sustainability

Review

An Overview of Vehicular Cybersecurity for Intelligent Connected Vehicles

Tian Guan, Yi Han *, Nan Kang, Ningye Tang, Xu Chen and Shu Wang

School of Automobile, Chang'an University, Xi'an 710064, China; 2021022003@chd.edu.cn (T.G.); 2021022008@chd.edu.cn (N.K.); 2020222023@chd.edu.cn (N.T.); 2020222061@chd.edu.cn (X.C.); wangshukayle@163.com (S.W.)

* Correspondence: hany@chd.edu.cn; Tel.: +86-132-2805-5890

Abstract: Cybersecurity is one of the most important challenges in the intelligent connected vehicle system. Interconnected vehicles are vulnerable to different network security attacks, which endanger the safety of passengers. This review paper firstly analyses the reasons why the current vehicle network is vulnerable to network attack and summarizes the three implementation methods of network security threats. The necessity of vehicle network security research and deployment is also analyzed. After giving a short introduction to the vehicular network security, this review paper identifies major security attacks on intelligent connected vehicles. Then the security enhancement technology of vehicle networks from three aspects are introduced, including vehicle network data encryption technology, vehicle network message authentication technology, and vehicle network anomaly intrusion detection technology. Then we analyze three common methods of abnormal intrusion detection in vehicle networks and explore the future research for preventing attacks on the network security of intelligent vehicle systems.

Keywords: vehicular network; intelligent connected vehicle; cyber security

Citation: Guan, T.; Han, Y.; Kang, N.; Tang, N.; Chen, X.; Wang, S. An Overview of Vehicular Cybersecurity for Intelligent Connected Vehicles. *Sustainability* **2022**, *14*, 5211. https://doi.org/10.3390/su14095211

Academic Editors: G G Md Nawaz Ali, Xuejun Li, Md. Noor-A-Rahim and Mohammad Omar Khyam

Received: 29 March 2022
Accepted: 23 April 2022
Published: 26 April 2022

1. Introduction

The intelligent connected vehicle (ICV) is becoming the mainstream of the automotive industry in the future. The advanced wireless technology enables vehicles to share and communicate information with each other and their surroundings in real-time, which will help to reduce crashes, congestion, and greenhouse gas emissions. Many advanced technologies, such as cloud computing, artificial intelligence, V2X (vehicle to everything) communication, and advanced driver assistance systems are being more and more widely used in cars, which makes connected vehicles more intelligent to provide comfortable services for people and ensure the safety of drivers and passengers. However, as our cars become more connected (to the Internet, to wireless networks, with each other, and with our infrastructure), the risk of cyber-attacks is a growing concern.

The complexity of the system and the increase of external communication interfaces make the connected cars more vulnerable to network attacks. In recent years, the continuous automobile information security recall events have attracted great attention. In view of the key attributes of ACPs (automotive cyber-physical systems) function security, the attack on the vehicle network will not only cause personal privacy disclosure and economic loss but also endanger people's life safety and even become a national public security problem. The U.S. Department of Transportation (USDOT) [1] understands the threat to the nation's cyberinfrastructure and has made cybersecurity a top priority. The Department is taking action to respond to the threat and improve the vehicle cybersecurity posture and capabilities of the United States. In 2015, 1.4 million vehicles were the subject of a recall by Chrysler because hackers could remotely take control of a jeep's digital system over the internet [2]. The hackers could disable the car's brakes at low speeds. By sending carefully crafted messages on the vehicle's internal network known as a CAN bus, hackers could pull off even more dangerous, unprecedented tricks like causing unintended acceleration and slamming on the car's brakes or turning the vehicle's steering wheel at any speed. In another report, a team of hackers remotely hijacked a Tesla Model S from a distance of 12 miles. By hijacking the car's CAN bus, the hackers could move the seats back and forth, trigger the indicators, wing mirrors, and windscreen wipers, and open the sunroof and boot while the car was driving and in parking mode. More worryingly, the hackers could also control the car's brakes, which could be dangerous if deployed suddenly while the vehicle was traveling at high speed on a motorway [3]. In a recent study, researchers have found 14 vulnerabilities in the infotainment system in several BMW series [4]. If the Telematics Control Unit has fallen into a rogue base station, attackers can extend the attack distance to a wide-range with the help of some amplifier devices. Technically speaking, it's possible to launch the attack from hundreds of meters even when the car is in the driving mode. Overall, these cases support the view that security in intelligent vehicular systems becomes essential and must be addressed in order to protect the vehicle and driver. Therefore, the number of intrusion attacks targeting the security loopholes of the Internet of Vehicles and smart cars has gradually increased in new crimes. From the perspective of network security, the intelligent networking of automobiles is a double-edged sword. If the vehicle is hacked, hackers can engage in a variety of illegal activities or make money from it, such as taking control of the vehicle, stealing the personal information of the vehicle and its owner, and hacking the vehicle and then the external system of the Internet of Vehicles.

Like connected mobile phones and computers, smart cars are subject to network security threats such as computer viruses, malicious programs, hacking, and data leakage. Compared with hardware cracking, remote non-contact attacks are more threatening to smart cars, which are mainly manifested in four aspects: (1) Potential security risks on the mobile terminal. There is a risk of it being stolen and controlled in terms of vehicle information; (2) Hidden dangers of communication security, that is, there is a risk of cracking and theft of information transmission between people, vehicles, roads, and clouds on the Internet of Vehicles; (3) Hidden dangers of in-vehicle terminal security, namely the security loopholes in the bus control and information transmission of the smart car itself may be exploited by hackers; (4) Cloud security risks, that is, there may be security loopholes on the Internet of Vehicles' cloud server, causing hackers to send malicious files through the cloud.

Currently, successful cyber security attacks on vehicles are mainly due to shared information and wireless communication, thus increasing the sensitivity of vehicles to different malicious attacks. Faced with the threat of information security, the existing vehicular network protocols lack information security considerations at the beginning of the design, so it is urgent to strengthen information security. The major motivation that led us to carry out this work is the ever-expanding gap between security attacks and existing safety measures.

This paper first summarizes the challenges and constraints of vehicle network information security design under functional security assurance and the main security attacks on intelligent connected vehicles and makes a comprehensive review of the existing defense measures and solutions. Then it summarizes three common methods of anomaly intrusion detection in the vehicle network. Finally, it summarizes three new technologies to solve the network security problems of intelligent network automobiles, which provides a new technical direction for solving the related problems of intelligent network automobiles.

2. Analysis of Vehicular Network Security

2.1. Severe Security Threats

In order to deploy the vehicles safely and successfully, the security threats must be mitigated whenever possible. As the current standard protocol of vehicle networks, the CAN bus lacks an encryption mechanism and protection mechanism at the beginning of its design. All nodes receive their own message ID and obtain data on the bus without involving any information at the sending end, and the receiving end will not judge whether the source message is invasive. In addition, the increase or decrease of nodes in the CAN bus is arbitrary. People can only access the bus through the physical layer and can normally send and receive messages on the bus without verifying the newly accessed nodes. With the popularization of automotive intelligence, the proportion of in-car electronic control equipment is increasing. Advanced electronic equipment data and vehicle data have also become the cutting-edge evaluation standards of the automotive industry and are also the core factors to attract consumers and improve product competitiveness. Advanced electronic equipment data have also become the cutting-edge evaluation standards of the automotive industry and are also the core factors to attract consumers and improve product competitiveness. If the enhancement technologies of vehicle network security are not carried out in time, it will suffer malicious attacks in all aspects due to potential security vulnerabilities [5]. Table 1 shows the analysis and comparison of automobile network supply in the recent 10 years. In terms of attack methods, the security threats in recent years can be divided into three implementation methods: direct physical access attack, short-range wireless attack, and long-range wireless attack. Direct physical access attack is mainly carried out by illegally accessing CAN and OBD interfaces; short-range wireless attacks are mainly carried out through illegal access to Bluetooth and wireless sensor channels; remote wireless attacks are mainly carried out through illegal access to WiFi and mobile digital cellular network ports.

Table 1. Analysis and comparison of network attacks against vehicles in the recent 10 years.

Attack Mode	Document	Attack Entrance	Attack Model	CIA Threat
Direct physics	Document [6]	CAN illegal access OBD port	Frame sniffing, message playback, etc.	Integrity and confidentiality
	Document [7,8]	OBD port	Frame sniffing, message playback, and camouflage, DOS attack, etc.	Integrity, confidentiality usability
A little distance Wireless attack	Document [9]	Bluetooth	Frame sniffing, message playback, and camouflage	Integrity and confidentiality
	Document [10]	TMPS, tire pressure monitoring system	Sniffing, message replay, and camouflage	Integrity and confidentiality
Integrity and confidentiality	Document [11–13]	Remote wireless/Wi-Fi, etc.	Message replay and camouflage, etc.	Integrity and confidentiality

2.2. *Vehicle Network Lacking Information Security*

The existing vehicle network protocols, such as CAN and FlexRay, lack the design of an information security mechanism at the beginning of its design, which makes the vehicle network vulnerable to sniffing, forgery, modification, and replay. Its vulnerability is mainly reflected in the following three aspects.

(1) Point to line communication has poor confidentiality. The message in the CAN bus is transmitted by broadcast. All nodes can accept the message transmitted by the bus, which makes it possible to monitor the message information. The automobile bus data is easy to be captured and analyzed, and the availability and integrity can not be guaranteed.

(2) The propagated message source is incomplete. There is no original address information in the protocol, and the receiving electronic control units (ECU) cannot confirm that the received data is the original data, which makes it easy for the attacker to forge and tamper with the CAN bus message by injecting false information, which allows the message to be stolen and tampered with, and the authenticity of the message cannot be guaranteed.

(3) Bus vulnerability. The arbitration mechanism given priority in the CAN bus protocol makes it possible for hackers to carry out denial of service attacks on bus messages. The attacker can replay or flood the vehicle bus by means of sniffing or monitoring so that the ECU cannot send and receive messages normally.

2.3. Network Security Attacks

This section will summarize and classify the external interfaces of intelligent networked vehicles that may be attacked from the perspective of network layering, and divide attacks into different levels according to the source of the attack. Potential attackers often implement different levels of network attacks on cars through these external interfaces. The characteristics of these network attacks are as follows.

(1) Attacks from the sensing layer (physical layer). Today's automobile is developing towards electrification, intelligence, networking, and sharing. In order to meet the needs of all aspects, we need to be equipped with a series of advanced sensors, such as lidar, millimeter-wave radar, camera, and GPS, which are used to collect the perceived information of the external environment and provide the ability to perceive the environment for automatic driving decision-making. It is also equipped with more and more electronic control units (ECU) and wireless connections. Although these measures improve the safety and efficiency of vehicles, they also bring new weaknesses. Therefore, attacking vehicles through the physical layer will become a new threat to vehicle network security. For example, Rouf et al. [9] proposed an attack that interferes with the tire pressure monitoring system through the radio channel, making the vehicle tire pressure monitoring system ineffective. Tao et al. [14] proposed to attack the keyless start system through the control of the radio channel and illegally start the target vehicle.

(2) Illegal access (data link layer). Due to the lack of data encryption and message verification mechanism in the vehicle network, once the attacker can access the network equipment, they can easily carry out the attack. The attack modes of the data link layer include frame injection, frame forgery, frame sniffing, pause, and DoS attack. The availability of the network will be seriously threatened. For example, it has been proven how to use the vulnerability of remote endpoint to destroy ECU, access the vehicle network, and then control vehicle mobility. Attackers can simply inject arbitrary messages into the CAN bus or monopolize the network by continuously sending the highest priority frames [15].

(3) Attacks from the interface (application layer). In order to improve the safety and efficiency of the automobile transportation system, automobile manufacturers integrate wireless communication systems into automobiles [10]. In recent years, there have been many reports on remote network attacks on vehicles by using vulnerabilities in external network interfaces and devices [6,16]. Attack portals include Bluetooth and OBD- II, Wi-Fi, etc. In the network application layer, attackers can carry out more targeted attacks that are not easily found and are more likely to be interfered or deceived because there is no need for a physical connection [10]. Since such attacks do not have illegal access to nodes and obvious data frame exceptions, they are more difficult to detect. For such attacks, researchers at home and abroad mainly focus on the design of intrusion detection methods based on machine learning [9–11]. At present, there are many problems such as excessive consumption of computing resources, lack of test data sets, and model evaluation.

2.4. Functional Safety Guarantee of Vehicle Network

Functional safety is the premise of the development of intelligent connected vehicles. The traditional designs of vehicle safety include seat belts, passive safety airbags, active safety ABS, anti-lock braking systems, electronic brake-force distribution (EBD), and ADAS, etc. Dangerous events are caused by a failure in driving behavior, and risks such as system failure and hardware failure of random vehicle systems [17]. Risk refers to the possibility of injury or damage caused by these failures and the severity of the consequences of injury or damage [17]. It is recommended to use functional safety to deal with the above risks. This means that there is no unreasonable risk of failure behavior of electrical and electronic systems [17]. Functional security enhancement design should not only follow the corresponding security standards (such as ISO 26262) but also face the reliability constraints of computing and network resources.

In terms of ensuring vehicle functional safety, a large number of researchers have carried out corresponding research work in terms of schedulability and task priority allocation [18–20]. Tindell and burns showed how to study the fixed-priority preemptive scheduling of a single processor system and apply it to the message scheduling on CAN, and transfer it to industrial applications in the form of commercial CAN analysis tools. Prior to Tindell's work, low bus utilization of up to 30% or 40% usually occurs in automotive applications, and a lot of tests are needed to ensure that CAN messages can be completed before the deadline. With the schedulability analysis, the utilization rate of CAN bus can be increased to around 80%, while still ensuring the completion on schedule [20]. In addition, Xie et al. [21] carried out a lot of research on the adaptive scheduling method of multi-functional hybrid key and high-performance real-time scheduling of multi-functional hybrid key, and a fast functional security verification (FFSV) method for distributed automotive applications is proposed to give priority to ensuring high critical tasks (functional security). At the same time, it takes into account the balance between performance and cost, which can obtain a higher acceptance rate than the current methods of existing similar products. Vehicle network security includes two aspects: information security and functional security. Serious information security will threaten functional security, but they face competition in system resources in the process of implementation.

In order to eliminate the competition between information security and functional security in design resources and solve the potential adverse impact of information security on the realization of functional security, it is necessary to take into account the attributes of functional security and information security of the system and comply with the ISO 26262 standard and AUTOSAR specifications. Considering the increasing bandwidth demand of automotive information physical systems (ACPs), Xie et al. [22] proposed an AUTOSAR compatible system model considering time and safety constraints on the signal encapsulation of can and CAN-FD (CAN with flexible data rate) from the perspective of a vehicle CAN message encapsulation and bandwidth utilization optimization. An integrated mixed-integer linear programming formula (I-milp) is used for the optimal DSE of a CAN FD, and a divide and conquer method is used to solve the time complexity problem of I-milp. The scheme balanced the security and bandwidth overhead of the vehicle network.

At the same time, it has good scalability and higher bandwidth utilization in the industrial scale system, ensuring the schedulability for more signal sets. With regard to the relationship between vehicle network security and functional security, the literature [23,24] emphasizes that the threat of network information security will directly affect the safety of personnel inside and outside the vehicle. IIA (identity, integrity, availability) principle [25] establishes a framework for evaluating the information security characteristics of the network system, and explains the most important goal of vehicle network security design, where confidentiality represents the confidentiality of information, integrity represents the consistency or integrity of information, and availability represents the availability of authorized users. In order to clarify the relationship and interaction between functional security and information security, this paper summarizes the relationship between them from the aspects of design objectives, constraints, and their interaction, as shown in Figure 1. After the summary of this paper, the following four points are obtained: the challenges and constraints faced by the vehicle network information security design under the functional security guarantee.

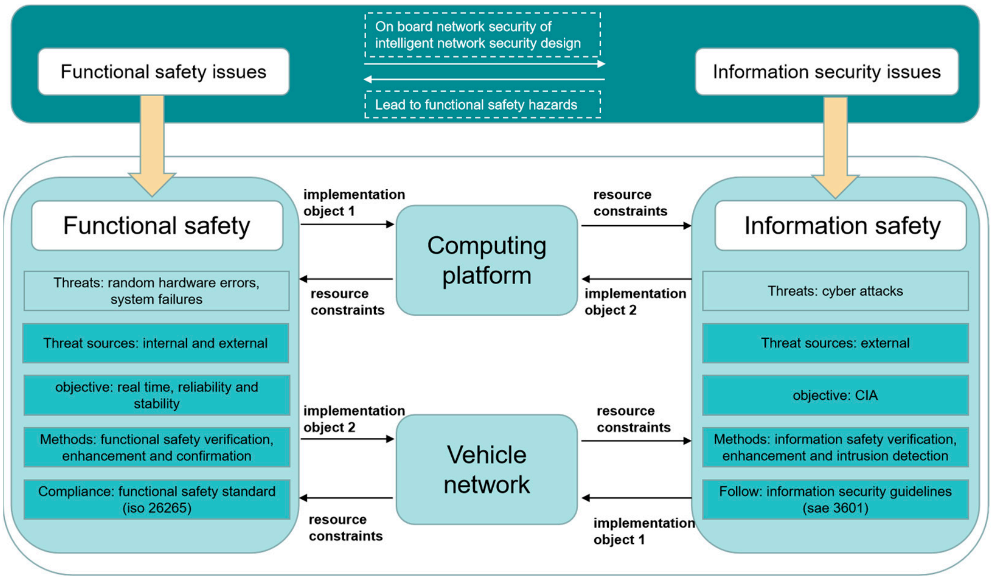
On board network security of intelligent network security design
Functional safety issues
Information security issues
Lead to functional safety hazards
Functional safety
Threats: random hardware errors, system failures
Threat sources: internal and external
objective: real time, reliability and stability
Methods: functional safety verification, enhancement and confirmation
Compliance: functional safety standard (iso 26265)
implementation object 1
resource constraints
Computing platform
resource constraints
implementation object 2
implementation object 2
resource constraints
Vehicle network
resource constraints
implementation object 1
Information safety
Threats: cyber attacks
Threat sources: external
objective: CIA
Methods: information safety verification, enhancement and intrusion detection
Follow: information security guidelines (sae 3601)

Figure 1. Relationship between function security and information security in intelligent network-connected vehicles.

(1) The constraints of computing, storage, and communication bandwidth resources make the internal hardware resource constraints of the vehicle mainly manifest as computing, storage, bandwidth, and energy constraints.

(2) Complex and heterogeneous software and hardware structure. The interior of the vehicle is composed of a large number of heterogeneous and complex software and hardware components, which communicate through heterogeneous vehicle network protocols and gateways. The complexity and heterogeneity of the system not only add uncertainty to the functional security and information security but also increase the difficulty of system functional security guarantee test and verification.

(3) Considering the balance of cost and performance, the computing and storage resources of ECUs in ACPs are often limited and the high cost of deployment may give low priority to network security deployment, and the vehicle network security design is subject to strict cost constraints, which also leads to the network information security enhancement scheme of traditional information can not be deployed in the automotive environment.

(4) The constraints of vehicle networks on functional safety design are mainly manifested in the real-time performance of message transmission, end-to-end delay boundary, system task schedulability, and so on, which will affect the reliability and stability of the system. At present, the research work on vehicle network message schedulability analysis mainly focuses on exploring the upper bounds of communication delay [26–28], network message schedulability analysis [29,30], and meeting deterministic delay analysis [31].

3. Enhancement Technology of Vehicular Network Security

This section focuses on the development of security enhancement technology for vehicle networks under security threats and summarizes it from three aspects: vehicle network data encryption technology, vehicle network message authentication technology, and vehicle network anomaly intrusion detection technology.

3.1. Vehicle Network Data Encryption Technology

Encryption and authentication are widely used in the security field of communication channels. This technology is also widely used in the vehicle network environment (MAC technology has been included in AUTOSAR protocol specification). However, the traditional message encryption and authentication technology face the problems of heterogeneous architecture, limited bandwidth, and computing resources in the vehicle network environment. In view of the limited capacity of the CAN bus, any countermeasure to solve its loopholes should consider this limitation rather than overload the bus. The security solution of the CAN bus can be divided into encryption, authentication, and redesign of the protocol stack. Additional functions can be realized by replacing the fields in the frame, splitting the message into multiple frames, or adding nodes and components to the bus. Cryptography-based methods focus on protecting the CAN bus from malicious messages, while the intrusion detection system (IDS) focuses on detecting malicious messages. Firewalls and intrusion prevention systems (IPS) can be used for external interfaces to prevent access to the bus. It may be necessary to implement dedicated nodes to implement IDs and firewalls. However, the cost of implementing these methods in existing vehicles is still high.

In order to solve the problem of insufficient computing resources, Wang et al. [32] used a hardware security module (HSM) to reduce the computing burden of resource-limited ECUs, so as to provide better encryption/decryption time and effectively reduce the impact of message encryption on network performance. Its disadvantage is that it will increase the cost of hardware deployment. In order to deal with the vulnerabilities and attack models of various vehicle ECUs, Siddiqui et al. [33] proposed the hardware-based secure and trusted communication technology through the CAN bus in the in-vehicle network connecting electronic control units (ECUs), and constructed hardware-based secure and trusted framework, which enables the framework to realize mutual authentication and secure encryption based on lightweight PUF (physical unclonable function) on insecure communication channels. The experimental results show that the time overhead of sending an encrypted data frame in a 1 mbit/s vehicle CAN is 108 µs. Gu [34] et al. proposed a MILP (mixed-integer linear model programming) formula, divide-and-conquer heuristic algorithm, and simulated annealing algorithm, which maps the application task graph to the FlexRay based distributed hardware platform to meet the requirements of security and deadlines and minimize the number of hardware co-processors required in the system. The disadvantage is that the network protocol is very complex.

3.2. Vehicle Network Message Authentication Technology

In recent years, a variety of lightweight message authentication protocols for vehicles' CAN have been proposed to protect vehicles from camouflage attacks. The protocol was originally proposed by Herrewege et al. [35]. In recent years, Jo et al. [36] proposed a new authentication protocol for camouflage attacks, which realizes the balance between network bandwidth consumption and prevents camouflage attacks without modifying the hardware of the CAN controller. The design of a lightweight message authentication protocol can solve the problem of the lack of security authentication design of CAN protocol and ensure the authenticity of vehicle network communication.

3.3. Vehicle Network Intrusion Detection Technology

Compared with information security enhancement means such as message encryption, access control, and protocol authentication, intrusion detection has the characteristics of small bandwidth resources and easy deployment of existing vehicles. It is more suitable for vehicle networks with limited resources and cost. Intrusion detection can be divided into host-based IDS and network-based IDS according to data sources. Detection technology can be divided into detection methods based on feature observation, information theory, statistical analysis, machine learning, etc., as shown in Figure 2, which summarizes the existing relevant research in this area.

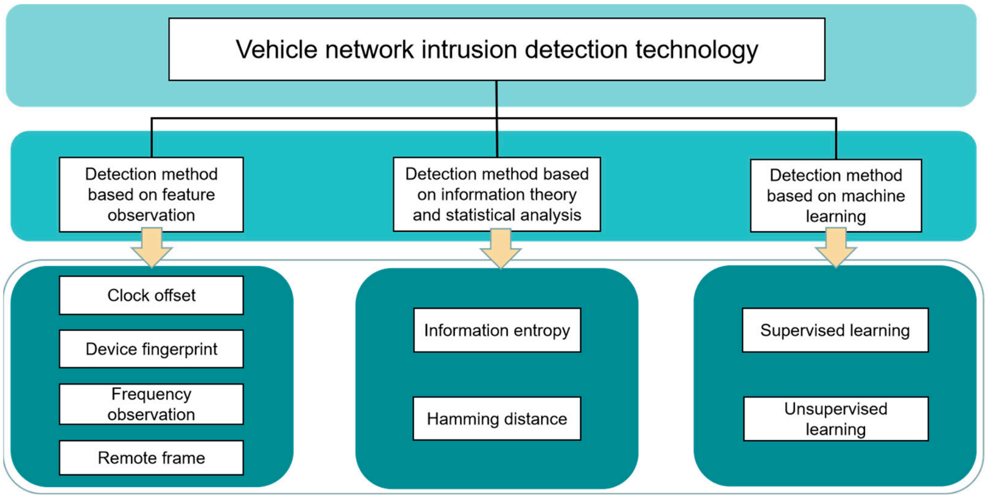
Vehicle network intrusion detection technology
Detection method based on feature observation
Detection method based on information theory and statistical analysis
Detection method based on machine learning
Clock offset
Device fingerprint
Frequency observation
Remote frame
Information entropy
Hamming distance
Supervised learning
Unsupervised learning

Figure 2. Intrusion detection technology classification of vehicle network.

(1) Detection method based on feature observation

Feature observation is one of the common intrusion detection methods, which is widely used in the research of vehicle network intrusion detection [24]. Through the analysis of vehicle network architecture and network protocol, it is found that the network features that can be used for intrusion detection observation mainly include equipment fingerprint (extracted by time-domain and frequency-domain information) [37], clock offset [38], frequency observation [39], and remote frame [40], etc. For example, Li et al. [41] proposed a vehicle network intrusion detection method and system based on clock offset. The CUSUM (cumulative sum) algorithm is used to detect mutation from the cumulative sum of deviation of the target value, mine the association mode and association degree between ECUs in the vehicle network, establish association rules, and add the data with normal association rules into the cumulative clock offset model of the vehicle. The system has a good detection effect for slight deviation from the target.

In 2019, Guan et al. [42] proposed an adaptive intrusion detection algorithm based on message cycle characteristics and an intrusion detection algorithm based on dache characteristics on the basis of analyzing the characteristics of in-vehicle CAN bus communications and various attack characteristics, and took BP neural network as the classification model of the algorithm. Finally, the bus-off attack and intrusion detection was realized based on the in-vehicle CAN communication simulation platform. Qin et al. [43] proposed a vehicle network intrusion detection method based on message sequence prediction, which enables the system to learn the attack type message and then identify it, to achieve the effect of anti-attack.

In recent years, using the uniqueness of ECU electrical characteristics to establish equipment fingerprint information has become a popular vehicle network attack traceability method, which is widely used in vehicle network intrusion detection research. This method was first proposed by Cho et al. [44]. Subsequently, Song et al. [45] realized intrusion detection through the extraction and statistics of network signal features. Lee et al. [40] proposed an intrusion detection method based on the analysis of the offset ratio and time interval between request and response messages in the CAN. Through monitoring to detect the intrusion offset ratio and time interval, it can realize fast intrusion and high-precision detection. Yang et al. [46] proposed a long-term and short-term memory unit recursive neural network (rnn-lstm) identity authentication method based on fingerprint signal characteristics and a method of generating an electronic control unit (ECU) simulated fingerprint signal to train the proposed rnn-lstm classifier. The experimental results show that the proposed rnn-lstm model can effectively detect flooding attacks. Ning et al. [47] proposed an attack detection scheme based on a local outlier factor (LOF). The scheme uses the voltage physical characteristics of the CAN frame to judge whether the message is sent by a legal ECU. The proposed algorithm has low time and space complexity. Experiments in real vehicle network environment data show that the recognition accuracy of the specific attack model can reach more than 98%.

The detection method based on feature observation can often achieve high detection accuracy for specific attack models and has the characteristics of short response time and low network bandwidth overheads [37].

(2) Detection method based on information theory and statistical analysis

By analyzing the information entropy of 6.673 million CAN messages, it is found that the average information entropy in a vehicle's CAN is 11.436 [32,48]. In case of malicious attacks (such as DOS, replay, etc.), the information entropy of the vehicle CAN will be significantly reduced, which is widely used in the research of vehicle network intrusion detection with limited resources [49–51]. We focus on providing an experimental evaluation of entropy-based anomaly detectors. For example, Marchetti et al. [50] evaluated the vehicle network intrusion detection algorithm based on information theory and found that in the vehicle network intrusion detection evaluation, using a single information theory model can only be effective against a single flood attack. Muter et al. [51] first used the concept of information entropy in vehicle detection networks and discussed its applicability. On this basis, Wu et al. [52] proposed a new method based on information entropy which takes a fixed amount of information as the sliding window. By improving the sliding window strategy and optimizing the decision-making conditions, the detection accuracy is increased and the false positive rate is reduced. Experimental results show that this method is more effective, can provide real-time response to attacks, and significantly improve the accuracy of intrusion detection in the vehicle network environment.

In recent years, Qin et al. [53–55] have carried out a series of research work on vehicle network anomaly detection by using the method of information theory. Firstly, in the literature [53], they proposed a vehicle CAN bus network anomaly detection method using information entropy and verified the effectiveness of this method through experiments. Theoretical analysis and experimental results show that the anomaly detection method of the vehicle CAN bus network using information entropy is effective and feasible. Subsequently, in reference [54], a CAN bus anomaly detection method based on Renyi information entropy is proposed. Through the analysis and statistics of messages in the CAN bus network, Renyi information entropy and Renyi divergence are calculated, and an anomaly detection model is established, which effectively improves the detection accuracy. However, the model is still limited to the detection of replaying and flooding attacks. In reference [55], a random forest model is constructed with a large number of normal and abnormal message data collected, and a series of parameter adjustments are made. Then, input the CAN bus message to be detected into the random forest model of the corresponding ID. Finally, the normal or abnormal message classification is completed through the model. The simulation results show that the model can effectively detect the abnormal data on the bus and improve the safety of vehicle operation.

(3) Detection method based on machine learning

Machine learning, neural network, and other theories have also become a hot direction to study vehicle network intrusion detection technology [56–58]. Andreas [59] proposed to use a class of support vector machine (SVM) with radial basis function (RBF) kernel to learn baseline normal behavior and classify deviations as exceptions, and the generated classifier is suitable for message time series. Low dimensional data characteristics are extracted. Normal and hacker data packets are distinguished by training the vehicle network data packets of the electronic control unit (ECU). This technology can monitor the switching packets in the vehicle network and provide real-time high detection rate response. Literature [60] uses the Bayesian network method to quickly identify malicious message attacks on the CAN and uses Carla (car learning to act) [61] to simulate CAN messages under various operating states of real vehicles. The disadvantage is that its detection accuracy can not meet the requirements of functional security levels. Biggio et al. [62] investigated a series of support vector machine (SVM) poisoning attacks, which showed that such attacks take advantage of the natural or well-distributed characteristics of machine learning data sets to inject compiled data into the data set to increase the test error of the SVM probability. The authors experimentally demonstrate that the gradient ascent procedure reliably identifies good local maxima of the non-convex validation error surface, which significantly increases the classifier's test error. Demontis et al. [63] proposed to classify potential attack scenarios for learning-based malware detection tools by modeling attackers with different skills and abilities. The study proposed a simple and scalable secure learning paradigm that mitigates the impact of evasion attacks while only slightly reducing the detection rate in the absence of attacks. Biggio et al. [64] proposed a simple but effective gradient-based approach to systematically evaluate the security of several widely used classification algorithms against evasion attacks.

Based on the recently proposed security assessment framework, the literature simulates attack scenarios with different levels of risk against the classifier by increasing the attacker's knowledge of the system and the ability to manipulate attack samples. Kolosnjaji et al. [65] propose a gradient-based attack, which can avoid the recently proposed deep network by changing only a few specific bytes at the end of each malware sample while retaining its intrusion function. Roli et al. [66] summarized poisoning attacks that compromise the training data used to learn machine-learning models, including attacks that aim to reduce the overall performance, manipulate the predictions on specific test samples, and even implant backdoors in the model.

The main limitations of the current work and future challenges for designing safer learning algorithms are discussed. ML (Machine Learning) is being used in multiple domains, however, adversarial attacks are able to exploit its intrinsic weaknesses to reduce its predictive power, common in the CV/NLP domain. However, in the field of network security, these studies rarely appear, because the scenario is inherently influenced by the adversary. Most of the literature on adversarial attacks do not discuss the level of the proposed attack method, merely making assumptions and analyzing the effects under that assumption, without fully considering the feasibility of their assumptions. Apruzzese et al. [67] not only analyzed the real feasibility of adversarial attacks against ML-NIDS by identifying the necessary attacker capabilities and attack scenarios but also gave five elements of the target system. The literature analyzed the real attack environment by building an attacker model.

Finally, the researchers complemented an in-depth study of the feasibility and constraints of real ML-NIDS operating environments, which can be used to evaluate arbitrary adversarial attacks against ML-NIDS. For an invasion detector of adversarial escape attacks, Apruzzese et al. [68] presented an original approach to enhance the intrusion detector against adversarial escape attacks. Combined with a detector layer specifically designed to monitor the behavior of the applications used by the organization, the integrated ensemble learning is applied to a real network environment.

Contemporary machine learning algorithms have not been designed bearing in mind the adversarial nature of the environments they are deployed in. Therefore, machine learning solutions are currently the target of a range of attacks. Pawlicki et al [69] researched adversarial attacks using four recently proposed methods, by which the authors evaluated the possibility of performance degradation of the optimized intrusion detection algorithm in the test time. Afterward, they offered a way to detect those attacks. Usama [70] proposed an adversarial ML attack using generative adversarial networks (GANs) that can successfully circumvent ML-based IDSs. They also demonstrated that GAN can be used to enhance the robustness of IDS. Black-box adversarial attacks become extremely harmful to self-driving cars with real-time "safety" concerns. Kumar et al. [71] presented a new query-based attack method, namely the improved simple black-box attack (M-SimBA), to overcome the application of white-box sources in transmission-based attack methods.

With the continuous development of the use of ML in the Internet of Vehicles (IOV), confrontational threats and their impact have become an important issue. Focusing on Sybil-based adversarial threats against a deep reinforcement learning (DRL)-assisted IoV framework and more specifically, Talpur et al. [72] analyzed the impact of DRL-based dynamic service placement applications on service latency and resource congestion under different attack scenarios through real vehicle trajectory experiments, which also demonstrated that Sybil-based data poisoning attacks have a significant impact on performance. Qayyum et al. [73] provided an in-depth overview of various challenges related to the application of ML in vehicular networks. In addition, the literature not only developed an ML pipeline for CAVs but also presented various potential security issues associated with the adoption of ML methods. In particular, the authors focus on perspectives of adversarial ML attacks on CAVs and outline solutions to defend against adversarial attacks in a variety of settings.

The vehicular network has heterogeneous characteristics, showing a heterogeneous structure in which multiple functional domains realize message communication through the vehicular gateway. Therefore, the attacks at different network layer entrances target different vehicular network security vulnerabilities, the achievable attack models are also different, and the observation characteristics that can be used for intrusion detection are also different. In this regard, through literature research, this paper establishes the relationship between attack entry, security vulnerability, attack model, and exploitable features of vehicle networks, as shown in Figure 3.

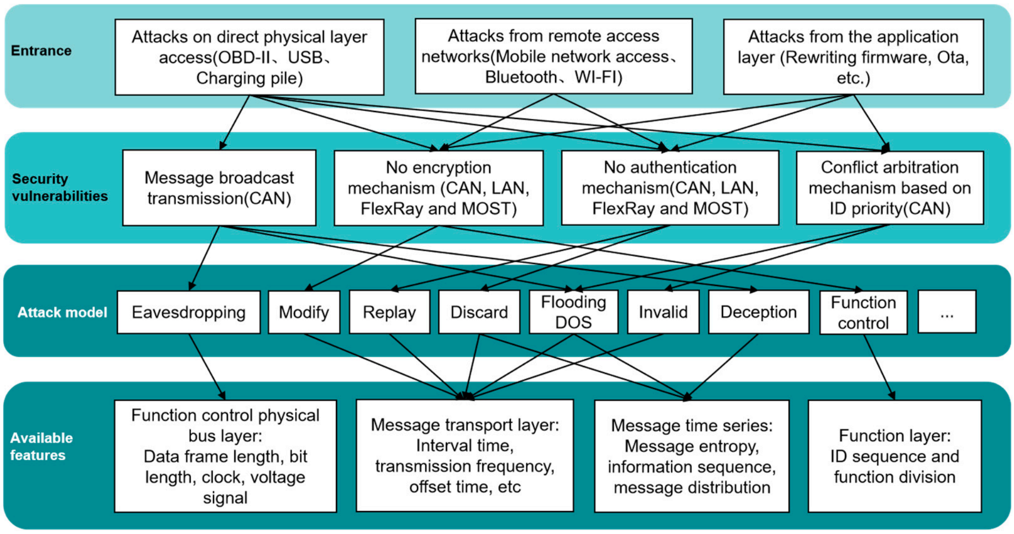
Entrance
Attacks on direct physical layer access(OBD-II、USB、Charging pile)
Attacks from remote access networks(Mobile network access、Bluetooth、WI-FI)
Attacks from the application layer (Rewriting firmware, Ota, etc.)
Security vulnerabilities
Message broadcast transmission(CAN)
No encryption mechanism (CAN, LAN, FlexRay and MOST)
No authentication mechanism(CAN, LAN, FlexRay and MOST)
Conflict arbitration mechanism based on ID priority(CAN)
Attack model
Eavesdropping
Modify
Replay
Discard
Flooding DOS
Invalid
Deception
Function control
...
Available features
Function control physical bus layer: Data frame length, bit length, clock, voltage signal
Message transport layer: Interval time, transmission frequency, offset time, etc
Message time series: Message entropy, information sequence, message distribution
Function layer: ID sequence and function division

Figure 3. Relationship between attack entry, security vulnerability, and exploitable features of intrusion detection in vehicle networks.

This section selects representative work for three types of information security enhancement means combined with an intelligent network-connected vehicle environment, and makes a comparative analysis, as shown in Table 2. The vehicle network anomaly intrusion detection system has the characteristics of strong scalability, low cost, and downward compatibility. It can be applied to the traditional vehicle network environment with limited resources. It is an information security technology that can effectively ensure the authenticity and availability of vehicle network messages of an intelligent network. Therefore, compared with data encryption and message authentication technology, vehicle network intrusion detection technology is more suitable for the vehicle network environment of intelligent network-connected vehicles with key functions, limited resources, and cost sensitivity. It can effectively make up for the computing and communicating overhead brought by encryption and authentication mechanisms, which can be predicted. Vehicle network intrusion detection is still an important development direction of intelligent network vehicle information security enhancement research for a long time in the future.

Table 2. Comparison and analysis of vehicle network security enhancement technologies.

Technology	Scope of Application	Representative Literature and Technology	Information Security Guarantee	Characteristics and Challenges
Data encryption	Data link layer	Lightweight AES [74], hardware password acceleration module [75], MAC decomposition transmission [76]	Safety, Integrity, and Correctness	The enhancement of network message transmission security, integrity, and correctness mainly includes: Facing the balance between security and computing resources
Message authentication	Physical layer, Data link layer	TESLA [35], MAuth-CAN [36], One-way hash chain [77]	Correctness	The enhanced protection of the correctness of network message transmission mainly faces the network band Design constraints in broadband networks
Intrusion detection	Physical layer, Data link layer, Application layer	A class of SVM [59], deep neural network [78], Bayesian network [60], rnn-lstm [46]	Availability and Integrity	To enhance the protection of network availability and integrity, the main challenge is to provide High detection accuracy and robustness, reducing false alarm rate and detection response time

4. Recommendations

This review highlights the consequences and causes of cybersecurity threats. Aiming at this problem, the commonly used vehicle network security enhancement technologies are investigated. Through the analysis and evaluation of the current technologies, the recommendations arising from this review are presented here.

4.1. Recommendations for Vehicle Cybersecurity Threats

1. Through data research and analysis, it can be concluded that whether it is based on a wired or wireless data transmission layer, or a relatively advanced application layer and perception layer, there are certain risks in their information security. The development trend of the in-vehicle network of connected vehicles will be from a composite architecture to a central computing architecture, forming a domain network architecture suitable for autonomous driving.
2. The CAN bus, which plays a representative role in the in-vehicle network, is the starting point and the end of the automotive information security problem and has extremely high requirements for its security and anti-malicious attack capabilities. On the basis of the existing infrastructure, the security of the vehicle network is guaranteed by adjusting the message scheduling method and optimizing the assignment of task priorities. The development of a multi-functional, high-performance and highly adaptable information scheduling method can not only improve the utilization efficiency of the CAN bus but also balance the cost and performance of the system.
3. It is an inevitable development trend to classify and isolate networks and domains, establish in-depth multi-layer architecture defenses for key modules, and use a combination of software and hardware for security protection.
4. The complex heterogeneous hardware architecture and multi-source heterogeneous sensor information on intelligent vehicles increase the vulnerabilities of intelligent vehicle network security, which greatly increases the risk of vehicle networks being attacked. Reducing the time and links of the intelligent vehicle information transmission link, reducing the complexity of hardware and multi-source heterogeneous information can improve the functional safety and information security of the system, and reduce the difficulty of system testing.
5. Adding data encryption and message authentication mechanisms to the vehicle network can effectively avoid illegal attacks on the vehicle network. Reducing computer resource consumption, improving relevant information datasets, and optimizing machine learning techniques can all improve the accuracy and efficiency of system security detection.

6. Reduce the delay of vehicle information transmission, ensure the real-time nature of information transmission, optimize the system of vehicle communication network, research the communication architecture suitable for intelligent vehicle network transmission on the basis of traditional vehicle communication system, and reduce the information network caused by the vehicle itself paralysis.

4.2. Recommendations for Vehicle Cybersecurity Enhancement Technology

1. Layout and application of technology. Limited by the communication network bandwidth and computing resources, the application of traditional information encryption and authentication technologies to intelligent vehicles with more complex information links will greatly increase the cost of network communication and the bloated degree of the system, which is not conducive to intelligent vehicle data encryption. Researching more stable and mature lightweight information security protection modules can reduce the workload of ECUs and improve the work efficiency of ECU.
2. Considering the current requirements of vehicle network bandwidth resources and message response time, the problems and challenges in the design of existing message authentication protocols mainly lie in how to improve the security of message authentication and avoid the functional reliability and real-time problems caused by message schedulability due to communication bandwidth consumption.
3. Considering the long life cycle of an automobile (about 20 years) and the dynamic change of the network environment, there are three main problems in the existing research. ① Detection methods often correspond to specific attack models; ② The robustness of detection effect is not strong (there are many preconditions and lack of perception of vehicle state); ③ Lack of evaluation of detection response time and impact on functional safety guarantee. Considering the key attributes of ACPs functional security, it is urgent to solve the problems through the optimization research of the intrusion detection model and algorithm to avoid the serious functional security crisis of intelligent network=connected vehicles caused by network security problems.
4. The existing research on vehicle network intrusion detection methods based on information theory often ignores the impact of vehicle network information entropy jitter caused by different vehicle states on the detection results. Its detection model has high detection accuracy in limited vehicle states, but its robustness to different vehicle states needs to be improved. These problems result in these methods not meeting the high-level security requirements in the current automotive safety integration level (AISl). Therefore, this paper intends to carry out the optimization research of a state-aware vehicle network intrusion detection algorithm through the perception of the vehicle state.
5. It can be seen that the framework based on machine learning can strengthen the security of the computer network in the vehicle without affecting the network performance. How to use machine learning for resource allocation and mobile target defense deployment is the future research direction. How to determine the best IP shuffle frequency and bandwidth allocation through vehicle network and provide effective and long-term mobile target defense are further problems to be solved. Building a more secure vehicle CAN network intrusion detection system through an advanced machine learning algorithm can improve the efficiency of the vehicle CAN network threat detection, reduce the false positive rate and false negative rate of intrusion detection, and lay a foundation for the development of vehicle can network security.

5. Conclusions

The purpose of this paper was to focus on these security issues and the ways to deal with them accordingly. In this review paper, we have analyzed the reasons why the current vehicle network is vulnerable to network attacks, and we have stated the security requirements of vehicular networks, a number of security attacks on intelligent vehicle systems, and challenges related to them. Moreover, the security enhancement technologies for intelligent interconnected vehicles have been classified regarding their effectiveness against these identified attacks. Our major purpose was to discover some advantages and shortcomings of the proposed defenses. Finally, we comprehensively reviewed three common methods of abnormal intrusion detection in vehicle networks. This review paper provides a good reference for researchers interested in intelligent vehicle safety and project solutions.

Author Contributions: Writing—original draft preparation, T.G. and N.K.; writing—review and editing, N.T.; collection and analyses of data, X.C. and S.W.; supervision and critical review, Y.H. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by National Key Research and Development Program of China under Grant 2021YFE0203600, in part by National Natural Science Foundation of China under Grant U1864204 and in part by the Fundamental Research Funds for the Central Universities in China, CHD (300102220204).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Brecht, B.; Therriault, D.; Weimerskirch, A.; Whyte, W.; Kumar, V.; Hehn, T.; Goudy, R. A security credential management system for V2X communications. *IEEE Trans. Intell. Transp. Syst.* **2018**, *19*, 3850–3871. [CrossRef]
2. Greenberg, A. Hackers remotely kill a jeep on the highway—With me in it. *Wired* **2015**, *7*, 21–22.
3. Ring, T. Connected cars–The next target for hackers. *Netw. Secur.* **2015**, *2015*, 11–16. [CrossRef]
4. Researchers Hack BMW Cars, Discover 14 Vulnerabilities. Available online: https://www.helpnetsecurity.com/2018/05/23/hack-BMW-cars/ (accessed on 25 August 2018).
5. China Information and Communication Research Institute. White paper on Internet of vehicles network security. *China Inform. Secur.* **2017**, *10*, 29–34.
6. Checkoway, S.; McCoy, D.; Kantor, B.; Anderson, D.; Shacham, H.; Savage, S.; Koscher, K.; Czeskis, A.; Roesner, F.; Kohno, T. Comprehensive experimental analyses of automotive attack surfaces. In Proceedings of the Usenix Conference on Security, San Francisco, CA, USA, 8–12 August 2011.
7. 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.
8. 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.* **2015**, *16*, 993–1006. [CrossRef]
9. Foster, I.; Prudhomme, A.; Koscher, K.; Savage, S. Fast and vulnerable: A story of telematic failures. In Proceedings of the Usenix Conference on Offensive Technologies, Washington, DC, USA, 10–11 August 2015.
10. Rouf, I.; Miller, R.; Mustafa, H.; 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 19th Usenix Security Symposium*; Washington, DC, USA, 11–13 August 2010.
11. Khan, Z.; Chowdhury, M.; Islam, M.; Huang, C.Y.; Rahman, M. In-vehicle false information attack detection and mitigation framework using machine learning and software defined networking. *arXiv* **2019**, arXiv:1906.10203.
12. Taylor, A.; Leblanc, S.; Japkowicz, N. Anomaly detection in automobile control network data with long short-term memory networks. In Proceedings of the 3rd IEEE International Conference on Data Science and Advanced Analytics, Montreal, QC, Canada, 17–19 October 2016.
13. Lv, S.; Nie, S.; Liu, L.; Lu, W. *Car Hacking Research: Remote Attack Tesla Motors*; Keen Security Lab of Tencent: Shenzhen, China, 2016; Volume 2016, pp. 37–45.
14. Yang, T.; Kong, L.; Xin, W.; Hu, J.; Chen, Z. Resisting relay attacks on vehicular passive keyless entry and start systems. In Proceedings of the 2012 9th International Conference on Fuzzy Systems and Knowledge Discovery, Chongqing, China, 29–31 May 2012.
15. Cho, K.T.; Shin, K.G. Error handling of in-vehicle networks makes them vulnerable. In Proceedings of the 23rd ACM Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016.
16. Sun, J.; Iqbal, S.; Arabi, N.S.; Zulkernine, M. A classification of attacks to in-vehicle components (IVCs). *Veh. Commun.* **2020**, *25*, 100253. [CrossRef]
17. Xie, G.; Chen, Y.; Liu, Y.; Li, R.; Li, K. Minimizing development cost with reliability goal for automotive functional safety during design phase. *IEEE Trans. Reliab.* **2017**, *67*, 196–211. [CrossRef]

18. Pop, T.; Eles, P.; Peng, Z. Schedulability analysis for distributed heterogeneous time/event triggered real-time systems. In Proceedings of the 15th Euromicro Conference on Real-Time Systems, Porto, Portugal, 2–4 July 2003.
19. Davis, R.I.; Cucu-grosjean, L.; Bertogna, M.; Burns, A. A review of priority assignment in real-time systems. *J. Syst. Architect.* **2016**, *65*, 64–82. [CrossRef]
20. Davis, R.I.; Burns, A.; Bril, R.J.; Lukkien, J.J. Controller area network (CAN) schedulability analysis: Refuted, revisited and revised. *Real-Time Syst.* **2007**, *35*, 239–272. [CrossRef]
21. Xie, G.; Zeng, G.; Liu, Y.; Zhou, J.; Li, R.; Li, K. Fast functional safety verification for distributed automotive applications during early design phase. *IEEE Trans. Ind. Electron.* **2018**, *65*, 4378–4391. [CrossRef]
22. Xie, Y.; Zeng, G.; Kurachi, R.; Takada, H.; Xie, G. Security/timing-aware design space exploration of CAN FD for automotive cyber-physical systems. *IEEE Trans. Ind. Inform.* **2019**, *15*, 1094–1104. [CrossRef]
23. PiryadarshiniI, I. *Introduction on Cyber Security*; John Wiley & Sons: New York, NY, USA, 2019; pp. 1–37.
24. Wu, W.; Li, R.; Xie, G.; An, J.; Bai, Y.; Zhou, J.; Li, K. A survey of intrusion detection for in-vehicle networks. *IEEE Trans. Intell. Transp. Syst.* **2020**, *21*, 919–933. [CrossRef]
25. Lee, H.; Geum, Y. Development of the scenario-based technology roadmap considering layer heterogeneity: An approach using CIA and AHP. *Technol. Forecast. Soc. Chang.* **2017**, *117*, 12–24. [CrossRef]
26. Peng, C.; Zeng, H. Response time analysis of digraph real-time tasks scheduled with static priority: Generalization, approximation, and improvement. *Real-Time Syst.* **2018**, *54*, 91–131. [CrossRef]
27. Chen, G.; Guan, N.; Liu, D.; He, Q.; Huang, K.; Stefanov, T.; Yi, W. Utilization-based scheduling of flexible mixed-criticality real-time tasks. *IEEE Trans. Comput.* **2018**, *67*, 543–558. [CrossRef]
28. Xie, G.; Zeng, G.; Kurachi, R.; Takada, H.; Li, Z.; Li, R.; Li, K. WCRT analysis of CAN messages in gateway-integrated in-vehicle networks. *IEEE Trans. Veh. Technol.* **2017**, *66*, 9623–9637. [CrossRef]
29. Davis, R.I.; Altmeyer, S.; Reineke, J. Response-time analysis for fixed-priority systems with a write-back cache. *Real-Time Syst.* **2018**, *54*, 912–963. [CrossRef]
30. Chang, W.; Chakraborty, S. Resource-aware automotive control systems design: A cyber-physical systems approach. *Found. Trends Electron. Des. Autom.* **2016**, *10*, 249–369.
31. Vatanpavar, K.; Al Faruque, M.A. ACQUA: Adaptive and cooperative quality-aware control for automotive cyber-physical systems. In Proceedings of the 36th IEEE/ACM International Conference on Computer-Aided Design, Irvine, CA, USA, 13–16 November 2017.
32. Wang, E.; Xu, W.; Sastry, S.; Liu, S.; Zeng, K. Hardware module-based message authentication in intra-vehicle networks. In Proceedings of the 8th ACM/IEEE International Conference on Cyber-Physical Systems, Pittsburgh, PA, USA, 18–20 April 2017.
33. Siddiqui, A.S.; Gui, Y.; Plusquellic, J.; Saqib, F. Secure communication over CAN bus. In Proceedings of the 60th IEEE International Midwest Symposium on Circuits and Systems, Boston, MA, USA, 6–9 August 2017.
34. Gu, Z.; Han, G.; Zeng, H.; Zhao, Q. Security-aware mapping and scheduling with hardware co-processors for Flex Ray-based distributed embedded systems. *IEEE Trans. Parallel Distrib. Syst.* **2016**, *27*, 3044–3057. [CrossRef]
35. Herrewege, A.V.; Singelee, D.; Verbauwhede, I. CAN AUTH-a simple, backward compatible broadcast authentication protocol for CAN bus. In Proceedings of the ECRYPT Workshop on Lightweight Cryptography, Louvain-la-Neuve, Belgium, 28–29 January 2011.
36. Jo, H.J.; Kim, J.H.; Choi, H.Y.; Choi, W.; Lee, D.H.; Lee, I. MAuth-CAN: Masque-Rade-Attack-Proof authentication for in-vehicle networks. *IEEE Trans. Veh. Technol.* **2020**, *69*, 2204–2218. [CrossRef]
37. Cho, K.T.; Shin, K.G. Fingerprinting electronic control units for vehicle intrusion detection. In Proceedings of the 25th USENIX Security Symposium, Austin, TX, USA, 10–12 August 2016.
38. Halder, S.; Conti, M.; Das, S.K. COIDS: A clock offset based intrusion detection system for controller area networks. In Proceedings of the 21st International Conference on Distributed Computing and Networking, Kolkata, India, 4–7 January 2020.
39. Li, F.; Wang, C. Research on Intrusion Detection Technology Based on Association Rules Mining in Vehicular Networks. *Data Mining* **2017**, *7*, 65–69. [CrossRef]
40. Lee, H.; Jeong, S.H.; Kim, H.K. OTIDS: A novel intrusion detection system for in-vehicle network by using remote frame. In Proceedings of the 15th Annual Conference on Privacy, Security and Trust, Calgary, AB, Canada, 27–29 August 2017.
41. Li, F.; Liao, Z.; Zhang, P. A Method and System of On-Board Network Intrusion Detection Based on Clock Offset. China Patent CN201811137466.0, 22 January 2019.
42. Guan, Y. Research on in Car CAN Bus Intrusion Detection Algorithm. Master's Thesis, Harbin Institute of Technology, Harbin, China, 2019.
43. Qin, H.; Yan, M.; Ji, H.; Wang, J.; Wang, Y. A Vehicle-Mounted Network Intrusion Detection Method Based on Message Sequence Prediction. China Patent CN201910499446.6, 20 August 2019.
44. Cho, K.T.; Shin, K.G. Viden: Attacker identification on in-vehicle networks. In Proceedings of the 24th ACM SIGSAC Conference on Computer and Communications Security, Dallas, TX, USA, 30 October November 2017.
45. Song, H.M.; Kim, H.R.; Kim, H.K. Intrusion detection system based on the analysis of time intervals of CAN messages for in-vehicle network. In Proceedings of the 30th International Conference on Information Networking. Off Jalan Sepanggar Bay, Locked Bag 100, Kota Kinabalu, Sabah, Malaysia, 13–15 January 2016.

46. Yang, Y.; Duan, Z.; Tehranipoor, M. Identify a spoofing attack on an in-vehicle CAN bus based on the deep features of an ECU fingerprint signal. *Smart Cities* **2020**, *3*, 17–30. [CrossRef]
47. Ning, J.; Liu, J. An experimental study towards attacker identification in automotive networks. In Proceedings of the 2019 IEEE Global Communications Conference, Waikoloa, HI, USA, 9–13 December 2019.
48. Wang, Q.; Sawhney, S. VeCure: A practical security framework to protect the CAN bus of vehicles. In Proceedings of the 2014 International Conference on the Internet of Things, IOT 2014, Cambridge, MA, USA, 6–8 October 2014.
49. Van Wyk, F.; Wang, Y.; Khojandi, A.; Masoud, N. Real-time sensor anomaly detection and identification in automated vehicles. *IEEE Trans. Intell. Transp. Syst.* **2020**, *21*, 1264–1276. [CrossRef]
50. Marchetti, M.; Stabili, D.; Guido, A.; Colajanni, M. Evaluation of anomaly detection for in-vehicle networks through information-theoretic algorithms. In Proceedings of the 2nd IEEE International Forum on Research and Technologies for Society and Industry Leveraging a Better Tomorrow, Bologna, Italy, 7–9 September 2016.
51. Müter, M.; Asaj, N. Entropy-based anomaly detection for in-vehicle networks. In Proceedings of the 2011 IEEE Intelligent Vehicles Symposium (IV), Baden-Baden, Germany, 5–9 June 2011; pp. 1110–1115.
52. Wu, W.; Huang, Y.; Kurachi, R.; Zeng, G.; Xie, G.; Li, R.; Li, K. Sliding window optimized information entropy analysis method for intrusion detection on in-vehicle networks. *IEEE Access* **2018**, *6*, 45233–45245. [CrossRef]
53. Yu, H.; Qin, G.; Sun, M.; Yan, X.; Wang, X. Cyber security and anomaly detection method for in-vehicle CAN. *J. Jilin Univ. (Eng. Technol. Ed.)* **2016**, *46*, 1246–1253.
54. Yan, X. CAN Bus Anomaly Detection Method Based on Renyi Information Entropy. Master's Thesis, Jilin University, Changchun, China, 2017.
55. Wu, L.; Qin, G.; Yu, H. Anomaly detection method for in-vehicle CAN bus based random forest. *J. Jilin Univ. (Sci. Ed.)* **2018**, *56*, 663–668.
56. Jeon, B.; Ju, H.; Jung, B.; Kim, K.; Lee, D. A study on traffic characteristics for anomaly detection of Ethernet-based IVN. In Proceedings of the 10th International Conference on Information and Communication Technology Convergence, Jeju Island, Korea, 16–18 October 2019.
57. Mousavinejad, E.; Yang, F.; Han, Q.L.; Ge, X.; Vlacic, L. Distributed cyber-attacks detection and recovery mechanism for vehicle platooning. *IEEE Trans. Intell. Transp. Syst.* **2020**, *21*, 3821–3834. [CrossRef]
58. Gmiden, M.; Gmiden, M.H.; Trabelsi, H. An Intrusion Detection Method for Securing In-Vehicle CAN bus. In Proceedings of the 17th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering, Sousse, Tunisia, 19–21 December 2016.
59. Theissler, A. Anomaly detection in recordings from in-vehicle networks. *Big Data Appl.* **2014**, *3*, 23–37.
60. Casillo, M.; Coppola, S.; Santo, M.D.; Pascale, F.; Santonicola, E. Embedded intrusion detection system for detecting attacks over CAN-BUS. In Proceedings of the 4th International Conference on System Reliability and Safety, Rome, Italy, 20–22 November 2019.
61. Dosovitskiy, A.; Ros, G.; Codevilla, F.; Lopez, A.; Koltun, V. CARLA: An open urban driving simulator. *arXiv* **2017**, arXiv:1711.03938.
62. Biggio, B.; Nelson, B.; Laskov, P. Poisoning attacks against support vector machines. *arXiv* **2012**, arXiv:1206.6389.
63. Demontis, A.; Melis, M.; Biggio, B. Yes, machine learning can be more secure! a case study on android malware detection. *IEEE Trans. Dependable Secure Comput.* **2017**, *16*, 711–724. [CrossRef]
64. Biggio, B.; Corona, I.; Maiorca, D.; Nelson, B.; Šrndić, N.; Laskov, P.; Giacinto, G.; Roli, F. Evasion attacks against machine learning at test time. In Proceedings of the Joint European Conference on Machine Learning and Knowledge Discovery in Databases, Prague, Czech Republic, 23–27 September 2013; Springer: Berlin/Heidelberg, Germany, 2013; pp. 387–402.
65. Kolosnjaji, B.; Demontis, A.; Biggio, B.; Maiorca, D.; Giacinto, G.; Eckert, C.; Roli, F. Adversarial malware binaries: Evading deep learning for malware detection in executables. In Proceedings of the 26th European Signal Processing Conference, Rome, Italy, 3–7 September 2018.
66. Biggio, B.; Roli, F. Wild patterns: Ten years after the rise of adversarial machine learning. *Pattern Recogn.* **2018**, *84*, 317–331. [CrossRef]
67. Apruzzese, G.; Andreolini, M.; Ferretti, L.; Marchetti, M.; Colajanni, M. Modeling realistic adversarial attacks against network intrusion detection systems. *arXiv* **2021**, arXiv:2106.09380. [CrossRef]
68. Apruzzese, G.; Andreolini, M.; Marchetti, M.; Colacino, V.G.; Russo, G. AppCon: Mitigating evasion attacks to ML cyber detectors. *Symmetry* **2020**, *12*, 653. [CrossRef]
69. Pawlicki, M.; Choraś, M.; Kozik, R. Defending network intrusion detection systems against adversarial evasion attacks. *Future Gener. Comput. Syst.* **2020**, *110*, 148–154. [CrossRef]
70. Usama, M.; Asim, M.; Latif, S.; Qadir, J.; Ala-Al-Fuqaha. Generative adversarial networks for launching and thwarting adversarial attacks on network intrusion detection systems. In Proceedings of the 15th IEEE International Wireless Communications and Mobile Computing Conference, Tangier, Morocco, 24–28 June 2019.
71. Kumar, K.; Vishnu, C.; Mitra, R.; Mohan, C. Black-box adversarial attacks in autonomous vehicle technology. In Proceedings of the 2020 IEEE Applied Imagery Pattern Recognition Workshop (AIPR), Washington, DC, USA, 13–15 October 2020.
72. Talpur, A.; Gurusamy, M. Adversarial Attacks Against Deep Reinforcement Learning Framework in Internet of Vehicles. In Proceedings of the 2021 IEEE Globecom Workshops (GC Wkshps), Madrid, Spain, 7–11 December 2021.
73. Qayyum, A.; Usama, M.; Qadir, J.; Al-Fuqaha, A. Securing connected & autonomous vehicles: Challenges posed by adversarial machine learning and the way forward. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 998–1026.

74. Luo, F.; Hou, S. Cyberattacks and countermeasures for intelligent and connected vehicles. *SAE Int. J. Passeng. Cars-Electron. Electr. Syst.* **2019**, *12*, 55–67. [CrossRef]
75. Gurgens, S.; Zelle, D. A hardware-based solution for freshness of secure onboard communication in vehicles. In Proceedings of the 4th International Workshop on the Security of Industrial Control Systems and Cyber-Physical Systems, Barcelona, Spain, 6–7 September 2018.
76. Sarpm. Secure Message Authentication Protocol for CAN. Master's Thesis, Middle East Technical University, Ankara, Turkey, 2020.
77. Kang, K.D. A Practical and Lightweight Source Authentication Protocol Using One-Way Hash Chain in Can. Master's Thesis, Daegu Gyeongbuk Institute of Science & Technology, Daegu, Korea, 2017.
78. Kang, M.J.; Kang, J.W. A novel intrusion detection method using deep neural network for in-vehicle network security. In Proceedings of the 83rd IEEE Vehicular Technology Conference, Nanjing, China, 15–18 May 2016.