sensors

MDPI

Review

In-Vehicle Communication Cyber Security: Challenges and Solutions

Rajkumar Singh Rathore [1], Chaminda Hewage [1], Omprakash Kaiwartya [2,*] and Jaime Lloret [3]

[1] Department of Computer Science, Cardiff School of Technologies, Cardiff Metropolitan University, Cardiff Llandaff Campus, Cardiff CF5 2YB, UK
[2] Department of Computer Science, Nottingham Trent University, Clifton Campus, Nottingham NG11 8NS, UK
[3] Department of Communications, Universitat Politècnica de València, 46022 Valencia, Spain
* Correspondence: omprakash.kaiwartya@ntu.ac.uk

Abstract: In-vehicle communication has become an integral part of today's driving environment considering the growing add-ons of sensor-centric communication and computing devices inside a vehicle for a range of purposes including vehicle monitoring, physical wiring reduction, and driving efficiency. However, related literature on cyber security for in-vehicle communication systems is still lacking potential dedicated solutions for in-vehicle cyber risks. Existing solutions are mainly relying on protocol-specific security techniques and lacking an overall security framework for in-vehicle communication. In this context, this paper critically explores the literature on cyber security for in-vehicle communication focusing on technical architecture, methodologies, challenges, and possible solutions. In-vehicle communication network architecture is presented considering key components, interfaces, and related technologies. The protocols for in-vehicle communication have been classified based on their characteristics, and usage type. Security solutions for in-vehicle communication have been critically reviewed considering machine learning, cryptography, and port-centric techniques. A multi-layer secure framework is also developed as a protocol and use case-independent in-vehicle communication solution. Finally, open challenges and future dimensions of research for in-vehicle communication cyber security are highlighted as observations and recommendations.

Keywords: machine learning; cryptography; cyber attacks; cyber security; intrusion detection system; smart intelligent vehicles; in-vehicle network; controller area network (CAN)

check for updates

Citation: Rathore, R.S.; Hewage, C.; Kaiwartya, O.; Lloret, J. In-Vehicle Communication Cyber Security: Challenges and Solutions. *Sensors* **2022**, *22*, 6679. https://doi.org/10.3390/s22176679

Academic Editor: Federico Tramarin

Received: 18 July 2022
Accepted: 31 August 2022
Published: 3 September 2022

1. Introduction

The current era is the witness of tremendous development in in-vehicle automotive technologies since modern intelligent vehicles can be considered cyber-physical systems with excellent capabilities to connect with external infrastructures [1]. The in-vehicle technology enabled modern intelligent vehicles should not be perceived similar to mechanical systems, but the integrated architecture consists of million lines of complex code to provide various real-time information to vehicle occupants. Current advancements in in-vehicle communication technologies enable the more refined in-vehicle dashboard centric communications including with smart phone, sensors, earphone or laptop, and roadside units (see Figure 1). The embedded hardware enabled in-vehicle short range communications need urgent attentions considering cyber security risks [2]. Recently, we can see a high inclination in research trends towards secure in-vehicle network architectures. Researchers are developing new protocols, and the development of new smart applications are the outcome of this growth [3]. There is an urgent need for the development of efficient protocols for automotive industries which should be fully compatible with current trends and technologies [4]. Next, Figure 1 illustrates the in-vehicle communication security scenarios with security threats.

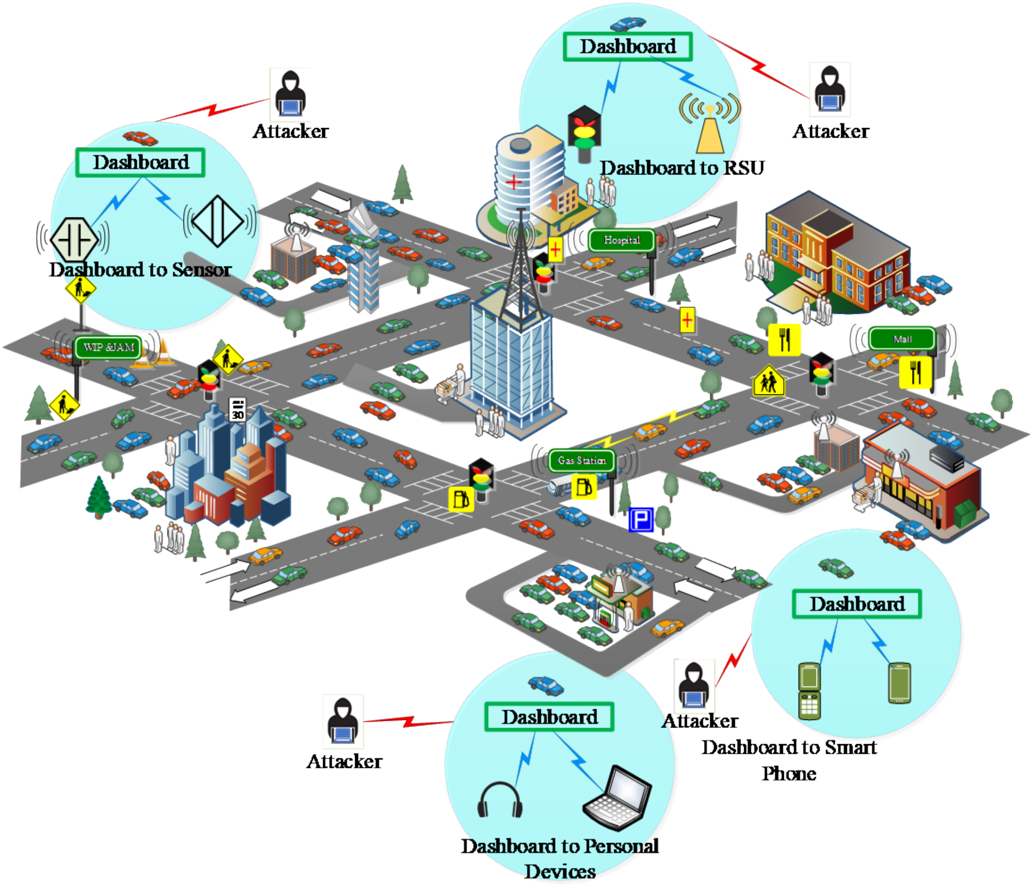


Figure 1. In-Vehicle security scenarios with possible threats.

The advanced in-vehicle functionality in modern intelligent vehicles is provided by electronic control units (ECUs) equipped with the vehicles. Further, these units are connected via serial buses. Controller Area Network (CAN) protocol is responsible for maintaining effective in-vehicle communication among these modules in modern intelligent vehicles [5]. It is a fact that modern in-vehicle technology enabled intelligent vehicles with smart connectivity and computerization have various unique features such as enhanced road safety, connectivity with the outside world, many new services for enhancing the customer experience, etc. However, on the other aspects, these connected smart features have paved the way for hackers to hijack vehicles functionalities, since these features are exposing the vehicle to possible attacks. Hackers may open a new attack surface by accessing the electronic in-vehicle components of modern intelligent vehicles [6].

The existing protocols of the in-vehicle network have various vulnerabilities, such as ID-based arbitration mechanism for contention resolution, unavailability of message authentication and encryption, etc. [7]. There is an urgent requirement for the security of modern intelligent vehicles since adversaries may use existing vulnerabilities and attack the modern intelligent vehicle which may lead to hazards to life and damage to the vehicle on the road. Recent decades are witness of advancements in technology for modern smart intelligent vehicles as well as self-driving vehicles. The modern automotive industries have seen several breakthroughs due to enhanced connectivity, and significant development towards communication channels and access points. On the other hand, these developments open the door for new challenges consisting of security and privacy of data [8]. The safety of life is at the stake due to these cyber security vulnerabilities. Since modern connected vehicles are growing with efficient communication capabilities and sharing critical safety-related information with nearby vehicles as well as with infrastructure around in real-time [9]. This growth is responsible for dynamic and rapid change in the automotive cyber security environment. The cyber security issues should be handled with utmost priority with the detection of any vulnerabilities at the earliest possible time. Cyber security issues may jeopardize modern intelligent vehicles on roads [10,11].

Artificial Intelligence (AI) and Machine Learning (ML) techniques have been used for solving a variety of in-vehicle domain issues [12]. Currently, these techniques have transpired as a reasonable solution for complex application domains. One of the complex application domains is the security of in-vehicle networks [13]. Recently, research innovations have shown that ML-based schemes can effectively address security issues in in-vehicle networks [14]. Since the modern intelligent vehicle network consists of wireless communication between vehicles or infrastructure and increased connectivity has widened the security holes thereby making it vulnerable to a large number of different types of attacks [15]. Additionally, various researchers have significantly contributed in this direction by utilizing machine learning techniques and their variants for developing security frameworks to identify potential attacks and guard against several security-related issues in modern vehicular networks [16]. In the past, cryptographic approaches have been used to propose solutions to handle various types of security issues. For authentication in in-vehicle networks, some traditional authentication techniques include biometric security techniques, key-based authentication, and password protection, etc. The main limitation of cryptographic approaches in handling security issues of in-vehicle networks is low accuracy in validating whether the transferred value is real or spoofed. Additionally, cryptographic approaches are generally implemented in low-powered vehicle security systems [17].

In this context, this paper presents a critical survey of in-vehicle communication focusing on following research questions:

- What are the main components of in-vehicle network?
- Why there is a need to secure in-vehicle network environment?
- Which are the main approaches for securing the in-vehicle network?
- What kind of challenges exist in securing the in-vehicle network?
- Where the future research on in-vehicle cybernetics will move forward?

It first identifies the broad categories of attacks on in-vehicular system. These attacks are classified into four major categories as sensor initiated, infotainment initiated, telematics initiated, and direct interface initiated. Then, we investigate and summarize the available defenses against these in-vehicle cyber-attacks and classify them into two major categories including machine learning-based approaches and cryptography-based approaches. We provide detailed survey and comparison of cryptographic approaches as well as machine learning approaches for designing security solutions against several cyber threats on in-vehicular system. We have developed multi-layered in-vehicle security framework. Open research challenges and future directions for preventing attacks on in-vehicle network systems have been discussed. We are sure that this systematic survey provides the foundation stone about in-vehicle networks' attacks and security solutions based on machine leaning as well as cryptography techniques and it is therefore will play a crucial role in serving as a groundwork and point of reference for variety of stakeholders with different levels. The contribution can be summarized as below:

1. In-vehicle communication network architecture is presented considering key components, interfaces, and related technologies.
2. The protocols for in-vehicle communication have been classified based on their characteristics, and usage type.
3. Security solutions for in-vehicle communication have been critically reviewed considering machine learning, cryptography, and port centric techniques.
4. A multi-layer secure framework is also developed as a protocol and use case independent in-vehicle communication solution.
5. Finally, open challenges, and future dimension of research for in-vehicle communication cyber security is highlighted as observation and recommendation.

The rest of the paper is organized in following sections. Section 2 presents the architecture and components of in-vehicular communication system. Section 3 briefly describes the classification and characteristics of in-vehicle automotive protocols. Section 4 illustrates the broad classification of attacks on in-vehicle communication system. A comprehensive survey of security solutions for in-vehicle network against malicious threats is presented in Section 5. A multi-layered in-vehicle security framework is proposed in Section 6. Open challenges and future research directions are highlighted in Section 7, followed by conclusions in Section 8.

2. Architecture and Components of In-Vehicular System

In-vehicle networks (IVNs) are an emerging research field in modern vehicular networks. The in-vehicle network architecture consists of several core components, namely Sensor Domain consisting of high precision sensors, Chassis Domain, Infotainment Domain, Telematics Domain, Powertrain Domain, etc. For effective communication between these core components of in-vehicle networks, protocols play a major role such as Ethernet, FlexRay, and Controller Area Network (CAN), etc. The rapid growth in connectivity among transportation facilities integrated with modern advanced technologies, for example, V2X-communications, have resulted in widening the security holes and subsequently, attackers can get access to the in-vehicle network.

2.1. Internal Configuration of Electronic Control Units

Critical information is exchanged among different electronic control units (ECUs) installed in the vehicle. In advanced modern vehicles, as the number of ECUs increases, the complexity level in in-vehicle networks also increases since each distinct component are having different requirements in terms of bandwidth and latency. The number of ECUs is continuously rising in modern intelligent vehicles to enable the modern advanced vehicle with a variety of new functionality for safety, security, convenience, etc. Additionally, for the interconnections of a large number of ECUs, several in-vehicle protocols have been developed and research is still going on with more advanced features. Additionally, ECUs are usually connected with more than one bus network due to their diversified functionality including controlling and monitoring the vehicle [18]. Figure 2 demonstrates the internal configuration of ECU in detail.

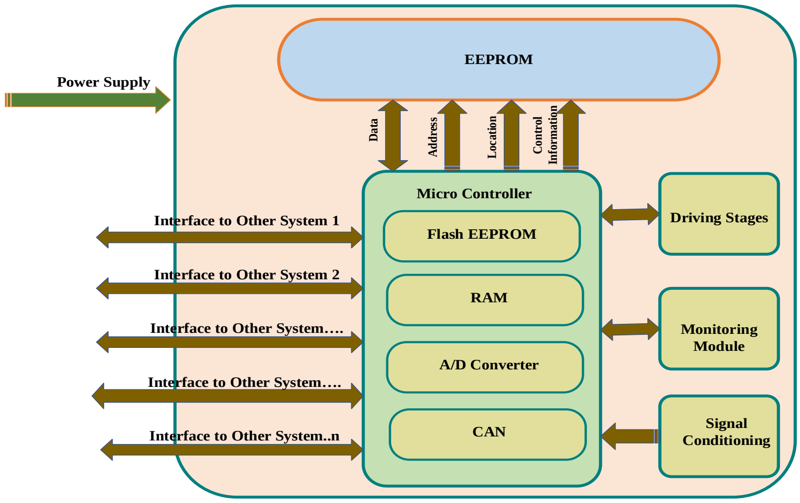


Figure 2. Internal Configuration of ECUs.

2.2. In-Vehicle Network Architecture

In-vehicle networks which are also known as internal communication networks are responsible for interconnecting various components inside modern intelligent vehicles. ECUs, gateways, sensors, actuators, etc. are considered the main core components inside modern intelligent vehicles. Additionally, the modern intelligent vehicle has various units, namely Telematics Domain, Infotainment Domain, Chassis Domain, Powertrain Domain, Body Domain and Sensor Domain, etc. Sensors give inputs to these electronic units for further computation [19]. Figure 3 presents the general architecture of in-vehicle network.

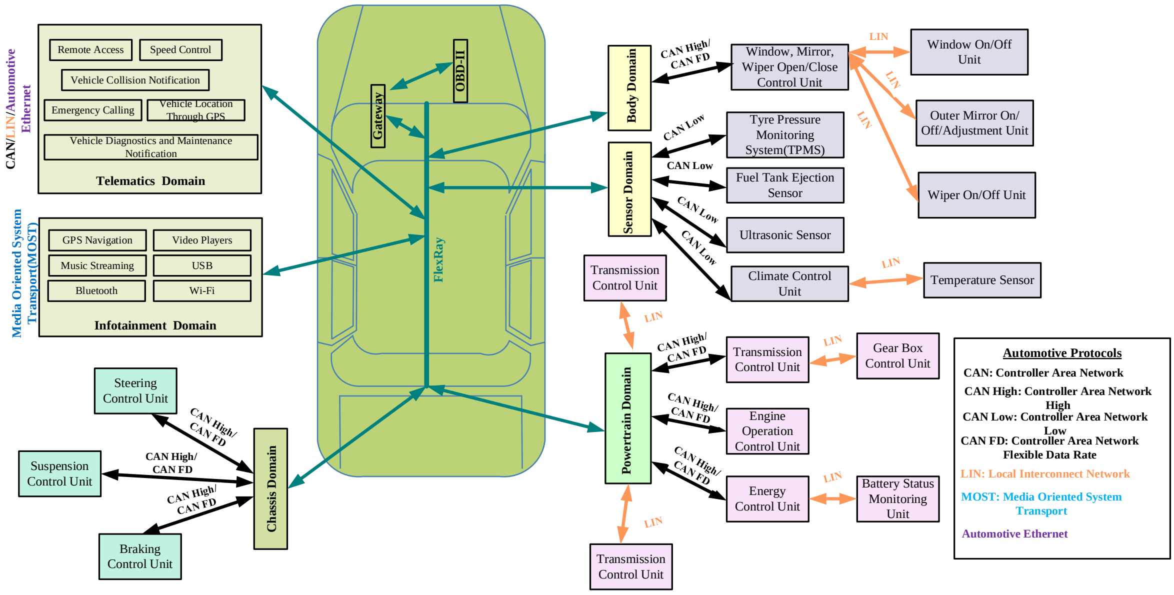

CAN/LIN/Automotive Ethernet
Remote Access
Speed Control
Vehicle Collision Notification
Emergency Calling
Vehicle Location Through GPS
Vehicle Diagnostics and Maintenance Notification
Telematics Domain
Media Oriented System Transport(MOST)
GPS Navigation
Video Players
Music Streaming
USB
Bluetooth
Wi-Fi
Infotainment Domain
Steering Control Unit
Suspension Control Unit
Braking Control Unit
CAN High/ CAN FD
CAN High/ CAN FD
CAN High/ CAN FD
Chassis Domain
Gateway
OBD-II
FlexRay
Body Domain
CAN High/ CAN FD
Window, Mirror, Wiper Open/Close Control Unit
LIN
Window On/Off Unit
LIN
Outer Mirror On/ Off/Adjustment Unit
LIN
Wiper On/Off Unit
Sensor Domain
CAN Low
Tyre Pressure Monitoring System(TPMS)
CAN Low
Fuel Tank Ejection Sensor
CAN Low
Ultrasonic Sensor
CAN Low
Climate Control Unit
LIN
Temperature Sensor
Transmission Control Unit
LIN
Powertrain Domain
CAN High/ CAN FD
Transmission Control Unit
LIN
Gear Box Control Unit
CAN High/ CAN FD
Engine Operation Control Unit
CAN High/ CAN FD
Energy Control Unit
LIN
Battery Status Monitoring Unit
LIN
Transmission Control Unit
Automotive Protocols
CAN: Controller Area Network
CAN High: Controller Area Network High
CAN Low: Controller Area Network Low
CAN FD: Controller Area Network Flexible Data Rate
LIN: Local Interconnect Network
MOST: Media Oriented System Transport
Automotive Ethernet

Figure 3. In-Vehicle Network Architecture with Automotive Protocols.

It is a fact that tiny sensors are the backbone of modern intelligent vehicles since sensors typically recognize and immediately report the problem for resolution example including service due, component fault, etc. Sensors observe various key events such as car speed, fuel, temperature, speed of crankshaft's rotation, tire pressure, oxygen ratio in the exhaust gases, air density in the engine, etc. therefore tiny sensors should have high standards, such as precision, resolution, sensitivity, accuracy, low power consumption with less noise. The observation and reporting of these events help in the early detection of the problem and result in the prevention of vehicle damage. Autonomous vehicles have sensors of different types ranging from electric, mechanical, optical, sound, image, and light sensors, etc.

2.3. Classification of In-Vehicle Network Architecture

The in-vehicle network architecture can be classified into three types. The first classification consists of the central gateway and this type of architecture is known as distributed electrical and electronics(E/E) type. In the second classification, multiple operational domains are connected via a central gateway and this type of architecture is known as the domain-centralized electricals and electronics(E/E) type. The third type of in-vehicle network architecture is known as future E/E architecture or zonal architecture. This architecture has a centralized high-performance computing unit (HPCU) which is useful in reducing the complexity of previously existing two architectures [20]. Figure 4 illustrates the distributed electrical and electronics (E/E) architecture.

The two main components of this architecture are function-specific ECUs along with central gateway. The controller area network (CAN) bus is used for the interconnection. A strong collaboration among the ECUs can be achieved with the help of the central gateway. Therefore, complex functions, such as cross-functional connections as well as adaptive cruise control, can be executed efficiently in this type of architecture with the help of a centralized gateway.

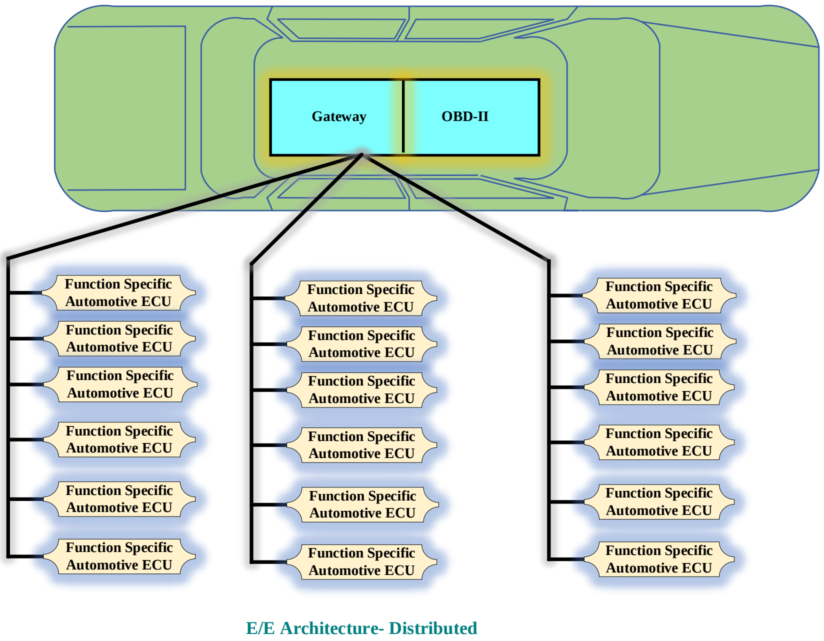

Gateway
OBD-II
Function Specific Automotive ECU
E/E Architecture- Distributed

Figure 4. E/E Architecture-Distributed.

The main limitation of electrical and electronics(E/E) type in-vehicle network architecture is increased communication overhead since different ECUs communicate via a central gateway. For addressing this limitation, an architecture was developed based on several functional domains for in-vehicle network architecture in which different functional/operational domains are interconnected via the central gateway. Additionally, the communication load on the central gateway is significantly reduced since the majority of communication happens within these operational/functional domains themselves. This architecture has scalable capability because more functional domains can be added easily [21].

In this architecture also, the central gateway plays a crucial role. The main feature of this type of architecture is the use of function-specific automotive ECUs and domain-specific ECUs. Additionally, through CAN bus and Ethernet connections, function-specific automotive ECUs are connected to domain-specific ECUs. This architecture is much more efficient than the previous architecture in terms of handling stringent complex functions. With the help of the consolidation of functions. Domain centralized architecture has become extremely elaborate over time. The autonomous driving feature requires a large number of sensors and actuators which results in higher data processing and bandwidth requirements, and subsequently, the architecture becomes more complex in these scenarios. Figure 5 depicts the domain centralized E/E architecture [22].

The third type of in-vehicle architecture is futuristic architecture also known as zonal architecture. The architecture reflects futuristic smart vehicle functions as well as technologies with a significant reduction in weight and cost. The three main components of the zonal architecture are function-specific automotive ECUs, HPCU, and zonal ECUs. In this architecture, the central controller is HPCU which is responsible for processing all data received from several different zones of the vehicle. The data is transferred from one zone to another through HPCU which works as a central gateway. To match the high bandwidth and speed requirements for data transmission in the vehicle network, the Ethernet connections are utilized for the connection of the ECUs and HPCU. The unique feature of this futuristic architecture is support for the virtual domain. For HPCU, the two key functionalities are transferring the embedded functions into the cloud and the next feature provides software update/download support over the air (OTA) [23,24]. Figure 6 presents the zonal architecture.

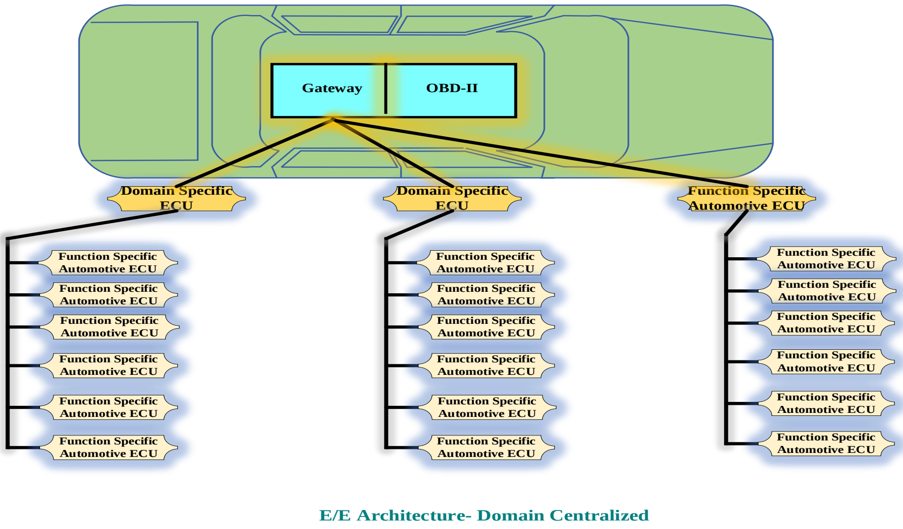

Gateway
OBD-II
Domain Specific ECU
Domain Specific ECU
Function Specific Automotive ECU
Function Specific Automotive ECU
E/E Architecture- Domain Centralized

Figure 5. E/E Architecture-Domain Centralized.

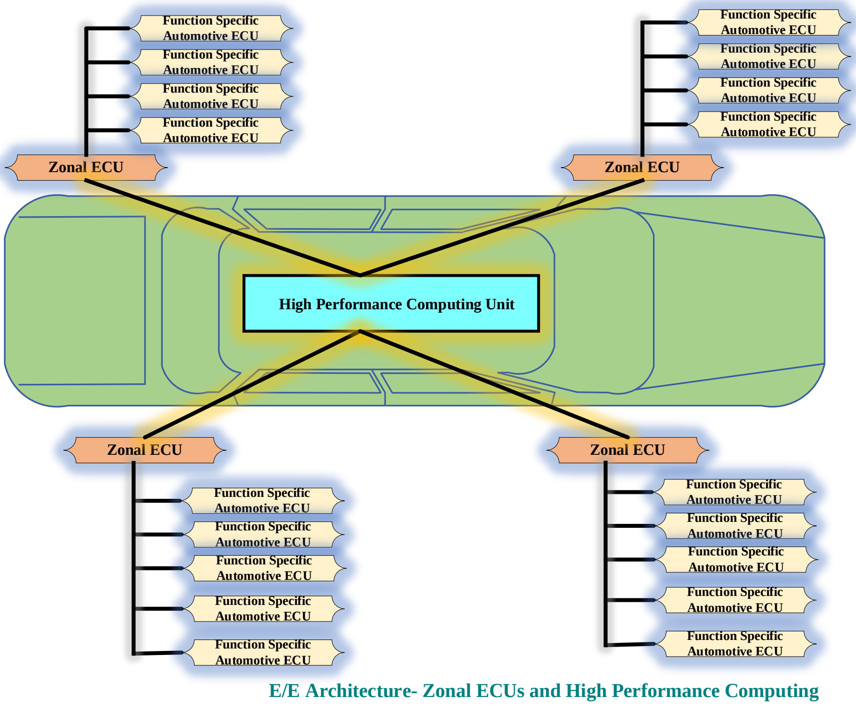

Function Specific Automotive ECU
Zonal ECU
Zonal ECU
High Performance Computing Unit
Zonal ECU
Zonal ECU
E/E Architecture- Zonal ECUs and High Performance Computing

Figure 6. E/E Architecture-Zonal ECU and High-Performance Computing.

The door is open for significant opportunities in the automotive sector by transferring consumer electronics technology and information technology to the automotive sector. The only factor in this transformation is a lot of adaptions. In the current era, rapid changes can be seen in the automotive electronics architecture [25].

3. Classifications and Characteristics of In-Vehicle Automotive Protocols

In advanced vehicles (electric, hybrid, driverless), stringent real-time information is exchanged among different modules for smooth function of the vehicle and this requirement is fulfilled by the rapid development of various applications of CAN. Other heterogeneous and complex architectures of in-vehicle networks include networks such as Media-Oriented Systems Transport (MOST), FlexRay, Local Interconnect Networks (LIN), and Automotive Ethernet (AE). Table 1 describes the classification of protocols for in-vehicle network communications.

Table 1. Classification of in-vehicle network communication protocols.

In-Vehicle Network Communication Protocols	Domain	Bandwidth	Salient Features	Drawbacks	Topology	Standard	Cabling	Max. Nodes Supported	Messaging
Controller Area Network (CAN)	Powertrain, Body Control	125 Kbps–1 Mbps	Low cost	Less Bandwidth	Star, Ring, Linear bus	ISO 11898	UTP	30	Multi-Master
Local Interconnect Network (LIN)	Simple Applications (Less Time Critical)	125 Kbps–1 Mbps	Low cost	Low Speed	Liner bus	ISO 17987	1-Wire Cabling	16	Master-Slave
FlexRay	Advanced Chassis Control	Up to 10 Mbps	High Speed	High Cost	Star, Linear bus, hybrid	ISO 17458	UTP	22	Multi-Master
Media-Oriented Systems Transport (MOST)	Infotainment Applications	Up to 150 Mbps	High Speed	High Cost	Ring	ISO 21806	UTP and Optical	64	Streams/Cyclic Frames
Automotive Ethernet	High Bandwidth Applications	Up to 100 Mbps	High Speed	High Cost	Star, Linear bus	ISO 21111	UTP	Based on Switch ports	Based on IP

3.1. Controller Area Network (CAN)

For in-vehicle communications, the CAN protocol is generally mainly used. CAN packets are transmitted between multiple ECUs through inter-connected buses. The broadcast communications mechanism is used in the CAN protocol. The CAN protocol has various advantages such as simplicity, low network complexity, and reduced wiring costs since CAN utilizes the multiplex wire architecture for eliminating the need of complex excessive wiring for communication among different ECUs. CAN is unable to provide real-time performance which is a crucial factor for applications related to critical security. the CAN protocol is not able to handle security challenges. The lack of authentication mechanism and encryption is considered the main limitation of the CAN protocol. Additionally, the rapid advancement in automotive applications require support from high bandwidth backend protocols but CAN has bandwidth limitations [26].

3.2. Local Interconnect Network (LIN)

LIN is a single wire network for connecting sensors and actuators. Reliability of LIN is not up to the mark as compared with CAN thereby it is not suitable for time critical applications. LIN utilizes the parity bits and checksums for detecting the incorrect messages in the network [27].

3.3. FlexRay Protocol

FlexRay protocol utilizes two parallel channels for data transmission in synchronous as well as asynchronous mode. FlexRay can be utilized for time critical applications. Although FlexRay has reliability and fault tolerance features, but implementation cost is very high. FlexRay handles logical errors by using checksums and redundancy mechanisms [28].

3.4. Media-Oriented Systems Transport (MOST)

The MOST protocol has been developed by domestic digital bus. MOST protocol support synchronous as well as asynchronous mode for data transmission. MOST protocol also support the GPS applications and radio. Although MOST protocols satisfy the infotainment requirements, but MOST protocols failed to provide bandwidth requirements when the requirement is increased exponentially [29].

3.5. Automotive Ethernet

This protocol is considered as physical layer standard in the automotive domain. Due to the diversified capability of this protocol, it can be used in more advanced applications in vehicles such as advanced driving assistance systems, etc. The main advantage of this protocol is the reduced wiring cost since it supports switched network technology [30].

4. Classification of Attacks on In-Vehicle Network System for Possible Entry Points

This paper first identifies the broad categories of attacks on in-vehicular system. These attacks are classified into four major categories as sensor initiated, infotainment initiated, telematics initiated, and direct interface initiated as shown in Figure 7. There are generally two attack vectors, namely wireless access and physical access, attackers are using these attack vectors to get access to the internal networks of the vehicle. External inputs use these interfaces so that ECUs can be exploited. The attackers may use software bugs, the vehicle's remote key (via the internet) and much more to exploit the ECUs easily. The in-vehicle network has several security issues, research is going on to develop an advanced security framework. Wireless networks can be used for exploiting the bus system of the in-vehicle network.

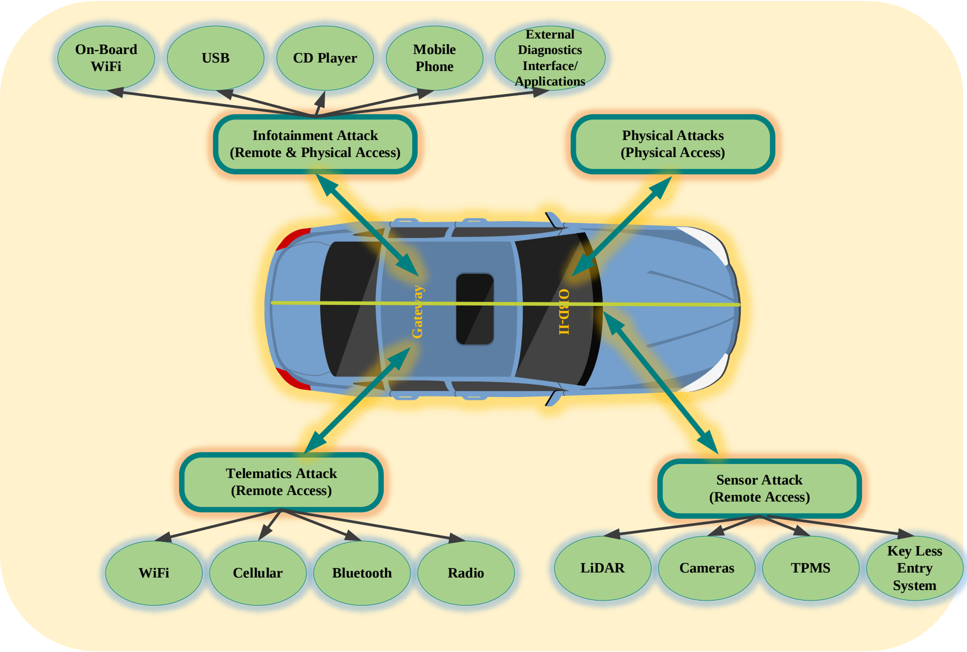

On-Board WiFi
USB
CD Player
Mobile Phone
External Diagnostics Interface/ Applications
Infotainment Attack (Remote & Physical Access)
Physical Attacks (Physical Access)
Gateway
OBD-II
Telematics Attack (Remote Access)
Sensor Attack (Remote Access)
WiFi
Cellular
Bluetooth
Radio
LiDAR
Cameras
TPMS
Key Less Entry System

Figure 7. Classification of in-vehicle network attacks.

4.1. *Entry points to Smart Vehicles*

Smart intelligent vehicles have lots of features due to rapid development in automotive technologies. No security mechanism is sufficient enough to handle all security threats. With tremendous evolution in technology, hackers are also using advanced techniques to hack smart vehicles. There are several entry points to smart vehicles which are listed in Figure 8.

4.1.1. OBD-II Port

This port is used for monitoring various details such as emissions from vehicles, speed, mileage, etc. OBD-II ports are considered the weakest link in the vehicle since the attacker may collect diagnostic data easily and subsequently get success in accessing the in-vehicle network and deployment of malicious programs. Two types of attacks are possible on the OBD-II port, namely an in-vehicle network access attack and a Dongle exploitation attack. In the former attack type, the attacker may utilize an OBD-II port for installing the malicious device in the in-vehicle network with the main objective of obtaining physical access. In the later attack type, dongles are fitted in the OBD-II ports. These dongles can be remotely handled and decrypted by the attacker [31].

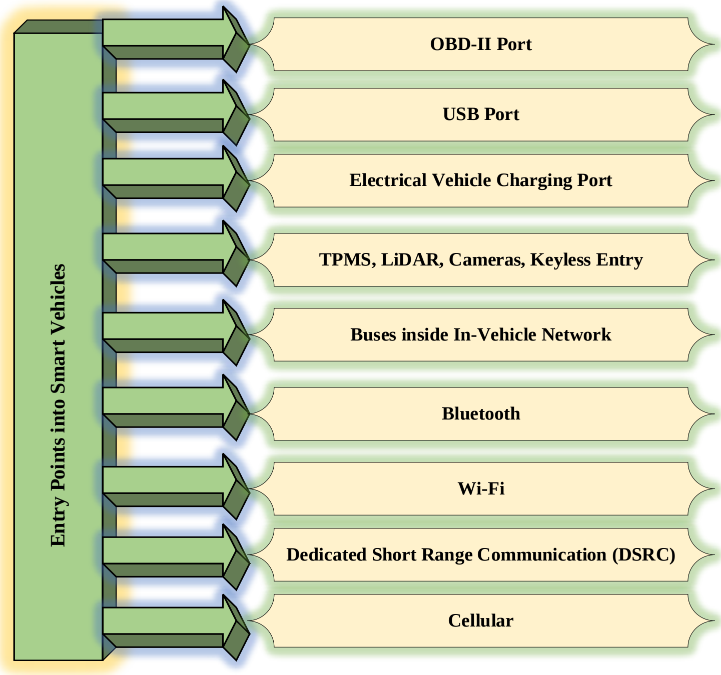

Entry Points into Smart Vehicles
OBD-II Port
USB Port
Electrical Vehicle Charging Port
TPMS, LiDAR, Cameras, Keyless Entry
Buses inside In-Vehicle Network
Bluetooth
Wi-Fi
Dedicated Short Range Communication (DSRC)
Cellular

Figure 8. Illustrating entry points to smart intelligent vehicles.

4.1.2. USB and Charging Ports

Severe security threats are posed by the use of USB ports in the vehicle. Several examples of severe security threats are reprogramming of the controller processor, installation of several types of malicious codes, network card tampering, and changes in operating system functionalities. Additionally, the malicious codes inside a USB pen drive or CD can be used to hack the infotainment system. After hacking the infotainment system, hackers can easily control other parts of the vehicle such as the braking system and engine control system [32]. During the charging mechanism, Electric Vehicles (EV) are susceptible to several attacks via charging infrastructure. Additionally, the smart grid may be attacked by utilizing a charging system [33].

4.1.3. Tire Pressure Monitoring System (TPMS), LiDAR and Keyless Entry Ports

The attacker can use the TPMS for eavesdropping attack to get access to the vehicle network and perform malicious activities. LiDAR and cameras are opening the door for signal jamming attack. For keyless entry attack, the hacker tries to intercept the signal for further capturing and re-directing purposes. There does not exist any adequate mechanism to protect the radio signals hence radio signals transmitted from vehicles' keys can be easily captured by hackers. This area is open to researchers [34].

4.1.4. Buse Network Ports

There does not exist a communication protection mechanism for CAN. This protocol reflects a broadcast nature and therefore each node is intended to receive the frame. This frame is not secured by either MAC or digital signature. Confidential data can be stolen or manipulated in this protocol. The hacker can send fake frames to each node and thereby vehicle may start showing unintended behavior [35].

4.1.5. Vehicular Communication Ports

All the smart vehicles are enabled with Bluetooth with a range of 10 m. The mobile phone can easily get connected with infotainment as well as telematics systems for performing a range of activities such as making calls, streaming music etc. Through Bluetooth, hackers can get full access to vehicles to perform malicious activities [36]. Almost all smart vehicles are enabled with wi-fi. These smart vehicles can be connected to the internet through roadside wi-fi hot spots. The low-security level at the wi-fi hot spot may expose the vehicle to several threats since wi-fi hot spots may have outdated security mechanisms for the connection and hackers can easily target the vehicles through these weak access points [37].

Dedicated Short Range Communication (DSRC) is one of the onboard units. It utilizes radio frequency for communication. It supports short-range communication for the vehicle to infrastructure as well as vehicle-to-vehicle communication. The hacker can easily get access to the vehicle through DSRC and may perform severe undesirable activities [38]. Almost all smart vehicles are equipped with cellular technologies (3 G/4 G/5 G, etc.). These smart vehicles are now capable of vehicle-to-infrastructure as well as vehicle-to-vehicle communication with distances of several miles. hackers can perform two types of attacks, namely jamming and eavesdropping on the cellular networks [39].

4.2. Corrective Mechanisms to Port Threats

Several threats due to OBD-II ports can be handled by designing the framework for frame injection tracking which are coming from the OBD-II port. The second strategy can be used for firmware updates by encryption and message signing. The threats due to USB ports can be handled by designing the standard USB security framework since there exist large applications of USB devices and thereby posing severe security vulnerabilities. There are two ways to provide protection against threats due to USB ports; in the first approach, a security certificate should be required by the USB whenever it tries to connect with the internet and subsequently this certificate may give permission to link to the vehicle. In the second approach, the malware/viruses are prevented to access the restricted security area through the USB port. The threats due to electric vehicle charging ports can be handled by utilizing three schemes, namely secure firmware updates, cryptographic signatures, and authentication schemes. To protect the electric vehicle charging infrastructure, Open Charging Point Protocol (OCPP) has been developed for securing charging systems in the smart grid [40].

5. Comprehensive Survey of Security Solutions for In-Vehicle Network

5.1. Related Existing Surveys

The rapid development in advanced automotive technologies leads to prominent growth in smart vehicles manufacturing. The speedy transition towards advanced smart vehicles opens the next door to several security threats therefore in recent years, the researchers are showing more interest in designing new security frameworks for automotive protocols and particularly focused on the CAN. A large number of surveys have been published recently considering security aspects on in-vehicle network. A comprehensive survey is presented by Zeng et al. [41] considering all five protocols used in-vehicle networks. For analyzing the performance of the protocols, they assume specific parameters such as fault tolerance, cost and data transmission ability. Security threats along with appropriate solutions are discussed in this comprehensive survey covering authentication schemes, and physical controlled approach, etc. Further, in [42], a review is presented on solutions for CAN message authentication. Additionally, they analyzed the main requirements needed with aligned to the industry. Next, for improving the CAN security, a survey of proposed solutions is presented in [43]. The survey of proposed solutions also reflects the readiness and maturity for applicability in industry. For increasing the users' safety and comfort a large number of applications have been developed but on the other hand these advanced applications pose new security threats.

Furthermore, Avatefipour et al. [44] presented a survey for describing the current limitations of CAN-bus protocol. They discussed the various different solutions for ensuring the secure communication thereby overcoming the CAN bus limitations. Additionally, a survey of attack scenarios and corresponding solutions for CAN bus is described in [45]. The survey presented the security vulnerabilities in detail owing to absence of authentication and encryption schemes for CAN bus. The survey reflected the fact that transition in technological development of automotive industry is primarily based on the CAN without considering the security factor carefully. Tomlinson et al. [46] presented the survey for CAN intrusion detection. The survey discussed the several methods for intrusion detection while considering all challenges in terms of requirements and practicability. Huynh et al. [47] reviewed several approaches for the protection of automotive applications. The main aim is to recognize the potential gaps for further improvement in performance of automotive applications. Intrusion detection systems are considered as prominent solution for protecting the CAN bus from malicious attacks.

Young et al. [48] presented a very deep survey on IDS approaches. In [49], a detailed survey of security mechanisms is presented with focus on specifically on cryptography and IDS. Wu et al. [50] presented the characteristics and constraints for designing the intrusion detection system (IDS). The detailed survey consists of the several different proposed IDS designs with corresponding limitations. Lokman et al. [51] demonstrated the deep analysis on IDS approaches. For this deep analysis, specific criteria are considered such as statistics, machine learning, frequency, and hybrid model. Bozdal et al. [52] provided the detailed outlook on security issues for CAN bus. They also presented the security vulnerabilities along with attack surface and appropriate corresponding different solutions. In [53], a review is presented with focus on three-layer security framework. The three layers considered are control, communication and sensing level. A detailed analysis is conducted considering attack perspective on security frameworks with focus on enhanced user reliability. Sun et al. [54] presented a broad survey on the security issues and challenges. The survey further illustrates corresponding defense approaches for ensuring security. Karopoulos et al. [55] presented complete survey on in-vehicle IDS. All existing in-vehicle IDS are analyzed and further classified. This paper presents the detailed analysis of security mechanisms on in-vehicle communications.

5.2. Security Threats to In-Vehicular Protocols and Countermeasures

Classification of automotive protocols and possible security threats are illustrated in Figure 9. This classification is used as based on further discussion in this subsection.

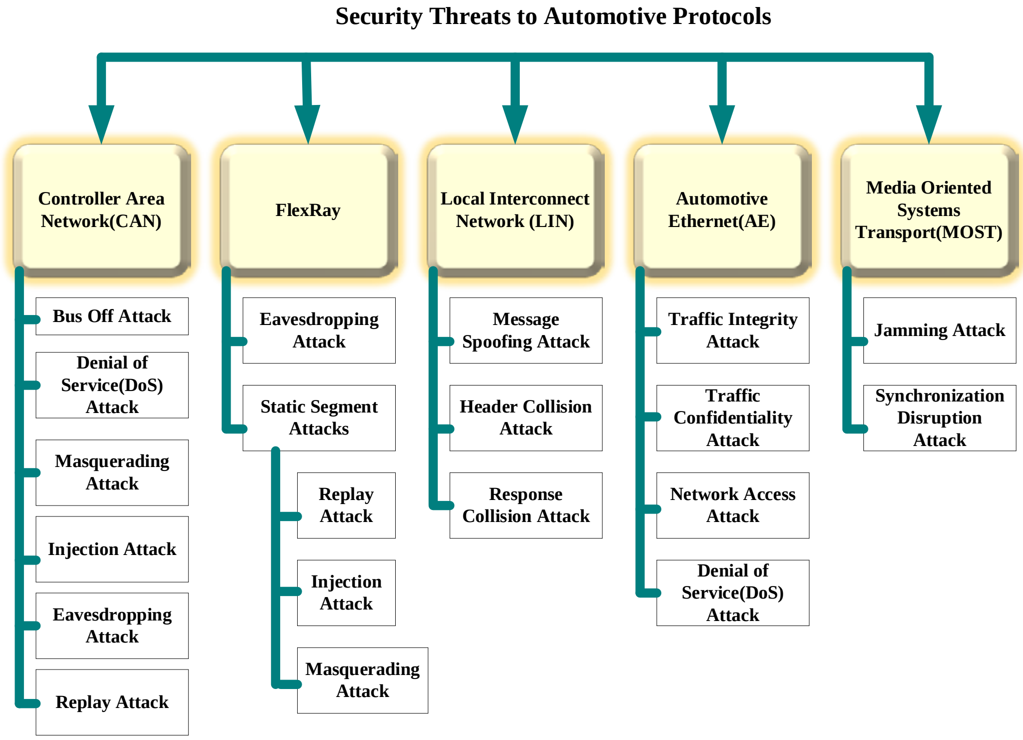


Figure 9. Classification of automotive protocols and possible security threats.

5.2.1. CAN-Centric Security Threats

Research reports reported on six types of attacks on CAN bus systems, namely bus-off attacks [56], denial of service (DoS) [57], masquerading, injection, eavesdropping, and replay attacks [58]. The attackers may get knowledge of the CAN frame since CAN frames are generally not encrypted and fail to support message authentication thereby attackers may get entry to the network easily, this type of attack is known as a Masquerading attack. Additionally, the broadcasted vehicular CAN messages may be eavesdropped on by the attackers and subsequently, they may break into the in-vehicle networks, this type of attack is known as an eavesdropping attack. Next, the attackers may try to place false signals in the bus system of the vehicle. Through OBD-II ports, the attackers may successfully establish a connection with the in-vehicle system and consequently may try to compromise the ECUs, this type of attack is known as an injection attack. Further, the vehicle's operation in real-time may be hindered by the attacker by constantly re-sending the legitimate frames, this type of attack is known as a replay attack. Furthermore, the attacker may constantly send bits in the identification field and other fields also. This type of attack is known as a bus-off attack. Besides, the attacker may disrupt the normal processing of the in-vehicle communication by constantly delivering the CAN packet with high-priority that block valid packets of low-priority and may take control of the vehicle, this type of attack is known as a DoS attack. The first general guideline to guard against these attacks is to use encryption and authentication of the messages exchanged between ECUs [59].

Survey of Security Solutions Based on Machine Learning Algorithms

In today's world of wireless networks, machine learning (ML) approaches are considered as the most promising choice for handling security-related issues. Researchers are proposing solutions utilizing ML to deal with vehicle security issues. machine learning (ML) approaches have significant advantages as compared with other mechanisms, one of the main important features is to get optimal predictions about several types of attacks. Figure 10 reflects the use of machine learning model in intrusion detection.

For in-vehicle networks, Song et al. [60] designed an efficient intrusion detection framework. Time intervals-based analysis is conducted on the CAN messages in this lightweight framework. The analysis is started by capturing CAN messages from the CAR and performing message injection attacks. The significant insights have been derived in this analysis as attacks on the CAN traffic can be detected by carefully deep analysis of time intervals. Results revealed the fact that this lightweight framework has not been suffering from false-positive errors while detecting all of message injection attacks. Next, Kang et al. [61] designed the deep neural network-based intrusion detection framework for enhancing the security level. From the in-vehicle network packets, feature vectors (probability-based) are extracted and DNN model is trained with these feature vectors. After training, the DNN model can easily discriminate the attack and normal packets and thereby any malicious attack on the vehicle can be identified. The detection accuracy of the proposed framework is much improved as compared to traditional AI-based systems since the parameters are initially initialized via unsupervised approach of deep belief networks (DBN).

Further, Ghaleb et al. [62] proposed machine learning-based model for misbehavior detection. To detect the misbehavior effectively, regularly new features are updated and derived representing the misbehavior, status of communication. Next, historical data consisting of both normal and attacked traffic data is utilized for training the misbehavior classifier based on feed forward and backpropagation techniques of Artificial Neural Network. Jagielski et al. [63] designed intrusion detection methods using machine learning and physical-based constraints. They provided an extensive analysis of attacks targeting the adaptive cruise control, and the local sensors, namely RADAR, LiDAR, etc. The analysis of attacks revealed the fact that these attacks have a high impact on safety, comfort, and efficiency, etc. For in-vehicle networks, Seo et al. [64] designed intrusion detection system utilizing deep learning approach. For detecting the unknown attacks, the proposed framework only utilizes the normal data. Additionally, Ferdowsi et al. [65] designed the deep reinforcement learning-based system to enhance the robustness of dynamics control for the autonomous vehicles against cyber physical attacks. Game-theoretic environment is utilized for the analysis of the vehicles' reaction to cyber physical attacks in this proposed framework.

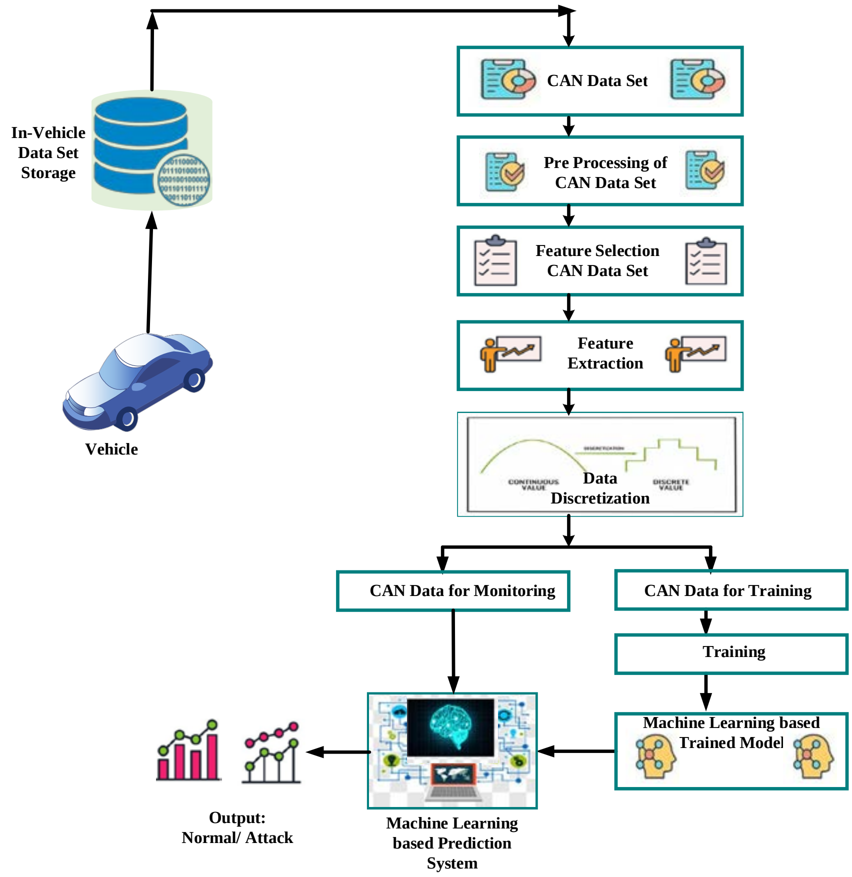


Figure 10. General Flow Diagram reflecting series of steps for intrusion detection using machine learning model.

Zhu et al. [66] designed an efficient intrusion detection framework utilizing distributed long-short-term-memory. The complexity is reduced in the detection mechanism since only binary CAN messages are utilized in this framework and thereby semantics of messages are not revealed which is a complex procedure. The proposed framework has multidimensional nature since data as well as time dimensions are taken into consideration for detection based on LSTM. The results showed high accuracy in detection. Furthermore, Eziama et al. [67] conducted a comparative analysis considering total five machine learning approaches, namely K-Nearest Neighbor, Linear and Radial Support Vector Machine, model based on Decision Tree, model based on Naive Bayes, and finally, a model based on Random Forest. To distinguish honest as well as malicious data, the recommendation system utilizes different communication nodes. The trust computation measures have been utilized to authenticate the performances of these five models, such as Recall and Precision, Receiver Operating Characteristics (ROCs).

Next, Sherazi et al. [68] proposed an Intrusion Detection framework utilizing Q-learning and fuzzy logic specifically for countering Distributed Denial of Service attacks. The simulations results attest the fact the proposed framework perform well for providing defense against Distributed Denial of Service attacks. Additionally, Khanapuri et al. [69] designed security framework utilizing convolutional neural network and deep neural network. The various sensors (RADAR, LIDAR, etc.) fitted with the smart vehicles play a major role in providing real time sensor data such as relative speed of the neighbors, as well as range, etc. These noisy sensor data are followed a Guassian Distribution and then finally utilized for training the convolutional neural network and deep neural network. Furthermore, Song et al. [70] designed a deep convolutional neural network-based effective intrusion detection framework for enhancing the protection level of the CAN bus. In the proposed framework, deep convolutional neural network model easily identifies the malicious traffic after properly learning the pattern of the traffic data. The proposed framework provides a high detection performance with significant reduction in complexity. Xiao et al. [71] proposed lightweight security framework to counter against attacks on the CAN bus through various accessing points. The proposed security framework is divided into two individual frameworks, namely simplified attention (SIMATT) framework based on the machine learning and second one known as security control unit (SECCU) framework. The use of two individual framework instead of single one reduces the computational cost significantly.

Next, Guo et al. [72] proposed security framework consisting of two parts, namely designing of context-aware trust management model as well as reinforcement learning model. The first model aimed at evaluating the trustworthiness of messages. The second model is used to select the appropriate evaluation strategy in order to ensure the high precision in evaluated results. Katragadda et al. [73] designed sequence mining methodology for detecting low-rate injection attacks in CAN. The efficacy of the proposed approach is measured by gradually changing characteristics of the attacks. Additionally, Rasheed et al. [74] proposed deep reinforcement learning-based framework for maximizing the robustness of control for autonomous vehicle. In this environment, the attacker tries to manipulate the sensor readings of the vehicle for disrupting the optimal working mechanism of autonomous vehicle on the road. By manipulating the sensor readings such as safe distance, etc., accident of autonomous vehicles may happen. Lin et al. [75] proposed effective intrusion detection framework utilizing deep learning for the three specified attacks known as impersonation, Denial of Service, and fuzzy on the CAN traffic. The proposed framework reflects good efficacy in handling premature convergence by using evolutionary optimization algorithm. The results proved the outstanding performance of the proposed framework.

Besides, Hossain et al. [76] proposed Intrusion Detection framework utilizing Long Short-Term Memory for providing protection against CAN bus attacks. First, attack free normal data is extracted from the CAR for generating the genuine data set subsequently attack data is extracted by injecting attacks. This real time genuine data set is used in training the LSTM-based model. Additionally, Angelo et al. [77] proposed an intrusion detection framework utilizing two algorithms. First algorithm aimed at learning the behavior of the traffic data while second is data-driven algorithm. These two algorithms are used to focus on real-time classification of traffic data resulting into prior alert towards the presence of malicious messages. Further, Table 2 illustrates the summary of in-vehicle security solutions based on machine learning algorithm.

From the above extensive research, we get the crucial facts such as the use of machine learning approaches are considered as prominent solution for detecting and predicting several types of attacks on in-vehicle network. Therefore, machine learning-based frameworks are used for analyzing CAN traffic effectively. The effectiveness of machine learning-based approaches is based on several factors. The first crucial factor is the pre-processing methodology adopted for pre-processing the raw CAN data. This is considered as crucial factor since no specification is provided by the automotive manufactures on decoding the raw data features. Supervised machine learning-based approaches are quite time consuming due to labelling of raw CAN data, identification and classification CAN attacks, etc. On the other hand, unsupervised machine learning-based mechanisms use data for finding the common patterns and further utilizing these patterns for classification of CAN traffic and identifying the anomalous behavior.

Table 2. Summary of characteristics of security solutions based on machine learning algorithm.

Focused Area	Algorithm Used for Detection	Adversary Model	Robustness	Strength	Weakness	Complexity Level	Accuracy in Detection (%)
CAN Bus	Time Intervals-based Framework for Analysis [60]	Denial of Service Attack	High	Lightweight IDS	No provision of Sequence Analysis	Low	>90
CAN Bus	Deep Neural Network [61]	Intrusion Detection System	High	Effective Class Discrimination	Extensive Data Set is required for learning	High	>90
VANET Applications	Artificial Neural Network [62]	Misbehavior Detection System	High	Effective Data Analysis and Feature Extraction before building Classifier	Lack of Comprehensive Detection Mechanism	High	>90
Connected Vehicle	Physical-based constraints and Machine Learning Algorithm [63]	Manipulation of Data	Medium	Collaborative Adaptive Cruise Control Attack Analysis	Unable to find dependencies in hidden states	High	90% for velocity and Position change attack
CAN Bus	Generative Adversarial Networks based on Deep Learning [64]	Fuzzy Attack, Denial of Service Attack, Spoofing Attack	High	Real time IDS for In-Vehicle Network	Lack of Efficiency in distinguishing other type of Anomalous Traffic	High	>90
Autonomous Vehicle	Long Short-Term Memory and Reinforcement Learning [65]	Cyber Physical Attack	High	Effective extraction of temporal features using LSTM	Extensive Data Set for learning	High	Not Available
CAN Bus	Long Short-Term Memory [66]	Flood Attack, Replay Attack, Spoofing Attack	Medium	Multi-Dimensional Anomaly Detection Model	Issues of Random Weight Initializations	High	>80
Machine to Machine Communication	Five machine learning approaches, namely K-Nearest Neighbor, Linear and Radial Support Vector Machine, model based on Decision Tree, model based on Naive Bayes, and finally model based on Random Forest [67]	Trust Computation	Medium	Comparative Analysis of machine learning-based trust models	Issues in finding the optimality in trust boundaries	High	Not Available
Internet of Vehicles	Fuzzy and Q-Learning [68]	Distributed Denial of Service Attack	High	Self-Learning Capability	Unable to Provide Efficient Protection Against other Types of Attacks	High	Not Available
Autonomous Vehicle	Convolutional Neural Network and Fully Connected Deep Neural Network [69]	Platoon Attack	High	Effective Performance with Time Series Classification	Scalability Issues	High	>90
CAN Bus	Deep Convolutional Neural Network [70]	Spoofing, Denial of Service, Fuzzy	Medium	Experiment is Performed on the Real Vehicle	Semantic Features are not considered for further detecting the unknown attack	High	>80
CAN Bus	Recurrent Neural Network [71]	Impersonation, Denial of Service, Fuzzy	High	Vehicle status can be monitored in real time without domain knowledge	Issues with long sequences	High	>90
VANET	Reinforcement Learning [72]	Trust Computation	High	Model for evaluating the reliability of information	Issue of overloading of states resulting into diminishing output	High	90%

Table 2. *Cont.*

Focused Area	Algorithm Used for Detection	Adversary Model	Robustness	Strength	Weakness	Complexity Level	Accuracy in Detection (%)
CAN Bus	Intrusion Detection based on Frequency Analysis [73]	Replay Attack	Medium	Model can be adaptable to different Automotive Manufacturer	No consideration about different vehicle states	Medium	Not Available
Autonomous Vehicle	Long-Term Short-Term Memory, Generative Adversarial Network, Reinforcement Learning [74]	Cyber Physical Attack	High	Model can Extract Features from huge data sets	No consideration for non-linear modelling with dynamics	High	Not Available
CAN Bus	Deep Learning [75]	Impersonation, Denial of Service, Fuzzy	Medium	Sequential Patterns Analysis for Detecting the Change in Traffic Behavior	No consideration for other Cyber Attacks	High	>80
CAN Bus	Long Short-Term Memory [76]	Spoofing, Denial of Service, Fuzzy	Medium	CAN data sets are collected from real Vehicle	Experiment is conducted in offline mode, no consideration for other unknown attacks	High	>90
CAN Bus	Cluster-based learning algorithm and Data Driven algorithm [77]	RPM Attack, Fuzzy Attack, GEAR Attack, Denial of Service Attack	High	Data driven model with classification based on unsupervised approach	No consideration about self adaptability feature and other attack types	High	>90
CAN Bus, Cloud-based IDS	Deep Learning [78]	Malware, Denial of Service, Command Injection	Medium	Mathematical Modelling and Testbed Experiment on Robotic Vehicle	No consideration against physical jamming threat	High	>85
CAN Bus	Deep Learning [79]	Replay, Spoofing	High	Experiment is conducted on the real data acquired from the physical vehicle	No Comparative Analysis with other Deep Learning Schemes	High	>95
CAN Bus	Deep Contractive Autoencoders [80]	Fuzzy, Impersonation, Denial of Service	Medium	Three different Vehicles are utilized for AN Data Collection and Discriminating the Anomalies.	Lack of Efficiency in distinguishing other type of Anomalous Traffic	High	>90
CAN Bus	Machine Learning [81]	Spoofing, Denial of Service, Fuzzy	High	Simulation is performed on the real data collected from licensed vehicle	Support Vector Machine underperform with more noisy data set	High	>90
CAN Bus	Long-Term Short-Term Memory and Recurrent Neural Network [82]	Spoofing	High	Authentication based on finger print signals	No provision for optimization of FPGA Accelerator	High	>95
Internet of Vehicles	Deep Transfer Learning [83]	Flooding, ARP, Impersonation	High	For New Attack type, Model can update without any labelled data requirements	Issue of Negative Transfer	High	>90
CAN Bus	Machine Learning [84]	Denial of Service	Medium	High Search Ability and Avoidance of Premature Convergence	No consideration for other Cyber Attacks	High	>90
CAN Bus	Long Short-Term Memory and Convolutional Neural Network [85]	Replay, Denial of Service, Fuzzy, Spoofing	High	Model is verified with automatic vehicle data sets	No consideration for other attacks types	High	>90

Survey of Security Solutions Based on Cryptography Techniques

Cryptography algorithms are used to counter the diversified cyber-attacks on the in-vehicle network of smart vehicles. Several security frameworks have been proposed using cryptography algorithms. The hackers are using real time latest advanced techniques to attack on the vehicles and therefore, no standard security framework is available with guaranteed resolutions for latest threats. Researchers are using new advanced cryptographic algorithms in designing security framework to provide protection to CAN bus and thereby protecting the data frames from manipulation. Figure 11 depicts the general asymmetric approach used in securing the vehicle-to-vehicle communication.

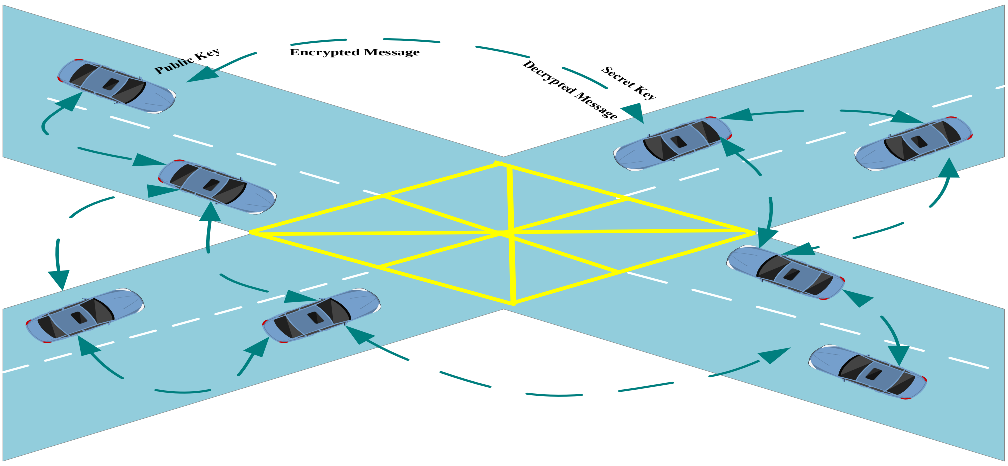
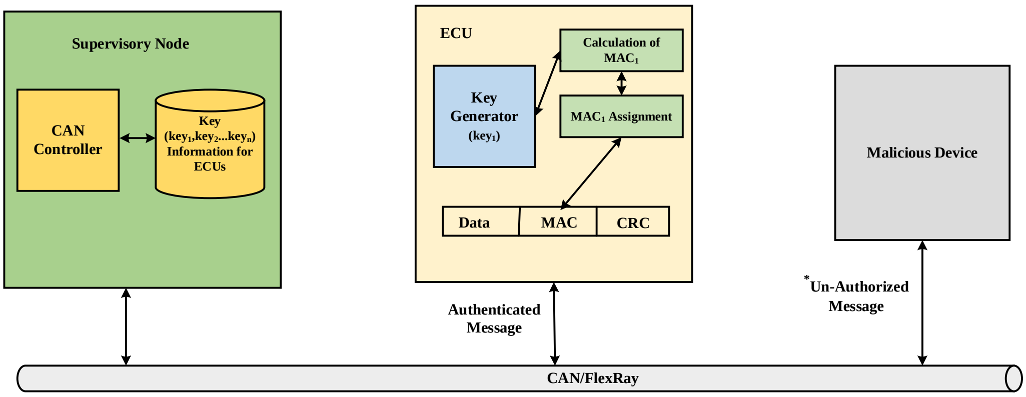


Figure 11. Use of general asymmetric cryptography approach for securing vehicle to vehicle communication.

Nilsson et al. [86] proposed a data authentication framework for modification and injection attacks. The proposed data authentication is known as delayed authentication since MAC is derived on a compound of successive messages and sent with other subsequent messages. Next, Herrewege et al. [87] explored the implementation issues of the message authentication protocol for CAN bus. After successful investigation, they find out various constraints which are related with backward compatible message authentication protocol and presented a new message authentication protocol in order to address the existing constraints. Additionally, Hazem et al. [88] designed a new protocol known as message source authentication protocol. The proposed authentication protocol performs well with minimum overhead. The implementation of the proposed protocol does not require neither any modifications in hardware for CAN network nor any changes in existing CAN message sets. Further, Groza et al. [89] utilize symmetric primitives for designing the authentication protocol having two main mechanisms, namely mixing of MAC and splitting of keys. In the proposed protocol, authentication keys are split among multiple groups of nodes results in progressive authentication as compared with traditional approach of authentication for each node independently.

In [90], several different methodologies are presented for preventing the unauthorized data transmission thereby increasing the security level in CAN and in [91], protocol is presented to counter against DoS attacks. Additionally, a secure channel is provided by the proposed protocol between external devices and in-vehicle network components. The proposed protocol consists of two main authentication processes, namely checking the authenticity of transmitter and data validation through message authentication. Further in [92], a centralized framework is presented for CAN with enhanced CAN controller. The monitoring system in the proposed centralized framework utilizes a message authentication code. The mechanism starts by authenticating each ECU in the bus by a node and then message authentication codes are reviewed which are assigned to messages being transmitted in the bus. Figure 12 illustrates the working of centralized framework in detail.



*Supervisor node detects the un-authorized message in the network and immediately destroy it.

Figure 12. Centralized framework consisting of Supervisory Node [92].

Next, in [93], an advanced framework is proposed which is based on runtime verification to provide security against several attacks on CAN. The proposed framework uses copilot method for performing run time detection. Additionally, in [94] a CAN authentication protocol is presented for providing immunity against attacks. The proposed lightweight authentication protocol is effective against a DoS attack. The proposed authentication protocol has three main stages and through these stages all weak points are addressed to provide secure and robust environment for CAN. Further, authors in [95] designed a security framework for providing security in CAN. For the security of transmitted messages, the proposed framework utilizes a truncated MAC. Additionally, in a data frame, it utilizes a segment of MAC. Therefore, the proposed framework is using two different mechanisms to secure the CAN against malicious attacks. The results attested the fact that the proposed framework effectively handle the replay and tampering attacks. Furthermore, new methodology based on cryptographic techniques is presented in [96] for increasing security in CAN. The proposed lightweight framework uses stream cipher to encrypt messages while protection against external attacks is provided through a key management mechanism. The results shown that the proposed framework is characterized with two main features such as minimum memory requirements as well as high efficiency as compared with other MAC-based schemes. Further Table 3 illustrates the summarized key points of literature representing security solutions based on cryptographic techniques.

From the above extensive research, we get the crucial facts such as the use of cryptography approach against security threats to in-vehicle network has all potential advantages except that the CAN bus controller requires additional computational resources. Generally, there are two main components in the Cryptography approach. First is known as Message Authentication Code (MAC) and another is called as cryptosystems having two fields symmetric and asymmetric. Further, Integrity and Authentication is ensured by the MAC while confidentiality is provided by the symmetric and asymmetric cryptosystems. Additionally, session keys can be utilized for providing authentication. For vehicle safety, the load on the CAN bus and latency issue in response time should be within specified limit. Additionally, error detection in data frame transmission is provided by the Cyclic Redundancy Code (CRC) at CAN bus. ECUs are having their own limitations in terms of computational capacity thereby lightweight encryption is one of the solutions for handling this issue since ECUs are core components inside the vehicle handling various functions simultaneously. The bus may be heavily loaded during key exchange and pre-loaded keys in the ECUs can tackle this situation in key distribution environment. The Hardware Security Module (HSM) in ECUs can be effectively utilized for performing encryption and decryption in optimal time and compensating the issue of resource constrained ECUs. Although several significant developments towards security framework based on cryptography algorithms can be seen but cost factor in successful implementation of these schemes cannot be ignored.

Table 3. Summary of characteristics of security solutions based on Cryptographic techniques.

Focused Area	Strength	Approach/Methodology	Weakness	Adversary Model	Key Aspects
CAN Bus	Delayed Data Authentication for avoiding disruption with real time traffic	CBC-MAC [86]	No provision for MAC calculation with diversified compound sizes	Spoofing, Injection	1. The proposed scheme utilizes compound message authentication codes for delayed data authentication. 2. In this scheme, on a compound of successive messages, message authentication code is calculated.
CAN Bus	Backward Compatibility, no need to modify existing nodes	Counters, HMAC, Symmetric Key [87]	All nodes must know about pre-shared key before verifying the messages	Replay, Sniffing, Injection, Spoofing	The proposed scheme utilizes HMAC in designing lightweight authentication protocol.
CAN Bus	The proposed protocol can be practically deployed in the vehicle without hardware modification	Session Keys, Magic Number [88]	Issues in exchange of authentication data owing bandwidth limitations	Injection, Replay	A lightweight authentication protocol is proposed to CAN bus.
CAN Bus	Source authentication is effectively managed	LMAC, MD5 [89]	The proposed scheme works well with only lower number of nodes	Injection, Replay	In the proposed scheme, authentication protocol is designed utilizing MAC mixing and key splitting mechanism.
CAN Bus	Proposed solution is software-based and can be easily applied	Secret Keys (Symmetric Pair wise) and MAC [90]	No comparative analysis is provided for testbed experiment	Replay, Masquerade	1. Different parameters are used to design the scheme, namely MAC ID, Secret Keys. 2. Transmitter and Receiver use shared secret key.
CAN Bus	Provide Secure channel for vehicle to external communication	CRC, MAC [91]	No comparative analysis is provided for other types of attacks	Denial of Service	Designing of new secure protocol for CAN.
CAN Bus	The proposed centralized security scheme is verified with FPGA board	HMAC, SHA-256 [92]	No comparative analysis is provided for key exchange environment	Spoofing	In the proposed scheme, central authentication framework is designed.
CAN Bus	The proposed scheme authenticate ECU with provision of session keys establishment	Session Keys, ECC, HMAC [93]	AVISPA tool is used for Security Validity, other platforms should be used for measuring the efficacy	Authentication of ECU in CAN for providing protection against attacks	1. The proposed scheme utilizes the ECC. 2. In the adapted protocol, elliptic curves are implemented with variety of different parameters.
CAN Bus	Simulation is performed using Vector Canoe.	Authentication (Lightweight) [94]	No comparative analysis is provided for other types of attacks	Denial of Service	A new CAN authentication protocol is proposed.
CAN Bus	The proposed scheme utilize two different MAC methods.	Key Management, MAC [95]	No comparative analysis is provided for other types of attacks	Replay, Tampering	A new message authentication-based protocol is proposed for CAN.
CAN Bus	The proposed scheme requires less memory and speed is high	SHA, RC4, AES-128 [96]	No comparative analysis is provided for other types of attacks	Flood, Replay, Masquerade, Eavesdrop, Brute-force	For authentication and encryption, a new lightweight protocol is proposed for CAN bus.
CAN Bus	Proposed scheme has high compatibility with existing architectures and testbed experiment is performed	Symmetric Key, HMAC, Trusted Group [97]	No comparative analysis is provided for other types of attacks	Injection, Sniffing, Spoofing	A practical framework is proposed for solving issue of message authentication.
CAN Bus	The proposed scheme has built in fault detection mechanism	CRC, Lightweight Stream Cipher [98]	No comparative analysis is provided for other types of attacks	Masquerade	1. Proposed scheme utilizes CRC for finding bit errors if any. 2. CAN Data frame part is encrypted using light weight stream cipher.
CAN Bus	The proposed security scheme provide secure environment for CAN-FD and performance is evaluated with microcontrollers and oftware	SHA-256, AES-128, HMAC [99]	No comparative analysis is provided for other types of attacks	Spoofing, Sniffing, Replay	A security architecture is proposed for developing secure communication environment for CAN-FD.
CAN Bus	Backward Compatibility, no need to modify existing nodes	Counter, MAC, 128-bit key [100]	No comparative analysis is provided for other types of attacks	Spoofing, Replay, Injection	An authentication protocol is proposed in which ECUs are allowed to authenticate each other.

Table 3. *Cont.*

Focused Area	Strength	Approach/Methodology	Weakness	Adversary Model	Key Aspects
CAN Bus	Message authentication for CAN bus with the presence of existing constraints	SHA1, HMAC [101]	No comparative analysis is provided for other types of attacks	Replay, Denial of Service	In the proposed scheme, time stamp as well as HMAC are used for the message authentication.
CAN Bus	The proposed scheme can change the encrypted messages frequently	Symmetric Key (Dynamically Managed) [102]	No comparative analysis is provided for other types of attacks	Replay	1. In the proposed scheme, payload data is encrypted using symmetric key. 2. Key generators are used to dynamically changing the symmetric key.
CAN Bus	The proposed security framework is hardware-based	PUFs, ECDH [103]	No comparative analysis is provided for other types of attacks	Spoofing, Eavesdropping	1. In the proposed scheme, ECDH is utilized. 2. In this scheme shared key is not stored.
CAN Bus	The proposed security model block the compromised data on the receiver as well as sender side simultaneously.	Blacklisting, MAC, Whitelisting [104]	No comparative analysis is provided for other types of attacks	Denial of Service, Man in the Middle	1. A hardware-based security framework is designed. 2. For secure booting, trusted hardware modules are used.
CAN Bus	The proposed scheme is evaluated on several embedded systems environment	128-bit key, ChaskeyMAC, Pre-shared [105]	No comparative analysis is provided for other types of attacks	Spoofing, Replay	An authentication protocol is proposed for CAN-FD, utilizing ChaskeyMAC.
CAN Bus	In the proposed scheme CAN ID is shuffled using NAS frequently.	HMAC, AES-128, SHA-256, Shuffling-CAN ID, AKEP-2 [106]	No comparative analysis is provided for other types of attacks	Replay, Impersonation	In the proposed scheme, attack surface is dynamically shuffled using one time Id.
CAN Bus	Communication security is provided by group-based approach, effective group key management	Keys (Public andPrivate), Gateway-ECU [107]	No comparative analysis is provided for other types of attacks	Spoofing, Sniffing, Replay	A new security architecture is proposed in which Gateway-ECU is used for communication among ECUs.
CAN Bus	Experiment is conducted on real hardware.	GHASH, AES-128 [108]	Delay Issue, no comparative analysis is provided for other types of attacks	Sniffing, Replay, Spoofing	In the proposed scheme, encrypted CAN frames are assigned several different priorities for handling the increased delay in the system.
CAN Bus	The proposed scheme does not require any changes to existing hardware.	AKEP2, MAC, Session Keys [109]	No comparative analysis is provided for other types of attacks	Denial of Service, Masquerade, Bus-Off	A new authentication protocol is proposed. No need of any hardware modifications.
CAN Bus	Design optimization is performed in the proposed scheme for ensuring time critical execution of applications	HMAC 64 bits, Key distribution process based on Diffie-Hellman [110]	No comparative analysis is rovided for other types of attacks	Denial of Service, Injection, Replay, Impersonation, Bus off	The proposed scheme uses HMAC for ensuring security on CAN bus.
CAN Bus	Sender nodes are authenticated using software-based mechanism	AES-128, MAC [111]	No comparative analysis is provided for other types of attacks	Concatenation, Injection, Replay	The proposed scheme utilizes the ordered CMAC buffer for authenticating the CAN frames ID.
CAN Bus	The proposed scheme has two significant contributions, namely sender authentication and effective key management	MAC, Session Keys [112]	No comparative analysis is provided for other types of attacks	Replay, Impersonation	The proposed scheme is characterized with two features, namely authentication of the sender as well as management of keys.
CAN Bus	Overhead of CAN communication is reduced significantly by mixing diversified authentication tags.	SHA-256, MAC, Symmetric Key Cryptography, Bloom Filters [113]	No provision of key distribution and no comparative analysis is provided for other types of attacks	Replay, Man in the Middle	In the proposed scheme, CAN bus data authentication is carried out with the help of Bloom Filters attributes.
CAN, Automotive Ethernet	Mutual identity authentication is provided to all communication parties and session key confidentiality is effectively managed	Symmetric Cryptography, Session Keys, AEAD Algorithm [114]	No comparative analysis is provided for other types of attacks	Eavesdropping, Replay, Man in the Middle, Masquerade	The proposed scheme is featured with efficient authentication as well as secure communication. Session keys are updated regularly.

5.2.2. Security Threats—FlexRay

Eavesdropping [115] and static segment attacks [116] are the two main types of threats in FlexRay. In the case of the former type of attack, FlexRay messages are accessed by the attackers and consequently, the attacker can obtain all the critical information. This attack results in leakages of data, impact on data confidentiality, and also security concerns. In the case of later types of attack, the communication cycle of FlexRay having a static segment is attacked. This attack also includes replay, injection, and masquerading types of attacks. The preventive mechanism for both these types of attacks consists of the implementation of an advanced scheme for authenticating the message within the static segment [117]. Timed Efficient Stream Loss-tolerant Authentication (TESLA) [118] is the authentication protocol.

5.2.3. Security Threats—Local Interconnect Network (LIN)

Three attacks usually occur to LIN, namely message spoofing [119], header collision, and response collision attacks. In the message spoofing attack, the attacker tries to interrupt vehicular communication by sending false unauthorized messages with the only objective of shutting down LIN. This attack is caused by the vulnerabilities in the master-slave model of LIN. In the collision response attack, the hacker tries to exploit the error handling protocol of LIN. In this attack, along with a valid message, the attacker sends an illicit message consisting of a false header concurrently. Consequently, the message transmission is stopped by the legitimate slave node immediately, whereas illegitimate messages will be accepted by all other nodes. In the header collision attack, the hacker tries to create a conflicting situation. The attacker sends an incorrect header to create a conflicting situation since a valid header from the master node is also present in the system. According to the valid header, the response should be released by the specified slave node, on the other hand, an incorrect header states that the changes occur in the source node. This attack may create several life-threatening unwanted functions for the example steering wheel of the vehicle can be locked while the vehicle is driving on the road, opening the sliding doors of the vehicle and much more, these functions not only cause threats to the life of passengers but also damage the overall vehicle. In the corrective mechanism against these types of attacks, the slave node can send unusual signals for overwriting the fake messages of the hacker whenever the value of the bus mismatches from its response [120].

5.2.4. Security Threats—Automotive Ethernet (AE)

Four types of attacks usually occur to Automotive Ethernet such as traffic integrity, traffic confidentiality, network access, and DoS attacks [121]. In the network access attacks, the hacker first establishes a connection with the unsecured port of the switch and then via this connection hacker tries to connect to the Ethernet network. The ultimate objective of the attacker is to get access to the network and subsequently take control over several different nodes or control the network remotely. In the traffic confidentiality attacks, the attacker first gets access to the network and then he attacks the network and tries to overhear activities in the network. The traffic integrity attacks can be considered similar to attacks as a man-in-the-middle. In this type of attack, information is exploited by diverting the traffic towards the compromised node. There are two types of these attacks, namely session hijacking as well as replay attacks. DoS attacks are classified into two categories in Ethernet. In the first category of DoS attack, the attacker tries to disrupt the Ethernet infrastructure and convert it totally into an unusable form. In this attack, the attacker first physically destroys links or hardware. Next, the second category of DoS attack is also known as resource depletion attacks or protocol-based DoS attacks. In this attack, the attacker constantly submits frames for analysis in order to waste energy. The corrective mechanism should consider the authentication, and frame replication along with the virtual local area network segmentation scheme [122].

5.2.5. Security Threats—Media-Oriented Systems Transport (MOST)

Two types of attacks which are generally occurred to MOST, namely jamming and synchronization disruption attacks. In the synchronization disruption attacks, the hacker tries to tamper with the synchronization of MOST by sending the fake timing frames continuously. In jamming attacks, the hacker tries to interrupt low-priority legitimate messages having specified length by continuously delivering misleading messages. Additionally, the hacker may continuously request data channels on MOST transmission via control channels. The corrective mechanism has three main approaches such as source node authentication, exchanged messages should be encrypted, and strict enforcement of firewalls and gateway [123].

6. Multi-Layered Security Framework

The modern advanced vehicles have complex and sophisticated in-vehicle architecture. Additionally, these vehicles are equipped with highly sensitive sensors, different electronic devices, computer systems, etc. in order to secure these sophisticated systems, a coordinated, systemic integrated cybersecurity framework is needed to design the solutions and to minimize security risks. For the cyber security of in-vehicle networks, a multi-layered approach is the need of the hour. We need an integrated security approach since hackers invade vehicles through cyber and via the physical world. Further, Figure 13 illustrates the multi-layered security framework for in-vehicle networks with corresponding automotive protocols. In the context of scientific novelty, it is highlighted that the multi-layered security framework is proposed based on the findings of critical investigation of existing literature. Each layer addresses a specific type of security threat for in-vehicle communication network. It is highlighted that the multilayer security framework is proposed based on the understanding and knowledge aided by critical analysis and findings of existing approaches for the security of in-vehicle network. We found that the literature is lacking in terms of cohesive multi-layer security framework for in-vehicle network. In this framework, we addressed different security issues of in-vehicle network in specific layers including ECU-boot level security, ECU to ECU communication, domains/sub-domains communication, application software update or version issues, gateway security controller, and vehicle to outside services.

However, it is clarified that in the proposed integrated multilayer security framework, each layer ensures specific functionality and address security threats. This is the reason we divided the framework into six layers staring from ECU-boot level security, ECU to ECU communication, domains/sub-domains communication, application software update/version issues, gateway security controller, and finally in-vehicle network to vehicle outside services security issues. In the Secure Gateway/Domain Controller layer, we are more concerned about security of gateway while at the secure external communication layer, we have a priority to protect the communication channels. In terms of in-general functional roles all automotive protocols are somehow or other play role in all layers due to complex structuring of modern in-vehicular system. However, if we make deep analysis based on maximum effectiveness of automotive protocols in terms of providing functionality to domain/sub-domain of in-vehicular system, then we can identify which specific automotive protocol is more suitable to a layer. Therefore, we used a protocol for a layer with more effective and suitable functionality consideration in mind while developing the framework.

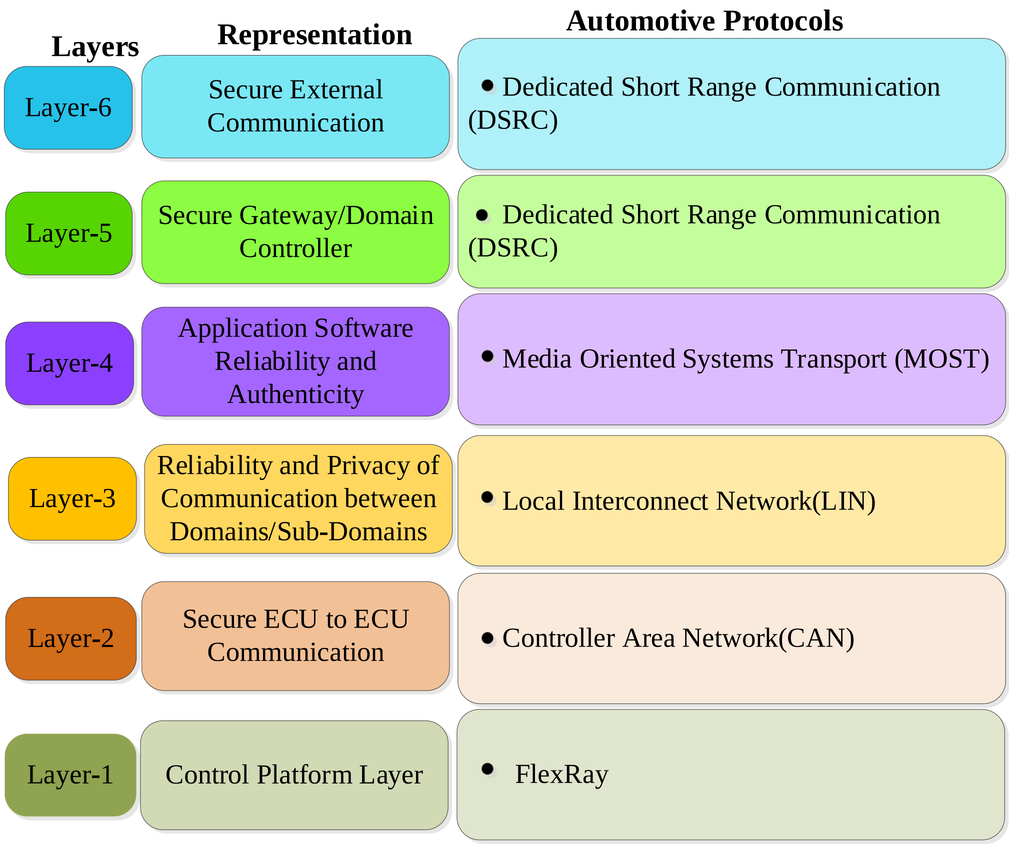

Layers
Representation
Automotive Protocols
Layer-6
Secure External Communication
• Dedicated Short Range Communication (DSRC)
Layer-5
Secure Gateway/Domain Controller
• Dedicated Short Range Communication (DSRC)
Layer-4
Application Software Reliability and Authenticity
• Media Oriented Systems Transport (MOST)
Layer-3
Reliability and Privacy of Communication between Domains/Sub-Domains
• Local Interconnect Network(LIN)
Layer-2
Secure ECU to ECU Communication
• Controller Area Network(CAN)
Layer-1
Control Platform Layer
• FlexRay

Figure 13. Multi-layered Security Framework for in-Vehicle Network.

6.1. Control Platform Layer

This layer aims at enhancing the security of platform. This layer can be assumed as vehicle main nerve center for securing the in-vehicle network of smart intelligent vehicle against malicious threats. Control layer aspect deals with security solutions for protecting firmware of ECU, enhancing security at booting level, and also security of hardware modules (HM). The original equipment manufacturer (OEM) trusted server and trusted platform module (TPM) chip at ECU play a major role in this mechanism. The secure connection is effectively maintained between these two modules for the exchange of encrypted firmware update image file and data for enhancing security at booting level, ECU firmware, etc. The ECU firmware should be updated frequently to counter the diversified attacks in current advanced technological automotive era. Further, authenticity of ECU firmware update can be verified via signing/secure flashing mechanism.

6.2. Secure ECU to ECU Communication in In-Vehicle Network

This layer ensures message delivery with integrity proof between ECUs. The hackers are targeting a large volume of sensitive information which is actually generated by The ECUs. The security mechanism should ensure the reliability, confidentiality, and integrity of this sensitive information. A hardware security module (HSM) chip should exist in the modern in-vehicle network that work as security controller. The security controller has three main modules, first module is responsible for ECU id authentication and ECU state verification, second module handles encryption/decryption of messages exchanged and third module control the secure flash storage. All messages from the ECUs should be forwarded to HSM chip (security controller). The security controller will analyze the messages and identify the destination ECU. Based on the state of the destination ECU and message security properties, it decides whether the message should be forwarded to the destination ECU or not.

6.3. Reliability and Privacy of Communication between Domains/Sub-Domains in In-Vehicle Network

This layer ensures the reliability and privacy of communication between domains/sub domains in the vehicle. A vehicle domains/sub-domain reflects the grouping of functions and systems with respect to specified areas, for example telematics domain, infotainment domain, chassis domain, powertrain domain, sensor domain, and body domain, etc. This layer protects the domains/subdomains by using four security mechanisms as follows:

○ Message authentication system: Cryptographic certificate is used to ensure an authenticated sender and message integrity. This certificate is added to all messages in the network.

○ Encryption: Messages are encrypted inside the vehicles to guard against loss of data and identity theft since messages are distributed with several different ECUs.

○ Detection of intrusion: The corrective mechanism should use the cryptographic accelerators and security subsystems integrated with the microcontroller to guard against threats.

○ Validation at ECU level: In the vehicle network, ECU's validity is checked first at the start of the engine and also afterwards at specified time intervals.

6.4. Application Software Reliability and Authenticity

All application software should ensure reliability and authenticity qualities. The hackers are using software download/update features for attacks. The secure mechanism immediately updates the vehicle software whenever any security vulnerabilities is detected. The application software is generally developed by the third-party manufacturer and verified software file image is sent to original equipment manufacturer (OEM) trusted server for uploading. The software update manager module at OEM trusted server sends notification to vehicle owner for the availability of updated software version. After confirmation from the vehicle owner, the updated software version is installed in secure in-vehicle network storage area. In this entire mechanism, security of channels is a prime concern. There are various techniques exists for enhancing the security of channels, namely hash function, digital signatures, blockchain technologies, etc. Additionally, for verifying the trustworthiness of the encryption mechanism, modern advanced microcontrollers have features such as integrity testing in real time, etc.

6.5. Secure Gateway /Domain Controller

This layer ensures the security of gateway/domain controller. All modern critical gateways must be equipped with next generation advanced security mechanisms such as advanced key management schemes/firewalls, intrusion detection schemes, etc. The main responsibility of the gateway is to maintain the secure configuration of the system. Context-aware routing is implemented by the gateway, in this routing mechanism, the gateway checks the validity of the messages, and all valid messages are permitted to transfer via the gateway to the corresponding destination through a different number of complex controls. The automotive manufacturers are working towards designing robust and secure gateway controller module. The cryptographic credentials are stored in the secure hardware extension (SHE) chip which is the part of secure gateway controller module. The main role of SHE chip is to protect the cryptographic credentials from the hackers. The public key infrastructures (PKI) of various communication service providers manages the cryptographic credentials inside the SHE chip.

6.6. Secure External Communication

This layer ensures secure communication from in-vehicle network to various services outside the vehicle. This layer provides authentication and message validation functionality for protecting message integrity and thereby protecting the communication channels from data manipulation and data theft. Due to these features, vehicle-to-everything communication, telematics, etc. are secured. All communications from in-vehicle communication stack to roadside unit (RSU) must be established via trusted communication authority (TCA) for providing authentication and message validation. Certificates which are used during communication between in-vehicle communication stack and TCA, further between TCA to RSU should be changed frequently for maintaining the integrity of the sender. Additionally, the integrity of the message content can be protected with the help of digital signature.

7. Open Challenges and Future Research Directions

The rapid development in vehicular communication paves the way for more threats. There is an urgent requirement for the development of security mechanisms to counter these threats. The diverse cyber-attacks on in-vehicle network of smart vehicles may lead to damage to the vehicle as well as possible loss of life. All stack holders should consider the security of in-vehicle networks a high priority. The below section will discuss in detail various challenges and future research directions for in-vehicle network security aspects [124,125]. Figure 14 illustrates the open challenges for in-vehicle network.

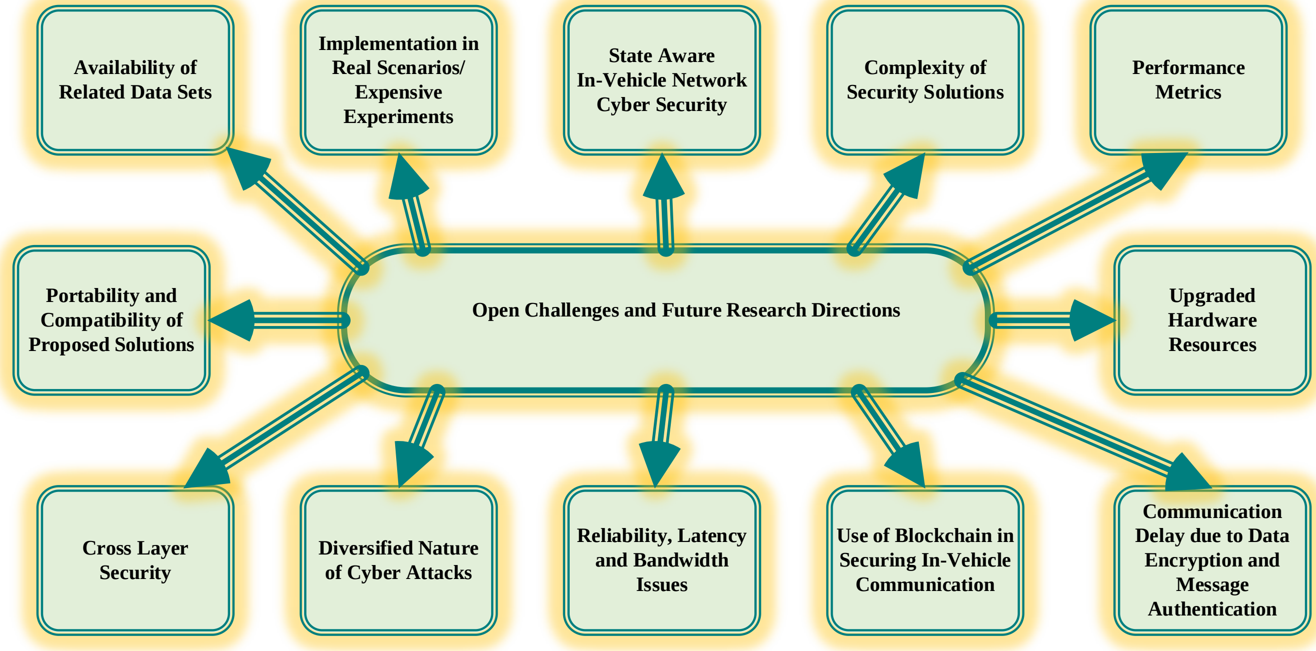

Availability of Related Data Sets
Implementation in Real Scenarios/ Expensive Experiments
State Aware In-Vehicle Network Cyber Security
Complexity of Security Solutions
Performance Metrics
Portability and Compatibility of Proposed Solutions
Open Challenges and Future Research Directions
Upgraded Hardware Resources
Cross Layer Security
Diversified Nature of Cyber Attacks
Reliability, Latency and Bandwidth Issues
Use of Blockchain in Securing In-Vehicle Communication
Communication Delay due to Data Encryption and Message Authentication

Figure 14. Open challenges for security of in-vehicle network.

7.1. Availability of Related Data Sets

The impact of advanced research on the security of vehicles depends on the genuine real-time data sets containing message semantics for experimentation. Unfortunately, the availability of related genuine datasets is the main constraint in advanced research. The CAN bus datasets are the intellectual property of particular automobile manufacturers and therefore these data sets are not available publicly for experimentation. The possible solution to this issue is a collaboration between automobile manufacturers and the researcher. Further, data frames in the in-vehicle networks are generated in milliseconds therefore labelling of data is a complex issue. Although predefined attacks are identified by supervised learning, we have to focus on developing security solutions having the capability of handling new and diversified attacks [124].

7.2. Implementation in Real Scenarios/Expensive Experiments

The research advancements for countering cyber-attacks on smart vehicles should be implemented in real scenarios for achieving optimum results. However, the implementation of research solutions in real scenarios has various limitations. A researcher cannot afford to buy a car for conducting experiments. The seamless solution in these circumstances is collaborative efforts between research organizations and automotive manufacturers [125].

7.3. State Aware In-Vehicle Network Cyber Security

Some security approaches do not consider the different vehicle states. Therefore, the efficacy of the security approaches is only limited to specified vehicle states. The security mechanisms should be robust in nature with higher coverage to different vehicle states [116].

7.4. The Complexity of Security Solutions

Researchers are proposing a variety of security solutions based on AI/machine learning, neural network, cryptography, etc. The performance of the proposed security solutions can be increased by combining different backbone techniques used in developing security solutions. Several vibrant factors can be considered while developing security solutions such as computational requirements in the proposed security solution should be low [117].

7.5. Performance Metrics

The performance of the security solutions can be observed concerning a variety of metrics such as accuracy, recall, precision, F-score, etc. The proposed security solutions should have improved false-positive percentages for detecting attacks. In the real-world scenario, there is a need of developing security solutions having autonomous actions in terms of indicating and mitigating attacks [118].

7.6. Portability and Compatibility of Proposed Solutions

The proposed security solutions should have portability and compatibility features, this can be achieved by testing the performance of the proposed security solutions in real-time scenarios. The proposed security solutions should also qualify for the minimum standard mark as per the cyber security standards [119].

7.7. Upgraded Hardware Resources

The advanced security solutions need upgraded hardware resources used on in-vehicle networks. There is a need for scalable hardware resources in in-vehicle networks for supporting new functionality. Research is going on developing next-generation ECU's and gateways for identifying the suspicious messages and thereby stopping the transmission of these fake messages. In the network [120].

7.8. Cross-Layer Security

The advanced security solutions are more efficient enough than the traditional approaches since they focus on cross-layer security for providing secure data communications for in-vehicle networks. The traditional security solutions either focus on physical layer or application layer security which is why their efficiency is limited [121].

7.9. Diversified Nature of Cyber Attacks

Researchers are now working on developing security solutions to counter as many attack patterns as possible. The rapid development of smart vehicles gives rise to advanced security issues as well. The next-generation security solutions will protect against manipulation of CAN frame semantics [122].

7.10. Use of Blockchain in Securing In-Vehicle Communication

Future research directions towards securing CAN bus of in-vehicle networks should include blockchains. Blockchain technology is new technology and has the capability to combat cyber-attacks. Blockchain is defined as a distributed data structure. The blocks in the distributed data structure are in chronological order and chained cryptographically. The main security challenge in utilizing blockchain technology for securing in-vehicle systems is a consensus mechanism. The consensus mechanism utilized in blockchain technology will have a direct impact on the security of the system [123].

7.11. Reliability, Latency and Bandwidth Issues

Reliability is the crucial factor for optimal performance of in-vehicle networks, for example, consider the case of ADAS data transmission, if the ADAS data transmission is unreliable then it may result in damage to the vehicle and probable life hazards to passengers. Latency is another important parameter in the vehicle network. All safety components have stringent delay specifications for ensuring optimal reliability. The third important issue is bandwidth, for high bandwidth and communication efficiency additional requirements are needed in in-vehicle networks which raises several challenges [124].

7.12. Communication Delay Due to Data encryption and Message Authentication

The communication delay is directly affected by the processing capabilities of the microcontroller since data encryption and message authentication require additional computational resources. Additionally, the size of the data frame is also a crucial factor in communication delay as the transmission mechanism takes additional processing time [125].

8. Conclusions

Manufacturing of modern smart intelligent vehicles are the result of integration of communication technologies and advanced computing with automotive industries. Initially automotive protocols are designed without considering the security threats, but current scenarios require advanced security schemes for these protocols to counter against malicious attacks. The security schemes are using different technology environments such as using cryptography techniques and machine learning algorithms. For enhancing the security of in-vehicle network, several research articles have been published that have used cryptography and machine learning algorithms for designing security frameworks and still research is going on for finding optimal solutions. Cryptography techniques generally use identifiers in data frames, finding manipulations in sending time, and message authentication, etc. for enhancing the security levels on the other hand machine learning approaches are using different algorithms to design the framework and train the model accordingly with training data. There are two aspects while developing security solutions, namely transfer layer and physical layer security solutions. Applying cryptography approach at transfer layer by utilizing message authentication code, etc. is having various constraints due to the limitation of memory, computational capability, etc. Therefore, it will be good practice to choose security solutions at physical layer. Though significant improvements can be seen in current development of automotive protocols, still there are open research issues such as security against advanced attacks, bandwidth requirements, attack detection and resolution efficiency, latency, compatibility issues, and cost, etc. There is a need of designing the efficient robust security scheme which can handle various issues of automotive protocols as well provide protection against variety of security threats.

In this noble piece of research work, we presented a systematic survey covering the communication vulnerabilities of in-vehicle network, proposed security methods based on machine learning algorithms and cryptography techniques, characteristics of in-vehicle protocols, integrated multilayer security architecture of in-vehicle network, significant insights about improvement of the security level in in-vehicle communication. Finally, we provided the detailed discussions about futuristics potential research directions for securing the in-vehicle communication. Both sectors, including academia and the industry, have shown incredible concerns towards security of in-vehicle network therefore we are sure that this systematic survey will provide a strong base for the research and development team for acquiring valuable inputs regarding security challenges of in-vehicle network and designing enhanced solutions.

Author Contributions: Conceptualization, R.S.R.; Formal analysis, R.S.R.; Investigation, R.S.R.; Methodology, R.S.R.; Supervision, C.H. and O.K.; Validation, R.S.R. and O.K.; Writing, R.S.R.; and Review and Editing, O.K. and J.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Cybersecurity and Information Networks Centre (CINC) at Cardiff School of Technologies, Cardiff Metropolitan University, Cardiff, UK.

Acknowledgments: The authors thank to the support by the Nottingham Trent University, U.K.

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

References

1. Kaiwartya, O.; Abdullah, A.H.; Cao, Y.; Altameem, A.; Prasad, M.; Lin, C.T.; Liu, X. Internet of vehicles: Motivation, layered architecture, network model, challenges, and future aspects. *IEEE Access* **2016**, *4*, 5356–5373. [CrossRef]
2. Song, H.M.; Kim, H.K. Self-supervised anomaly detection for in-vehicle network using noised pseudo normal data. *IEEE Trans. Veh. Technol.* **2021**, *70*, 1098–1108. [CrossRef]
3. Kang, S.; Seong, J.; Lee, M. Controller area network with flexible data rate transmitter design with low electromagnetic emission. *IEEE Trans. Veh. Technol.* **2018**, *67*, 7290–7298. [CrossRef]
4. Lee, Y.S.; Kim, J.H.; Jeon, J.W. FlexRay and Ethernet AVB synchronization for high QoS automotive gateway. *IEEE Trans. Veh. Technol.* **2016**, *66*, 5737–5751. [CrossRef]
5. Kong, W.; Luo, Y.; Qin, Z.; Qi, Y.; Lian, X. Comprehensive fault diagnosis and fault-tolerant protection of in-vehicle intelligent electric power supply network. *IEEE Trans. Veh. Technol.* **2019**, *68*, 10453–10464. [CrossRef]
6. Zhang, L.; Yang, F.; Lei, Y. Tree-based intermittent connection fault diagnosis for controller area network. *IEEE Trans. Veh. Technol.* **2019**, *68*, 9151–9161. [CrossRef]
7. Iorio, M.; Reineri, M.; Risso, F.; Sisto, R.; Valenza, F. Securing SOME/IP for in-vehicle service protection. *IEEE Trans. Veh. Technol.* **2020**, *69*, 13450–13466. [CrossRef]
8. Choi, W.; Jo, H.J.; Woo, S.; Chun, J.Y.; Park, J.; Lee, D.H. Identifying ecus using inimitable characteristics of signals in controller area networks. *IEEE Trans. Veh. Technol.* **2018**, *67*, 4757–4770. [CrossRef]
9. Jeong, W.; Han, S.; Choi, E.; Lee, S.; Choi, J.W. CNN-based adaptive source node identifier for controller area network (CAN). *IEEE Trans. Veh. Technol.* **2020**, *69*, 13916–13920. [CrossRef]
10. Xie, G.; Yang, L.T.; Liu, Y.; Luo, H.; Peng, X.; Li, R. Security enhancement for real-time independent in-vehicle CAN-FD messages in vehicular networks. *IEEE Trans. Veh. Technol.* **2021**, *70*, 5244–5253. [CrossRef]
11. Kaiwartya, O.; Kumar, S. Cache agent-based geocasting in VANETs. *Int. J. Inf. Commun. Technol.* **2015**, *7*, 562–584. [CrossRef]
12. Moulahi, T.; Zidi, S.; Alabdulatif, A.; Atiquzzaman, M. Comparative Performance Evaluation of Intrusion Detection Based on Machine Learning in In-Vehicle Controller Area Network Bus. *IEEE Access* **2021**, *9*, 99595–99605. [CrossRef]
13. Zhang, L.; Ma, D. A Hybrid Approach Toward Efficient and Accurate Intrusion Detection for In-Vehicle Networks. *IEEE Access* **2022**, *10*, 10852–10866. [CrossRef]
14. Kumar, S.; Singh, K.; Kumar, S.; Kaiwartya, O.; Cao, Y.; Zhou, H. Delimitated anti jammer scheme for Internet of vehicle: Machine learning based security approach. *IEEE Access* **2019**, *7*, 113311–113323. [CrossRef]
15. He, Y.; Jia, Z.; Hu, M.; Cui, C.; Cheng, Y.; Yang, Y. The Hybrid Similar Neighborhood Robust Factorization Machine Model for Can Bus Intrusion Detection in the In-Vehicle Network. *IEEE Trans. Intell. Transp. Syst.* **2021**, *1*, 1–9. [CrossRef]
16. Lo, W.; Alqahtani, H.; Thakur, K.; Almadhor, A.; Chander, S.; Kumar, G. A hybrid deep learning based intrusion detection system using spatial-temporal representation of in-vehicle network traffic. *Veh. Commun.* **2022**, *35*, 100471. [CrossRef]
17. Carvajal-Roca, I.E.; Wang, J.; Du, J.; Wei, S. A Semi-Centralized Dynamic Key Management Framework for In-Vehicle Networks. *IEEE Trans. Veh. Technol.* **2021**, *70*, 10864–10879. [CrossRef]
18. Kohnhäuser, F.; Püllen, D.; Katzenbeisser, S. May. Ensuring the safe and secure operation of electronic control units in road vehicles. In Proceedings of the 2019 IEEE Security and Privacy Workshops (SPW), San Francisco, CA, USA, 19–23 May 2019; pp. 126–131.
19. Walrand, J.; Turner, M.; Myers, R. An architecture for in-vehicle networks. *IEEE Trans. Veh. Technol.* **2021**, *70*, 6335–6342. [CrossRef]
20. Apostu, S.; Burkacky, O.; Deichmann, J.; Doll, G. Automotive Software and Electrical/Electronic Architecture: Implications for OEMs. 2019. Available online: https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/automotive-software-andelectrical-electronic-architecture-implications-for-oems (accessed on 16 July 2022).
21. Jiang, S. *Vehicle e/e Architecture and Its Adaptation to New Technical Trends*; Technical Report; SAE Technical Paper: Warrendale, PA, USA, 2019.
22. Zerfowski, D.; Lock, A. Functional Architecture and E/E-Architecture–A Challenge for the Automotive Industry. In *19. Internationales Stuttgarter Symposium*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 909–920.
23. Butzkamm, C.; Brand, K. E/E Architecture in the HARRI Innovation Platform. *Atzelektronik Worldw.* **2020**, *15*, 18–24. [CrossRef]

24. Freddie Holmes, J.H.; Moreton, J. Zonal E/E Architectures the Cornerstone of Future Mobility Development. 2021. Available online: https://www.automotiveworld.com/articles/zonal-e-e-architectures-the-cornerstone-of-future-mobility-development (accessed on 15 July 2022).
25. Bandur, V.; Selim, G.; Pantelic, V.; Lawford, M. Making the case for centralized automotive e/e architectures. *IEEE Trans. Veh. Technol.* **2021**, *70*, 1230–1245. [CrossRef]
26. Di Natale, M.; Zeng, H.; Giusto, P.; Ghosal, A. *Understanding and Using the Controller Area Network Communication Protocol: Theory and Practice*; Springer Science & Business Media: Berlin, Germany, 2012.
27. Ruff, M. October. Evolution of local interconnect network (LIN) solutions. In Proceedings of the 2003 IEEE 58th Vehicular Technology Conference. VTC 2003-Fall (IEEE Cat. No. 03CH37484), Orlando, FL, USA, 6–9 October 2003; Volume 5, pp. 3382–3389.
28. Shaw, R.; Jackman, B. An introduction to FlexRay as an industrial network. In Proceedings of the 2008 IEEE International Symposium on Industrial Electronics, Cambridge, UK, 30 June 2008–2 July 2008; pp. 1849–1854.
29. Sumorek, A.; Buczaj, M. New elements in vehicle communication "media oriented systems transport" protocol. *Teka Kom. Motoryz. I Energetyki Rol.* **2012**, *12*, 275–279.
30. Hank, P.; Müller, S.; Vermesan, O.; Van Den Keybus, J. Automotive ethernet: In-vehicle networking and smart mobility. In Proceedings of the 2013 Design, Automation & Test in Europe Conference & Exhibition, Grenoble, France, 18–22 March 2013; pp. 1735–1739.
31. Klinedinst, D.; King, C. *On Board Diagnostics: Risks and Vulnerabilities of the Connected Vehicle*; CERT Coordination Center: Pittsburgh, PA, USA, 2016.
32. 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 20th USENIX Security Symposium (USENIX Security 11), San Francisco, CA, USA, 10–12 August 2011.
33. Gottumukkala, R.; Merchant, R.; Tauzin, A.; Leon, K.; Roche, A.; Darby, P. Cyber-physical system security of vehicle charging stations. In Proceedings of the 2019 IEEE Green Technologies Conference (GreenTech), Lafayette, LA, USA, 3–6 April 2019; pp. 1–5.
34. Cao, Y.; Xiao, C.; Cyr, B.; Zhou, Y.; Park, W.; Rampazzi, S.; Chen, Q.A.; Fu, K.; Mao, Z.M. Adversarial sensor attack on lidar-based perception in autonomous driving. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, London, UK, 11–15 November 2019; pp. 2267–2281.
35. Miller, C.; Valasek, C. Adventures in automotive networks and control units. *Def. Con.* **2013**, *21*, 15–31.
36. Li, X.; Yu, Y.; Sun, G.; Chen, K. Connected vehicles' security from the perspective of the in-vehicle network. *IEEE Netw.* **2018**, *32*, 58–63. [CrossRef]
37. Nakhila, O.; Dondyk, E.; Amjad, M.F.; Zou, C. User-side wi-fi evil twin attack detection using ssl/tcp protocols. In Proceedings of the 2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC), Las Vegas, NV, USA, 9–12 January 2015; pp. 239–244.
38. Wu, X.; Subramanian, S.; Guha, R.; White, R.G.; Li, J.; Lu, K.W.; Bucceri, A.; Zhang, T. Vehicular communications using DSRC: Challenges, enhancements, and evolution. *IEEE J. Sel. Areas Commun.* **2013**, *31*, 399–408.
39. Ivanov, I.; Maple, C.; Watson, T.; Lee, S. Cyber security standards and issues in V2X communications for Internet of Vehicles. In Proceedings of the Living in the Internet of Things: Cybersecurity of the IoT—2018, London, UK, 28–29 March 2018.
40. Kim, S.; Shrestha, R. In-vehicle communication and cyber security. In *Automotive Cyber Security*; Springer: Gateway East, Singapore, 2020; pp. 67–96.
41. Zeng, W.; Khalid, M.A.; Chowdhury, S. In-vehicle networks outlook: Achievements and challenges. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 1552–1571. [CrossRef]
42. Nowdehi, N.; Lautenbach, A.; Olovsson, T. In-vehicle CAN message authentication: An evaluation based on industrial criteria. In Proceedings of the 2017 IEEE 86th Vehicular Technology Conference (VTC-Fall), Toronto, ON, Canada, 24–27 September 2017; pp. 1–7.
43. Groza, B.; Murvay, P.S. Security solutions for the controller area network: Bringing authentication to in-vehicle networks. *IEEE Veh. Technol. Mag.* **2018**, *13*, 40–47. [CrossRef]
44. Avatefipour, O.; Malik, H. State-of-the-art survey on in-vehicle network communication (CAN-Bus) security and vulnerabilities. *arXiv* **2018**, *1802*, 01725.
45. Bozdal, M.; Samie, M.; Jennions, I. A survey on can bus protocol: Attacks, challenges, and potential solutions. In Proceedings of the 2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE), Southend, UK, 16–17 August 2018; pp. 201–205.
46. Tomlinson, A.; Bryans, J.; Shaikh, S.A. September. Towards viable intrusion detection methods for the automotive controller area network. In Proceedings of the 2nd ACM Computer Science in Cars Symposium, Munich, Germany, 13–14 September 2018; pp. 1–9.
47. Le, V.H.; den Hartog, J.; Zannone, N. Security and privacy for innovative automotive applications: A survey. *Comput. Commun.* **2018**, *132*, 17–41. [CrossRef]
48. Young, C.; Zambreno, J.; Olufowobi, H.; Bloom, G. Survey of automotive controller area network intrusion detection systems. *IEEE Des. Test* **2019**, *36*, 48–55. [CrossRef]

49. Gmiden, M.; Gmiden, M.H.; Trabelsi, H. Cryptographic and Intrusion Detection System for automotive CAN bus: Survey and contributions. In Proceedings of the 2019 16th International Multi-Conference on Systems, Signals & Devices (SSD), Istanbul, Turkey, 21–24 March 2019; pp. 158–163.
50. 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.* **2019**, *21*, 919–933. [CrossRef]
51. Lokman, S.F.; Othman, A.T.; Abu-Bakar, M.H. Intrusion detection system for automotive Controller Area Network (CAN) bus system: A review. *EURASIP J. Wirel. Commun. Netw.* **2019**, *2019*, 1–17. [CrossRef]
52. Bozdal, M.; Samie, M.; Aslam, S.; Jennions, I. Evaluation of can bus security challenges. *Sensors* **2020**, *20*, 2364. [CrossRef] [PubMed]
53. El-Rewini, Z.; Sadatsharan, K.; Selvaraj, D.F.; Plathottam, S.J.; Ranganathan, P. Cybersecurity challenges in vehicular communications. *Veh. Commun.* **2020**, *23*, 100214. [CrossRef]
54. 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]
55. Karopoulos, G.; Kambourakis, G.; Chatzoglou, E.; Hernández-Ramos, J.L.; Kouliaridis, V. Demystifying In-Vehicle Intrusion Detection Systems: A Survey of Surveys and a Meta-Taxonomy. *Electronics* **2022**, *11*, 1072. [CrossRef]
56. Choi, W.; Joo, K.; Jo, H.J.; Park, M.C.; Lee, D.H. Voltageids: Low-level communication characteristics for automotive intrusion detection system. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 2114–2129. [CrossRef]
57. 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.
58. 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]
59. Mundhenk, P.; Steinhorst, S.; Lukasiewycz, M.; Fahmy, S.A.; Chakraborty, S. Lightweight authentication for secure automotive networks. In Proceedings of the 2015 Design, Automation & Test in Europe Conference & Exhibition (DATE), Grenoble, France, 9–13 March 2015; pp. 285–288.
60. 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 2016 International Conference on Information Networking (ICOIN), Kota Kinabalu, Malaysia, 13–15 January 2016; pp. 63–68.
61. Kang, M.J.; Kang, J.W. Intrusion detection system using deep neural network for in-vehicle network security. *PLoS ONE* **2016**, *11*, e0155781. [CrossRef]
62. Ghaleb, F.A.; Zainal, A.; Rassam, M.A.; Mohammed, F. An effective misbehavior detection model using artificial neural network for vehicular ad hoc network applications. In Proceedings of the 2017 IEEE Conference on Application, Information and Network Security (AINS), Miri, Malaysia, 13–14 November 2017; pp. 13–18.
63. Jagielski, M.; Jones, N.; Lin, C.W.; Nita-Rotaru, C.; Shiraishi, S. Threat detection for collaborative adaptive cruise control in connected cars. In Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks, Stockholm, Sweden, 18–20 June 2018; pp. 184–189.
64. Seo, E.; Song, H.M.; Kim, H.K. GIDS: GAN based intrusion detection system for in-vehicle network. In Proceedings of the 2018 16th Annual Conference on Privacy, Security and Trust (PST), Belfast, Ireland, 28–30 August 2018; pp. 1–6.
65. Ferdowsi, A.; Challita, U.; Saad, W.; Mandayam, N.B. Robust deep reinforcement learning for security and safety in autonomous vehicle systems. In Proceedings of the 2018 21st International Conference on Intelligent Transportation Systems (ITSC), Maui, HI, USA, 4–7 November 2018; pp. 307–312.
66. Zhu, K.; Chen, Z.; Peng, Y.; Zhang, L. Mobile edge assisted literal multi-dimensional anomaly detection of in-vehicle network using LSTM. *IEEE Trans. Veh. Technol.* **2019**, *68*, 4275–4284. [CrossRef]
67. Eziama, E.; Jaimes, L.M.; James, A.; Nwizege, K.S.; Balador, A.; Tepe, K. Machine learning-based recommendation trust model for machine-to-machine communication. In Proceedings of the 2018 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT), Louisville, KY, USA, 6–8 December 2018; pp. 1–6.
68. Sherazi, H.H.R.; Iqbal, R.; Ahmad, F.; Khan, Z.A.; Chaudary, M.H. DDoS attack detection: A key enabler for sustainable communication in internet of vehicles. *Sustain. Comput. Inform. Syst.* **2019**, *23*, 13–20. [CrossRef]
69. Khanapuri, E.; Chintalapati, T.; Sharma, R.; Gerdes, R. Learning-based adversarial agent detection and identification in cyber physical systems applied to autonomous vehicular platoon. In Proceedings of the 2019 IEEE/ACM 5th International Workshop on Software Engineering for Smart Cyber-Physical Systems (SEsCPS), Montreal, QC, Canada, 28–28 May 2019; pp. 39–45.
70. Song, H.M.; Woo, J.; Kim, H.K. In-vehicle network intrusion detection using deep convolutional neural network. *Veh. Commun.* **2020**, *21*, 100198. [CrossRef]
71. Xiao, J.; Wu, H.; Li, X. Internet of things meets vehicles: Sheltering in-vehicle network through lightweight machine learning. *Symmetry* **2019**, *11*, 1388. [CrossRef]
72. Guo, J.; Li, X.; Liu, Z.; Ma, J.; Yang, C.; Zhang, J.; Wu, D. TROVE: A context-awareness trust model for VANETs using reinforcement learning. *IEEE Internet Things J.* **2020**, *7*, 6647–6662. [CrossRef]
73. Katragadda, S.; Darby, P.J.; Roche, A.; Gottumukkala, R. Detecting low-rate replay-based injection attacks on in-vehicle networks. *IEEE Access* **2020**, *8*, 54979–54993. [CrossRef]

74. Rasheed, I.; Hu, F.; Zhang, L. Deep reinforcement learning approach for autonomous vehicle systems for maintaining security and safety using LSTM-GAN. *Veh. Commun.* **2020**, *26*, 100266. [CrossRef]
75. Lin, Y.; Chen, C.; Xiao, F.; Avatefipour, O.; Alsubhi, K.; Yunianta, A. An Evolutionary Deep Learning Anomaly Detection Framework for In-Vehicle Networks—CAN Bus. *IEEE Trans. Ind. Appl.* **2020**, *1*, 1–14. [CrossRef]
76. Hossain, M.D.; Inoue, H.; Ochiai, H.; Fall, D.; Kadobayashi, Y. LSTM-based intrusion detection system for in-vehicle can bus communications. *IEEE Access* **2020**, *8*, 185489–185502. [CrossRef]
77. D'Angelo, G.; Castiglione, A.; Palmieri, F. A cluster-based multidimensional approach for detecting attacks on connected vehicles. *IEEE Internet Things J.* **2020**, *8*, 12518–12527. [CrossRef]
78. Loukas, G.; Vuong, T.; Heartfield, R.; Sakellari, G.; Yoon, Y.; Gan, D. Cloud-based cyber-physical intrusion detection for vehicles using deep learning. *IEEE Access* **2017**, *6*, 3491–3508. [CrossRef]
79. Zhang, J.; Li, F.; Zhang, H.; Li, R.; Li, Y. Intrusion detection system using deep learning for in-vehicle security. *Ad Hoc Netw.* **2019**, *95*, 101974. [CrossRef]
80. Lokman, S.F.; Othman, A.T.; Musa, S.; Abu Bakar, M.H. Deep contractive autoencoder-based anomaly detection for in-vehicle controller area network (CAN). In *Progress in Engineering Technology*; Springer: Cham, Switzerland, 2019; pp. 195–205.
81. Avatefipour, O.; Al-Sumaiti, A.S.; El-Sherbeeny, A.M.; Awwad, E.M.; Elmeligy, M.A.; Mohamed, M.A.; Malik, H. An intelligent secured framework for cyberattack detection in electric vehicles' CAN bus using machine learning. *IEEE Access* **2019**, *7*, 127580–127592. [CrossRef]
82. 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]
83. Li, X.; Hu, Z.; Xu, M.; Wang, Y.; Ma, J. Transfer learning based intrusion detection scheme for Internet of vehicles. *Inf. Sci.* **2021**, *547*, 119–135. [CrossRef]
84. Al-Saud, M.; Eltamaly, A.M.; Mohamed, M.A.; Kavousi-Fard, A. An intelligent data-driven model to secure intravehicle communications based on machine learning. *IEEE Trans. Ind. Electron.* **2019**, *67*, 5112–5119. [CrossRef]
85. Aldhyani, T.H.; Alkahtani, H. Attacks to automatous vehicles: A deep learning algorithm for cybersecurity. *Sensors* **2022**, *22*, 360. [CrossRef]
86. Nilsson, D.K.; Larson, U.E.; Jonsson, E. Efficient in-vehicle delayed data authentication based on compound message authentication codes. In Proceedings of the 2008 IEEE 68th Vehicular Technology Conference, Calgary, AB, Canada, 21–24 September 2008; pp. 1–5.
87. Van Herrewege, A.; Singelee, D.; Verbauwhede, I. CANAuth-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 November 2011; Volume 2011, p. 20.
88. Hazem, A.; Fahmy, H.A. Lcap-a lightweight can authentication protocol for securing in-vehicle networks. In Proceedings of the 10th Escar Embedded Security in Cars Conference, Berlin, Germany, 28–29 November 2012; Volume 6, p. 172.
89. Groza, B.; Murvay, S.; Herrewege, A.V.; Verbauwhede, I. LiBrA-CAN: A lightweight broadcast authentication protocol for controller area networks. In Proceedings of the International Conference on Cryptology and Network Security, Darmstadt, Germany, 12–14 December 2012; pp. 185–200.
90. Lin, C.W.; Sangiovanni-Vincentelli, A. Cyber-security for the controller area network (CAN) communication protocol. In Proceedings of the 2012 International Conference on Cyber Security, Alexandria, VA, USA, 14–16 December 2012; pp. 1–7.
91. Han, K.; Weimerskirch, A.; Shin, K.G. Automotive cybersecurity for in-vehicle communication. *IQT Q.* **2014**, *6*, 22–25.
92. Ueda, H.; Kurachi, R.; Takada, H.; Mizutani, T.; Inoue, M.; Horihata, S. Security authentication system for in-vehicle network. *SEI Tech. Rev.* **2015**, *81*, 5–9.
93. Fassak, S.; El Idrissi, Y.E.H.; Zahid, N.; Jedra, M. A secure protocol for session keys establishment between ECUs in the CAN bus. In Proceedings of the 2017 International Conference on Wireless Networks and Mobile Communications (WINCOM), Rabat, Morocco, 1–4 November 2017; pp. 1–6.
94. Noureldeen, P.; Azer, M.A.; Refaat, A.; Alam, M. Replay attack on lightweight CAN authentication protocol. In Proceedings of the 2017 12th International Conference on Computer Engineering and Systems (ICCES), Cairo, Egypt, 19–20 December 2017; pp. 600–606.
95. Tashiro, A.; Muraoka, H.; Araki, S.; Kakizaki, K.I.; Uehara, S. A secure protocol consisting of two different security-level message authentications over CAN. In Proceedings of the 2017 3rd IEEE International Conference on Computer and Communications (ICCC), Chengdu, China, 13–16 December 2017; pp. 1520–1524.
96. Lu, Z.; Wang, Q.; Chen, X.; Qu, G.; Lyu, Y.; Liu, Z. LEAP: A lightweight encryption and authentication protocol for in-vehicle communications. In Proceedings of the 2019 IEEE Intelligent Transportation Systems Conference (ITSC), Auckland, New Zealand, 27–30 October 2019; pp. 1158–1164.
97. 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), Cambridge, MA, USA, 6–8 October 2014; pp. 13–18.
98. Ansari, M.R.; Yu, S.; Yu, Q. IntelliCAN: Attack-resilient controller area network (CAN) for secure automobiles. In Proceedings of the 2015 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFTS), Amherst, MA, USA, 12–14 October 2015; pp. 233–236.

99. Woo, S.; Jo, H.J.; Kim, I.S.; Lee, D.H. A practical security architecture for in-vehicle CAN-FD. *IEEE Trans. Intell. Transp. Syst.* **2016**, *17*, 2248–2261. [CrossRef]
100. Radu, A.I.; Garcia, F.D. LeiA: A lightweight authentication protocol for CAN. In Proceedings of the European Symposium on Research in Computer Security, Heraklion, Greece, 28–30 September 2016; pp. 283–300.
101. King, Z. Investigating and securing communications in the Controller Area Network (CAN). In Proceedings of the 2017 International Conference on Computing, Networking and Communications (ICNC), Silicon Valley, CA, USA, 26–29 January 2017; pp. 814–818.
102. Farag, W.A. CANTrack: Enhancing automotive CAN bus security using intuitive encryption algorithms. In Proceedings of the 2017 7th International Conference on Modeling, Simulation, and Applied Optimization (ICMSAO), Sharjah, United Arab Emirates, 4–6 April 2017; pp. 1–5.
103. Siddiqui, A.S.; Gui, Y.; Plusquellic, J.; Saqib, F. Secure communication over CANBus. In Proceedings of the 2017 IEEE 60th International Midwest Symposium on Circuits and Systems (MWSCAS), Boston, MA, USA, 06–09 August 2017; pp. 1264–1267.
104. Gui, Y.; Siddiqui, A.S.; Saqib, F. Hardware based root of trust for electronic control units. In Proceedings of the SoutheastCon 2018, St. Petersburg, FL, USA, 19–22 April 2018; pp. 1–7.
105. Carel, G.; Isshiki, R.; Kusaka, T.; Nogami, Y.; Araki, S. Design of a message authentication protocol for CAN FD based on chaskey lightweight MAC. In Proceedings of the 2018 Sixth International Symposium on Computing and Networking Workshops (CANDARW), Takayama, Japan, 27–30 November 2018; pp. 267–271.
106. Woo, S.; Moon, D.; Youn, T.Y.; Lee, Y.; Kim, Y. Can id shuffling technique (cist): Moving target defense strategy for protecting in-vehicle can. *IEEE Access* **2019**, *7*, 15521–15536. [CrossRef]
107. Agrawal, M.; Huang, T.; Zhou, J.; Chang, D. CAN-FD-Sec: Improving security of CAN-FD protocol. In *Security and Safety Interplay of Intelligent Software Systems*; Springer: Cham, Switzerland, 2018; pp. 77–93.
108. Zhang, M.; Masrur, A. Improving timing behavior on encrypted CAN buses. In Proceedings of the 2019 IEEE 25th International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA), Hangzhou, China, 18–21 August 2019; pp. 1–6.
109. Jo, H.J.; Kim, J.H.; Choi, H.Y.; Choi, W.; Lee, D.H.; Lee, I. Mauth-can: Masquerade-attack-proof authentication for in-vehicle networks. *IEEE Trans. Veh. Technol.* **2019**, *69*, 2204–2218. [CrossRef]
110. Mun, H.; Han, K.; Lee, D.H. Ensuring safety and security in CAN-based automotive embedded systems: A combination of design optimization and secure communication. *IEEE Trans. Veh. Technol.* **2020**, *69*, 7078–7091. [CrossRef]
111. Groza, B.; Popa, L.; Murvay, P.S. Highly efficient authentication for CAN by identifier reallocation with ordered CMACs. *IEEE Trans. Veh. Technol.* **2020**, *69*, 6129–6140. [CrossRef]
112. Youn, T.Y.; Lee, Y.; Woo, S. Practical sender authentication scheme for in-vehicle CAN with efficient key management. *IEEE Access* **2020**, *8*, 86836–86849. [CrossRef]
113. Lenard, T.; Bolboacă, R.; Genge, B.; Haller, P. MixCAN: Mixed and backward-compatible data authentication scheme for controller area networks. In Proceedings of the 2020 IFIP Networking Conference (Networking), Paris, France, 22–26 June 2020; pp. 395–403.
114. Ma, B.; Yang, S.; Zuo, Z.; Zou, B.; Cao, Y.; Yan, X.; Zhou, S.; Li, J. An Authentication and Secure Communication Scheme for In-Vehicle Networks Based on SOME/IP. *Sensors* **2022**, *22*, 647. [CrossRef]
115. Mousa, A.R.; NourElDeen, P.; Azer, M.; Allam, M. Lightweight authentication protocol deployment over FlexRay. In Proceedings of the 10th International Conference on Informatics and Systems, Giza, Egypt, 9–11 May 2016; pp. 233–239.
116. Gu, Z.; Han, G.; Zeng, H.; Zhao, Q. Security-aware mapping and scheduling with hardware co-processors for flexray-based distributed embedded systems. *IEEE Trans. Parallel Distrib. Syst.* **2016**, *27*, 3044–3057. [CrossRef]
117. Han, G.; Zeng, H.; Li, Y.; Dou, W. SAFE: Security-aware flexray scheduling engine. In Proceedings of the Conference on Design, Automation & Test in Europe, Dresden, Germany, 24–28 March 2014.
118. Perrig, A.; Tygar, J.D. TESLA broadcast authentication. In *Secure Broadcast Communication*; Springer: Boston, MA, USA, 2003; pp. 29–53.
119. Deng, J.; Yu, L.; Fu, Y.; Hambolu, O.; Brooks, R.R. Security and data privacy of modern automobiles. In *Data Analytics for Intelligent Transportation Systems*; Elsevier: New York, NY, USA, 2017; pp. 131–163.
120. 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. Processing* **2017**, *25*, 220–228. [CrossRef]
121. Kiravuo, T.; Sarela, M.; Manner, J. A survey of Ethernet LAN security. *IEEE Commun. Surv. Tutor.* **2013**, *15*, 1477–1491. [CrossRef]
122. Lin, C.-W.; Yu, H. INVITED: Cooperation or Competition? Coexistence of Safety and Security in Next-Generation Ethernet-Based Automotive Networks. In Proceedings of the 53rd ACM/EDAC/IEEE Design Automation Conference, Austin, TX, USA, 5–9 June 2016.
123. Wolf, M.; Weimerskirch, A.; Paar, C. Security in automotive bus systems. In *Workshop on Embedded Security in Cars*; Escrypt GmbH: Bochum, Germany, 2004; pp. 1–13.
124. Pekaric, I.; Sauerwein, C.; Haselwanter, S.; Felderer, M. A taxonomy of attack mechanisms in the automotive domain. *Comput. Stand. Interfaces* **2021**, *78*, 103539. [CrossRef]
125. 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. [CrossRef]