Enhancing Cybersecurity in In-Vehicle Networks: Challenges, Protocol Vulnerabilities, and Advanced Countermeasures

Suresh Sureddi

ssureddi@gmail.com

Abstract

The amount of data exchanged in connected vehicles has significantly increased with the increase in number of sensors in the car. Many advanced technologies, such as cloud computing, V2X (vehicle to everything) communication, ADAS (Advanced driver assistance systems), and artificial intelligence, are being more and more widely used in cars, which makes connected cars more intelligent to offer comfortable services for people and ensure the safety of drivers and passengers. However, cyber-attack risk is growing as our vehicles become more interconnected. Therefore, there is a critical need to prioritize cyber security in the automotive sector.

Several ECUs (electronic control units) with connected sensors in a car are connected over in-vehicle networks such as CAN, MOST, Ethernet, Flex Ray, and LIN. These network protocols lack the design of an information security mechanism at the beginning of their design, which makes them vulnerable to cyber-attacks such as sniffing, jamming, replay, or forgery of messages. This paper first presents a brief introduction and a list of the limitations of the original design of vehicle bus protocols. Then, the protocols for in-vehicle communication are classified based on their characteristics and usage type. Finally, various security solutions to address these limitations will be reviewed.

Keywords: Connected Vehicles, Automotive, Cybersecurity, Connectivity, CAN (Controller Area Network), Automotive Ethernet, Autonomous, V2X (Vehicle-to-Everything), Artificial Intelligence.

1. **Introduction**:

ECUs (Electronics Control Units) fuse data from different sensors in a car to provide accurate information to the driver and connected vehicles. The growth in functionality in the car due to the increase in the number of sensors and the adoption of advanced technologies such as ADAS, V2X communications, and Cloud services is making cars increasingly vulnerable to cyber-attacks. The increase in attack vectors and attack surfaces [1] such as CAN, MOST (Media Oriented System Transport), GPS, OBD (Onboard Diagnostics), and sensors (LiDAR, Cameras, TPMS, Wi-Fi, Bluetooth, and keyless entry) are making a vehicle even more vulnerable to cyber-attacks. The existing protocols of the in-vehicle network have various vulnerabilities, such as ID-based arbitration mechanisms for contention resolution, unavailability of message authentication and encryption, etc. [2].

This paper first introduces the details of different vehicle networking bus protocols, shares the limitations of their original design, and then details the various research and ongoing studies to overcome them. There is an urgent need to improve vehicle bus protocols for the automotive industry, which should be fully compatible with current trends and advanced technologies. If not, adversaries may use existing

vulnerabilities and attack the modern intelligent vehicle, which may lead to hazards to life and damage to the car on the road.

In-vehicle networks, also known as internal communication networks, are responsible for interconnecting various components inside modern intelligent vehicles. ECUs, gateways, sensors, actuators, etc., are the main core components of modern intelligent vehicles.[3]
With the growing number of sensors and ECUs in the vehicle, the in-vehicle network architecture is transforming to address the ever-increasing demand for advanced technologies in the car. 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 functional 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 helps reduce the complexity of previously existing two architectures.

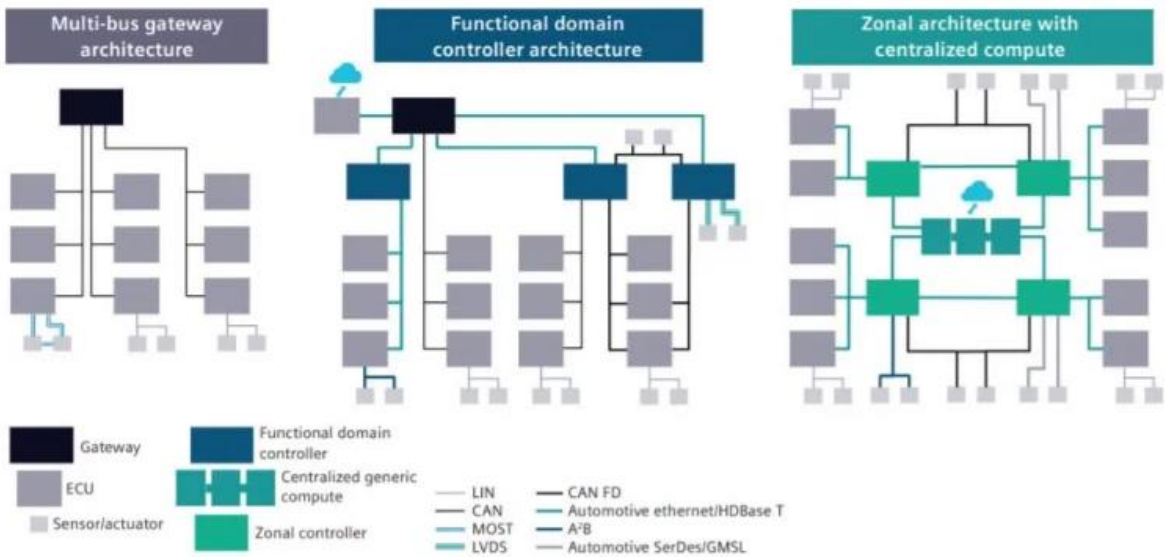

Figure 1: In-vehicle network architectures

2. In-vehicle automotive bus protocols and their limitations:
The CAN bus protocol is widely used to exchange real-time information between the car's modules. Other heterogeneous vehicle networks include Media-Oriented Systems Transport (MOST), FlexRay, Local Interconnect Networks (LIN), and Automotive Ethernet (AE).

2.1. CAN (Controller Area Network)
Data is exchanged between multiple ECUs through inter-connected buses. CAN is based on a broadcast communication mechanism. The CAN protocol has various advantages, such as simplicity, low network complexity, and reduced wiring costs, since CAN utilizes the multiplex wire architecture to eliminate the need for complex, excessive wiring for communication among different ECUs. CAN cannot 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. Its main limitation is the lack of authentication mechanisms and encryption. Additionally, the rapid advancement in automotive applications requires support from high-bandwidth backend protocols, but CAN has bandwidth limitations.

2.2. LIN (Local Interconnect Network)

LIN is a single-wire network for connecting sensors and actuators. The reliability of LIN is not up to the mark as compared with CAN. Hence, it is not suitable for time-critical applications. LIN utilizes the parity bits and checksums to detect incorrect messages in the network.[4]

2.3. FlexRay Protocol

The FlexRay protocol utilizes two parallel channels for data transmission in synchronous and asynchronous modes. It can be used for time-critical applications. Although FlexRay has reliability and fault tolerance features, the implementation cost is very high.
FlexRay handles logical errors by using checksums and redundancy mechanisms.

2.4. MOST (Media-Oriented Systems Transport)

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

2.5. 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 ADAS (Advanced Driver Assistance Systems). The main advantage of this protocol is the reduced wiring cost since it supports switched network technology.

3. Security threats and countermeasures

The rapid transition towards advanced connected vehicle technologies opens the door to several security threats. Therefore, researchers are more interested in finding security solutions for these in-vehicle networking protocols.

3.1. CAN-related Security Threats

A study reported six types of attacks on CAN bus systems, namely bus-off attacks [5], Denial of service (DoS) [6], masquerading, injection, eavesdropping, and replay attacks [7]. Attackers may gain knowledge of the CAN frame since CAN frames are generally not encrypted and fail to support message authentication. Thus, attackers may quickly gain entry to the network. 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 vehicle's bus system. Through OBD-II ports, the attackers may successfully establish a connection with the in-vehicle system and consequently 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, known as a replay attack. Furthermore, the attacker may continually send bits in the identification and other fields. This type of attack is known as a bus-off attack. Besides, the attacker may disrupt the standard processing of the in-vehicle communication by constantly delivering the CAN packet with high

priority, which blocks 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.

Proposed Solution based on Machine Learning:

One of machine learning's main benefits is that it helps to make optimal predictions about several types of attacks.

Kang et al. [8] designed a deep neural network-based intrusion detection framework to enhance security. From the in-vehicle network packets, feature vectors

(probability-based) are extracted, and the DNN model is trained with these feature vectors.

After training, the DNN model can easily discriminate between an attack and regular packets, thereby identifying any malicious attack on the vehicle. The proposed framework's detection accuracy is much improved compared to traditional AI-based systems since the parameters are initially initialized via an unsupervised approach of deep belief networks (DBN).

Seo et al. [9] designed an intrusion detection system for in-vehicle networks that utilizes a deep learning approach. The proposed framework only utilizes standard data to detect unknown attacks.

Song et al. [10] designed a deep convolutional neural network-based effective intrusion detection framework to enhance the CAN bus's protection level. A deep convolutional neural network model in the proposed framework quickly identifies malicious traffic after properly learning the traffic data pattern. The proposed framework provides a high detection performance with a significant reduction in complexity. Xiao et al. [11] proposed a lightweight security framework to counter attacks on the CAN bus through various access points. The proposed security framework is divided into two individual frameworks, namely the simplified attention framework based on machine learning and the second one known as the security control unit framework. Using two individual frameworks instead of one reduces the computational cost significantly.

Angelo et al. [12] proposed an intrusion detection framework utilizing two algorithms. The first algorithm aims to learn the behavior of traffic data, while the second is data-driven. These two algorithms focus on the real-time classification of traffic data, resulting in prior alerts regarding the presence of malicious messages.

The extensive research above shows that machine learning-based approaches were widely used for detecting and predicting several types of attacks on in-vehicle networks. The machine learning-based frameworks are used to analyze 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 crucial since automotive manufacturers do not provide specifications for decoding raw data features. Supervised machine learning-based approaches are quite time-consuming due to labeling raw CAN data, identifying and classifying CAN attacks, etc. On the other hand, unsupervised machine learning-based mechanisms use data to find common patterns and further utilize these patterns to classify CAN traffic and identify anomalous behavior.

Proposed Security solutions based on Cryptography:

Cryptography algorithms counteract diversified cyber-attacks on vehicles' in-vehicle networks. Researchers have proposed Several security frameworks using cryptography algorithms. Hackers are using the latest advanced techniques to attack vehicles, and therefore, no standard security framework with guaranteed resolutions for the latest threats is available. Researchers are using new advanced cryptographic algorithms to design security frameworks that protect the CAN bus, thereby protecting the data frames from manipulation.

Herrewege et al. [13] explored the CAN bus's message authentication protocol implementation issues. After a successful investigation, they found various constraints related to a backward-compatible message authentication protocol and presented a new message authentication protocol to address the existing constraints.

Hazem et al. [14] designed a new protocol known as a message source authentication protocol. The proposed authentication protocol performs well with minimum overhead. Implementing the proposed protocol does not require any modifications in hardware for the CAN network or changes in existing CAN message sets. Further, Groza et al. [15] utilize symmetric primitives for designing the authentication protocol, which has two main mechanisms: mixing of MAC and splitting of keys. In the proposed protocol, authentication keys are split among multiple groups of nodes, resulting in progressive authentication compared with the traditional approach of independently authenticating each node.

In [16], several different methodologies are presented for preventing unauthorized data transmission, thereby increasing the security level in CAN, and in [17], the protocol is presented to counter DoS attacks. Additionally, the proposed protocol provides a secure channel between external devices and in-vehicle network components. The proposed protocol consists of two main authentication processes, namely checking the authenticity of the transmitter and data validation through message authentication. Next, in [18], an advanced framework based on runtime verification is proposed to provide security against several attacks on CAN. The proposed framework uses the copilot method for performing run-time detection. In [19], a CAN authentication protocol is presented to provide 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 a secure and robust environment for CAN. Further, researchers in [20] designed a security framework for providing security in CAN. The proposed framework utilizes a truncated MAC to secure transmitted messages. Additionally, in a data frame, it utilizes a segment of MAC. Therefore, the proposed framework uses two mechanisms to protect the CAN against malicious attacks. The results attested that the proposed framework effectively handles the replay and tampering attacks. Furthermore, a new methodology based on cryptographic techniques is presented in [21] for increasing security in CAN. The proposed lightweight framework uses stream cipher to encrypt messages, while a key management mechanism protects against external attacks. The results show that the proposed framework is characterized by two main features: minimum memory requirements and high efficiency compared with other MAC-based schemes.

From the above extensive research, it’s evident that using a cryptography approach against security threats to in-vehicle networks has all potential advantages except that the CAN bus controller requires additional computational resources. Generally, there are two primary components in the Cryptography approach. The first is known as the Message Authentication Code (MAC), and the other is called a cryptosystem having two fields, symmetric and asymmetric. Further, the MAC ensures Integrity and Authentication, while the symmetric and asymmetric cryptosystems provide confidentiality. Additionally, session keys can be utilized to provide authentication. For vehicle safety, the load on the CAN bus and latency issue in response time should be within the specified limit. Additionally, the Cyclic Redundancy Code (CRC) at CAN bus detects data frame transmission errors. ECUs have their limitations in terms of computational capacity. Therefore, lightweight encryption is one of the solutions for handling this issue since ECUs are core components inside the vehicle that handle various functions simultaneously. The bus may be heavily loaded during the key exchange, and pre-loaded keys in the ECUs can tackle this situation in a key distribution environment. The Hardware Security Module (HSM) in ECUs can effectively perform encryption and decryption in optimal time and compensate for resource-constrained ECUs. Although several significant developments in security frameworks based on cryptography algorithms can be seen, the cost factor in successfully implementing these schemes cannot be forgotten.

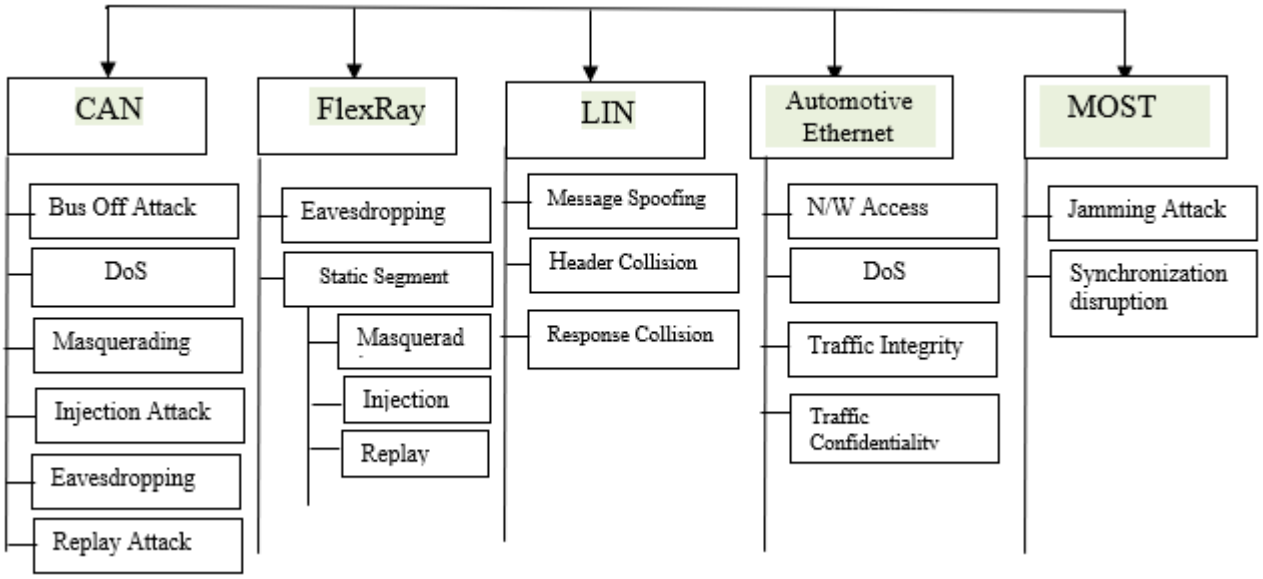

Figure 2: Types of security threats to Automotive Protocols

3.2. Security Threats—FlexRay

The two main types of attacks in FlexRay are Eavesdropping [22] and static segment attacks [23]. In the case of the Eavesdropping type of attack, FlexRay messages are accessed by the attackers, and consequently, the attacker can obtain all the critical information. This attack results in data leakage and impacts data confidentiality and security concerns. In the case of segment attack 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 implementing an advanced scheme for authenticating the message within the static segment [24]. Timed Efficient Stream Loss-tolerant Authentication [25] is the authentication protocol.

3.3. Security Threats—Local Interconnect Network (LIN)

Three attacks usually occur to LIN, namely message spoofing [26], header collision,
and response collision attacks. In the message spoofing attack, the attacker tries interrupting vehicular communication by sending false unauthorized messages to shut down LIN. The vulnerabilities in the master-slave model of LIN cause this attack. The hacker exploits the LIN's error-handling protocol in the collision response attack. In this attack, along with a valid message, the attacker concurrently sends an illicit message consisting of a false header. Consequently, the message transmission is stopped by the legitimate slave node immediately, whereas all other nodes will accept illegitimate messages. The hacker tries to create a conflicting situation in the header collision attack. The attacker sends an incorrect header to create a contradictory 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 example, the 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 [27].

3.4. Security Threats—Automotive Ethernet (AE)

Four types of attacks usually occur on Automotive Ethernet: traffic integrity,Btraffic confidentiality, network access, and DoS attacks [28].

Traffic integrity attacks can be considered man-in-the-middle attacks. In this type of attack, information is exploited by diverting the traffic towards the compromised node. There are two types of attacks, namely session hijacking and replay attacks.

In traffic confidentiality attacks, the attacker first gets access to the network, then attacks it and tries to overhear its activities.

In network access attacks, the hacker first establishes a connection with the switch's unsecured port and then tries to connect to the Ethernet network via this connection. The attacker's ultimate objective is to access the network and subsequently control several different nodes or control the network remotely.

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 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 to waste energy. The corrective mechanism should consider the authentication, frame replication, and the virtual local area network segmentation scheme [29].

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

Two types of attacks generally occur on the MOST bus protocol: jamming and synchronization disruption attacks. In the synchronization disruption attacks, the hacker tries to tamper with the synchronization of MOST by sending fake timing frames continuously. In jamming attacks, the hacker attempts 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: source node authentication, encrypted exchanged messages, and strict enforcement of firewalls and gateways [30].

Conclusion:

With the rising adoption of advanced technologies such as V2X (vehicle-to-everything) communication, ADAS (Advanced driver assistance systems), cloud computing, and artificial intelligence in the automotive sector, there is a growing concern about cyber-attacks on these connected vehicles. This article highlights the transformation of In-vehicle network architecture due to the increase in the number of sensors and ECUs in modern cars. It explores the characteristics of several in-vehicle bus protocols and their limitations with the original design. Initially, automotive protocols are designed without considering the security threats, but current advancements in connected car technologies require advanced security schemes for these protocols to counter malicious attacks. The security schemes use different technology environments, such as cryptography techniques and machine learning algorithms. To enhance the security of in-vehicle networks, several research articles have been published using cryptography and machine learning algorithms for designing security frameworks, and research is still ongoing to find optimal solutions. Cryptography techniques generally use identifiers in data frames, finding manipulations in sending time, and message authentication, etc., for enhancing security levels. On the other hand, machine learning approaches use different algorithms to design the framework and train the model accordingly with training data.

Both sectors, including academia and the industry, have shown incredible concerns about the security of the in-vehicle network, and extensive research has been conducted to improve the robustness of in-vehicle networking protocols.

References

[1] Garrad and Gilroy: Developments in Connected Vehicles and the Requirement for Increased Cybersecurity, August 2021.
[2] 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.
[3] 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
[4] 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.
[5] 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.
[6] 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.
[7] 8. Liu, J.; Zhang, S.; Sun, W.; Shi, Y. In-vehicle network attacks and countermeasures: Challenges and future directions. IEEE Netw. 2017, 31, 50–58.
[8] Kang, M.J.; Kang, J.W. Intrusion detection system using deep neural network for in-vehicle network security. PLoS ONE 2016, 11, e0155781.
[9] 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.
[10] Song, H.M.;Woo, J.; Kim, H.K. In-vehicle network intrusion detection using deep convolutional neural network. Veh. Commun. 2020, 21, 100198.
[11] Xiao, J.;Wu, H.; Li, X. Internet of things meets vehicles: Sheltering in-vehicle network through lightweight machine learning. Symmetry 2019, 11, 1388.
[12] 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.
[13] Van Herrewege, A.; Singelee, D.; Verbauwhede, I. CANAuth-a simple, backward compatible broadcast authentication protocol for CAN bus. In Proceedings of the ECRYPTWorkshop on Lightweight Cryptography, Louvain-la-Neuve, Belgium, 28–29 November 2011; Volume 2011, p. 20.
[14] 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.
[15] Groza, B.; Murvay, S.; Herrewege, A.V.; Verbauwhede, I. LiBrA-CAN: A lightweight broadcast authentication protocol forcontroller area networks. In Proceedings of the International Conference on Cryptology and Network Security, Darmstadt,Germany, 12–14 December 2012; pp. 185–200.
[16] 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.
[17] Han, K.;Weimerskirch, A.; Shin, K.G. Automotive cybersecurity for in-vehicle communication. IQT Q. 2014, 6, 22–25.
[18] 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.
[19] 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.
[20] 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.
[21] 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.
[22] 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.
[23] 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.
[24] 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.
[25] Perrig, A.; Tygar, J.D. TESLA broadcast authentication. In Secure Broadcast Communication; Springer: Boston, MA, USA, 2003; pp. 29–53.
[26] 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.
[27] 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.
[28] Kiravuo, T.; Sarela, M.; Manner, J. A survey of Ethernet LAN security. IEEE Commun. Surv. Tutor. 2013, 15, 1477–1491.
[29] 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.
[30] 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.