International Journal of Automotive Technology, Vol. 19, No. 5, pp. 879–894 (2018)
DOI 10.1007/s12239–018–0085–1

pISSN 1229–9138/ eISSN 1976–3832

REVIEW OF SECURE COMMUNICATION APPROACHES FOR IN-VEHICLE NETWORK

Qiang Hu and Feng Luo*

Clean Energy Automotive Engineering Center, School of Automotive Studies, Tongji University, Shanghai 201804, China

(Received 20 November 2017; Revised 18 March 2018; Accepted 15 April 2018)

ABSTRACT–In the connected vehicles, connecting interfaces bring threats to the vehicles and they can be hacked to impact the vehicles and drivers. Compared with traditional vehicles, connected vehicles require more information transfer. Sensor signals and critical data must be protected to ensure the cyber security of connected vehicles. The communications among ECUs, sensors, and gateways are connected by in-vehicle networks. This paper discussed the state-of-art techniques about secure communication for in-vehicle networks. First, the related concepts in automotive secure communication have been provided. Then we have compared and contrasted existing approaches for secure communication. We have analyzed the advantages/disadvantages of MAC and digital signatures for message authentication and compared the performance and limitations of different cryptographic algorithms. Firewall and intrusion detection system are introduced to protect the networks. The constraints and features of different intrusion detection approaches are presented. After that, the technical requirements for cryptographic mechanism and intrusion detection policy are concluded. Based on the review of current researches, the future development directions of the automotive network security have been discussed. The purpose of this paper is to review current techniques on automotive secure communication and suggest suitable secure approaches to implement on the in-vehicle networks.

KEY WORDS : Cyber security, Vehicle network, Secure communication, Intrusion detection

1. INTRODUCTION

The in-vehicle networks were isolated when originally designed. The design process didn't take the security mechanisms for networks into account. With the development of automotive network technology, the external interfaces on the car gradually increased, cyber security of automotive has become a new problem. Charlie Miller and Chris Valasek achieved the invasion of Toyota Prius and Ford Escape in 2013 and remotely invaded a Jeep Cherokee in 2015 (Miller and Valasek, 2013, 2015). Craig Smith put forward the possible paths of vehicle cyber attacking from the perspective of penetration testing (Smith, 2016). Researchers analyze the security issues in vehicles by experimental attacking (Checkoway *et al*., 2011; Koscher *et al*., 2010; Weimerskirch, 2011), the results show the severity of vehicular cyber-attacks. Petit *et al*. investigate potential network attacks and vulnerabilities for autonomous vehicles, the possible attack targets include traffic signs, machine vision, GPS signals, sensors, radar signals, lidar signals, navigation and so on (Petit and Shladover, 2015). Attacks against vehicles can be divided into logical attacks (password attacks, software attacks, communications attacks, etc.), physical attacks (side channel attacks, denial of service attacks, interference attacks, penetration attacks, tamper attacks, etc.) and other attacks (Wolf, 2009).

The National Highway Traffic Safety Administration (NHTSA) points out that the targets of modern vehicle cyber attacking are as follows (McCarthy and Harnett, 2014):

(1) Critical security data of vehicles, such as the communication data of V2X, and the signals related to autonomous driving;
(2) Critical business information such as the intellectual property of the Original Equipment Manufacturer (OEM);
(3) Automotive comfort systems, such as the infotainment systems;
(4) Automotive critical signals related to safety, including the signals for engine control, brake control, and steering control.

By now, researches on the cyber security of vehicles have been carried out in Japan, the United States, and Europe. In Japan, the Information-Technology Promotion Agency (IPA) released a guide to the approaches for protecting the vehicles information security in 2013. This guide presents an IPA-Car security model and proposes corresponding security strategies for various security

**Corresponding author.* e-mail: luo_feng@tongji.edu.cn

threats (Kobayashi *et al*., 2013). In the United States, the NHTSA has also been working on automotive cyber security issues for years, including establishing the Automotive Information Sharing and Analysis Center (AUTO-ISAC), developing the automotive cyber security standards (J3061, J3101), and so on (McCarthy *et al*., 2014). The targets of AUTO-ISAC are sharing the cyber threats on vehicles and working to deal with cyber-attacks on vehicles. J3061 is the first guidance document for the cyber security process in the automotive development lifecycle, including software design, hardware design and system design (SAE, 2016a). In Europe, some vehicles cyber security related projects are carried out by automotive manufacturers and research institutions, such as the E-Safety Vehicle Intrusion Protected Applications (EVITA, 2008-2011) and the Open Vehicular Secure Platform (OVERSEE, 2010-2012). In the EVITA project, researchers establish a vehicular cyber security architecture based on the three-level Hardware Security Module (HSM) and propose multiple security protocols, including key distribution, multi-purpose ECUs, policy management, secure bootstrapping, secure over-the-air firmware updates, key updates, secure transportation, and secure storage (Schweppe *et al*., 2011; Weyl *et al*., 2011). In the OVERSEE project, researchers establish a standardized and secure platform for developing vehicular applications (Grote *et al*., 2011).

In this paper, the basic concepts in secure communication are introduced. And in the following, we presented the techniques for secure communication, including message authentication, data encryption, and intrusion protection. The technical requirements of cryptographic mechanisms and intrusion detection policy are proposed. At last, we discussed the future directions of secure communication developments.

2. BASIC CONCEPT

A typical automotive network architecture can be divided into four layers from the perspective of security (Navale *et al*., 2015). As is seen in Figure 1, an automotive security architecture contains:

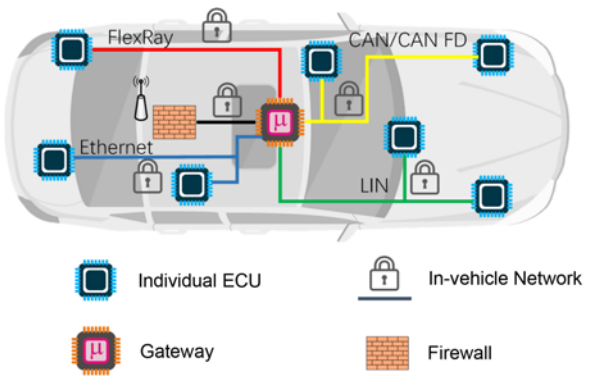

Figure 1. Automotive security network architecture.

(1) **Individual ECU Layer**: This layer contains software trusted execution and data protection, provides hardware foundation for upper layers security mechanism.
(2) **In-vehicle Network Layer**: Cryptography related mechanisms can be used to encrypt the transferring data in the network.
(3) **Gateway Layer**: Gateway layer has the critical security functions, including access control and intrusion detection, this layer helps the data exchange in different network domain (Seifert and Obermaisser, 2014).
(4) **Firewall Layer**: Firewall layer is used to protect the outside communication interfaces of vehicles, such as OBD-II interface, V2X on-board unit, and infotainment system.

In the following, the concepts about secure hardware, vehicle network, and security requirements will be introduced.

2.1. Security Hardware

Compared with traditional Microcontroller Unit (MCU), the main features of security MCU are secure storage and hardware-based cryptography algorithms. Besides, some security MCUs also provide other mechanisms like secure bootstrapping, firmware protection, and key distribution. The specifications about security hardware are mainly the following three:

(1) **Secure Hardware Extension (SHE)**: Herstellerinitiative Software (HIS) released the SHE specification in 2009. This specification mainly contains the realization of Cryptographic Service Engine (CSE) on MCUs and definitions of the application interface for encryption and decryption. Secure boot protocol and key distribution protocol are also defined (Escherich *et al*., 2009).
(2) **Hardware Secure Module**: In the European EVITA project, three kinds of HSM are designed according to the security requirements of the in-vehicle network communication. For example, the Light HSM can be used for communication between sensors and actuators, the Medium HSM for communication between ECUs, and the Full HSM usually be used for V2X communication. The cryptographic building blocks of HSM include encryption/decryption engine, random number generator, counter and so on. In the specifications of HSM, hardware components and software application interfaces are defined (Weyl *et al*., 2011). Besides, in the AUTomotive Open System Architecture (AUTOSAR) specifications, security-related interfaces are defined to be compatible with HSM (AUTOSAR, 2016a).
(3) **Trusted Platform Module (TPM)**: TPM 2.0 automotive thin profile was released in 2015 by Trusted Computing Group (TCG). Since the TPM was used on computer platform originally, the environment

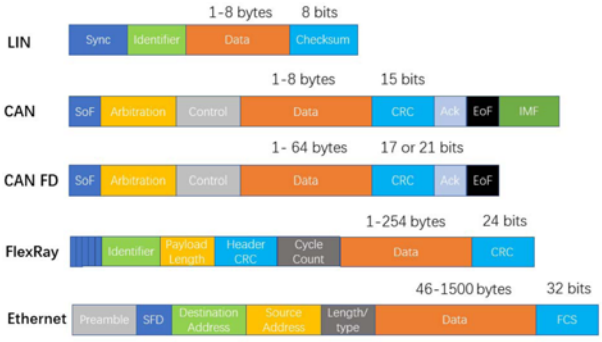

Figure 2. Frame structure of automotive network.

of vehicles can be too hard for TPM. Infineon and Toyota have developed the automotive-grade TPM. For some ECUs in vehicles, the computation performance is constrained, but integrity and certification are required. Automotive TPM is used as a security element of those ECUs. A typical usage of automotive TPM is the remote firmware update of ECU. Creation and verification of digital signatures can be achieved with automotive TPM (Trusted Computing Group, 2015).

2.2. Vehicle Network

In vehicles, signals and data are transferred by the automotive network system. Some typical vehicle networks are introduced in the following:

(1) **Controller Area Network (CAN)/Controller Area Network with Flexible Data Rate (CAN FD)**: CAN bus is the most widely used network in the field of the automotive network, it plays a major role in the automotive power system and comfort system. The maximum speed of high-speed CAN bus can reach 1 Mbps. The data field length of the CAN frame is 8 bytes. The cyclic redundancy check (CRC) is used to ensure the correctness of transmission. For CAN FD bus, the maximum speed can be 8 Mbps, and the data field length can be 64 bytes (ISO 11898-1, 2015).

(2) **Local Interconnect Network (LIN)**: LIN bus is mainly used for controlling the vehicles seats, doors, wipers, sunroof, and so on. The speed of LIN can be up to 20 kbps (ISO/DIS 17987-3, 2015). For LIN bus, the maximum of the data field in a frame is 8 bytes. The checksum is calculated to verify the communication. Unlike CAN bus, LIN bus uses the master/slave node mode for communication.

(3) **FlexRay**: FlexRay bus has a higher transferring speed than CAN bus and mainly used the automotive power control system. The maximum speed of FlexRay can be up to 10 Mbps. Time division multiple access (TDMA) and flexible time division multiple access (FTDMA) are used in FlexRay to ensure the real-time requirements of network communication (ISO 17458-1, 2013). The data field length of FlexRay frame is 254 bytes. The CRC is used to in FlexRay to check errors during bus communication.

(4) **Ethernet**: The Ethernet plays a major role in the new automotive E/E architecture. The IEEE 802.1 AVB (Garner *et al*., 2007) and TTEthernet (AS6802) (SAE, 2016b) based on the automotive Ethernet have been used for infotainment application. The Ethernet is also the foundation of the Internet protocol. With the Internet protocol, remote calibration, remote diagnosis and remote update between vehicle and server can be achieved. For the automotive Ethernet, transmission speed can be 100/1000 Mbps, the data field length of Ethernet frame can be more than a thousand bytes. The CRC is used in Ethernet frame to check to ensure the accuracy of transmission of data (Matheus and Königseder, 2015).

The frame structures of those bus system are shown in Figure 2. With the development of the connected vehicle, wireless sensor network, V2X communication network and the user's devices connection with vehicles are also the components of automotive networks.

All the data and signals are transferred by vehicle networks, including those safety-related signal, diagnosis, and firmware update related data. Therefore, the cyber security is one of the most important issues in those fields.

2.3. Security Requirements

Security requirements are the prerequisite for the design process of vehicle cyber security. The conclusion of security requirements for vehicle networks is based on threat analysis, Henniger *et al*. (2009) propose a hierarchical classification method for vehicle cyber threat. Fuchs *et al*. propose a threat assessment method based on functional dependency analysis (Fuchs and Rieke, 2009). Glas *et al*. (2015) refer to the standards of information security and industry, and puts forward automotive information security requirements, such as firmware integrity, communication integrity, data credibility, availability, and intellectual property protection. In the EVITA project, security requirements for automotive in-vehicle networks based on dark-side scenarios are analyzed by the attack tree methods (Ruddle *et al*., 2009). Those security requirements are shown in Table 1.

In the specification of in-vehicle networks, those security requirements are not taken into consideration. Additional mechanisms are required to meet the security requirements.

3. SECURE COMMUNICATION APPROACHES

At present, lots of studies prove the necessity that security mechanisms should be taken to in-vehicle network. Wolf *et al*. (2004) analyze the security of the automotive bus system and suggested that the security mechanisms should be considered. Kleberger *et al*. (2011) research the security

Table 1. Security requirements of vehicle networks (Ruddle *et al*., 2009).

Security requirements	Description
Data origin authenticity	The data source is authenticity and reliable
Integrity	The data is not modified when transferring
Access control	Authorization before the access to information
Freshness	Time information of related message
Non-repudiation	The actions of entity is undeniable
Privacy/anonymity	The information of entity is confidential
Confidentiality	Only authorized entities can get the information
Availability	The services provided are operational

of network based on the connected vehicles and introduce related security mechanism. Mansor *et al*. (2014) propose the failure mode and impact analysis (FMEA) for threats analysis of the CAN bus. Dariz *et al*. (2016) analyze the security of CAN and Ethernet, and list the corresponding security measures for specific security threats. Nilsson *et al*. (2009) analyze the security of FlexRay, prove that FlexRay bus lacks security mechanism. By reading the bus signal and injecting deceptive messages into the network, attacks to FlexRay can be achieved. But it doesn't propose corresponding security mechanisms for FlexRay.

The main security issues and related attack methods of in-vehicle networks are listed as the following:

(1) **No Authentication**: In the automotive bus, the communication between ECUs has no authentication mechanisms for the received messages. For example, in the CAN bus, ECU can't identify the sender by the ID of CAN message. Attacker can send a spoof message that has the same ID.
(2) **Broadcasting**: For automotive network that the message is broadcasting, the information can be easily attacked with eavesdropping. Attacker can just attach a fake ECU and receive the broadcasting messages.
(3) **Arbitration process**: The CAN (FD) bus offer an arbitration process to avoid the collisions between messages. A lower ID message always has a high priority in the CAN (FD) bus. Denial-of-service (DoS) attack is easily launched by sending low ID messages continuously.
(4) **No Freshness**: The frame structures of in-vehicle network don't have a timestamp information. Attackers can send a replay message to control the behavior of vehicle.

This section presents a review of current secure communication technologies used in the area of in-vehicle networks. Those secure communication technologies can be divided into three layers:

(1) **Message Authentication**: Do authentication and integrity check for transferring messages.
(2) **Data Encryption**: Use an algorithm to ensure the data confidentiality.
(3) **Intrusion Protection**: Use firewall and intrusion detection system to achieve access control in the automotive network.

3.1. Message Authentication

Integrity check for in-vehicle networks is one of the requirements of automotive functional safety. Checksum is used in LIN bus, and CRC check is used in CAN, FlexRay, Ethernet to implement integrity check. Those mechanisms can detect faults in the network system. According to the ISO 26262, those failure modes can be repetition, loss, delay, incorrect sequence and so on (ISO/DIS 26262-6, 2011). In AUTOSAR specifications, End-to-End (E2E) profiles are used for fault detection (AUTOSAR, 2016b; Forest and Jochim, 2011). But integrity check is not secure enough to ensure the data authentication. A hacker can tamper the data, intercept the message in the automotive bus system. Message authentication mechanisms are required to ensure the reliability of data. Message Authentication Code (MAC) and digital signatures are effective for message authentication.

Digital signatures usually occupy more than 40 bytes, while MAC can be both short and long. For CAN bus and LIN bus, the maximum data field length is 8 bytes. Short MAC is the better choice for message authentication.

3.1.1. Message authentication code

For in-vehicle networks, the real-time performance and busload rate are critical. MAC calculation causes additional latency during the transmission of a message. And the length of data may be reduced if MAC is filled in the data field. This will make the busload rate increase because more frames have to be used for data transmission. Hash-based message authentication code (HMAC) is commonly used in the security researches of the automotive bus (Bittl, 2014; Hazem and Fahmy, 2012; Herrewege *et al*., 2011; Ueda *et al*., 2015; Woo *et al*., 2016). Groza *et al*. test the computational performance of MCU with hash functions (Groza *et al*., 2012; Groza and Murvay, 2013). The results proved that the longer the input size, the longer the calculation time would cost. And the types of hash functions also affect the delay time. SHA 256 will cost more time than MD5 to calculate.

In some researches, the MAC is calculated by symmetric encryption algorithm (Hartkopp *et al*., 2012; Woo *et al*., 2015). Cipher-based message authentication code (CMAC) always costs long time to calculate. To reduce the delay

Table 2. Latency of AES-128 on MPC5748G HSM.

Blocks	ECB	CBC
1	32.0 μs	33.5 μs
2	32.5 μs	33.9 μs
4	33.2 μs	35.7 μs
8	34.8 μs	36.3 μs
16	38.0 μs	39.4 μs
32	44.7 μs	45.8 μs
64	57.8 μs	59.2 μs
128	83.8 μs	85.5 μs

time, the hardware-based acceleration is necessary. AES is a classical symmetric encryption algorithm (NIST, 2001). According to the SHE specification, the latency of the AES should be less than 2 μs for per block (Escherich *et al*., 2009). For NXP MPC5748G, the calculation of AES-128 is executed and accelerated by the internal core HSMv2. The test results of the AES-128 latency on MPC5748G are shown in Table 2, including the electronic codebook (ECB) mode and the cipher-block chaining (CBC) mode. When the number of calculation blocks is 32 or more, the latency is compliance with the SHE specification and is acceptable for real-time requirement of in-vehicle network. The minimum block length of AES-128 is 16 bytes, and it can't be used in CAN or LIN bus unless the length of MAC is truncated. But it can be implemented on CAN FD because the data field of CAN FD can be up to 64 bytes. In some researches, random-number or counter are used for message authentication (Han *et al*., 2015; Yoshikawa *et al*., 2015). Counters is used when the security level is lower.

For CAN bus, the MAC can be transmitted in the data field. The authenticity increases with the length of MAC. But the data field length is limited, even for CAN+ bus, the data field length is limited to 16 bytes (Ziermann *et al*., 2009). Herrewege *et al*. (2011) propose a 15 bytes MAC for CAN+ bus, but only one byte can be used for data transfer. If the MAC is used in the data field of CAN bus, the length of MAC should less than 8 bytes. Otherwise, multiple frames have to be used for authentication information.

Other approaches may change the format of CAN frame. For example, changing the CRC field to MAC (Bittl, 2014). Besides, a standard CAN frame identifier is 11 bits, while an extended CAN frame identifier is usually 29 bits. The rest identifier field of a standard frame can be used for MAC (Hazem and Fahmy, 2012). In some researchers, authentications are processed by randomizing frame

Table 3. Comparison of message authentication codes.

Study	Algorithm	MAC position and size	Bus	Need change format ?	Computational requirement	Data field usage	Constraints
Bittl (2014)	SHA-3, HMAC	CRC field: 15 bits	CAN	Yes	Low	8/8	CRC field change required
Herrewege *et al*. (2011)	HMAC	Data field: 15 bytes	CAN+	No	Low	1/16	Busload rate is high
Hartkopp *et al*. (2012)	CMAC	Data field: 4 bytes	CAN	No	High	4/8	Busload rate is relatively high
Ueda *et al*. (2015)	SHA-256, HMAC	Data field: 1 bytes	CAN	No	Low	7/8	Additional authentication required
Hazem and Fahmy (2012)	HMAC	Identifier field: 16 bits	CAN	Yes	Low	8/8	Only for Standard identifier
		Data field: 16 bits	CAN	No	Low	6/8	Buaload rate increase
Groza *et al*. (2012)	LM-MAC	Multiple frames	CAN+	No	Low	16/16	Busload rate increase
Woo *et al*. (2015)	CMAC	Extend identifier field + CRC field: 32 bits	CAN	Yes	High	8/8	Only for standard identifier
Han *et al*. (2015)	Pseudo-random number	Identifier field + data field	CAN	Yes	Low	-	Only for data frame
		Identifier field + DLC field	CAN	Yes	Low	8/8	DLC field change required

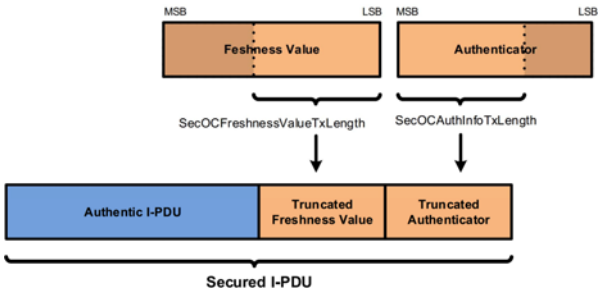

Figure 3. Secured I-PDU contents in AUTOSAR (AUTOSAR, 2016c).

identifier (Han *et al*., 2015). The comparisons between different MAC approaches are listed in Table 3.

The MAC solution is also applicable for FlexRay and Ethernet. Migrating the MAC authentication solution for FlexRay is available (Mousa *et al*., 2016) and the SAFE technology proposed by Han *et al*. (2014) proved to be effective and efficient for FlexRay. For Ethernet, MAC authentication is also a solution for message authentication, such as in the Cryptographic Link Layer (CLL) (Jerschow *et al*., 2008), MAC is used to guarantee the authenticity of Ethernet packet.

In the specifications of AUTOSAR, the generation and usage of MAC are defined (AUTOSAR, 2016c). In the AUTOSAR architecture, MAC is sent and received by Protocol Data Unit (PDU). Figure 3 shows the components of a secured PDU. MAC is generated by a symmetric key. The inputs of MAC generator contain the data value and freshness value. Considering the length of the secured PDU, truncation may be needed. Thus, it would can a better performance on CAN FD than CAN (Happel, 2014).

3.1.2. Digital signature

For in-vehicle networks, the real-time performance and busload rate are critical. MAC calculation causes additional latency during the transmission of a message. And the length of data may be reduced if MAC is filled in the data field. This will make the busload rate increase because more frames have to be used for data transmission.

Both digital signature and message authentication code can be used for data authentication. But digital signature has the property of non-repudiation. The key of a digital signature is asymmetric key.

Due to the length limitation, the digital signature can be used in CAN FD, FlexRay or Ethernet. If the digital signature is used in CAN bus, multiple frames have to be used, and this will affect the busload rate.

When using the Over-The-Air (OTA) approach for software updates, the security level is much higher than the on-board network. The security of OTA is the base of remote diagnostics, remote ECU update (Vuillaume *et al*., 2015). The digital signature is one of the security mechanism to prevent the malware updates and to ensure the integrity, authentication, and non-repudiation of messages in the application of OTA.

Table 4. Comparison between MAC and digital signature.

Features	MAC	Digital signature
Integrity	√	√
Authentication	√	√
Non-repudiation	×	√
Algorithm	Symmetric	Asymmetric
Execution time	Short	Long
Length	Short	Long
Applicable in-vehicle network	CAN, CAN FD, FlexRay, Ethernet	CAN FD, FlexRay, Ethernet

Asymmetric encryption algorithms require a high computational performance of MCU. In this case, TPM can be used for key storage and signature generation/verification (Klimke *et al*., 2015; Petri *et al*., 2016; Trusted Computing Group, 2015). At present, the studies of the OTA security include security protocols (Nilsson and Larson, 2008; Schweppe *et al*., 2011) and security architectures (Kuzhiyelil and Tverdyshev, 2015), and so on.

Except for the communication process of OTA, some researchers also pointed out that the downloaded firmware and related update repository also need authentication (Karthik *et al*., 2016; Nilsson *et al*., 2008), and a digital signature is necessary from the perspective of security.

The features of MAC and digital signatures are concluded in Table 4.

3.2. Data Encryption

Encryption is a security mechanism to make data and signals to be confidential. Confidentiality is an important property to prevent the network from spoofing attacks. In some researches, cryptographic algorithms are used for in-vehicle networks. Lin *et al*. propose a security mechanism with ID table, pair-wise key, and message-based counter. It can be used to protect the CAN bus against masquerade and replay attacks (Lin and Sangiovanni-Vincentelli, 2012). Woo *et al*. (2015) use the AES-128 algorithm to encrypt the data field of CAN FD. Groll and Ruland (2009) introduce trusted communication groups to enable confidential communication. Which algorithms to choose and how to distribute the keys are the main research contents for the data encryption of in-vehicle networks.

3.2.1. Cryptographic algorithms

When encryption is used for in-vehicle networks, the latency of algorithms must be considered. Groll and Ruland (2009) test some standard cryptographic algorithms on three different embedded processors, the asymmetric cryptographic algorithms take more time than symmetric

cryptographic algorithms to execute.

There are three methods to reduce the latency caused by encryption/decryption.

(1) Use MCUs with high calculational performance: The clock frequency and type of MCU have direct influences on the execution time of algorithms. Increasing the clock frequency of MCU can reduce the execution time of algorithms. And a 32-bit MCU performs better than a 16-bit MCU.
(2) Use lightweight algorithms for embedded processors: Lightweight algorithms require less calculational performance than standard cryptographic algorithms. The PRESENT algorithm is ultra-lightweight block cipher and can be used in the constrained MCU environment (Bogdanov *et al*., 2007). The plaintext and ciphertext of the PRESENT cipher are both 64 bits, thus it can be used for data encryption of CAN bus. Yoshikawa *et al*. perform spoofing attacks against the unencrypted CAN communication and the PRESENT encrypted CAN communication. The results prove the PRESENT algorithms can keep the confidentiality of CAN bus (Yoshikawa *et al*., 2015). Except for the PRESENT algorithms, there are some other lightweight algorithms, for example, the SEA (Standaert *et al*., 2006), can be used for embedded platforms.
(3) Use hardware engine to execute standard algorithms: The Security hardware can improve the performance of cryptography algorithms greatly. The SHE and EVITA HSM can accelerate the AES algorithms and generate the key. The TPM can provide RSA algorithms based on hardware.

3.2.2. Key distribution

In a secure communication group, an ECU usually has more than one key, including the key for MAC or signature generation and the key for data encryption. From the perspective of ECU lifetime, the keys for secure communication are session keys, and the keys for secure boot check and key distribution are pre-shared key. Session keys need to be updated frequently. An ECU may belong to different communication groups, thus the ECU usually have different keys for per communication group. A most widely used approach for key distribution is using a special key master as the Key Distribution Center (KDC).

Figure 4 illustrates the KDC working process. The KDC distributes the K1 as the communication key between ECU1 and ECU2. And the K2 is distributed as the communication key between ECU1 and ECU3.

Secure Mechanisms are needed during the process of key distribution. In the trusted communication groups proposed by Groll *et al*., symmetric keys are used for session communication, and asymmetric algorithms are used for the process of session keys distribution (Standaert *et al*., 2006). Symmetric algorithms can also be used for key distribution, but additional mechanisms like random number are needed to ensure the authentication of the key

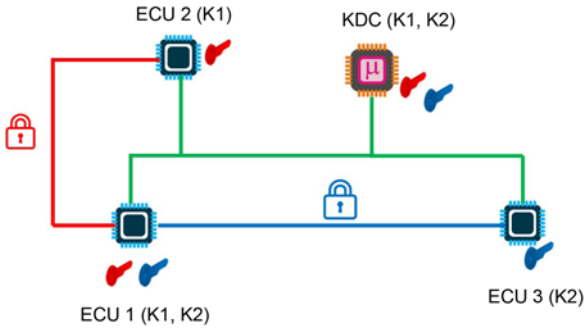

Figure 4. Key distribution process of KDC.

master. Timestamps are needed to protect the process against replay attacks. Data encryption can be used for networks that need confidentiality, such as diagnosis, firmware update, and mobile device connection. In those fields, the in-vehicle networks have the interfaces to the outside networks, implementing security layer can prevent the outside attacking (Dardanelli *et al*., 2013; Han *et al*., 2013; Kochanek *et al*., 2013).

3.3. Intrusion Protection

When attacked by hackers, the vehicle needs responding to the intrusion, starting protection mechanisms, and reporting the state of vehicles. The protections methods include firewall, intrusion detection system, and so on.

3.3.1. Firewall

Firewall is the security system to control the access between one domain and other domains. The concept of firewall can be software architecture or E/E architecture level. The firewall in the network architecture separates the trusted zone from the untrusted zone and blocks the attacking from unauthorized entities. In this architecture, the firewall is usually implemented in the security gateway. The firewall in the software architecture is the access control mechanism that authenticates the data flow between system domain, user domain, and OEM domain. For automotive firewall, access control and domain separation are the critical techniques to protect the security of vehicles.

Access control can work at the frame level or application level (Schmidt *et al*., 2016). Frame level access control is for the CAN, LIN bus and so on, and application level access control is for security diagnosis, OTA access and so on. Role-based access control is a widely used approach. Two mechanisms can be used to identify the roles in the automotive networks.

(1) **Access Control List (ACL)**: In this methods, whitelists or blacklists used for identifying the CAN, LIN, Ethernet frames. Whitelists only contain the frames that are allowed to access while frames in the blacklists are not allowed to access. Characteristics in the networks can be used for ACL definition. For

example, the ID of CAN, LIN bus, the destination address or sources address of Ethernet frames.

(2) **Session Authentication**: The MAC and digital signatures of messages can be used to identify and check the authenticity of the access in the network. Besides, Han *et al*. (2013) propose a three-step verification mechanism for the access of mobile device, and security layer is needed when connected with an IP-based network (Bouard *et al*., 2012b). The balance between authentication and network latency should be considered.

The firewall in the network architecture should separate the network domain into different security level layers. For example, the powertrain control data and signals should be isolated with the infotainment system, in case of the attacking from the USB, the DVD, the mobile device, and so on. And for an operation system of the infotainment, such as a QNX system, a Linux-based system, and so on, the firewall should isolate the critical system software zone from the application running zone, and prevent the network system from malicious applications.

3.3.2. Intrusion detection system

Network intrusion detection system should be able to identify external attacks, reduce the possible impact, prevent the attack or similar attacks, restore the network to a security state, and report the relevant abnormal activities (Northcutt and Novak, 2002). Intrusion detection for in-vehicle networks can be behavior-based or knowledge-based.

(1) **Behavior-based intrusion detection**: It is based on statistical analysis and data modeling to monitor the abnormal data. The approaches for behavior-based detection include machine learning (Cain, 2015; Kang and Kang, 2016), time analysis (Hamada *et al*., 2016; Otsuka and Ishigooka, 2014), physical signal characteristics utilization (Cho and Shin, 2017), entropy measurement (Müter and Asaj, 2011) and so on (Ahn *et al*., 2016; Larson *et al*., 2008).

(2) **Knowledge-based intrusion detection**: In a knowledge-based intrusion detection system, detection mechanisms are based on the rules that define the authentication in the network. MAC and digital signatures can be used for knowledge-based intrusion detection. Whitelist and blacklist can also be the rules for intrusion detection.

Intrusion detection based on machine learning usually uses a deep neural network to create the network traffic model. The ID, data can be used for training. When the in-vehicle network was attacked, anomaly behaviors in the network can be detected by the trained monitoring model. This approach has a good performance for unknown attacks, but the design information of the network is needed to create a trained model. Cain proposes a CAN traffic model, and trained the model with CAN ID and CAN signals (Cain, 2015). Online detection requires high computational performance, and this is difficult for an in-vehicle ECU. The method introduced by Kang fixes this weakness by using an offline trained model (Kang and Kang, 2016), as is shown in Figure 5. Compared the two approaches, an offline model trained by deep neural network costs less MCU resources to calculate, but the model can't update immediately when a new attack method is detected.

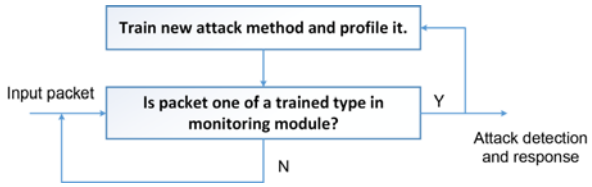

Figure 5. Profiling module and a monitoring module in (Kang and Kang, 2016).

Approaches based on time analysis usually focus on the behavior of frame frequency, network latency, and other time-related characteristics to monitor anomaly behaviors. These methods can be used for periodic messages. Figure 6 shows the waves when attacking happened in periodic frames, and the T34 would be detected as abnormal. For this method, identifying mode can be real-time decision or delayed decision. The real-time decision can respond immediately to protect the network when attacked, but false detection rate is higher than a delayed decision. Delay decision can be used for attacking logging (Hamada *et al*., 2016).

Combining the time analysis with the network frame details, Ahn *et al*. (2016) introduce a mechanism by detecting the frequency and sequences of CAN frame identifier. The detection rate of this method is high, and busload effect is low. But details of the network design information are required. Larson *et al*. (2008) propose an intrusion detection system for CAN/CANopen networks. By monitoring packets changes with time, it can detect the possible network intrusion. In this methods, additional monitors need to be configured in the ECUs and the gateway, hardware cost is relatively high.

Measuring and utilizing the physical signal characteristics of in-vehicle network is one of the solutions for attacker identification. The scheme proposed by Cho and Shin (2017) measures the output voltage of ECU on CAN bus to identify attacker. This scheme is based on the ACK threshold learning of CAN bus. The scheme proposed can identify which ECU is mounting the attack rather than just

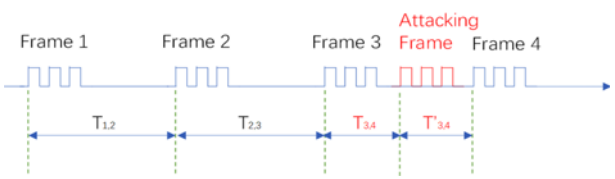

Figure 6. Time analysis for intrusion detection.

detect attacking behaviors of the CAN bus. But for a compromised device that directly attached to the in-vehicle network, this scheme is not applicable.

In another approach, the entropy is used to detect the abnormal state in the network. Entropy has a relationship with the system chaos. Müter *et al*. propose an entropy-based method to measure the CAN network anomaly information.

Compared with behavior-based intrusion detection, the knowledge-based systems provide more accurate detection rate in the rules defined. But for unknown attacks, the behavior-based intrusion systems have a better performance. A knowledge-based intrusion detection system should update its policies when a new attacking mode is founded.

The comparison of some intrusion detection approaches is concluded in Table 5. Most of them have some constraints for intrusion detection. In order to improve the performance of intrusion detection, combined detection methods are needed. The deployment of intrusion detection system can be host- based (deployed in the gateway) or distributed (deployed in the ECUs) depending on the detection principles or as a combination of them if needed.

3.3.3. Detection and protection

When the intrusion is detected, protection mechanisms should be able to prevent the attack and reduce the damages. The protection mechanisms can be passive or active. Passive protections include the intrusion logging and reporting. Active protections are used to defend against the attacking. Redundancy is beneficial for vehicle system. Redundantly actuated vehicle system can enable fault isolability and fault diagnosis when attacked by hackers (Park *et al*., 2016).

Matsumoto *et al*. (2012) propose a mechanism to

Table 5. Comparison of intrusion detection methods.

Study	Principle	Type	Detection accuracy	Overhead	Constraints
Cain (2015)	Using machine learning to build a model based on ID and frequency	Behavior-based	Relatively high	High	High computational performance is required
Kang and Kang (2016)	CAN packet model with the number of "1" bit	Behavior-based	Medium	High	Design information of network is required
Hamada *et al*. (2016)	Measuring the reception cycle period, comparing with threshold	Behavior-based	Medium	Relatively high	False detection rate is relatively high
	Measuring the reception cycle period, comparing with the previous one	Behavior-based	Relatively high	Relatively high	Detection is delayed.
Otsuka and Ishigooka (2014)	Measuring the delay time in the CAN bus	Behavior-based	High	Low	Hardware modification required ECU; Design information of network is required
Larson *et al*. (2008)	Monitoring the packets in the bus	Behavior-based	High	Low	Additional monitor is required for gateway and ECU; Design information of network is required
Cho and Shin (2017)	Measuring the output voltages of ECU on CAN bus	Behavior-based	High	Medium	Voltage profiles of ECU is necessary; Compromised ECU is required as one of those originally installed
Müter and Asaj (2011)	Measuring the entropy of the system	Behavior-based	Medium	Medium	Design information of network is required
Ahn *et al*. (2016)	Monitoring the sequence and frequency of CAN identifiers	Behavior-based	High	Relatively low	Design information of network is required
Herrewege *et al*. (2011)	Detection based on the authentication with digital signature	Knowledge-based	Very high	High	Only for known attacking
Nilsson *et al*. (2008a)	Detection based on the authentication with MAC	Knowledge-based	Very high	Medium	Only for known attacking

damage the anomaly messages in the CAN bus. If an intrusion message was detected, the protection system would send error frames to destroy the untrusted message. Dagan *et al*. propose an approach based on software. In this approach, not only the spoof messages would be damaged, but the untrusted ECU would also be isolated (Dagan and Wool, 2016). Ujiie *et al*. design a hardware-based method to protect the CAN bus. A center ECU with intrusion monitoring will hold up untrusted messages. The intrusion detection is based on whitelist rules (Ujiie *et al*., 2015).

For the DoS attacks in CAN (FD), the NXP semiconductors proposed a low-cost solution with secure CAN transceiver to limit the number of messages per unit of time (Elend and Adamson, 2017), but it works only when all the CAN nodes in the bus have those secure transceivers. Spatial and temporal isolation is a solution for the virtual CAN controllers with virtual machine to defend DoS attack (Herber *et al*., 2014), but it failed if the Dos attack is happened on physical interface. From the perspective of CAN controller, sending error frames to make the ECU that launched the attack to be " bus off " is a common method (Kurachi *et al*., 2015; Ujiie *et al*., 2015).

LIN bus works as the master/slave mode, and protection mechanism is different from CAN bus. Takahashi proposed a method to attack the LIN bus. By using the error handling mechanism, attackers can inject a false slave response on the LIN bus. This can interrupt the normal communication of LIN bus. Response abandoning mechanism is an effective method to avoid the attacking. When intrusion detected, protection system will act to abandon the response until the LIN bus return to a normal state (Takahashi *et al*., 2017).

3.4. Security for the IP-based Network

The security of the Internet protocol in automotive is more complicated than the CAN, LIN bus. Since the Internet protocol has been developed for years, there are many specifications can be used for reference. The security specifications for the Internet protocols based on the Open System Interconnection (OSI) reference model can be concluded in Table 6.

In the OSI architecture, security specifications cover the data link layer, network layer, and transport layer. For upper layers, special security mechanisms should be implemented. The Transport Layer Security (TLS) is a security protocols for IP-based network. Using TLS to secure in-vehicle network is investigated to be applicable with suitable hardware and encryption algorithms (Zelle *et al*., 2017), but considering the network latency caused by TLS, it is useful for non-realtime communication rather than vehicle control traffic (Lastinec and Hudec, 2016). Kleberger *et al*. compare the TLS and Internet Protocol Security (IPsec), and conclude that IPsec is better for the remote connection in automotive, such DoIP.

Bouard *et al*. (2012a) propose a secure middleware between the application layer and the network layer, as is in shown in Figure 7. The secure middleware is based on the SECURITY IN EMBEDDED IP-BASED SYSTEMS (SEIS) framework (Glass *et al*., 2010). In the secure middleware, crypto services, authentication management, and intrusion detection are implemented based on the EVITA-HSM. The secure middleware works as a proxy to allow vehicles to connect to the Internet (Bouard *et al*., 2012b). Secure middleware is in the client ECU. When connecting to a server using the Internet protocols, the client ECU opens a secure connection, gets the policy and starts authentication. After that, a session-establishment message will be sent to the server and the client ECU waits for the session-establishment response. Data can be sent to the server after getting the response and finishing the authentication. During the authentication and data transmitting process, the payloads in messages are encrypted. The limitation of computational performance in automotive ECU makes it different from the traditional Internet protocol, specialized security mechanisms are required.

Table 6. Security in the OSI reference model.

Layers	Security techniques
Application layer	User-defined
Presentation layer	User-defined
Session layer	User-defined
Transport layer	Packet filtering; TLS
Network layer	Virtual private network; IPsec
Data link layer	MAC security; Secure device identifier; Virtual local area network; Network access control; CLL
Physical layer	User-defined

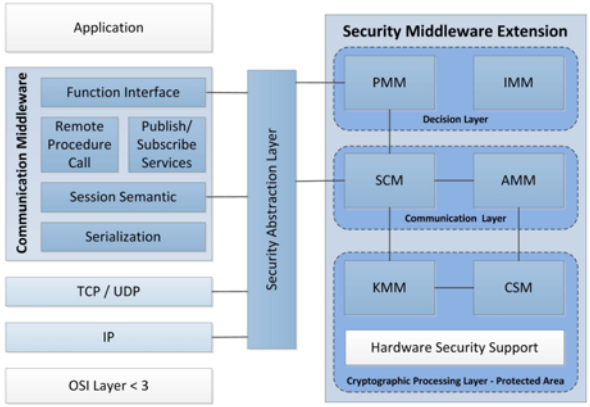

Figure 7. Security middleware extension in (Bouard *et al*., 2012a).

4. TECHNICAL REQUIREMENTS

In Section 3, secure communication approaches have been discussed. The technical requirements of security mechanisms are concluded in this section.

4.1. Cryptographic Mechanisms

To implement cryptographic mechanisms on the in-vehicle networks, the requirements of the following areas should be met.

(1) **Cryptographic Algorithm**: The cryptographic algorithms for message authentication and data encryption have the following requirement:
   - The algorithm should be executed efficiently in an automotive MCU. A lightweight algorithm or hardware-based algorithms can be a choice.
   - The algorithm should be secure enough to against key crack.
   - The algorithm should be compatible with the in-vehicle networks. For example, AES-128 requires at least 16 bytes for per block, but the CAN, LIN bus only contain 8 bytes in the data field of a frame, thus the AES-128 is not suitable for the CAN, LIN bus.

(2) **Busload Rate**: The security of MAC has a positive relationship with the length. From this perspective, increasing the MAC length is better. But if the MAC is in the data field of CAN, LIN frames, increasing the MAC length will make available data length decreasing, and results in a higher busload rate. If digital signatures are implemented, multiple frames have to be used, and this also affects the busload rate. For this reason, the security and the busload rate of the in-vehicle networks should have a balance.

(3) **Network Latency**: The authentication and encryption will cause additional calculation time. For in-vehicle networks, real-time control is important, especially in the safety-related systems. The latency of security mechanisms should not affect the real-time control.

(4) **Key Management**: The security of keys is the basis of cryptographic mechanisms. There are three aspects of key requirements:
   - The keys should be stored securely. The access to keys stored in the ECU should be controlled and authenticated. The storage of key should be able to against the side channel attack.
   - The generation of keys should be secure enough, and security mechanisms are required during the distribution or update of keys.
   - The keys should be divided if the ECU has communications with different groups. The keys for session communication and boot authentication are required to be different.

4.2. Intrusion Detection Policy

The security policies of intrusion detection system should be effective and efficient. Idrees and Roudier (2012). propose a security policy engine to configure the security mechanisms in automotive networks. For in-vehicle networks, the requirements of security policies are concluded as follows:

(1) **Real-Time**: The detection of network intrusion should be real-time that related protection can respond to prevent the attacks and reduce the damage of intrusion.

(2) **Detection Rate**: For a behavior-based intrusion detection, the false detection rate is unavoidable. For a knowledge-based intrusion detection, it can't detect unknown behavior. To improve the detection rate, the improvement of detection approaches is needed, and the combination of intrusion detection approaches can be a choice.

(3) **Network Capacity**: The network capacity for intrusion detection system should be high enough to deal with the possible attacking and keep the availability of in-vehicle networks. And a DoS attacking will make the busload rate full. Thus the related protection mechanisms are required.

(4) **Policy Update**: The policies for knowledge-based intrusion detection system should be updated when new attacking methods are found. And for the intrusion detection based on machine learning, the constraints of ECU computational performance make it hard to auto update the trained detection model, a policy update process is required. The updates of policies are based on the attacking reports. Remote updates from the server is a method for policy update.

5. DISCUSSION OF FUTURE DEVELOPMENTS

In this section, the directions of future developments on secure communication techniques are discussed. Based on the previous approaches discussed, the future research fields include the threat analysis, the security development with function safety, and the testing.

5.1. Threat Analysis and Security Assessment

Threat analysis is the basis of automotive cyber security researches. Through the full range of threat analysis, the relevant security vulnerabilities can be found and the security requirements can be defined.

A common threat analysis method is the attack trees. As is shown in Figure 8, the basic idea of attack trees is setting the attack target and trying possible methods to reach the target step by step. Hazard Analysis and Risk Assessment (HARA) is an approach used for functional safety research. Ward *et al*. (2013) propose the HARA for cyber security analysis.

The security assessment is an important process for secure communication. Based on threat analysis, it is necessary to define the security levels for in-vehicle networks. For example, the EVITA-HSM have three levels, the deployment of HSM is concerned with the security level. And how to choose suitable security mechanisms is

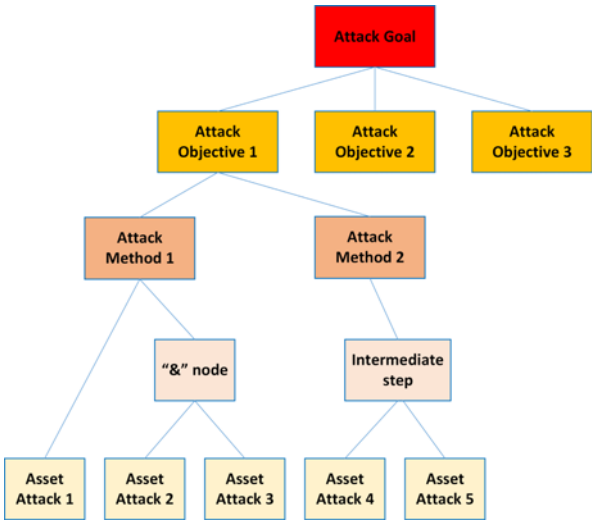

Figure 8. General attack tree structure.

also related to the security level. Classifying the security levels should consider the possibility and severity of threats.

5.2. Functional Safety and Cyber Security

According to the specification of J3061, the design process of cyber security should base on the V-model architecture (SAE, 2016a), and the V-model design process is also originated from functional safety design process. The relationship between functional safety and cyber security is shown in Figure 9 (Czerny, 2013). Macher *et al*. (2017) set

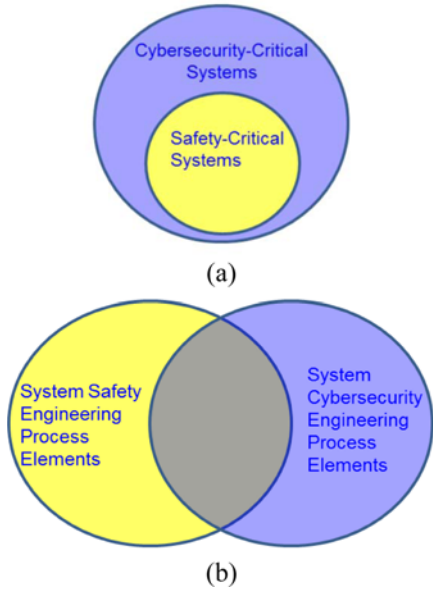

Figure 9. (a) Relationship between safety-critical and security-critical systems; (b) Relationship between system safety and system cyber security engineering elements (Czerny, 2013).

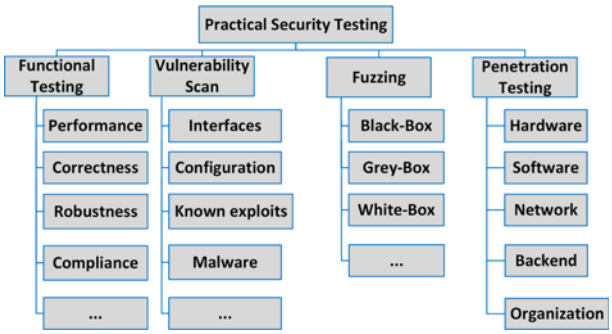

Figure 10. Classification of practical security testing methods (Bayer *et al*., 2014).

on addressing system safety and cyber security in combination.

The designing of security mechanisms should consider the related functional safety requirements. Further researches are needed in this field.

5.3. Testing and Validation

The functional test and performance test are important processes for the development of secure communication mechanisms. Bayer *et al*. (2015, 2016) propose that the automotive security test should include the functional validation, vulnerability scan, fuzzing test, and penetration test. In the Figure 10, Bayer *et al*. conclude the practical security testing methods. From the perspective of security development process, Wooderson and Ward (2017) explore the different kinds of testing during the development process of vehicle security.

Research directions in this field include test methods and test specifications.

6. CONCLUSION

This paper reviewed current researches about secure communication mechanisms for in-vehicle networks and discussed future directions. Secure communication approaches include message authentication, data encryption, and intrusion protection. MAC and digital signature are effective methods for message authentication and protect the integrity and authenticity. Data encryption is used to ensure the confidentiality. Intrusion protection countermeasures including the firewall mechanism and the intrusion detection system are designed to achieve the access control in the automotive networks and prevent the attacks from outsides.

This paper highlights the requirements for security mechanisms when implemented on real vehicle environment. Cryptographic mechanisms should meet the requirements on algorithms, busload rate, network latency, and key management. Intrusion detection policy should consider the real-time performance, detection rate, network capacity, and policy update. The fact is that those security

mechanisms can't avoid to increase the cost of in-vehicle network. For this reasons, it is suggested to classify the in-vehicle networks to different security levels. For a low-security-level network domain, message authentication can guarantee the security of communication. For a middle-security-level network domain, data encryption is necessary. And for a high-security level network domain, the intrusion detection and protection system are suggested to be implemented.

It is essential to note a variety of factors should be taken into consideration when implementing the security mechanisms, including the security level, the network performance, the cost, and so on.

REFERENCES

Ahn, S., Kim, H., Jeong, J. and Kim, K. (2016). A countermeasure against spoofing and DoS attacks based on message sequence and temporary ID in CAN. *Symp. Cryptography and Information Security*, Kumamoto, Japan.

AUTOSAR (2016a). Specification of Crypto Service Manager. AUTOSAR CP Release 4.3.0.

AUTOSAR (2016b). Requirements on E2E Communication Protection. AUTOSAR CP Release 4.3.0, 1–14.

AUTOSAR (2016c). Specification of Module Secure Onboard Communication. AUTOSAR Release 4.3.0.

Bayer, S., Enderle, T., Oka, D. K. and Wolf, M. (2015). Security crash test – Practical security evaluations of automotive onboard IT components. *Automotive – Safety & Security*, Stuttgart, Germany.

Bayer, S., Enderle, T., Oka, D., Wolf, M. and Gmbh, E. (2016). Automotive security testing – The digital crash test. *Energy Consumption and Autonomous Driving: Proc. 3rd CESA Automotive Electronics Cong*., Paris, France.

Bittl, S. (2014). Attack potential and efficient security enhancement of automotive bus networks using short MACs with rapid key change. *Communication Technologies for Vehicles*, 113–125.

Bogdanov, A., Knudsen, L. R., Leander, G., Paar, C., Poschmann, A., Robshaw, M. J., Seurin, Y. and Vikkelsoe, C. (2007). PRESENT: An ultra-lightweight block cipher. *Cryptographic Hardware and Embedded Systems – CHES*, 450–466.

Bouard, A., Glas, B., Jentzsch, A., Kiening, A., Kittel, T., Stadler, F. and Weyl, B. (2012a). Driving automotive middleware towards a secure ip-based future. *10th ESCAR Europe*, 1–9.

Bouard, A., Schanda, J., Herrscher, D. and Eckert, C. (2012b). Automotive proxy-based security architecture for CE device integration. *Int. Conf. Mobile Wireless Middleware, Operating Systems, and Applications*, 62–76.

Cain, H. (2015). Applying machine learning for anomaly detection in CAN bus networks. *13th ESCAR Europe*, 1–3.

Checkoway, S., Mccoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., Koscher, K., Czeskis, A., Roesner, F. and Kohno, T. (2011). Comprehensive experimental analyses of automotive attack surfaces. *Proc. 20th USENIX Conf. Security*, San Francisco, California, USA.

Cho, K. T. and Shin, K. (2017). Viden: Attacker identification on in-vehicle networks. *Proc. ACM SIGSAC Conf. Computer and Communications Security*, 1109–1123.

Czerny, B. J. (2013). System security and system safety engineering: Differences and similarities and a system security engineering process based on the ISO 26262 process framework. *SAE Int. J. Passenger Cars - Electronic and Electrical Systems* **6**, **1**, 349–359.

Dagan, T. and Wool, A. (2016). Parrot, a software-only anti-spoofing defense system for the CAN bus. *14th ESCAR Europe*, 1–10.

Dardanelli, A., Maggi, F., Tanelli, M., Zanero, S., Savaresi, S. M., Kochanek, R. and Holz, T. (2013). A security layer for smartphone-to-vehicle communication over bluetooth. *IEEE Embedded Systems Letters* **5**, **3**, 34–37.

Dariz, L., Ruggeri, M., Costantino, G. and Martinelli, F. (2016). A survey over low-level security issues in heavy duty vehicles. *14th ESCAR Europe*, 1–7.

Elend, B. and Adamson, T. (2017). Cyber security enhancing CAN transceivers. *16th Int. CAN Conf.*, Nuremberg, Germany.

Escherich, R., Ledendecker, I., Schmal, C., Kuhls, B., Grothe, C. and Scharberth, F. (2009). SHE – Secure Hardware Extension Functional Specification. HIS AK Security.

Forest, T. and Jochim, M. (2011). On the fault detection capabilities of AUTOSAR's end-to-end communication protection CRC's. *SAE Paper No*. 2011-01-0999.

Fuchs, A. and Rieke, R. (2009). Identification of authenticity requirements in systems of systems by functional security analysis. *Architecting Dependable Systems VII*, 74–96.

Garner, G. M., Feng, F., den Hollander, K., Jeong, H., Kim, B., Lee, B. J., Jung, T. C. and Joung, J. (2007). IEEE 802.1 AVB and its application in carrier-grade ethernet [Standards topics]. *IEEE Communications Magazine* **45**, **12**, 126–134.

Glas, B., Gramm, J. and Vembar, P. (2015). Towards an information security framework for the automotive domain. *Lecture Notes in Informatics, Proc. – Series of the Gesellschaft für Informatik*, Stuttgart, Germany, 109–124.

Glass, M., Herrscher, I., Meier, H. and Schoo, P. (2010). 'SEIS' – Security in embedded IP-based systems. *ATZ Elektronik*, 36–41.

Groll, A. and Ruland, C. (2009). Secure and authentic communication on existing in-vehicle networks. *IEEE Intelligent Vehicles Symp*., 1093–1097.

Grote, R., Friederici, F., Holle, J., Groll, A., Cankaya, H.

and Enderle, T. (2011). Specification of Secure Communication. Oversee Project Deliverable Report. D2.4.

Groza, B. and Murvay, S. (2013). Efficient protocols for secure broadcast in controller area networks. *IEEE Trans. Industrial Informatics* **9**, **4**, 2034–2042.

Groza, B., Murvay, S., Van Herrewege, A. and Verbauwhede, I. (2012). LiBrA-CAN: A lightweight broadcast authentication protocol for controller area networks. *Cryptology and Network Security*, 185–200.

Hamada, Y., Inoue, M., Horihata, S. and Kamemura, A. (2016). Intrusion detection by density estimation of reception cycle periods for in-vehicle networks: A proposal. *14th ESCAR Europe*, 1–10.

Han, G., Zeng, H., Li, Y. and Dou, W. (2014). SAFE: Security-aware flexray scheduling engine. *Design, Automation & Test in Europe Conf. & Exhibition (DATE)*, Dresden, Germany.

Han, K., Divya Potluri, S. and Shin, K. G. (2013). On authentication in a connected vehicle: Secure integration of mobile devices with vehicular networks. *Proc. IEEE Int. Conf. Cyber-Physical Systems (ICCPS)*, Philadelphia, Pennsylvania, USA, 160–169.

Han, K., Weimerskirch, A. and Shin, K. G. (2015). A practical solution to achieve real-time performance in the automotive network by randomizing frame identifier. *13th ESCAR Europe*, 1–10.

Happel, A. (2014). Secure communication for CAN FD. *CAN Newsletter*, **4**, 1–3.

Hartkopp, O., Reuber, C. and Schilling, R. (2012). MaCAN – Message authenticated CAN. *10th ESCAR Europe*, 1–7.

Hazem, A. and Fahmy, H. A. H. (2012). LCAP – A lightweight CAN authentication protocol for securing in-vehicle networks. *10th ESCAR Europe*, 1–10.

Henniger, O., Apvrille, L., Fuchs, A., Roudier, Y., Ruddle, A. and Weyl, B. (2009). Security requirements for automotive on-board networks. *Proc. IEEE Int. Conf. Intelligent Transport Systems Telecommunications*, Lille, France, 641–646.

Herber, C., Richter, A., Rauchfuss, H. and Herkersdorf, A. (2014). Spatial and temporal isolation of virtual CAN controllers. *ACM SIGBED Review* **11**, **2**, 19–26.

Herrewege, A. V., Singelee, D. and Verbauwhede, I. (2011). CANAuth – A simple, backward compatible broadcast authentication protocol for CAN bus. *ECRYPT Workshop on Lightweight Cryptography*, Louvain-la-Neuve, Belgium.

Idrees, M. S. and Roudier, Y. (2012). Effective and efficient security policy engines for automotive on-board networks. *Communication Technologies for Vehicles*, 14–26.

ISO 11898-1 (2015). Road Vehicles -- Controller Area Network (CAN) -- Part 1: Data Link Layer and Physical Signalling.

ISO 17458-1 (2013). Road Vehicles -- FlexRay Communications System -- Part 1: General Information and Use Case Definition.

ISO/DIS 17987-3 (2015). Road Vehicles – Local Interconnect Network (LIN) – Part 3: Protocol Specification.

ISO/DIS 26262-6 (2011). Road Vehicles -- Functional Safety -- Part 6: Product Development at the Software Level.

Jerschow, Y. I., Lochert, C., Scheuermann, B. and Mauve, M. (2008). CLL: A cryptographic link layer for local area networks. *Int. Conf. Security and Cryptography for Networks*, 21–38.

Kang, M. J. and Kang, J. W. (2016). A novel intrusion detection method using deep neural network for in-vehicle network security. *Proc. IEEE 83rd Vehicular Technology Conf. (VTC Spring)*, Nanjing, China.

Karthik, T., Awwad, S., Mccoy, D., Bielawski, R., Mott, C., Lauzon, S., Cappos, J. and Trishank, K. K. (2016). Uptane: Securing software updates for automobiles. *14th ESCAR Europe*, 1–11.

Kleberger, P., Olovsson, T. and Jonsson, E. (2011). Security aspects of the in-vehicle network in the connected car. *Proc. IEEE Intelligent Vehicles Symp. (IV)*, Baden-Baden, Germany, 528–533.

Klimke, M., Scheibert, K., Freiwald, A. and Steurich, B. (2015). Secure and seamless integration of Software Over The Air (SOTA) update in modern car board net architectures. *13th ESCAR Europe*, 1–19.

Kobayashi, H., Konno, C., Kayashima, M. and Nakano, M. (2013). Approaches for Vehicle Information Security. IPA Report.

Kochanek, R., Dardanelli, A., Maggi, F., Zanero, S. and Holz, T. (2013). Secure integration of mobile devices for automotive services. *11th ESCAR Europe*, 1–18.

Koscher, K., Czeskis, A., Roesner, F., Patel, S. and Kohno, T. (2010). Experimental security analysis of a modern automobile. *Proc. IEEE Symp. Security and Privacy (SP)*, Berkeley/Oakland, California, USA, 447–462.

Kurachi, R., Takada, H., Mizutani, T., Ueda, H. and Horihata, S. (2015). SecGW – Secure gateway for in-vehicle networks. *13th ESCAR Europe*, 1–8.

Kuzhiyelil, D. and Tverdyshev, S. (2015). A secure update architecture for high assurance mixed-criticality system. *13th ESCAR Europe*, 1–10.

Larson, U. E., Nilsson, D. K. and Jonsson, E. (2008). An approach to specification-based attack detection for in-vehicle networks. *Proc. IEEE Intelligent Vehicles Symp.*, Eindhoven, Netherlands, 220–225.

Lastinec, J. and Hudec, L. (2016). Comparative analysis of TCP/IP security protocols for use in vehicle communication. *Proc. IEEE 17th Int. Carpathian Control Conf. (ICCC)*, Tatranska Lomnica, Slovakia, 429–433.

Lin, C.-W. and Sangiovanni-Vincentelli, A. (2012). Cyber-security for the controller area network (CAN) communication protocol. *Proc. IEEE Int. Conf. Cyber Security*, Alexandria, Virginia, USA, 1–7.

Macher, G., Messnarz, R., Armengaud, E., Riel, A., Brenner, E. and Kreiner, C. (2017). Integrated safety and security development in the automotive domain. *SAE Paper No.* 2017-01-1661.

Mansor, H., Markantonakis, K. and Mayes, K. (2014). CAN bus risk analysis revisit. *Proc. Information Security Theory and Practice*, Heraklion, Crete, Greece, 170–179.

Matheus, K. and Königseder, T. (2015). *Automotive Ethernet*. Cambridge University Press. Cambridge, UK.

Matsumoto, T., Hata, M., Tanabe, M., Yoshioka, K. and Oishi, K. (2012). A method of preventing unauthorized data transmission in controller area network. *Proc. IEEE 75th Vehicular Technology Conf. (VTC Spring)*, Yokohama, Japan, 1–5.

McCarthy, C. and Harnett, K. (2014). National Institute of Standards and Technology Cybersecurity Risk Management Framework Applied to Modern Vehicles. NHTSA Technical Report. DOT HS 812 073.

McCarthy, C., Harnett, K. and Carter, A. (2014). A Summary of Cybersecurity Best Practices. NHTSA Technical Report. DOT HS 812 075.

Miller, C. and Valasek, C. (2013). Adventures in automotive networks and control units. *DEF CON 21 Hacking Conf*., Las Vegas, USA.

Miller, C. and Valasek, C. (2015). Remote exploitation of an unaltered passenger vehicle. *Black Hat USA*, Las Vegas, USA.

Mousa, A. R., NourElDeen, P., Azer, M. and Allam, M. (2016). Lightweight authentication protocol deployment over FlexRay. *Proc. 10th Int. Conf. Informatics and Systems*, Giza, Egypt, 233–239.

Müter, M. and Asaj, N. (2011). Entropy-based anomaly detection for in-vehicle networks. *Proc. IEEE Intelligent Vehicles Symp. (IV)*, 1110–1115.

Navale, V. M., Williams, K., Lagospiris, A., Schaffert, M. and Schweiker, M.-A. (2015). (R)evolution of E/E architectures. *SAE Int. J. Passenger Cars - Electronic and Electrical Systems* **8**, **2**, 282–288.

Nilsson, D. K. and Larson, U. E. (2008). Secure firmware updates over the air in intelligent vehicles. *Proc. IEEE Int. Conf. Communications*, Beijing, China, 380–384.

Nilsson, D. K., Larson, U. E., Picasso, F. and Jonsson, E. (2009). A first simulation of attacks in the automotive network communications protocol flexRay. *Proc. Int. Workshop on Computational Intelligence in Security for Information Systems*, 84–91.

Nilsson, D. K., Sun, L. S. L. and Nakajima, T. (2008). A framework for self-verification of firmware updates over the air in vehicle ECUs. *Proc. IEEE Globecom Workshops*, New Orleans, Louisiana, USA, 1–5.

NIST (2001). Announcing the Advanced Encryption Standard (AES). Federal Information Processing Standards Publication 197.

Northcutt, S. and Novak, J. (2002). *Network Intrusion Detection*. Sams Publishing. Indianapolis, Indiana, USA.

Otsuka, S. and Ishigooka, T. (2014). CAN security: Cost-effective intrusion detection for real-time control systems overview of in-vehicle networks. *SAE Paper No*. 2014-01-0340.

Park, S., Park, Y. and Park, Y. S. (2016). Degree of fault isolability and active fault diagnosis for redundantly actuated vehicle system. *Int. J. Automotive Technology* **17**, **6**, 1045−1053.

Petit, J. and Shladover, S. E. (2015). Potential cyberattacks on automated vehicles. *IEEE Trans. Intelligent Transportation Systems* **16**, **2**, 546–556.

Petri, R., Springer, M., Zelle, D., McDonald, I., Fuchs, A. and Krauß, C. (2016). Evaluation of lightweight TPMs for automotive software updates over the air. *4th ESCAR USA*, 1−15.

Ruddle, A., Ward, D., Idrees, S. and Roudier, Y. (2009). Security Requirements for Automotive On-board Networks Based on Dark-side Scenarios. EVITA Project Deliverable Report. D3.2.

SAE (2016a). Cybersecurity Guidebook for Cyber-physical Vehicle Systems. SAE International.

SAE (2016b). Time-triggered Ethernet. SAE International.

Schmidt, K., Zweck, H., Dannebaum, U. and Ag, I. T. (2016). Hardware and software constraints for automotive firewall systems. *SAE Paper No*. 2016-01-0063.

Schweppe, H., Idrees, S., Roudier, Y., Weyl, B., Khayari, R. E., Henniger, O., Scheuermann, D., Pedroza, G., Apvrille, L., Seudi'e, H., Platzdasch, H. and Sall, M. (2011). D3.3: Secure On-board Protocols Specification.

Seifert, S. and Obermaisser, R. (2014). Secure automotive gateway – Secure communication for future cars. *Proc. IEEE Int. Conf. Industrial Informatics (INDIN)*, Porto Alegre, Brazil, 213–220.

Smith, C. (2016). *Car Hacker's Handbook*. No Starch Press. San Francisco, California, USA.

Standaert, F.-X., Piret, G., Gershenfeld, N. and Quisquater, J.-J. (2006). SEA: A scalable encryption algorithm for small embedded applications. *Smart Card Research and Advanced Applications*, 222–236.

Takahashi, J., Aragane, Y., Miyazawa, T., Fuji, H., Yamashita, H., Hayakawa, K., Ukai, S. and Hayakawa, H. (2017). Automotive attacks and countermeasures on LIN-bus. *J. Information Processing*, **25**, 220–228.

Trusted Computing Group (2015). TCG TPM 2.0 Automotive Thin Profile. TCG Published, TCG Published Vol. 1.0.

Ueda, H., Kurachi, R., Takada, H., Mizutani, T., Inoue, M. and Horihata, S. (2015). Security authentication system for in-vehicle network. *SEI Technical Review*, **81**, 5–9.

Ujiie, Y., Kishikawa, T., Haga, T., Matsushima, H., Wakabayashi, T., Tanabe, M., Kitamura, Y. and Anzai, J. (2015). A method for disabling malicious CAN messages by using a centralized monitoring and interceptor ECU. *13th ESCAR Europe*, 1−10.

Vuillaume, C., Oka, D. K., Furue, T. and Etas, K. K. (2015). Cyber-security for engine ECUs: Past, present

and future. *SAE Paper No*. 2015-01-1998.

Ward, D., Ibara, I. and Ruddle, A. (2013). Threat analysis and risk assessment in automotive cyber security. *SAE Int. J. Passenger Cars - Electronic and Electrical Systems* **6**, **2**, 507–513.

Weimerskirch, A. (2011). Do vehicles need data security?. *SAE Paper No*. 2011-01-0040.

Weyl, B., Wolf, M., Zweers, F., Idrees, M. S., Roudier, Y., Schweppe, H., Khayari, R. E., Henniger, O., Scheuermann, D. and Apvrille, L. (2011). Secure On-board Architecture Specification. EVITA Project Deliverable Report. D3.2.

Wolf, M. (2009). *Security Engineering for Vehicular IT Systems*. Viewet + Teubner. Wiesbaden, Germany.

Wolf, M., Weimerskirch, A. and Paar, C. (2004). Security in automotive bus systems. *2nd ESCAR Europe*, 1–13.

Woo, S., Jo, H. J. and Lee, D. H. (2015). A practical wireless attack on the connected car and security protocol for in-vehicle CAN. *IEEE Trans. Intelligent Transportation Systems* **16**, **2**, 993–1006.

Woo, S., Jo, H. J., Kim, I. S. and Lee, D. H. (2016). A practical security architecture for in-vehicle CAN-FD. *IEEE Trans. Intelligent Transportation Systems* **17**, **8**, 2248–2261.

Wooderson, P. and Ward, D. (2017). Cybersecurity testing and validation. *SAE Paper No*. 2017-01-1655.

Yoshikawa, M., Sugioka, K., Nozaki, Y. and Asahi, K. (2015). Secure in-vehicle systems against Trojan attacks. *Proc. IEEE/ACIS 14th Int. Conf. Computer and Information Science (ICIS)*, Las Vegas, Nevada, USA, 29–33.

Zelle, D., Krauß, C. and Schmidt, K. (2017). On using TLS to secure in-vehicle networks. *Proc. 12th Int. Conf. Availability, Reliability and Security*, Reggio Calabria, Italy.

Ziermann, T., Wildermann, S. and Teich, J. (2009). CAN+: A new backward-compatible controller area network (CAN) protocol with up to 16x higher data rates. *Proc. Conf. Design, Automation and Test in Europe*, Nice, France.