Journal of Engineering and Applied Sciences 13 (Special Issue 2): 3007-3012, 2018
ISSN: 1816-949X

Security Service Technology in Self-Driving Environment

Jin-Keun Hong
Division of Information and Communication, Baekseok University,
76 Munamro Dongnamgu, 330-704 Cheonan City, South Korea

Abstract: Recently, research on autonomous driving technology has been actively carried out. However, the research on security technologies for various services provided by autonomous navigation technology and collaborative intelligent vehicle traffic system is also active. However, the debate on security technology is still unclear. The reason for this is that implementation accuracy and standards for autonomous navigation technology and collaborative intelligent transportation system technology are not yet clear. However, it is still necessary to look at aspects of security services including reviews of attacks and risks. For this purpose, this study has begun. The focus of this study is understanding of services and understanding of security service technologies in autonomous navigation technology and collaborative intelligent transportation system technology. Therefore, this study focuses on the policy issue and direction of the EU security service, the issue of privacy information and the security and safety issues considered in the platform. We also analyzed the performance of existing researches in relation to safety and safety of related vehicles. In this study, we find out the security issues required by the collaborative intelligent transportation system platform, focusing on EU. It is necessary to establish an appropriate regulatory framework based on PKI to establish a common and standardized C-ITS trust model or certificate policy across the EU and to establish compliance assessment and governance. This research is useful in understanding the importance of security and safety when studying collaborative intelligent transportation systems or autonomous navigation technology and the security requirements and current situations discussed. It also suggests that ultimate discussion is needed on how to proceed with the evaluation of personal information impacts in case of CAM or DENM messages.

Key words: Vehicle, attack, security, self-driving, auto, collaborative

INTRODUCTION

The characteristics of autonomous vehicles which are discussed recently are vehicles that can recognize the surrounding environment and judge the driving situation without the driver intervention and control the vehicle to travel. At this time, the vehicle recognizes itself and controls itself. However, the basic system that enables this autonomous vehicle technology is an advanced driving support system which is an advanced driving support system. This advanced driving support system includes frontal collision warning, lane departure warning and prevention, square area detection, automatic emergency braking and adaptive headlight technology. Frontal collision alerts typically utilize cameras, lasers and riders to proactively scan for potential obstacles to support advanced driving. Also, when the warning system detects the danger that the driver is clashed with another vehicle, the system will alert the driver if the driver does not take sufficient action. At the same time, the vehicle is prepared to stop completely through the braking device. Recently, collaborative vehicles have been actively studied for technology and autonomous driving technology for intelligent transportation systems. These projects have challenges such as AutoNet2030, adaptive, RobustSense and dense. There are also challenges such as Ecodriver, ADAS and ME, deserve, Udrive, team, enable-S3, Piper, prospect and seniors and I-game, companion, Citymobil2, Cats, V-charge and VRA. The I-game project focuses on the practical use of autonomous navigation systems that are safe for inter-vehicle communication. However, a major issue in such autonomous driving is the privacy issue. When considering the privacy issues here, you should be aware of data security issues, integrity, access control and ID retention and cancellation issues. It should also consider security issues such as improving vehicle safety issues, correcting lane departures, limiting autonomous parking and detecting obstacles in steering areas. In this respect, this study investigated the important situations and related issues in the autonomous driving environment. In this study, we first look at the related research on security services in self driving system and C-ITS environment. In addition, the focus will be on the study of vehicle vulnerability including security attacks.

Literaure review: Bendouma and Bensaber (2017) reviews road side unit authentication in vehicle network. This study focuses on exchanging security between different entities and this authentication scheme is guaranteed by the ECDSA algorithm. In addition, ECDSA's signature generation, signature verification and key generation performance are presented for security analysis and performance evaluation.

Conceicao *et al*. (2017) present about u TESLA protocol for vehicular network. In this study, they are interested in designing the uTESLA protocol in the car network.

Gifei and Salceanu (2017) considers safety and security in vehicle. This study emphasizes the importance of vehicle security if they are interested in identifying vulnerable areas in vehicle certification. Therefore, safety and security management are considered. When dealing with the problem of safety management system, they are interested in deriving safety management system values that take into account the process values of ISO 266262, numerical values of SAE J3061 and quality control figures. However, it is regrettable that the limitations of this study are not how to apply effectively, how to apply these figures based on certain weights and practical examples and models.

Gaikwad and Markande (2016) design a vehicle safety system consisting of a module consisting of a vehicle access system, a GSM Module, a transceiver configuration and a fingerprinting module, a wiper control system and a headlight system, a transceiver an optical sensor and a non. And the performance of the implementation is presented (Gaikwad and Markande, 2016).

Kilcoyne *et al.* (2016) conducted a study on the tire air pressure management system to improve vehicle security. In the experiment, the pressure sensor signal is analyzed. They are also analyzed the protocol of the pressure sensor system. However, the received pressure sensor management message consists of a frame composed of preamble, sensor ID, pressure, temperature and check value. In the experiment, this frame transmits the trigger signal first to spew the diagnostic tool. Security analysis shows that the original ID is spurred on data and spoiled data and the sensor ID is changed. This is a very interesting study. In this study, it is proposed an LFSR polynomial for solving this eavesdropping problem by encrypting a 64 bit sensor ID.

Malaney (2016) is looking at quantum vehicles. In this study, they are also studying quantum-based key distribution. Authentication of device real identity requires post-shared secret value. They are also studying quantum secret values (Malaney, 2016).

Wararkar and Dorle (2016) conducted a study on transmission security between vehicle networks using RF receivers. In this study, they are analyzing the characteristics of the vehicle network and they are examining sensing, proximity, recognition, processing, storage, routing and communication processes. Test cases are presented for messages displayed on vehicles, base stations and vehicles, server unit display messages and automated header light switching.

Ward (2016) studied safety and security for connected vehicles. It introduces the level of automation of autonomous vehicles and examines the cyber physics system. they will, of course, look at current security requirements and consider information security issues, including risks. Product integrity and assurance are discussed. Product assurance includes cybersecurity, availability, reliability, system engineering and product safety. It also focuses on the cyber security of the vehicle, taking into account security issues at the remote attack or vehicle level, system and ECU levels, hardware and software and silicon level. Therefore, when designing functional safety and security, the vehicle must be designed robustly. Functional safety issues should be considered in order to design electronic systems related to safety in ISO 26262 and as noted in SAE J3061, a cyber security guide for cyber physical vehicle systems. SAE J3061 identifies and evaluates existing security processes, practices and tools. This cyber security and functional safety can share parallel processing and risk assessment and threat analysis are considered in preparation for risk analysis. However, this specification includes protecting PII and sensitive data, using least privilege principles, applying DiD and preventing users from unauthorized changes at the vehicle level. Of course, the system should minimize data collection, enable user policies and controls and protect the use and delivery of storage, PII information. In addition, appropriate notifications should be provided for the data collected, stored and shared.

Kleberger *et al.* (2014) present a communication detection algorithm that is used in this study to identify in-vehicle domains based on other selection criteria such as vehicle safety integrity level, payload size and message type.

In this study, Moalla *et al*. (2014) analyzed security constraint requirements and requirements in C-ITS environment. In security constraint requirements, critical time constraint problems, very low error tolerance for errors, heterogeneous system scalability, mention the problem. Security requirements also include availability, authentication and authorization, integrity, confidentiality, non-repudiation, privacy and remediation. Of course, the C-ITS vehicle security framework requires the DiD Model and analyzes from the perspective of functional layers (secure platform layer, boundary protection layer, security policy layer, analysis and audit and monitoring layer, security management layer).

The composition of this study is as follows. This study first examine the service environment of self-driving and C-ITS in center of the collected data of ITS service and vehicle. Also, we will analyze security service in the self-driving and C-ITS environment and will conclude.

SERVICE TECHNOLOGY IN SELF-DRIVING AND C-ITS ENVIRONMENT

The demand for autonomous driving service technology which is being developed recently is of great interest as well. However, the key technologies required for this autonomous driving service are automobile autonomous navigation system, vehicle automatic valet parking system and co-pilot system technology. The vehicle autonomous navigation system collects obstacle and driving situation information based on the sensor and transmits the collected information and the traveling path through the V2X communication to the vehicle. At this time, the system that autonomously travels the vehicle through the control device mounted on the vehicle is the autonomous vehicle traveling system.

Here, the vehicle automatic valet parking system refers to a system in which the vehicle itself controls the parking of the vehicle to an appropriate parking space by mapping and mapping the predetermined parking lot by recognizing the public parking space by the vehicle itself. And the co-pilot system judges driving situation and driver's condition based on multiple sensors and vehicle communication technology. At this time, the driver status refers to a drowsy state or careless state and a non-responsive state or normal state. It is said that the co-pilot system is a system that determines the driving control right of the vehicle through this judgment and helps the vehicle itself to cooperate with the driver. The technologies for these three systems are helping to make autonomous navigation services complete. In this autonomous navigation technology, however, the need for establishing security governance has been greatly emphasized.

If so, you should pay attention to the recommendations of the platform for autonomous navigation services as well as intelligent transportation systems. These recommendations are based on PKI. In addition, a well-defined standardized trust model and certificate policy should be established with appropriate regulations. In addition, an evaluation process should be established. Since, CAM messaging and DENM messages are mainly used for the purpose of personal identification information, there should also be a discussion on how to carry out personal information impact assessment. Collaboration In intelligent vehicle transport systems, it is important to mention the notifications that are being discussed, notifications about dangerous locations, discussions of display application programs and many other factors. However, in case of notification service of dangerous location, it refers to warning function of vehicle traffic, warning function of road research, warning function of weather condition, emergency braking light and access to emergency vehicles.

In addition, display application programs should provide services such as in-vehicle signs, vehicle speed limits, signal violations or intersection safety services, traffic signal priority requests for specified vehicles, green optimal speed recommendations and local hazard warning. In addition, alternative fuel vehicles, fueling and filling station information, vulnerable road user protection, road parking management and road parking prohibition information and navigational information for connecting to urban centers and outskirts should be provided. Among the discussions on these services in the name of cooperative collaboration and strengthening of cooperation, European institutions are emphasizing requests for the co-operative vehicle's conformity assessment process, public key infrastructure and EU-wide security framework services.

If so, what challenges do the EU have? First, the EU should be governed by EU, national and industrial bodies, including public institutions, road operators, vehicle manufacturers and C-ITS service providers. A common security solution for installation and operation should be developed and a high level of autonomous navigation security should be established. In addition, the EU raises the need for a future multi-trust domain. This need requires a single EU trust domain with non-European countries and a realization of interoperability for this trust domain should be presented. This calls for standardization, retraction and compliance assessments. In addition, actor identification and participation issues are related to PKI governance.

Another fact is the lack of channel capacity being serviced in the platform of the collaborative vehicle intelligent transportation system. This results in limitations in service provision. Therefore, it is argued that it is necessary to establish the hybrid communication and communication channel and also to make the problem about geographical coverage introduction mandatory. In this respect, additional spectrum allocation is required which requires expansion of capacity for international cooperation. This frequency band needs to be secured in the 5.8 the 5.9 and the 63-64 GHz band.

According to the report on the platform of the collaborative vehicle intelligent transportation system recently published by EU EC, there are issues about data protection and privacy issues. That is, determining whether data exchanged through CAM and DENM will be classified as personal data. The problem also relates to the fact that this data is indirectly applied to vehicle identification information, the identity of the vehicle owner (ID) and the application of EU legislation on data privacy and data protection. The problem, however is that the EU's EC is not legally binding. Vehicles of cooperative intelligent transportation systems need a way to reasonably identify individuals. Nonetheless autonomous vehicles that communicate via GNSS or other infrastructure channels that provide location information can generate personal information. The problem is that organizations that are responsible for autonomous collection, use, disclosure, security and access to personal information must comply with and protect their privacy and surveillance laws. Therefore, we want to investigate safety problems, privacy problems and security service problems in the autonomous driving environment.

SECURITY ISSUE IN SELF-DRIVING AND C-ITS ENVIRONMENT

Autonomous driving and collaboration realistic problems in intelligent transportation systems are safety and security issues. Here, the security problem is closely related to the cyber security problem. Malfunctions in autonomous driving services soon lead to vehicle crashes and abnormal behavior. In this case, collision will occur if the gap between vehicles is not maintained properly. It can also pose a risk to the safety of autonomous driving which is unexpected when the vehicle's external and internal networks are exposed or attacked by an attacker. Therefore, what is most important in autonomous driving service is security service including privacy to provide vehicle safety and vehicle service safety. When discussing privacy issues, transparency, precise understanding of the situation, identity identification issues, data security and integrity, access control and accountability are some of the issues involved. The problem is that this safety and security issue is a matter to be solved by the vehicle manufacturer or operator.

Recently, it has been pointed out that steering safety problem is connected with security problem in steering conference of autonomous vehicle. Various techniques for correcting the steering function, improving the safety of the vehicle and correcting the lane departure have to be applied which is related to the damage problem from the security attack. Also, it is necessary to check the possibility of attack against autonomous parking. This problem may be caused when the speed of the vehicle is low, the operation condition of the system is maintained, the function to be operated and terminated by the driver is autonomous from other attacks, The ability of the system providing the device to properly detect obstacles and to avoid them can be related to security attack services. The problem that autonomous driving service keeps driving lane can also be connected with security attack service.

The United States is carrying out an empirical evaluation of V2V vehicle safety functions. In NHTSA, development guideline for autonomous vehicle technology is presented and there is an active movement in the revision of communication regulations. Among these contents, roadmap for safety enhancement, mandatory for vehicle standard V2V communication and introduction of security standards are also being promoted. In addition, electronic safety, functional safety, cyber security and autonomous vehicles are continuously being studied by establishing the safety division of electronic systems in NHTSA for autonomous driving safety. What about Europe? In the ApatIVE project in Europe, research is underway to improve cognitive performance in autonomous driving demonstration and road environment. In addition, studies are underway to change the control between the driver and the vehicle or to evaluate the road safety. What about EU EC/WP29? This research group defines autonomous driving techniques. It discusses legal limitations and issues and discusses safety issues and security issues.

When discussing the issue of security capability, it is important to consider the security capabilities and relevance of the transmission capacity. Several intelligent traffic system terminals transmit CAM and DENM messages. However, the transmission capability of this transmission message is limited. In general, it is difficult to exceed 1200 packets per second in the communication environment. The CAM should be triggered 1-10 times per second depending on the vehicle environment. In the case of DENM, it can be triggered every time an event occurs and can be transmitted at a maximum of 20 times per second. Therefore, considering the ability of security services to be considered in such a limited transmission capacity is an important issue. There is a problem with transmission capacity when messages in the In-Vehicle information (IVE), Signal Phase and Timing (SPaT) and road topology (MAP) types are transmitted or messages of longer length than this message are delivered.

We will discuss cyber security issues in autonomous vehicles. Key components of the vehicle's various systems include sensor systems and their associated

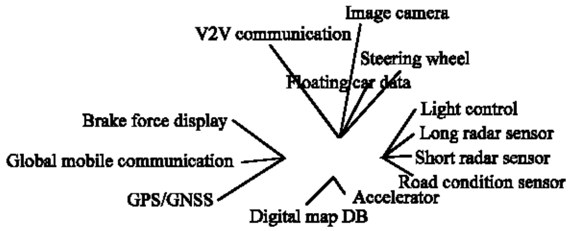

Fig. 1: Cyber security in self-driving environment

components. These sensor systems include braking device displays, global mobile communication systems, navigation systems, digital databases, inter-vehicle communications, cameras, active steering, adaptive light control, wide range or short range radar sensors and road condition sensors. However, a cyber attack on this sensor can occur. Attacks on ultrasonic sensors can have jamming or spoofing and millimeter wave channel attacks can also trigger relay attacks. A blinding attack may occur on an attack on a vehicle-mounted camera as follows in Fig. 1.

In autonomous vehicles, there may be a variety of security problems ranging from design to the environment in which the vehicle is actually operating. However, there are problems in the case of design issues that reflect the design of core software or hardware, how to provide a reliable platform or ensure interoperability and standardization.

Components of an autonomous vehicle that may be vulnerable to attack in cybersecurity include an inter-vehicle communication channel an engine control unit, a transmission control unit, a vehicle lock and open control unit, an interface with a wireless device, a Tyre Pressure Management System (TPMS) access interface, an On Board Device (OBD) interface, an HVAC control unit and the like. But why these units are vulnerable? Because there are complicated components such as devices, control units and interfaces. As modules and their functions become complex, inspections and inspections for insufficient software vulnerabilities can expose the unit to security vulnerabilities. In addition, as telematics and infotainment functions increase, the underlying vulnerable communication channels, vulnerable interfaces and vulnerable areas are exposed. In other words, audio, video and diagnostic devices may be vulnerable paths and measures should be taken. But why these units are vulnerable? Because devices, control units and interfaces made of hardware or software are complicated. As modules and their functions become complex, inspections for insufficient software vulnerabilities can expose the unit to security vulnerabilities. In addition, as telematics and infotainment functions increase, the underlying vulnerable communication channels, vulnerable interfaces and vulnerable areas are exposed. In other words, audio, video and diagnostic devices may be vulnerable paths and measures should be taken.

Another issue is the interface design that supports PKI. Appropriate computing power, storage capacity and memory space are required to design the appropriate platform. However, it is difficult to realistically provide this space and ability. In addition to this, if the system is to be extended or interoperability must be ensured, this can be a key issue in terms of security as well as major security aspects. Privacy services that provide pseudonym, services that detect compromised units, prevention of tampering during transmission or non-repudiation services are key considerations in the design of PKIs.

To summarize, an authentication function must be provided to prevent Spoofing (S). Tampering (T) attacks must be provided with integrity and non-Repudiation (R) functions should be provided to the tampering agent. For Information disclosure (I), there should be a confidentiality function and permission issues should be granted for permission issues. Finally, when analyzing a threat model against a vehicle attack, a threat model such as STRID can be applied.

So, what should you consider when evaluating privacy issues in autonomous vehicles? The question is as follows:

- Is it possible to handle autonomous vehicles under the current regulations?
- What type of data will be collected by autonomous navigation technology?
- And who can access this data?
- What can third parties do with this data?
- Is there an obligation to notify the self-driving vehicle driver of this collected data?
- Does the rule now release responsibilities? Are you resiliently testing cyber threats?
- Is the insurance company able to raise sufficient insurance premiums?

CONCLUSION

In recent collaborative intelligent transportation systems, security requirements for CAM are taken into account in state of static location, dynamic location and danger warning function at local location. How will this function be accommodated in authentication and authorization? And how to address this issue in confidentiality and privacy issues. In this study, we investigated technical issues in autonomous navigation service and collaborative intelligent transportation system. In addition, we focused on the understanding of security governance including PKI and integrated authentication system. Future research on this study should continue.

ACKNOWLEDGEMENT

This research study is made possible through the project funding of Industry Academia Cooperation Group in Baekseok University.

REFERENCES

Bendouma, A. and B.A. Bensaber, 2017. RSU authentication by aggregation in VANET using an interaction zone. Proceedings of the IEEE International Conference on Communications (ICC'17), May 21-25, 2017, IEEE, Paris, France, ISBN:978-1-4673-9000-2, pp: 1-6.

Conceicao, R.M.D., R.S. Lobato, A. Manacero, R. Spolon and M.A. Cavenaghi, 2017. iTESLA protocol in vehicular networks. Proceedings of the 12th Iberian Conference on Information Systems and Technologies (CISTI'17), June 21-24, 2017, IEEE, Lisbon, Portugal, ISBN:978-1-5090-5047-5, pp: 1-6.

Gaikwad, N. and S.D. Markande, 2016. Intelligent safety control for automotive systems. Proceedings of the International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT'16), September 9-10, 2016, IEEE, Pune, India, ISBN:978-1-5090-2081-2, pp: 653-656.

Gifei, S. and A. Salceanu, 2017. Integrated management system for quality, safety and security in developing autonomous vehicles. Proceedings of the 10th International Symposium on Advanced Topics in Electrical Engineering (ATEE'17), March 23-25, 2017, IEEE, Bucharest, Romania, ISBN:978-1-5090-5161-8, pp: 673-676.

Kilcoyne, D.K., S. Bendelac, J.M. Ernst and A.J. Michaels, 2016. Tire pressure monitoring system encryption to improve vehicular security. Proceedings of the IEEE Conference on Military Communications (MILCOM'16), November 1-3, 2016, IEEE, Baltimore, Maryland, ISBN:978-1-5090-3782-7, pp: 1219-1224.

Kleberger, P., N. Nowdehi and T. Olovsson, 2014. Towards designing secure in-vehicle network architectures using community detection algorithms. Proceedings of the IEEE Conference on Vehicular Networking (VNC'14), December 3-5, 2014, IEEE, Paderborn, Germany, ISBN:978-1-4799-7661-4, pp: 69-76.

Malaney, R., 2016. The quantum car. IEEE. Wirel. Commun. Lett., 5: 624-627.

Moalla, R., B. Lonc, H. Labiod and N. Simoni, 2014. Towards a cooperative its vehicle application oriented security framework. Proceedings of the IEEE Symposium on Intelligent Vehicles, June 8-11, 2014, IEEE, Dearborn, Michigan, ISBN:978-1-4799-3639-7, pp: 1043-1048.

Wararkar, P. and S.S. Dorle, 2016. Transportation security through inter Vehicular Ad-Hoc Networks (VANETs) handovers using RF trans receiver. Proceedings of the IEEE Students' Conference on Electrical, Electronics and Computer Science (SCEECS'16), March 5-6, 2016, IEEE, Bhopal, India, ISBN:978-1-4673-7919-9, pp: 1-6.

Ward, D., 2016. Aligning safety and security systems for connected vehicles. Proceedings of the Conference on Cyber-Security for Urban Transport Systems, February 24, 2016, IET, London, England, UK., ISBN:978-1-78561-234-3, pp: 1-28.