applied sciences

MDPI

Review

Aspects of Cyber Security in Autonomous and Connected Vehicles

Bhavesh Raju Mudhivarthi [1], Prabhat Thakur [1,2] and Ghanshyam Singh [2,*]

[1] Symbiosis Institute of Technology, Symbiosis International (Deemed University), Pune 412115, Maharashtra, India
[2] Centre for Smart Information and Communication Systems, Department of Electrical and Electronic Engineering Science, University of Johannesburg, Auckland Park Kingsway Campus, P.O. Box 524, Johannesburg 2006, South Africa
* Correspondence: ghanshyams@uj.ac.za

Abstract: An automobile is a computer on wheels after the integration of electronics. This handshake of electronics and mechanical systems makes a vehicle smart, and comfortable; driver assistance for achieving this involves data exchange and surroundings sensing. Devices such as sensors, telematics, protocols, etc., are responsible for data exchange and data sensing. This process contains some loopholes that are the preliminary sources for the attacker to attack the vulnerable devices to control the vehicle. This article provides a review of possible attacks and defenses on autonomous and connected vehicles. The attacker's area of autonomous and connected vehicles is classified into three categories that are safety system attacks, connectivity attacks, and diagnostics attacks, and provided all possible defenses for those attacks. In addition, we provided an analysis of the domain to understand the scenarios in this domain, recommendations, and future scope in this area for further work.

Keywords: automobile; cyber security; attacks; network security; intrusion detection

check for updates

Citation: Mudhivarthi, B.R.; Thakur, P.; Singh, G. Aspects of Cyber Security in Autonomous and Connected Vehicles. *Appl. Sci.* **2023**, *13*, 3014. https://doi.org/10.3390/app13053014

Academic Editors: Anikó Costa and Remigiusz Wiśniewski

Received: 11 January 2023
Revised: 16 February 2023
Accepted: 22 February 2023
Published: 26 February 2023

1. Introduction

As per the current demands of autonomous and connected vehicles, information and connected/communication technologies (ICT) play a specific role. Vehicles shake hands with electronics to reach user demands, ensure safety features, as well as invite new technologies. The vehicle changed its infrastructure to become a modern vehicle with mechanical and electronic components [1]. This transformation into a modern vehicle includes hundreds of electronic control units (ECU) and communication protocols and sensors. The purpose of the ECU is to collect the sensor data and other ECU data as per requirements to perform the desired task. This scenario is possible with the help of communication protocols such as controller area network (CAN), local interconnect network (LIN), Ethernet, and FlexRay. All components work together to develop an infotainment system, anti-lock braking system, advanced driver assistant system (ADAS) feature, and so on [2]. Sensors such as cameras, light detection and ranging (LIDAR), and radio detection and ranging (RADAR) play an important role in sensing surroundings to help the vehicle in taking decisions. In [3], the authors have discussed the 3D point-cloud (3DPC) processing and learning for autonomous vehicles. Lidar accurately captures the outer surfaces of scenes and objects using 3DPC. The learning tools in the 3DPC help in creating maps, perceptions, and localization devices in an autonomous vehicle. Similarly, images captured by the camera are important in taking decisions. In [4], the authors have discussed generalized pixel value ordering (PVO) base reversible data hiding using firefly algorithm (GPVOFA) for digital images. The role is to embed the secret information in the host image while recovering the embedded secret information and original image from the stego image.

The modern vehicle geared up its growth with help of the trending technologies such as big data, internet of things (IoT) [5], cloud computing [6], and wireless communication protocols such as hypertext transfer protocol (HTTP), internet protocol (IP) [7], etc., to become an intelligent vehicle and to design more safety and advanced features such as telematics, artificial intelligence (AI) and, machine learning(ML) integration [8]. A vehicle with more features includes more scope for vulnerability for the attackers to hack the vehicle systems. Therefore, cyber security measurements are important for the next generation of connected vehicles or vehicular networks [9].

Automobile cyber security is the protection of electronic systems, control units, communication networks, the data of the user, and so on to avoid malicious attacks. Security is necessary because today's cars are computers on wheels rather than just mechanical boxes. If an automobile developed a vulnerability, a hacker might easily compromise the vehicle, which could result in undesirable events [10]. To demonstrate the possibilities of hacking an automobile by performing reverse engineering on the CAN network, the authors [11] conducted a study on the vehicle in 2010. Consider the following examples to illustrate the significance of cyber security: In 2015, two hackers, Charlie Miller and Chris Valasek, demonstrated how important it is by remotely hacking a Jeep Cherokee without any physical contact using the CAN bus, cellular connection, and inter-process communication desktop bus (IPC- D bus) [12] and. In the year 2016, scientists provided a way to hack the Tesla Model S car through the Wi-Fi interface and different vulnerabilities in the software [13]. These examples show that vulnerable parts of the vehicles are the more interesting areas for hackers to hack the vehicle.

There are two possible ways to hack a vehicle, one is physical, and the other is wireless. A few parts which are more vulnerable to physical attack are onboard diagnostics (OBD) ports, and wireless attacks are keyless car entry and telematics. These attacks are carried out by automotive protocols such as CAN, Ethernet, and FlexRay due to a lack of authentication and encryption capabilities [14]. Considering the CAN protocol, a hacker can inject unwanted messages through an OBD-II connection or telematics. Once undesired input reaches the vehicle network, the hacker can control the remaining units of the car as shown in Figure 1 [15]. Therefore, in this article, we have emphasized the various perspectives of cyber security in the field of connected and autonomous vehicles and vehicular networks. In addition, it is the collection of cyber-attacks and defenses for a connected and autonomous vehicle.

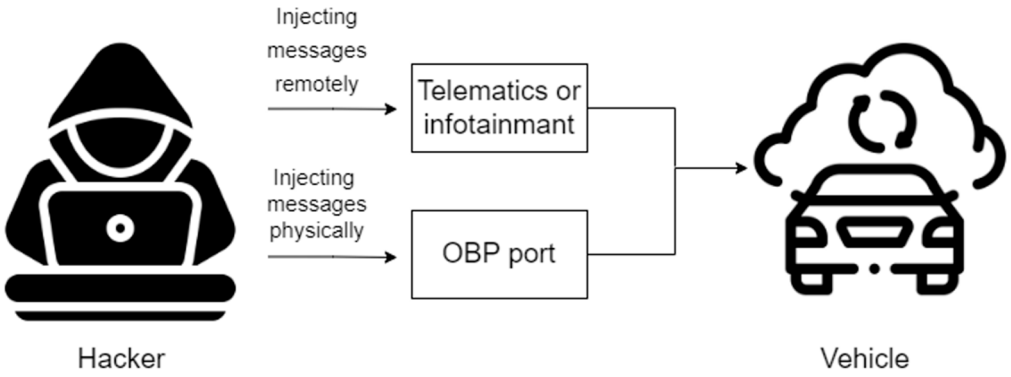


Figure 1. Injecting messages into the CAN network.

The author's potential contributions are summarized as follows.

- We have illustrated the bibliometric survey and reviewed the collected data from the Scopus database.
- Further, we have classified the various attacks in autonomous and connected vehicles.
- Moreover, we have researched various defenses for the attacks on the classified regions as well as recommended a few future works.

Further, this paper is structured as follows. Section 2 is a description of related work, Section 3 describes contributions, Section 4 gives a clear overview of the autonomous and connected vehicle, Section 5 gives an idea about the possible attacks on the autonomous and connected vehicles, Section 6 describes all possible defenses for autonomous and connected vehicles, Section 7 describes the result of the review, and Section 8 describes recommendations and future directions.

2. Related Work

The authors in [16], surveyed attacks and defenses for connected and autonomous vehicles (CAV). Attacks on CAV are classified into three regions: in-vehicle network attacks, vehicle-to-everything (V2X) attacks, and other attacks. We provide defense strategies and necessary actions to overcome the attacks. Authors in [17], explained the basic concept of in-vehicle networks. The vulnerabilities and attacks on the in-vehicle networks and countermeasures to overcome them are provided. Authors in [18], provided a clear review of cyber-attacks on the sensing layers. The sensing layer is classified into two categories: vehicle dynamics sensors and environmental sensors. Vehicle dynamics sensors include magnetic encoders, inertial sensors, etc. Environmental sensors include cameras, lidars, radars, etc. Countermeasures for the two types of sensor attacks are provided. The authors in [19] have surveyed autonomous vehicles. We classified the possible attacks into five categories, vehicular ad hoc networks (VANETs) based on sensors, hardware attacks, adversarial attacks, and malicious attacks. Authors in [20], provided a clear review of the possible attacks on the connected vehicle. Based on the attacks, provided defenses were classified into four types of network security, software vulnerability detection, cryptography, and malware detection, and mentioned future possible defenses.

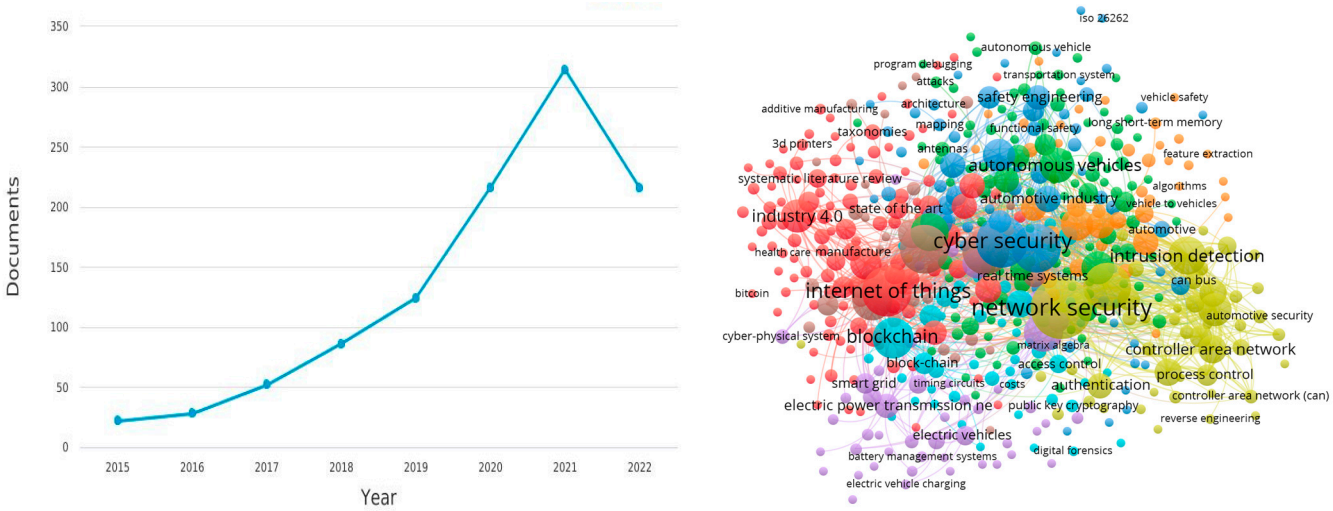
The authors have surveyed attacks and defenses on vehicles from 2008 to 2019 based on analysis attacks are classified into an autonomous driving system, autonomous control systems components, and V2X communications [21]. Defenses for those attacks are classified into security architecture, intrusion detection, and anomaly detection. In the end, they discussed the artificial intelligence integration in autonomous and connected vehicles relates to smart cities. The authors in [22], focused on connectivity including V2X and in-vehicle communication and considered communication technology implementation as one of the major reasons for the cyber-attacks on these systems. They discussed the major cyber-attacks on intelligent connected vehicles and available defenses. They categorized the defenses into four likely cryptographies, network security, software vulnerability detection, and malware detection. They discussed future directions to avoid attacks on intelligent connected vehicles. A discussion on the attacks and defenses of the connected vehicle considers V2X as a major concern and challenge in state-of-the-art intra-inter vehicle communication which is well explored in [23]. The authors have discussed defenses that can avoid these attacks and understand the hacker's methods or way of attacking. Authors in [24], discussed the safety failures and cyber-attacks on the autonomous vehicle and collected possible countermeasures to take care of the safety and security of the autonomous vehicle.

Existing works worked on attacks and defenses on one region such as a connected vehicle, autonomous vehicle, etc. This article is a review of possible attacks and defenses on a autonomous and connected vehicle. Attack regions for a autonomous and connected vehicle are classified into three categories safety systems, connectivity, and diagnostics. Safety systems include active safety systems and passive safety systems, connectivity is further classified into three regions V2X, in-vehicle, smart features, and diagnostics are classified as OBD ports and firmware over the air (FOTA). High possible attacks on these three classifications are explained and defenses for the attacks are mentioned. Future recommendations are provided to work on new defense strategies to overcome attacks.

3. Domain Analysis

This domain analysis is made with the help of data collected from the Scopus database by using the keywords cyber security and automobile. Matches for the search are more than 1000 documents. English is the most preferred language in this domain, and articles are the most preferred document type, network security is the most used keyword, Choo, K.K.R. published more publications in this area, and the national natural science foundation of China is the funding agency with a greater number of publications, this research is greater in the United States.

Figure 2a describes the number of publications per year, publications are increasing yearly describes it as a good area to pursue research. It is a good area to pursue research. Figure 2b is a cluster of co-occurring keywords network security, cyber security, intrusion detection, internet of things, autonomous vehicle, and block-chain are the most co-occurring keywords.



(**a**) (**b**)

Figure 2. (**a**) Number of documents per year (**b**)The cluster of co-occurrences of keywords.

4. Autonomous and Connected Vehicle

Considering security as a major point, autonomous and connected vehicles are classified into three main areas which are shown in Figure 3.

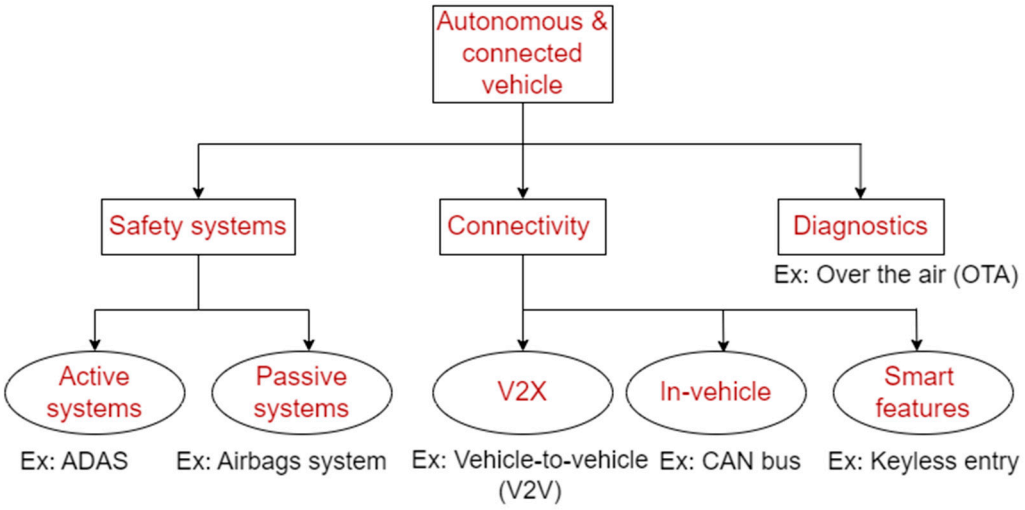


Figure 3. Classification of attack paths in autonomous and connected vehicle.

4.1. Safety Systems

Vehicle safety systems are classified into two types: active safety systems (ASS) and passive safety systems (PSS). The ASSs are designed to prevent accidents by giving support to the driver. The ASS mainly includes three important things to work sensors for sensing the environment, processors for processing, and actuators to perform an action to prevent undesired events [25]. The ADAS features are the best examples of ASS. According to the national highway traffic safety administration, ADAS includes five levels of autonomous safety features from level 0 to level 4 [26]. A few of ADAS' features are lane departure warnings, an anti-lock braking system (ABS), adaptive cruise control, and so on. Lane departure warning is invented to avoid road accidents while changing lanes this system displays the lane changing in formation and alerts while changing lanes [27]. ABS is mostly used nowadays to prevent accidents. Input for this system is a wheel speed sensor with the help of the collected data it will stop the wheel from locking during the breaking process [28]. Adaptive cruise control is one of the popular systems designed to maintain a certain distance from the vehicle ahead, stay at the limit speed, and automatically change the speed if the driver is not alert [29].

A PSS uses the same components as ASS to work but PSS deals after an accident to reduce the risk of injury [30]. This system includes airbags system, seat belts, etc. The airbag system works with the help of crash sensors. When a crash sensor detects a reduction in speed or crashes it will send the signal to the airbag module to start operating then with the help of some chemical reaction nitrogen gas will fill in the airbags to inflate them within 0.05 s. The airbag will stay inflated for 0.1 s and deflate in 0.3 s. Seat belts are designed to keep the passengers in a stable position and avoid collision with things ahead [31].

4.2. Connectivity

Connectivity is an area that includes all connected features. This area is classified into three sub-regions such as V2X, smart connected features to provide more comfort to the users, and in-vehicle connections [32].

Figure 4 illustrates the V2X which includes a few connected features such as vehicle-to-pedestrian (V2P), vehicle-to-infrastructure (V2I), vehicle-to-network (V2N), and vehicle-to-vehicle (V2V) [33]. V2P is a connected feature that alerts the driver about people on the road by making direct communication between the vehicle and vulnerable road users such as walking people, cyclists, people in wheelchairs, and so on [34]. V2I communication is for sharing vehicle information with some devices which are related to road and highway systems [35]. Devices include cameras, traffic lights, etc. V2I was traditionally designed with the help of VANETs [36]. V2V connectivity makes two vehicles talk to each other by sharing location, speed, and needed information to overcome traffic and avoid collisions. V2V is also designed with VANETs [37]. V2N provides a service to develop communication between vehicles, traffic lights, and people on the road. In simple words, V2N provides cloud services to exchange data [38]. The integration of AI in V2X collects data from different devices and helps in the prediction of road accidents, improving comfort, safety, and driver experience [39]. AI can be achieved by using techniques such as swarm intelligence, machine learning, etc. In V2X the swarm intelligence is used to interact with another local vehicle or the surrounding environment with the independence of the central server. In [40], the authors clearly explained the swarm intelligence for wireless communication. The ML concept plays an important role in AI and achieves this in three methods supervised learning, unsupervised learning, and reinforcement learning [41]. An ML follows a two stage process to achieve goals through training and testing. During the training stage, the ML is trained with collected data and then tested in the test stage to obtain predictions [39].

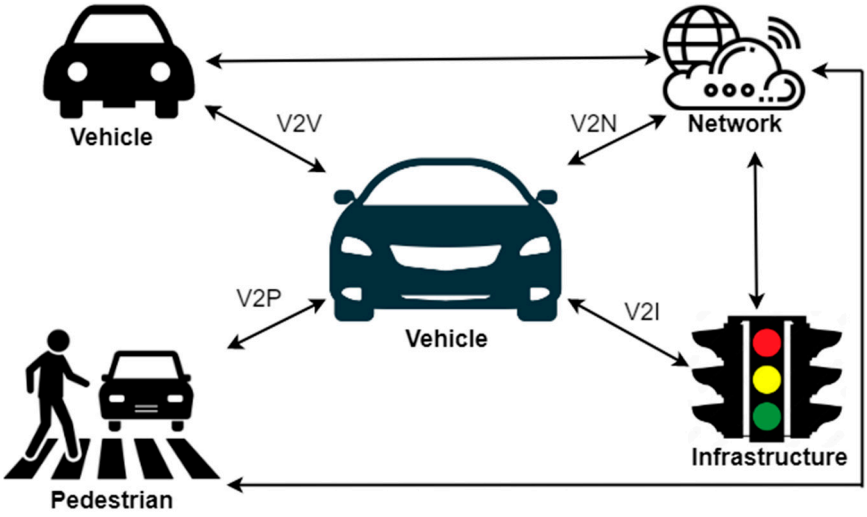


Figure 4. Types of V2X applications in connected vehicles.

Smart features of the vehicle include an infotainment system, a smart app, and so on. The infotainment system's main purpose is to provide entertainment. It contains radio, internet, and an mp3 player which provide a wide number of applications to the user such as providing music, providing web browsing, services to book tickets, setting up maps for reaching the destination, etc. [38]. A few vehicles introduced a smart app for the vehicle to control to obtain information and control some systems. Information such as the availability of parking slots, vehicle health information, etc., will be received through the application [42].

In-vehicle connectivity includes the communication protocols that are providing communication inside the vehicle such as CAN, LIN, FlexRay, and Ethernet. The CAN network is the widely used network in the automobile designed by Robert Bosch in the year 1980. A CAN bus is used to provide communication between different controllers, sensors, and actuators. This comes in two variants, high-speed CAN with a data rate of up to 1 Mb/s and low-speed CAN with a data rate of up to 125 b/s. A CAN bus sends data of 8 bytes which uses carrier sense multiple access/collision detection [43]. LIN is used for low-speed applications. It is a single wired protocol that acts as a sub-network for the main network such as CAN and Ethernet [44]. It can transfer data of 8 bytes with a data rate of 20 Kb/s. It follows the master-slave approach and provides up to 16 slaves [45]. FlexRay is used for high-speed applications such as safety-critical applications. It transfers 254 bytes of data with a data rate of 5 Mb/s. It uses the time division multiple access techniques to solve errors and accurate transfer of data [43]. Ethernet is the most popular local area network. It uses carrier sense multiple access/collision detection technique. It transfers data of 1500 bytes with a data rate of 40 Gb/s. It is based on the IEEE 802.3 standard [43]. Table 1 describes the in-vehicle communication protocols data rate and payload size.

Table 1. In-vehicle connectivity specifications.

Protocols	CAN [43]	LIN [45]	FlexRay [43]	Ethernet [43]
Data rate	1 Mb/s	20 Kb/s	5 Mb/s	40 Gb/s
Data field	8 bytes	8 bytes	254 bytes	1500 bytes

4.3. Diagnostics

Vehicle diagnostics is the process to find out the problem and any other issues that are affecting normal vehicle operation. Figure 5 describes the diagnostics. One way is performing physically through the OBD port, and another way is through the cloud server likely over-the-air (OTA).

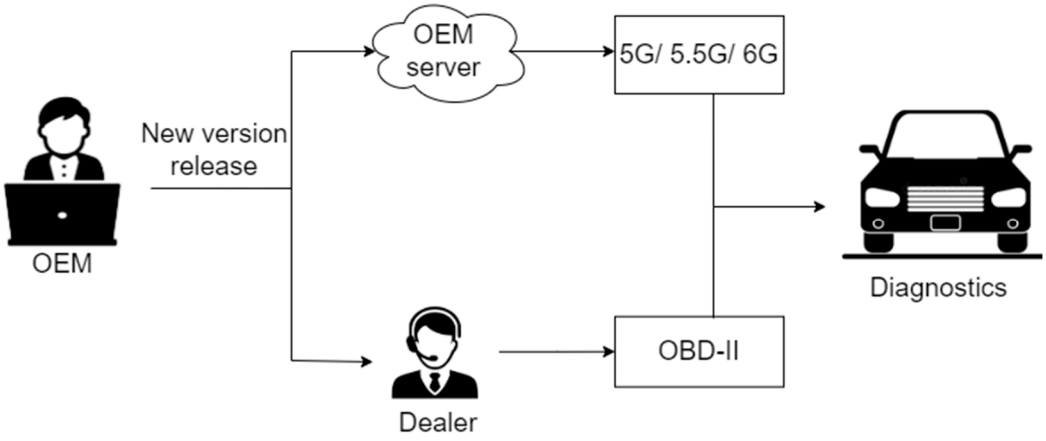


Figure 5. The types of approaches for vehicle diagnostics.

The OBD allows the technician or vehicle operators to check the status of the major systems that are connected through the engine. An OBD is a port presented inside the vehicle to receive data and faults [46]. OBD ports are used to detect the firmware details of the ECU. If the firmware is outdated or the firmware contains bugs. The OBD port is useful to reflash the firmware [47]. The OTA has come with the trend of the connected car. It is used to download an application, services, and needed configurations over Wi-Fi, 3G or LTE [48]. OTA is used to update the firmware and software of the vehicle automatically [49].

5. Attacks on Autonomous and Connected Vehicle

Attacks on autonomous and connected vehicles are classified based on safety, connectivity, and diagnostics. The devices which sense the surrounding environment, collect data from external devices, and interfaces for data exchange in the vehicle are more vulnerable to carry attacks.

5.1. Attacks on Safety Systems

Safety systems are designed to avoid road accidents or reduce the risk after an accident. The main components of these systems are sensors, ECU, and actuators. These principal components are more vulnerable to attacks [50].

Authors in [51], designed a model to attack a frequency-modulated continuous wave (FMCW) radar. That system uses one modulation scheme such as fast chirp modulation and rough radar. This system is a cable for spoofing the distance and velocity measured by the targeted vehicle. To spoof the distance, it uses delay and to spoof velocity it uses compensation of phase. This system used software-defined radio and demonstrated two real-life situations to spoof the target vehicle. Authors in [52], showed the way of hacking an ABS that leads to a disruptive attack and spoofing attack. Attackers can interrupt the magnetic field of the ABS by placing an electromagnetic actuator between the ABS wheel speed sensor (WSS) that interrupts the output of the wheel speed sensor which may lead to misbehavior of the entire ABS. Authors in [53], showed the way to approach an eavesdropping attack on the tire pressure monitor sensor (TPMS). This attack leads an attacker to know the location of the vehicle and they can spoof the pressure readings then the driver can stop the vehicle to check the pressure which may lead to physical attacks or robbery. Authors in [54], explained location spoofing leads a driver to follow the map as per the hacker's desire. Few systems in the vehicle are global positioning system (GPS) dependent, if the GPS is hacked it may be easy for the hackers to hack the remaining dependent systems in the vehicle.

Lidars are one of the most important sensors in safety systems to sense external environmental situations. Authors in [55], explained the replay attack where attackers can record the signals from the lidar. After some time, they will reuse the signals to insert some malware or unwanted things to interrupt the lidar operation to detect the objects which

are not present. Authors in [18], explained the relay attack which is an extended version of the replay attack. Here attackers receive the signals from the lidar. The received signals are sent to the receiver at a different location which leads to the interruption of the lidar. Authors in [56], explained the blinding attack on the lidar. attackers create this attack by injecting light of the same wavelength as the pulses of the lidar. This leads to the instability of the lidar, and it will not provide accurate services to the automobile. Authors in [34], explained the denial of service (DoS) attack on the lidar. Attackers create a large number of objects using jamming or spoofing. If the number of objects increases that may lead to instability of the lidar.

Ultrasonic sensors are used in safety systems to detect nearby objects by generating ultrasonic waves. Authors in [57], explained blind spot exploitation attacks and sensor interference attacks on the ultrasonic sensor. In the case of a blind spot exploitation attack, the sensor has vulnerabilities. It cannot detect a thin object which helps the attackers to keep the thin objects while reversing the vehicle. In case of a sensor interference attack, attackers place another ultrasonic sensor to interrupt the vehicle's ultrasonic sensor.

Cameras are another major sensor used to sense the surroundings to alert the driver regarding that safety. Authors in [18], explained the blinding attack on the camera. Attackers use strong light beams to interrupt the cameras if the light beams fall on the camera continuously which may lead to emergency braking. Authors in [44,45], described the phantom attacks on ADAS features. ADAS are integrated into the modern vehicle for full automation or semi-automation. For operation, they need to sense the surrounding environment with the help of sensors such as cameras to take necessary actions such as taking a diversion and applying breaks. Phantoms are illusions created by the hacker on the road with the use of drowning with a projector to project objects such as a human on the street then cameras in the vehicle sense it as a real object and take necessary actions that may cause risk to passengers. Table 2 is the collection of existing attacks on the safety systems with vulnerable parts.

5.2. Attacks on Connectivity

Connectivity is included in the vehicle to make it smart. This feature includes in-vehicle connectivity using bus networks to communicate the system to the system and V2X features to communicate with the external environment and smart connecting features such as infotainment, keyless entry, etc.

The V2X feature comes under connectivity enabling the vehicle to exchange data with other vehicles, pedestrians, infrastructure, and network. Authors in [58,59], described DoS attacks in the connected car. It will happen when the hacker blocks the communication channel with interference signals. The hacker inserts undesired messages on the network to increase the load which creates a delay in the communication, increases latency, and sometimes the message will not reach the destination. Authors in [60], described impersonation attacks in the connected car. Every vehicle has a unique identity to communicate with the remaining things. These attacks are created by using a fake identity. This attack is implemented by using a single identity. If multiple identities are used to spoof them, it comes under sybil attacks. Authors in [16], described replay attacks in the connected car. It happens in the network or transportation layer. This is created when the hacker reuses the previous packets. It plays with authorities and traffic in the network and may cause transportation damage. Authors in [61–63], described routing attacks. Routing attacks are from vulnerabilities and loopholes in the routing protocols. Routing attacks include three types black hole attack, grey hole attack, and wormhole attack. A black hole attack is created when one node is compromised or some cooperated nodes. Grey hole attack makes attackers inject packets in a selective way; this attack is difficult to detect. A wormhole attack creates when one or two nodes are compromised. Authors in [64,65], described data falsification attacks. The received data should be accurate to avoid road accidents. Undesired data may lead to fatal accidents. Attackers give false information and false safety warnings to the driver that may lead to unwanted situations. This includes message tam-

pering, suppression, and alteration to produce false information. For example, an attacker can give false information regarding the route that may create some delay in reaching the destination or chances of creating traps. Authors in [66], described eavesdropping attacks. These attacks are difficult to detect as the attackers will not disturb the communication. Attackers only listen to the information that is passing through the network and collect all privacy details.

Smart features make life easier with connectivity such as Bluetooth. Authors in [67], described password and key attacks. There are three kinds of attacks possible under this category: dictionary attacks, brute force attacks, and rainbow table attacks. Dictionary attackers use a list of words repeatedly to crack the password. Brute force attackers use non-letter characters repeatedly to crack the password. Rainbow table attackers use hash values to crack passwords or algorithms. Authors in [16], described the keyless entry or key fob attacks. Attackers block the signals of the key while locking the car by using different devices. These devices are hidden in secret places in the car park to block signals. In the keyless entry, the signals to open the door are listened to by the attacker and replay those signals to open the door.

In-vehicle connectivity includes the buses providing communication in the vehicle systems. Authors in [68], Explained the CAN frame sniffing attack. Attackers can sniff the malicious node in the CAN network and collect the data frames and interrupt the CAN communication. Authors in [11], Explained the CAN frame falsifying attack. Attackers create a fake CAN frame and send that frame into the network which leads to malicious functions or interrupts communication. Authors in [69], explained the ethernet content-addressable memory (CAM) table overflow. CAM attacks focus to disturb the media access control (MAC) address of the in-vehicle communication. Attackers flood the random packets with different MAC addresses into the network until the target ECU stops accepting the MAC addresses. The CAM table of the target ECU becomes the reason behind it. Authors in [70], Explained the LIN false frame attack. The attackers inject false frames on the network in order to tamper with the slave node which leads to malfunctioning. Authors in [71], explained the FlexRay full DoS attack and targeted DoS attack. The attacker generates continuous dominant signals on the bus to disturb communication in a full DoS attack. To achieve this, the attacker has to enable the transmitter pin to be low. In a targeted DoS attack, the attackers disable the node to send the data to the target or make the data unavailable to reach the target. To achieve this the attacker has to generate the continuous dominant bit during the transmission which leads the receiver to start avoiding the data. Attacks on the vehicle connectivity systems are mentioned in Table 2.

5.3. Attacks on Diagnostics

Diagnostics involves identifying the improper operations of the vehicle to cure those to make the vehicle operate properly. OBD ports are present in the vehicle nowadays to provide diagnostics to the vehicle by detecting problems in the ECU, sensor, and actuator operations.

Authors in [72,73], discussed an in-vehicle access attack. The OBD port is the reason behind the attack. OBD ports give gate passes to the attackers to enter the malware into the vehicle. This causes attacks on vehicles and buses. Authors in [73], Explained OBD ports are the reason for the CAN frame sniffing and CAN frame injection. If OBD provides access to these two attacks it is easy for the attacker to take over the entire vehicle. Authors in [74], explained control override attacks. This attacker downloads the OTA firmware and adds the required malfunctions to control the vehicle. Authors in [72], explained the firmware spoofing attack. FOTA is the new trend to send the firmware to update the flash memory of the ECU over the air by the original equipment manufacturer (OEM). The attackers create new firmware that can control the vehicle. Attacks on vehicle diagnostics are mentioned in Table 2.

Table 2. Possible attacks on the autonomous and connected vehicle.

Autonomous and Connected Vehicle Classification	Sub-Systems	Vulnerable Parts or Systems	Attacks
Safety systems	ASS	FMCW radar	Spoofing of radar [51]
		Wheel speed sensor of ABS	Disruptive attack and spoofing attack [52]
		TPMS	Eavesdropping attack [53]
		GPS	Location spoofing [54]
		Lidar	Replay attack [55], relay attack [18], blinding attack [56], DoS attack [50]
		Ultrasonic sensor	Blind spot exploitation attacks [57], sensor interference attacks [57]
		Camera	Blinding attack [18], phantom attack [75,76]
Connectivity	V2X	Communication channel	DoS attack [58,59], sybil attack [60], impersonation attack [60]
		Network or transport layer	Replay attack [16], data falsification attack [64,65], eavesdropping attacks [66]
		Routing protocols	Black hole attack [61], grey hole attack [62], wormhole attack [63]
	Smart features	Key less entry system	Password attack [67], keyless entry attacks [16], key fob attacks [16]
	In-vehicle	CAN bus	Frame sniffing attack [68], frame falsifying attack [11]
		Ethernet	CAM attack [69]
		LIN bus	False frame attack [70]
		FlexRay	Full and target DoS attack [71]
Diagnostics	OBD port	In-vehicle buses	In-vehicle access attack [72,73]
		CAN bus	frame sniffing [73]
			frame injection [73]
	FOTA	Firmware	Control override attacks [74]
			Spoofing attack [72]

6. Defenses or Countermeasures for Autonomous and Connected Vehicles

Attacks on automobiles are increasing rapidly. To ensure these attacks and to secure the automobile mechanisms are required. These defenses are described in Table 3.

6.1. Defenses for V2X

6.1.1. Symmetric and Asymmetric Encryption

Cryptography is used to transfer data into encrypted data for communication. This process is conducted with the help of keys and there are two types of cryptography techniques symmetric encryption and asymmetric encryption. In symmetric encryption, a single key is used for both encryption and decryption of the data as shown in Figure 6a. These are mostly used in point-to-point communication and used in situations where data is stored on the main server. This method is popular because easy to implement and secure [22]. There are different ways to approach this encryption, the two-factor lightweight privacy-preserving (2FLIP) algorithm works in two ways [76,77], pseudonymous authentication with conditional privacy (PACP) generates keys to authenticate the data [78], the elliptic-curve digital signature (ECDSA) algorithm works in three ways: key and signa-

ture generation and signature verification [79], secure and authenticated key-management protocol (SAKMP) [80].

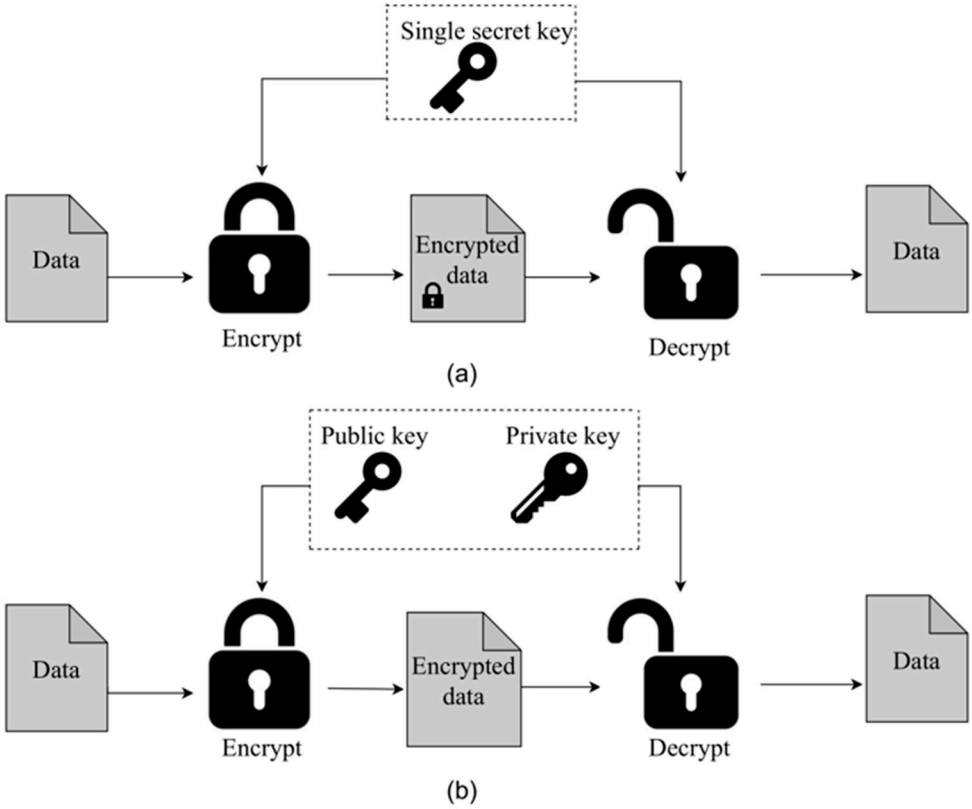


Figure 6. (**a**) Symmetric encryption (**b**) Asymmetric encryption.

In asymmetric encryption, two keys are used one is for encryption and another for the decryption of data as shown in Figure 6b. The asymmetric method is slower than the symmetric method because two keys are involved and more mathematical calculations are involved in this process. Different ways to achieve this are the pseudonym-based authentication method [81], privacy-preserving group communication scheme (PPGCV) [82], temporary anonymous certified keys (TACKs) [83], temporary authentication and revocation indicator (TARI) [84], and group signature and identity-based signature (GSIS) [85].

6.1.2. Intrusion Detection Systems (IDS)

Networks play an important role in a vehicle to keep connectivity and communication. The automobile includes wired and wireless networks which are targets of the attacker. IDS is a reliable method to secure networks. IDS is carried out by signature-based detection and anomaly-based detection [86,87].

In this approach signatures of the various attacks are stored in the database and retrieved to compare. If the comparison matches it detects the related attack shown in Figure 7a. In [88] this method is shown for vehicle movement data and it can detect a single fake vehicle and detect sybil attacks. In [89] a novel IDS was developed for detecting false messages in VANETs. It uses a dynamic engine to analyze and monitor the data. The detection rate of fake messages is very high with this method.

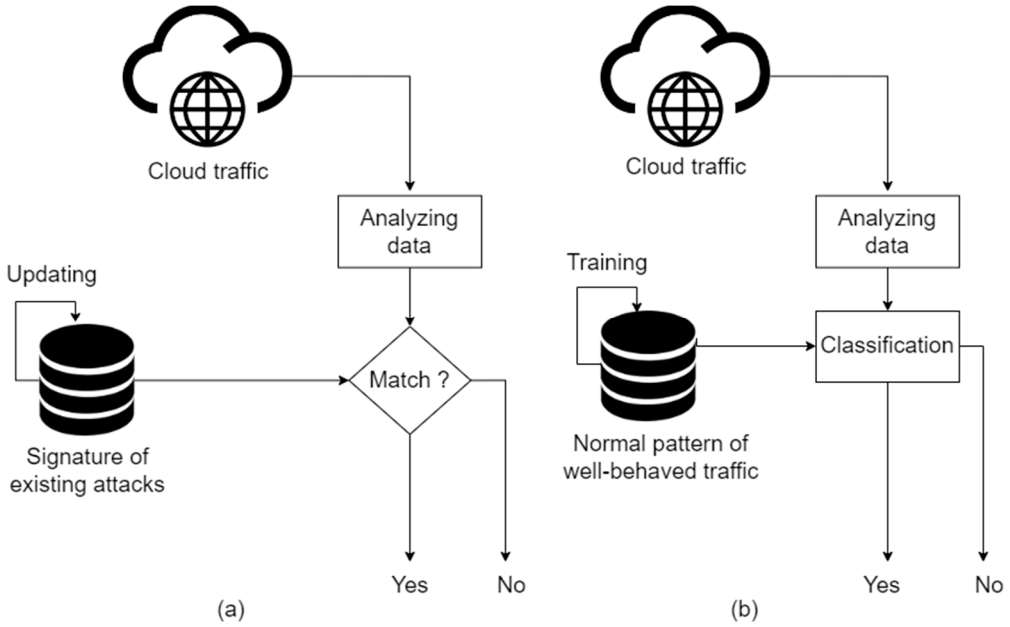


Figure 7. (**a**) Signature-based detection (**b**) Anomaly-based detection.

The signature-based approach has the drawback of detecting new attacks. The anomaly-based approach is designed to overcome it by predefining the baseline for normal cases. If a new type of attack appears it will detect the abnormal conditions with baseline as shown in Figure 7b. In [90] a presence evidence system (PES) was developed to detect the sybil attacks. This method considers the analysis of signal strength distribution to detect the vehicle location. If the vehicle's position is known, then it is easy to detect sybil attacks. In [91] an AECFV method was developed to detect blackhole, wormholes, and sybil attacks. This kind of IDS is carried out in three levels of cluster members and heads and roadside units with the help of a supervised machine learning algorithm. In [92] a domain-aware IDS method was developed to detect falsification information. This method used the ternary content addressable memories (TCAMs) approach for achieving anomaly IDS for the CAN bus to detect traffic on the CAN bus to find fake information.

6.1.3. Smart Features Defenses

In [93], cryptography is one of the mechanisms to overcome password and key attacks by increasing key size, better algorithms, and secure passwords. In the future, it might be easy to crack cryptography by using smart hacking methods; to prevent this, the authors mentioned another method to secure passwords and keys. Multi-factor authentication is the better approach, it provides multiple-layer security. Keyless entry and key fob attacks come close to vulnerabilities. To ensure this [16] suggested using strong cryptography algorithms with strong keys, passwords, and algorithms.

6.1.4. In-Vehicle Connectivity Defenses

In [68], a security protocol was proposed to secure the CAN bus using advanced encryption standard (AES) encryption with a 32-bit message authentication code (MAC). The first 16 bits are extended IDs, and the remaining 16 bits are cyclic redundancy check (CRC) bits to make the CAN frame more robust. In [94], a secure specification was proposed in ECU with a preloaded pattern to detect false frames of CAN and avoid false frames. In [95], the proposed gateway firewall is the best solution to secure LIN, CAN, and FlexRay. For secure communication, gateways need to develop firewalls. If the ECU is capable of generating digital signatures or MAC, then the firewall's purpose is to follow the authorization given in the certificates of the ECU. Only authorized ECU can communicate with the firewall. In [69], the proposed convolutional neural network (CNN) IDS is used to

avoid attacks on the Ethernet. This model is tested for audio and video packets carried by the Ethernet.

6.2. Defenses for Safety Systems

6.2.1. Countermeasures on Radar and GPS

In [96], the filter method is explained to avoid undesired digital radio frequency memory (DRFM) signals to prevent jamming and spoofing attacks created using DRFM repeaters. In [97], a novel spatiotemporal challenge response (STCR) method was used to detect the spoofing attacks made with multiple-input and multiple-output (MIMO) antennae and multiple beam forming. If reflected signals cross the threshold value of noise those are considered undesired signals. In [98], a signal encryption approach used analysis of drift, and direction of the upcoming signal to prevent GPS spoofing. In [67], two ways were provided to protect from GPS spoofing checking of GPS signals for threshold value if exceeds it leads to malfunction, and cryptography for GPS signal.

6.2.2. Countermeasures on TPMS and WSS

In [99], it was suggested to use TPMS when signal propagation is within limits. In [100], an anonymity encryption and certificate approach were proposed to secure the location from the usage data. In [101], physical challenge-response authentication (PyCRA) was used to protect WSS; this is based on inductive type sensors or magnetic encoders. This method deals to secure analog data before it is converted into digital data and follows the laws of physics. So, it is difficult for attackers to attack magnetic encoders.

6.2.3. Countermeasures on Lidar

Few studies proved that relay and replay attacks are related to spoofing and jamming attacks. If spoofing and jamming are controlled, it reduces the probability of relay and replay attacks. In [102], side-channel information was used to avoid spoofing that attack-injected messages are unknown to the side channel secret keys. In [18], it was suggested to vary the wavelengths of the lidar signals. It is difficult for the attacker to detect rapid changes in the wavelength. In [18], it was suggested that increasing the number of objects sensed by the lidar at a time prevents a DoS attack.

6.2.4. Countermeasures on Ultrasonic Sensors and Camera

In [102], a method to use a backup camera along with an ultrasonic sensor was proposed to detect thin objects to avoid physical attacks and relate the sensors while starting the vehicle to avoid tampering and sensor interference attacks. Algorithms suggested obtaining 360 degrees of sensor details that help in detecting blind spots. In [18], using inferred light filters or photochromic lenses was suggested. Inferred light filters are used to prevent inferred rays during the daytime. Photochromic lenses only allow a certain range of wavelengths. These methods can avoid the blinding camera. In [75], a model that can detect the spoofing of cameras with phantoms was designed. This model can detect phantoms 0.99 AUC.

6.3. Defenses for Diagnostics

In [47], a role-based access control (RBAC) was proposed with an end-to-end mechanism to secure the OBD port. This denies unauthored access that disturbs the vehicle functionality. This system is independent of automotive open system architecture (AUTOSAR) and is architecture-independent. In [103], it was suggested to follow a balanced approach to protecting the in-vehicle connectivity from OBD attacks. OEMs have to follow the granular access control policy and authentication schemes while giving access to the OBD ports in service centers. Then, only certified service centers have access to the OBD port. In [104], a secure protocol was proposed to secure FOTA. The protocol provides integrity, confidentiality, authentication, and freshness value to the data. Authenticators sign the packets and symmetric keys are used to encrypt the packets; this protocol requires

low memory. In [105], ECU self-verification was proposed to secure FOTA updates. A code is sent along with the firmware to the ECU. Then the ECU verifies the code to check integrity once verification is conducted then flashes the code.

Table 3. Defenses for attacks on autonomous and connected vehicles.

Autonomous and Connected Vehicle Classification	Sub-Systems	Defenses or Countermeasures
Safety systems	ASS	Filter method [96], STCR [97], PyCRA [101], anonymity encryption [100], signal encryption [98], side channel approach [102], increasing objects [18], camera integration [102], inferred light filters [18], photochromic lenses [18]
Connectivity	V2X	2FLIP [77], SAKMP [80], GSIS [85], novel IDS [89], TACKs [83], AECFV [91], PACP [78], domain aware IDS [92], ECDSA [79], PPGCV [82], TARI [84],
	Smart features	Multifactor authentication [93], cryptography [16]
	In-vehicle	AES encryption [68], domain aware IDS [92], CNN IDS [69], secure ECU [94], gateway firewall [95]
Diagnostics	OBD port	RBAC [47], balanced approach [103]
	FOTA	secure protocol [104], ECU self-verification [105]

7. Result of Analysis

Table 4 is the result of the review of possible attacks and defenses of autonomous and connected vehicles. Attacks on safety systems are due to vulnerabilities in sensors, and attacks on connectivity are because of vulnerabilities present in networks, and communication protocols. Attacks on diagnostics are due to low security at the OBD port and fewer security layers of the firmware. Implementing the available defenses and ensuring countermeasures increases the security level of the autonomous and connected vehicle.

Table 4. Result of the review.

Key Element Classification	Type of Division	Attacks	Defenses
Safety	ASS	Spoofing of radar [51]	Filter method [96], STCR [97]
		Disruptive attack and spoofing attack on WSS [52]	PyCRA [101]
		Eavesdropping attack on TPMS [53]	Anonymity encryption [100]
		GPS location spoofing [54]	Signal encryption [98]
		Lidar replay attack [55]	Side channel approach [102]
		Lidar relay attack [18]	
		Lidar blinding attack [56]	
		Lidar DoS attack [50]	Increasing objects [18]
		Blind spot exploitation attacks on ultrasonic sensor [57]	Camera integration [102], Algorithms
		Sensor interference attacks on ultrasonic sensor [57]	
		Blinding attack on camera [18]	Inferred light filters [18], photochromic lenses [18]
		Phantom attack on camera [75,76]	Model to avoid phantoms [75]

Table 4. *Cont.*

Key Element Classification	Type of Division	Attacks	Defenses
Connectivity	V2X	DoS attack [58,59]	2FLIP [77], SAKMP [80], GSIS [85]
		Impersonation attack [60]	SAKMP [80], novel IDS [89]
		Sybil attack [60]	TACKs [83], AECFV [91]
		Replay attack [16]	PACP [78], SAKMP [80]
		Black hole routing attack [61]	AECFV [91]
		Grey hole routing attack [62]	
		Wormhole routing attack [63]	
		Data falsification attack [64,65]	Domain aware IDS [92], novel IDS [89]
		Eavesdropping attacks [66]	PACP [78], Tacks [83]
	Smart features	Password attack [67]	Multifactor authentication [93]
		Key less entry attacks [16]	cryptography [16]
		Key fob attacks [16]	
	In-vehicle	CAN frame sniffing attack [68]	AES encryption [68]
		CAN frame falsifying attack [11]	AES encryption [68], Domain aware IDS [92]
		Ethernet CAM attack [69]	CNN IDS [69]
		LIN false frame attack [70]	Secure ECU [94] Domain aware IDS [92], Gateway firewall [95]
		FlexRay full DoS attack [71]	
		FlexRay targeted DoS attack [71]	
Diagnostics	OBD port	In-vehicle access attack [72,73]	RBAC [47], balanced approach [103]
		CAN frame sniffing [73]	
		CAN frame injection [73]	
	FOTA	Control override attacks [74]	secure protocol [104]
		firmware spoofing attack [72]	ECU self-verification [105]

8. Recommendations and Scope

An automobile is fully loaded with electronic devices to make it a modern vehicle. Electronics present in the vehicle are vulnerable for attackers to hack which may be sensors, controllers, networks, etc. This article helps us understand possible attacks on the systems designed for safety, and connectivity features such as V2X, smart features, in-vehicle communication buses, and diagnostics such as OBD ports and FOTA updates. Recommendations are to work on defenses for the attacks; the provided defense may have loopholes or small limits that may become an advantage to the attackers. If the defenses are stronger it will be difficult for an attacker to attack.

The future direction in this area is to take countermeasures for the sensors, work on secure onboard communication (SecOC) for protecting communication protocols, and the update framework (TUF) kind of FOTA for securely updating ECUs.

9. Conclusions

Vulnerabilities to attack an automobile are increasing due to the integration of electronics in the vehicle. A vehicle has become a daily need nowadays, electronics are integrated to develop smart systems to sense surrounding environments, assist drivers, increase user comfort, and avoid accidents. Electronics consists of vulnerabilities, so attackers focus on those vulnerabilities to attack the vehicle. This article provided numerous attacks on

autonomous and connected vehicles and countermeasures to overcome attacks. Primarily attack areas of the vehicle are classified into three regions safety systems, connectivity, and diagnostics. We collected all possible attacks in this classification and countermeasures are presented for the same. This analysis of attacks and defenses helps researchers and engineers to know about existing attacks and vulnerabilities. In addition to this, domain analysis is provided that helps researchers to select this domain, and recommendations and future directions are provided to pursue work in this area.

Author Contributions: B.R.M.; writing, data collection, analysis of the collected data. P.T.; supervision, corrections, tools for analysis. G.S.; guidance, corrections. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Informed consent was obtained from all individuals involved in this study.

Data Availability Statement: The collected for this research are available in the Scopus database.

Acknowledgments: The authors are thankful to Symbiosis International (Deemed University) and Verolt Engineering Pvt Ltd. for giving guidance for this study.

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

References

1. Patsakis, C.; Dellios, K.; Bouroche, M. Towards a distributed secure in-vehicle communication architecture for modern vehicles. *Comput. Secur.* **2014**, *40*, 60–74. [CrossRef]
2. Alam, M.S. Securing vehicle Electronic Control Unit (ECU) communications and stored data. Ph.D. Dissertation, Queen's University, Kingston, ON, Canada, 2018.
3. Abbasi, R.; Bashir, A.K.; Alyamani, H.J.; Amin, F.; Doh, J.; Chen, J. Lidar point cloud compression, processing and learning for au-tonomous driving. *IEEE Trans. Intell. Transp. Syst.* **2022**, *24*, 962–979. [CrossRef]
4. Abbasi, R.; Faseeh Qureshi, N.M.; Hassan, H.; Saba, T.; Rehman, A.; Luo, B.; Bashir, A.K. Generalized PVO-based dynamic block re-versible data hiding for secure transmission using firefly algorithm. *Trans. Emerg. Telecommun. Technol.* **2022**, *33*, e3680.
5. Maphathe, B.F.; Thakur, P.; Singh, G.; Iddi, H.E. The Terahertz Channel Modeling in Internet of Multimedia Design In-Body Antenna. *Int. J. E-Health Med. Commun.* **2022**, *13*, 1–17. [CrossRef]
6. Hao, J.; Han, G. On the Modeling of Automotive Security: A Survey of Methods and Perspectives. *Future Internet* **2020**, *12*, 198. [CrossRef]
7. Thakur, P.; Singh, G. Security and interference management in the cognitive-inspired Internet of Medical Things. In *Intelligent Data Security Solutions for e-Health Applications*; Academic Press: Cambridge, MA, USA, 2020; pp. 131–149. [CrossRef]
8. Juliussen, E. The future of automotive telematics. In *Business Briefing: Global Automotive Manufacturing & Technology*; Business Briefings Ltd.: London, UK, 2003; pp. 1–4.
9. Mudhivarthi, B.R.; Thakur, P. Integration of artificial intelligence in robotic vehicles: A bibliometric analysis. *Paladyn, J. Behav. Robot.* **2022**, *13*, 110–120. [CrossRef]
10. Rizvi, S.; Willet, J.; Perino, D.; Marasco, S.; Condo, C. A Threat to Vehicular Cyber Security and the Urgency for Correction. *Procedia Comput. Sci.* **2017**, *114*, 100–105. [CrossRef]
11. Koscher, K.; Czeskis, A.; Roesner, F.; Patel, S.; Kohno, T.; Checkoway, S.; McCoy, D.; Kantor, B.; Anderson, D.; Shacham, H.; et al. Experimental security analysis of a modern automobile. In Proceedings of the 2010 IEEE Symposium on Security and Privacy, Oakland, CA, USA, 16–19 May 2010; pp. 447–462.
12. Miller, C.; Valasek, C. Remote exploitation of an unaltered passenger vehicle. *Black Hat USA* **2015**, *91*, 1–91.
13. Nie, S.; Liu, L.; Du, Y. Free-fall: Hacking tesla from wireless to can bus. *Brief. Black Hat USA* **2017**, *25*, 1–6.
14. Khatri, N.; Shrestha, R.; Nam, S. Security Issues with In-Vehicle Networks, and Enhanced Countermeasures Based on Blockchain. *Electronics* **2021**, *10*, 893. [CrossRef]
15. Aliwa, E.; Rana, O.; Perera, C.; Burnap, P. Cyberattacks and Countermeasures for In-Vehicle Networks. *ACM Comput. Surv.* **2021**, *54*, 1–37. [CrossRef]
16. Sun, X.; Yu, F.R.; Zhang, P. A Survey on Cyber-Security of Connected and Autonomous Vehicles (CAVs). *IEEE Trans. Intell. Transp. Syst.* **2021**, *23*, 6240–6259. [CrossRef]
17. Liu, J.; Zhang, S.; Sun, W.; Shi, Y. In-Vehicle Network Attacks and Countermeasures: Challenges and Future Directions. *IEEE Netw.* **2017**, *31*, 50–58. [CrossRef]

18. El-Rewini, Z.; Sadatsharan, K.; Sugunaraj, N.; Selvaraj, D.F.; Plathottam, S.J.; Ranganathan, P. Cybersecurity Attacks in Vehicular Sensors. *IEEE Sens. J.* **2020**, *20*, 13752–13767. [CrossRef]
19. Kumar, A.D.; Chebrolu, K.N.; KP, S. A brief survey on autonomous vehicle possible attacks, exploits and vulnerabilities. *arXiv* **2018**, arXiv:1810.04144.
20. Dibaei, M.; Zheng, X.; Jiang, K.; Maric, S.; Abbas, R.; Liu, S.; Zhang, Y.; Deng, Y.; Wen, S.; Zhang, J.; et al. An overview of attacks and defences on intelligent connected vehicles. *arXiv* **2019**, arXiv:1907.07455.
21. Luo, F.; Jiang, Y.; Zhang, Z.; Ren, Y.; Hou, S. Threat Analysis and Risk Assessment for Connected Vehicles: A Survey. *Secur. Commun. Netw.* **2021**, *2021*, 1263820. [CrossRef]
22. Dibaei, M.; Zheng, X.; Jiang, K.; Abbas, R.; Liu, S.; Zhang, Y.; Xiang, Y.; Yu, S. Attacks and defences on intelligent connected vehicles: A survey. *Digit. Commun. Netw.* **2020**, *6*, 399–421. [CrossRef]
23. Al-Sabaawi, A.; Al-Dulaimi, K.; Foo, E.; Alazab, M. Addressing Malware Attacks on Connected and Autonomous Vehicles: Recent Techniques and Challenges. In *Malware Analysis Using Artificial Intelligence and Deep Learning*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 97–119. [CrossRef]
24. Cui, J.; Liew, L.S.; Sabaliauskaite, G.; Zhou, F. A review on safety failures, security attacks, and available countermeasures for autonomous vehicles. *Ad Hoc Netw.* **2018**, *90*, 101823. [CrossRef]
25. Hamdane, H.; Serre, T.; Masson, C.; Anderson, R. Issues and challenges for pedestrian active safety systems based on real world accidents. *Accid. Anal. Prev.* **2015**, *82*, 53–60. Available online: https://www.sciencedirect.com/science/article/pii/S0001457515001979 (accessed on 17 December 2021). [CrossRef]
26. Rödel, C.; Stadler, S.; Meschtscherjakov, A.; Tscheligi, M. Towards autonomous cars: The effect of autonomy levels on acceptance and user experience. In Proceedings of the 6th International Conference on Automotive User Interfaces and Interactive Vehicular Applications, Seattle, WA, USA, 17–19 September 2014; pp. 1–8.
27. Kaur, G.; Kumar, D. Lane detection techniques: A review. *Int. J. Comput. Appl.* **2015**, *112*, 4–8.
28. Bhasin, K. A Review Paper on Anti-Lock Braking System (ABS) and its Future Scope. *Int. J. Res. Appl. Sci. Eng. Technol.* **2019**, *7*, 372–375. [CrossRef]
29. Vahidi, A.; Eskandarian, A. Research advances in intelligent collision avoidance and adaptive cruise control. *IEEE Trans. Intell. Transp. Syst.* **2003**, *4*, 143–153. [CrossRef]
30. Udugu, K.; Saddala, V.R.; Lingan, S. Active and Passive Safety: An Overview on Establishing Safety Assessment Standards in India. *SAE Tech. Pap.* **2016**, *1*. [CrossRef]
31. Singh, G.; Thakur, P. *Spectrum Sharing in Cognitive Radio Networks: Towards Highly Connected Environments*; John Wiley & Sons:: Hoboken, NJ, USA, 2021.
32. Perales, M.A.; Kebriaei, P.; Kean, L.S.; Sadelain, M. Building a safer and faster CAR: Seatbelts, airbags, and CRISPR. *Biol. Blood Marrow Transplant.* **2018**, *24*, 27–31. [CrossRef] [PubMed]
33. Wang, J.; Shao, Y.; Ge, Y.; Yu, R. A Survey of Vehicle to Everything (V2X) Testing. *Sensors* **2019**, *19*, 334. [CrossRef]
34. Mishra, P.; Thakur, P.; Singh, G. Sustainable Smart City to Society 5.0: State-of-the-Art and Research Challenges. *SAIEE Afr. Res. J.* **2022**, *113*, 152–164. [CrossRef]
35. Nguyen, T.; Lechner, B.; Wong, Y.D. Response-based methods to measure road surface irregularity: A state-of-the-art review. *Eur. Transp. Res. Rev.* **2019**, *11*, 1–18. [CrossRef]
36. Ali, I.; Li, F. An efficient conditional privacy-preserving authentication scheme for Vehicle-To-Infrastructure communication in VANETs. *Veh. Commun.* **2019**, *22*, 100228. [CrossRef]
37. Ameen, H.A.; Mahamad, A.K.; Saon, S.; Nor, D.M.; Ghazi, K. A review on vehicle to vehicle communication system applications. *Indones. J. Electr. Eng. Comput. Sci.* **2020**, *18*, 188–198. [CrossRef]
38. Sheikh, M.S.; Liang, J.; Wang, W. Security and Privacy in Vehicular Ad Hoc Network and Vehicle Cloud Computing: A Survey. *Wirel. Commun. Mob. Comput.* **2020**, *2020*, 1–25. [CrossRef]
39. Tong, W.; Hussain, A.; Bo, W.X.; Maharjan, S. Artificial Intelligence for Vehicle-to-Everything: A Survey. *IEEE Access* **2019**, *7*, 10823–10843. [CrossRef]
40. Kassabalidis, I.; El-Sharkawi, M.; Marks, R.; Arabshahi, P.; Gray, A. Swarm intelligence for routing in communication networks. *IEEE Glob. Telecommun. Conf.* **2002**, *6*, 3613–3617. [CrossRef]
41. Swarnkar, R.; Harikrishnan, R.; Thakur, P.; Singh, G. Electric Vehicle Lithium-ion Battery Ageing Analysis Under Dynamic Con-dition: A Machine Learning Approach. *SAIEE Afr. Res. J.* **2022**, *114*, 4–13. [CrossRef]
42. Wang, S.-S. A BLE-Based Pedestrian Navigation System for Car Searching in Indoor Parking Garages. *Sensors* **2018**, *18*, 1442. [CrossRef]
43. Jadhav, S.; Kshirsagar, D. A survey on security in automotive networks. In Proceedings of the 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), Pune, India, 16–18 August 2018; pp. 1–6.
44. Ngene, C.E.; Thakur, P.; Singh, G. Free-space optical link optimization in visible light communication system. *J. Opt. Commun.* **2021**. [CrossRef]
45. Inambao, F.; Cunden, K. Offshore wind resource assessment off the South African coastline. *Int. J. Me-Chanical Eng. Technol.* **2019**, *10*, 95–119.
46. Rimpas, D.; Papadakis, A.; Samarakou, M. OBD-II sensor diagnostics for monitoring vehicle operation and consumption. *Energy Rep.* **2019**, *6*, 55–63. [CrossRef]

47. Ammar, M.; Janjua, H.; Thangarajan, A.S.; Crispo, B.; Hughes, D. Securing the on-board diagnostics port (obd-ii) in vehicles. *SAE Int. J. Transp. Cybersecur. Priv.* **2020**, *2*, 83–106. [CrossRef]
48. John, A.A.; Thakur, P.; Singh, G. Potential, concepts, and key advances for a ubiquitous adaptive indigenous microengineering and nanoengineering in 6G network. *Int. J. Commun. Syst.* **2022**. [CrossRef]
49. La Manna, M.; Treccozzi, L.; Perazzo, P.; Saponara, S.; Dini, G. Performance evaluation of attribute-based encryption in automotive embedded platform for secure software over-the-air update. *Sensors* **2021**, *21*, 515. [CrossRef] [PubMed]
50. Salfer, M.; Eckert, C. Attack surface and vulnerability assessment of automotive electronic control units. In Proceedings of the 2015 12th International Joint Conference on e-Business and Telecommunications (ICETE), Colmar, France, 20–22 July 2015; Volume 4, pp. 317–326.
51. Komissarov, R.; Wool, A. Spoofing attacks against vehicular FMCW radar. In Proceedings of the 5th Workshop on Attacks and Solutions in Hardware Security, Seoul, Republic of Korea, 19 November 2021; pp. 91–97.
52. Shoukry, Y.; Martin, P.; Tabuada, P.; Srivastava, M. Non-invasive spoofing attacks for anti-lock braking systems. In Proceedings of the Cryptographic Hardware and Embedded Systems-CHES 2013: 15th International Workshop, Santa Barbara, CA, USA, 20–23 August 2013; Springer: Berlin/Heidelberg, Germany, 2013; pp. 55–72.
53. Rouf, I.; Miller, R.D.; Mustafa, H.A.; Taylor, T.; Oh, S.; Xu, W.; Gruteser, M.; Trappe, W.; Seskar, I. Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study. In Proceedings of the USENIX Security Symposium, San Jose, CA, USA, 11–13 August 2010; Volume 10.
54. Lim, K.; Tuladhar, K.M.; Kim, H. Detecting location spoofing using ADAS sensors in VANETs. In Proceedings of the 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 11 January 2019; pp. 1–4.
55. Stottelaar, B.G. Practical Cyber-Attacks on Autonomous Vehicles. Master's Thesis, University of Twente, Enschede, The Netherlands, 2015.
56. Shin, H.; Kim, D.; Kwon, Y.; Kim, Y. Illusion and dazzle: Adversarial optical channel exploits against lidars for automotive ap-plications. In Proceedings of the Cryptographic Hardware and Embedded Systems–CHES 2017: 19th International Conference, Taipei, Taiwan, 25–28 September 2017; pp. 445–467.
57. Lim, B.S.; Keoh, S.L.; Thing, V.L. Autonomous vehicle ultrasonic sensor vulnerability and impact assessment. In Proceedings of the 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), Singapore, 5–8 February 2018; pp. 231–236.
58. Kumar, S.; Mann, K.S. Prevention of DoS Attacks by Detection of Multiple Malicious Nodes in VANETs. In Proceedings of the 2019 International Conference on Automation, Computational and Technology Management, London, UK, 24–26 April 2019; pp. 89–94. [CrossRef]
59. He, Q.; Meng, X.; Qu, R. Survey on cyber security of CAV. In Proceedings of the 2017 Forum on Cooperative Positioning and Service (CPGPS), Harbin, China, 19–21 May 2017; pp. 351–354.
60. Appathurai, A.; Manogaran, G.; Chilamkurti, N. Trusted FPGA-based transport traffic inject, impersonate (I2) attacks beaconing in the Internet of Vehicles. *IET Netw.* **2019**, *8*, 169–178. [CrossRef]
61. Albouq, S.S.; Fredericks, E.M. Lightweight detection and isolation of black hole attacks in connected vehicles. In Proceedings of the 2017 IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW), Atlanta, GA, USA, 5–8 June 2017; pp. 97–104.
62. Purohit, K.C.; Dimri, S.C.; Jasola, S. Mitigation and Performance Analysis of Routing Protocols Under Black-Hole Attack in Vehicular Ad-hoc Network (VANET). *Wirel. Pers. Commun.* **2017**, *97*, 5099–5114. [CrossRef]
63. Kumar, P.; Verma, S. Detection of wormhole attack in VANET. *Natl. J. Syst. Inf. Technol.* **2017**, *10*, 71.
64. Shukla, R.M.; Sengupta, S. Analysis and detection of outliers due to data falsification attacks in vehicular traffic prediction ap-plication. In Proceedings of the 2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York City, NY, USA, 8–10 November 2018; pp. 688–694.
65. Lin, J.; Yu, W.; Zhang, N.; Yang, X.; Ge, L. Data Integrity Attacks Against Dynamic Route Guidance in Transportation-Based Cyber-Physical Systems: Modeling, Analysis, and Defense. *IEEE Trans. Veh. Technol.* **2018**, *67*, 8738–8753. [CrossRef]
66. Balakrishnan, S.; Wang, P.; Bhuyan, A.; Sun, Z. Modeling and Analysis of Eavesdropping Attack in 802.11ad mmWave Wireless Networks. *IEEE Access* **2019**, *7*, 70355–70370. [CrossRef]
67. Parkinson, S.; Ward, P.; Wilson, K.; Miller, J. Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges. *IEEE Trans. Intell. Transp. Syst.* **2017**, *18*, 2898–2915. [CrossRef]
68. Woo, S.; Jo, H.J.; Lee, D.H. A Practical Wireless Attack on the Connected Car and Security Protocol for In-Vehicle CAN. *IEEE Trans. Intell. Transp. Syst.* **2014**, *16*, 1–14. [CrossRef]
69. Jeong, S.; Jeon, B.; Chung, B.; Kim, H.K. Convolutional neural network-based intrusion detection system for AVTP streams in au-tomotive Ethernet-based networks. *Veh. Commun.* **2021**, *29*, 100338.
70. Takahashi, J.; Aragane, Y.; Miyazawa, T.; Fuji, H.; Yamashita, H.; Hayakawa, K.; Ukai, S.; Hayakawa, H. Automotive Attacks and Countermeasures on LIN-Bus. *J. Inf. Process.* **2017**, *25*, 220–228. [CrossRef]
71. Murvay, P.-S.; Groza, B. Practical Security Exploits of the FlexRay In-Vehicle Communication Protocol. In *Risks and Security of Internet and Systems: 13th International Conference, CRiSIS 2018, Arcachon, France, 16–18 October 2018*; Revised Selected Papers 13; Springer International Publishing: Berlin/Heidelberg, Germany, 2019; pp. 172–187. [CrossRef]

72. Carsten, P.; Andel, T.R.; Yampolskiy, M.; McDonald, J.T. In-vehicle networks: Attacks, vulnerabilities, and proposed solutions. In Proceedings of the 10th Annual Cyber and Information Security Research Conference, Oak Ridge, TN, USA, 7–9 April 2015; pp. 1–8.
73. Miller, C.; Valasek, C. Adventures in automotive networks and control units. *Def Con.* **2013**, *21*, 15–31.
74. Philipsen, S.G.; Andersen, B.; Singh, B. Threats and attacks to modern vehicles. In Proceedings of the 2021 IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS), Bandung, Indonesia, 23–24 November 2021; pp. 22–27.
75. Hodge, C.; Hauck, K.; Gupta, S.; Bennett, J.C. *Vehicle Cybersecurity Threats and Mitigation Approaches*; National Renewable Energy Lab.(NREL): Golden, CO, USA, 2019. [CrossRef]
76. Schaffer, T.; Glaser, A.; Rao, S.; Franzon, P. A flip-chip implementation of the Data Encryption Standard (DES). In Proceedings of the 1997 IEEE Multi-Chip Module Conference, Santa Cruz, CA, USA, 4-5 February 1997; pp. 13–17.
77. Wang, F.; Xu, Y.; Zhang, H.; Zhang, Y.; Zhu, L. 2FLIP: A Two-Factor Lightweight Privacy-Preserving Authentication Scheme for VANET. *IEEE Trans. Veh. Technol.* **2015**, *65*, 896–911. [CrossRef]
78. Huang, D.; Misra, S.; Verma, M.; Xue, G. PACP: An Efficient Pseudonymous Authentication-Based Conditional Privacy Protocol for VANETs. *IEEE Trans. Intell. Transp. Syst.* **2011**, *12*, 736–746. [CrossRef]
79. Knezevic, M.; Nikov, V.; Rombouts, P. Low-Latency ECDSA Signature Verification—A Road Toward Safer Traffic. *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.* **2016**, *24*, 3257–3267. [CrossRef]
80. Tan, H.; Ma, M.; Labiod, H.; Boudguiga, A.; Zhang, J.; Chong, P.H.J. A Secure and Authenticated Key Management Protocol (SA-KMP) for Vehicular Networks. *IEEE Trans. Veh. Technol.* **2016**, *65*, 9570–9584. [CrossRef]
81. Calandriello, G.; Papadimitratos, P.; Hubaux, J.P.; Lioy, A. Efficient and robust pseudonymous authentication in VANET. In Proceedings of the Fourth ACM International Workshop on Vehicular ad Hoc Networks, Montréal, QC, Canada, 10 September 2007; pp. 19–28.
82. Wasef, A.; Shen, X. PPGCV: Privacy Preserving Group Communications Protocol for Vehicular Ad Hoc Networks. In Proceedings of the 2008 IEEE International Conference on Communications, Beijing, China, 19–23 May 2008; pp. 1458–1463. [CrossRef]
83. Studer, A.; Shi, E.; Bai, F.; Perrig, A. TACKing together efficient authentication, revocation, and privacy in VANETs. In Proceedings of the 2009 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, Rome, Italy, 22–26 June 2009; pp. 1–9.
84. Chen, R.; Ma, D.; Regan, A. TARI: Meeting delay requirements in VANETs with efficient authentication and revocation. In Proceedings of the 2nd International Conference on Wireless Access in Vehicular Environments (WAVE), Shanghai, China, 21–22 December 2009.
85. Manvi, S.S.; Tangade, S. A survey on authentication schemes in VANETs for secured communication. *Veh. Commun.* **2017**, *9*, 19–30. [CrossRef]
86. Zaidi, K.; Milojevic, M.B.; Rakocevic, V.; Nallanathan, A.; Rajarajan, M. Host-Based Intrusion Detection for VANETs: A Statistical Approach to Rogue Node Detection. *IEEE Trans. Veh. Technol.* **2015**, *65*, 6703–6714. [CrossRef]
87. Dhaliwal, S.S.; Nahid, A.-A.; Abbas, R. Effective Intrusion Detection System Using XGBoost. *Information* **2018**, *9*, 149. [CrossRef]
88. Bissmeyer, N.; Stresing, C.; Bayarou, K.M. Intrusion detection in VANETs through verification of vehicle movement data. In Proceedings of the 2010 IEEE Vehicular Networking Conference, Jersey City, NJ, USA, 13–15 December 2010; pp. 166–173. [CrossRef]
89. Tomandl, A.; Fuchs, K.P.; Federrath, H. REST-Net: A dynamic rule-based IDS for VANETs. In Proceedings of the 2014 7th IFIP Wireless and Mobile Networking Conference (WMNC), Vilamoura, Portugal, 20–22 May 2014; pp. 1–8.
90. Yu, B.; Xu, C.Z.; Xiao, B. Detecting sybil attacks in VANETs. *J. Parallel Distrib. Comput.* **2013**, *73*, 746–756. [CrossRef]
91. Sedjelmaci, H.; Senouci, S.M. An accurate and efficient collaborative intrusion detection framework to secure vehicular networks. *Comput. Electr. Eng.* **2015**, *43*, 33–47. [CrossRef]
92. Markovitz, M.; Wool, A. Field classification, modeling and anomaly detection in unknown CAN bus networks. *Veh. Commun.* **2017**, *9*, 43–52. [CrossRef]
93. Khankari, N.B.; Kale, G.V. One time password generation for multifactor authentication using graphical password. *Int. J. Eng. Res. Gen. Sci.* **2020**, *3*, 489–494.
94. Larson, U.E.; Nilsson, D.K.; Jonsson, E. An approach to specification-based attack detection for in-vehicle networks. In Proceedings of the 2008 IEEE Intelligent Vehicles Symposium, Eindhoven, The Netherlands, 4–6 June 2008; pp. 220–225. [CrossRef]
95. Wolf, M.; Weimerskirch, A.; Paar, C. Security in automotive bus systems. In Proceedings of the Workshop on Embedded Security in Cars, Bochum, Germany, 10–11 November 2004; pp. 1–13.
96. Lu, G.; Zeng, D.; Tang, B. Anti-jamming filtering for DRFM repeat jammer based on stretch processing. In Proceedings of the 2010 2nd International Conference on Signal Processing Systems, Dalian, China, 5–7 July 2010; Volume 1, pp. V1–V78.
97. Kapoor, P.; Vora, A.; Kang, K.D. Detecting and mitigating spoofing attack against an automotive radar. In Proceedings of the 2018 IEEE 88th Ve-hicular Technology Conference (VTC-Fall), Chicago, IL, USA, 27–30 August 2018; pp. 1–6.
98. Psiaki, M.L.; Humphreys, T.E. GNSS spoofing and detection. *Proc. IEEE* **2016**, *104*, 1258–1270. [CrossRef]
99. Kolodgie, A.; Berges, P.; Burrow, R.; Carman, M.; Collins, J.; Bair, S.; Moy, G.D.; Ernst, J.M.; Michaels, A.J. Enhanced TPMS security through acceleration timed transmissions. In Proceedings of the MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM), Baltimore, MD, USA, 23–25 October 2017; pp. 35–39.

100. Amoozadeh, M.; Raghuramu, A.; Chuah, C.-N.; Ghosal, D.; Zhang, H.M.; Rowe, J.; Levitt, K. Security vulnerabilities of connected vehicle streams and their impact on cooperative driving. *IEEE Commun. Mag.* **2015**, *53*, 126–132. [CrossRef]
101. Shoukry, Y.; Martin, P.; Yona, Y.; Diggavi, S.; Srivastava, M. Pycra: Physical challenge-response authentication for active sensors under spoofing attacks. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver, CO, USA, 12–16 October 2015; pp. 1004–1015.
102. Matsumura, R.; Sugawara, T.; Sakiyama, K. A secure LiDAR with AES-based side-channel fingerprinting. In Proceedings of the 2018 Sixth International Symposium on Computing and Networking Workshops (CANDARW), Takayama, Japan, 27–30 November 2018; pp. 479–482.
103. Markham, T.R.; Chernoguzov, A. A balanced approach for securing the OBD-II port. *SAE Int. J. Passeng. Cars-Electron. Electr. Syst.* **2017**, *10*, 390–399. [CrossRef]
104. Nilsson, D.K.; Larson, U.E. Secure firmware updates over the air in intelligent vehicles. In Proceedings of the ICC Workshops-2008 IEEE Interna-tional Conference on Communications Workshops, Beijing, China, 19–23 May 2008; pp. 380–384.
105. Nilsson, D.K.; Sun, L.; Nakajima, T. A Framework for Self-Verification of Firmware Updates over the Air in Vehicle ECUs. In Proceedings of the 2008 IEEE Globecom Workshops, New Orleans, LA, USA, 30 November–4 December 2008; pp. 1–5.