ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 3, Issue 11 , November 2016

An Architecture of Car Diagnostic Service by using Enhanced Security Protocol

Jang hun Kim, Sung rae Cho, Seonghun Lee

Daegu-Gyeonbuk Institute of Science & Technology, 333. Techno jungang-daero, Hyeonpung-myeon, Dalseong-Gun, Daegu, 42988, Korea

ABSTRACT:In the automotive industry, Ethernet is being used as a vehicle communication network in order to increase the speed and data bandwidth of the vehicle network. Due to the characteristic of the disclosed protocol, Ethernet can be easily applied to various industrial fields. Also,since it is a standard specification based on open protocol, there aresome advantages, such as the compatibility between existing functions and other industrial fields. In recent years, automotive operating systems such as AUTOSAR have also supported Ethernet as a vehicle communication network. This is because functions such as advanced driver assistance system (ADAS) and around view monitoring system (AVMS) in vehicles require large data transfer and speed. It is also used to diagnose the vehicle remotely using Ethernet and to provide diagnostic information to a driver. However, the characteristic of the disclosed protocol causes Ethernet to be vulnerable to the security issues. Therefore, to ensure the safety of the vehicle and the driver, the enhanced method for the security and controlling access to the Ethernet is imperative.

In this paper, we propose a security and authentication protocol based on IPSec that encrypts the diagnostic information of the vehicle. With this security protocol, we can encrypt and authenticate diagnosis information of the vehicle on Ethernet. Therefore, the safety level of the vehicle can be enhanced.And,it will prevent to access diagnosis information from unauthorized user.

KEYWORDS: DoIP, Automotive Ethernet/IP, Ethernet Security, IPSec, Access Control.

I. INTRODUCTION

In an automobile field, the fault diagnosis is exploited to check the faults in a system. In order to obtain the vehicle diagnosis information, a diagnosis port in the inside of a driver's seat is used and by connecting to the in-vehicle network, the diagnosis information is displayed on a diagnosis equipment [1].

Various types of the vehicle communication network are used for newly launched vehicles. Nowadays, it supports Ethernet, including a well-used CAN, LIN, FlexRay, and MOST. The reason of the increase in the diversity of the vehicle network is related to the high complex vehicle functions.

Recently, many researches on Ethernet based vehicle communication network have been studied. [2][3][4] or name of authors proposed the method to wirelessly obtain the diagnostic information from a vehicle without the direct connection and to display the information on the diagnostic equipment.

The use of the wireless Ethernet brings several advantages. For example, in order to diagnosis a vehicle, a driver doesn't need to visit a repair shop, which reduces the time and cost for a driver [2]. However, when using Ethernet as a vehicle networks in other industries, the security problems could occur. Especially, the diagnostic information of the vehicle can be accessed from the outside the diagnostic port of the vehicle not the inside diagnostic port. Above all, using the internet network, the vehicle information can be stolen and a driver loses the control of the vehicle, which makes a driver in a dangerous situation [6]

In this paper, the diagnosis method using the Ethernet-based service, Diagnostics over Internet Protocol (DoIP), is introduced [5] and in order to prevent an intruder from the malicious access, we propose the method using the security protocol and access control.

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 3, Issue 11 , November 2016

In Section 2, the related works regarding the vehicle Ethernet and security protocol are introduced and Section 3 proposes the DoIP service design using the security protocol. Lastly, in Section 4, the paper is concluded with future works.

II. RELATED WORK

A. Automotive Ethernet/IP

With the increase in the consideration of functions regarding the infotainment, entertainment and safety, the amount of data transmission using the vehicle network also increases. Many drivers use the various multi medias like a smart phone. It is because the functions for the driver's safety and convenience, such as Advanced driver assistance system (ADAS) and Around view monitoring system(AVMS), are developed.

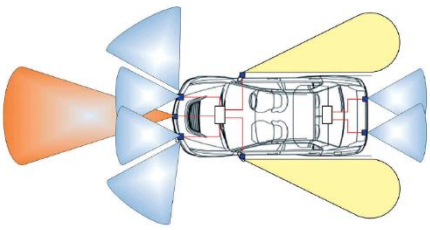


Fig. 1. Camera and radar for Driver Assistance Systems

Due to the driver's requirement and the development of functions for the safety and convenience, the conventional in-vehicle communication (MOS, CAN, LIN, and FlexRay) shows the limitation of data transmission. To address the limitation, in a recent automobile filed, Ethernet is considered as the vehicle communication for the massive data transmission [7].

Instead of using the existing vehicle networks, Ethernet-based method has several advantages. First, it overcomes the problem of the slower speed and lower bandwidth which CAN, LIN, FlexRay, and MOST have. This is because Ethernet supports at least 100 Mbps. Second, when using the same Ethernet protocol, the communication with other devices and vehicles is easily established.

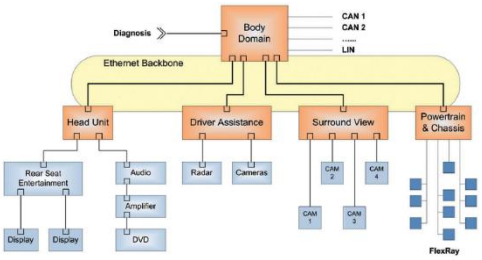


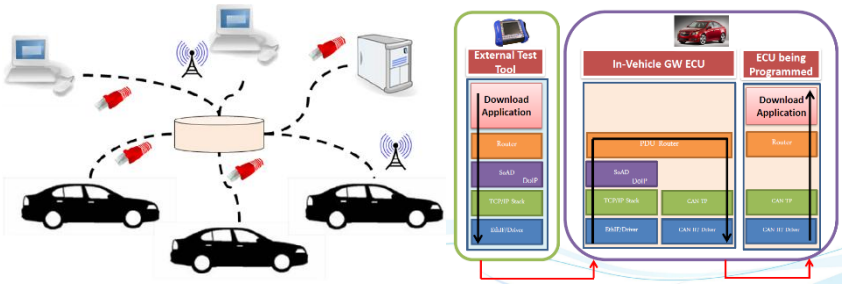
Fig. 2. Ethernet backbone in domain architecture

B. DoIP(Diagnostics over Internet Protocol)

In general, CAN and LIN are mostly used as the network for the body system of a vehicle. Recently, because of the requirement of the safety and the expansion of the bandwidth, the standard of MOST for FlexRay and the multimedia is introduced. However, in order to replace CAN or LIN with FlexRay and MOST for the vehicle diagnosis function of the body system, it has the limitation, such as the complexity and cost. In addition, CAN and LIN have the limitation of the speed and data transmission.

As a solution of the problem, in the vehicle diagnostic field, Ethernet is introduced and used for the diagnosis of a vehicle's electronic control unit (ECU) and the software update. DoIP is one of representatives of Ethernet-based diagnosis service [3] [4] [5].

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 3, Issue 11 , November 2016



(a) (b)

Fig. 3. (a)Highly interconnected system via the DoIP (b) the DoIP Architecture in AUTOSAR OS

There are the advantages when using the Ethernet network instead of the conventional vehicle network. First of all, since it uses IP-based protocols, the payload of a packet is exploited, so it transmits more data compared to the existing method. In addition, by applying the encryption protocols (IPSec and TLS), the encryption of the diagnosis information becomes possible, which the existing network could not provide [8] [9].

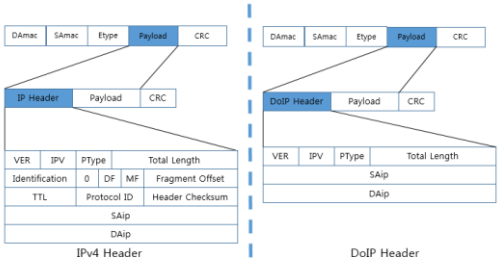


Fig. 4. IP Frame vs. DoIP Frame Structure

C. IPSec(Internet Protocol Security)

Internet Protocol Security (IPSec) is a most well-known standard method as the security protocol for IP. IPSec protocol is implemented on a network layer and is transparent to an application layer. Therefore, it has the advantage that doesn't influence on the user's application. It also has the great expandability, so it is utilized in various fields as the security protocol. Especially, for IPv6, it is compulsory to use IPSec. These days, many IPSec products are in a market and it is considered as the solution technology of the virtual private network (VPN).

IPSec consists of the authentication header and encapsulating security payload. The authentication header supports the data integrity of a sender and IP packet authentication and the encapsulating security payload is exploited for the encryption of sender's data. To transmit the encrypted data, tunnel mode and transport model are used and Internet key exchange (IKE) manages and distributes the key used for the encryption [9].

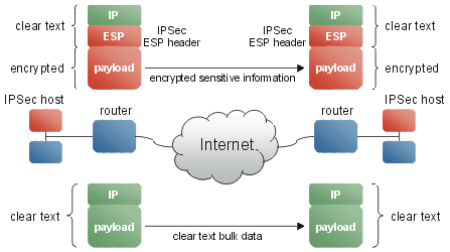


Fig. 5. The Architecture of IPsec

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 3, Issue 11 , November 2016

III.PROPOSED ARCHITECTURE

In this paper, the architecture of the proposed DoIP service for the vehicle diagnosis is shown in Fig. 6.

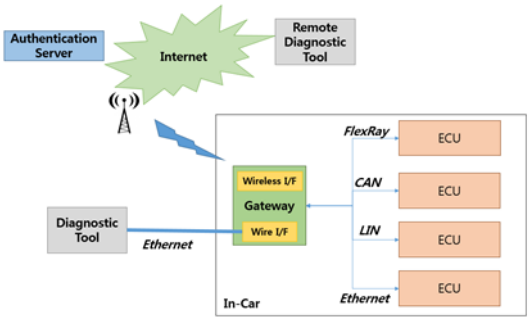


Fig. 6. the Architecture of a Security Enhanced DoIP

In this section, the characteristics of DoIP service are described as below.

1. It provides the access control method for the diagnosis information via the authentication.
2. It encrypts the diagnosis information to prevent the malicious use from the hacking.

The terms used this paper are explained as below.

1. Diagnostic Tool: Computer or equipment to exchange the diagnosis information with Ethernet gateway
2. Ethernet: Vehicle Ethernet wire-wireless network to exchange the diagnosis information
3. Ethernet Gateway: (i) it sends the encryption key to encrypt the diagnosis information of a vehicle. (ii) it sends the information of accessibility for each diagnostic equipment. (iii) it is a gateway to convert the diagnosis information to the Ethernet packet type.
4. Authentication Server: (i) it registers the diagnostic equipment. (ii) it provides the accessibility to the diagnosis information by identifying the unique ID of the diagnostic equipment. (iii) it generates the key to encrypt the diagnosis information.

The use of the diagnosis information via the malicious hacking causes the catastrophic situation. Especially, an electric car has more ECUs and exchanges the complex and various information, which is more vulnerable to hacking. For instance, if a hacker steals the information of the battery and changes the information, the vehicle might not be working properly and need the unnecessary charge, which reduces the battery life and causes the danger of the over charge problem. Therefore, we propose the method to prevent the malicious access to the encryption and the diagnosis information of a vehicle from a hacker.

A. **Authentication of Vehicle Diagnostic Equipment**

The authentication and registration for the diagnostic equipment are performed via the outside authentication server. The authentication server registers and manages the diagnostic equipment. Also, it assigns the access control of the diagnosis information to each diagnostic equipment. Therefore, it prevents the access from unauthorized equipment.
Tab. 1.shows the proposed access control level for the diagnosis information.

1. HIGH Level: Possible to read and write on the all diagnosis information of a vehicle
2. Medium Level: Possible to read the all diagnosis information of a vehicle, but can't write on the certain important information.
3. Low Level: Only possible to read the all diagnosis information of a vehicle

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 3, Issue 11 , November 2016

Access Control Level	Access Method	Diagnostic Information
High	Read, Write	ALL
Medium	Read, Write	ALL (except ECU Control information*)
Low	Read	ALL

Tab. 1. Access Control Level for Diagnostic Information

The method to authenticate the diagnostic equipment and set the accessibility is explained as below.

1. The diagnostic equipment is connected to Ethernet network and the unique ID is sent to Ethernet gateway.
2. Ethernet gateway sends the unique ID of equipment to the outside server.
3. The authentication server tries to authenticate the diagnostic equipment and sends the information of the encryption key and the accessibility of the diagnostic equipment to Ethernet gateway.
4. Ethernet gateway sends the information of the received encryption key and accessibility of the diagnostic equipment.

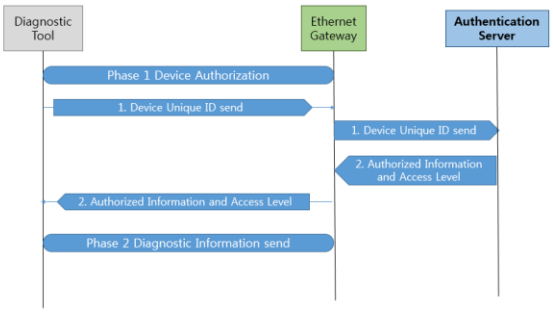


Fig. 7. An authorization process of Diagnostic Device

B. **Encryption of Diagnosis Information**

To encrypt the diagnosis information, only diagnostic equipment registered in the authentication server can receive the key. Therefore, the encryption of the diagnosis information is only conducted by the authenticated equipment. Also, the key for the encryption is distributed using the algorithm called IKE. However, since the distributed key is the one-time password, the new key is generated when the diagnostic equipment connects to the network again.

In this section, IPSec protocol is used as the method of encryption of the diagnosis information and the process is like below.

1. The diagnostic equipment requires the diagnosis information using the information of the received accessibility.
2. The Ethernet gateway encrypts the diagnosis information using the shared encryption key and send it to the diagnostic equipment.
3. The diagnostic equipment displays the information by decrypting the received diagnosis information with the shared encryption key.

The IPSec mode is classified into two models based on the encryption of the sender/receiver's address: the transport mode and tunnel mode. The tunnel model performs the encryption while the transport model does not. It is because the tunnel model has the better performance to analyze the network than the transport model. Therefore, though a hacker steals the vehicle's diagnosis information, he can't know whether it is.

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 3, Issue 11 , November 2016

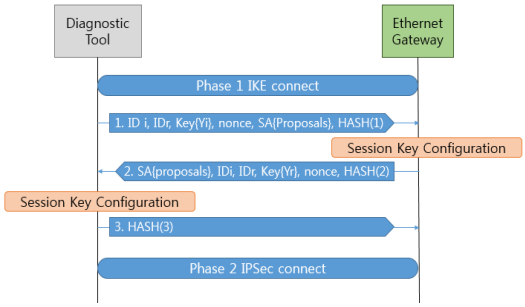


Fig. 8. The 2 Phase Connection of IPSec

The diagnosis information or not since he doesn't know the sender/receiver's address. As a result, in a case of a wireless network, the diagnosis information is communicated through several routers or switches, so it is well suited to use the tunnel model to send the diagnosis information.

IV. CONCLUSION

As increasing the driver's user experience (UX) and the interest in functions for the safety and convenience, the conventional network changes to the mass network, such as Ethernet. Also, as the vehicle Ethernet becomes a more common network for the vehicle communication network, it causes many issues regarding the safety.

In this paper, we introduced vehicle Ethernet based-DoIP service and surveyed the security protocols, such as IPSec to encrypt the diagnosis information, and the authentication method for the unauthorized equipment. Additionally, it is explained how to control the malicious access from the outside by using the security protocol and the access control when implementing DoIP service.

As future works, we plan to investigate more Ethernet security protocols, which are not introduced in the paper and plan to develop the Vehicle-Ethernet based functions for the driver's convenience, such as Automotive vehicle management system (AVMS) and Advanced driver assistance system (ADAS).

V. ACKNOWLEDGEMENT

This work was supported by the DGIST R&D Program of the Ministry of Science, ICT and Future Planning of Korea(16-RS-03).

REFERENCES

[1] T. V. Ramadasu. Trends in Automotive Remote Diagnosis. In International Mobility Engineering Congress & Exposition 2005~SAE India Technology for Emerging Markets, 23-25 October 2005.
[2] S. You, M. Krage and L. Jalics. Overview of Remote Diagnosis and Maintenance for Automotive Systems. In 2005 SAE World Congress, 11-14 April 2005.
[3] ISO/DIS 13400-1:2010-09-13: Road vehicles . Diagnostic communication over Internet Protocol (DoIP) . Part 1: General information and use case definition.
[4] ISO/DIS 13400-2:2010-09-13: Road vehicles . Diagnostic communication over Internet Protocol (DoIP) . Part 2: Network and transport layer requirements and services.
[5] ISO/DIS 13400-3:2010-09-13: Road vehicles . Diagnostic communication over Internet Protocol (DoIP) . Part 3: IEEE802.3 based wired vehicle interface.
[6] Sagstetter, Florian, et al. "Security challenges in automotive hardware/software architecture design." Proceedings of the Conference on Design, Automation and Test in Europe. EDA Consortium, 2013.
[7] Hank, Peter, Thomas Suermann, and Steffen Muller. "Automotive Ethernet, a holistic approach for a next generation in-vehicle networking standard." Advanced Microsystems for Automotive Applications 2012. Springer Berlin Heidelberg, 2012. 79-89.
[8] Glass, Michael, et al. ""Seis"-security in embedded IP-based systems." ATZelektronik worldwide 5.1 (2010): 36-40.
[9] Security Architecture for the Internet Protocol, http://tools.ietf.org/html/rfc4301.