2018-01-0018 Published 03 Apr 2018

Security Mechanisms Design for In-Vehicle Network Gateway

Feng Luo and Qiang Hu Tongji University

Citation: Luo, F. and Hu, Q., "Security Mechanisms Design for In-Vehicle Network Gateway," SAE Technical Paper 2018-01-0018, 2018, doi:10.4271/2018-01-0018.

Abstract

In the automotive network architecture, the basic functions of gateway include routing, diagnostic, network management and so on. With the rapid development of connected vehicles, the cybersecurity has become an important topic in the automotive network. A spoof ECU can be used to hack the automotive network. In order to prevent the in-vehicle networks from attacking, the automotive gateway is an important part of the security architecture. A secure gateway should be able to authenticate the connected ECU and control the access to the critical network domain. The data and signals transferred between gateway and ECUs should be protected to against wiretap attacking. The purpose of this paper is to design a secure gateway for in-vehicle networks. In this paper, the designing process of the automotive secure gateway is presented. Based on the threat analysis, security requirements for automotive gateway are defined. Secure communication, key master, and firewall are proposed as the security mechanisms to protect the automotive gateway. Secure communication mechanisms contain the message authentication and data encryption. Key master is a gateway function to distribute and update the keys for the secure communication of connected ECUs. Firewall based on message filter is designed to isolate the untrusted network domain and trusted network domain. The security functions of the automotive gateway are validated in a simulated attacking environment. A microcontroller with HSM is used to implement the secure gateway. Considering the influences of security mechanisms, the network latency is tested and the results have proved the secure gateway is effective and efficient.

Introduction

Motivation

With the development of information technology, connected vehicles are in the hot research fields. For the connect vehicle researches, cybersecurity is one of the critical requirements of in-vehicle networks. Hackers proved that connected vehicles can be attacked. The vulnerability of a connected vehicle may bring car theft, privacy disclosure, traffic accidents, and even terrorist attacks. Hacking methods to connected vehicles include in-vehicle network attacks, ECU firmware tampering, virus injecting and wireless signal disturbing [1]. The security of in-vehicle networks is important especially for safety-related systems, such as the engine control system, the brake control system, and so on. A spoofing message in those domains can result in heavy traffic accidents. The automotive gateway is the center of the network architecture. In the automotive network architecture, the gateway connects different network domains and manages the network status. Security mechanisms are needed for the network gateway to ensure the secure communication for in-vehicle networks. Besides, the in-vehicle network gateway is the interface that connected to the OBD-II, WLAN, Bluetooth, and so on, it should prevent the in-vehicle network from outside attacks.

Related Work

Related works in automotive cybersecurity have been promoted for years. In the EVITA project, HSM is proposed as the basis of ECU hardware security. Light HSM, middle HSM, and full HSM are defined for different security level requirements. Secure storage mechanisms and hardware acceleration engines for AES algorithm, random number generation are provided by HSM [2]. In the AUTOSAR specifications, crypto drivers are defined to be compatible with the HSM and to provide security interfaces to the crypto service module [3].

For the cybersecurity development, SAE published the J3061 Standard in 2016. The J3061 is the first standard on vehicle cybersecurity. The main contents of J3061 are as follows [4]:

- Defines the framework for the development of automotive cybersecurity. Integrate cybersecurity into the lifecycle process of automotive cyber-physical systems.
- Provides guiding principles for automotive cybersecurity development.
- Provides information on tools and methods that are used for cybersecurity designing and validating.
- Lays the foundation for the further standard development of automotive cybersecurity.

Besides, the SAE also proposed the standard J3101 to define the security requirements for ground vehicles hardware.

For the security of automotive gateway, there are some researches in this field. Seifert et al. introduce a secure gateway and create a language to detect failures and configure the gateway. But secure communication approaches and real-environments test results are not included [5]. Kurachi et al. present a secure gateway with a hardware-based filtering and anomaly detection. In the gateway, MAC is used for malicious messages monitoring, but data encryption is not included. Besides, this gateway is only suitable for CAN bus [6]. The cybersecurity development process of gateway should cover software level, hardware level, and system level, further researches are needed for the automotive gateway security.

Organization of this Paper

This paper proposed a secure gateway with secure communication, key master, and access control. This gateway is implemented and validated on the security MCU. Simulated attacking environments are designed to test the performance of security mechanisms.

In the first section, this paper describes the motivation and related works in automotive cybersecurity researches. Then the security requirements for in-vehicle network gateway are defined based on vulnerability analysis. In the following section, the designing of security mechanisms for gateway are proposed. The hardware implementation and test results are discussed in the last.

Threats and Security Requirements

In this section, the potential threats for automotive gateway are analyzed and the cybersecurity requirements are identified.

Gateway Functions

The research is based on a CAN/CAN FD/Ethernet gateway. Gateways need transferring messages between different domains and managing the connected network. The automotive network gateway is a main part of the automotive network architecture. The gateway connects powertrain domain, chassis domain, body electric domain, and infotainment domain. Besides, the gateway usually provides the diagnosis interface.

In this network architecture, the basic functions of the in-vehicle network gateway can be concluded as follows:

- Routing: message level, packet level, signal level
- Diagnostic
- Network management

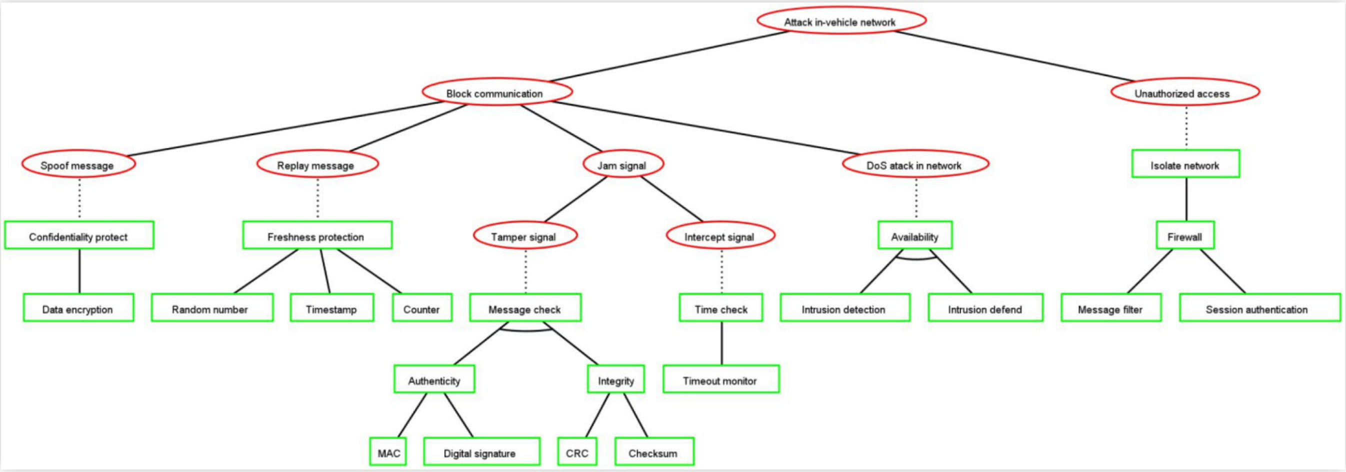
The automotive gateway should have the security mechanisms to prevent the in-vehicle networks from attacking.

Threat Analysis and Risk Assessment

TARA method is used to define the potential threats to the in-vehicle networks and identify the cybersecurity goals of the automotive gateway [7]. To identify the vulnerability of the in-vehicle network, attack tree (Figure 1) is used for threat analysis. In Figure 2, the attacks to in-vehicle networks can be achieved by injecting spoofing messages, tampering or intercepting network packets, replaying a time-critical message, DoS attacking, and invading the gateway with an unauthorized access.

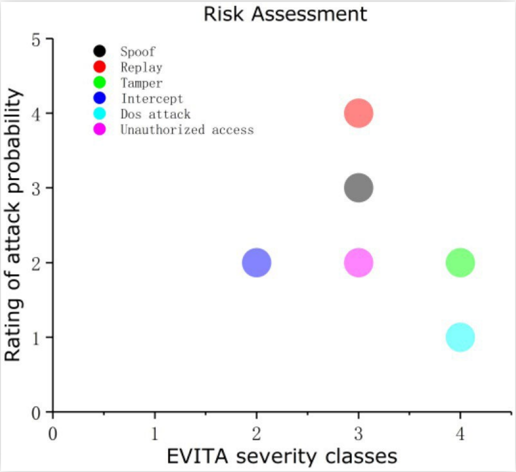
According to the attack tree, the possible attacking approaches can be found. Risk assessment for attacks can be helpful to identify the cybersecurity goals. The EVITA TARA method is used to for risk assessment in this research. This method is based on the analysis of the severity and the probability of attacks. Results of the risk assessment are shown in Figure 2. The attacks to in-vehicle networks can impact the driver's safety, privacy, financial issues, and the operation of vehicles.

FIGURE 1 Attack tree and defend tree for in-vehicle network



© SAE International

FIGURE 2 Risk assessment for in-vehicle network



© SAE International

The risk assessment proved the vulnerability of in-vehicle networks. A secure gateway in the automotive network architecture should have the following security features:

- Establishing secure communication with ECU nodes in the network, protecting critical signals and data.
- Controlling the access to the protected domain, isolating the untrusted domain from the trusted domain.
- Detecting intrusion in the network, logging status and responding to defend the attacks.

According to the defend tree (See Figure 1), the security requirements for networks attacks include confidentiality, freshness, authenticity, integrity, availability and access control. In a secure gateway, data encryption and message authentication are the security mechanisms for the routing in the gateway. The gateway is required to control the access to the network and prevent unauthorized access. Besides, the gateway is usually the key master that distributes and updates the keys for secure communication between ECU nodes.

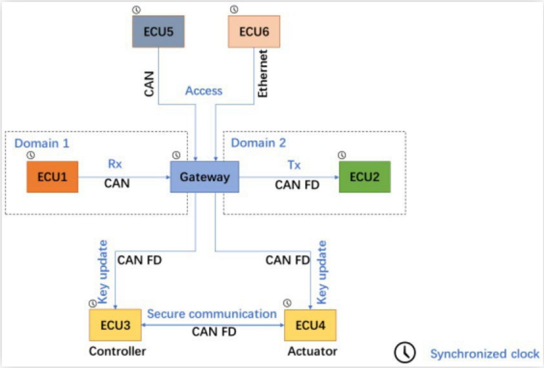
Security Mechanisms Design

In this section, the details of the security mechanisms in the automotive gateway are described. The method proposed in this paper is based on the assumption that the ECU nodes have a synchronized clock with the gateway. Clock synchronization can be achieved by clock synchronization protocols when ECU booting. The secure gateway proposed in this paper is shown in Figure 3.

Secure Communication

Routing is one of the most important functions of the automotive gateway. Data encryption and message authentication can be used for the secure communication between gateway and ECU node. As is shown in Figure 3, the gateway receives data from ECU1 by CAN bus and transmit the data to ECU2 by CAN FD bus. In this network architecture, CAN bus is connected to the domain 1 and CAN FD bus is connected to the domain 2. Domain 2 requires high security level. For the security of CAN bus, HMAC authentication is used for integrity and authenticity. For the security of CAN FD bus, AES encryption and CMAC authentication are used [8]. The AES encryption keeps the confidentiality of the data and CMAC is used for message authentication. The frame structure of CAN/CAN FD is depicted in Figure 4.

FIGURE 3 Secure gateway in the automotive network



© SAE International

The length of the data field in CAN frame is 8 bytes. To transmit the data and HMAC in a frame, the length of HMAC is truncated to 1 byte. This is a compromise approach between the security and the limitation of data field length. The increase of HMAC length can improve the authentication and the integrity of messages but the available length for data transfer is reduced. When higher security level required, the length of HMAC should be increased and the length of data should be reduced.

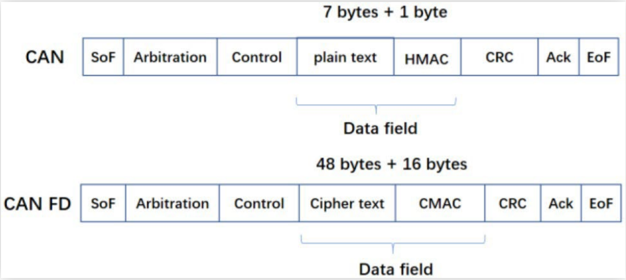
The protocol of authentication between ECU1 and gateway is shown in (1):

$$\text{ECU1} \rightarrow \text{Gateway} : M, \left\{ \{M, T, ID\}_{k_H} \right\}_{truncated} \tag{1}$$

Where M is the transferring signals in CAN bus, T is the value of synchronized clock in the ECU1, ID is the identifier of the CAN frame, the k_H is the sharing hash key between ECU1 and gateway.

The length of the data field in CAN FD frame is 64 bytes. 48 bytes of the data field are encrypted by AES-128, and

FIGURE 4 CAN/CAN FD frame structure



© SAE International

16 bytes of the data field are for CMAC. The protocol of authentication between gateway and ECU2 is shown in (2):

$$\text{Gateway} \rightarrow \text{ECU2}: \{M\}_{k_E},\ \{M, T, ID\}_{k_{MAC}} \tag{2}$$

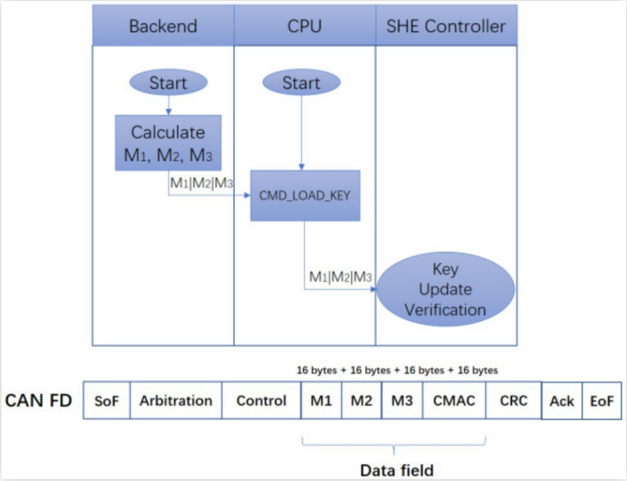
Where M is the transferring data in CAN FD bus, T is the value of the synchronized clock in the gateway, ID is the identifier of the CAN FD frame, k_E is the sharing encryption key between ECU2 and gateway, k_{MAC} is the sharing authentication key between ECU2 and gateway.

Key Master

The key for message authentication is a pre-shared key between the ECUs that is stored in the ECU firmware. For CAN bus, the truncated HMAC based on SHA-1 is used for message authentication, and length of key is 20-byte. For CAN FD bus, the CMAC based on AES-128 is used for message authentication, and length of key is 16-byte. The key for data encryption is distributed and updated by the key master. Since the countermeasure of data encryption is only available in CAN FD, the key distribution and update of key master also only suit for CAN FD. As is shown in Figure 3, ECU3 is a controller and ECU4 is the actuator. The communication between ECU3 and ECU4 is based on a secured CAN FD bus. The keys for the secure session include encryption key and authentication key. The secure gateway is the key master that distributes and updates the session key shared by ECU nodes. The key update process between the gateway and the secured communication group is based on CAN FD bus, HMAC is used for keep authenticity.

According to the SHE specification, the M1, M2, and M3 are the input parameters for key update [9]. The lengths of the M1, M2, and M3 are all 16 bytes. The key update protocol and CAN FD frame structure for the key update process are depicted in Figure 5. The M1, M2, and M3 is calculated with the updated keys and the unique IDs of the connected ECU. For this reason, the M1, M2 and M3 can keep the confidentiality of the keys. The updated key is generated by ECU3, ECU4 with the values of M1, M2 and M3, and keys will not be exposed in the memory in ECU3, ECU4 or in the CAN FD bus. A 16-byte CMAC is used during the key update session.

FIGURE 5 Key update protocol and message frame structure



© SAE International

The protocol of key updates can be described in (3, 4):

$$\begin{aligned}&\text{Gateway} \rightarrow \text{ECU3}: M1_3, M2_3, M3_3,\\&\{M1_3, M2_3, M3_3, T, ID_3\}_{k_{MAC_3}}\end{aligned} \tag{3}$$

$$\begin{aligned}&\text{Gateway} \rightarrow \text{ECU4}: M1_4, M2_4, M3_4,\\&\{M1_4, M2_4, M3_4, T, ID_4\}_{k_{MAC_4}}\end{aligned} \tag{4}$$

Where $M1_3$, $M2_3$, $M3_3$, $M1_4$, $M2_4$, $M3_4$ are the key update parameters for ECU3 and ECU4, T is the value of synchronized clock in the gateway, ID_3, ID_4 are the identifier of the CAN FD frame received by the ECU3, ECU4, k_{MAC_3}, k_{MAC_4} are the sharing MAC key between gateway and ECU3, ECU4.

Access Control

A secure gateway provides access control mechanism to protect the security domain in the automotive architecture. In this paper, a rule-based firewall is designed for controlling the access to security domain and filtering the unauthorized messages.

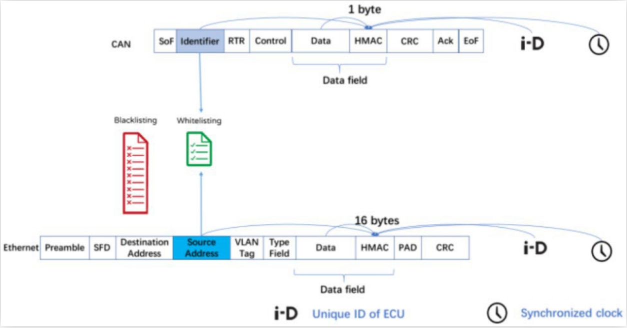
Security policies are divided into three levels for different security requirements:

1. Low security level: access without control;
2. Medium security level: access control based on ACL;
3. High security level: access control based on session authentication.

The security level of the security domain is decided according to the security requirements. The low security level allows all the messages to communicate with the security domain. The security policies of medium security level and high security level are introduced in this session (Figure 6).

Access Control List ACL is a whitelist rule that only the messages the recorded in the ACL are allowed to communicate with the security domain. The identifier of CAN/CAN FD bus frame and the source address of Ethernet frame are the characteristics to be recorded in the whitelist (See Figure 6).

FIGURE 6 Access control policies for the in-vehicle networks



© SAE International

Session Authentication The characteristics in the whitelist can be recorded by monitoring the bus data and then attackers can use a spoof message to access the security zone. Authentication is needed for defending the attacker monitoring. Session authentication policies are is executed by hash verification (See Figure 6).

The ECU5 and ECU 6 (see Figure 3) both have a unique ID, as is defined in the SHE specification. The access from ECU5 to gateway is by CAN bus and the access from ECU6 to gateway is by Ethernet. The ECU authentication messages are described in (5, 6):

$$\text{ECU5} \rightarrow \text{Gateway}: M, \left\{\left\{M, T, ID_5, UID_5\right\}_{k_{H_5}}\right\}_{truncate} \quad (5)$$

$$\text{ECU6} \rightarrow \text{Gateway}: M, \left\{M, T, SA_6, UID_6\right\}_{k_{H_6}} \quad (6)$$

Where M are the request data from ECU5, ECU6, T is the value of synchronized clock in the ECU5, ECU6, ID_5 is the identifier of the CAN frame sent by the ECU5, SA_6 is the source address of the Ethernet frame sent by the ECU6, UID_5, UID_6 are the unique ID of ECU5, ECU6, k_{H_5}, k_{H_6} are the sharing hash key between gateway and ECU5, ECU6.

Since the hash function is one-way function and it has the backward security, even if a hacker got the authentication message, he cannot decrypt it to find the inputs of the hash function. This feature can keep the security of the session authentication process.

System Implementation and Test

System implementation of the secure gateway and test results are presented in this section. And the network performances are analyzed to verify the effectiveness of security mechanisms.

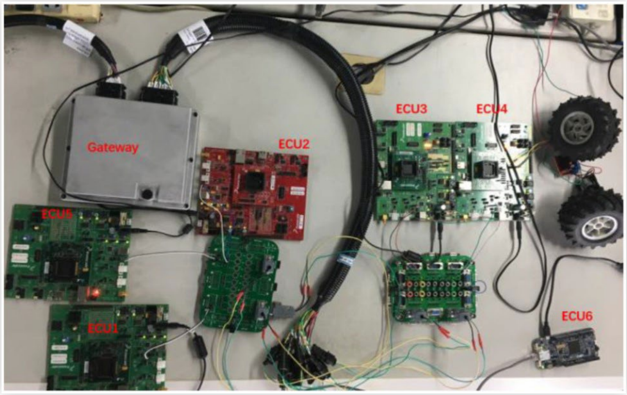
Implementation

The MCUs of the automotive gateway and the connected ECUs are MPC5748G. HSM provides the hardware-based security mechanisms. And in this gateway, there are 4 CAN channels, 4 CAN FD channels and 1 Ethernet channel (See Figure 7). The functions of ECU1~ECU6 are defined in Figure 3.

SHE firmware is implemented in the HSM module. It provides acceleration on AES-128 encryption/decryption, CMAC generation/verification, random number generation, and key generation. The hash function in this security system is SHA-1, and it is calculated by a software algorithm.

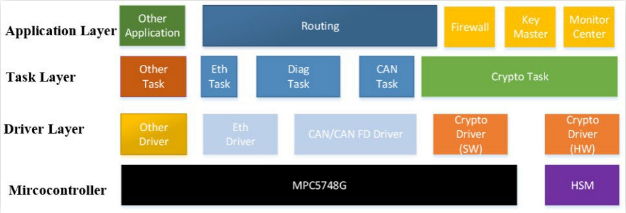
From the perspective of software, the software architecture can be divided into three layers (See Figure 8): application layer, task layer, and driver layer. The application layer provides network services and security services. Network services contain routing, network management and so on. Security services contain firewall, status monitor, key master, and the secure communication mechanisms. Task layer is based the driver layer and provides the application interface to the application layer. Among the tasks, the crypto task has two crypto drivers. One is the SHE firmware driver provided by HSM and another is the software algorithms driver provided by MPC5748G main cores.

FIGURE 7 System architecture demo of secure gateway and connected ECUs



© SAE International

FIGURE 8 Software architecture of secure gateway



© SAE International

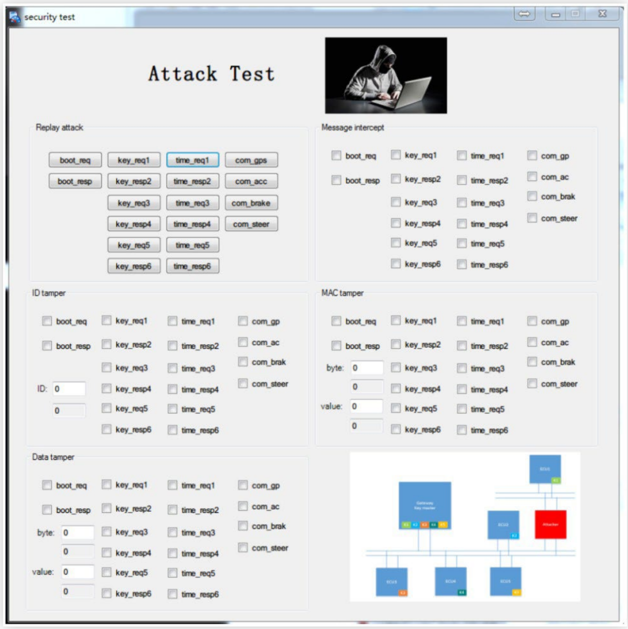
Test Cases

The attack tests to the security mechanism are simulated in the in-vehicle network and the network performances are recorded. In the test, the frequency of MCU is 160 MHz, arbitration rate of CAN/CAN FD is 500 Kbps, and the data rate of CAN FD is 2 Mbps. The clock is synchronized between ECUs and gateways.

Simulated Attack Test The attack to secure gateway is simulated with the CANoe environment (See Figure 9) and the MPC5748G. The attack methods are based on the Dolev-Yao model [10]. A virtual attacking ECU is simulated for MITM attack. A man-in-the-middle attack is an "indirect" intrusion attack. In this attack method, a spoof ECU node will the placed between two nodes which are in communication. The spoof ECU node can intercept or tamper the message transmitted and resend a fake message to the destination ECU node. The attacking methods in this experimental are listed in the following:

- Data leaking: Trying to get the meaning of data and signals in the data field of automotive network;
- Message replaying: Sending the recorded data to the bus.
- Message Tampering: A MITM ECU tamper the ID, data, or MAC in the automotive network.

FIGURE 9 Attack simulation panel in CANoe



- Message intercepting: A MITM ECU isolated the message to prevent the transferring.
- DoS attack: Sending a large number of meaningless messages to the bus and making the bus nodes unable to work.
- Unauthorized access: Trying to access the critical data in the security domain without permission.

Data leaking, message replaying, message tampering, and message intercepting are the attacks for secure communication and key update process. DoS attack is for secure communication. Unauthorized invasion attack is for firewall mechanism.

Performance Test Performance test mainly focuses on the network latency and busload rate. The test is in a real hardware environment. The factors that cause additional network latency include the encryption/decryption of data and the verification of CMAC or HMAC. Busload rate is affected by the valid data length in the data filed of bus frame. The network latency is observed by the oscilloscope.

Test Results

The monitor statuses of the attacks to secure communication, key master and firewall are listed in Table 1.

The Table 1 shows that during the secure communication session and key updates session, MACs (HMAC, CMAC) can prevent the automotive network from tamper attacks. For a clock-related MAC, it provides the freshness to against replay attacks. An intercept attack or DoS attack will result in a timeout status. The monitor in the gateway can only be applied for intrusion detection, the countermeasures for intrusion protection are not included in this research. The ciphertext in the CAN FD bus can help keep the confidentiality of data and the parameters M1, M2, and M3 also provide confidentiality function for the key to be updated. The results of firewall attacks prove that unauthorized frames that are not in the whitelist will be rejected to access the gateway. But if the frames are monitored by hackers, the hackers can use the frames that in the whitelist to visit the gateway. Session authorization mechanisms are needed to identify those unauthorized frames access.

The latency of the algorithms is listed in Table 2. Although the encrypted data is 48 bytes and CMAC is 16 bytes. The network latency caused by AES128 or CMAC calculation is much shorter than the network latency of 1-byte HMAC calculation. This is caused by the hardware acceleration of AES encryption and CMAC verification.

The busload rate has a direct relationship with the MAC length. Increasing the MAC length can increase the security of message authentication, but with the increase of MAC length, the field for data transferring decreases. For the reason, frame frequencies have to be increased to transfer the data within the specified time. This will result in a higher busload rate. In our experiments, the effective data field usage in CAN bus is 87.5% and effective data field usage in CAN FD bus is 75%. For Ethernet, the effective data field usage is 99%.

The test results prove that secure communication, key master, and firewall mechanisms in automotive gateway can increase the security level of the networks. Confidentiality, integrity, authority, freshness and access

TABLE 1 The test results of the attacks on automotive network

	Secure communication			Firewall	
Attacks	CAN	CAN FD	Key updates	ACL	Session authentication
Data leaking	Plaintext	Ciphertext	Ciphertext	_______	_______
Replay	HMAC error	CMAC error	HMAC error	_______	_______
Tamper	HMAC error	CMAC error	HMAC error	_______	_______
Intercept	Timeout	Timeout	Timeout	_______	_______
DoS	Timeout	Timeout	_______	_______	_______
Unauthorized frame	_______	_______	_______	Access reject	Access reject
Unauthorized ECU with monitored frame	_______	_______	_______	Access accepted	Access reject

TABLE 2 Network latency of the algorithms in one frame

Security mechanisms	Algorithms	Encryption/ MAC generation	Decryption/ MAC verification
Data encryption	AES128	52.64 μs	52.76 μs
Message authentication	HMAC	212.2 μs	213.9 μs
	CMAC	65.85 μs	69.59 μs

© SAE International

control are guaranteed by the security mechanisms in the gateway. The test results also show that the security mechanisms also cause additional network latency in the network. Hardware-based algorithms can accelerate the algorithms calculation, but this will raise the cost of microcontrollers. The balance among security, real-time, and cost should be considered.

Conclusions

This paper proposed a secure gateway that contains secure communication mechanism, key master, and access control firewall. Threat analysis and risk assessment are presented with the attack tree and defend tree, and security requirements are concluded to ensure the cybersecurity of the automotive network. Based on the security requirements, secure communication, key master, and firewall are proposed as the security mechanisms to protect the automotive gateway. Secure communication mechanisms contain the message authentication and data encryption. Message authentication is based on the verification of MAC, and it provides integrity and authenticity. Data encryption and decryption are calculated by the hardware accelerated algorithms and it provides confidentiality. Key master in the gateway is a module that distributes and updates the keys for the secure communication of connected ECUs. The firewall in the gateway is based on whitelist or session authentication to filter the access messages. The security functions of the automotive gateway are validated in a simulated attacking environment and a microcontroller with HSM is used to implement the secure gateway. The network latency of the security algorithms are tested and the results prove the secure gateway is effective and efficient.

References

1. Koscher, K., Czeskis, A., Roesner, F., and Patel, S., "*Experimental Security Analysis of a Modern Automobile*," Proceedings of the Symposium on Security and Privacy, May 2010.
2. Weyl, B., " D3.2: Secure On-board Architecture Specification", EVITA Project, 2011.
3. Specification of Crypto Service Manager, AUTOSAR Release 4.3.0.
4. Vehicle Cybersecurity Systems Engineering Committee, "Cybersecurity Guidebook for Cyber-Physical Vehicle Systems," SAE Standard J3061, 2016.
5. Seifert, S., Roman O., "Secure Automotive Gateway-Secure Communication for Future Cars," *Proceedings of 2014 12th IEEE International Conference on Industrial Informatics (INDIN)*. IEEE, 2014.
6. Kurachi, R., Takada, H., Mizutani, T., and Ueda, H., "SecGW - Secure Gateway for In-Vehicle Networks," Embedded Security in Cars Conference, 2015.
7. Ruddle, A., "D2.3: Security requirements for automotive on-board networks based on dark-side scenarios", EVITA Project, 2009.
8. Samuel, W., "A Practical Security Architecture for In-Vehicle CAN-FD," *IEEE Transactions on Intelligent Transportation Systems* 17(8):2248-2261, Aug. 2016.
9. Escherich, R., Ledendecker, I., Schmal, C., and Kuhls, B., "SHE-Secure Hardware Extension Functional Specification," Hersteller Initiative Software (HIS) AK Security, Version 1.1(rev439), 2009
10. Dolev, D. and Yao, A., "On the Security of Public Key Protocols," *IEEE Transactions on Information Theory* 29:198-208, 1983.

Contact Information

Feng Luo
Clean Energy Automotive Engineering Center
School of Automotive Studies, Tongji University
Shanghai, 201804
China
luo_feng@tongji.edu.cn

Qiang Hu
Clean Energy Automotive Engineering Center
School of Automotive Studies, Tongji University
Shanghai, 201804
China
404huqiang@tongji.edu.cn

Acknowledgments

This study is supported by "the Fundamental Research Funds for the Central Universities" (22120170265).

Definitions/Abbreviations

ACL - Access control list

AES - Advanced encryption standard

AUTOSAR - Automotive open system architecture

CAN - Controller area network

CAN FD - Controller area network with flexible data rate

CMAC - Cipher-based message authentication code

DoS - Denial-of-service

ECU - Electronic control unit

EVITA - E-safety vehicle intrusion protected applications

HMAC - Hash-based message authentication code

HSM - Hardware security module

Kbps - Kilobits per second

MAC - Message authentication code

Mbps - Million bits per second

MCU - Microcontroller unit

MITM - Man-in-the-middle

OBD-II - On-board diagnostics II

TARA - Threat analysis and risk assessment

WLAN - Wireless local area networks

Positions and opinions advanced in this paper are those of the author(s) and not necessarily those of SAE International. The author is solely responsible for the content of the paper.

ISSN 0148-7191