International Journal of Control and Automation
Vol.10, No.6 (2017), pp.35-48
http://dx.doi.org/10.14257/ijca.2017.10.6.05

Secure Vehicle Pseudonym Certificate for Smart Car in Internet of Vehicles*

Taekjung Kim[1], Byungwook Jin[1], Si-Ho Cha[2†] and Moon-Seog Jun[1]

[1]*Department of Computer Science, Soongsil University*
kimmycode23@gmail.com
[2]*Dept. of Multimedia Science, Chungwoon University*
shcha@chungwoon.ac.kr

Abstract

As the vehicle communication technology developed in Korea is implemented as a real service, interest in smart cars is increasing. With this, concerns over safety of vehicles are also rising and vehicle communication is based on authentication. Therefore, there may be risks when the authentication is stolen. If the vehicle's ID is known through a stolen authentication while the car is moving at a high speed and the control over the vehicle is hijacked, this can lead to a fatal accident for the driver. This paper suggests a method that generates the authentication through a pseudonym ID to prevent such cases.

Keywords*: WAVE, ITS, Certificate, C2C, Vehicle*

1. Introduction

The Cooperative Intelligent Transport Systems (C-ITS), that was operated as part of a pilot program between Daejeon and Sejong in September, 2016 saw the newly developed WAVE (Wireless Access for Vehicular Environment) technology applied to actual services, leading to high anticipation for the commercialization of this technology. Intelligent Transport Systems (ITS) converges IT with the components of the transport system such as roads and vehicles to use real-time transport information, to achieve lower cost and higher efficiency. ITS can be categorized into V2V (Vehicle-to-Vehicle) and V2I (Vehicle-to-Infrastructure). V2V enables direct communication between vehicles that move at a high speed to offer safety, while V2I enables the exchanges of information between a moving vehicle and nearby infrastructure.

Existing ITS services offered static services when the vehicle moves through a specific spot or section, limiting its ability for prompt response. But the C-ITS which is operated as a pilot in Korea offers dynamic services for mutual communication that is constant between the moving vehicle and the road infrastructure. This makes preempting of accidents and prevention possible. The WAVE system technologically supports the communication between the moving vehicle and other vehicles or user devices to offer real-time transport data. This is expected to help prevent crashes or fatal accidents. With the increase in applied wireless communication technologies, MITM (Man in the Middle) attacks or replay attacks have also increased, exposing the security of vehicles to risks. If the message of a crash is exposed to a third party and is changed, then nearby vehicles might not know of this, which can lead to an even bigger accident. To prevent such a scenario, the existing system aims for a reliable authentication and mutual authentication given that the vehicles are moving at high speed.

* This paper is a revised and expanded version of a paper entitled 'A Study on Issuance of Secure Vehicle Certificate for Vehicle to Vehicle Communications in Internet of Vehicles' presented at SIT2016, Jeju, Korea, 23th December, 2016.
† Corresponding Author: Si-Ho Cha

ISSN: 2005-4297 IJCA

Authentication forms are easy to access and to copy but if it is not managed well or stored online such as in a cloud, there is the risk of theft through hacking or viral attacks. In fact, there are many incidents where authentication forms are stolen. In September, 2016, there was an incident where a user accessed a weather information site and her PC was infected with a malicious code through the website. The public authentication form was leaked, leading to financial loss or loss of control over one's PC. If such authentication form theft occurs in a fast-moving vehicle, then this can generate high risk that may be fatal to the driver. For this reason, this paper suggests a method to issue safely an authentication form in the WAVE system.

This paper consists of the following: Chapter 2 describes WAVE which is related to the suggested method, and describes the international standards and authentication form issuance method. Chapter 3 describes the suggested method for authentication form. Chapter 4 describes the evaluation of the suggested method and Chapter 5 describes the conclusion.

2. Related Work

2.1. WAVE

WAVE is the IEEE technology standard of V2V/V2I networking for ITS services and public safety. When the WAVE standard first appeared, the existing vehicle communication environment used DSRC (Dedicated Short Range Communications) for offering transport information or for charging fees. However, needs to meet the ITS environment that changes in real-time emerged. This led to the existing Wi-Fi communication standard which was IEEE 802.11a to be the basis upon which the electronic wave environment of the road and vehicle was reflected. The IEEE 802.11p standard was set as WAVE. IEEE 802.11p, in order to simplify the process of joining, the step of the existing authentication of IEEE 802.11 or combination were omitted. This led to security issues. To address this, the IEEE 1609.2 standard which provides security services in the MAC upper hierarchy was combined. The current WAVE standard came into being. The structure is as seen in Figure 1.

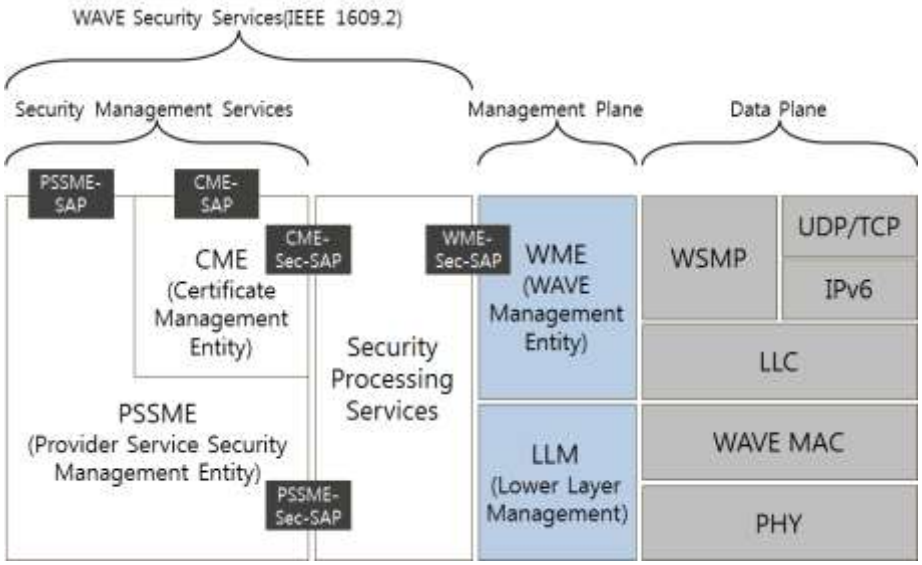

Figure 1. WAVE System

It can be categorized into three parts of WAVE Security Service, Data Plane, and Management Plane. In the WAVE Security Service, a service that can complement the

omitted authentication of IEEE 802.11p is offered, and the Management Plane either requests or advertises the services from RSU (Road-Side Unit) or OBU (On-Board Unit). Data Plane owns the Data Flow to receive or send practical data.

2.2. IEEE 1609.2

IEEE 1609.2 defines the vehicle communication encryption in the WAVE system. By encrypting the message, confidentiality is secured, authentication is offered to the user and it is used for broadcasting to anonymous users. The calculation for the encryption is summarized in Table 1.

Table 1. Wave Encryption

	Encryption	Calculation description
Encryption Calculation	ECDSA	Signature algorithms
	ECIES	Public key encryption algorithms
	AES-CCM	Symmetric algorithms
	SHA-256	Hash algorithms

ECDSA is an electronic signature algorithm that uses an oval shaped curve P-256 and P-24 defined in the NIST SEC2. It uses an open key and ECIES as the encryption algorithm. To generate an encrypted sentence, SHA-256 is used. For the value on the encrypted sentence, the tag value, encrypted sentence and open key value are delivered. Because of this not only is confidentiality secured, but integrity of the message is also delivered through the tag value. For the symmetrical encryption algorithm, AES-CCM is used but part of the parameter defined by NIST is limited. For the hash algorithm, SHA-256 is used as a random value when the pair of keys is generated in the ECDSA and ECIES, and for authentication.

2.3. CAMP VSC

CAMP (Crash Avoidance Metrics Partnership) emerged when the U.S. Department of Transportation and the NHTSA (National Highway Traffic Safety Administration) under it established a PKI-related standard and promoted a VII (Vehicle Infrastructure Integration) project. In the CAMP standard, authentication form is issued based on the ID issued by making a LA (Linkage Authority) in the traditional PKI structure. This makes it impossible to verify the generation information between the vehicle and the authentication form unless all the LA's or CA's (Certificate Authorities) that know the ID are hacked. The process in which the pseudonym authentication form of CAMP VSC3 is issued is as follows.

The issuance process has each step separated. This is because the valid period of the pseudonym authentication form is very short and when it is issued in the unit of month and year, it must be issued and transmitted in mass. Because of this, there could be various issues if it is issued in the method of synchronizing while maintaining the session. The general approach is to make an issuance request from the vehicle and sending regularly a transmission request.

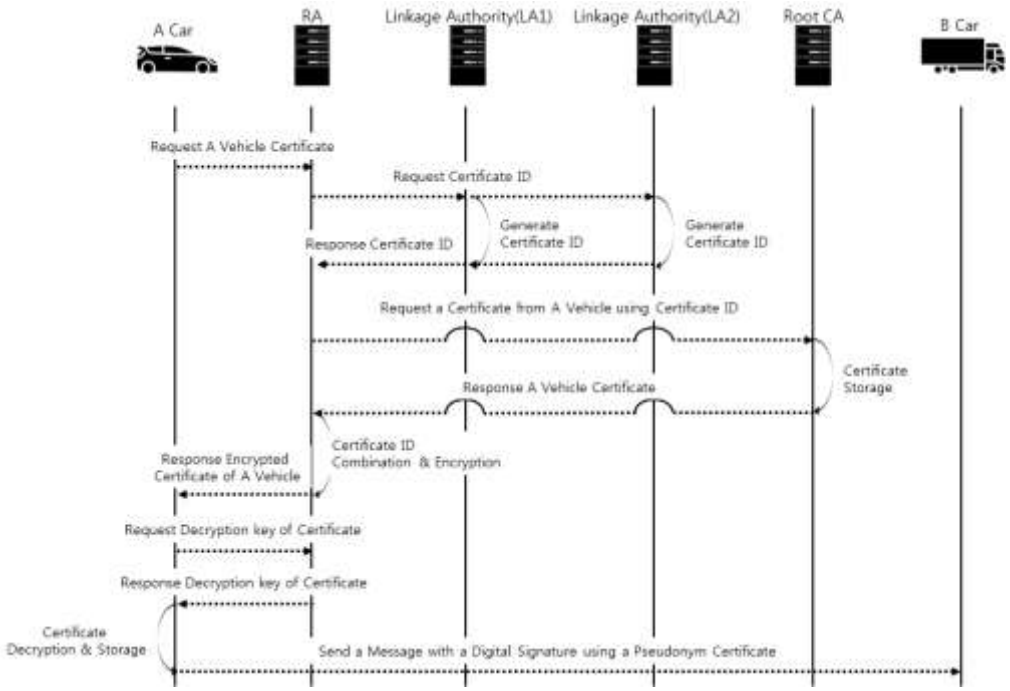

Figure 2. CAMP VSC3

2.4. C2C-CC

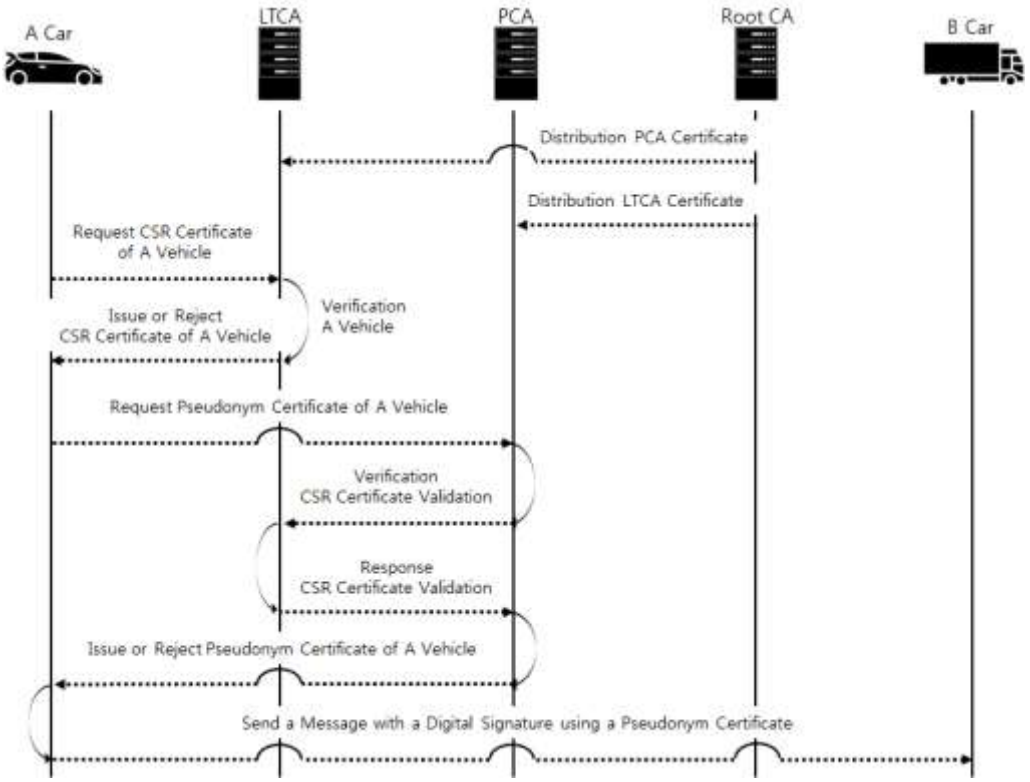

Figure 3. C2C-CC

One of the leading characteristics of the C2C-CC is that the agent that issues the authentication form is all different. The CSR authentication is issued by LTCA (Long Term CA), while the pseudonym authentication is issued by PCA (Pseudonym CA). To receive a pseudonym authentication, the vehicle makes a request to the PCA using the CSR authentication it had received from LTCA. PCA that receives this verifies the validity of the CSR authentication through LTCA. If the validity is verified, a pseudonym authentication is issued. In the CAMP-VSC3 method, an insider that can access the RA that issues the authentication cannot know the ID information that generates the CSR authentication or the pseudonym authentication, but in the C2C-CC method, an insider that can access the PCA that generates a pseudonym authentication can discover the ID of the CSR authentication and pseudonym authentication. This makes it extremely important to prevent the leakage through strict authority management, auditing and training.

3. Protocol Design

3.1. Proposed Vehicle Environment

The suggested protocol consists of the five units of LTCA (Long Term CA), PCA (Pseudonym CA), Root CA, RCA (Random CA), and the vehicle. LTCA issues the CSR authentication used to receive the pseudonym authentication by the vehicle. This becomes an authentication associated with the lifetime of the vehicle and has a long valid period.

PCA is an institution issuing pseudonyms. Once it has the validity of the pseudonym issuance verified by the LTCA, it generates a pseudonym for the vehicle's ID. The pseudonym may contain the open key, valid period and signature of PCA. If necessary, the vehicle's ID and related information may also be included to make it easier to track.

Root CA is the institution that issues the authentication of LTCA and PCA. To LTCA, it distributes the authentication of PCA, while to PCA it distributes the authentication of LTCA. In the suggested protocol, since there is an RCA that exists to generate a random ID, Root CA distribute the authentication of PCA to the RCA, too.

RCA generates the random ID using the vehicles ID sent by PCA so that the relation between the pseudonym and the vehicle ID cannot be traced.

In this paper, through the above four CA's, the messages are sent and received including the digital signature that uses a pseudonym in communication between vehicles to prevent any counterfeiting or theft of the message. A pseudonym authentication is used so that the relation between the vehicle ID and pseudonym cannot be traced and the privacy is protected.

The issue with the existing C2C-CC is that when PCA issues a pseudonym authentication, a pseudonym for the vehicle ID is generated and issued to the vehicle. At this time, the vehicle ID can be stored to track the vehicle's ID that uses the pseudonym. Because of this, there is the risk of the vehicle ID being stolen when an insider with PCA access or a malicious attacker accesses PCA. If the vehicle ID is stolen, the route of the vehicle can be tracked. To address this issue, the ID that can generate authentication using RCA is not made to be known to PCA. The steps of issuing a CSR authentication to receive a pseudonym authentication is as follows.

3.2. Proposed CSR Certificate Protocol

3.2.1. Distribution of Root CA authentication

step1) The authentication of PCA and the open key is distributed to LTCA after encryption.

$$E_{K_{LTCA-pub}}(CERT_{PCA}||PCA_{pub}) \quad (1)$$

step2) The authentication and open key of LTCA and RCA are distributed to PCA after encryption.

$$E_{K_{PCA-pub}}(CERT_{LTCA}||LTCA_{pub}||CERT_{RCA}||RCA_{pub}) \quad (2)$$

step3) The authentication and open key of PCA are distributed to RCA by encrypting them with the open key of LTCA.

$$E_{K_{RCA-pub}}(CERT_{PCA}||PCA_{pub}) \quad (3)$$

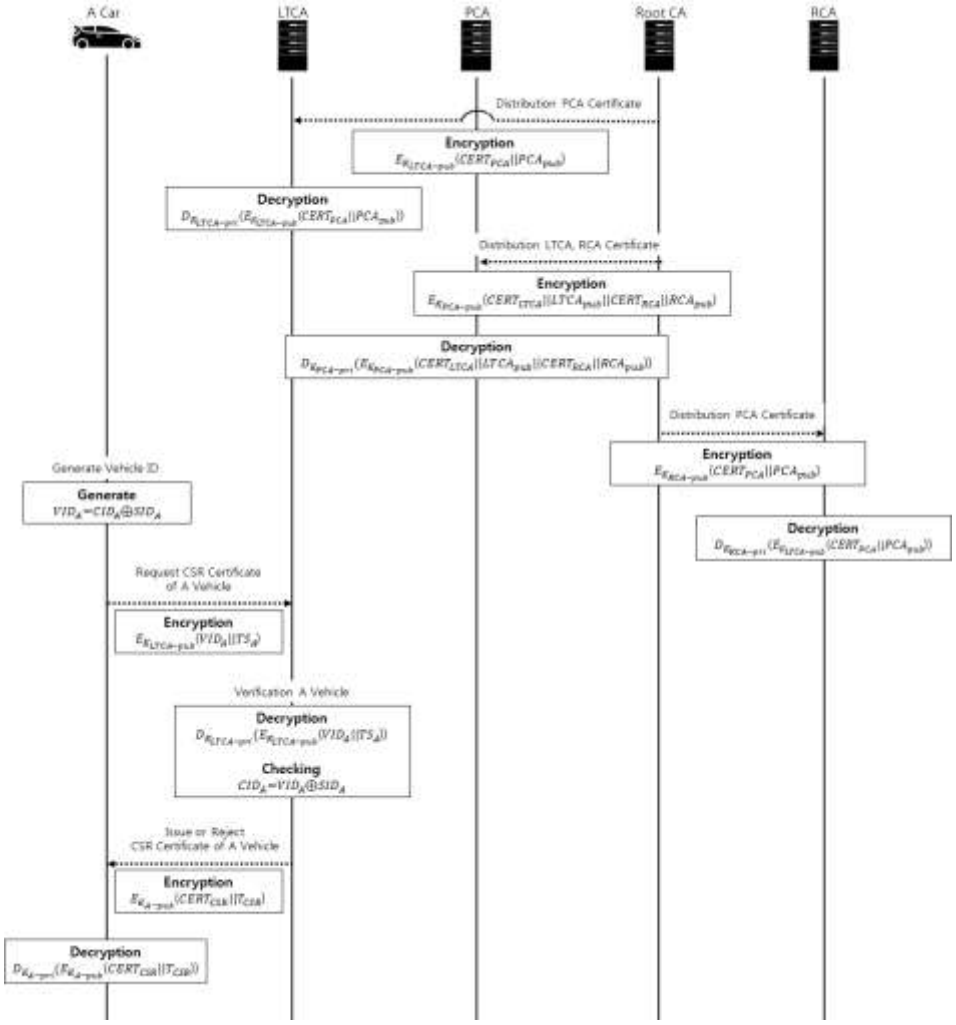

Figure 4. CSR Certificate Protocol

3.2.2. Issuance of CSR Authentication for LTCA

step1) A vehicle requests CSR authentication to LTCA. In this step, the vehicle calculates the CID (vehicle ID) and SID (service ID) with XOR to generate VID.

$$VID_A = CID_A \oplus SID_A \quad (4)$$

$$E_{K_{LTCA-pub}}(VID_A||TS_A) \quad (5)$$

step2) It verifies that it is A vehicle through VID acquired by decryption.

$$D_{K_{LTCA-pri}}(E_{K_{LTCA-pub}}(VID_A||TS_A)) \quad (6)$$

$$CID_A = VID_A \oplus SID_A \quad (7)$$

step3) CSR authentication is issued to vehicle A. A vehicle decrypts this and stores the authentication.

$$E_{K_{A-pub}}(CERT_{CSR}||T_{CSR}) \quad (8)$$

$$D_{K_{A-pri}}(E_{K_{A-pub}}(CERT_{CSR}||T_{CSR})) \quad (9)$$

3.3. Proposed Pseudonym Certificate Protocol

3.3.1. Issuance of the Pseudonym Authentication of PCA

step1) Vehicle A requests to PCA using CSR authentication that a pseudonym authentication be issued.

$$E_{K_{LTCA\_pub}}(T_{CSR}||TS_A) \quad (10)$$

$$E_{K_{PCA-pub}}(TS_A||VID_A||CERT_{CSR}) \quad (11)$$

step2) PCA requests to LTCA that the validity of CSR authentication be tested.

$$E_{K_{LTCA-pub}}(T_{CSR}||TS_A) \quad (12)$$

step3) LTCA tests the validity of CSR authentication that it acquired through decryption and responds.

$$D_{K_{LTCA-pri}}(E_{K_{LTCA-pub}}(T_{CSR}||TS_A)) \quad (13)$$

$$T_{CSR} \geq TS_A \quad (14)$$

3.3.2. Request for a Pseudonym ID for the Issuance of a Pseudonym Authentication for PCA

step1) PCA requests to RCA an RID to generate a pseudonym authentication for the vehicle.

$$E_{K_{RCA-pub}}(Info||CERT_{PCA}||VID_A) \quad (15)$$

step2) PCA combines the RID's issued by RCA to generate a pseudonym authentication. The generated pseudonym authentication is issued to the vehicle.

$$D_{K_{RCA-pri}}(E_{K_{RCA-pub}}(Info||CERT_{PCA}||VID_A)) \quad (16)$$

$$\mathrm{A} = N_1 \oplus VID_A \quad (17)$$

$$\mathrm{B} = N_2 \oplus VID_A \quad (18)$$

$$RID_1 = g^A \bmod \mathrm{q} \quad (19)$$

$$RID_2 = g^B \bmod \mathrm{q} \quad (20)$$

$$E_{K_{RCA-pub}}(Info||CERT_{PCA}||VID_A) \quad (21)$$

step3) PCA combines the RID's issued by RCA to generate a pseudonym authentication. The generated pseudonym authentication is issued to the vehicle.

$$D_{K_{PCA-pri}}(E_{K_{RCA-pub}}(Info||CERT_{PCA}||VID_A)) \quad (22)$$

$$RID_A = RID_1 \oplus RID_2 \quad (23)$$

$$E_{K_{A-pub}}(CERT_{RID}||PCA_{pub}||T_{CERT}) \quad (24)$$

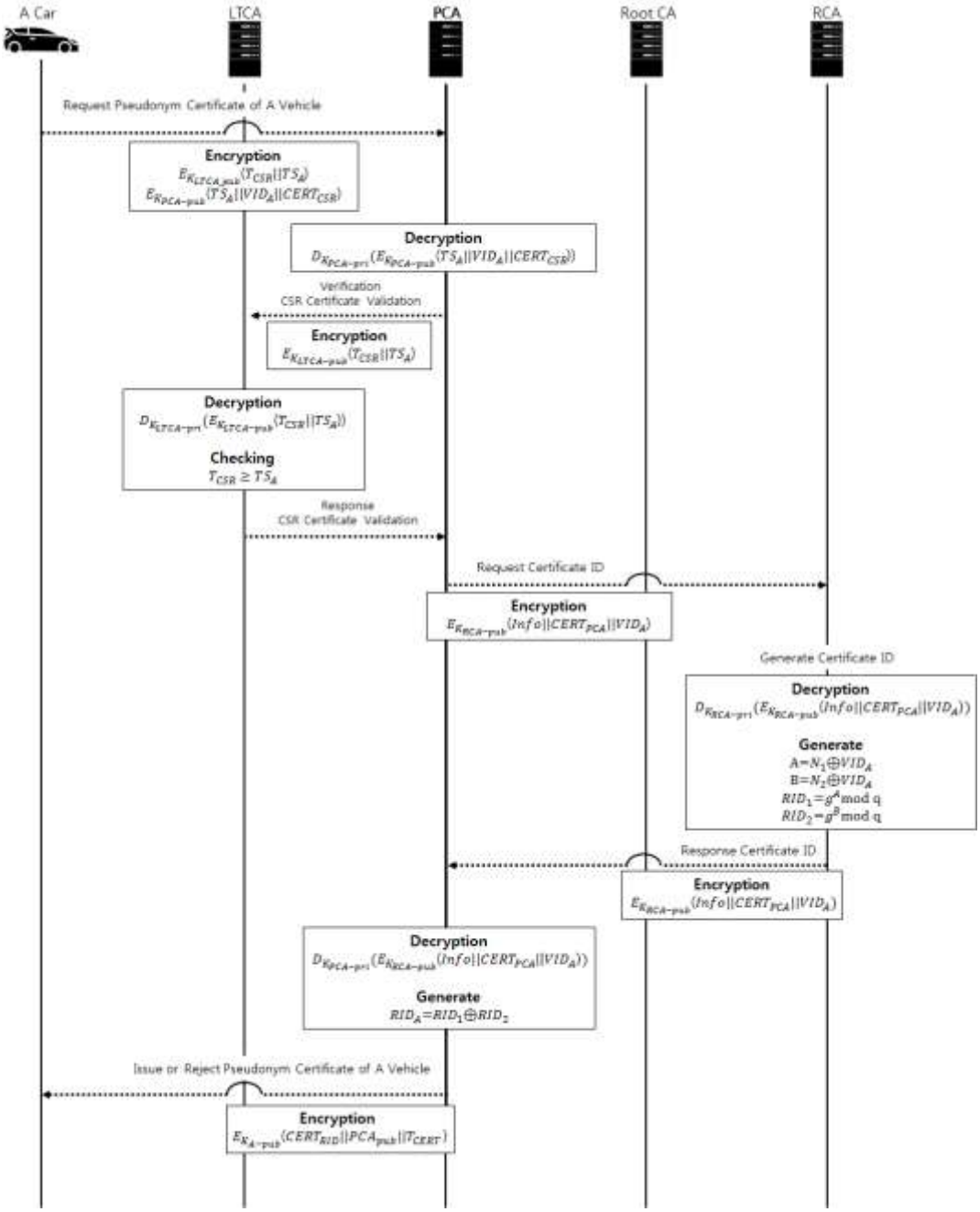

Figure 5. Pseudonym Certificate Protocol

3.4. Proposed Pseudonym Certificate Protocol

3.4.1. Issuance of the Pseudonym Authentication of PCA

step1) Vehicle A sends the message including the issued pseudonym authentication to vehicle B.

$$M(Info||CERT_{RID}||PCA_{pub}||T_{CERT}||TS_A \quad (25)$$

step2) Vehicle B verifies the valid period of the pseudonym authentication and verifies the pseudonym authentication of the authentication using the open key of PCA. If the valid period has expired, the message is discarded immediately.

$$T_{CERT} \geq TS_A \tag{26}$$

$$D_{K_{RCA-pub}}(CERT_{RID}) \tag{27}$$

step3) If there are no issues after verification, the information is received.

$$Info \tag{28}$$

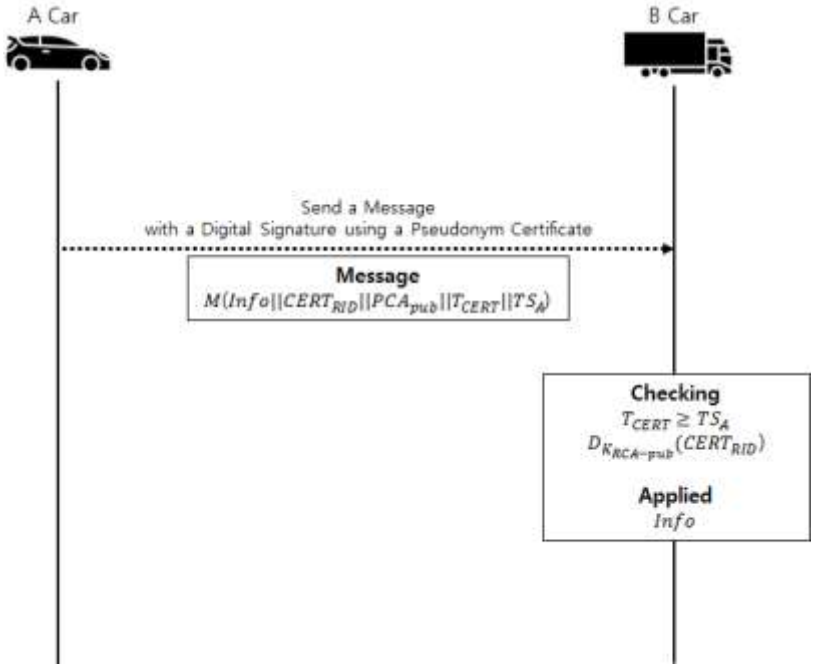

Figure 6. V2V Communicate Protocol

4. Performance Analysis

4.1. Safety Analysis

4.1.1. Authentication and Data Integrity

As smart cars progress and become widely used in the vehicle environment, a security threat emerges to authentication and data integrity. This paper suggests a method through which the $CERT_{RID}$ value is verified using the ECC signature technology to identify the agent of the message sender. Moreover, by controlling the access of unauthorized vehicles, data integrity is strengthened.

4.1.2. Threat to Confidentiality

In the vehicle communication environment, there are frequent cases where the confidentiality is threatened when an unauthorized user eavesdrops on a message. To prevent this from happening, the suggested protocol verifies the T_{Cert} value that checks the validity period when a vehicle message is received. By verifying the value of the digital signature given to only member users, unnecessary messages are rejected.

4.1.3. Threat to Privacy

Messages generated in the vehicle communication environment includes important information on the user and thus must be protected. By applying the VID_A value

generated during CSR authentication ($CERT_{PCA}$) and pseudonym authentication steps, messages and information in them cannot be tracked. Privacy is thus protected.

4.1.4. Non-repudiation

Non-repudiation that occurs in a vehicle environment is an attack related to digital signatures. It manipulates the relationship between the pseudonym authentication and CSR authentication. In the suggested protocol, the pseudonym ID is generated through RCA, and thus the relation between the CSR authentication and the pseudonym authentication cannot be tracked. This prevents non-repudiation.

4.1.5. Availability

In vehicle communication, there can be a DoS attack that threatens the usability by making it impossible to send or receive normal messages by controlling the communication channel. To prevent this, T_{CERT} that is a value with the valid period of the authentication applied is generated when authentication is generated. T_{CERT} is used in the communication protocol for a safe communication.

4.2 Efficiency Analysis

To evaluate the function of the suggested protocol, in the Intel ® Core™2 Quad CPU Q940 @ 2.66GHz, 2.67GHZ, RAM 4.00GB, 64bit Windows 7 Enterprise k environment, Eclipse Java Cryptography was used to analyze the efficiency of the communication protocol and signature value. Encryption, decryption, key generation, authentication generation and the overall communication process were analyzed in the suggested system and the existing system. In the signature value analysis, the suggested ECDSA signature method was compared with WPA and PKI which are used in the existing system.

Table 2. Process Comparison of Exist System and Proposed System

	Exist System	Proposed System
Issuance Process of Certification	6Encryption+6Decryption+2Hash	5Encryption+5Decryption
Temporary Issuance Process of Certification	6Encryption+5Decryption	5Encryption+ 4Decryption
Message of Communication Process	1Encryption+1Decryption +1Signature	1Siganture

In Table 2, the authentication issuance, pseudonym issuance and message communication process of the existing and suggested systems are shown. In the existing system, PCA took charge of the process of generating a pseudonym authentication by using the hash algorithm, but in the suggested system the pseudonym authentication ID is generated through RCA, and thus address the internal vulnerability of issuing pseudonym authentication. Figure 7. Shows the evaluation results of the existing and suggested systems.

In the suggested system, approximately 18% for the authentication issuance, about 20% for the pseudonym authentication issuance process, and about 68% for the communication protocol since it only verifies the signature value were found. Table 3 and Figure 8 analyzed the efficiency of encryption, decryption and key generation signature method of the suggested signature method (ECDSA) and the existing signature method (PKI, WPA).

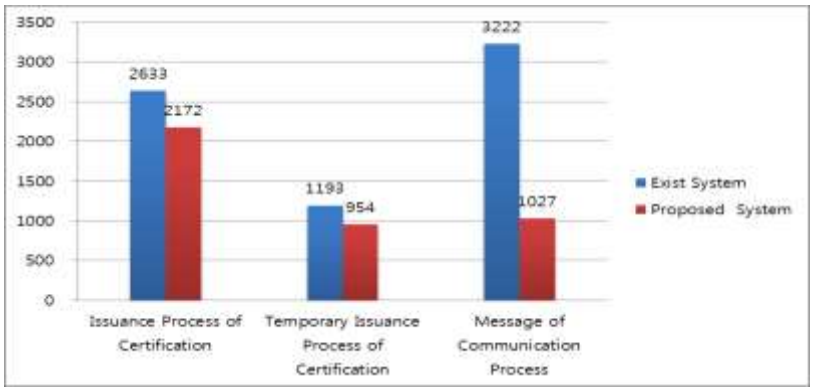

Figure 7. Exist System and Proposed System (Speed: Millisecond)

Table 3. Comparison Analysis of Proposed Algorithm Performance (Time – nanosecond)

	PKI	WPA	ECDSA
Encryption	1836531	2008064	1194910
Decryption	14531487	3857065	2492219
Key Pair Generation	2238248754	143043185	92066332
Total	2254616772	148908314	95753461

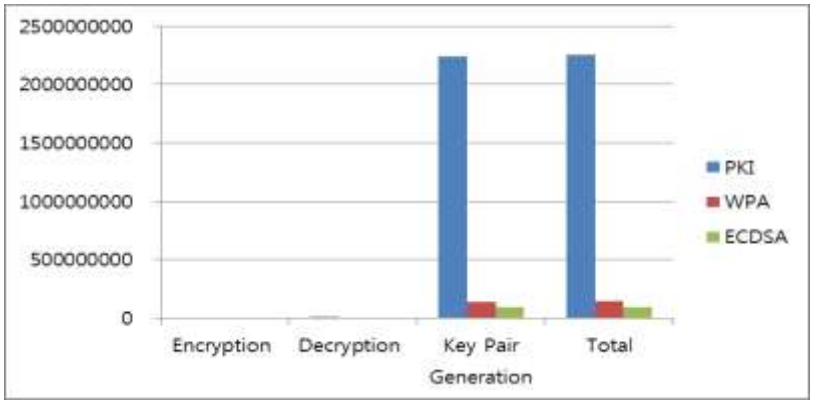

Figure 8. Efficiency Analysis of Proposed Signature Algorithm and Exist Signature Method (Speed: Nanosecond)

5. Conclusion

In an authentication-based vehicle communication environment, measures must be taken so that an unauthorized user cannot find out the location information of the vehicle through the vehicle ID or track the route of the car. If the location information of the vehicle that is moving at a high speed is stolen by a malicious attacker, then there can be a situation that is fatal to the driver. In order to prevent the tracking of the vehicle's location or route through vehicle ID and to address the internal vulnerabilities of the existing system, this paper presents a method that generates and issues a pseudonym ID issued by RCA during the vehicle communication process.

Acknowledgements

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF2016R1D1A1A09917662).

References

[1] S. S. Park and K. Kim, "A Study on Minimalize V2V Communication Authentication Procedure for Enhancing Privacy", Korea Institute of Communication Sciences, **(2016)**, pp. 117-118.
[2] L. Y. Sik, S. S. Gyoo and K. D. Soo, "A Study on Security technology for V2X communication", Korea Institute of Information Security and Cryptology, **(2014)**, pp. 28-34.
[3] H. An, S. Kang, M. Kim and J. Jung, "A Study on the IEEE WAVE 1609.2 ECDSA Performance based on Open Source", Korea Institute of Communication Sciences, **(2015)**, pp. 856-857.
[4] K. Bumryong, C. Keunchang, K. Joonho and S. Sangkee, "A Design of Inter-Working System between Secure Coding Tools and Web Shell Detection Tools for Secure Web Server Environments", Journal of the Korea Society of Digital Industry and Information Management, vol. 11, no. 4, **(2015)**, pp. 81-87.
[5] K. J. Gu, "Automatic Guided Vehicle Design and Implementation for Intelligent Unmanned Mobile systems", Journal of the Korea Society of Digital Industry and Information Management, vol. 10, no. 1, **(2014)**, pp. 73-79.
[6] J. C. Ryong, L. Y. Kwon and L. D. Sik, "The Design and Implementation of a Multi-Session Processing Between RMA and RCP within a Vehicle Tracking System", Journal of the Korea Society of Digital Industry and Information Management, vol. 10, no. 3, **(2014)** pp. 127-141
[7] S. J. Ho, C. D. Hyun and P. J. Oh, "A Design of Interdependent Multi Session Authentication Scheme for Secure Cloud Service", Journal of the Korea Society of Digital Industry and Information Management, vol. 10, no.3, **(2014)**, pp.181-196
[8] Y. Hwanseok, "A Study on Location-based Routing Technique for Improving the Performance of P2P in MANET", Journal of the Korea Society of Digital Industry and Information Management, vol. 11, no. 2, **(2015)**, pp. 37-45

Authors

Taekjung Kim, received his B.S. degree in Multimedia Science from Chungwoon University, Incheon, Korea in 2016. He is currently a M.Eng. course in the Computer Science, Soongsil University. His research interests include Intelligent Transport Systems, Information Security Management System, Authentication System, and Network Security.

Byungwook Jin, received his B.S. degree in Multimedia Science from ChungWoon University, Chungnam, Korea in 2011, and M.S. degree in Computer Science from Soongsil University, Seoul, Korea, in 2013. He is currently a Ph.D. course in the Computer Science, Soongsil University. His research interests include Internet of Thing, Authentication System, and Network Security.

Si Ho Cha, is a professor in the Department of Multimedia Science, Chungwoon University, Incheon, Korea. He received his Ph.D. degree in Computer Science from Kwangwoon University, Seoul, Korea in 2004. From 1997 to 2000, he worked as a senior researcher at Daewoo Telecom R&D Center, Korea. His research interests include network management, wireless sensor networks, vehicular ad hoc networks, semantic web, and web of things.

Moon Seog Jun, Ph.D. degrees in Computer Science from Maryland University, United State pf America, in 1989. He is currently a Professor in Soongsil University, Seoul, Korea. His research interests include Information Protect, Authentication System, and Cryptography.