Security Considerations for In-Vehicle Secure Communication

Hongil Ju, BooSun Jeon, Daewon Kim, Boheung Jung
Information Security Research Division
ETRI
Daejeon, Korea
juhong, bsjeon, dwkim77, bhjungon@etri.re.kr

Kyudong Jung
Electronic design
THN Corp.
Daegu, Korea
guedong35@th-net.co.kr

***Abstract*—This paper describes security considerations and the expected E/E architecture for applying automotive Ethernet to vehicles. Automotive Ethernet cannot completely replace the existing legacy networks and will be used with them for a fairly long term. With the introduction of automotive Ethernet, security threats and vulnerabilities in automobiles are rapidly increasing, so it should be applied considering the safety and security of in-vehicle network from the beginning stage. In particular, this paper describes the security considerations required for secure communication in-vehicle networks including automotive Ethernet and proposes the needs of defining security levels according to the importance of transmission data.**

***Keywords*—automotive security, in-vehicle network, security level, automotive Ethernet**

I. Introduction

In recent, the electronic devices and software in automotive system are getting more complicated due to the emergence of new services such as autonomous vehicles and connected cars. And the amount of data to be transmitted in vehicles is rapidly increasing. So, the automotive Ethernet has been introduced to vehicle networks in order to improve the communication performance and to reduce the network complexity. In other words, automotive Ethernet is increasingly applied for the large amount of data transmission, cable cost reduction, weight reduction, communication efficiency, scalability and so on. Recently, several major OEMs have also announced plans to gradually introduce of Ethernet-based vehicles, and already have been launching them. For example, for luxury and premium vehicles, the BMW X5, the Jaguar Land Rover XJ, the Volkswagen Passat and several luxury brands already have automotive Ethernet on some models. Due to the needs of users and the development of technology, automotive Ethernet has been rapidly adopted and applied in vehicles. However, with the introduction of automotive Ethernet, security issues are also increasing. In order to resolve this security problems, new security solutions based on automotive Ethernet are required[1-2].

The conventional in-vehicle networks are independent and isolated environments, but recent automobiles are more complex and communicate with various external networks. In other words, because everything can be connected to automobiles, they have a number of external interfaces. As a result, it makes them a target for hackers to attack, and automotive security threats are rapidly increasing. In addition, as vehicles become more intelligent and evolve into autonomous vehicles, there are growing concerns about automobile security. In fact, in many recent cases, the security functions are provided as defined in each device or they are not provided at all. Therefore, automotive Ethernet should be designed and applied into vehicles with security in mind. The development of vehicle security technology based on automotive Ethernet is now the beginning stage. For the secure automotive services, this paper describes upcoming automotive network topologies and the security considerations on the change of automotive network environments.

The remainder of this paper is constructed as follows. Section II describes related works and Section III shows the security considerations and guidelines. Finally, we present the conclusions of this paper in Section IV.

II. Related Works

As the existing conventional vehicles based on legacy networks are not designed with security in mind from the beginning, there are various security vulnerabilities. In order words, since the legacy networks are a simple message frame based on broadcasting scheme, they are very vulnerable to cyberattacks such as eavesdropping of data, denial of service, transmission of fake messages, non-repudiation, and so on. In addition, if an attacker controls only a single ECU connected on network because of security weaknesses in ECU authentication and authorization control, it can control fully over the other ECUs in-vehicle networks[3].

Nowadays, in order to resolve this security threats on vehicles, several automotive security solutions have been researched and implemented. However, most existing security solutions are dedicated to legacy vehicle environments considering only legacy networks. In other words, they are single network domain based solutions that do not consider the interconnection with other domains. In addition, due to the limited capability and bandwidth of existing legacy networks, they are still vulnerable to the ECU authentication and message verification during interworking with the different network domains.

978-1-7281-0893-3/19/$31.00 ©2019 IEEE

However, automotive Ethernet-based security solutions can be novel security solutions considering the security threats and vulnerabilities of legacy networks and automotive Ethernet. The integration of Ethernet into the vehicles will bring opportunities to support for various automotive security solutions[1]. There are security weakness because Ethernet technology is well known networking technology. It means that not only the technical merits of automotive Ethernet but also the security technologies considering automotive security vulnerabilities due to automotive Ethernet should be applied. In recent, automotive Ethernet-based security solutions such as secure communications between ECUs, unauthorized ECU control, unauthorized traffic blocking, intrusion detection(IDS) or intrusion prevention(IPS) and so on have been researching and developing[3-5].

In addition, with the introduction of automotive Ethernet in vehicles, it is possible to design various Electric/Electronic-Architecture(E/E Architecture) topologies. So, automotive security vulnerabilities must be considered according to the new vehicle network topologies. For example, the conventional E/E architecture is the simple structure in which there is no gateway, or all ECUs are connected to only one gateway. However, nowadays, it is changing to domain-based E/E architecture with central gateway[5-6]. Also, there are studies on zone architecture based on the physical location in the vehicle, which has the effect of reducing cabling by about 20%[6]. In this paper, we present the general E/E Architecture expected in short-term future which interworks between legacy networks and automotive Ethernet. And, we describes security considerations and security guidelines for secure communications in vehicle network.

III. Security Considerations and Guidelines

In recent, automotive Ethernet has been applied to advanced driver-assistance systems (ADAS) and infotainment services which are independent of the existing legacy networks for vehicle safety. This is the reason that automobiles consider safety to be a top priority, and this approach is inevitable in order to apply a new network technology to existing vehicles. And, it will be expected that automotive Ethernet may coexist rather than replacing existing legacy networks completely. Therefore, this paper proposes the heterogeneous network topology that guarantees safety and security by physically isolating domains connected with legacy networks and automotive Ethernet as shown in Fig. 1.

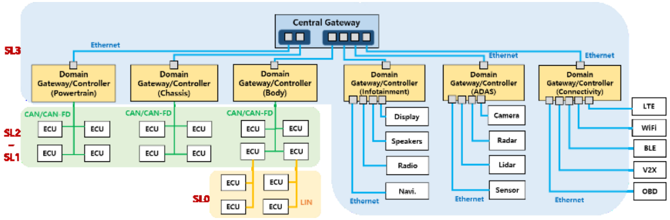
Central Gateway
Ethernet
SL3
Ethernet
Ethernet
Domain Gateway/Controller (Powertrain)
Domain Gateway/Controller (Chassis)
Domain Gateway/Controller (Body)
Domain Gateway/Controller (Infotainment)
Domain Gateway/Controller (ADAS)
Domain Gateway/Controller (Connectivity)
CAN/CAN-FD
CAN/CAN-FD
CAN/CAN-FD
SL2 – SL1
ECU
Display
Speakers
Radio
Navi.
Camera
Radar
Lidar
Sensor
LTE
WiFi
BLE
V2X
OBD
SL0
LIN
Ethernet
Ethernet
Ethernet

Fig. 1. The expected architecture of automotive Ethernet-based in-vehicle network

In Fig. 1, each domain is controlled by the Domain Gateway(DG) and communicates with another domain through the DG. The DG may be also called by Domain Controller(DC). In Fig. 1, the left three domains (Powertrain, Chassis, Body) have legacy networks and can communicate with other DGs through a central gateway. And the right three domains (Infotainment, ADAS, Connectivity) are connected to the automotive Ethernet and can communicate with other domains. Although the infotainment and ADAS domain can also be logically separated, the connectivity domain must be physically isolated from the vehicle's internal network. In other words, the connectivity domain that connects to the external network must be physically separated as well as logically. In results, it can enhance the security and safety of the vehicle's internal network.

In addition, there is the needs for classifying security levels according to the type of the using networks or the importance of transmission data, just as the existing vehicle networks are classified into class A ~ D according to bandwidth[7]. For more secure and safety automotive services, it is necessary to guide for applying the necessary security functions according to the security levels. Although Automotive Safety Integrity Level(ASIL) is a risk classification scheme defined by the ISO 26262, it does not describe about security levels[3]. In general, security functions that can be supported depend on the their capability of the device, and necessary security functions are different according to the sensitivity of the data. However, in many cases, security functions have been provided regardless above descriptions. Therefore, this paper describes the security functions required for secure communication in-vehicle networks and defines security levels according to the importance of transmission data.

In general, it is required at least three main security functions for secure communications. In order to provide this end, this paper classify and define four security levels (SL3 ~ SL0) according to security functions which are authentication, confidentiality and integrity of data. In this paper, SL3 is the highest security level and provides all security functions (authentication, integrity, confidentiality) necessary for secure communication. SL2 is the medium security level and provides the message authentication and integrity. And, SL1 is the low security level and provides integrity verification only. Finally, SL0 is the lowest security level and does not provide any security functions. Table 1 shows security levels classified in this paper.

TABLE I. SECURITY LEVELS FOR SECURE COMMUNICATIONS

Security Level	**Classification Category**		
	Security Functions	***Network Types***	***Overhead & Strength***
SL3	Authentication/Integrity/ Cofidentiality	Ethernet/ CAN-FD	High
SL2	Authentication/Integrity	CAN-FD	Medium
SL1	Integrity	CAN	Low
SL0	None	LIN	None

In Table 1, network types are also classified by security levels (SL3 ~ SL0). However, it does not mean that CAN network provides only the integrity and CAN-FD cannot provide the confidentiality. In other words, due to the limited bandwidth of CAN and CAN-FD, automotive Ethernet is more suitable than them for providing authentication and confidentiality. Therefore, Table 1 shows that there is the need to classification of the security levels for network types.

As shown in Fig. 1, the LIN network can be classified as SL0 which is checking only the transmission errors without any security functions. Because in the body domain, LIN bus is used for services that do not have speed and security requirements, such as power mirror control, door lock opening/closing, window opening/closing, and sunroof control. However, in Fig. 1, the CAN and CAN-FD network can be classified as SL1 or SL2 according to the device's limited capability or the importance of the data. It can be classified as SL1 if only the integrity verification is provided, and classified as SL2 if both the confidentiality and integrity are provided. In addition, in Fig. 1, automotive Ethernet can be classified as SL3 which is the highest security level and provides above three security functions. As shown in Fig. 1, automotive Ethernet is used for the communications with other domains through DGs. And, it is possible that above described DGs can provide additional security functions which are the access control for other domains and secure communication with other domains. Also, it can provide the authentication and authorization for devices connected to the same domain. In order to provide more various security functions, it is possible to use asymmetric cryptography algorithm such as digital signature. Compared with MAC using a symmetric key, digital signature can be provide authentication and non-repudiation. It means that, the device classified as SL3, like DGs, can support advanced security functions because they are very powerful compared with other devices.

In fact, regardless of the importance of data or the capability of the device, only some security functions are provided as defined in each device or they are not provided at all. It means that the conventional vehicles were initially designed without security considerations, they are limited to applying security mechanisms. Therefore, for the effective and secure automotive services, it is necessary to security guidelines considering the change of automotive network environments including automotive Ethernet.

IV. Conclusions

In this paper, we present the architecture and security guidelines for automotive Ethernet-based in-vehicle network. Especially, this paper focuses on onboard secure communication in the heterogeneous network topology. Since there is no standard yet for security levels described in this paper, we propose the needs of classifying security levels. And, we present the security considerations for applying automotive Ethernet to vehicle's network. Although safety is the most important factor in cars, it cannot be guaranteed if security is not ensured. Therefore, in order to resolve various security threats, more various security solutions should be designed and tried to apply because automotive Ethernet based in-vehicle networks are in the beginning stage.

Acknowledgment

This work was supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIT) (No.2018-0-00312, Developing Technologies to Predict, Detect, Respond, and Automatically Diagnose Security Threats to Automotive Ethernet-based Vehicles).

References

[1] C Corbett, E Schoch, F Kargl, and P Felix, "Automotive Ethernet: Security opportunity or challenge?", Sicherheit 2016, pp.45~54, 2016.

[2] Zelle, Daniel, et al. "On Using TLS to Secure In-Vehicle Networks", Proceedings of the 12th International Conference on Availability, Reliability and Security, ACM, 2017.

[3] Hu, Qiang, and Feng Luo. "Review of Secure Communication Approaches for In-Vehicle Network." International Journal of Automotive Technology 19.5 (2018): 879-894.

[4] Road Vehicles—Functional Safety, ISO 26262, International Organization for Standardization, 2011.

[5] den Hartog, Jerry, and Nicola Zannone. "Security and privacy for innovative automotive applications: A survey." Computer Communications 132 (2018): 17-41.

[6] Brunner, Stefan, et al. "Automotive E/E-architecture enhancements by usage of ethernet TSN." 2017 13th Workshop on Intelligent Solutions in Embedded Systems (WISES). IEEE, 2017.

[7] Huo, Yinjia, et al. "A survey of in-vehicle communications: Requirements, solutions and opportunities in IoT." 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT). IEEE, 2015.