Location Dependent Implicit Public Key Scheme for Vehicle Communication Systems

EunGi Kim

Faculty of Information and Communication Engineering, Hanbat National University, Daejeon, Republic of Korea, egkim@hanbat.ac.kr

In a vehicle communication system, each vehicle transmits a BSM message including information about its location, speed, direction, etc. together with a signature of the message in a broadcasting mode once at regular intervals. The receiving side can use the signature of the received BSM message to confirm that the contents of the message are not forged/falsified and are normal. When generating the signature of the BSM message, the sender's private key is used, and the receiver's public key is used to determine whether the received BSM message is normal or not. In this study, a method was studied to allow the private key and public key used for message signature and verification to be changed according to location. The user who generates the signature holds a location-independent secret key (KRs), and based on KRs, a secret key that changes depending on the location (KRld-s) is generated. This location dependent private key is used in the message signature. A location independent public key (KUs) is stored in the certificate. The receiving side generates a public key (KUld-s) that changes according to location based on KUs, and uses it to determine whether the received message is normal. Therefore, the receiving side has the advantage of not needing to separately verify the location information.

Keywords: Location dependent, Public key, Certificate, Security, Vehicle Communication.

1. Introduction

An entity or person and a public key are linked together by means of an electronic document called a certificate, which bears a digital signature. The company that validates the true identity of the person who holds the certificate and issues the certificate is known as the certificate authority (CA), and it is a reliable third party (Jake, 2017). The purpose of a certificate is to establish a trust relationship between two parties that are communicating over the Internet. Public key certificates are commonly used in secure communication protocols such as HTTPS, FTPS (ftp secure), SMTPS (simple mail transfer protocol secure), and virtual private networks (VPNs).

Public Key Infrastructure, or PKI, is the specification that describes how certificates and CA work. By combining public and private keys, PKI is a technique that aids in securing online communication. The PKI system employs a sender's private as well as public keys in conjunction to safely interact with another person or device. According to Josh (2020) and Adams et al. (2003), the exchange of messages takes place via the use of a sender's private key for encryption and a receiver for decryption. In a vehicle communication system, this kind of PKI system is used and used. A vehicle communication system is a system that allows vehicles to communicate with each other and with roadside equipment (RSE). This communication can be used for improving safety, optimizing traffic flow, or providing infotainment services. There are several technologies that can be used for vehicle communication, including dedicated short-range communication (DSRC), cellular networks, and IEEE defined wireless access in vehicular environments (WAVE) technologies.

Particularly intended for use in transportation, the DSRC is a form of wireless communication operating in the 5.9 GHz frequency region. Over short distances, it enables direct communication between cars and roadside infrastructure. Automotive communication can also be facilitated via cellular networks, including 4G and 5G. One of the wireless communication protocols in the IEEE 802.11 family is IEEE WAVE, also referred to as IEEE 802.11p. It is designed specifically for use in vehicular communication systems and the WAVE uses the DSRC protocol (IEEE, 2013; IEEE, 2010). In addition to these technologies, there are also various protocols and standards that have been developed to enable interoperability between different communication systems and devices. Examples include Vehicle-to-Everything (V2X) communication, which allows vehicles to communicate with other vehicles, pedestrians, and infrastructure (Ahmad et al., 2021; Zhao et al., 2022). In V2X communication, each vehicle periodically transmits a Basic Safety Message (BSM) in broadcast mode. This BSM message stores data such as the vehicle's position, speed, heading, and other basic safety-related information. The BSM message is transmitted in broadcast mode, and neighboring cars or roadside infrastructure devices that receive this message can use it to improve the safety and efficiency of vehicle operation (Noah, 2018). Car functioning may be seriously jeopardized if an attacker generates and transmits a malicious BSM message. As a result, the ability to discern if a BSM communication is forged must be provided to the recipient for the message. Currently, to do this, the sender signs the message using their secret key, and the receiver checks the signature to see whether it was faked. Nevertheless, this method raises the recipient-side cost of message verification. Every automobile has to be able to validate one BSM message every 5ms, for instance, if 20 cars are in the area and one car transmits the message once per 100ms. In this study, we propose a solution that supports a public key that is automatically changed according to the location information, and we research how to apply it to car communication. The proposed method has the advantage of not requiring the sender to transmit location information, and the recipient can quickly verify the received BSM message (IEEE, 2022; SAE, 2020).

In section 2, we describe the general methods for creating and verifying certificates and the structure of certificates, and explain the methods of transmitting location information based on these conventional methods. Section 3 describes the operation and advantages of the method proposed in this study, and Section 4 describes the conclusion.

2. TRANSMISSION AND VERIFICATION OF LOCATION INFORMATION

In this chapter, we describe the structure, creation, and verification of certificates, and the traditional method of using certificates to transmit location information in a car communication system.

2.1 Certificate creation and verification

Figure 1 shows the process of creating and verifying a certificate.

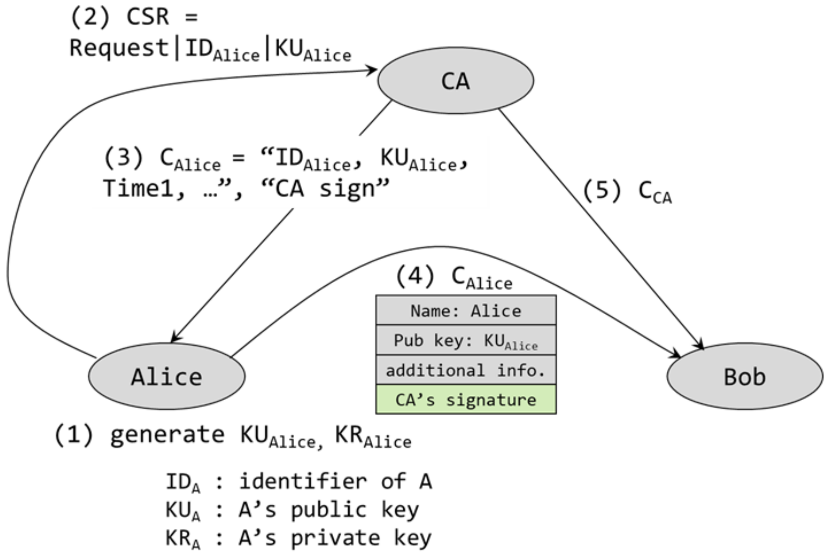

Fig. 1: Certificate creation and verification

There are several steps involved in creating a digital certificate (Villanueva et al., 2022; Eungi, 2019; Cooper et al., 2005).

- Generate a Public/Private Key Pair: The production of a public/private key pair (KUA, KRA) is the initial stage in the certificate creation process. The owner keeps the private key confidential, but others can access the public key.
- Submit a CSR: A CSR (Certificate Signing Request) is a message that requests the creation of a certificate and includes the requester's ID and public key.
- Certificate Creation: The CA will verify the information in the CSR and, if everything is in order, will issue a digital certificate. A certificate is composed of the owner's ID, public key, and the CA's signature that can verify it.

Digital certificates are used to verify the identity of a person or organization. In order to verify a digital certificate, the following steps can be taken:

- Check the Expiration Date: The certificate should still be valid and not have expired.
- Check the Issuing CA: The entity validating the certificate, or the person checking it, should trust the CA that issued the certificate.
- Check the Chain of Trust: The intermediate CAs must be legitimate and the certificate must be signed by a reliable root CA.
- Check the Revocation Status: The issuing CA had no right to revoke the certificate.

- Verify The Signature: The "CA's signature" field of the certificate is verified to prove that the contents of the certificate are correct. This process uses the CA public key stored in the CA's certificate.

2.2 Certificate Structure

In Figure 2, the structure of an X.509 certificate, which is currently the most widely used, is shown (Cooper et al., 2008).

The structure of a X.509 digital certificate consists of several fields that contain information about the certificate and the entity it belongs to. These fields are organized into several sections, including:

- The header, which identifies the certificate as a X.509 certificate and the version of the X.509 standard that it follows.

- The serial number, which is a unique identifier assigned to the certificate by the issuing CA.

- The digital signature of the certificate was created using a cryptographic technique, which is specified by the signature algorithm. (For example, SHA-256)

- The issuer, which is the name of the CA that issued the certificate.

- The validity period, which specifies the dates between which the certificate is valid.

- The subject, which is the name of the entity to which the certificate belongs (e.g., an individual, an organization, or a device). (ex. Alice)

- The subject's public key, which is the entity's public key. (ex. KU_{Alice})

- The extensions, which contain additional information about the certificate or the entity it belongs to.

- The digital signature, which is used to verify the integrity and authenticity of the certificate. (CA’s signature)

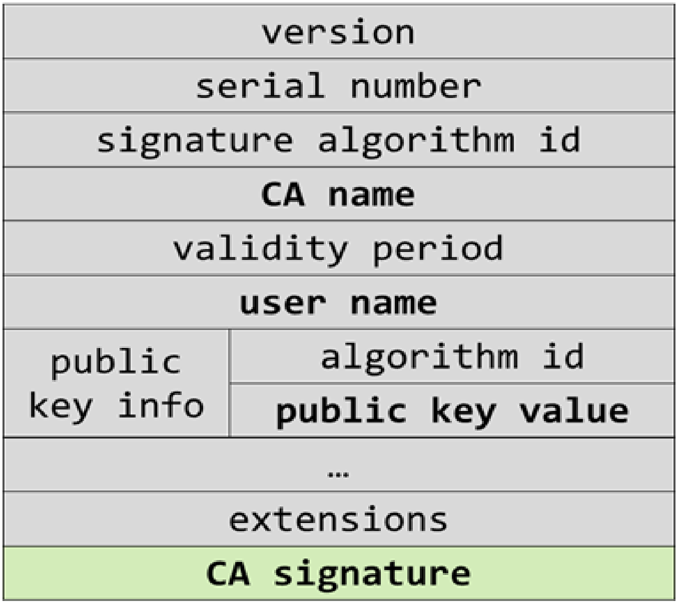

Fig. 2: X.509 certificate format

2.3 Verification of Location Information in a Vehicle Communication System

In the vehicle communication system, each vehicle broadcasts a BSM message once every certain amount of time. The transmitted BSM message is signed with the sender's private key so that the receiver can verify that the received message is normal.

Figure 3. shows the process of signing the location information message. A message containing location information is hashed to create a message digest, which is then encrypted using the sender's private key and used as the message's signature.

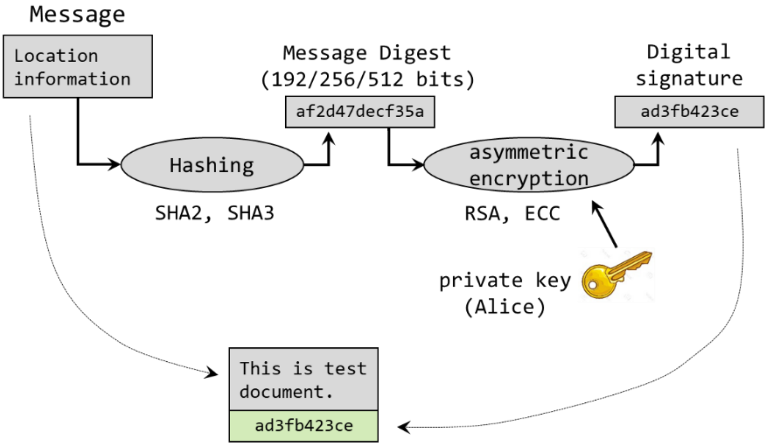

Fig. 3: Location information signing process

Figure 4, the signature verification process of a received message is shown. At the receiving side, the signature of the received message is decrypted using the sender's public key and the resulting value is compared with the calculated digests of the received message. If the two values are the same, it can be confirmed that the message is normal.

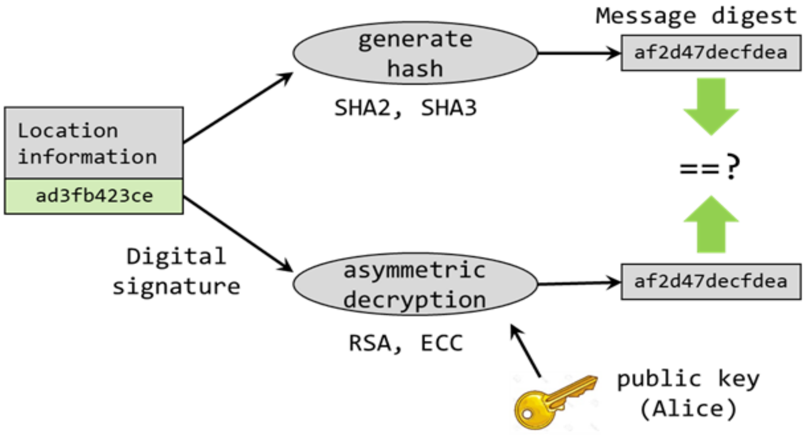

Fig. 4: Location information verification process

3. LOCATION DEPENDENT PUBLIC KEY SCHEME

3.1 Our Designed Scheme

Each vehicle in a car communication system transmits its location, direction, speed, etc. information in a BSM message in broadcast mode periodically. In this study, we propose a solution to quickly verify the location information at the receiver using a location dependent public key.

Figure 5 shows the operation of the proposed method using ECC (Elliptic Curve cryptography).

- KR_S: sender original private key
- KU_S: sender original public key

$KU_S = KR_S \times G$ (G: generator)

- $KR_{ld\text{-}S}$: sender location dependent private key

$KR_{ld\text{-}S} = KR_S +$ (location information)

- $KU_{ld\text{-}S}$: sender location dependent public key

$KU_{ld\text{-}S} = KR_{ld\text{-}S} \times G$

$= (KR_S + \text{location information}) \times G$

$= (KR_S \times G) + (\text{location information}) \times G$

$= (KU_S) + (\text{location information}) \times G$

Fig. 5: key generation methods

The user has a unique secret key/public key (KR_S, KU_S) and in actual signature and encryption, the location dependent secret key/public key ($KR_{ld\text{-}S}$, $KU_{ld\text{-}S}$) is used depending on the location. The user's unique public key KU_S is stored in the certificate in the usual way. This method does not need to separately verify the location information, and has an advantage that the location information is automatically verified. Figure 6. compares the operation of the existing signature method and the method proposed in this study.

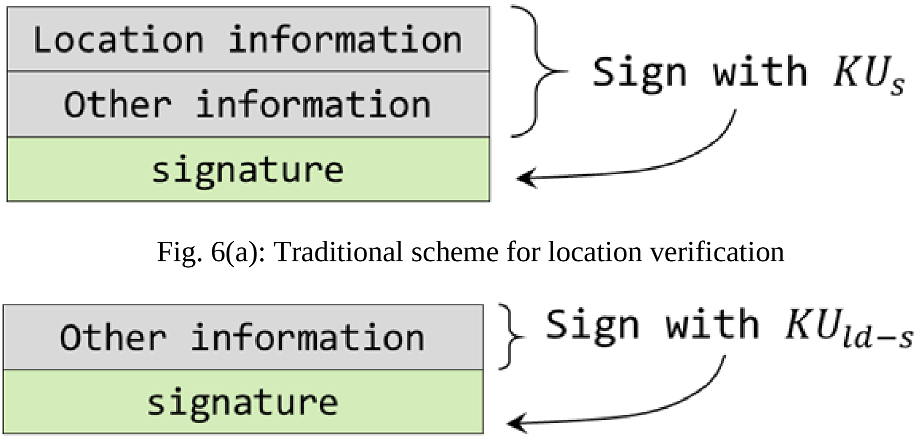

Fig. 6(a): Traditional scheme for location verification

Fig. 6(b): Our designed scheme for location verification

Fig. 6: Comparison of proposed and existing methods

3.2 Processing of Our Designed Scheme

Figure 7 shows the operation of the receiving side for processing location information including digital signatures in the conventional method. The receiving side calculates the hash value including the location information and verifies whether the value is the same as the value decrypted by the signature of the message. The method proposed in this study does not require such a process, and has the advantage of being able to verify location information through a process of simply verifying a certificate.

```
verify sender certificate;
digest = hash (“Location information | Other information”);
decrypted_sig = decrypt the signature using the public key stored in the sender certificate;
if (digest = decrypted_sig)
    verification success;
else
    verification fail;
```

Fig. 7: Traditional location verification methods

3.3 Processing Overheads

In the method proposed in this study, an operation of adding location information to an existing secret key is required, and an operation of multiplying the result of this addition by a generator must be performed.

Figure 8 shows the overhead required for the processing of the method proposed in this study. This experiment was programmed using openssl in Intel(R) Core (TM) i7-12700K CPU, RAM 64 GB, Linux fedora 6.1.14-200.fc37.x86_64 environment. Encryption uses the ECC method, and the compared ECC curves are as follows.

- prime256v1: (NID_X9_62_prime256v1)
- secp224r1: NIST/SECG curve over a 224 bit prime field (NID_secp224r1)
- secp256k1: SECG curve over a 256 bit prime field (NID_secp256k1)
- secp384r1: NIST/SECG curve over a 384 bit prime field (NID_secp384r1)

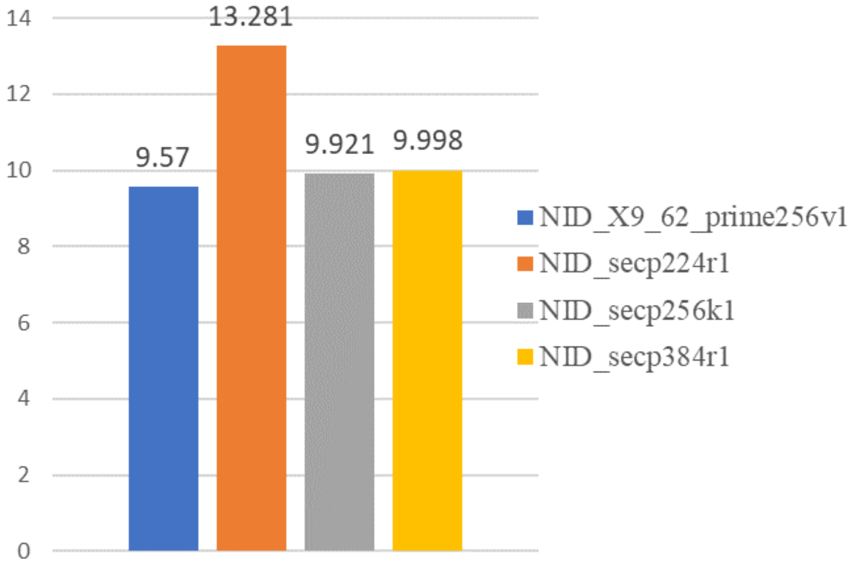

Fig. 8(a): private key processing overheads (micro-sec)

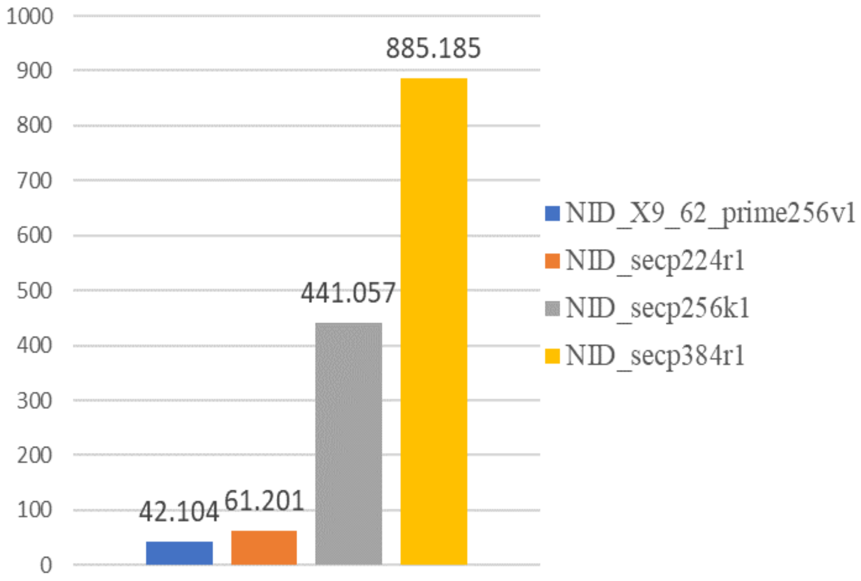

Fig. 8(b): public key processing overheads (micro-sec)

Fig. 8: Processing overheads of our designed methods

4. CONCLUSION

Our approach in this study is to modify the user's public key and private key dynamically based on where they are. Our suggested approach involves the user having a temporal secret key (KRld-S) that varies based on location and his or her personal secret key (KRS) that is used to sign messages. When a message is received, its authenticity is assessed by the receiving end using the temporal public key (KRld-S), which is created based on the location and is saved in the certificate. Our proposed method has the advantage of not requiring separate location verification because the public key used for message verification itself contains location information. Therefore, our designed method can be applied to all systems that require periodic transmission and verification of location information.

Afterwards, we plan to conduct research to apply the results of this research to actual vehicle communication systems.

References

1. Eungi Kim (2019). Design and Implementation of Multiple ECQV Implicit Certificate Generation Algorithms, April 5, 2019, Volume-8 Issue-3C, International Journal of Innovative Technology and Exploring Engineering
2. Jake A., Berkowsky, Thaier Hayajneh. (2017). Security issues with certificate authorities, 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), 19-21 October 2017, pp. 449–455.
3. Josh Fruhlinger (2020). What is PKI? And how it secures just about everything online, 29 May 2020, https://www.csoonline.com/article/3400836/what-is-pki-and-how-it-secures-

just-about-everything-online.html

4. ITS joint program office (2013). IEEE 1609 - Family of Standards for Wireless Access in Vehicular Environments (WAVE). US Department of Transportation. 2013 Apr. https://www.standards.its.dot.gov/Factsheets/Factsheet/80
5. IEEE 802.11p-2010 (2010). IEEE Standard for Information technology -- Local and metropolitan area networks-- Specific requirements-- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments.
6. Ahmad Alalewi, I. Dayoub, S. Cherkaoui (2021). On 5G-V2X Use Cases and Enabling Technologies: A Comprehensive Survey, IEEE Access. 9: 107710-107737, July 26, 2021
7. Chengcheng Zhao, Xiaoming Duan, Lin Cai, Peng Cheng (2022). Vehicle Platooning with Non-ideal Communication Networks, IEEE Transactions on Vehicular Technology, 70(1):18-32, Jan. 2022.
8. Adams Carlisle, Lloyd, Steve (2003). Understanding PKI: concepts, standards, and deployment considerations. Addison-Wesley Professional. pp. 11–15. ISBN 978-0-672-32391-1.
9. Noah Carter, Mohammad A. Hoque, Md Salman Ahmed (2018). Simulating Vehicle Movement and Multi-Hop Connectivity from Basic Safety Messages, IEEE SoutheastCon 2018, 19-22 April 2018, St. Petersburg, FL, USA
10. IEEE Std 1609.2.1 (2022). IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Certificate Management Interfaces for End Entities, IEEE Vehicular Technology Society, March 2022
11. Villanueva, John Carl (2022). How do Digital Certificates Work - An Overview, www.jscape.com, November 25, 2022, https://www.jscape.com/blog/an-overview-of-how-digital-certificates-work
12. Eungi Kim (2019). Design and Implementation of Multiple ECQV Implicit Certificate Generation Algorithms, April 5, 2019, Volume-8 Issue-3C, International Journal of Innovative Technology and Exploring Engineering
13. M. Cooper, Y. Dzambasow, P. Hesse, S. Joseph, R. Nicholas (2005). Internet X.509 Public Key Infrastructure: Certification Path Building, RFC 4158, IETF, sept. 2005
14. D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk (2008). Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, RFC 5280, RIETF, may 2008
15. SAE International Standards (2016). On-Board System Requirements for V2V Safety Communications, J2945/1, April, 2020