Received: 30 July 2020 | Revised: 7 December 2020 | Accepted: 13 January 2021

DOI: 10.1002/spe.2965

SPECIAL ISSUE PAPER

WILEY

Cybersecurity protection on in-vehicle networks for distributed automotive cyber-physical systems: State-of-the-art and future challenges

Yong Xie[1] | Yu Zhou[2] | Jing Xu[2] | Jian Zhou[1] | Xiaobai Chen[1] | Fu Xiao[1]

[1]School of Computer Science, Nanjing University of Posts and Telecommunications, Xianlin, R.P. China

[2]Department of Computer and Information Engineering, Xiamen University of Technology, Xiamen, R.P. China

Correspondence
Yong Xie, School of Computer Science, Nanjing University of Posts and Telecommunications, No.9, Wenyuan Road, Xianlin, Nanjing, R.P. China.
Email: yongxie@njupt.edu.cn

Funding information
National Natural Science Foundation of China, Grant/Award Numbers: 61872436, 61972210; Natural Science Foundation of Fujian Province, China, Grant/Award Number: 2018J01571; NUPTSF, Grant/Award Numbers: NY220133, XK0040920081; Research Foundation of Jiangsu, Grant/Award Number: BRA2020065

Abstract

The ever-evolving trip mode of human being leads the automobiles moving toward connected, autonomous, sharing, and electrified vehicles rapidly. But the connection introduces new cybersecurity problems on in-vehicle networks, which poses great challenges for safety guarantee of distributed automotive cyber-physical systems. This article first analyzes the cybersecurity vulnerabilities and defines the security requirements for in-vehicle networks, and then introduces the architecture evolution of in-vehicle network. Based on the definition on architecture of in-vehicle networks, this article defines a security protection framework for it. And then, it surveys the state-of-the-art works for availability protection, integrity protection, and confidentiality protection of in-vehicle networks, respectively, and detailed analysis and comparisons are given about the proposed cybersecurity protection mechanisms. Finally, it summarizes the future challenges for cybersecurity protection of in-vehicle networks, and proposes possible solutions for these challenges.

KEYWORDS

controller area network, cybersecurity protection, distributed automotive cyber-physical systems, in-vehicle networks, system design and optimization

1 | INTRODUCTION

1.1 | Background and motivations

The automotive industry is at the beginning of a major change, where the ever-evolving trip mode of human being leads the automobiles moving toward connected, autonomous, sharing and electrified distributed automotive cyber-physical systems (DACPS) rapidly. The amount of software continues to grow rapidly in DACPS, as well as its complexity. For some luxury cars, the number of electronic control units (ECU) is over 100, and the underlying software inside these ECUs contains approximately 100 million lines of code.[1] Inside the DACPS, ECUs are connected and cooperated with each other with the help of different kinds of in-vehicle networks, such as controller area network (CAN), controller area network with flexible data-rate (CAN FD), FlexRay and Ethernet, where over 6000 signals are exchanged on in-vehicle networks. Outside the DACPS, automobiles are connected and cooperated with each other by using different kinds of wireless network technologies, such as V2X (V2V/-V2I/V2N/V2P), BlueTooth, and WIFI, which laid a good basis to realize the intelligent and connected vehicles. However, cybersecurity protection is not considered for protocol of in-vehicle networks, the introduction of various network interfaces brings great cybersecurity challenges for DACPS, Figure 1 shows the 16 potential attack interfaces in DACPS.[2] Different types of attacks have been identified in in-vehicle networks,[3] and the potential security flaws have lead to car recall event recently.[4] NHTSA proposes cybersecurity best practices for modern vehicles,[5] and SAE provides a cybersecurity process framework and guidance in SAE-J3061.[6] Recently, ISO and SAE are cooperated to set the ISO/SAE 21434 standard for automotive cybersecurity.[7]

1.2 | Contributions

There are some recent surveys about cyber-security of in-vehicle networks, such as References 8-10. However, Reference 8 describes mainly the attack interfaces for in-vehicle networks, and it pays little attention to the security protection of in-vehicle networks. The focus of Reference 9 is about the intrusion detection system (IDS) of in-vehicle networks, and although[10] also surveys the security protection techniques for in-vehicle networks, it did not present the security protection framework for DACPS from the system architecture's point of view, it did not present the state-of-the-art works from the perspective of CIA and gives no analysis of each security protection technique's advantages and disadvantages, it did not consider the overhead that would be brought by security protection, and most importantly, it gives no thorough comparison between different security protection techniques.

The main contributions of this article are as follows: (1) we analyze the vulnerabilities of in-vehicle networks, and define the cybersecurity protection requirements for DACPS; (2) we analyze the future trend of in-vehicle network's architecture, based on it we define the cybersecurity protection framework for DACPS; (3) we give a comprehensive survey about the state-of-the-art works of each cybersecurity protection technology, and give an analysis of each security protection technique's advantages and disadvantages; (4) we give a thorough comparison among different cybersecurity protection technologies; (5) we summarize the key challenges for cybersecurity protection of DACPS, and some possible solutions are proposed to solve these challenges as well.

1.3 | Article organization

This article is organized as follows: Section 2 gives the vulnerability analysis and security requirement definition of in-vehicle networks. Section 3 presents architecture evolution of in-vehicle networks, and proposes the cybersecurity protection framework for DACPS. In Section 4, the state-of-the-art works about cybersecurity protection technologies are survey and compared, and Section 5 describes the key challenges and the possible solutions for cybersecurity protection of DACPS. The article is concluded in Section 6.

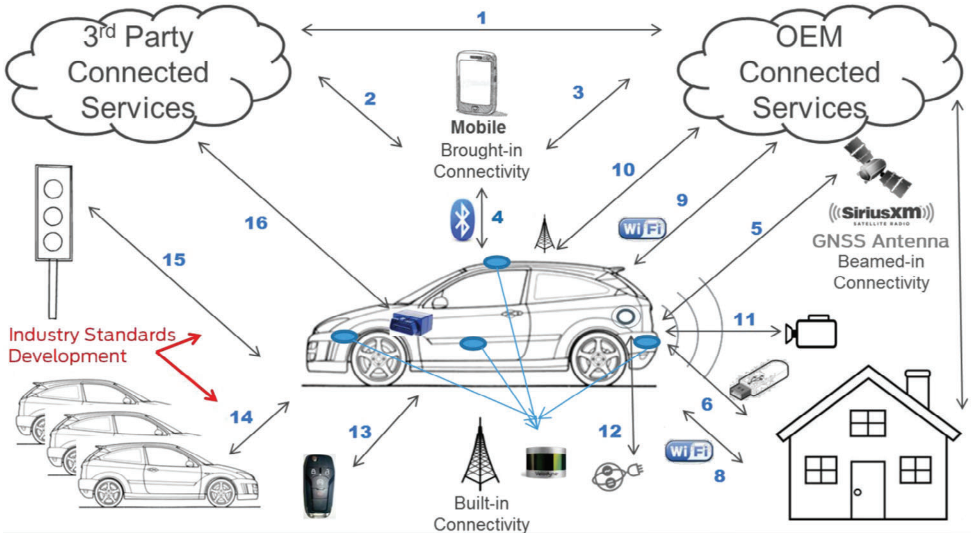
3rd Party Connected Services
1
OEM Connected Services
2
3
Mobile
Brought-in Connectivity
10
9
4
Wi Fi
5
((SiriusXM)) SATELLITE RADIO
GNSS Antenna Beamed-in Connectivity
16
15
11
7
Industry Standards Development
14
13
12
6
Wi Fi
8
Built-in Connectivity

FIGURE 1 The 16 potential attack surfaces for DACPS[2]

2 | SECURITY REQUIREMENT DEFINITION AND VULNERABILITY ANALYSIS OF IN-VEHICLE NETWORKS

2.1 | Security requirement definition

Cybersecurity is the preservation of availability, integrity, and confidentiality of information in the cyberspace. For traditional information systems, availability indicates that information should be accessible and usable upon appropriated demand by an authorized user (prevention of unauthorized withholding of information), confidentiality indicates the prevention of unauthorized disclosure of information, integrity indicates the unauthorized writing or modification of information. The importance of the three elements of cybersecurity are ordered as confidentiality, integrity, and availability. While for in-vehicle networks, availability indicates the security against interruption of messages, confidentiality indicates the security of a message against being read by an attacker, and integrity indicates protection against creation or alteration of messages. The DACPS is a typical safety-critical system, it is of the most significance to guarantee that the DACPS functions are executed correctly and timely in any cases. As the interruption of messages will lead to the corruption of DACSP functions, which would cause economic damage or even fatal accidents, thus availability is the most important element for cybersecurity of in-vehicle networks, and the importance of the three elements of cybersecurity are ordered as availability, integrity, and confidentiality.

2.2 | Vulnerability analysis

In current DACPS, the most common in-vehicle networks are local interconnect network (LIN), CAN/CAN FD, media oriented system transport (MOST), FlexRay and Ethernet, and they are employed in different subsystems of DACPS to meet specific requirements. For example, LIN is usually employed for body electronic functions, such as air conditioner and seat heaters; CAN is usually employed for powertrain functions, chassis functions and body electronics; FlexRay is usually employed for X-by-wire functions, such as steer-by-wire and brake-by-wire; MOST is usually employed for infotainment functions, and Ethernet is usually employed for instrument cluster, diagnose port and gateway. Table 1 shows the comparison between different in-vehicle networks.

Due to the characteristics of high performance, low cost and high reliability, CAN is the most widely used network protocol in DACPS, thus current research about cyber-security of in-vehicle networks is mainly about CAN. CAN is proposed by Robert Bosch GmbH in 1986, thereafter it is standardized in ISO 11898 and ISO 11519, and established itself as the standard protocol for in-vehicle network. When CAN is proposed, there is little electronic functions inside the automobiles, and the electronic system inside the automobile is a closed system at that time. As a result, no cybersecurity protection mechanism is employed in the specification of CAN protocol. When it comes to the era of internet of vehicles, CAN is exposed to the attackers. The vulnerabilities of CAN are listed as follows:

- Confidentiality: CAN is a multimaster protocol, and message transmission is granted based on carrier sense multiple access with collision detection method, which means that message can be received by any node in CAN network.
- Authenticity: no information is attached in message to authenticate its sender, which means that potential attackers can masquerade and replay message.

TABLE 1 The comparison between different in-vehicle networks

	LIN	CAN	FlexRay	MOST	Ethernet
Maximum data rate	19.2 kbps	1 Mbps	10 Mbps	150 Mbps	100 Mbps
Topology	Linear bus	Linear bus, star, ring	Linear bus, star, or hybrid	Ring	Linear bus, star
Cost	Low	Medium	High	High	Medium
Main applications	Low bandwidth control	Low bandwidth control, real-time control, safety applications	Real-time control, safety applications	Multimedia transmission	Real-time control, multimedia transmission

Abbreviations: CAN, controller area network; LIN, local interconnect network; MOST, media oriented system transport.

- Availability: messages are arbitrated nonpreemptively based on an unique identifier (ID), which make it easy for an attacker to launch the denial of service (DoS) on the bus, and this would lead to the malfunction of DACPS functions.
- Integrity: CAN uses a cyclic redundancy check (CRC) code to check if a message has been modified by a transmission error, but as it is easy to forge a correct CRC for a fake message, CRC mechanism is inefficient to prevent an attacker from modifying a correct message or creating a false message.
- Nonrepudiation: there is currently no way to prove that a message is sent or received by an ECU.

Due to the characteristics of high time determinism and reliability, FlexRay is employed in safety-critical functions of DACPS, such as steer-by-wire and brake-by-wire function. Thus, some research also try to analyze the security vulnerability of FlexRay communication, and the details are as follows:[11-13]

- Availability: FlexRay is a time-triggered communication protocol, thus time synchronization is a key component of FlexRay. The DoS attack can be mounted on all nodes of a FlexRay network by purposely affecting node synchronization. And as the slots of the static segment are assigned to each node, the DoS attack on a targeted node is also possible by sending the target messages in the appropriate slots to cause message collision.
- Integrity: the spoofing attack against the dynamic segment is possible, as the dynamic segment is used for event-triggered message transmission, any node can send message on the bus when it wins the bus arbitration. While the spoofing attack against the static segment is impossible, as the slots of the static segment are assigned to each node, the spoofing message will cause message collision and lead to the unpredictable bus state.
- Confidentiality: FlexRay also lacks confidentiality protection mechanism, messages sent on the bus can be recorded by an attacker who has access to the network. And as FlexRay is time-triggered and the slots are assigned to specific node, the message related information such as channel, ID, direction and data length can be obtained by the attacker.

3 | SECURITY PROTECTION FRAMEWORK FOR DACPS

The architecture of in-vehicle networks is the fundamental organization of vehicle electrical and electronic components, including ECUs, sensors, actuators, wiring, power distribution, onboard and wireless communication, and so forth, to realize the desired function and performance goals, which emphasis on the interactions and interdependencies among the components and with the environment, as well as the principles guiding the design and evolution. Figure 2 shows the architecture evolution of in-vehicle networks for DACPS.[14] In current automobiles, DACPS are divided into several subsystems, and they are interconnected with a gateway. In each subsystem, several ECUs are connected by an in-vehicle network, such as CAN and FlexRay, and each ECU implements one electronic function. But as the number of electronic functions increases rapidly in DACPS, the number of ECUs also increases, which cause the complexity explosion of DACPS, the sharp increase of wiring length and power consumption and so forth. To meet the SWaP (size, weight, and power) requirement and keep down the cost, several electronic functions are integrated into one ECU. However, as the introduction of different kinds of intelligent distributed functions, such as advanced driver assistance system (ADAS) and autonomous driving, the interaction and interdependency between different ECUs and different subsystems become stronger, which poses high bandwidth requirement on in-vehicle networks and high data processing requirement on gateway. As a result, the architecture of in-vehicle network will evolve from gateway-centralized architecture to domain-controller centralized architecture in the near future. For domain-controller centralized architecture, there is a domain controller in each subsystem (domain), and domain controllers are connected with Ethernet (such as time-sensitive network and time-triggered ethernet) of high bandwidth. Thus, the functions of the gateway is divided into several domain controllers, which would lower down the requirement on data processing for each domain controller. And as the advances of hardware technology, high performance hardware platforms such as multicore, manycore, and GPU will be introduced into DACPS to meet the auto industry's requirement on cost, power consumption, and so forth, and this would further lead to the convergence of different domains.

The architecture of in-vehicle network is composed by ECUs, gateway or domain controllers, in-vehicle networks, and external network interfaces that connect automobiles with surrounding environment (such as WIFI, Bluetooth, and V2X). Thus as Figure 3 shows, the cybersecurity protection framework of in-vehicle networks is divided into four layers, which are ECU level, in-vehicle network level, gateway or domain controller level, and external communication interface level.[15]

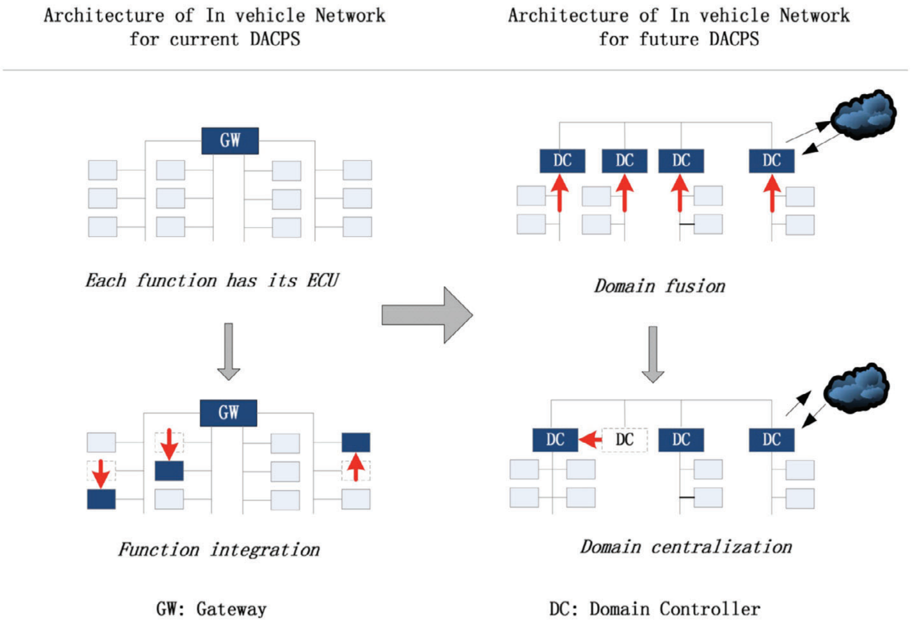
Architecture of In vehicle Network for current DACPS
Architecture of In vehicle Network for future DACPS
GW
Each function has its ECU
GW
Function integration
DC
DC
DC
DC
Domain fusion
DC
DC
DC
DC
Domain centralization
GW: Gateway
DC: Domain Controller

FIGURE 2 The architecture evolution of in-vehicle networks

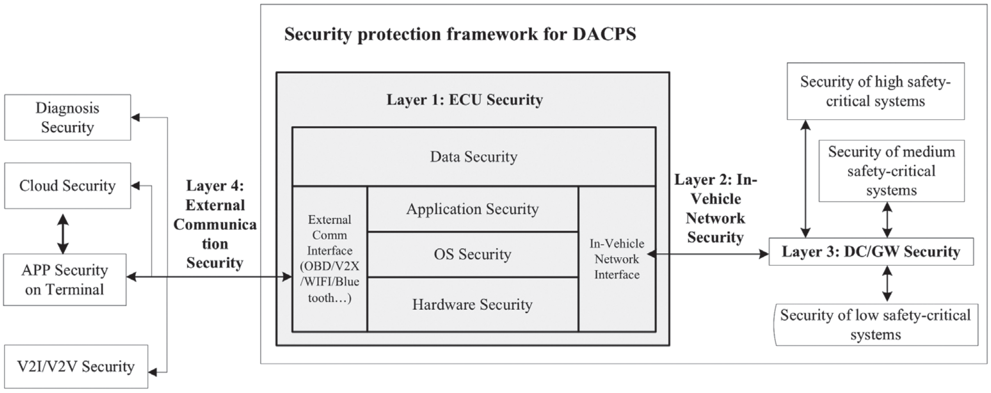
Security protection framework for DACPS
Layer 1: ECU Security
Data Security
External Comm Interface (OBD/V2X /WIFI/Blue tooth…)
Application Security
OS Security
Hardware Security
In-Vehicle Network Interface
Layer 2: In-Vehicle Network Security
Security of high safety-critical systems
Security of medium safety-critical systems
Layer 3: DC/GW Security
Security of low safety-critical systems
Layer 4: External Communica tion Security
Diagnosis Security
Cloud Security
APP Security on Terminal
V2I/V2V Security

FIGURE 3 The security protection framework for distributed automotive cyber-physical systems (DACPS)[15]

- Layer 1: ECU level's cybersecurity. ECU is the physical platform to implement electronic functions, which connects with sensors and actuators. Different kinds of software, such as operating systems (OS), network drivers, and applications are all executed inside the ECU, and the generated data and logs are also kept inside the ECU. As a result, ECU level's cybersecurity can be further divided into hardware security, OS security, application security, and data security.
- Layer 2: In-vehicle network level's cybersecurity. ECUs are communicated with each other based on in-vehicle networks, thus if one ECU is cracked and manipulated by an attacker, it can launch different kinds of attacks (such as the replay attack, masquerade attack and DoS attack) by taking use the vulnerabilities of in-vehicle networks. As a result, security protection mechanisms such as identity authentication, integrity verification, data encryption and decryption, firewall, and so forth, should be employed to protect in-vehicle network's security.
- Layer 3: Gateway or domain controller level's cybersecurity. Gateway and domain controller are the key component to realize the communication and also the isolation between different subsystems. First, gateway and domain controller are a special ECU node in each subsystem, ECU level's security protection should be considered for gateway and domain controller as well. Next, different subsystems have different security requirements, thus security protection mechanisms such as firewall and IDS, should be integrated into the gateway and domain controller to realize the isolation between different subsystems.
- Layer 4: External communication level's cybersecurity. In the era of internet of vehicles, automobile is evolving from a physical entity to a digital entity, and it becomes an IoT nodes in smart city, which interconnect with surrounding environment (such as roadside unit, drivers, other automobiles) by WIFI, Bluetooth, and V2X technologies. As a result,

identity authentication, digital signature, and firewall technologies should be employed to guarantee that automobiles can interact with the external environment securely.

ECU is a typical embedded system, security protection technologies proposed for embedded systems can be reused for ECU directly, interested readers can refer to related surveys for more details.[16,17] The security protection about external network interfaces of DACPS is out of the scope of this article, interested readers can refer to related surveys to get more information.[18,19]

4 | THE STATE-OF-THE-ART WORKS ABOUT SECURITY PROTECTION OF IN-VEHICLE NETWORKS

In this article, we focusing on security protection of in-vehicle networks. As CAN receives the most attention, we survey about the state-of-the-art works about cybersecurity protection technologies of CAN according to the order of importance of the CIA as follows.

4.1 | Availability protection

Availability indicates the security against interruption of messages for in-vehicle networks. If the attacker can access CAN at a level where it can inject any message at any rate, which allows it to launch the DoS attack by flooding the CAN bus with high priority messages. As a result, network traffic of in-vehicle networks should be monitored and analyzed in real-time, and security protection mechanisms such as firewall technology, intrusion detection technology, and so forth, should be employed to guarantee the availability of in-vehicle networks.

4.1.1 | Firewall and secure gateway

With the emerge of new automotive trends such as connected vehicles and V2X connectivity, automobile can no longer be regarded as a closed system as an increasing number of external interfaces with unpredictable input are introduced into it. As a result, all incoming external traffics have to be monitored and analyzed for potential malicious data, as they will affect the proper functioning of safety-critical functions inside the DACPS. Furthermore, DACPS are divided into several subsystems with different security requirements, and they are interconnected by gateway or domain controllers in future E/E architecture of DACPS. Thus, internal communication between different ECUs and different subsystems represents a considerable amount of traffic and constitutes another attack surface. Consequently, firewall technologies such as stateless packet filter, stateful packet inspection, proxy servers, and application layer firewall with deep packet inspection are also needed to be implemented into the switching ECUs, such as gateway, domain controller, in-vehicle infotainment system, and T-Box.

Kurachi et al.[20] propose a secure gateway with characteristics of whitelist-based firewall, DoS attack detection and response, centralized authentication and malware detection, and the gateway is also implemented and evaluated based on automotive grade controller. Luo and Hu[21] define security requirements of gateway based on threat analysis, where the message-filter based firewall is employed to isolate untrusted network domain from trusted network domain, a key master function is realized for key distribution and update, the HMAC-based authentication and AES encryption are employed for secure in-vehicle communication. The secure gateway is implemented based on hardware security module (HSM)-attached MPC5748G to show its effectiveness. Pese et al.[22] give a hardware and software codesign method for automotive firewall, which employs whitelist-based policy and status monitoring-based policy to realize the packet filter. The hardware and software implementation of the firewall is based on Aurix TC297-TF and Altera Cyclone V FPGA, respectively, and the delay, jitter, CPU load and memory consumption of the firewall is analyzed. Rizvi et al.[23] propose a distributed implementation of automotive firewall, where the malicious message filtering function is placed at each ECU. Seifert and Roman[24] suggest to use hierarchical timed automata to describe the internal communication behaviors, and based on it, a communication behavior specification-based secure gateway is implemented. Table 2 gives a summarization about the proposed firewall technologies for in-vehicle networks.

	20	21	22	23	24
Availability protection	Yes	No	Yes	Yes	Yes
Integrity protection	Yes	Yes	Yes	Yes	No
Confidentiality protection	No	Yes	No	No	No
Hardware support	Yes	Yes	Yes	No	No
Bandwidth cost	Low	Mid	No	No	No
Computation cost	Low	Mid	Mid	Mid	Low

TABLE 2 The summarization about the firewall technologies

4.1.2 | Intrusion detection systems

IDS is usually used for security protection of information systems, and many works also try to introduce it for availability protection of in-vehicle networks. We summarize and divide the state-of-the-art works about IDS of CAN into four categories as follows.

Physical characteristics-based IDS

CAN message do not carry any identity information, it is difficult to tell if a message is sent by a genuine ECU or not. Although the message authentication code (MAC) plus freshness value (FV) approach can solve this problem, it would bring considerable bandwidth and timing overheads, and how to realize global synchronization of FV remains challenging. Nevertheless, each ECU has unique physical invariants, such as clock offset, voltage distribution, and signal characteristics, which can be used as the fingerprint information to identify the genuine ECU, thus it can tell if an intrusion is happened on the CAN network or not.

Each ECU has a unique quartz crystal clock, there is a small difference in clock frequency of any two clocks, and this is defined as the clock skew. Clock skew can be used to implement an IDS to identify attacks launched by malicious ECUs. Cho and Shin[25] use timestamps of periodically received messages to get the clock skew of each ECU and posit messages with the same skew are sent from the same ECU. The advantage of the clock skew based IDS is that it needs no hardware support or software modification, while the disadvantage of this approach is that it can be used for periodically received message only. But the message scheduling, queuing, and arbitration delay will cause deviation in message's period, which would make the clock skew based IDS unstable.

Murvay and Groza[26] and Choi et al.[27] suggest to use the inimitable signal characteristics for ECU's fingerprinting, this kind of IDS can be used for both periodically and aperiodically transmitted messages. But it needs to add a monitor node to extract characteristics from measured signals, and complex analysis methods such as support vector machine (SVM), neural network (NN), and bagged decision tree are employed for classification and ECU identification, which would cause considerable timing and memory overheads.

Voltage characteristics are also used for fingerprinting of ECU. Ning et al.[28] propose a local outlier factor based IDS which uses the waveform characteristics of voltage for ECU identification, and this method can be used for detection of spoofing attack and bus-off attack. Choi et al.[29] also provide a voltage characteristics based ECU identification method for IDS, and this method is robust against environmental factors by using incremental learning. Sagong et al.[30] explore attack surfaces of voltage-based IDS, they give three voltage-based attacks and a hardware-based intrusion response system by disconnecting the attacker ECU from CAN network. Besides, Wang et al.[31] propose an IDS based on the physical location of the ECU in the CAN network to help in identifying malicious ECU, and this is realized by monitoring the unique delay difference between the dominant to recessive transition of CAN controller. Table 3 shows a comparison about the physical characteristics-based IDS.

	31	27	29	25
Computation overhead	Mid	High	High	Low
Hardware support	Yes	Yes	Yes	No
Avoid injection attack	Yes	Yes	Yes	Yes
Avoid masquerade attach	Yes	Yes	Yes	Yes
Avoid DoS attack	Yes	No	Yes	No
Avoid replay attack	No	Yes	Yes	Yes

TABLE 3 The comparison about the physical characteristics-based intrusion detection systems

The physical characteristics-based IDS does not depend on the timing properties (such as period and jitter) or data content of the transmitted messages, thus it has high ability of generalization. It adds no extra content into the message, so no bandwidth overhead is introduced. And it requires no modification to CAN controller, which makes it to be compatible with existing CAN systems. However, it is still challenging to extract stable physical characteristics in automotive grade level, as the harsh environment inside the automobiles such as huge temperature range, vibrations, and electromagnetic interference will make those features unstable and inconsistent.

Timing interval-based IDS

Most messages are sent periodically on the CAN bus, thus an IDS can be realized by monitoring the message intervals (message period) and the average message content changes. Ying et al.[32] propose a covert-channel based ECU identification method via a centralized monitor node, where the interarrival time based covert channel can be used for periodically transmitted messages, and the least significant bit based covert channel can be used for aperiodically transmitted messages. Taylor et al.[33] give an IDS that measures intermessage timing over a sliding window, and the average times are compared with historical averages to yield an anomaly alert. Salem et al.[34] use interarrival curve to analyze the message's traces by providing upper and lower bounds of the interarrival occurrence, and a classification framework that detects deviations within these bounds is further provided for IDS. Olufowobi et al.[35] propose a specification-based IDS, where the timing specification is generated based on schedulability analysis of CAN messages. This work is extended by improving the classification performance, expansion of the evaluation using additional metrics and data from real attacks Olufowobi et al..[36] Song et al.[37] and Moore et al.[38] both propose message interval-based IDS and evaluate how different types of message injection attacks affect the timing intervals of CAN messages.

The timing interval-based IDS is like the statistical based IDS, which assumes that messages' period is known beforehand and remain unchangeable, but the message scheduling, queuing, and arbitration delay will cause much noise in message's arriving time, which would make the timing interval-based IDS unstable. Young et al.[39] found that message's period will change for different driving modes, and it provide a message frequency-based IDS which is effective for different driving modes.

Entropy-based IDS

Entropy is used to indicate the randomness of a system, and some research use entropy to evaluate the normal behavior of CAN traffic. This is because that message's period, message's length, and message's payload are specified in the design phase, thus the traffic of in-vehicle networks is relatively restricted. If security attacks (such as masquerade attack, replay attack, and injection attack) are launched on in-vehicle networks, the entropy of it will be increased. Given a set of classes C_X for a dataset X, where each data item belongs to a class $x \in C_X$, the entropy of X relative to C_X is defined as follows:[40]

$$H(X) = \sum_{x \in C_X} P(x) \log \frac{1}{P(x)}. \tag{1}$$

Consequently, entropy-based IDS can be realized by monitoring if the entropy of in-vehicle network's traffic exceeds the specified threshold.

Muter and Asaj[40] first introduce the entropy for IDS of CAN network, but they only consider one single class of CAN traffic, and only a simple attacking scenario that message with all 0's is evaluated. Later, Marchetti et al.[41] propose another entropy-based IDS that considers different kinds of forged CAN messages at variable rates, and this method is evaluated based on real CAN traffic gathered from an unmodified licensed vehicle in real driving conditions. Wu et al.[42] suggest to use sliding window strategy to avoid information entropy interference caused by different baud rate and aperiodic CAN messages, and a simulated annealing (SA)-based heuristic algorithm is used to choose the best sliding window parameters for entropy-based IDS.

The advantage of entropy-based IDS is that it requires no detailed information about the semantic meaning of CAN messages, and it can be used for CAN with both periodically triggered and aperiodically triggered messages. But the difficulty is how to analyze and decide the threshold for entropy-based IDS, as this is the key to judge if an intrusion is happened or not.

Artificial learning-based IDS

Artificial intelligence algorithms have shown their effectiveness on data processing in several applications, such as image processing, speech recognition, copyright protection of intellectual protection circuit resource,[43,44] and so forth. They are also introduced to implement the IDS for in-vehicle networks recently. The basic principles of this approach is to train the artificial intelligence model to get the features of normal CAN messages first, and then by monitoring the exchanging message and comparing it with the artificial intelligence model to distinguishing between normal and abnormal messages.

Kang and Kang[45] use deep NN to train high-dimensional CAN message to analyze the underlying statistical properties of normal and hacking messages to extract the corresponding features, and by monitoring the exchanging message on CAN bus to decide whether the CAN system is being attacked or not. Jichici et al.[46] evaluate the possibilities for integrating the NN-based IDS on automotive-grade embedded platforms, and the experiment results show that this task is quite challenging due to large requirement of memory size and computational power. Pawelec et al.[47] test the effectiveness of employing DNN to predict CAN message at the bit level, which would offer the IDS capability but avoiding reverse engineering proprietary encodings of CAN messages. Kuwahara et al.[48] study the applicability of statistical anomaly detection methods to identify malicious CAN messages, where a pipeline technology is proposed to extract the timestamp and ID information in each messages quickly, and the efficiency of the proposed method is evaluated in real message datasets and in supervised and unsupervised cases. Besides NNs, other artificial intelligence algorithms, such as LSTM,[49] Bayesian networks,[50] hidden Markov models,[51] SVM,[52] compound classifier,[53] and singular spectrum analysis[54] are also introduced to build an IDS for CAN bus.

One of the key prerequisites of artificial learning-based IDS is that it needs to conduct reverse-engineering investigation of CAN to get message parameters, such as message ID, message payload, and so forth. And as Jichici et al.[46] find that artificial intelligence algorithm-based IDS would introduce too much computational, timing and memory overhead, while automotive-grade embedded platforms are usually based on 16 bit and 32 bit embedded processors, thus artificial intelligence algorithm-based IDS is difficult to be implemented on real vehicles. Furthermore, the data and the related code are not open for most existing works, which makes it difficult to compare them fairly. Last but not least, current research focus on intrusion detection only, little attention has paid to the construction of the response mechanism for DACPS, which are the key backup strategy to guarantee the safety of DACPS. Table 4 gives a comparison about the proposed artificial learning-based IDS methods, and Table 5 gives a comparison about the different types of IDS.

TABLE 4 The comparison about the different artificial learning-based IDS

Reference	Algorithm	Real implementation	Real data	Open data or code
45	DNN	No	No	No
46	Neural networks	Yes	Yes	No
47	LSTM	No	Yes	No
48	Statistical method	No	Yes	No
49	Transfer learning	No	Yes	No
50	Bayesian network	Yes	No	No
51	HMM	No	Yes	No
52	SVM	No	Yes	No
53	Compound classifier	No	Yes	No
54	Singular spectrum analysis	Yes	Yes	Yes

Abbreviation: BCs, boundary conditions.

TABLE 5 The comparison about the different types of IDS

IDS Types	Overhead	Physical environment impacted	Ability of dynamic evolution	Ability of generalization
Physical characteristics-based	High	Yes	No	High
Time-interval-based	Mid	No	No	Average
Entropy-based	Mid	No	Yes	Average
Artificial learning-based	High	No	Yes	Low

Abbreviation: IDS, intrusion detection system.

4.2 | Integrity protection

4.2.1 | MAC and FV

If an attacker has access to a CAN network at a level where they can receive and send message, it would not want to break a system but instead extract or manipulate status or control information.[55] Thus, integrity protection of CAN attracts lots of attention right now.

AUTOSAR proposes to address the integrity and authenticity protection of in-vehicle networks by combining the MAC with FV, and this approach is standardizing as the SecOC specification.[56] Both MAC and FV are attached to the message payload to be transmitted on the bus, where the adding of MAC can avoid masquerade attack and tampering attack, and the adding of FV can avoid replay attack. The detailed processing flow of SecOC is shown in Figure 4. First, the message sender and receiver have to agree on a shared cryptographic key, this key can be loaded into the ECUs during production by OEMs. Then, the sender adds a FV into the payload, and computes the MAC based on message data and FV by using symmetric encryption algorithms, such as CMAC standardized in NIST SP 800-38B.[57] The message data, MAC and FV form the payload of a secured message that will be transmitted on the bus. For message receiver, it dissembles the message payload to message data, MAC and FC first. And then, it compares the received FV to the last successfully verified and internally stored FV, computes the MAC itself and compares the result with the received MAC. If there is no match, the message is dropped and ignored. Since the payload of CAN is limited to 8 bytes, both MAC and FV need to be truncated. Table 6 shows the SecOC profiles about the length of MAC and FV.

As the security-enhancing operations such as MAC generation, message encryption, and decryption are computation-intensive tasks, which would bring considerable timing and resource overhead, and key management and distribution related cost. DACPS is a typical safety-critical system, most electronic functions in DACPS are required to meet the tight timing constraints. Furthermore, automobiles are mass-produced products, resource, and hardware related cost are also need to be considered seriously for the design and optimization of DACPS.

Wu et al.[58] analyze the timing overhead of security enhancing operations based on Infineon's Aurix processors. According to their experiment results, the software implementation of AES128 consumes as high as 1196 μs, which cannot meet the timing requirement of DACPS. Aurix has a HSM attached as the security coprocessor, the HSM-based hardware implementation of AES128 is only 48.7 μs. Thus, HSM-based security mechanism is recommended by auto industry as

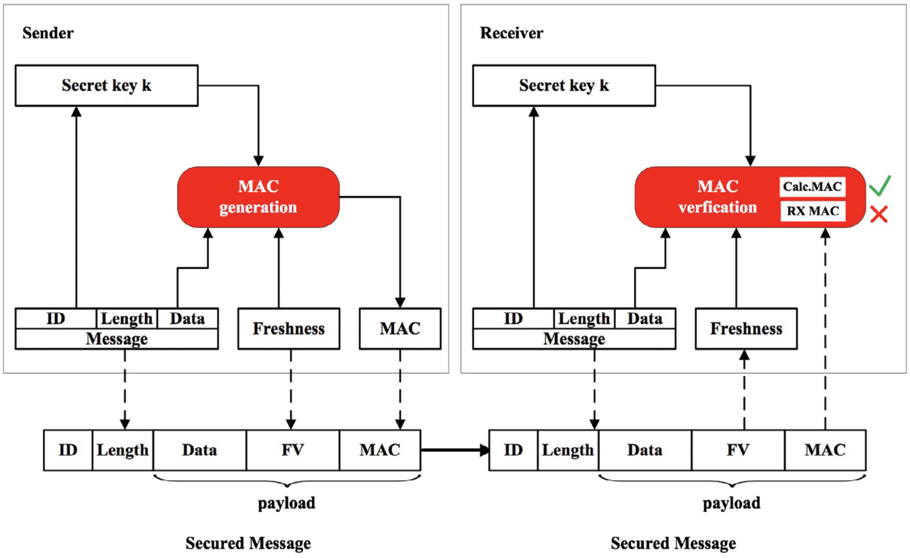

FIGURE 4 The processing flow recommended by AUTOSAR SecOC specification[56]

TABLE 6 The security profiles given in AUTOSAR SecOC specification[56]

Network	Profile 1	Profile 2	Profile 3
MAC (in bits)	8	0	4
FV (in bits)	24	24	24

Abbreviations: FV, freshness value; MAC, message authentication code.

it would decrease the timing and memory overhead of security-enhancing operations to an acceptable level. The EVITA project[59] proposes three kinds of HSM implementation, including the light HSM for sensors and actuators, medium HSM for in-vehicle networks, full HSM for V2X communications. Stumpf[60] compare HSM with other hardware-assisted security mechanisms, such as trusted platform modules, Smart Card, on-chip security engines, and secure hardware extension. The HIS organization propose the specification of HSM.[61] Automotive processor suppliers such as Infineon, Renesas, and Freescale are producing HSM-attached MCU, such as Aurix, JDP PowerPC, ICM-M, and so forth. OEM and Tier-1 suppliers are providing HSM-based security protection solutions, such as ESCRYPT's CycurHSM[62] and Elektrobit's zentur HSM.[63]

HSMs offer a number of advantages, such as secure key storage, secure cryptographic engine (hardware implementation of symmetric/asymmetric cryptographic algorithms and hash functions), secure log, and so forth. However, HSM-based mechanism will introduce extra hardware cost. Taking Aurix processors from Infineon as an example, the Aurix TC299TP-128F300N and Aurix TC299T128F300S are with similar performance (in terms of CPU and memory), but the price of Aurix TC299TP128F300N (about 47 dollars) is higher than that of the Aurix TC299T128F300S (about 41 dollars) as it has the HSM, the adding of HSM increases the hardware cost of Aurix TC299TP128F300N by about 15%.[64]

As HSM will introduce hardware cost for DACPS, Gu et al.[65] propose to minimize the HSM-related hardware cost under the timing and security constraints for FlexRay-based DACPS, and both a mixed-integer linear programming (MILP) based method and a SA-based method are proposed to solve this problem. Lin et al.[66] assume that MAC and FV are added into message to protect the integrity of CAN, and the end-to-end worst-case response time are optimized by exploring the task assignment and message scheduling. Based on the same system model, they also propose heuristic algorithm to minimize the security risk.[67] Xie et al.[68] propose a new multilevel security model for CAN, and a MILP formulation of the signal packing is suggested to minimize the bandwidth utilization. Xie et al.[69] propose another security model based on AUTOSAR SecOC specification, and both a MILP formulation and a heuristic algorithm are proposed for signal packing to minimize the bandwidth utilization of CAN FD under the security and schedulability constraints. Aminifar et al.[70] research about the trade-off between security protection and timing overhead, and an optimization algorithm is given to maximize confidentiality under real-time constraints in a dynamic setting. Table 7 summarize the state-of-the-art works about integrity protection of in-vehicle networks. Xie et al.[71] give a security enhancement approach for CAN FD-based parallel automotive applications, where as many as the bytes of MACs are added into CAN FD payload by exploiting the laxity interval from the lower bound to the deadline.

Although the MAC plus FV approach is effective in integrity protection of in-vehicle networks and is also standardized in AUTOSAR's SecOC specification, there are three challenges that need to be resolved before it can be applied to real automobiles: (1) it assumes that cryptographic keys are preshared between message senders and receivers, nevertheless it is challenge to manage and distribution keys among ECUs and automobiles for OEMs, this would lead to another security flaw if this problem is not handled properly. The message authentication protocol is proposed to solve this problem. (2) the MAC generation and verification would bring considerable timing overhead, although the HSM-based hardware implementation can decrease it to an acceptable level, it brings extra hardware cost as well. (3) the adding of MAC and FV into message payload would expand the message to a large extent, although the truncation of MAC and FV would decrease the message expansion to some extent, this approach is acceptable only if a risk assessment yields a solid argumentation.

TABLE 7 The summarization about the integrity protection of CAN

Reference	Network	Objective	Constraint	Algorithm	Security consideration
65	FlexRay	Hardware cost	Timing	MILP, SA	HSM for integrity and confidentiality
66	CAN	End to end timing	Security	MILP	MAC and FV for integrity
67	CAN	Security risk of direct attack	Timing	Heuristic algorithm	MAC and FV for integrity
68	CAN	Bandwidth utilization	Timing and security	MILP	MAC and FV for integrity
69	CAN FD	Bandwidth utilization	Timing and security	MILP	MAC and FV for integrity
70	CAN	Confidentiality	Timing	MILP	Iterated block ciphers for confidentiality

Abbreviations: CAN, controller area network; FV, freshness value; HSM, hardware security module; MAC, message authentication code; MILP, mixed-integer linear programming; SA, simulated annealing.

To sum up, system-level design optimization algorithms should be proposed to realize the trade-off between security protection and the related overheads.

4.2.2 | Message authentication protocol

To ensure real-time behavior of in-vehicle networks, many security protection mechanisms (such as MAC and FV-based integrity protection, message encryption-based confidentiality protection) require that cryptographic keys are preshared between message senders and receivers. However, this ignores the key management and distribution related risks. Thus, message authentication protocols are proposed for security protection of in-vehicle network.

Van Herrewege et al.[72] propose CANAuth for CAN+, which is an extension of CAN that would increase the bandwidth to 16 times. CANAuth uses 128-bit preshared group keys to establish group session keys of the same length, and 80-bit HMAC and 32-bit counter are added into every authenticated message to guarantee the message freshness. As CANAuth assign one key for each message ID, it would require a large number of keys to be stored on each ECU, and the long HMAC and counter bring too much overhead. Schweppe et al.[73] propose an authentication framework that includes entity authentication and policy-based access control. They assume that a HSM is attached in each ECU, and one or several key masters are exist for key distributions. Each ECU uses two preshared keys with the key master, one for authenticating itself, and another for sending generated session keys. Groza et al.[74] give another authentication protocol called LiBrA-CAN, which is based on key splitting and MAC mixing. The key management of LiBrA-CAN is rather complex, and as every message needs to be authenticated, LiBrA-CAN also has high bandwidth overhead. Hartkopp et al.[75] devise an on-demand authentication protocol using 32-bit CMAC, where it employs a key master for session key management and a time master to avoid replay attack. Kurachi et al.[76] propose a centralized authentication architecture CaCAN, where a monitor node verifies the signature of each message. If authentication fails, the monitoring node can discard message by overriding it with an error frame using a special CAN controller. This approach requires specific hardware support, and the monitoring node is possible to be a single point of failure. Woo et al.[77] propose another authentication protocol, where all ECUs contact with the gateway to derive the initial authentication keys during the start-up, and the keys need to be updated for each session. Mundhenk et al.[78] propose a lightweight authentication protocol which can enable the secure and efficient distribution of symmetric keys among ECUs without preshared keys. They combine symmetric and asymmetric cryptographic methods to realize a two-phase authentication of ECUs and message traffic, and by leveraging the fixed architecture of in-vehicle networks, the bandwidth and computation overheads are minimized. Jo et al.[79] suggest an authentication protocol MAuth-CAN that can secure against masquerade attack and DoS attack. MAuth-CAN requires no hardware modification of CAN controller, and it needs to transmit an additional CAN message only when an attack message is discovered, thus it has low bandwidth overhead. Table 8 shows a comparison about the proposed message authentication protocols.

4.2.3 | Message ID hopping and obfuscation

Each CAN message has a unique ID, which indicates its priority during the arbitration phase. Some research try to enforce randomness and obfuscation on message's ID to improve the CAN network's security, such as defending against starvation

TABLE 8 The summarization about the message authentication protocols

Reference	Hardware support	Bandwidth overhead	Implementation details	Back compatibility
72	Yes	High	No	No
73	Yes	High	Yes	No
74	No	High	Yes	No
75	No	High	No	Yes
76	Yes	Mid	Yes	No
77	No	Low	Yes	No
78	No	Low	Yes	Yes
79	No	Low	Yes	Yes

attack, replay attack, improving the ability to resist against reverse engineering, and avoiding attacking spreading across a fleet of vehicles with the same platform.

Han et al.[80] propose the ID anonymization mechanism IA-CAN that provides sender authentication. For IA-CAN, message ID are encrypted and refreshed for each message during the communication process, thus only ECU with shared keys can receive the message successfully, and masquerade attack and starvation attack can be prevented. Sun et al.[81] give a dynamic ID virtualization method that keeps the relative priority order of messages, this can prevents CAN logs from being analyzed and makes it difficult for attackers to generate valid messages. Xia et al.[82] extends IA-CAN with a robust recovery mechanism, and a central monitor node is employed to realize the synchronization and anonymized ID generation. The ID generation information are also transmitted by authenticated messages to prevent replay attack. Humayed and Luo[83] propose a software implemented ID hopping mechanism, where an offset is preshared among ECUs, and a new set of alternative IDs are generated if an attack is detected. This mechanism is lightweight as no hopping information need to be transmitted among ECUs, but the software implementation of ID-hopping will introduce considerable delay. Wu et al.[84] give a new ID hopping mechanism based on message counter and ID hopping table, and existing CAN controller needs to be replaced with a FPGA-based ID hopping controller to realize ID translation. Lukasiewycz et al.[85] suggest to use the quadratically constrained quadratic program approach to assign a fixed set of IDs for each message, and then a Monte Carlo method is further employed to determine the specific priority assignment for each vehicle. Madl et al.[86] propose to obfuscate ID and message content using randomization and permutation of data and ID filed, which would create unique CAN profiles for each vehicle. Xie et al.[87] present a security-aware obfuscated priority assignment for CAN FD, where a fast sequence pruning technique is employed to reduce the undesirable priority assignment sequence and improve the verification acceptance rate. Woo et al.[88] propose to use network address shuffling technology to realize ID shuffling, where one-time IDs are generated using a one-way hash function with a group session key and counter value. This approach can keep the relative priority of messages, and prevent replay attack, masquerade attack. Table 9 shows a comparison about the proposed message ID hopping and obfuscation methods.

4.3 | Confidentiality protection

As symmetric encryption methods can achieve the same level of security with much smaller keys than asymmetric approaches and can be implemented compactly and efficiently in software and hardware,[56] they are employed for message encryption of in-vehicle networks. Jiang et al.[89] propose an iterated block ciphers based symmetric encryption method (AES) for confidentiality protection of in-vehicle networks, and they formulate a constraint logic programming-based optimization problem that considers both security and schedulability constraints, and the objective is to minimize the number of FPGA unit that need to be added into the system for encryption and decryption operations. Amnifar et al.[70] also propose to use iterated block ciphers based symmetric encryption method (RC5/RC6) for confidentiality protection of in-vehicle networks, they formulate a tradeoff problem between confidentiality protection and the amount of resource overhead, and propose heuristic method to maximize confidentiality while guaranteeing the schedulability of real-time

	80	83	84	85	86	88	81	82
Bandwidth cost	Low	Low	Low	–	Mid	Low	Low	Low
Computation cost	Low	Mid	Low	–	Mid	Mid	Mid	Low
Hardware cost	No	No	Yes	No	No	No	No	No
Key management	Yes	Yes	No	No	Yes	Yes	Yes	Yes
Avoid masquerade attack	No	No	No	No	No	Yes	No	Yes
Avoid replay attack	Yes	No	Yes	No	No	Yes	No	Yes
Avoid starvation attack	Yes	Yes	Yes	No	No	No	No	Yes
Avoid attack spreading	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
Confidentiality protection	No	No	No	No	Yes	Yes	No	No
Limit reverse engineering	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes

TABLE 9 The summarization about the ID hopping and obfuscation methods

TABLE 10 The summarization about the confidentiality protection methods

	89	70	90	91
Security algorithm	AES	RC5/RC6	AES for confidentiality, HMAC for integrity	SPECK64/128
Constraint	Timing	Timing	Timing and reliability	–
Optimization algorithms	Constraint logic programming, list scheduling	Heuristic algorithm	Heuristic algorithm	–
Integrity consideration	No	No	Yes	Yes
Hardware support	Yes	No	No	No
Dynamic setting support	No	Yes	No	No

applications. Munir and Koushanfar[90] consider the integrated design of secure and dependable CAN using a case study of steer-by-wire application, where AES is employed for confidentiality protection, HMAC is employed for integrity and authentication protection. Bella et al.[91] achieve the security in terms of authenticity, integrity, and confidentiality by leveraging the Chaskey MAC algorithm for MAC generation and the lightweight block cipher algorithm SPECK64/128 for message encryption and decryption. Table 10 shows a comparison about the proposed confidentiality protection methods.

Confidentiality received relatively little attention for security protection of in-vehicle networks, as message encryption and decryption are needed to be implemented for both message senders and message receives, respectively. Even for unidirectional message transmission (such as diagnosis information and logs), and message transmission between ECUs with different level of security requirement, message receivers are required to be capable of message decryption, which would cause too much computation and timing overhead and hardware cost.

4.4 | Comparison between different security protection mechanisms

As it explained from Sections 4.1 to 4.3 that several kinds of security mechanisms are proposed to protect the availability, integrity, and confidentiality of in-vehicle networks, Table 11 summarize the advantages and disadvantages of these mechanisms, hoping it would give a general guidance to choose specific protection mechanisms for a given DACPS.

TABLE 11 The comparison among different types of security protection mechanisms

Protection mechanism	Objective	System layer	Ability of dynamic evolution	Timing overhead	Bandwidth overhead	Cost
MAC+FV	Integrity	In-vehicle network	No	Mid	Mid	HW, KEY
Message authentication protocol	Integrity, confidentiality	In-vehicle network	No	Mid->high	Mid->high	KEY
ID hopping and obfuscation	Integrity, availability	In-vehicle network	No	Mid	No	HW, KEY
Message encryption	Confidentiality	In-vehicle network	No	Mid	No	HW, KEY
Firewall and secure gateway	Availability	GW, DC	Yes	Mid	No	No
IDS	Availability, integrity	GW, DC	Yes	High	No	No

Note: GW indicates gateway, DC indicates domain controller, HW cost indicates hardware related cost, such as adding a HSM into ECU and modifying CAN controller for ID hopping and obfuscation; KEY cost indicates key management and distribution related cost, as special equipment and management system are needed to be employed to generate and protect the key in a secure and efficient manner.

5 | CHALLENGES AND POSSIBLE SOLUTIONS FOR SECURITY PROTECTION OF IN-VEHICLE NETWORKS

Cybersecurity protection of in-vehicle networks has attracted a lot of attention from both the industry and the academic world. Although existing works provide some solutions to improve the availability, integrity, and confidentiality of in-vehicle networks, there are still several serious challenges as follows that require great efforts to be made.

5.1 | Risk assessment and management

Risk assessment and management is the basis for security protection, as the security requirement and the corresponding security level are defined based on the risk assessment results, and the security requirement determines which security protection mechanism should be employed. The process of risk assessment focuses on the identification of assets, the analysis of possible vulnerabilities and the evaluation and measurement of possible damages to users, while no mature risk assessment method and tool exists for DACPS. The NIST Special Publication (SP) 800-82 provides a comprehensive cybersecurity approach for securing industrial control systems (ICS), and it considers the performance, reliability and safety requirement of ICS, thus this standard would be tailed for DACPS. Existing security risk assessment methods such as attack tree analysis, CYPSec, STPA-sec, Bayesian network, and block-chain can be employed for DACPS. In addition to this, the STRIDE threat modeling tool developed by Microsoft Corporation can also be used to evaluate the security risk of all kinds of wire and wireless interfaces. Currently, the ISO/SAE 21434 standard about the cybersecurity engineering of road vehicles is undergoing to tackle automotive cybersecurity issues and protecting assets, the draft of this standard is available.

5.2 | Lightweight and low cost security protection mechanisms

Automotive grade embedded controllers are mostly 16-bit and 32-bit, they have quite limited computation power and memory size. Most in-vehicle networks have relatively low bandwidth, such as CAN, its maximal bandwidth is 1 Mbps, and the message payload is limited to be 8 bytes. While existing research pay not enough attention about these facts, they would cause considerable computational, timing and resource overhead and cost, which restrict their application on real vehicles. Considering the fact that automobiles are mass produced, lightweight and low cost security protection mechanisms are in urgent need and of real value for auto industry.

We suggest that much efforts can be made in the following aspects: (1) lightweight and distributed IDS can be employed to decrease the requirement on memory size and computational power, and the placement of the detecting tasks should be optimized to ensure the full-coverage of the whole in-vehicle network. Furthermore, different sensors are employed to realize the intelligent distributed DACPS functions (such as ADAS), thus the sensor consistency and function dependency can also be incorporated into the IDS to downsize the IDS; (2) the MAC plus FV approach will introduce considerable timing and memory overhead, the introduction of HSM-attached processor can decrease the overhead to an acceptable level. However, HSM introduce extra hardware cost as well, and the schedulability analysis of messages for the HSM-based security architecture is still an open problem. The hardware cost can be decreased by only adding HSM to those ECU with high security level, but system level optimization methods that explore the task allocation, signal packing, and message scheduling should be proposed. (3) as the evolution of E/E architecture of DACPS, high-performance computing (HPC) platform (such as manycore, GPU) will be introduced into DACPS as domain controllers or central computing node, where several functions can be integrated on those HPC platforms. However, how to realize the tradeoff between the safety and resource efficiency is still an open research problem.

5.3 | Holistic security protection framework with the ability of dynamic evolution

The lifecycle of automobiles can be as long as 10–15 years, attacking techniques will evolve and updated in this process, thus the security protection mechanisms applied during the production of automobiles will become ineffective. Furthermore, more and more software contents and network interfaces will be introduced into the automobiles to realize the automotive trends such as autonomous vehicles and connected vehicles, the security flaws in DACPS will be increasing as well.

As Table 11 shows that different security protection mechanisms have their own advantages and disadvantages, thus a holistic security framework that employs multilayered security mechanisms should be employed for DACPS, which can realize the complete security protection loop (from access control, intrusion detection, influence decreasing to system's flaw fixing and update). Table 11 summarizes the possible security protection mechanisms that can be employed in the different system layer of DACPS. In addition, the security protection framework should has the ability of dynamic evolution, which means that the applied security protection mechanisms should be dynamically evolvable and extensible to tackle with new attacks. IDS and access control method are helpful to do this job, but they are concentrating on intrusion detection only right now, the system response mechanism that cannot only identify and block attacks, but also limit the DACPS functions to safe operation and activate corresponding security counter-measures, should also be implemented to guarantee the safety of DACPS. Furthermore, as the evolution of E/E architecture of DACPS, both the vehicle level IDS and the cloud level IDS should be implemented and combined to monitor all the network traffics, events and logs inside and outside of the DACPS. Update over-the-air (OTA) function should be employed as well, as it can realize the remote update of ECU's firmwares, thus the security protection ability of DACPS can be updated and improved accordingly.

5.4 | An integrated approach to functional safety and cybersecurity

The placement of safety-critical mechanism components with electronic components has led to an increasing risks from systematic failures and random hardware failures, which poses great challenges on dependability and reliability of DACPS.[92,93] Thus, safety plays a central role in the development of DACPS, such as ADAS system, X-by-wire systems, and so forth. And recently, the automotive trends toward autonomous and connected vehicles make cybersecurity another key factor to be taken into consideration by auto industry. Lack of safety, reliability, availability, integrity, and other dependability properties might lead to the malfunction of safety-critical functions, which could cause property loss, or even casualty accidents. ISO 26262 is a standardized functional safety process that is initially proposed for functional safety of automobiles, an important recent trend is to adapt it for security engineering. While functional safety address systematic and random faults resulting in malfunctioning behavior of E/E systems, cybersecurity address issues resulting from malicious intent external to the E/E systems. Although the range of concerns is not the same for functional safety and cybersecurity, they are having a considerable overlap. To achieve functional safety, it can be advantageous to get relevant information from cybersecurity (such as the employed security protection mechanisms), as it can negatively influence functional safety or can support the achievement of functional safety. As a result, an integrated analysis and verification framework with both safety and security considerations should be employed for the design and implementation of DACPS.

As it recommended in the second edition of ISO 26262, in order to support the completeness of the hazard analysis and risk assessment and the safety goals, cybersecurity threats should be analyzed as a hazard from a functional safety's perspective. Functional safety can provide information such as hazards and related risks to support the identification of cybersecurity threats. To defend against a detected attack, cybersecurity protection mechanisms will be employed in the E/E system. Their impact to the behavior of the E/E system should be evaluated to determine if there is any potential impacts on safety goals or safety concepts.

5.5 | Cybersecurity protection of DACPS in the era of IoT

In the era of IoT, automobile becomes a moving digital node that communicates with surrounding environment (such as other automobiles, roadside units, passengers, and so forth) through V2X technologies, different kinds of sensors and actuators, and so forth. Due to the increasing importance of automobiles in people's daily life, V2X networks, sensors such as camera and LIDAR are becoming a major target for attackers, making them vulnerable to physical threats, wire and wireless network threats. In-vehicle data shared with third-parties would lead to the misuse of the requested data for other purposes than stated, so privacy-related attacks (such as driver fingerprinting, driving behavior analysis and location analysis) attract increasing attention worldwide. Thus, the safety and privacy of passengers, automobiles, roads and other entities inside the IoT system, will influence each other, the cybersecurity and privacy protection of DACPS cannot be isolated from the safety of surrounding IoT environment.

The cybersecurity of automobiles should be considered from the system of system's (SoS) point of view. Although the V2X technologies increase the attack surfaces of automobiles, the cooperation between different individual systems (such as DACPS and roadside units) inside the SoS are capable based on the data sharing of them, thus their ability to defend against attacks will be enhanced as well. And through the crosslayer cooperation on security enhancing (from vehicle layer, to edge computing layer and cloud server level), the security event logging and analysis capabilities of DACPS are enforced and become extensible, and its ability to defend against new attacks can be improved instantly with the OTA support.

6 | CONCLUSION

As the use of information technologies in automobiles is advancing, the importance of cybersecurity is also increasing. Especially for in-vehicle networks, as no security mechanisms is employed in their protocols, which poses great challenges for safety guarantee of DACPS. First, this article analyzes the cybersecurity vulnerabilities and defines the security requirements for in-vehicle networks. Second, the architecture evolution of in-vehicle network are introduced, and based on it, a security protection framework is defined for in-vehicle networks. And then, it surveys the current practices for availability protection, integrity protection, and confidentiality protection of in-vehicle networks, respectively, and gives detailed analysis about the advantages and disadvantages of the proposed cybersecurity protection mechanisms. Finally, future challenges on cybersecurity protection of in-vehicle networks are analyzed, and possible solutions are proposed to tackle these challenges.

ACKNOWLEDGMENTS

This work was supported by the National Natural Science Foundation of China under Grant No. 61872436 and No. 61972210, in part by the Natural Science Foundation of Fujian Province, China under Grant No. 2018J01571, NUPTSF under Grant No. NY220133 and No. XK0040920081, the Research Foundation of NJUPT for “1311 Talents Training Project,” and the Research Foundation of Jiangsu for “333 High Level Talents Training Project” under Grant No. BRA2020065.

ORCID

Yong Xie https://orcid.org/0000-0001-8728-2757
Jian Zhou https://orcid.org/0000-0002-1864-3894

REFERENCES

1. Fischer A. Bosch pools its software and electronics expertise in one division with 17,000 associates; 2020. https://www.bosch-presse.de/pressportal/de/en/bosch-pools-its-software-and-electronics-expertise-in-one-division-with-17000-associates-216256.html. Accessed June 22, 2020.
2. Boran L, Czerny BJ, Ward D, Mira H. Overview of recommended practices-SAE J3061; 2020. https://nmi.org.uk/wp-content/uploads/2016/06/4_SAE-J3061-and-friends-for-NMI-Jun-16.pdf. Accessed July 23, 2020.
3. Koscher K, Czeskis A, Roesner F, et al. Experimental security analysis of a modern automobile. Paper presented at: Proceedings of the IEEE Symposium on Security and Privacy; 2010; California.
4. With ’recall’ fiat chrysler makes its car hack worse; 2016. www.networkworld.com/article/2953836/security/with-recall-fiat-chrysler-makes-its-car-hack-worse. Accessed November 10, 2016.
5. National Highway Traffic Safety Administration (NHTSA), Cybersecurity best practices for modern vehicles; 2016. https://www.nhtsa.gov/technology-innovation/vehicle-cybersecurity. Accessed December 20, 2016.
6. SAE standard J3061: cybersecurity guidebook for cyber-physical vehicle systems; 2016. http://standards.sae.org/wip/j3061/. Accessed December 30, 2016.
7. ISO/SAE 21434; 2020. https://www.iso.org/standard/70918.html. Accessed July 26, 2020.
8. Li X, Yu Y, Sun G, Chen K. Connected vehicles’ security from the perspective of the in-vehicle networks. *IEEE Netw*. 2018;32(3):58-63.
9. Wu W, Li R, Xie G, et al. A survey of intrusion detection for in-vehicle networks. *IEEE Trans Intell Transp Syst*. 2020;21(3):919-933.
10. Bozdal M, Samie M, Aslam S, Jennions I. Evaluation of CAN bus security challenges. *Sensors*. 2020;20(8):1-16.
11. Kishikawa T, Hirano R, Ujiie Y, et al. Intrusion detection and prevention system for FlexRay against spoofed frame injection. Paper presented at: Proceedings of the Embedded Security in Cars; 2019; Detroit Metropolitan,
12. Murvay PS, Groza B. Practical security exploits of the FlexRay in-vehicle communication protocol. Paper presented at: Proceedings of the International Conference on Risks and Security of Internet and Systems; 2018; Arcachon, France.
13. Nilsson D.K, Larson U.E, Picasso F, Jonsson E. A first simulation of attacks in the automotive network communications protocol FlexRay. Paper presented at: Proceedings of the International Workshop on Computational Intelligence in Security for Information Systems; 2008; Genova, Italy.

14. Lock A. Robert Bosch GmbH trends of future E/E architecture. 2020. https://www.gsaglobal.org/wp-content/uploads/2019/05/Trends-of-Future-EE-Architectures.pdf. Accessed July 23, 2020.
15. ESCYPRT Multi-layered protection concepts; 2019.. https://www.escrypt.com/en/solutions/protection-concepts. Accessed October 1, 2019.
16. Serpanos DN, Voyiatzis AG. Security challenges in embedded systems. *ACM Trans Embed Comput Syst*. 2013;12(1s):66.1-66.10.
17. Ravi S, Raghunathan A, Kocher PC, Hattangady S. Security in embedded systems: design challenges. *ACM Trans Embed Comput Syst*. 2004;3(3):461-491.
18. Luo Q, Liu JJ. Wireless telematics systems in emerging intelligent and connected vehicles: threats and solutions. *IEEE Wirel Commun Mag*. 2018;25(6):113-119.
19. Sharma S, Kaushik B. A survey on internet of vehicles: applications, security issues and solutions. *Veh Commun*. 2019;20:100182.1-100182.44.
20. Kurachi R, Takada H, Mizutani T, Ueda H, Horihata S. SecGW-secure gateway for in-vehicle networks. *Paper presented at: Embedded Security in Cars*. Romulus, Michigan; Detroit Metropolitan; 2015.
21. Luo F, Hu Q. Security mechanisms design for in-vehicle network gateway. SAE technical papers.2018-01-0018; 2018.
22. Pese MD, Schmidt K, Zweck H. Hardware/software co-design of an automotive embedded firewall. SAE technical paper. 2017-01-1659; 2017.
23. Rizvi R, Willett J, Perino D, Vasbinder T, Marasco S. Protecting an automobile network using distributed firewall system. Paper presented at: Proceedings of the International Conference on CAN; 2017; Nuremberg, Germany.
24. Seifert S, Roman O. Secure automotive gateway-secure communication for future cars. Paper presented at: Proceedings of the IEEE International Conference on Industrial Informatics; 2014; Porto Alegre, Brazil.
25. Cho KT, Shin KG. Fingerprinting electronic control units for vehicle intrusion detection. Paper presented at: Proceedings of the USENIX Security Symposium; 2016; Austin.
26. Murvay PS, Groza B. Source identification using signal characteristics in controller area networks. *IEEE Signal Process Lett*. 2014;21(4):395-399.
27. Choi W, Jo HJ, Woo S, Chun JY, Park J, Lee DH. Identifying ECUs using inimitable characteristics of signals in controller area networks. *IEEE Trans Veh Technol*. 2018;67(6):4757-4770.
28. Ning J, Wang JD, Liu JJ, Kato N. Attacker identification and intrusion detection for in-vehicle networks. *IEEE Commun Lett*. 2019;23(11):1927-1930.
29. Choi W, Jo HJ, Woo S, et al. low-level communication characteristics for automotive intrusion detection system. *IEEE Trans Inf Forens Secur*. 2018;13(8):2114-2129.
30. Sagong SU, Ying X, Poovendran R, Bushnell L. Exploring attack surfaces of voltage-based intrusion detection systems in controller area networks. Paper presented at: Proceedings of the Embedded Security in Cars. Brussels, Belgium; 2018.
31. Wang Q, Qian YM, Lu ZJ, Shoukry Y, Qu G. A delay based plug-in-monitor for intrusion detection in controller area network. Paper presented at: Proceedings of the Asian Hardware Oriented Security and Trust Symposium; 2018; Hong Kong, China.
32. Ying XH, Bernieri G, Conti M, Poovendran R. TACAN: transmitter authentication through covert channels in controller area networks. Paper presented at: Proceedings of the ACM/IEEE International Conference on Cyber-Physical Systems; 2019; Montreal, CA.
33. Taylor A, Japkowicz N, Leblanc S. Frequency-based anomaly detection for the automotive can bus. Paper presented at: Proceedings of the World Congress on Industrial Control Systems Security; 2015; London, UK.
34. Salem M, Crowley M, Fischmeister S. Anomaly detection using inter-arrival curves for real-time systems. Paper presented at: Proceedings of the Euromicro Conference on Real-Time Systems; 2016; Toulouse, France.
35. Olufowobi H, Bloom G, Young C, Zambreno J. Real-time modeling for intrusion detection in automotive controller area network. Paper presented at: Proceedings of the Real-Time Systems Symposium, Work-in-Progress; 2018; Nashville.
36. Olufowobi H, Young C, Zambreno J, Bloom G. SAIDuCANT: specification-based automotive intrusion detection using controller area network (CAN) timing. *IEEE Trans Veh Technol*. 2020;69(2):1484-1494.
37. Song HM, Kim HR, Kim HK. Intrusion detection system based on the analysis of time intervals of CAN messages for in-vehicle network. Paper presented at: Proceedings of the International Conference on Information Networking; 2016; Kota Kinabalu, Malaysia.
38. Moore MR, Bridges RA, Combs FL, Starr MS, Prowell SJ. Modeling inter-signal arrival times for accurate detection of CAN bus signal injection attacks: a data-driven approach to in-vehicle intrusion detection. Paper presented at: Proceedings of the 12th Annual Conference on Cyber and Information Security Research; 2017; Oak Ridge.
39. Young C, Olufowobi H, Bloom G, Zambreno J. Automotive intrusion detection based on constant CAN message frequencies across vehicle driving modes. Paper presented at: Proceedings of the ACM Workshop on Automotive Cybersecurity; 2019; Richardson Texas.
40. Muter M, Asaj N. Entropy-based anomaly detection for in-vehicle networks. Paper presented at: Proceedings of the IEEE Intelligent Vehicles Symposium; 2011; Baden-Baden, Germany.
41. Marchetti M, Stabili D, Guido A, Colajanni M. Evaluation of anomaly detection for in-vehicle networks through information-theoretic algorithms. Paper presented at: Proceedings of the IEEE International Forum on Research and Technologies for Society and Industry Leveraging a Better Tomorrow; 2016; Bologna, Italy.
42. Wu WF, Huang YZ, Kurachi R, et al. Sliding window optimized information entropy analysis method for intrusion detection on in-vehicle networks. *IEEE Access*. 2018;6:45233-45245.
43. Liang W, Huang W, Long J, Zhang K, Li K, Zhang D. Deep reinforcement learning for resource protection and real-time detection in IoT environment. *IEEE IoT J*. 2020;7(7):6392-6401.

44. Liang W, Zhang D, Lei X, Tang M, Zomaya Y. Circuit copyright blockchain: blockchain-based homomorphic encryption for IP circuit protection. *IEEE Trans Emerg Top Comput*. 2020. https://doi.org/10.1109/TETC.2020.2993032.
45. Kang MJ, Kang JW. A novel intrusion detection method using deep neural network for in-vehicle network security. Paper presented at: Proceedings of the Vehicular Technology Conference Spring; 2020; Nanjing, China.
46. Jichici C, Groza B, Murvay PS. Examining the use of neural networks for intrusion detection in controller area networks. Paper presented at: Proceedings of the International Conference on Innovative Security Solutions for Information Technology and Communications, SecITC 2018, Bucharest, Romania; 2018:109-125; Springer, Berlin, Germany.
47. Pawelec K, Bridges RA, Combs FL. Towards a CAN IDS based on a neural-network data field predictor. Paper presented at: Proceedings of the ACM Workshop on Automotive Cybersecurity; 2018; Richardson.
48. Kuwahara T, Bara Y, Kashima H, et al. Supervised and unsupervised intrusion detection based on CAN message frequencies for in-vehicle network. *J Inf Process*. 2018;26:306-311.
49. Tariq S, Lee S, Woo SS. CANTansfer-transfer learning based intrusion detection on a controller area network using convolutional LSTM network. Paper presented at: Proceedings of the ACM/SIGAPP Symposium on Applied Computing; 2020; Brno, Czech Republic.
50. Bezemskij A, Loukas G, Gan D, Anthony RJ. Detecting cyber-physical threats in an autonomous robotic vehicle using Bayesian networks. Paper presented at: Proceedings of the IEEE International Conference on Internet of Things; 2017; Exeter, UK.
51. Boumiza S, Braham R. An efficient hidden Markov model for anomaly detection in CAN bus networks. Paper presented at: Proceedings of the International Conference on Software, Telecommunications and Computer Networks; 2019; Split, Croatia.
52. Avatefipour O, AI-Sumaiti AS, EI-SHerbeeny AM, et al. An intelligent secured framework for cyberattack detection in electric vehicles'CAN bus using machine learning. *IEEE Access*. 2019;7:127580-127592.
53. Tomlinson A, Bryans J, Shaikh SA. Using a one-class compound classifier to detect in-vehicle network attacks. Paper presented at: Proceedings of the Genetic and Evolutionary Computation Conference Companion; 2018; Kyoto, Japan.
54. Nowdehi N, Aoudi W, Almgren M, Olovsson T. CASAD: CAN-aware stealthy-attack detection for in-vehicle networks; 2019. https://arxiv.org/abs/1909.08407. Accessed September 26, 2019.
55. Pfeiffer O, Keydel C. Scalable CAN security for CAN, CANopen and other protocols. Paper presented at: Proceedings of the International Conference on CAN; 2017; Nuremberg, Germany.
56. AUTOSAR Specification of module secure onboard communication, release 4.3.0; 2019. www.autosar.org. Accessed June 2, 2019.
57. NIST Recommendation for block cipher modes of operation: the CMAC mode for authentication, special publication 800-38B; 2017. https://www.nist.gov/publications/recommendation-block-cipher-modes-operation-methods-format-preserving-encryption. Accessed July 23, 2017.
58. Wu Z, Zhao J, Zhu Y, Li Q. Research on vehicle cybersecurity based on dedicated security hardware and ECDH algorithm. SAE technical paper ; 2017-01-2005; 2017.
59. Evita project; 2014. https://www.evita-project.org. Access June 9, 2014.
60. Stumpf F. An analysis and comparison of hardware security modules for the automotive domain. Paper presented at: Proceedings of the Embedded Security in Cars; 2014; Detroit Metropolitan.
61. Herstellerinitiative software (HIS), SHE secure hardware extension, version 1.1; 2013. http://portal.automotive-his.de. Accessed February 2, 2013.
62. ESCYPRT CycurHSM. https://www.escrypt.com/en/products/cycurhsm. Accessed October 1, 2018.
63. Elektrobit zentur HSM. https://www.elektrobit.com/products/security/. Accessed July 23, 2020.
64. The price of aurix processors. https://www.arrow.com. Accessed May 23, 2020.
65. Gu ZH, Han G, Zeng HB, Zhao QL. Security-aware mapping and scheduling with hardware co-processors for Flexray-based distributed embedded systems. *IEEE Trans Parall Distrib Syst*. 2016;27(10):3044-3057.
66. Lin CW, Zhu Q, Phung C, Sangiovanni-Vincentelli A. Security-aware mapping for CAN-based real-time distributed automotive systems. Paper presented at: Proceedings of the IEEE/ACM International Conference on Computer-Aided Design; 2013; San Jose, CA.
67. Lin CW, Zhu Q, Sangiovanni-Vincentelli A. Security-aware modeling and efficient mapping for CAN-based real-time distributed automotive systems. *IEEE Embed Syst Lett*. 2014;7(1):11-14.
68. Xie Y, Liu LJ, Li RF, Hu JQ, Han Y, Peng X. Security-aware signal packing algorithm for CAN-based automotive cyber-physical systems. *IEEE/CAA J Automat Sin*. 2015;2(4):422-430.
69. Xie Y, Zeng G, Kurachi R, Takada H, Xie GQ. Security/timing-aware design space exploration of CAN FD for automotive cyber-physical systems. *IEEE Trans Ind Inform*. 2019;15(2):1094-1104.
70. Aminifar A, Eles P, Peng ZB. Optimization of message encryption for real-time applications in embedded systems. *IEEE Trans Comput*. 2018;67(5):748-754.
71. Xie G, Yang LT, Wu W, Zeng K, Xiao X, Li R. Security enhancement for real-Time parallel in-vehicle applications by CAN FD message authentication. *IEEE Trans Intell Transp Syst*. 2020. https://doi.org/10.1109/TITS.2020.3000783.
72. Van Herrewege A, Singelee D, Verbauwhede I. CANAuth-a simple, backward compatible broadcast authentication protocol for CAN bus. Paper presented at: Proceedings of the Embedded Security in Cars. Dresden, Germany; 2011.
73. Schweppe H, Roudier Y, Weyl B, Apvrille L, Scheuermann D. Car2x communication: securing the last meter-a cost-effective approach for ensuring trust in car2x applications using in-vehicle symmetric cryptography. Paper presented at: Proceedings of the Vehicular Technology Conference Fall; 2011; San Francisco.

74. Groza B, Murvay S, Van Herrewege A, Verbauwhede I. LiBrA-CAN: a lightweight broadcast authentication protocol for controller area networks. Paper presented at: Proceedings of the International Conference on Cryptology and Network Security, CANS 2012; 2012:185-200; Springer, Berlin, Germany.
75. Hartkopp O, Reuber C, Schilling R. MaCAN-message authenticated CAN. Paper presented at: Proceedings of the Embedded Security in Cars. Dresden, Germany; 2012.
76. Kurachi R, Matsubara Y, Takada H, Adachi N, Miyashita Y, Horihata S. CaCAN-centralized authentication system in CAN(controller area network). *Paper presented at: Embedded Security in Cars*. Romulus, Michigan; Detroit Metropolitan; 2014.
77. Woo S, Jo HJ, Lee DH. A practical wireless attack on the connected car and security protocol for in-vehicle CAN. *IEEE Trans Intell Transp Syst*. 2015;16(2):993-1006.
78. Mundhenk P, Paverd A, Mrowca A, et al. System level design approaches to security in automotive networks. *ACM Trans Des Automat Electron Syst*. 2017;22(2):25.1-25.27.
79. Jo HJ, Kim JH, Choi HY, Choi W, Lee DH, Lee I. MAuth-CAN: masquerade-attack-proof authentication for in-vehicle networks. *IEEE Trans Veh Technol*. 2020;69(2):2204-2218.
80. Han K, Weimerskirch A, Shin KG. A practical solution to achieve real-time performance in the automotive network by randomizing frame identifier. *Paper presented at: Embedded Security in Cars*. Romulus, Michigan; Detroit Metropolitan; 2015.
81. Sun H, Lee SY, Joo K, Jin H, Lee DH. Catch ID if you CAN: dynamic ID virtualization mechanism for the controller area network. *IEEE Access*. 2019;7:158237-158249.
82. Xia ZF, Kawabata T, Komano Y. A secure design for practical identity-anonymized CAN application. Paper presented at: Proceedings of the Embedded Security in Cars. Munich, Germany; 2016.
83. Humayed A, Luo B. Using ID-hopping to defend against targeted DoS on CAN. Paper presented at: Proceedings of the International Workshop on Safe Control of Connected and Autonomous Vehicles; 2017; Pittsburgh PA.
84. Wu WF, Kurachi R, Zeng G, Matsubara Y, Takada H, Li RF. IDHCC: a security-enhanced ID hopping CAN controller design to guarantee real-time. Paper presented at: Proceedings of the Workshop on Security and Dependability of Critical Embedded Real-Time Systems; 2017; Paris, France.
85. Lukasiewycz M, Mundhenk P, Steinhorst S. Security-aware obfuscated priority assignment for automotive CAN platforms. *ACM Trans Des Autom Electron Syst*. 2016;21(2):32.1-32.32.
86. Madl T, Bruckmann J, Hof HJ. CAN obfuscation by randomization(CANORa). Paper presented at: Proceedings of the ACM Computer Science in Cars Symposium; 2018; Munich, Germany.
87. Xie G, Li R, Hu S. Security-aware obfuscated priority assignment for CAN FD messages in real-time parallel automotive applications. *IEEE Trans Comput-Aid Des Integrat Circuits Syst*. 2020;39(12):4413-4425.
88. Woo S, Moon D, Youn TY, Lee Y, Kim Y. CAN ID shuffling technique (CIST): moving target defense strategy for protecting in-vehicle CAN. *IEEE Access*. 2019;7:15521-15536.
89. Jiang K, Eles P, Peng ZB. Co-design techniques for distributed real-time embedded systems with communication security constraints. Paper presented at: Proceedings of the Design, Automation and Test in Europe Conference; 2012; Dresden, Germany.
90. Munir A, Koushanfar F. Design and analysis of secure and dependable automotive CPS: a steer-by-wire case study. *IEEE Trans Depend Secure Comput*. 2018;17(4):813-827.
91. Bella G, Biondi P, Costantino G, Matteucci I. Are you secure in your car? Paper presented at: Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks; 2019; Miami.
92. Zhou J, Sun J, Zhang M, Ma Y. Dependable scheduling for real-time workflows on cyber-physical cloud systems. *IEEE Trans Ind Inform*. 2020. https://doi.org/10.1109/TII.2020.3011506.
93. Zhou J, Zhang M, Sun J, Wang T, Zhou X, Hu S. DRHEFT: deadline-constrained reliability-aware HEFT algorithm for real-time heterogeneous MPSoC systems. *IEEE Trans Reliab*. 2020. https://doi.org/10.1109/TR.2020.2981419.

How to cite this article: Xie Y, Zhou Y, Xu J, Zhou J, Chen X, Xiao F. Cybersecurity protection on in-vehicle networks for distributed automotive cyber-physical systems: State-of-the-art and future challenges. *Softw Pract Exper*. 2021;51:2108–2127. https://doi.org/10.1002/spe.2965