March - April 2020
ISSN: 0193-4120 Page No. 4067 - 4072

MAC Address Autochange Methods for Supporting Anonymity in VANETs

Eun-Gi Kim
Professor, Department of Information and Communication Engineering, Hanbat National University, Republic of Korea
egkim@hanbat.ac.kr,

Article Info
Volume 83
Page Number: 4067 - 4072
Publication Issue:
March - April 2020

Article History
Article Received*: 24 July 2019*
Revised*: 12 September 2019*
Accepted*: 15 February 2020*
Publication*: 26 March 2020*

Abstract
Establishment and focus: This study proposes a method that a vehicle can automatically change its MAC address for anonymity in vehicle communication system. After a shared key is established between the two cars participating in the communication, the two cars can use this shared key to generate and use a large number of new MAC addresses. Vehicles not participating in the communication cannot know the newly changed medium access control (MAC) address, thereby ensuring anonymity of the vehicle communication.

System: The sender and the receiver can calculate $hv(i) = HMAC_{SHA512}(rs, Cert_A, Cert_B)$ using the shared secret number *rs*, and can generate up to 10 MAC addresses in one *hv(i)*. The HMAC used for the calculation of each *hv(i)* uses *rs* which is secretly shared by the sender and receiver, so that the attacker cannot find out the generated MAC address. In this study, it is assumed that the vehicle communication system is made according to the IEEE WAVE standard. Therefore, the key value is shared between the transmitter and the receiver by using ECIES (Elliptic Curve Integrated Encryption Scheme). However, even if this study is used in a different environment, the results of the study can be applied as long as the transmitting and receiving vehicles share the same key value. The vehicle transmitting the MAC frame can guarantee anonymity of the vehicle communication by arbitrarily changing its MAC address.

Keywords: *Vehicle, Communication, Anonymity, VANET, MAC address, WAVE.*

1. Introduction

Vehicle communication technology incorporating communication functions into automobiles is being actively researched as a core technology of future transportation systems. The automotive communication system enables vehicles to be connected based on vehicle-to-everything (V2X) communication technology to provide safe driving, traffic congestion prevention, and various services through two-way communication with nearby vehicles, road infrastructure, and pedestrians [1,2]. Future car technology is expected to evolve into autonomous cars, connected cars, smart cars, etc. Standardization of vehicle communication technology includes: 1) IEEE WAVE system, which can modify existing IEEE 802.11 wireless LAN standard and apply to fast moving cars, 2) 5G V2X system that utilizes 5G mobile communication technology for automobile communication, 3) many of V2X projects that are being researched around the European Telecommunications Standards Institute (ETSI) [3]. The core technology of the automotive communication system being studied in these systems basically requires fast data transmission, low-latency high reliability, ultra-precision positioning information, and security functions. Among them, the car security functions can be classified into an internal car security system and

an inter vehicle security system. In-vehicle security system is a technology for protecting various devices inside the car such as ECU, sensors, actuators, and inter vehicle security system is a technology that adds a security function to the car communication. The inter vehicle security system requires the function of encrypting the content of the transmitted message and the message authentication function to detect the forgery of the message. In addition, since the vehicle transmits a number of BSM (basic safety message) messages in broadcasting mode, anonymity support function for protecting the privacy of the driver is also required [4]. In this paper, we propose a method for auto-changing of MAC address for anonymity in automobile communication systems. In chapter 2, related research is described. In chapter 3, MAC address generation methods for auto change of MAC address is described. Chapters 4 and 5 describe performance analysis, verification, and conclusions.

2. Related research

2.1 Security Requirements in Vehicle Communications

Because automotive communication systems are used in a variety of environments, they must be able to support secure communications from multiple security threats [5]. The security requirements of the automotive communication system are as follows.

• Entity authentication

It is to verify that the other party participating in the communication is a normal user. Generally, a method of using a pre-shared key, digital signature, or public key is used for entity authentication. However, in a vehicle communication, a PKI certificate dedicated to a car communication system is appropriate [6].

• Privacy preservation

Cars participating in communication exchange important information about their safety and mobility with other cars or road side equipment (RSE) wirelessly. This sharing of information between cars and RSEs can lead to personal privacy violations. In order to solve this problem, the message transmitted in the vehicle communication should not include information that can directly or indirectly identify a particular person or vehicle [7].

• Non-Repudiation

Since the messages sent from the car communication system can be directly related to the safety of the car, the entity sending the message must not later deny the message sent by it. These features can be used to defend against network attacks by malicious vehicles or to identify problems in the event of an accident.

• Confidentiality

All data sent in automotive communication is transmitted over the air, allowing all users to receive messages. Thus, if necessary, the content of the message should be encrypted so that the third party cannot know the content.

• Message authentication

The vehicle receiving the message must be able to confirm that the content of the received message has not changed and that the sender of the message is a normal user. This feature can be used to defend against network attacks by malicious vehicles.

2.2 WAVE security system

Wireless Access in Vehicular Environment (WAVE) system for vehicle communication is a standard communication method established by IEEE for V2X vehicle networking. In the WAVE system, the IEEE 802.11p standard is defined as Layers 1 and 2, which are modified to fit the

March - April 2020
ISSN: 0193-4120 Page No. 4067 - 4072

physical and MAC layer functions of the IEEE 802.11 standard for automobile communication. The WAVE system consists of 1609.3 for networking services on top of IEEE 802.11p, 1609.4 for defining operations on multiple channels, and 1609.2 for defining security functions of communication systems. Among them, the 1609.2 standard, which is responsible for security functions, has been revised to the current standard after several revisions since it was first published in 2006[3]. Security algorithms used in the IEEE 1609.2 WAVE standard include ECDSA for digital signature and ECIES for encrypting data. Figure 1. shows the WAVE protocol stack.

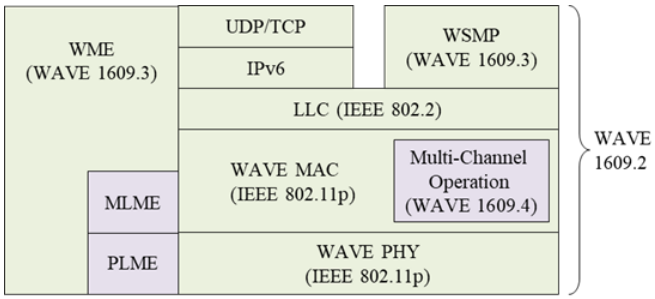


Figure 1. WAVE protocol layers

2.3 Security Algorithms in WAVE Systems

The IEEE WAVE system uses ECDSA and ECIES algorithms for message authentication and confidentiality [8-10]. Each algorithm works as follows:

• ECDSA (Elliptic Curve Digital Signature Algorithm, ECDSA)

WAVE systems require the use of ECDSA specifications as described in FIPS 186-4. The elliptic curves required for the application of this specification use the NIST P256 curve described in FIPS 186-4 or the brainpoolP256r1 described in RFC 5639[11-13]. Figure 2 shows the simplified ECDSA operations. The sender generates its own private key d and computes the public key Q_A ($Q_A = \mathrm{dG}$, G is generator). Sender generates random number k ($1 \le \mathrm{k} \le \mathrm{n}-1$) to sign message M, computes $\mathrm{R}(R_x, R_y) = \mathrm{kG}$ and sets $\mathrm{r} = R_x$. Sender calculates $\mathrm{hash(M)}$ and s, and transmits to the other the "$\mathrm{M}, \mathrm{s}, \mathrm{r}$ ".

The receiving side calculates $R'(R'_x, R'_y)$ using the received s and r, and determines that the verification is successful if R'_x is equal to r. As can be seen from equation 1, the calculated R' is the same value as R calculated by the sender, so R'_x and R_x become the same if the contents of the message have not changed.

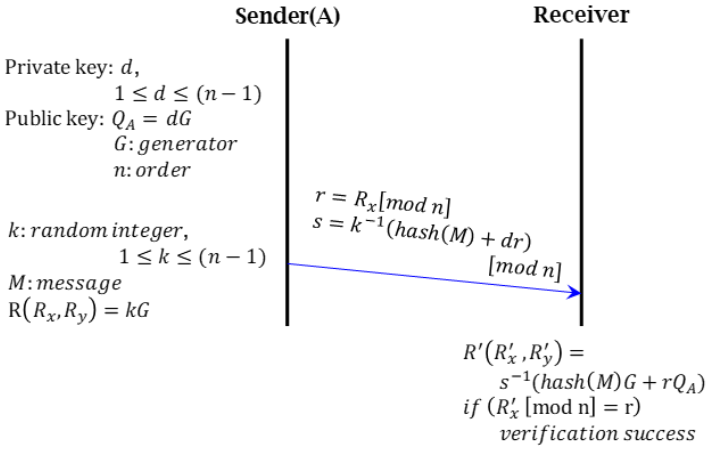


Figure 2. Simplified ECDSA operation

$$
\begin{aligned}
R' &= \frac{k}{hash(M)+dr}(hash(M)G + rQ_A) \\
&= \frac{k}{hash(M)+dr}(hash(M)G + rdG) \\
&= \frac{k}{hash(M)+dr}(hash(M)+rd)G \\
&= kG
\end{aligned} \qquad (1)
$$

• ECIES (Elliptic Curve Integrated Encryption Scheme)

In the WAVE system, ECIES described in IEEE 1363a is used as an asymmetric encryption algorithm. The elliptic curves used are the same as those used in ECDSA. The user transmits the key to be used by the symmetric encryption algorithm (AES-CCM) to the other party using ECIES, and then transmits the data encrypted by the AES-CCM method using the shared session key.

March - April 2020
ISSN: 0193-4120 Page No. 4067 - 4072

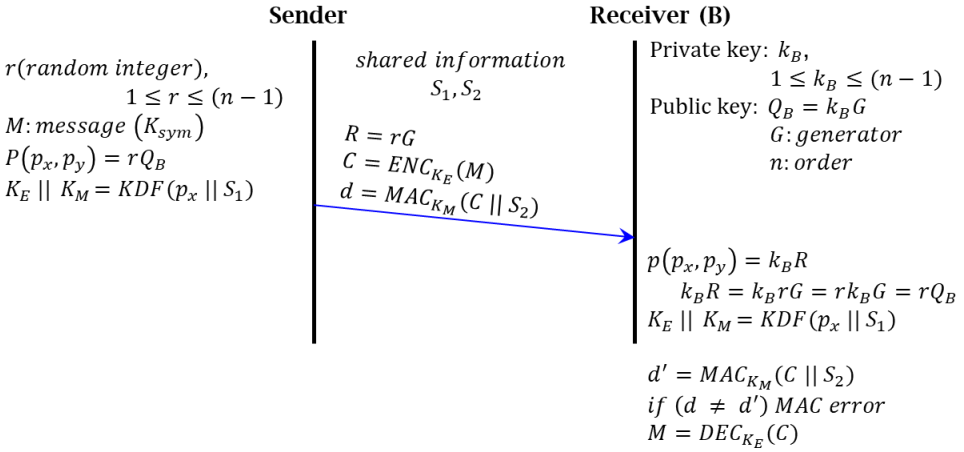


Figure 3. Simplified ECIES operation

Figure 3 shows the simplified ECIES operations. The sender generates a random integer r ($1 \le r \le n-1$) and calculates $P = rQ_B$ by multiplying this value by the receiver's public key Q_B. Since P is a point on the elliptic curve, it has a value of $P(P_x, P_y)$, and this P_x input to the KDF (key derivation function) function. The output of the KDF function is used as an encryption key (K_E) and MAC key (K_M). The sender sends a message such as $R(=rG)$, ciphertext ($Enc - K_E(plaintext)$, d ($MAC - K_M(C||S2)$) to the receiver. The receiver calculates the value of $P(P_x, P_y)$, by multiplying the received R by its secret key k_B. The calculated P' has the same value as P calculated by the sender according to equation (2). Since the sender and the receiver have the same P, the receiver can decrypt the received message and verify the MAC code using K_E, K_M.

$$k_B R = k_B rG = rk_B G = rQ_B \qquad (2)$$

In the WAVE system, AES CCM mode is used as a symmetric key encryption algorithm.

3. MAC address auto-change methods

In this study, we propose a scheme to change its MAC address after sharing key value using ECIES. In this study, it is assumed that the vehicle communication system is made according to the IEEE WAVE standard. Therefore, the key value is shared between the transmitter and the receiver by using ECIES. However, even if this study is used in a different environment, the results of the study can be applied as long as the transmitting and receiving vehicles share the same key value. Figure 4 shows the MAC address generation algorithm.

$$rs \text{ is shared secret;}$$
$$\text{for each } hv(i) \quad (i = 0, 1, 2, \dots)$$
$$hv(i) = HMAC_{SHA512}(rs + i,\ \text{Cert}_A \mid Cert_B);$$
$$MAC\ address\ (j) = hv(i)_{64j} \sim hv(i)_{64(j+1)-1} \qquad (j = 0, 1, .., 9)$$
$$hv(i)_k \text{ is the } k'\text{th bits of } hv(i), \quad (k = 0, 1, \dots, 511)$$

Figure 4. MAC address generation algorithm

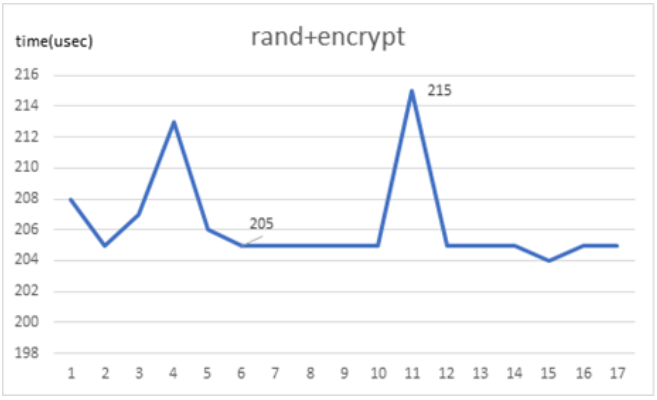
The sender and the receiver can calculate hv(i) using the shared secret number rs, and can generate up to 10 MAC addresses in one hv(i). The HMAC used for the calculation of each hv(i) uses rs secretly shared by the sender and receiver, so that the attacker cannot find out the generated MAC address. The generated large amount of MAC address can be used in various ways depending on the needs of the application. For example, the MAC address can be changed periodically at a certain time, or it can be changed whenever a specific event occurs.

4. Performance Verification and Analysis

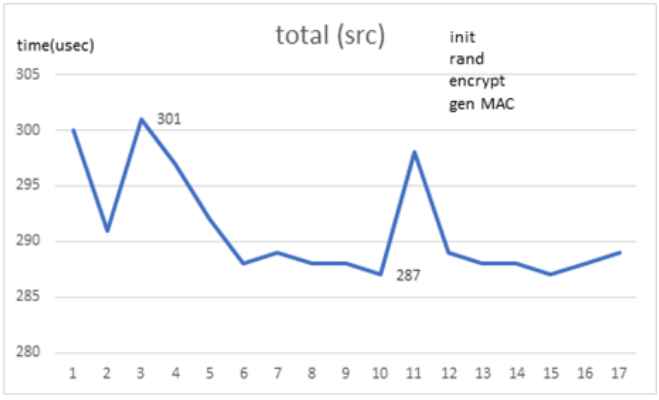
In this study, we implemented the proposed MAC address automatic change algorithm and analyzed

March - April 2020
ISSN: 0193-4120 Page No. 4067 - 4072

the performance in real environment. Source code for performance analysis is implemented in C using the Openssl library. Time for performance analysis was measured in a notebook using the Ubuntu 18 operating system (Linux Kernel 4.15.0-58) (Intel (R) Core (TM) i5-3570 CPU @ 3.40GHz, 8G RAM). Figure 4 shows the sender's performance for secret key generation, encryption with ECIES, and sending. Figure 5 (a) shows the performance of generating a random number and encrypting it, and (b) shows the total time required to initialize ECIES, generate random numbers, encrypt ECIES and generate MAC addresses.



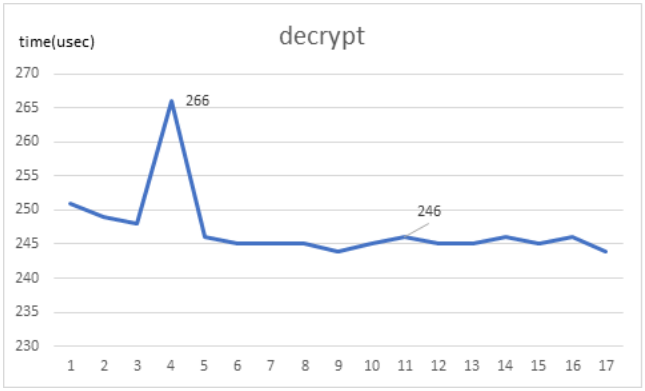
(a) Time for random number generation and encryption



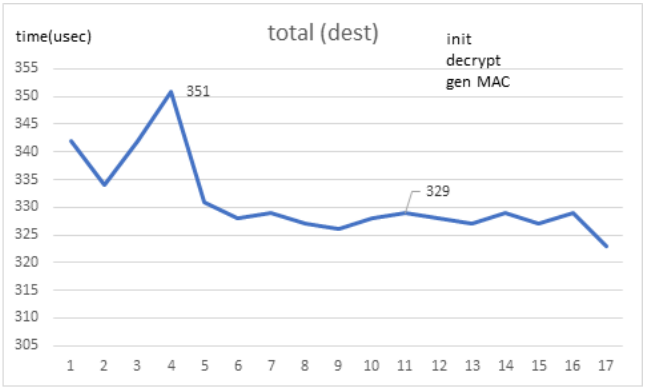
(b) Total sender processing time

Figure 5. Sender processing time for MAC address generation

Figure 6 shows the performance of the message receiver. Figure 6 (a) shows the time required for ECIES decryption, and Figure 6 (b) shows the total time required for ECIES initialization, ECIES decryption, and MAC address generation.



(a) ECIES decryption time



(b) Total receiver processing time

Figure 6. Receiver processing time for MAC address generation

5. Conclusion

V2X research is being actively conducted to increase the safety of road operation by adding communication functions to automobiles. In addition to the security requirements of a typical wireless communication system, automotive communication systems also require anonymity support for privacy protection. In order to guarantee the confidentiality of the message in the vehicle communication system, a shared key must be established between the two vehicles participating in the communication. Such a shared key may be set using an ECIES algorithm as in the IEEE WAVE system, or may be set using an

March - April 2020
ISSN: 0193-4120 Page No. 4067 - 4072

Elliptic-curve Diffie-Hellman (ECDH) algorithm or a certificate. In this study, we propose a scheme to support anonymity in automotive communication systems and analyze its performance. When a shared key is established between two cars participating in the communication system, the two cars can use the shared key to generate a large amount of new MAC address. Then, the two vehicles participating in the communication can change their MAC address as needed. Terminals not participating in the communication cannot know the newly changed MAC address, thereby ensuring the anonymity of the vehicle communication. Later, we will conduct a study to apply the proposed method in the actual environment.

5. References

1. Georgios Karagiannis, Onur Altintas, Eylem Ekici, Geert Heijenk, Boangoat Jarupan, Kenneth Lin, et al. Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards, and Solutions. IEEE Communication Surveys & Tutorials. 2011 Jul;13(4): 584-616.
2. Cesar Bernardinia, Muhammad Rizwan Asgharb, Bruno Crispocd. Security and privacy in vehicular communications: Challenges and opportunities. Vehicular Communications. 2017 Oct;10: 13-28.
3. IEEE Standards Association. IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Security Services for Applications and Management Messages. IEEE Standards 1609.2. 2016.
4. Michael W. Whalen, Darren Cofer, and Andrew Gacek. Requirements and Architectures for Secure Vehicles. IEEE Software. 2016 July;33(4): 22-25.
5. Ahmer Khan Jadoon, Licheng Wang, Tong Li, Muhammad Azam Zia. Lightweight Cryptographic Techniques for Automotive Cybersecurity. Hindawi Wireless Communications and Mobile Computing, 2018. Available from: https://www.hindawi.com/journals/wcmc/2018/1640167/
6. Jie Li, Huang Lu, and Mohsen Guizani. ACPN: A Novel Authentication Framework with Conditional Privacy-Preservation and Non-Repudiation for VANETs. IEEE Transactions on Parallel and Distributed Systems. 2015 Apr;26(4): 938~948.
7. Jae-Won Ahn, Seung-Peom Park, Kwon-Jeong Yoo and Eun-Gi Kim. A Study on the New Ethernet Communication Method Using Virtual MAC Address. Lecture Notes in Electrical Engineering, Springer, 2015 Dec:373: 613~618. Available from: https://link.springer.com/chapter/10.1007/978-981-10-0281-6_87
8. D. Richard Kuhn, Vincent C. Hu, W. Timothy Polk, Shu-Jen Chang. Introduction to public key technology and the federal PKI infrastructure. NIST Standards. SP 800-32, 2001 Feb. Available from: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-32.pdf
9. Lawrence C. Washington. Elliptic Curves: Number Theory and Cryptography. 2nd ed. CRC Press, 2008 Apr.
10. IEEE Standards Association. IEEE Standard Specifications for Public-Key Cryptography-Amendment 1: Additional Techniques. IEEE Std 1363a-2004. 2004 Sept.
11. Standards for Efficient Cryptography Group. SEC 4: Elliptic Curve Qu-Vanstone Implicit Certificate Scheme (ECQV). Version 1.0. Certicom Research. 2013 Jan. Available from: https://www.secg.org/sec4-1.0.pdf
12. Information Technology Laboratory, National Institute of Standards and Technology. Digital Signature Standard (DSS). FIPS PUB 186-4. 2013 Jul. Available from: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf
13. M. Lochter, J. Merkle. Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation. Request for Comments 5639. 2010 Mar. Available from: https://tools.ietf.org/html/rfc5639