefore, besides performing core intrusion detection primarily on each intra-vehicle system in distributed manner, cooperative neighboring vehicles within same cluster (e.g., a physical platoon) or cloud platform can provide further verification of the local detection results within the time constraint imposed by different applications.

*4.2. Cyber-attacks on inter-vehicle system*

CAV typically cooperate with each other to form a certain type of driving patterns with some common interests in the traffic, which can significantly improve road capacity and traffic efficiency. The cooperative driving pattern effectively integrates computing, communication and control technologies to achieve the stability, reliability, and efficiency of the inter-vehicle system. A representative pattern is a platoon, which is shown in Figure 6. Multiple vehicles form a string in one lane; a vehicle follows the preceding vehicle with a small and nearly constant distance. In the early stage, the platoon relies on Adaptive Cruise Control (ACC) function, which mainly utilizes local sensors measurements to maintain the string pattern. Currently, platoon is mainly achieved by Cooperative Adaptive Cruise Control (CACC) functions, which enables each vehicle in the platoon to directly obtain state information of leading vehicle through wireless communication to

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 September 2022 doi:10.20944/preprints202209.0230.v1

maintain shorter spaces and stronger string stability of the platoon [87, 88]. Due to the reliance on vehicular communication, the performance of communication, like delay, packet delivery loss, has a considerable impact on platoon vehicles' dynamics [89]. Therefore, attackers can utilize reliance to impact the performance of a platoon. Typically, cyber-attacks can degrade the string stability and control performance of a platoon by influencing vehicular communication in the platoon. As a result, cyber-attacks can directly damage the mobility pattern and cause unsafe operation of inter-vehicle systems [90]. In this subsection, we use a platoon to illustrate how cyber-attacks impact the performance of inter-vehicle systems by compromising vehicle connectivity.

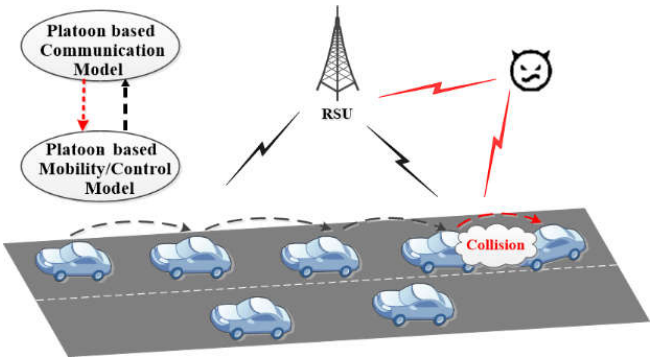


**Figure 6.** Cyber-attack on cooperative platoon [89].

4.2.1. Models of attacks on platoon

Due to the dependence of platoon dynamics and control on inter-vehicle communications, the imperfections of communications, such as transmission delay, packet loss, channel interference, etc., will directly impact the performance of platoon mobility and vehicles dynamics. Firstly, we quantitatively analyze how the networking performances impact platoon dynamics and control.

Xu et al. used a three-cars-platoon model to illustrate the platoon safety performance under different information content (e.g., distances, speeds and drivers action) and different communication uncertainties (e.g., delay, Doppler effects) [91]. They pointed out that the data rates and PDR, transmission distances with/without obstacles and multi-hops all significantly impact the communication delay, and finally affect the safety distance between vehicles and platoon performance. Compared with the inter-vehicles distances of platoon only relying on ACC functions, the transmitted distance or speed information through vehicular communications can effectively shorten the inter-vehicle distance.

Essentially, string stability stands for the platoon dynamics from the perspective of vehicles control, which is defined as the spacing error between the desired and actual inter-vehicle spacing not amplifying to the upstream of the platoon [92]. It is analyzed in the frequency domain, and the specific steady state error transfer function is defined as

$$H_i(s) = \left| \frac{E_i(s)}{E_{i-1}(s)} \right| \quad (1)$$

$E_i(s) = \mathcal{L}(e_i)$, $E_{i-1}(s) = \mathcal{L}(e_{i-1})$, is the Laplace transformation of the spacing error. Theoretically, platoon stability is guaranteed if the following condition is satisfied:

$$||H_i(s)||_\infty \leq 1 \quad (2)$$

Oncu et al. designed a CACC system from the perspective of Networked Control System (NCS) and considered the effect of communication sampling, hold and delays [93]. They analyzed the string stability of the platoon, which follows a constant time headway spacing policy based on these imperfections in vehicular communication. A feed-back/ feed-forward controller is included in the CACC model: the feedback controller $C_{i,ACC}$ (s)

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 September 2022 doi:10.20944/preprints202209.0230.v1

constitutes the ACC part and is a PD-type controller that acts on locally-sensed data, while the vehicular communication is introduced as an addition to ACC part to constitute the CACC operation. Given the spacing policy, a time-domain representation of the CACC feed-back/feedforward control input is expressed as,

$$u_i = u_{fb,i} + u_{ff,i} = K_{i,i-1}x_{i-1} + K_{i,i}x_i,\ 1 \le i \le n \tag{3}$$

They considered each vehicle in the platoon to be an individual closed-loop CACC model. For an individual closed-loop CACC model, the i-th CACC-equipped vehicle dynamics ($2 \le i \le n$) in a n-vehicle string is described by,

$$\dot{x}_i = A_{i,i}x_i + A_{i,i-1}x_{i-1} + B_{s,i}\check{u}_i + B_{c,i}\hat{u}_{i-1}, \tag{4}$$

$x_i^T = [e_i, v_i, a_i, u_{ff,i}]$ represents the state variables, $\check{u}_i(t) = u_i(t - \tau_{a,i})$ accounts for the delays in throttle actuation; $\hat{u}_{i-1}$ denotes that $u_{i-1}$ is transmitted over the network, which includes network-induced effects (e.g., sampling, hold, and delays). Furthermore, they lumped the n models in the platoon to derive a complete discrete-time CACC NCS model for the string stability analysis,

$$\xi_{k+1} = \bar{A}_\xi(\tau, h)\xi_k + \Gamma_r(h)u_{r,k} \tag{5}$$

Their experiment results show that how string stability is compromised by delays and other imperfections in wireless communications.

Clearly, CACC-based platoon stability highly depends on communication performance. Therefore, cyber-attacks mainly utilize the dependence to impact platoon dynamics and safe operations by degrading the networking performances. Fanid et al. analyzed the stability and safety of platoon according to a model including Rician fading channels and jamming attacks [94]. When the attacker launches the jamming signal over the platoon, with the assumption of Rician fading, the probability density function of the instantaneous signal-to-interference-plus-noise ratio (SINR) of the received signal of the i-th vehicle at time k, $\gamma_i^k$, is derived by,

$$f_i^k(\gamma_i^k) = \frac{1+K}{\overline{\gamma_i^k}} \exp\left(-K - \frac{(1+K)\gamma_i^k}{\overline{\gamma_i^k}}\right) * I_0\left(2\sqrt{\frac{K(K+1)}{\overline{\gamma_i^k}}}\right) \tag{6}$$

The state space representation of the platoon under Rician fading channel and jamming attacks is derived as,

$$x_n[k+1] = \bar{\bar{A}}_n x_n[k] + \bar{\bar{B}}_c \bar{u}_{n-1}[k] + \bar{\bar{B}}_s \mu_l[k] \tag{7}$$

Considering various scenarios with different settings, including various attacker's location and vehicles signal transmission power, they proved that platoon stability and safety are highly sensitive to jamming attacks. They also derived the best location and best time to launch the jamming attacks to destabilize the platoon. In addition, they computed the minimum transmission power to maintain string stability and advised that the minimum transmission power needs to increase with the increase of jamming signal power.

Currently, much work has been done investigating the string stability under imperfect communication performances [90, 95-97]. There is little work to consider how cyber-attacks utilize the imperfections of communications to impact the performance of the platoon. The most common one is jamming, which has severe damage to the safety of the platoon and is hard to prevent. Besides string stability, platoon management involving platoon formation, merging and splitting is another fundamental issue. It's still challenging to form the stable cluster or platoon, especially in heterogeneous and drastic changing scenarios. In this process, traffic dynamics, communication behavior and security are supposed to be considered. In addition, platoon typically consists of master and multiple following vehicles and operates within one lane, while another cooperative pattern, convoy, which has no master vehicle and operates on multi-lanes, considerably relies on vehicles to self-organize a more complex cooperative pattern. It would be challenging to model such a pattern under a communication.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 September 2022 doi:10.20944/preprints202209.0230.v1

4.2.2. Diverse types of cyber-attacks

Various types of cyber-attacks may have been discussed in previous sections. Here, we systematically summarize these types of cyber-attacks and mainly consider their impact on the platoon. Miao et al. analyzed the different attacks on a platoon, including replay attack, jamming attack, DoS attack, and provides a SDN solution to mitigate these types of attacks [95]. Amir et al. performed the string stability analysis of CACC under jamming attacks [96]. Petrillo et al. provided a collaborative control strategy for platoons to defend against falsification attacks [97]. Table 8 summarizes the cyber-attacks on platoon and workable solutions.

**Table 8.** Summary of common cyber physical attacks on cooperative vehicles

| | |
|---|---|
| Message tampering | 1) data correction; 2) challenge response authentication. |
| Forgery attacks | 1) Use vehicular PKI for authentication;<br>2) Sign warning message;<br>3) Establish group communication;<br>4) Use non-cryptography checksum and plausibility check per message. |
| Message saturation | 1) Limit message traffic;<br>2) Build location-based grouping and aggregation signature. |
| Replay attack | 1) Use time stamping technique;<br>2) Include sequence number in message;<br>3) MAC via ARAN routing protocol. |
| Node Impersonation | 1) Use variable MAC and IP addresses;<br>2) Authentication via digital certificates;<br>3) Use cryptographic certificates via ARAN routing protocol. |
| Routing attack (i.e., Black hole, Grey hole, Worm hole and Tunneling) | 1) Digital signature of software and sensors;<br>2) Cryptographic certificate, symmetric cryptography, MAC and one-way hash in routing protocol;<br>3) enhance the trust among different nodes. |
| Spoofing & jamming attack | 1) Switch the transmission channel;<br>2) Use the frequency hopping technique;<br>3) Switch between different wireless technologies. |

4.2.3. Open issues of inter-vehicle system security

Although the diverse types of cyber-attacks on platoon and the corresponding solutions have been well studied, there still exist some open issues to be considered.

Presently, the platooning probability on the road is low. Most existing work either assume individual driving pattern or consider cooperative driving (e.g., platoon) only in the design of inter-vehicle message dissemination. Furthermore, in most cases, several vehicles can communicate through V2V to form/maintain a platoon without much involvement of infrastructure, such as RSU. The capabilities of the infrastructure have not been fully exploited, yet. However, a report form USDOT indicated that platooning probability on highway could be higher than 70% in the future [98]. In this case, the cooperative driving frequently exchanges periodic safety beacons to maintain the pattern, while individual driving may broadcast event-driven messages. The heterogenous driving patterns would impose great burden on vehicle communication and stringent requirements on transmission scheduling. Given that cyber-attacks on inter-vehicle system mainly decease the communication availability or reliability, how to effectively allocate the communication resources and improve the communication reliability for the heterogeneous driving

 doi:10.20944/preprints202209.0230.v1

patterns would be a key problem. Currently, some work has studied the strategy of allocating resources, avoiding collision, and ensuring communication availability and reliability under the assistance of infrastructure (e.g., RSU, cloud). For example, [99] utilized the capability of infrastructures to combine TDMA and CSMA/CA scheduling to guarantee the timely and reliable message delivery for the heterogeneous driving patterns. In [100], cloud was introduced to assist safety massage dissemination in VANET-Cellular heterogeneous networks. In fact, infrastructure would play a critical role in channel allocation, caching, content download, data aggregation/dissemination, hand-off, location, routing and security of vehicular communication in the future [101, 119]. If the infrastructure was compromised by cyber-attacks, it would cause large-scale damage. Meanwhile, the infrastructure may adopt different architectures besides incorporating existing devices, such as the cooperative architecture, virtual architecture, etc. which leaves it vulnerable to many cyber-attacks, too. Therefore, defending infrastructure against cyber-attacks will be a great challenge.

Cyber-attacks on inter-vehicle systems can be from either the outside or inside of the platoon. In most cases, the cyber-attacker is outside the platoon. In [94], the jammer was mounted on a drone flying over the platoon. Theoretically, it is not very difficult to recognize attacks from the outside. Some state-of-the art measures can effectively detect and limit the capabilities of outside attacker, but it's still challenging to effectively defend against inside attackers. In addition, due to the coupling of physical and cyber aspects of the inter-vehicle system, the co-attacks of a malicious vehicle inside the platoon which takes disturbing accelerations and an attacker outside the platoon would be greatly threatening. It's considerably challenging to identify the attacks sources, to cut off the cooperation of two attackers, and to eliminate the insider vehicle as well as re-stabilize the platoon. Some researchers proposed maintaining a lower and upper bound of inter-vehicle spacing to possibly mitigate the impact of cyber-attacks [94], which is a trade-off between traffic efficiency and safety. However, given that the message within a platoon contains control parameters, if an insider attacker directly tampers the message content when the message is transmitted from head to the end, it would directly cause collisions without noticeably degrading the communicate quality. Therefore, security mechanisms are urgently needed to detect and defend against insider attacks and co-attacks.

## 5. Discussion and Future Works

As for future work, we believe that our study highlights some directions in this area. On one hand, for fully-autonomous vehicles, the reliable and secure perception, functioning and operation are the top requirement and concern on the CAV system. On the other hand, with the evolvement of vehicular connectivity and the occurrence of IoV (Internet of Vehicles), cloud can be integrated in vehicle connectivity and fully exploited to defend against cyber-attacks under the CAV environment.

### *5.1. Secure the perception and operation of CAV*

Fully-autonomous vehicle operates without driver's assistance or monitoring. Accurately perceiving the surroundings and understanding the context, such as the road conditions [115], the weather status, would be the prerequisite for the safe driving of CAV. The accurate perception lies in the robust sensing of its surrounding environments and the reliable fusion of information. For CAV, the sensing ability is possibly impacted by malicious attacks via spoofing/deception attacks (e.g., faked GPS signals) to generate fraud or unreliable data. Also, attackers can delay the acquisition and transmission of the data vis DoS attacks to disable the delay-sensitive applications, and thus, threaten the vehicle safety. Recently, due to the development of artificial intelligence (AI) technology, the perceiving capabilities of sensors can be enhanced to improve detection rate and decrease error rate [102, 103]. A typical example is that the detection accuracy of cameras can be improved using neural network tools and methods [104, 105, 106]. Therefore, the

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 September 2022 doi:10.20944/preprints202209.0230.v1

advancement in AI technology, to an extent, can make the sensors more robust to malicious attacks.

On the other hand, coupling different sensors and fusing multi-sources data would be indispensable for a CAV to accurately perceive the surrounding environment [106]. For instance, stereo vision uses an overlapping region of two cameras to determine depth; Google Driverless Car fuses LiDAR with stereo-vision and Enhanced Maps (E-maps) for road scenery understanding. Besides multiple sensors, with the introduction of vehicles connectivity, vehicles communication provides another information source for data fusion. In [107], data from long-range radar and the VANET network are associated and fused to provide accurate data of tracked objectives in front of the vehicle. Traditionally, Kalman filter and particle filter can be used for data fusing of multiple sources [108, 109]. Presently, some machine learning methods are also applied in data fusion processes, like SVM classification, unsupervised clustering, etc. However, these methods are usually time-/resources-consuming. Meanwhile, received data from multiple sources are within different coordinate system, and use unsynchronized clock. Spatial and temporal alignment of incoming data is needed before data is further fused [29, 106]. Therefore, "lightweight" and efficient fusion algorithm is still needed. In addition, multi-modality fusion needs to deal with some issues in practice when they are implemented. For example, information from the GPS was not available when the vehicle was under tunnels or bridges; information from one sensor source is possibly blocked by malicious attackers. Therefore, reliable fusion is needed to handle these situations.

Furthermore, attack-aware and error-tolerant end-to-end learning can be developed for fully-autonomous operations.

Currently, autonomous vehicles mainly utilize module-based learning to achieve some functions, such as object detection and pattern recognition. Recent efforts have been dedicated to applying end-to-end learning in autonomous driving. Typically, the operation mode of autonomous driving goes through three steps: perception, understanding and planning [110-112]; one level up, end-to-end learning can be used to innovatively update the operation mode, which shorten the process as perception and action [113-115]. It indicates that the new driving mode takes the raw data as input, like the image, and outputs control commands directly. In [116], Karol trained a convolutional neural network to map raw pixels from a single front-facing camera directly to steering commands. Undoubtedly, the application of end-to-end learning in autonomous vehicles shows great advantages in enhancing vehicular operations and reducing the perception-control period. However, neural networks are proven to easily fooled or perturbed by interferences [123]. The end-to-end learning built on neural network would be susceptible to the complex environment. For example, the adversarial image may be captured by the network as regular input; the noise and uncertainty of the input data cannot be effectively filtered, and thus, distract the output command. Therefore, reliable end-to-end learning is needed for future fully-autonomous operations.

### *5.2. CAV integrated with cloud*

Recently, much work has considered integrating cloud with CAV systems [117-118]. On one hand, cloud provides resourceful information to CAV; on the other hand, the cloud can provide powerful resources to support large storage and fast computation, which is indispensable to implement some sophisticated AI algorithms. Therefore, the cloud shows great advantages to secure CAV. In essence, CAV integrated with cloud is a large-scale hybrid platform composed of remote centralized infrastructure cloud and distributed nodes with fog/edge computing. The architecture of the platform is shown in Figure 7. Locally, each vehicle and RSU/BS are enhanced with extra computing units and storage to process some data/ information to meet the requirement of time-sensitive applications. Meanwhile, multiple types of commercial clouds, like Microsoft Azure, AWS, are readily available to cooperate with the possible automaker clouds and traffic center

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 September 2022 doi:10.20944/preprints202209.0230.v1

clouds in the future, to support some advanced functions with heavily-computing overload.

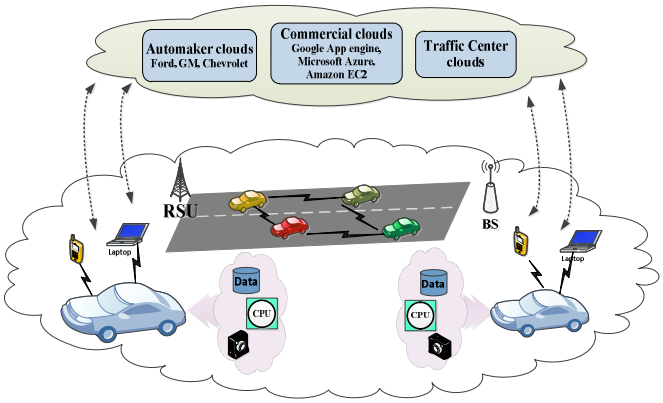


**Figure 7.** Architecture of CAV integrated with cloud.

Typically, data collected from local sensors have a direct impact on the vehicle's safety by providing obstacle detection and navigation operation. With the assistance of the cloud, these data can be processed and explored remotely to provide complementary measures to enhance vehicles security and safe operations. In the future, enormous volumes of diverse types of messages will be transmitted through vehicular communication channels. Due to the limited capacities of the communication channels, all messages will compete for the temporal and spatial resources, which can be easily utilized by malicious attackers to launch resources-availability attacks. Meanwhile, it is inevitable that many messages are collected by vehicles from the same region, which indicates that there exist great duplicate and redundancy in the messages. With clouds involvement, these messages can be merged and pruned through data relevance analysis before they are re-transmitted to a region or a certain number of vehicles. By transmitting compact but useful messages the communication channels utility can be improved. Cyber-attacks, such as DoS/spoofing, may be prevented.

Furthermore, the cloud can collect information from multiple vehicles in a region to generate reports about traffic flow, traffic density and traffic speed of that region. This way, the cloud can provide vehicles with reference and surveillance for safe driving. For example, being aware of the average traffic speed provided by cloud reports, autonomous vehicles can recognize the obviously-abnormal behaviors of some vehicles in time to avoid malicious operations or potential dangers. Another good example is that, in bad weather (e.g., heavy rain or storm), the perception of local sensors is easily susceptible, even completely disabled. In this case, the transmitted messages can provide navigation and guidance to the vehicle for safe movement. However, there are some issues which should be well considered when the cloud is deployed in practice. Typically, the preliminary aggregation and fusion of the raw data can be achieved within local fog/vehicular nodes, which is applicable to the low-delay applications, like emergency navigation and obstacle recognition. Considering high-level fusion, either feature fusion or decision fusion, it typically has a loss of information and needs co-relation through complicated algorithms (e.g., support vector machine or kernel-based clustering), which are time-/resources-consuming. Therefore, it can be achieved on the remote cloud to meet the requirements of delay-tolerant applications. It is still an open issue how to assign the assignments to local fog/edge computing and remote cloud computing.

On the other hand, as we mentioned in cyber-attacks on intra-vehicle systems, malware would be a type of smart attack, which will be greatly threatening to CAV in the future. A good example is polymorphic and metamorphic malware, which changes itself each time it replicates. It has been proven that individual vehicles are fragile when they face such powerful attacks [80]. Therefore, taking some defense measures on the cloud will provide extra guard to protect CAV from smart attacks.

 doi:10.20944/preprints202209.0230.v1

Basically, intrusion detection can protect CAV from security issues. Traditional intrusion detection uses some static analysis approaches, such as comparing programs to known malware based on the program code, looking for signatures or using other heuristics, which gradually expired to defend against the deformation of these attacks because they still expose some security loopholes [80, 120]. Incidentally, the cloud platform presents tremendous advantages for implementing new types of AI-based detection methods [121-126]. With the management of the cloud, large volumes of data can be captured from the Internet and collected from traffic situations by setting up some honeypot and trapping, and sufficiently-powerful hardware can be provided to support these sophisticated algorithms. This way, the components relevant to the reliable driving operations of each vehicle can be monitored by the cloud. In practice, the local vehicle can collect anomaly data in the first time. Each vehicle primarily performs core intrusion detection in a distributed manner, which is referred to as local layer intrusion detection. If a local vehicle cannot decide whether the data is malicious, they transmit the data to the cloud for further detection. The remote cloud can provide further verification of the local detection results within the time constraint, which is referred to as outer layer intrusion. Therefore, how to relieve the delay in communication in the multi-layer detection process to meet the requirements imposed by some applications is challenging.

## 6. Conclusions

In this survey, we reviewed a substantial number of literatures on CAV security since AV was developed. In the beginning, attacks mainly aimed at individual vehicles and were implemented through physical connectivity. With the increase of wireless connectivity on the vehicle, like Bluetooth, VANET, and cellular network, potential vulnerabilities of vehicles are increasingly exposed, and cyber-attacks are possibly implemented to exploit the vulnerabilities to impact the performance and operation of CAV. We analyzed the impact of cyber-attacks on CAV from the viewpoints of intra-vehicle system and inter-vehicle system. For both, the operation of CAV will be severely impacted if the vehicle connectivity is compromised, which may further cause damage to the vehicle or accidents directly. In the future, to employ fully-autonomous vehicle in practice, vehicle's perception and operation must be well secured, which is the top requirement on CAV application. In addition, with the development of IoV, some powerful detection and defense measures can be carried out on the cloud, which possesses enormous amounts of information and powerful resources, to protect CAV from some types of smart attacks. In a word, the security of CAV must be well considered and built before the CAV is fully developed and deployed in practice.

**Author Contributions:** Conceptualization, Z.W., J.W., and X.Z.; methodology, Z.W. and H.W.; software, Z.W.; validation, Z.W. and Y.C.; formal analysis, Z.W.; investigation, Z.W., J.W., X.Z. and H.W.; resources Z.W., Y.C. and H.W.; data curation, Z.W.; writing—original draft preparation, Z.W.; writing—review and editing, Z.W., H.W, J.W., X.Z., and Y.C.; visualization, Z.W. and H.W.

**Funding:** This research received no external funding.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. "NHTSA, SAE Define 5 Levels of Vehicle Automation，https://www.sema.org/sema-enews/2017/11/ettn-tech-alert-nhtsa-sae-define-5-levels-of-vehicle-automation."
2. K. Koscher et al., "Experimental security analysis of a modern automobile," in Security and Privacy (SP), 2010 IEEE Symposium on, 2010, pp. 447-462: IEEE.
3. V. Chris and M. Charlie, "Remote Exploitation of an Unaltered Passenger Vehicle," White Paper, p. 93, 2015.
4. J. Petit and S. E. Shladover, "Potential cyberattacks on automated vehicles," IEEE Transactions on Intelligent Transportation Systems, vol. 16, no. 2, pp. 546-556, 2015.
5. S. Parkinson, P. Ward, K. Wilson, and J. Miller, "Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges," IEEE Transactions on Intelligent Transportation Systems, 2017.

6. S. Checkoway et al., "Comprehensive Experimental Analyses of Automotive Attack Surfaces," in USENIX Security Symposium, 2011: San Francisco.
7. "Understanding the fatal Tesla accident on Autopilot and the NHTSA probe, https://electrek.co/2016/07/01/understanding-fatal-tesla-accident-autopilot-nhtsa-probe/."
8. S. Mahajan, R. Bhosale, and P. Kulkarni, "Obstacle detection using mono vision camera and laser scanner," Int. J. Res. Eng. Technol, vol. 2, no. 12, pp. 684-690, 2013.
9. J. Du, J. Masters, and M. Barth, "Lane-level positioning for in-vehicle navigation and automated vehicle location (AVL) systems," in Intelligent Transportation Systems, 2004. Proceedings. The 7th International IEEE Conference on, 2004, pp. 35-40: IEEE.
10. P. Grisleri and I. Fedriga, "The braive autonomous ground vehicle platform," IFAC Proceedings Volumes, vol. 43, no. 16, pp. 497-502, 2010.
11. J. Petit, "AUTOMATED VEHICLES VULNERABILITIES," ESCAR USA, June 01 2016.
12. B. G. Stottelaar, "Practical cyber-attacks on autonomous vehicles," University of Twente, 2015.
13. G. Lu, D. Zeng, and B. Tang, "Anti-jamming filtering for DRFM repeat jammer based on stretch processing," in Signal Processing Systems (ICSPS), 2010 2nd International Conference on, 2010, vol. 1, pp. V1-78-V1-82: IEEE.
14. Y. Cui and S. S. Ge, "Autonomous vehicle positioning with GPS in urban canyon environments," IEEE transactions on robotics and automation, vol. 19, no. 1, pp. 15-25, 2003.
15. N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Capkun, "On the requirements for successful GPS spoofing attacks," in Proceedings of the 18th ACM conference on Computer and communications security, 2011, pp. 75-86: ACM.
16. R. M. Ishtiaq Roufa et al., "Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study," in 19th USENIX Security Symposium, Washington DC, 2010, pp. 11-13.
17. M. Wolf, A. Weimerskirch, and C. Paar, "Security in automotive bus systems," in Workshop on Embedded Security in Cars, 2004.
18. M. Wolf, A. Weimerskirch, and T. Wollinger, "State of the art: Embedding security in vehicles," EURASIP Journal on Embedded Systems, vol. 2007, no. 1, p. 074706, 2007.
19. S. Jafarnejad, L. Codeca, W. Bronzi, R. Frank, and T. Engel, "A car hacking experiment: When connectivity meets vulnerability," in Globecom Workshops (GC Wkshps), 2015 IEEE, 2015, pp. 1-6: IEEE.
20. 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, no. 2, pp. 993-1006, 2015.
21. "An Analysis and Comparison of Hardware Security Modules for the Automotive Domain available https://www.escar.info/images/Datastore/2014_escar_Vortraege_USA/Frederic_Stumpf_escar_USA_2014.pdf," ESCAR USA, 2014.
22. I. Studnia, V. Nicomette, E. Alata, Y. Deswarte, M. Kaâniche, and Y. Laarouchi, "Survey on security threats and protection mechanisms in embedded automotive networks," in Dependable Systems and Networks Workshop (DSN-W), 2013 43rd Annual IEEE/IFIP Conference on, 2013, pp. 1-12: IEEE.
23. C. Valasek and C. Miller, "A survey of remote automotive attack surfaces," Scribd, Washington, USA, 2014.
24. D. Nilsson, U. Larson, and E. Jonsson, "Creating a secure infrastructure for wireless diagnostics and software updates in vehicles," Computer Safety, Reliability, and Security, pp. 207-220, 2008.
25. D. K. Nilsson and U. Larson, "A Defense-in-Depth Approach to Securing the Wireless Vehicle Infrastructure," JNW, vol. 4, no. 7, pp. 552-564, 2009.
26. Qualcomm, "Expanding and evolving the cellular system for V2X communications -- Introduced in 3GPP Release 14—part of LTE Advanced Pro," Jun. 2016.
27. J. D. T. a. Q. Y. Y. H. Sawant, "Using Bluetooth and sensor networks for intelligent transportation systems," IEEE intelligent Transportation Systems Conference 3-6 Oct. 2004.
28. A. Dardanelli et al., "A security layer for smartphone-to-vehicle communication over bluetooth," IEEE embedded systems letters, vol. 5, no. 3, pp. 34-37, 2013.
29. A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-Physical Systems Security--A Survey," IEEE Internet of Things Journal, 2017.
30. K. Han, S. D. Potluri, and K. G. Shin, "On authentication in a connected vehicle: Secure integration of mobile devices with vehicular networks," in Cyber-Physical Systems (ICCPS), 2013 ACM/IEEE International Conference on, 2013, pp. 160-169: IEEE.
31. D. Spill and A. Bittau, "BlueSniff: Eve Meets Alice and Bluetooth," WOOT, vol. 7, pp. 1-10, 2007.
32. K. Haataja, Security threats and countermeasures in Bluetooth-enabled systems. University of Kuopio, 2009.
33. B. B. Rhoades and J. M. Conrad, "A survey of alternate methods and implementations of an intelligent transportation system," in SoutheastCon, 2017, 2017, pp. 1-8: IEEE.
34. B. B. R. a. J. M. Conrad, "A survey of alternate methods and implementations of an intelligent transportation system," SoutheastCon, 30 March-2 April 2017 2017.
35. C.-M. Chou, C.-Y. Li, W.-M. Chien, and K.-c. Lan, "A feasibility study on vehicle-to-infrastructure communication: WiFi vs. WiMAX," in Mobile Data Management: Systems, Services and Middleware, 2009. MDM'09. Tenth International Conference on, 2009, pp. 397-398: IEEE.
36. S. Jeong, Y. Baek, and S. H. Son, "A Hybrid V2X System for Safety-Critical Applications in VANET," in Cyber-Physical Systems, Networks, and Applications (CPSNA), 2016 IEEE 4th International Conference on, 2016, pp. 13-18: IEEE.
37. K.-C. Su, H.-M. Wu, W.-L. Chang, and Y.-H. Chou, "Vehicle-to-vehicle communication system through wi-fi network using android smartphone," in Connected Vehicles and Expo (ICCVE), 2012 International Conference on, 2012, pp. 191-196: IEEE.

38. H. Viittala, S. Soderi, J. Saloranta, M. Hamalainen, and J. Iinatti, "An experimental evaluation of wifi-based vehicle-to-vehicle (V2V) communication in a tunnel," in Vehicular Technology Conference (VTC Spring), 2013 IEEE 77th, 2013, pp. 1-5: IEEE.
39. W.-F. C. P. O. A. http://www.wi-fi.org/discover-wi-fi/wi-fi-certified-passpoint.
40. J. Jansons and A. Barancevs, "Using wireless networking for vehicular environment: IEEE 802.11 a standard performance," in Digital Information Processing and Communications (ICDIPC), 2012 Second International Conference on, 2012, pp. 5-9: IEEE.
41. N. Lu, N. Cheng, N. Zhang, X. Shen, and J. W. Mark, "Connected vehicles: Solutions and challenges," IEEE internet of things journal, vol. 1, no. 4, pp. 289-299, 2014.
42. "Security Issues of WiFi - How it Works, https://www.alienvault.com/blogs/security-essentials/security-issues-of-wifi-how-it-works."
43. M. Vanhoef and F. Piessens, "Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2," ed: CCS, 2017.
44. H. Seo, K.-D. Lee, S. Yasukawa, Y. Peng, and P. Sartori, "LTE evolution for vehicle-to-everything services," IEEE Communications Magazine, vol. 54, no. 6, pp. 22-28, 2016.
45. J. Lee et al., "LTE-advanced in 3GPP Rel-13/14: an evolution toward 5G," IEEE Communications Magazine, vol. 54, no. 3, pp. 36-42, 2016.
46. G. Araniti, C. Campolo, M. Condoluci, A. Iera, and A. Molinaro, "LTE for vehicular networking: a survey," IEEE Communications Magazine, vol. 51, no. 5, pp. 148-157, 2013.
47. S.-h. Sun, J.-l. Hu, Y. Peng, X.-m. Pan, L. Zhao, and J.-y. Fang, "Support for vehicle-to-everything services based on LTE," IEEE Wireless Communications, vol. 23, no. 3, pp. 4-8, 2016.
48. "EXPANDING YOUR HORIZONS WITH LTE DIRECT -- ENABLING THE NEXT GENERATION OF PROXIMAL SERVICES https://www.qualcomm.com/documents/srg-whitepaper-expanding-your-horizons-lte-direct," Sep. 2015.
49. "V2X Cellular Solutions," Oct. 2016.
50. M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET security challenges and possible cryptographic solutions," Vehicular Communications, vol. 1, no. 2, pp. 53-66, 2014.
51. P. Papadimitratos and J.-P. Hubaux, "Report on the secure vehicular communications: results and challenges ahead workshop," ACM SIGMOBILE Mobile Computing and Communications Review, vol. 12, no. 2, pp. 53-64, 2008.
52. A. E. S. H. Hasrouny, C. Bassil and A. Laouiti, "VANET Security Challenges and Solutions: A Survey," Vehicular Communications, Elsevier, pp. 7-20, 2017.
53. K. Mershad and H. Artail, "A framework for secure and efficient data acquisition in vehicular ad hoc networks," IEEE Transactions on vehicular technology, vol. 62, no. 2, pp. 536-551, 2013.
54. A. Dhamgaye and N. Chavhan, "Survey on security challenges in VANET 1," 2013.
55. M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," Journal of computer security, vol. 15, no. 1, pp. 39-68, 2007.
56. J.-L. Huang, L.-Y. Yeh, and H.-Y. Chien, "ABAKA: An anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks," IEEE Transactions on Vehicular Technology, vol. 60, no. 1, pp. 248-262, 2011.
57. A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "The TESLA broadcast authentication protocol," Rsa Cryptobytes, vol. 5, 2005.
58. A. Wasef, Y. Jiang, and X. Shen, "ECMV: efficient certificate management scheme for vehicular networks," in Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE, 2008, pp. 1-5: IEEE.
59. A. Studer, E. Shi, F. Bai, and A. Perrig, "TACKing together efficient authentication, revocation, and privacy in VANETs," in Sensor, Mesh and Ad Hoc Communications and Networks, 2009. SECON'09. 6th Annual IEEE Communications Society Conference on, 2009, pp. 1-9: IEEE.
60. C. K. Wong, M. Gouda, and S. S. Lam, "Secure group communications using key graphs," IEEE/ACM transactions on networking, vol. 8, no. 1, pp. 16-30, 2000.
61. X. Zheng, C.-T. Huang, and M. Matthews, "Chinese remainder theorem based group key management," in Proceedings of the 45th annual southeast regional conference, 2007, pp. 266-271: ACM.
62. J. Zhou and Y. H. Ou, "Key tree and Chinese remainder theorem based group key distrubution scheme," Journal of the chinese institute of engineers, vol. 32, no. 7, pp. 967-974, 2009.
63. G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in VANET," in Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks, 2007, pp. 19-28: ACM.
64. R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in INFOCOM 2008. The 27th Conference on Computer Communications. IEEE, 2008, pp. 1229-1237: IEEE.
65. A. Boualouache, S.-M. Senouci, and S. Moussaoui, "A survey on pseudonym changing strategies for Vehicular Ad-Hoc Networks," arXiv preprint arXiv:1704.00679, 2017.
66. J. Freudiger, M. Raya, M. Félegyházi, P. Papadimitratos, and J.-P. Hubaux, "Mix-zones for location privacy in vehicular networks," in ACM Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS), 2007, no. LCA-CONF-2007-016.
67. 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, no. 1, pp. 86-96, 2012.
68. K. Emara, W. Woerndl, and J. H. Schlichter, "POSTER: Context-Adaptive User-Centric Privacy Scheme for VANET," in SecureComm, 2015, pp. 590-593.
69. K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, "AMOEBA: Robust location privacy scheme for VANET," IEEE Journal on Selected Areas in Communications, vol. 25, no. 8, 2007.

70. L. Buttyán, T. Holczer, A. Weimerskirch, and W. Whyte, "Slow: A practical pseudonym changing scheme for location privacy in vanets," in Vehicular Networking Conference (VNC), 2009 IEEE, 2009, pp. 1-8: IEEE.
71. B. Wiedersheim, Z. Ma, F. Kargl, and P. Papadimitratos, "Privacy in inter-vehicular networks: Why simple pseudonym change is not enough," in Wireless On-demand Network Systems and Services (WONS), 2010 Seventh International Conference on, 2010, pp. 176-183: IEEE.
72. S. Lefevre, J. Petit, R. Bajcsy, C. Laugier, and F. Kargl, "Impact of v2x privacy strategies on intersection collision avoidance systems," in Vehicular Networking Conference (VNC), 2013 IEEE, 2013, pp. 71-78: IEEE.
73. I. Wagner and D. Eckhoff, "Privacy assessment in vehicular networks using simulation," in Simulation Conference (WSC), 2014 Winter, 2014, pp. 3155-3166: IEEE.
74. D. Eckhoff, "Simulation of privacy-enhancing technologies in vehicular ad-hoc networks," 2016.
75. D. Eckhoff, M. Protsenko, and R. German, "Toward an open source location privacy evaluation framework for vehicular networks," in Vehicular Technology Conference (VTC Fall), 2014 IEEE 80th, 2014, pp. 1-2: IEEE.
76. J. Zhang, "A survey on trust management for vanets," in Advanced information networking and applications (AINA), 2011 IEEE international conference on, 2011, pp. 105-112: IEEE.
77. C. A. Kerrache, C. T. Calafate, J.-C. Cano, N. Lagraa, and P. Manzoni, "Trust management for vehicular networks: An adversary-oriented overview," IEEE Access, vol. 4, pp. 9293-9307, 2016.
78. T. Hoppe, S. Kiltz, and J. Dittmann, "Security threats to automotive CAN networks–practical examples and selected short-term countermeasures," Computer Safety, Reliability, and Security, pp. 235-248, 2008.
79. V. L. Thing and J. Wu, "Autonomous Vehicle Security: A Taxonomy of Attacks and Defences," in Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2016 IEEE International Conference on, 2016, pp. 164-170: IEEE.
80. T. Zhang, H. Antunes, and S. Aggarwal, "Defending connected vehicles against malware: Challenges and a solution framework," IEEE Internet of Things Journal, vol. 1, no. 1, pp. 10-21, 2014.
81. C. Vallance, "Car hack uses digital-radio broadcasts to seize control," BBC, July, 2015.
82. N. Idika and A. P. Mathur, "A survey of malware detection techniques," Purdue University, vol. 48, 2007.
83. Z. M. Fadlullah, H. Nishiyama, N. Kato, and M. M. Fouda, "Intrusion detection system (IDS) for combating attacks against cognitive radio networks," IEEE network, vol. 27, no. 3, pp. 51-56, 2013.
84. U. E. Larson, D. K. Nilsson, and E. Jonsson, "An approach to specification-based attack detection for in-vehicle networks," in Intelligent Vehicles Symposium, 2008 IEEE, 2008, pp. 220-225: IEEE.
85. 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 Information Networking (ICOIN), 2016 International Conference on, 2016, pp. 63-68: IEEE.
86. M.-J. Kang and J.-W. Kang, "A Novel Intrusion Detection Method Using Deep Neural Network for In-Vehicle Network Security," in Vehicular Technology Conference (VTC Spring), 2016 IEEE 83rd, 2016, pp. 1-5: IEEE.
87. T. Acarman, Y. Liu, and U. Ozguner, "Intelligent cruise control stop and go with and without communication," in American Control Conference, 2006, 2006, p. 6 pp.: IEEE.
88. S. Tsugawa and S. Kato, "Energy ITS: another application of vehicular communications," IEEE Communications Magazine, vol. 48, no. 11, 2010.
89. D. Jia, K. Lu, J. Wang, X. Zhang, and X. Shen, "A survey on platoon-based vehicular cyber-physical systems," IEEE Communications Surveys & Tutorials, vol. 18, no. 1, pp. 263-284, 2016.
90. M. Amoozadeh et al., "Security vulnerabilities of connected vehicle streams and their impact on cooperative driving," IEEE Communications Magazine, vol. 53, no. 6, pp. 126-132, 2015.
91. L. Xu, L. Y. Wang, G. Yin, and H. Zhang, "Communication information structures and contents for enhanced safety of highway vehicle platoons," IEEE Transactions on vehicular Technology, vol. 63, no. 9, pp. 4206-4220, 2014.
92. P. Seiler, A. Pant, and K. Hedrick, "Disturbance propagation in vehicle strings," IEEE Transactions on automatic control, vol. 49, no. 10, pp. 1835-1842, 2004.
93. S. Öncü, J. Ploeg, N. van de Wouw, and H. Nijmeijer, "Cooperative adaptive cruise control: Network-aware analysis of string stability," IEEE Transactions on Intelligent Transportation Systems, vol. 15, no. 4, pp. 1527-1537, 2014.
94. A. Alipour-Fanid, M. Dabaghchian, and K. Zeng, "Platoon Stability and Safety Analysis of Cooperative Adaptive Cruise Control under Wireless Rician Fading Channels and Jamming Attacks," arXiv preprint arXiv:1710.08476, 2017.
95. A. Di Maio et al., "Enabling sdn in vanets: What is the impact on security?," Sensors, vol. 16, no. 12, p. 2077, 2016.
96. A. Alipour-Fanid, M. Dabaghchian, H. Zhang, and K. Zeng, "String stability analysis of cooperative adaptive cruise control under jamming attacks," in High Assurance Systems Engineering (HASE), 2017 IEEE 18th International Symposium on, 2017, pp. 157-162: IEEE.
97. A. Petrillo, A. Pescapé, and S. Santini, "A collaborative control strategy for platoons of autonomous vehicles in the presence of message falsification attacks," in Models and Technologies for Intelligent Transportation Systems (MT-ITS), 2017 5th IEEE International Conference on, 2017, pp. Ze-115: IEEE.
98. R. Hall and C. Chin, "Vehicle sorting for platoon formation: Impacts on highway entry and throughput," Transportation Research Part C: Emerging Technologies, vol. 13, no. 5, pp. 405-420, 2005.
99. B. Liu et al., "Infrastructure-assisted message dissemination for supporting heterogeneous driving patterns," IEEE Transactions on Intelligent Transportation Systems, vol. 18, no. 10, pp. 2865-2876, 2017.

100. B. Liu, D. Jia, J. Wang, K. Lu, and L. Wu, "Cloud-Assisted Safety Message Dissemination in VANET–Cellular Heterogeneous Wireless Network," ieee systems journal, vol. 11, no. 1, pp. 128-139, 2017.
101. C. M. Silva, B. M. Masini, G. Ferrari, and I. Thibault, "A survey on infrastructure-based vehicular networks," Mobile Information Systems, vol. 2017, 2017.
102. Cao B, Kim MJ, Wang JR, van Santen JP, Mau T, Wang J. Articulation-to-Speech Synthesis Using Articulatory Flesh Point Sensors' Orientation Information. In Interspeech, pp. 3152-3156, 2018.
103. Wei, H. and Kehtarnavaz, N. Simultaneous utilization of inertial and video sensing for action detection and recognition in continuous action streams. IEEE Sensors Journal, 20(11), pp.6055-6063, 2020.
104. Wei, H. and Kehtarnavaz, N. Semi-supervised faster RCNN-based person detection and load classification for far field video surveillance. Machine Learning and Knowledge Extraction, 1(3), p.44, 2019.
105. Zhu, H., Wei, H., Li, B., Yuan, X. and Kehtarnavaz, N. A review of video object detection: Datasets, metrics and methods. Applied Sciences, 10(21), p.7834, 2020.
106. Zeng, X., Wang, Z. and Hu, Y., 2022. Enabling Efficient Deep Convolutional Neural Network-based Sensor Fusion for Autonomous Driving. arXiv preprint arXiv:2202.11231.
107. G. Thomaidis, K. Vassilis, P. Lytrivis, M. Tsogas, G. Karaseitanidis, and A. Amditis, "Target tracking and fusion in vehicular networks," in Intelligent Vehicles Symposium (IV), 2011 IEEE, 2011, pp. 1080-1085: IEEE.
108. S. S. Haykin, Kalman filtering and neural networks. Wiley Online Library, 2001.
109. A. Rauch, F. Klanner, R. Rasshofer, and K. Dietmayer, "Car2x-based perception in a high-level fusion architecture for cooperative perception systems," in Intelligent Vehicles Symposium (IV), 2012 IEEE, 2012, pp. 270-275: IEEE.
110. Bateni, S., Wang, Z., Zhu, Y., Hu, Y. and Liu, C., 2020, April. Co-optimizing performance and memory footprint via integrated cpu/gpu memory management, an implementation on autonomous driving platform. In 2020 IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS) (pp. 310-323). IEEE.
111. Wang, Z., Jiang, Z., Wang, Z., Tang, X., Liu, C., Yin, S. and Hu, Y., 2020. Enabling Latency-Aware Data Initialization for Integrated CPU/GPU Heterogeneous Platform. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 39(11), pp.3433-3444.
112. Wang, Z., Wang, Z., Liu, C. and Hu, Y., 2020. Understanding and tackling the hidden memory latency for edge-based heterogeneous platform. In 3rd USENIX Workshop on Hot Topics in Edge Computing (HotEdge 20).
113. S. Levine, P. Pastor, A. Krizhevsky, J. Ibarz, and D. Quillen, "Learning hand-eye coordination for robotic grasping with deep learning and large-scale data collection," The International Journal of Robotics Research, p. 0278364917710318, 2016.
114. V. Mnih et al., "Human-level control through deep reinforcement learning," Nature, vol. 518, no. 7540, pp. 529-533, 2015.
115. C. Chen, A. Seff, A. Kornhauser, and J. Xiao, "Deepdriving: Learning affordance for direct perception in autonomous driving," in Proceedings of the IEEE International Conference on Computer Vision, 2015, pp. 2722-2730.
116. M. Bojarski et al., "End to end learning for self-driving cars," arXiv preprint arXiv:1604.07316, 2016.
117. J. Wan, D. Zhang, S. Zhao, L. Yang, and J. Lloret, "Context-aware vehicular cyber-physical systems with cloud support: architecture, challenges, and solutions," IEEE Communications Magazine, vol. 52, no. 8, pp. 106-113, 2014.
118. E.-K. Lee, M. Gerla, G. Pau, U. Lee, and J.-H. Lim, "Internet of Vehicles: From intelligent grid to autonomous cars and vehicular fogs," International Journal of Distributed Sensor Networks, vol. 12, no. 9, p. 1550147716665500, 2016.
119. Liu, S., Wang, J., Wang, Z., Yu, B., Hu, W., Liu, Y., Tang, J., Song, S.L., Liu, C. and Hu, Y., 2022, May. Brief industry paper: The necessity of adaptive data fusion in infrastructure-augmented autonomous driving system. In 2022 IEEE 28th Real-Time and Embedded Technology and Applications Symposium (RTAS) (pp. 293-296). IEEE.
120. M. Christodorescu and S. Jha, "Static analysis of executables to detect malicious patterns," Wisconsin Univ-Madison Dept of Computer Sciences2006.
121. Wang, Z., Wang, R., Jiang, Z., Tang, X., Yin, S. and Hu, Y., 2021, November. Towards a Secure Integrated Heterogeneous Platform via Cooperative CPU/GPU Encryption. In 2021 IEEE 30th Asian Test Symposium (ATS) (pp. 115-120). IEEE.
122. M. G. Schultz, E. Eskin, F. Zadok, and S. J. Stolfo, "Data mining methods for detection of new malicious executables," in Security and Privacy, 2001. S&P 2001. Proceedings. 2001 IEEE Symposium on, 2001, pp. 38-49: IEEE.
123. Wang, Z., Zeng, X., Tang, X., Zhang, D., Hu, X. and Hu, Y., 2022. Demystifying Arch-hints for Model Extraction: An Attack in Unified Memory System. arXiv preprint arXiv:2208.13720.
124. Wang, Z. and Hu, Y., 2022. Towards a High-performance and Secure Memory System and Architecture for Emerging Applications. arXiv preprint arXiv:2205.04002.
125. Wang, Z., Wang, J., Wang, Z. and Hu, Y., 2021, December. Characterization and Implication of Edge WebAssembly Runtimes. In 2021 IEEE 23rd Int Conf on High Performance Computing & Communications; 7th Int Conf on Data Science & Systems; 19th Int Conf on Smart City; 7th Int Conf on Dependability in Sensor, Cloud & Big Data Systems & Application (HPCC/DSS/SmartCity/DependSys) (pp. 71-80). IEEE.
126. G. J. Tesauro, J. O. Kephart, and G. B. Sorkin, "Neural networks for computer virus recognition," IEEE expert, vol. 11, no. 4, pp. 5-6, 1996.
127. Khanh, Q.V., Hoai, N.V., Manh, L.D., Le, A.N. and Jeon, G., 2022. Wireless communication technologies for IoT in 5G: vision, applications, and challenges. Wireless Communications and Mobile Computing, 2022.
128. Cheng, N., Lyu, F., Chen, J., Xu, W., Zhou, H., Zhang, S. and Shen, X., 2018. Big data driven vehicular networks. Ieee Network, 32(6), pp.160-167.

129. Quy, V.K., Nam, V.H., Linh, D.M., Ban, N.T. and Han, N.D., 2021. Communication solutions for vehicle ad-hoc network in smart cities environment: a comprehensive survey. Wireless Personal Communications, pp.1-25.
130. Zhang, K., Ni, J., Yang, K., Liang, X., Ren, J. and Shen, X.S., 2017. Security and privacy in smart city applications: Challenges and solutions. IEEE Communications Magazine, 55(1), pp.122-129.
131. Péter, G., Kiss, B. and Tihanyi, V., 2019. Vision and odometry based autonomous vehicle lane changing. ICT Express, 5(4), pp.219-226.
132. Zablocki, É., Ben-Younes, H., Pérez, P. and Cord, M., 2021. Explainability of vision-based autonomous driving systems: Review and challenges. arXiv preprint arXiv:2101.05307.
133. Zhang, F., Wang, Z., Zhong, Y. and Chen, L., 2022. Localization Error Modeling for Autonomous Driving in GPS Denied Environment. Electronics, 11(4), p.647.
134. Yang, S., Chen, Y., Shi, R., Wang, R., Cao, Y. and Lu, J., 2022. A Survey of Intelligent Tires for Tire-road Interaction Recognition. IEEE Transactions on Intelligent Vehicles.
135. Liu, Z., Wang, L., Wen, F. and Zhang, H., 2021, May. IMU/vehicle calibration and integrated localization for autonomous driving. In 2021 IEEE International Conference on Robotics and Automation (ICRA) (pp. 4013-4019). IEEE.