International Journal of Engineering & Technology, 8 (1.4) (2019) 308-315

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

A Design of Safe Communication Protocol for Secure Service Provision in Vehicular Communication Environments

Byung-Wook Jin[1], Si-Ho Cha[2]*

[1]Korea Intellectual property Protection Agency (KOIPA),
131 Tehran-ro, Kangnam-gu, Seoul, South Korea
[2]Dept. of Multimedia Science, Chungwoon University,
113, Sukgol-ro, Michuhol-gu, Incheon, 402-803, South Korea
**Corresponding author E-mail: shcha@chungwoon.ac.kr*

Abstract

Vehicular communication technology is being developed as an intelligent transportation system, and studies are being actively carried out to enhance the safety of vehicle driving and provide services with high efficiency in communication. Vehicular communication technology is evolving rapidly in order to realize fully autonomous vehicles, with the development of information technology (IT) and active technological development in national, enterprise and research institutes. However, the convergence with IT has created a vulnerability to cyber-attacks that occur between the vehicle and the transportation infrastructure, and therefore, research on security technology is required. The study designed a protocol to provide efficient and secure services in the vehicular communication environments. The security of the attack techniques occurring in the existing vehicular communication environment was analyzed and it was confirmed there was efficiency of 49% in the verification process compared to the protocol used in the communication environment and 71% in the verification process.

Keywords: *Vehicular Communication, Safe Communication Protocol, Autonomous Vehicle, Cyber-attacks, Secure Service*

1. Introduction

Vehicular communication environments use the communication technology that combines vehicles technologies and wireless communication networks. It provides various services such as ITS (Intelligent Transport Systems) and telematics to enhance convenience and efficiency. In addition, investment in research and technology development of autonomous vehicles is increasing both domestically and abroad. Autonomous vehicles are based on radar, GPS, vehicle and vehicle, and communication technology between the vehicle and the road base, which recognize the surrounding information of the vehicle, and standardization of vehicular communication technology is underway [1][3].

However, various security vulnerabilities in vehicular communication technology need to be addressed. Security threats in the vehicular communication environment can threaten not only physical damage but also the life of the driver, and research on the security framework is required. There are various vulnerabilities and threats such as privacy violation, lack of certificate for vehicle, and hacking threat against vehicle environment infrastructure [2-4].

Therefore, in this paper, a secure communication protocol was designed to provide efficient services in the vehicular communication environment. In order to perform the performance evaluation of the proposed protocol, the security of the attack method occurring in the existing vehicle environment was analyzed and compared the effectiveness of the signature value issuance and verification.

The composition of this study is as follows. Section 2 deals with vehicular communication technology trends, threats to the vehicular communication environment, and security threats in related research. Section 3 outlines the designed vehicle registration, communication protocol, and vehicle update and revocation protocol. Section 4 performs safety analysis and security evaluation by performance analysis. Section 5 describes future research and concludes the paper.

2. Related Works

2.1. Trend of Vehicular Communication Technology

The service types of vehicular communication technology can be divided into 4 types, vehicle to vehicle (V2V) warning propagation service, V2V group communication service, V2V security service, and vehicle to infrastructure (V2I) warning service [3].

V2V warning propagation service is a service that sends a warning message to a specific vehicle or group of vehicles for safe driving. This is, for example, a service for allowing an emergency vehicle to proceed by transmitting a message so that the emergency vehicle can pass through [2-6].

V2V group communication service is a service that can perform communication between vehicles included in each group. It is a service provided from a vehicle that runs in a specific area and is mainly used to notify specific information to all groups [7].

V2V security service is a service used by the vehicle to increase the safety of the vehicle by periodically managing the specification of the speed, direction, and breaks and providing information on the criticality [2][8].

V2I warning service is a service that sends warning messages or accident risk messages to various infrastructures around the road rather than vehicles for the danger of driving among vehicles [3][9-10].

2.2. Threats and Security Requirements in Vehicular Communication Environments

Vehicle to everything (V2X) communication is a technology that can increase the safety of autonomous vehicles by exchanging information about traffic, vehicles, roads, and pedestrians conditions through V2V and V2I communication through wireless networks. V2V warning propagation service is a service that sends a warning message to a specific vehicle or group of vehicles for safety [3][5]

In 2015, integrated security technologies for autonomous vehicles are being actively researched at public institutions, corporations and educational institutions on V2X vehicle security services. It guarantees the reliability of the service of vehicular communication technology and there are studies to prevent user privacy threats. Security threats and vulnerabilities in the vehicular communication environment are shown in Figure 1 [4].

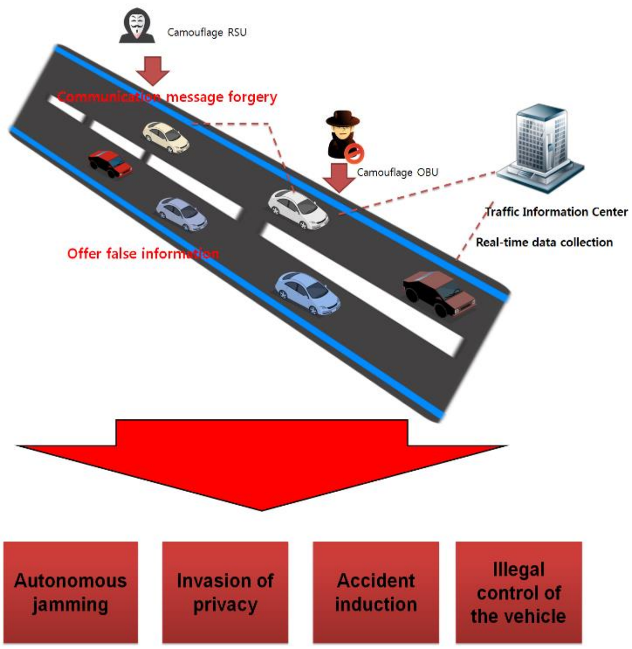
Camouflage RSU
Communication message forgery
Camouflage OBU
Traffic Information Center
Real-time data collection
Offer false information
Autonomous jamming
Invasion of privacy
Accident induction
Illegal control of the vehicle

Fig. 1: Threats of Vehicle Communication Environment

The threats and security requirements in vehicular communication environment are as follows.

Vehicle and Road Side Unit (RSU) Certification: Identify the identity of the communication entity and the proper owner of the communication entity, and perform entity authentication. When the owner of the vehicle carries out communication, it should identify the current member and verify the integrity of the message [2][5].

Message Integrity: Messages sent and received between vehicles should not be forged or tampered with [4][7].

Confidentiality: Messages between communication entities must be protected against unauthorized users and attackers [6].

Privacy Protection of User Information: The owner of the vehicle must protect the identification value from other vehicles (driver identification number, drive number, chassis number, etc.). If protection is not provided, it can be easily tracked and the reliability of the message may be lost. Therefore, the information about the message users who have the vehicle should be protected, and the security of hacking and leakage should be strengthened.

3. Design of Proposed Protocol

3.1. Configuration

This section describes the communication configuration for the proposed communication protocol. Figure 2 shows the overall communication procedure for vehicle, Service Provider, Traffic Management Center, and RSU.

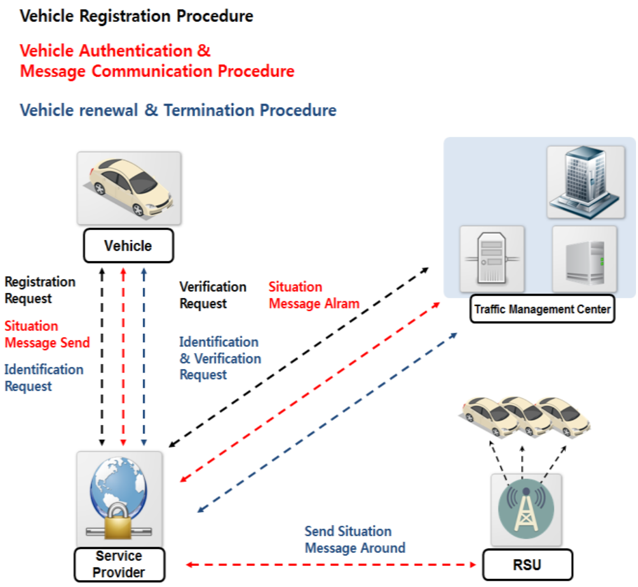
Vehicle Registration Procedure
Vehicle Authentication & Message Communication Procedure
Vehicle renewal & Termination Procedure
Vehicle
Registration Request
Situation Message Send
Identification Request
Verification Request
Situation Message Alram
Identification & Verification Request
Traffic Management Center
Service Provider
Send Situation Message Around
RSU

Fig. 2: Proposed communication protocol procedure

The abbreviations used in the vehicle registration procedure, vehicle certification and message communication procedure, and vehicle update communication procedure of the proposed vehicular communication environment are shown in Table 1.

Table 1: Abbreviation

Abbreviation	**Description**
USER_{PWD}	Password of User
$\text{Nonce}_{\text{Vehicle}}$	Random numbers generated by the vehicle
Nonce_{SP}	Random numbers generated by Service Provider
$\text{USER}_{\text{LicenseNumber}}$	License Number of User
$\text{SP}_{\text{Inherence-Code}}$	Inherence Code of Service Provider
TIMESTAMP	Time Stamp
$\text{E}_{\text{PUB-X}}$	Public Key Encryption of X
$\text{E}_{\text{PRI-X}}$	Private Key Encryption of X

3.2. Vehicle Registration Procedure

This section describes the procedures for vehicle identification and verification to perform vehicle registration in the vehicular communication environment. The parameters generated during the vehicle registration process are USER_{PWD}, $\text{Nonce}_{\text{Vehicle}}$, and Nonce_{SP}. The exchange parameters are $\text{USER}_{\text{LICENSE-NUMBER}}$, $\text{Vehicle}_{\text{Code}}$, and $\text{SP}_{\text{Inherence-Code}}$. The detailed procedure of the identification and parameter exchange of the vehicle registration procedure is shown in Figure 3.

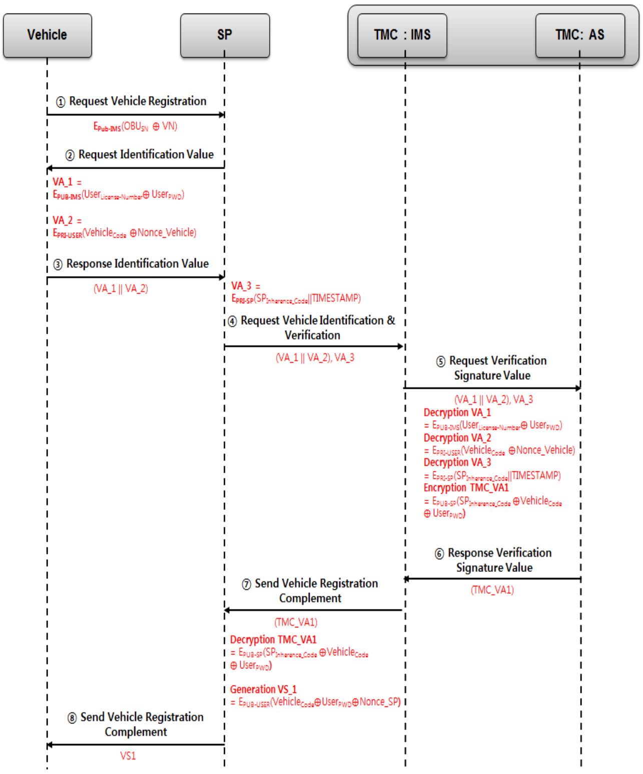
Vehicle
SP
TMC : IMS
TMC: AS
① Request Vehicle Registration
E_Pub-IMS(OBU_SN ⊕ VN)
② Request Identification Value
VA_1 = E_PUB-IMS(User_License-Number⊕ User_PWD)
VA_2 = E_PRI-USER(Vehicle_Code ⊕Nonce_Vehicle)
③ Response Identification Value
(VA_1 || VA_2)
VA_3 = E_PRI-SP(SP_Inherence_Code||TIMESTAMP)
④ Request Vehicle Identification & Verification
(VA_1 || VA_2), VA_3
⑤ Request Verification Signature Value
(VA_1 || VA_2), VA_3
Decryption VA_1 = E_PUB-IMS(User_License-Number⊕ User_PWD)
Decryption VA_2 = E_PRI-USER(Vehicle_Code ⊕Nonce_Vehicle)
Decryption VA_3 = E_PRI-SP(SP_Inherence_Code||TIMESTAMP)
Encryption TMC_VA1 = E_PUB-SP(SP_Inherence_Code ⊕Vehicle_Code ⊕ User_PWD)
⑥ Response Verification Signature Value
(TMC_VA1)
⑦ Send Vehicle Registration Complement
(TMC_VA1)
Decryption TMC_VA1 = E_PUB-SP(SP_Inherence_Code ⊕Vehicle_Code ⊕ User_PWD)
Generation VS_1 = E_PUB-USER(Vehicle_Code⊕User_PWD⊕Nonce_SP)
⑧ Send Vehicle Registration Complement
VS1

Fig. 3: Vehicle Registration Procedure

1. The vehicle transmits a vehicle registration request message from the Service Provider.

$E_{Pub\text{-}IMS}(OBU \oplus VN)$

2. Upon receiving the message, the Service Provider requests an identification value from the vehicle. The vehicle generates VA_1, VA_2 after receiving the message.

$VA\_1 = E_{Pub\text{-}IMS}(USER_{License\text{-}Number} \oplus USER_{PWD})$
$VA\_2 = E_{Pub\text{-}USER}(Vehicle_{Code} \oplus Nonce_{Vehicle})$

3. The vehicle transmits VA_1 and VA_2 from the Service Provider. Service Provider creates VA_3.

$VA\_3 = E_{PRI\text{-}SP}(SP_{Inherence\text{-}Code} \parallel TIMESTAMP)$

4. The Service Provider requests from the TMC: IMS for vehicle identification and verification by attaching the messages VA_1, VA_2, and VA_3.

5. After receiving the message, TMC: IMS requests verification of the message about the signature value with TMC: AS. Then, the VA_1, VA_2, and VA_3 messages are decrypted.

$VA\_1 = D_{Pub\text{-}IMS}(USER_{License\text{-}Number} \oplus USER_{PWD})$
$VA\_2 = D_{Pub\text{-}USER}(Vehicle_{Code} \oplus Nonce_{Vehicle})$
$VA\_3 = D_{PRI\text{-}SP}(SP_{Inherence\text{-}Code} \parallel TIMESTAMP)$

6. After that, the TMC: AS transmits a message from TMC_IMS after performing encryption of the message for TMC_VA1.

$TMC\_VA1 = E_{PUB\text{-}SP}(SP_{Inerrence\text{-}Code} \oplus Vehicle_{Code} \oplus USER_{PWD})$

7. TMC: IMS sends the vehicle registration completion message to the Service Provider. Then, after receiving the message, VS_1 is generated.

$TMC\_VA1 = D_{PUB\text{-}SP}(SP_{Inherence\text{-}Code} \oplus Vehicle_{Code} \oplus USER_{PWD})$
$VS\_1 = E_{PUB\text{-}USER}(Vehicle_{Code} \oplus USER_{PWD} \oplus Nonce\_SP)$

8. The Service Provider sends a vehicle registration completion message from the vehicle.

3.2. Vehicle Authentication and Message Communication Procedures

This section describes vehicle certification and message communication procedures in the vehicular communication environments. The parameter generated in the vehicle authentication and message communication procedure is Message, and the exchange parameters are

$\text{USER}_{\text{License-Number}}$, USER_{PWD}. The detailed procedure of the vehicle authentication and message communication procedure is shown in [Figure 4].

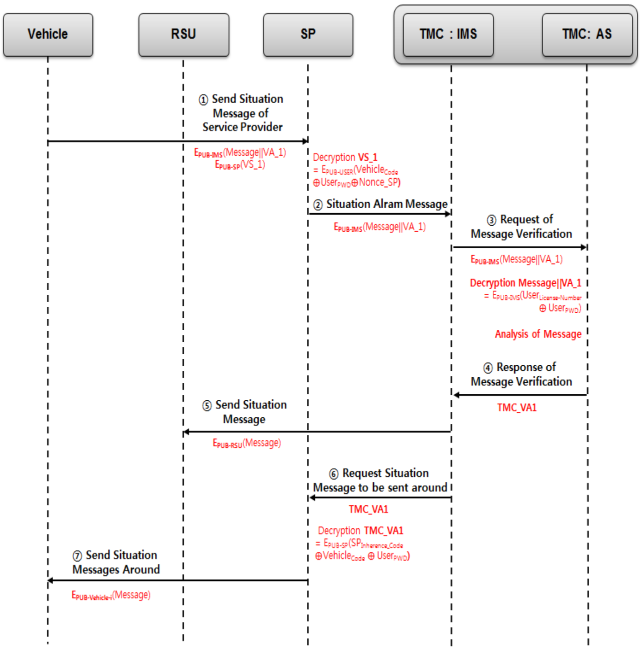
Vehicle
RSU
SP
TMC : IMS
TMC: AS
① Send Situation Message of Service Provider
E_PUB-IMS(Message||VA_1)
E_PUB-SP(VS_1)
Decryption VS_1 = E_PUB-USER(Vehicle_Code ⊕User_PWD⊕Nonce_SP)
② Situation Alram Message
E_PUB-IMS(Message||VA_1)
③ Request of Message Verification
E_PUB-IMS(Message||VA_1)
Decryption Message||VA_1 = E_PUB-IMS(User_License-Number ⊕ User_PWD)
Analysis of Message
④ Response of Message Verification
TMC_VA1
⑤ Send Situation Message
E_PUB-RSU(Message)
⑥ Request Situation Message to be sent around
TMC_VA1
Decryption TMC_VA1 = E_PUB-SP(SP_Inherence_Code ⊕Vehicle_Code ⊕ User_PWD)
⑦ Send Situation Messages Around
E_PUB-Vehicle-i(Message)

Fig. 4: Vehicle Authentication and Message Communication procedure

1. The vehicle sends a message about the current road situation to the Service Provider.

$\text{E}_{\text{PUB-IMS}}(\text{Message} \parallel \text{VA\_1})\ \text{E}_{\text{PUB-SP}}(\text{VS-1})$

2. The Service Provider decrypts the received message VS_1 and then sends a status message from the TMC: IMS.

$\text{VS\_1} = \text{D}_{\text{PUB-USER}}(\text{Vehicle}_{\text{CODE}} \oplus \text{USER}_{\text{PWD}} \oplus \text{Nonce\_SP})$
$\text{D}_{\text{PUB-IMS}}(\text{Message}\|\text{VA\_1})$

3. TMC: IMS requests message verification from TMC: AS, then decodes the received message.

$\text{D}_{\text{PUB-IMS}}(\text{Message}\|\text{VA\_1})$

4. After analyzing the status message, the TMC: AS sends a message verification response message from the TMC: IMS.

5. TMC: IMS encrypts the message with the public key from the RSU in the vicinity.

6. It then asks the Service Provider to send a status message to the nearby vehicle by attaching TMC_VA1. The Service Provider then decrypts the received message.

$\text{TMC\_VA1} = \text{D}_{\text{PUB-SP}}(\text{SP}_{\text{Inherence-Code}} \oplus \text{Vehicle}_{\text{Code}} \oplus \text{USER}_{\text{PWD}})$

7. The Service Provider transmits the status message from the neighboring vehicle after performing the encryption with the public key.

3.4. Vehicle Renewal and Termination Procedures

This section describes the vehicle renewal and cancellation procedures in the vehicular communication environment. The parameters generated in the vehicle renewal and cancellation procedure are R_VA1, R_VA2, R_TMC_VA1, and the exchange parameters are VA_1, VA_2, and VA_3. The details of the vehicle renewal and cancellation procedure are shown in Figure 5.

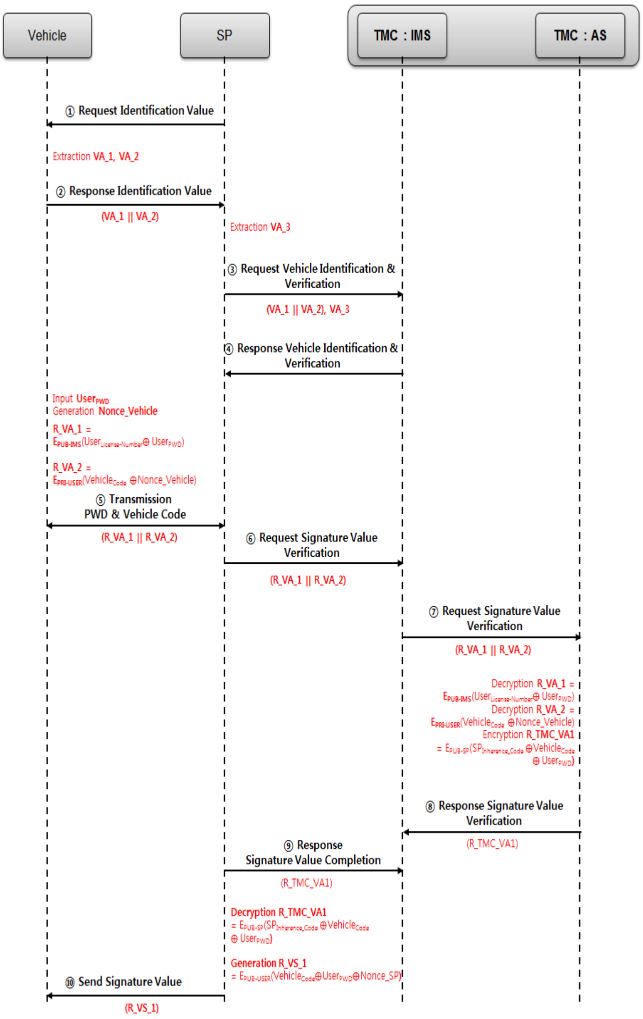
Vehicle
SP
TMC : IMS
TMC : AS
① Request Identification Value
Extraction VA_1, VA_2
② Response Identification Value
(VA_1 || VA_2)
Extraction VA_3
③ Request Vehicle Identification & Verification
(VA_1 || VA_2), VA_3
④ Response Vehicle Identification & Verification
Input User_PWD
Generation Nonce_Vehicle
R_VA_1 = E_PUB-IMS(User_License-Number⊕ User_PWD)
R_VA_2 = E_PRI-USER(Vehicle_Code ⊕Nonce_Vehicle)
⑤ Transmission PWD & Vehicle Code
(R_VA_1 || R_VA_2)
⑥ Request Signature Value Verification
(R_VA_1 || R_VA_2)
⑦ Request Signature Value Verification
(R_VA_1 || R_VA_2)
Decryption R_VA_1 = E_PUB-IMS(User_License-Number⊕ User_PWD)
Decryption R_VA_2 = E_PRI-USER(Vehicle_Code ⊕Nonce_Vehicle)
Encryption R_TMC_VA1 = E_PUB-SP(SP_Inherence_Code ⊕Vehicle_Code ⊕ User_PWD)
⑧ Response Signature Value Verification
(R_TMC_VA1)
⑨ Response Signature Value Completion
(R_TMC_VA1)
Decryption R_TMC_VA1 = E_PUB-SP(SP_Inherence_Code ⊕Vehicle_Code ⊕ User_PWD)
Generation R_VS_1 = E_PUB-USER(Vehicle_Code⊕User_PWD⊕Nonce_SP)
⑩ Send Signature Value
(R_VS_1)

Fig. 5: Vehicle Renewal and Cancellation procedure

1. The Service Provider sends an identification value request message from the vehicle. The vehicle extracts the parameters VA_1 and VA_2.

2. The vehicle extracts the VA_1 and VA_2 parameters from the Service Provider and sends the identification value response message.

3. The Service Provider sends a vehicle identification and verification request message from TMC: IMS including VA_1, VA_2, and VA_3.

4. TMC: IMC receives the message, decrypts it, and sends the identification and verification response message to the Service Provider for vehicle update.

5. The Service Provider receives a request message for the password and the vehicle code from the vehicle after the request.

$R\_VA\_1 = E_{PUB\text{-}IMS}(USER_{License\text{-}Number} \oplus USER_{PWD})$
$R\_VA\_2 = E_{PUB\text{-}USER}(Vehicle_{Code} \oplus Nonce_{Vehicle})$

6. The Service Provider transmits a request message for signature value verification to the TMC: IMS including the parameters R_VA_1 and R_VA_2.

7. TMC: IMS sends a signature value verification request message to TMC: AS. And decodes the received message and generates it for R_TMC_VA1.

$R\_VA\_1 = D_{PUB\text{-}IMS}(USER_{License\text{-}Number} \oplus USER_{PWD})$
$R\_VA\_2 = D_{PUB\text{-}USER}(Vehicle_{Code} \oplus Nonce_{Vehicle})$
$R\_TMC\_VA\_1 =$
$E_{PUB\text{-}SP}(SP_{Inherence\text{-}Code} \oplus Vehicle_{Code} \oplus USER_{PWD})$

8. TMC: AS sends a response message with R-TMC-VA1 attached for TMC: IMC.

9. TMC: The IMC attaches the R-TMC-VA1 to the Service Provider and sends a signature value verification completion message. The Service Provider decrypts the R_TMC_VA1 message.

R_TMC_VA_1 =
$D_{PUB\text{-}SP}(SP_{Inherence\text{-}Code} \oplus Vehicle_{Code} \oplus USER_{PWD})$
R_VS_1 = $E_{PUB\text{-}USER}(Vehicle_{Code} \oplus USER_{PWD} \oplus Nonce_{SP})$

10. The Service Provider sends the R_VS_1 message from the vehicle and completes the procedure for updating the signature value

4. Performance Evaluation

4.1. Safety Analysis

This section describes the communication configuration for the proposed communication protocol. Proposed communication protocol procedure is shown in Figure 2.

Threats to User Privacy Exposure and Disclosure: In addition to the vehicular communication environment, attack techniques in which hackers threaten important information of users in a wired and wireless communication environment are occurring steadily, and accidents occur in data leakage. In order to prevent the threat of the user's personal information from being leaked, the communication protocol is designed so that the confidentiality of the message is not threatened by encrypting the VA_1 generated in the registration process by the public key after the connection.

Spoofing Attacks: A spoofing attack may occur where an unauthorized user carries out vehicular communication technology on a vehicle by physically seizing the vehicle rather than the vehicular communication technology process. However, by verifying the parameters that combine the user's password and license number, the spoofing attack will fail.

Man-in-the-Middle Attacks: The man-in-the-middle attack is a typical weakness of the vehicular communication environment, which is an attack method in which an attacker seizes a message in communication between vehicle and vehicle, or vehicle and infrastructure, thereby modifying the captured message and causing harm to the user who sent or received the message. In the paper, by using the TMC_VA1 generated in the vehicle registration process, the authentication process is performed in the communication process, so that it is safe against the man-in-the-middle attacks.

Threat of Message Integrity: In the traditional vehicular communication technology process, a threat of message integrity arises from a hacker's attack attempt. In this paper, TMC_VA1 is generated by performing XOR on the vehicle code of the vehicle signature message, the unique code of the service provider, and the password of the user in order to compensate for the threat of message integrity. Also, R_TMC_VA1 is periodically generated after re-verification in the update process, and it is used in the communication process to complement the integrity of the message.

4.2. Communication Efficiency Analysis

This section describes the efficiency evaluation of the proposed communication protocol. In order to perform performance evaluation on signature value, a server was built using Apache Tomcat in Linux based Ubuntu 64Bit operating system, and an efficiency analysis was conducted on PKI, WPA2 and the proposed signature scheme in the existing communication environment using Open SSl and RSA. In order to compare and analyse the existing signature scheme and the proposed signature scheme, the comparative analysis results of certificate issuance and certificate verification are shown in Figure 6.

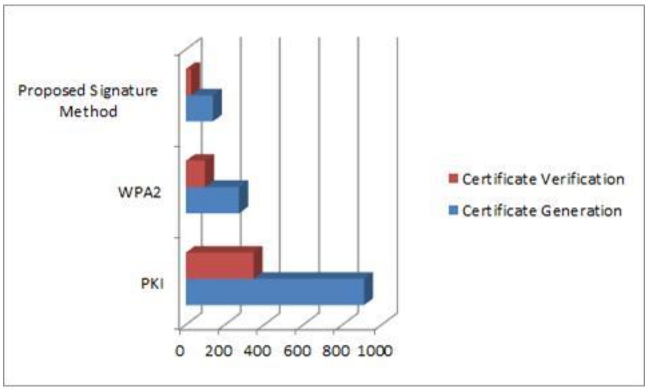

Fig. 6: The comparative analysis results of certificate issuance and certificate verification

The efficiency of certificate issuance is about 84% compared to PKI and about 49% for WPA2. As a result of comparison, it had high effectiveness of 90% of the PKI and 71% of the WPA2. A comparison analysis based on the existing certificate issuance and the certificate issuance amount was performed. The number of certificates generated by issuing certificates based on the power of 2 is as shown in Table 2 and Table 3. It can provide high quality service in terms of verification and efficiency compared with existing certificate management.

Table 2: Generation and Efficiency compared with existing certificate management.

	PKI based Signature Generation	**WPA2 based Signature Generation**	**Proposed Method based Signature Generation**
2	0.1856	0.054	0.023
4	0.365	0.102	0.042
8	0.723	0.212	0.0801
16	1.48	0.434	0.1512
32	2.87	0.872	0.2945
64	5.96	1.74	0.57421
128	12.2	3.34	1.12123
256	24.32	6.78	2.172
512	47.32	13.21	4.1952
1024	98.354	27.21	8.9464

Table 3: Verification and Efficiency compared with existing certificate management.

	PKI based Signature Verification	**WPA2 based Signature Verification**	**Proposed Method based Signature Verification**
2	0.03663	0.016667	0.010857
4	0.12633	0.043333	0.021714
8	0.30533	0.104444	0.043486
16	0.68383	0.227778	0.084114
32	1.37883	0.471111	0.166
64	2.92383	0.953333	0.325834
128	6.04383	1.842222	0.638417
256	12.10383	3.753333	1.238857
512	23.60383	7.325556	2.394971
1024	49.12083	15.10333	5.109943

5. Conclusion

Vehicular communication environment is a communication technology that combines technologies of vehicles and wireless communications. In this paper, a secure communication protocol was designed to provide efficient services in the vehicular communication environment. The proposed communication protocol generates VA_1, VA_2, and VA_3 by using $USER_{PWD}$, $Nonce_{Vehicle}$, and $Nonce_{SP}$, in the registration process of the vehicle, and performs secure communication in the vehicle environment. In the vehicle renewal and cancellation procedure, the generated parameters of the existing vehicle are verified to generate R_VA_1, R_VA_2, and R_TMC_VA1 to reinforce security.

The vulnerabilities and threats to user privacy exposure, camouflage attacks, man-in-the-middle attacks, and message integrity threats in the existing vehicle environment were analyzed, and by performing the efficiency evaluation in the existing communication environment, during the issuance process, it was about 84% of the PKI and about 49% of the WPA2, and in the verification process, it was about 90% of the PKI and about 71%.

6. Discussion

Currently, research on vehicular communication technology services is actively conducted, but technical studies on security threats and weaknesses in the vehicular communication environment are lacking. The vehicular communication environment inherits the attack techniques that occur in the existing wireless communications environment and requires countermeasures against new and variant attacks. Therefore, it is required to provide a secure communication environment for the user, and a more secure security policy is required.

Acknowledgements

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2016R1D1A1A09917662).

References

[1] TTAK.KO-12.0208, “Security Requirements for Vehicle-to-Vehicle Communication,” TTA, 2012. 12. 21.

[2] TTAK. KO-06.0174, “Requirements for Wide-Area Wireless Communication for ITS/Teleics,” TTA, 2008. 6. 26

[3] TTAK. K0-12.121241, “Security Requirements for Vehicle-to-Vehicle Communication,” TTA, 2012. 8. 12

[4] IEEE 1609.2-2013, “IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages,” April 2013.

[5] P. Papadimitratos et. al., “Secure Vehicular Communication Systems: Design and Architecture,” IEEE Communications Magazine, Nov. 2008, pp. 100-109.

[6] PRESERVE (PREeparing SEcuRe VEhicle-to-X Communication Systems) Deliverable 1.1, “Security Requirements of Vehicle Security Architecture,” June 2011.

[7] J Reinold, JD Bruner, EA Dabbish, WL Fehr, “Method and system for vehicle authentication of a component,” google patents, 2006.

[8] Ho-Jeon Jung, Jae-Chon Lee, “An Improved Method of FTA and Associated Risk Analysis Reflecting Automotive Functional Safety Standard,” Journal of the Korea Academia-Industrial cooperation Society, Vol. 18, No. 9 pp. 9-17, 2017.

[9] S.Y Min, K.H Lee, B.W Jin, “A Design of Authority Management Protocol for Secure Storage Access Control in Cloud Environment,” Journal of the Korea Academia-Industrial cooperation Society, Vol. 17, No. 9 pp. 12-20, 2016.

[10] S.Y Min, B.W Jin, S.Y Min, K.H Lee, B.W Jin, “A Design of Authority Management Protocol for Secure Storage Access Control in Cloud Environment,” Journal of the Korea Academia-Industrial cooperation Society, Vol. 16, No. 7 pp. 12-20, 2015.