A Secure and Efficient Message Authentication Scheme for Vehicular Networks based on LTE-V

Cheng Xu[1], Xiaohong Huang[1], Maode Ma[2] and Hong Bao[3]
[1] Institute of Network Technology, Beijing University of Posts and Telecommunications
Beijing, China
[xc-f4@163.com , huangxh@bupt.edu.cn]
[2] School of Electrical and Electronic Engineering, Nanyang Technological University
Singapore
[emdma@ntu.edu.sg]
[3] Beijing Key Laboratory of Information Service Engineering, Beijing Union University
Beijing, China
[baohong@buu.edu.cn]
*Corresponding author: Xiaohong Huang

Received August 14, 2017; revised January 10, 2018; accepted January 24, 2018; published June 30, 2018

Abstract

Vehicular networks play an important role in current intelligent transportation networks and have gained much attention from academia and industry. Vehicular networks can be enhanced by Long Term Evolution-Vehicle (LTE-V) technology, which has been defined in a series of standards by the 3rd Generation Partnership Project (3GPP). LTE-V technology is a systematic and integrated V2X solution. To guarantee secure LTE-V communication, security and privacy issues must be addressed before the network is deployed. The present study aims to improve the security functionality of vehicular LTE networks by proposing an efficient and secure ID-based message authentication scheme for vehicular networks, named the ESMAV. We demonstrate its ability to simultaneously support both mutual authentication and privacy protection. In addition, the ESMAV exhibit better performance in terms of overhead computation, communication cost, and security functions, which includes privacy preservation and non-frameability.

Keywords: Message authentication, LTE-V, Vehicular network, Privacy preserving

This work has been supported by Project U1603261 supported by Joint Funds of National Natural Science Foundation of China and Xinjiang, the National Natural Science Foundation of China (Grant No. 61602055) and the Project of High-level Teachers in Beijing Municipal Universities in the Period of 13th Five-Year Plan (IDHT20170511)

http://doi.org/10.3837/tiis.2018.06.022 **ISSN : 1976-7277**

1. Introduction

With the rapid development of wireless communication technology, vehicular ad hoc networks have become a key technology in intelligent transportation systems (ITS). Several ITS applications aim to enable wireless connectivity in vehicles to support road safety and traffic efficiency through vehicle-to-vehicle (V2V), vehicle-to-pedestrian (V2P), and vehicle-to-infrastructure (V2I) communications [1]. Various wireless access technologies are available to provide the radio interface required by the vehicular communications, including traditional Wi-Fi, IEEE 802.11p, cellular systems, and infrared communications. These operate in different frequency bands provide varying communication ranges, data rates, channel bandwidths, and mobility supporting capability features [2]. Traffic accidents have caused billions of dollars’ worth in losses as compared to health-related incidents. Therefore, the enhancement and fusion of vehicular wireless network communication technology between vehicles, pedestrians, infrastructure, and the environment can ultimately improve traffic safety and efficiency [3].

In order to accommodate for increasing mobile data transmission demands and new multimedia applications, 3GPP have characterized long-term evolution (LTE) and LTE-Advanced (LTE-A) technologies as emerging mobile communication technologies as next generation broadband mobile wireless networks [4]. LTE technologies exhibit high data rates, high penetration rates, comprehensive QoS supporting, and extended coverage. These technologies possess natural benefits to provide V2I communications. Three LTE application challenges are observed in V2V communications [5]. Firstly, the centralized architecture lacks V2V communication support. Secondly, it requires a better capacity to support the heavy load that is strongly generated by periodic messages. Thirdly, LTE applications potentially penalize the delivery of traditional applications. A complementary relationship between cellular and ad-hoc communication technologies is suggested rather than one that focuses on competition. The extension of LTE technologies with direct communication capabilities between vehicles is a promising and possibly integrated vehicle-to-everything (V2X) solution [6].

Many international companies, including Huawei, Qualcomm, Ericsson, and Google have researched vehicular long-term evolution-vehicle (LTE-V) technologies. LTE-V is a fast deployment technology that uses the legacy LTE network. However, one chipset, namely the LTE (telematics)/VDC (Vehicle Direct Communication), is used by all technologies. LTE-VDC often called LTE Device-to-Device (LTE-D2D). It could provide a decentralized approach to proximity discovery and vehicle-to-vehicle communication, which is now also included in 5G networks. The researchers believe that LTE-V standardization development also presents a strong compatibility for 5G [7]. Vehicles that are part of LTE-V vehicular networks are equipped with on-board units (OBUs). OBUs enable vehicles in the LTE-V network to exchange messages with nearby nodes. Each vehicle is able to communicate with nearby vehicles and roadside units (RSU) as well as traffic control centers through the internet [8].

In terms of the wireless communication mode, adversaries can attack the LTE-V network and easily control communication channels [9]. LTE is composed of an evolved packet core (EPC) and an evolved UMTS terrestrial radio access network (E-UTRAN). In the LTE, the mobility management entity (MME) is essential to control the nodes of LTE access networks. The home subscriber server (HSS) exhibits high computation and communication capabilities and is responsible for the generation of system parameters and offline OBU preloading in vehicles. HSS is the only participant that fully obtains the real identity of the vehicle based on intercepted messages [10]. However, LTE is vulnerable to many types of attack given that adversaries can intercept, modify, replay, and delete messages between the sender and the receiver [11].

1.1 Our Contributions

To address the authentication request challenges that are applicable to massive OBUs in LTE-V-based networks, the present study designed and proposed an efficient identity-based message authentication for LTE-V networks (ESMAV). The contributions of the presented work can be summarized as follows.

1) An efficient identity-based message authentication scheme was proposed for LTE-V networks. The non-repudiation of simple messages and batch messages were included to further enhance the performance.

2) As compared to existing schemes, the proposed ESMAV scheme can greatly reduce the amount of signal exchange. In massive OBU and RSU, it has lower signaling overload in LTE-V-based networks.

3) Robust security functions were achieved, which includes privacy preservation, resistance to various attacks, non-frameability, and non-repudiation verification.

1.2 Organization of the Remainder of the Paper

The remainder of this paper is organized as follows. Sections 2 and 3 introduce the related work, the network model, and security goals. Section 4 presents the proposed ESMAV scheme in detail. Section 5 presents the evaluation of the security functionality of the proposed scheme. The efficiency analysis of the proposed scheme will be performed in Section 6. Finally, Section 7 presents the conclusion.

2. Related Work

Many research works have discussed 3GPP network message authentication and key agreement protocol. To deal with the aforementioned challenges, many vehicular network authentication schemes have been proposed. Lai et al. [11] research a secure and efficient group authentication and key agreement (SE-AKA) scheme that employs the asymmetric key cryptosystem and elliptic curve Diffie-Hellman scheme to provide robust security protection that includes privacy preservation. The authentication process of the SE-AKA scheme adopts GTK generation to simplify the entire authentication process. By adopting the concept of the SE-AKA scheme, the EAP-based group (EG-AKA) scheme in [12] facilitates a group of MTCDs that access the LTE core network through a non-3GPP access network. The above-mentioned schemes do not employ a group key generation method and dynamic group member management mechanisms. A novel lightweight group authentication protocol (LGTH) was proposed in [13] for MTC authentication in LTE networks based on aggregate message authentication codes (MACs). In the LGTH, a group leader collects message authentication codes from all the members and validates them. As compared to public key methods, the LGTH scheme significantly reduces OBU computational costs but requires the application of a verification process, which increases overhead signaling. The GLARM scheme in [14] employs group authentication to reduce severe authentication signaling congestion. The GLARM scheme is a novel lightweight group authentication scheme. It is employed for resource-constrained devices in the 3GPP network model. GLARM achieves efficient and secure 3GPP and non-3GPP group authentication.

Transmitted LTE networks messages may be easily detected, intercepted, modified, and replayed by malicious adversaries [15]. To solve these problems, Lai et al. [16] proposed the reservation of idle radio resources in the LTE for vehicular safety services. The proposed mechanism can significantly improve the reliability of safety applications by borrowing limited LTE bandwidth. Fu et al. [17] proposed a novel privacy-preserving group authentication protocol for machine-type communication (MTC) in LTE/LTE-A networks. The proposed protocol can simultaneously authenticate a group of MTCDs and minimize overhead signaling. In additions, it provides robust privacy preservation in each MTCD, which includes anonymity, unlinkability, and non-traceability. Moreover, key chains used in handover processes did exhibit backward security. Therefore, Ma et al. [18] proposed a scheme based on the elliptic curve cryptography (ECC) algorithm, which is a proxy signature-based algorithm that generates a smaller handover process computational cost as compared to other handover schemes. However, the expansion and increased openness of LTE networks has shifted security practices to ensure user and data protection [19]. Many schemes have incorporated identity-based authentication for heterogeneous vehicular networks [19-24].

The identity authentication scheme can effectively solve storage and management problems, and presents good security and efficiency. Recently, Shim et al. [20] proposed an efficient conditional privacy-preserving authentication scheme for vehicular sensor networks named CPAS. In the CPAS, the RSU simultaneously verifies multiple received signatures, thus reducing considerable total verification time. Lee et al. [21] proposed an authentication scheme for vehicular ad hoc networks (VANETs) using an elliptical curve-based signature, though it does not solve the non-repudiation of simple and batch messages. Zhang et al. [22] discovered the inability of Lee’ s scheme to withstand impersonation attacks. To overcome these flaws, they proposed an improved authentication scheme for the security of a secure batch verification with group testing. Bayat et al. [23] also proposed a secure authentication scheme with batch verification. However, bilinear pairing operation is one of the most complex operations in modern cryptography. To enhance the performance and reduce the computational complexity of information processing, He et al. [24] proposed a CPPA scheme that did not use bilinear paring. The present study demonstrated its ability to simultaneously support mutual authentication and privacy protection. At present, a scheme that simultaneously solves safety, efficiency, and privacy protection issues while maintaining message authentication has not been proposed. Therefore, the present study argues for practical applications to design an ID-based scheme for vehicular networks based on LTE-V without bilinear pairing.

3. Preliminary

3.1 *Network Model*

Compared with other ITS solutions, LTE-V technology features low cost and rapid deployment [25]. A systematic and integrated solution for V2X communications was generated based on the LTE. We tried to design and develop architecture and the hardware layout of the prototype system. Some telecoms firms, such as Huawei and Datang Telecom, already have a communication system prototype. **Fig. 1** presents the LTE-V, which provides two communication modes:

1) LTE-V-Direct is specially proposed for V2V communications in decentralized architecture. It supports mesh topology and provides direct V2V communication to support road safety applications with low-latency and high-reliability.

2) LTE-V-Cell is the centralized system of LTE-V for supporting V2I communications using star topology. The design philosophy of the LTE-V presented in Fig. 1 aims to maintain reasonable LTE-V-Direct and LTE-V-Cell similarities based on the LTE, thereby resulting in a shared hardware platform between the LTE and LTE-V to achieve cost-effective solutions.

OBU and RSU: The RSU is a wireless communication device that uses the LTE-V. RSUs are located roadside and communicate with vehicles to verify the validity of received messages as well as transfer messages to traffic management centers for local processing. In comparison, OBUs are equipped to support the LTE-V. The OBU is a tamper-proof device (TPD) which never discloses its information. The vehicle communicates wirelessly with RSUs using the OBU.

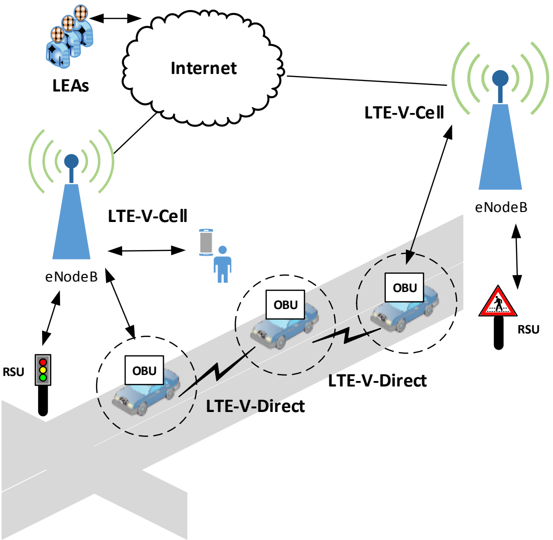


Fig. 1. LTE-V Network Model

3.2 Elliptic Curve Cryptography

Certain important calculation problems are generally observed during the use of elliptic curve groups for designing secure encryption schemes [26].

Problem 1: Computational discrete logarithm (CDL).

Given $R=xP$, where P and $R \in Gp$, R can be calculated given x and P. However, in the case where R and P are given, it is still difficult to determine X.

Problem 2: Computational Diffie-Hellman (CDH).

Given P, xP, and $yP \in Gp$, it is difficult to compute $xyP \in Gp$.

Problem 3: Elliptic curve factorization (ECF).

Given two points, namely P and $R=x \bullet P+y \bullet P$, for $x,y \in Z_q{}^*$, it is difficult to determine $x \bullet P$ and $y \bullet P$.

3.3 Security Goals

Both security and privacy are essential in the maintenance of secure communications in vehicular networks. Under the presented LTE-V network model, we demonstrated three security goals for the communication environment. The security goals of the proposed scheme must be achieved to guarantee the fulfillment of the security requirements, which include:

1) Message authentication. RSUs must be able to check the validity of the messages sent by the OBU. In addition, RSUs must be able to detect any modifications on the received message.

2) Privacy preserving. We essentially defined OBU privacy have been required and applied to achieve anonymity, unlinkability, non-traceability and non-frameability.

(a) Anonymity [27]. The ID-based of the ESMAV must be hidden from normal message receivers in the authentication process.

(b) Unlinkability [28]. The external observer is unable to transmit encrypted information for any positive information during the analysis of traffic information. Adversaries are unable to use individual vehicle tracking to hinder or generate vehicle location privacy problems.

(c) Traceability [29]. A trusted entity can trace an OBU by revealing user identities in cases involving disputed situations such as liability investigations.

(d) Non-frameability [30]. The tracing of misbehaving users and their respective OBUs should not be abused by a single trusted entity. Instead, cooperation between trusted entities must be applied to reveal user identities to minimize the framing of innocent users. A trusted entity or entities (e.g., HSS and LEAs) have the right to verify original information and ensure vehicle information. Controversial information may acquire the assistance of a credible agency to independently recovery the vehicle's true identity.

3) Attack resistance. The ESMAV scheme must be able to resist various LTE-V-based network attacks, including replay attacks, impersonation attacks, modification attacks, redirection attacks, and man-in-the-middle attacks [31].

4. Proposed Scheme: ESMAV

In this section, we describe our proposed scheme in detail. The proposed ESMAV scheme can be used for both V2V and V2I communications. The LTE-V wireless technologies are available to provide the radio interface required by the vehicular communications. There are four phases: the system initialization phase, anonymous identity generation and message signing phase, and the message verification phase and identity tracking. The notations used in the scheme are defined in **Table 1**.

Table 1. Definitions of the scheme notations

Notation	Definition
OBU	On-board unit
HSS	Home subscriber server
RSU	Road side unit
TPD	Tamper-proof device
LEAs	Law enforcement authorities
p, q	Large prime numbers
E	Temporary group key
G	An additive group with the order q, where G contains a point at infinity *O* and all points are on the elliptic curve *E*
Zp	Prime finite field
G_1, G_2	Two elliptic curve groups
P	A generator for group *G*
H_1, H_2, H_3, H_4	Hash function
RID	Real identity of the vehicle

PWD	Password of the TPD
PID	Pseudo-identity of the OBU
P_{pub1}; P_{pub2}	Public key of the HSS
T_i	A time stamp generated by OBU_i
M_i	A message sent by vehicle OBU_i

4.1 System Initialization Phase

The HSS generates the system parameters in the system initialization phase, which are then sent to all RSUs and for TPD pre-loading into each OBU. The HSS first initializes the whole system according to the following steps.

Step 1: The HSS first chooses two large prime numbers *p* and *q*, and a non-singular elliptic curve *E* defined by the equation $y^2 = x^3 + ax + b$ mod *p*, where $a,\ b \in F_p$.

Step 2: The HSS chooses a generator *P* with an order *q* from group G_p . The G_p contains a point at infinity *O* and all points on the elliptic curve *E*.

Step 3: The HSS chooses a random number $s_1,\ s_2 \in Z_q^*$ as the private key of the system and computes the public system key $P_{pub1} = s_1 P$, $P_{pub2} = s_2 P$.

Step 4: The HSS chooses four secure hash functions H_1, H_2, H_3, and H_4, where H_1: $G \times \{0,\ 1\}^* \to Z_q$, H_2:$\{0,\ 1\}* \times G \times G \to Z_q$, H_3: $G \times \{0,\ 1\}^* \times \{0,\ 1\}^* \to Z_q$, and the mapping binary string to integer H_4:$\{0,\ 1\}^* \times \{0,\ 1\}^* \times G \times G \times \{0,\ 1\}^* \to Z_q$.

Step 5: The HSS assigns a real identity *RID* and a password *PWD* for each OBU and pre-loads {*RID, PWD,* s_1, s_2} into its TPD.

Step 6: The HSS sends the system parameters $Paras = \{p, q, a, b, P_{pub1}, P_{pub2}, H_1, H_2, H_3, H_4\}$ to all OBUs and RSUs.

4.2 Pseudo-identity Generation and Message Signing Phase

In this phase, the OBU's TPD generates an anonymous identity and a digital signature for the message. The OBU uses a secure channel to send identities, messages, and signatures to the nearby RSU. This process phase is described in detail as follows.

Step 1: The OBU_i inputs its real identity RID_i and password PWD_i into its TPD. The TPD checks if RID_i and PWD_i are equal to the stored ones. If these are not equal, then the TPD rejects the request.

Step 2: The TPD generates random number $r_1,\ u_2 \in Z_q^*$, and T_i, which is the current timestamp, to compute $R_i = r_i \cdot P$, $U_i = u_i \cdot P$, $PID_i = RID_i \oplus H_1\left(r_i \cdot P_{pub1}\right)$, $H_{r_i} = H_2\left(PID_i \| T_i \| R_i\right)$ $H_{r_i} = H_2\left(PID_i \| T_i \| R_i\right)$, $H_{u_i} = H_3\left(PID_i \| T_i \| U_i\right)$, $SK_i^1 = s_1 \cdot H_{r_i} + r_i \bmod q$, and $SK_i^2 = s_2 \cdot H_{u_i} + u_i \bmod q$. The TPD then gives $\left\{PID_i, R_i, U_i, SK_i^1, SK_i^2, T_i\right\}$ to the OBU.

Step 3: The OBU receives $\left\{PID_i, R_i, U_i, SK_i^1, SK_i^2, T_i\right\}$ and signs the M_i, which is the traffic status message. The message digest $H_i = H_4\left(M_i, PID_i, R_i, U_i, T_i\right)$ and message signature $\sigma_i = SK_i^1 + h_i SK_i^2 \bmod q$ are computed. The OBU then broadcasts $\left\{M_i, PID_i, R_i, U_i, T_i, \sigma_i\right\}$ to the nearby RSU and OBU.

Step 4: For the actual LTE-V scene, Step 1 is executed only once within a given period. The TPD checks success and computes $R_i, U_i, PID_i, T_i, SK_i^1, SK_i^2$ in one period. The OBU uses the PID to send message M_i , thereby generating the corresponding signature $\zeta_i = \{R_i, U_i, \sigma_i\}$.

4.3 Message Verification Phase

In this phase, the RSU or OBU checks the validity of he received messages $\{M_i, PID_i, R_i, U_i, T_i, \sigma_i\}$. The verifier can check the validity of a received message through the traditional verification process. The proposed ESMAV scheme supports batch verification and single verification to stimulate performance enhancement, the process of which is described as follows.

Single verification of one message. Upon receiving a message from the OBU, the verifier uses the system parameters $Paras = \{p, q, a, b, P_{pub1}, P_{pub2}, H_1, H_2, H_3, H_4\}$ to verify the validity of the message.

Step 1: The verifier checks the freshness of T_i. If it is not fresh, the verifier rejects the message.

Step 2: The verifier computes $H_{r_i} = H_2(PID_i \| T_i \| R_i)$, $H_{u_i} = H_3(PID_i \| T_i \| U_i)$, and $H_i = H_4(M_i, PID_i, R_i, U_i, T_i)$.

Step 3: The verifier check the correctness of the single verification of one message.

$$\sigma_i \cdot P = H_{r_i} \cdot P_{pub1} + H_i \cdot H_{u_i} \cdot P_{pub2} + H_i U_i + R_i \tag{1}$$

If it does not hold, the verifier rejects the message. Otherwise, the verifier accepts the message.

Batch verification of multiple messages. In order to improve the verification efficiency and guarantee the non-repudiation of signatures using batch verification, the proposed ESMAV scheme used small exponent test technology [24] for the batch verification of multiple messages. Upon receiving multiple messages $\{M_1, PID_1, R_1, U_1, T_1, \sigma_1\}$, $\{M_2, PID_2, R_2, U_2, T_2, \sigma_2\}, \ldots,$ $\{M_n, PID_n, R_n, U_n, T_n, \sigma_n\}$ from some OBUs, the verifier uses the system parameters $Paras = \{p, q, a, b, P_{pub1}, P_{pub2}, H_1, H_2, H_3, H_4\}$ to verify the validity of these messages as follows.

Step 1: The verifier checks the freshness of T_i, where $i= 1, 2, \cdots, n$. If it is not fresh, the verifier rejects the message.

Step 2: In order to prevent the attacker batch sum, the verifier randomly chooses a vector $\lambda = \{\lambda_1, \lambda_2, \ldots, \lambda_i, \ldots, \lambda_n\}$, where λ_i is a small random integer and $\lambda_i \in [1, 2^t]$, and t is a small integer and has very little computation overhead.

Step 3: The verifier check the correctness of the batch verification of multiple messages.

$$(\sum_{i=1}^{n} \lambda_i \cdot \sigma_i) \cdot P = (\sum_{i=1}^{n} \lambda_i \cdot H_{r_i}) \cdot P_{pub1} + (\sum_{i=1}^{n} \lambda_i \cdot H_i \cdot H_{u_i}) \cdot P_{pub2} + (\sum_{i=1}^{n} \lambda_i \cdot H_i \cdot U_i) + (\sum_{i=1}^{n} \lambda_i \cdot R_i) \tag{2}$$

If it does not hold, the verifier rejects the message. Otherwise, the verifier accepts the message.

4.4 OBU's Real ID Trace Phase

In this phase, a message $\{M_i, PID_i, R_i, U_i, T_i, \sigma_i\}$ that generates dispute requires the assistance and cooperation of law enforcement authorities (LEAs) to trace the real ID of the OBU [32]. The HSS obtains the sender real identity RID_{OBU} as follows.

Step 1: For $r_{i,m}$ corresponding to the LEAs, a polynomial $y_i(x)=\sum_{c=1}^{t} f_i(c)w_c(x)$ is constructed, where $\sum_{c=1}^{t} f_i(c)=r_{i,1}+r_{i,2}+\ldots+r_{i,\ t}$, and $w_c(x)=\prod_{d=1,d\neq c}^{t}\frac{x-d}{c-d}$ is the Lagrange interpolation coefficients.

Step 2: Construct $R_i=y_i(0)=\sum_{c=1}^{t} f_i(c)w_c(0)$.

Step3: Compute the real ID of the OBU as $RID_{OBU}=PID_i\oplus H_1(s_1\cdot R_i)$

Based on the system settings, only the HSS can hold the system private key s_i, thereby allowing HSS extraction of the real ID of the sender.

5. Security Evaluation

In this section, the security objectives of the ESMAV scheme are analyzed. The analysis indicated that the ESMAV scheme can work correctly to achieve these security objectives. In addition, a comparative analysis of functionality was performed against the other relevant schemes, wherein the results indicate that the proposed scheme is secure and efficient for the LTE-V network.

5.1 Proof of Security Objectives

The correctness of the ESMAV scheme is embodied in the signature verification process. It need to prove the validity of equations (1) and (2).

The succeeding steps were followed in accordance with $P_{pub1}=s_1P$, $P_{pub2}=s_2P$, $R_i=r_i\cdot P$, $U_i=u_i\cdot P$, $SK_i^1=s_1\cdot H_{r_i}+r_i \bmod q$, $SK_i^2=s_2\cdot H_{u_i}+u_i \bmod q$, and $\sigma_i=SK_i^1+h_iSK_i^2 \bmod q$.

The single verification in equation (1) for one message is proved as follows:

$$\begin{aligned}\sigma_i\cdot P &= (SK_i^1+H_i\cdot SK_i^2)\cdot P\\ &=(s_1\cdot H_{r_i}+r_i+H_i\cdot(s_2\cdot H_{u_i}+u_i))\cdot P\\ &=H_{r_i}\cdot P_{pub1}+H_i\cdot H_{u_i}\cdot P_{pub2}+H_i\cdot U_i+R_i\end{aligned}$$

The batch verification in equation (2) for multiple messages is proved as follows:

$$\begin{aligned}(\sum_{i=1}^{n}\lambda_i\cdot\sigma_i)\cdot P &= (\sum_{i=1}^{n}\lambda_i\cdot(SK_i^1+H_i\cdot SK_i^2))\cdot P\\ &=(\sum_{i=1}^{n}\lambda_i\cdot(s_1\cdot H_{r_i}+r_i+H_i\cdot(s_2\cdot H_{u_i}+u_i)))\cdot P\\ &=\sum_{i=1}^{n}\lambda_i\cdot(s_1\cdot H_{r_i}\cdot P+r_i\cdot P+H_i\cdot s_2\cdot H_{u_i}\cdot P+H_i\cdot u_i\cdot P)\\ &=\sum_{i=1}^{n}\lambda_i\cdot(H_{r_i}\cdot P_{pub1}+H_i\cdot H_{u_i}\cdot P_{pub2}+H_i\cdot U_i+R_i)\\ &=(\sum_{i=1}^{n}\lambda_i\cdot H_{r_i})\cdot P_{pub1}+(\sum_{i=1}^{n}\lambda_i\cdot H_i\cdot H_{u_i})\cdot P_{pub2}+(\sum_{i=1}^{n}\lambda_i\cdot H_i\cdot U_i)+(\sum_{i=1}^{n}\lambda_i\cdot R_i)\end{aligned}$$

5.2 Security Analysis

In this section, we analyzed the security properties of the proposed ESMAV scheme. Specifically, our analysis focused specifically on the achievement of the above security goals.

Proposition 1. Message authentication

Proof. In the ESMAV, the adversary was not able to forge a valid message given the difficulties of the CDL. The verifier was unable to check the validity and integrity of the message. Verification of the message $\{M_i, PID_i, R_i, U_i, T_i, \sigma_i\}$ validated the equation $\sigma_i \cdot P$. The proposed ID-based ESMAV scheme for LTE-V was validated in terms of its preservation of the authenticated message.

Proposition 2. Preserving identity privacy

Proof. In the ESMAV, the OBU sent messages using random pseudo-identities and random keys. The pseudo-identity consisted of random numbers and a real ID, namely $PID_i = RID_i \oplus H_1(r_1 \cdot P_{pub1})$, given that $P_{pub1} = s_1 P$, $R_i = r_i \cdot P$, $U_i = u_i \cdot P$, $SK_i^1 = s_1 \cdot H_{r_i} + r_i \bmod q$, and $SK_i^2 = s_2 \cdot H_{u_i} + u_i \bmod q$, where r_1, $u_2 \in Z_q^*$ $H_{r_i} = H_2\left(PID_i \| T_i \| R_i\right)$, $H_{u_i} = H_3\left(PID_i \| T_i \| U_i\right)$, and T_i is the current timestamp. The OBU generated different and uncorrelated signatures. In addition, different u_1, r_i, T_i values generate different and uncorrelated pseudo IDs.

Therefore, adversary extraction of the RID from $PID_i = RID_i \oplus H_1(r_i \cdot P_{pub1}) = RID_i \oplus H_1(s_1 \cdot R_i)$ must solve the elliptic CDH problem in accordance with the hardness of the CDH problem, the random oracle model, and unknown s_1, r_i. It is impossible to compute $r_i \cdot P_{pub1}$ or $s_1 \cdot R_i$ in polynomial time. The proposed ID-based ESMAV scheme for LTE-V preserved of the identity privacy of the user.

Proposition 3. Anonymity and unlinkability

Proof. In the ESMAV, each OBU received a pseudo-identities *ID* and their corresponding private keys instead of the OBU's real identity from the HSS at the time of registration. The random number r_i challenged the exposure of OBU's real identity *ID*. This anonymity prevents attackers from tracing the movement history and current location of the OBU.

To generate a message, the TPD in the ESMAV scheme generated two random r_i, $u_i \in Z_q^*$. Given that $SK_i^1 = s_1 \cdot H_{r_i} + r_i \bmod q$, $SK_i^2 = s_2 \cdot H_{u_i} + u_i \bmod q$, and the randomness of r_i and u_i, the adversary is unable to link two anonymous identities or two signatures generated from the same OBU.

Therefore, the proposed ID-based ESMAV scheme for LTE-V preserved the anonymity and unlinkability of the user.

Proposition 4. Traceability and non-frameability

Proof. In the ESMAV, the real identity of the OBU was only disclosed to trusted LEAs that recognized the relationship between the pseudo-identity and the real identity. With the exception of the LEAs, all persons, including the MME, were unable to utilize the acquired ID to trace the OBU's movement route. Tracing the message sender's real identity followed $P_{pub1} = s_1 P$ and $PID_i = RID_i \oplus H_1\left(r_i \cdot P_{pub1}\right)$. The HSS used the private key to extract the real ID by computing $RID_{OBU} = PID_i \oplus H_1(s_1 \cdot R_i)$. The OBU's real ID was found, thereby avoiding the abuse of user privacy preservation by the malicious OBU.

To achieve non-frameability, the LEAs cooperated with each other to trace the real identity of the OBU rather than the single entity such as the HSS or the group manager, thereby eliminating the erroneous prosecution of innocent OBUs by corrupted or abusive entities.

Therefore, the proposed ID-based ESMAV scheme for LTE-V preserved the traceability and non-frameability of the user.

Proposition 5. Resistance to replay attacks

Proof. The ESMAV employed the random parameters produced by the HSS, MME, and OBU. The timestamp T_i was included in the message $\{M_i, PID_i, R_i, U_i, T_i, \sigma_i\}$ and presents a digital signature. The verifier checked the freshness of the T_i. If it is not fresh, the verifier rejects the message. The attacker was provided with a random number for the certification process, though the generation of a challenge message using the random number is still not possible. The ESMAV resisted replay attacks.

Proposition 6. Resistance to man-in-the-middle attacks

Proof. Message authentication was preserved due to ESMAV similarities in the computational CDL problem, thereby providing authentication between the sender and the receiver to withstand man-in-the-middle attacks.

Proposition 7. Resistance to impersonation attacks

Proof. The ESMAV is able to perform mutual authentication in the LTE-V vehicular network. The adversary must generate a message $\{M_i, PID_i, R_i, U_i, T_i, \sigma_i\}$ to impersonate a vehicle to the RSU or other vehicles. Given that it requires the computation of message signature $\sigma_i = SK_i^1 + h_i SK_i^2 \bmod q$, the adversary was unable to generate such messages given that $\sigma_i \cdot P = H_{r_i} \cdot P_{pub1} + H_i \cdot H_{u_i} \cdot P_{pub2} + H_i U_i + R_i$. The RSU and other vehicles were employed to check the validity of $\sigma_i \cdot P$ to withstand the impersonation attacks.

Proposition 8. Resistance to modification attacks

Proof. In the ESMAV, the message $\{M_i, PID_i, R_i, U_i, T_i, \sigma_i\}$ presented a digital signature $\zeta_i = \{R_i, U_i, \sigma_i\}$. If the message is modified, the modified signature $\zeta_i^{'} = \{R_i^{'}, U_i^{'}, \sigma_i^{'}\}$ must check the validity of $\sigma_i \cdot P = (s_1 \cdot H_{r_i} + r_i + H_i \cdot (s_2 \cdot H_{u_i} + u_i)) \cdot P$. Given that the attacker has unknown private keys s_1, s_2, they are unable to compute SK_i^1, SK_i^2 and $\sigma_i^{'} = SK_i^1 + h_i^{'} SK_i^2 \bmod q$ to prevent modification attacks.

5.3 Functionality Comparison

In this section, we compared the functionality of our proposed scheme with some previously schemes. **Table 2** lists the functionality comparisons between the related schemes and the ESMAV scheme. The presented scheme has many excellent features and is more secure than other related schemes. Vehicular networking application modules, which exhibited a high fault tolerance to avoid data loss and machine operation disorders due to the presence of ESMAV without practice in industrial grade and level gauge module products, also did not have industrial grade and level gauge module products. In the same base station of the handover process, the ESMAV can effectively extend the quickly detection and mobile mutual authentication, thereby generating a rapid mobility environment.

According to **Table 2**, none of the schemes satisfied the non-frameability security requirement, namely resistance to common main attacks such as replay attacks, impersonation attacks, modification attacks, redirection attacks, and man-in-the-middle attacks. The other schemes were unable to fulfill the security requirements in the LTE-V.

Table 2. Functionality comparison between the related schemes and our scheme

Function	Lee's scheme [15]	Zhang's scheme [16]	Bayat's scheme [17]	EIMA
Message authentication	Yes	Yes	Yes	Yes
Preservation privacy	Yes	Yes	Yes	Yes
Anonymity	Yes	Yes	Yes	Yes
Unlinkability	Yes	Yes	Yes	Yes
Resistant Man-in-the-Middle attack	Yes	Yes	Yes	Yes
Resist impersonation attack	Yes	Yes	Yes	Yes
Resist modification attack	Yes	Yes	Yes	Yes
Resistant replay attacks	No	Yes	Yes	Yes
Traceability	No	Yes	Yes	Yes
Non-frameability	No	No	No	Yes

6. Performance Analysis

This section calculated the ESMAV scheme in the communication and computation overhead in accordance with the presented literature. Lee's scheme [21], Zhang's scheme [22], Bayat's scheme [23], and He's scheme [24] used different authentication calculation methods. For convenience, we built a security different level for the 80-bit operation scheme. For the bilinear pairings, we used a bilinear pairings $e: G_1 \times G_1 \to G_2$ to achieve the security level. The G_1 is an additive group that was generated by a point $\bar{P}$ with an order $\bar{q}$. The point $\bar{P}$ is degree 2 from the super singular elliptic curve $\bar{E}: y^2 = x^3 + x \bmod \bar{p}$, where $\bar{P}$ is a 512-bit prime number, $\bar{q}$ is a 160-bit prime number, and $\bar{q} = 2^{159} + 2^{17} + 1$. For the ECC, the present study used an additive group G to achieve the security level, thereby generating a point P with an order q. Point P is on the non-singular elliptic curve $E: y^2 = x^3 + ax + b \bmod p$, where p and q are two 160-bit prime numbers, and $a, b \in Z_P^*$. We computed the execution time of the above cryptographic operations using MIRACL [33]. The MIRACL library is a famous cryptographic operations library and has been widely used to implement cryptographic operations in many environments.

The present study defined some notations about the execution time for the analysis of the computational and communication overheads. The execution time of the cryptographic operations are listed in **Table 3**. Our hardware platform consisted of an Intel Core E5-1607 processor with a 3.00 GHz clock frequency, 32 gigabytes of memory on a Windows 7 operating system.

Table 3. Cryptographic operations list

Name		Cryptographic operations	Execution time(ms)
Bilinear Pairing	Bilinear pairing operation	T_{bp}	4.9622
	Scale multiplication operation	T_{bm}	2.1242
	Small factor multiplication operation	T_{bsm}	0.2264
	Point addition operation	T_{ba}	0.0102
Elliptic Curve Cryptography	Scale multiplication operation	T_{em}	0.5622
	Small scale multiplication operation	T_{esm}	0.0336
	Point addition operation	T_{ea}	0.0028
General hash function operation		T_h	0.0002
Map-to-point operation		T_{mtp}	3.286

6.1 Communications Overhead

The communication overhead of the ESMAV was analyzed and compared with the other schemes using a similar calculation method for the performance comparison. **Table 4** demonstrates the major benefit of the proposed ESMAV scheme in the signature process, the single verification of one message, and the batch verification of multiple messages.

Table 4. Comparison of communication overhead

	Signature process	**Single verification of one message**	**Batch verification of multiple Messages**
Lee's scheme [21]	$1T_{bm}+1T_{ba}+2T_{mtp}+1T_h$ ≈ 8.7066ms	$3T_{bp}+1T_{bm}+1T_{mtp}+1T_h$ ≈ 20.297ms	$3T_{bp}+nT_{bm}+3(n\text{-}1)T_{ba}+nT_{mtp}+nT_h \approx$ $(3.3168n+14.856)$ms
Zhang's scheme [22]	$6T_{bm}+2T_{ba}+1T_{mtp}+4T_h$ ≈ 16.0524ms	$3T_{bp}+2T_{bm}+1T_{ba}+3T_h$ ≈ 19.1458ms	$3T_{bp}+(n+1)T_{bm}+2nT_{bsm}+(3n\text{-}2)T_{ba}$ $+3nT_h$ $\approx (2.6082n+16.9904)$ms
Bayat's scheme [23]	$5T_{bm}+1T_{ba}+1T_{mtp}+5T_{hB}$ ≈ 13.9182ms	$3T_{bp}+1T_{bm}+1T_{mtp}+1T_h$ ≈ 20.297ms	$3T_{bp}+nT_{bsm}+3(n\text{-}1)T_{ba}+nT_{mtp}+nT_h$ $\approx (3.5432n+14.856)$ms
He's scheme [24]	$3T_{em}+3T_h$ ≈ 1.6872ms	$3T_{em}+2T_{ea}+2T_h$ ≈ 1.6926ms	$(n+2)T_{em}+2nT_{esm}+(3n\text{-}1)T_{ea}+2nT_h$ $\approx (0.6382n+1.1216)$ms
ESMAV	$3T_{em}+4T_h$ ≈ 1.6874ms	$3T_{em}+3T_{ea}+3T_h$ ≈ 1.6956ms	$(n+3)T_{em}+nT_{esm}+(2n+1)T_{ea}+3nT_h$ $\approx (0.602n+1.6894)$ms

According to **Table 4**, for the signature process, Lee's scheme [21] required the execution of one scale multiplication operation related to bilinear pairing, one point addition operation related to bilinear pairing, two map-to-point operations related to bilinear pairing, and one general hash function operation related to the bilinear pairing for a total execution time of $1T_{bm}+1T_{ba}+2T_{mtp}+1T_h \approx 8.7066$ ms. Zhang's scheme [22] required the execution of six scale multiplication operations related to bilinear pairing, two point addition operations related to bilinear pairing, one map-to-point operation related to bilinear pairing, and four general hash function operations related to bilinear pairing for a total execution time of $6T_{bm}+2T_{ba}+1T_{mtp}+4T_h \approx 16.0524$ ms. Bayat's scheme [23] required the execution of five scale multiplication operations related to bilinear pairing, one point addition operation related to bilinear pairing, one map-to-point operation related to bilinear pairing, and five general hash function operations related to bilinear pairing for a total execution time of $5T_{bm}+1T_{ba}+1T_{mtp}+5T_{hB} \approx 13.9182$ ms. He's scheme [24] requires the execution of three scale multiplication operations related to elliptic curve cryptography and three general hash function operations for a total execution time of $3T_{em}+3T_h \approx 1.6872$ ms. The proposed ESMAV scheme required the execution of three scale multiplication operations related to elliptic curve cryptography and four general hash function operations for a total execution time of $3T_{em}+4T_h \approx 1.6872$ ms. The presented scheme exhibited the highest improvement in terms of the total execution time. The percentage improvement with the signature process step of the ESMAV scheme over Lee's scheme [21] for the total execution time was about 80.6%. In addition, an improvement of 89.5% and 87.9% was observed as compared to Zhang's [22] and Bayat's schemes [23], respectively.

For the single verification of one message, Lee's scheme [21] required the execution of three bilinear pairing operations related to bilinear pairing, one scale multiplication operation related to bilinear pairing, one map-to-point operation related to bilinear pairing, and one general hash function operation related to bilinear pairing for a total execution time of $3T_{bp}+1T_{bm}+1T_{mtp}+1T_{h}\approx20.297$ ms. Zhang's scheme [22] required the execution of three bilinear pairing operations related to bilinear pairing, two scale multiplication operations related to bilinear pairing, one point addition operation related to bilinear pairing, and one general hash function operation related to bilinear pairing for a total execution time of $3T_{bp}+2T_{bm}+1T_{ba}+3T_{h}\approx19.1458$ ms. Bayat's scheme [23] required the execution of three bilinear pairing operations related to bilinear pairing, one scale multiplication operation related to bilinear pairing, one map-to-point operation related to bilinear pairing, and one general hash function operation related to bilinear pairing for a total execution time of $3T_{bp}+1T_{bm}+1T_{mtp}+1T_{h}\approx20.297$ ms. He's scheme [24] required the execution of two scale multiplication operations related to elliptic curve cryptography, two point addition operations related to elliptic curve cryptography, and two general hash function operations for a total execution time of $3T_{em}+2T_{ea}+2T_{h}\approx1.6926$ ms. The proposed ESMAV scheme required the execution of two scale multiplication operations related to elliptic curve cryptography, three-point addition operations related to elliptic curve cryptography, and three general hash function operations for a total execution time of $3T_{em}+3T_{ea}+3T_{h}\approx1.6956$ ms. The presented scheme exhibited the high total execution time improvement. The ESMAV scheme exhibited an about 91.6%percentage improvement for the single verification of one message step over Lee's scheme [21]. In addition, an improvement of 91.1% and 91.6% was observed as compared to Zhang's [22] and Bayat's schemes [23], respectively.

For the batch verification of multiple messages, Lee's scheme [21] required the execution of three bilinear pairing operations related to bilinear pairing, (*n*) scale multiplication operations related to bilinear pairing, 3(n-1) point addition operations related to bilinear pairing, (*n*) map-to-point operations related to bilinear pairing, and (*n*) general hash function operations related to bilinear pairing for an execution time of $3T_{bp}+nT_{bm}+3(n-1)T_{ba}+nT_{mtp}+nT_{h}\approx(3.3168n + 14.856)$ ms. Zhang's scheme [22] required the execution of three bilinear pairing operations related to bilinear pairing, (n+1) scale multiplication operations related to bilinear pairing, (2*n*) small factor multiplication operation related to bilinear pairing, (3n-2) point addition operation related to bilinear pairing, and (3*n*) general hash function operation related to bilinear pairing for a total execution time of $3T_{bp}+(n+1)T_{bm}+ 2nT_{bsm}+(3n-2)T_{ba} +3nT_{h}\approx(2.6082n+16.9904)$ ms. Bayat's scheme [23] required the execution of three bilinear pairing operations related to bilinear pairing, (*n*) scale multiplication operations related to bilinear pairing, 3(n-1) point addition operations related to elliptic curve cryptography, (*n*) map-to-point operations, and (*n*) general hash function operations related to bilinear pairing for a total execution time of $3T_{bp}+ nT_{bsm}+3(n-1)T_{ba}+nT_{mtp}+nT_{h}\approx(3.5432n+14.856)$ ms. He's scheme [24] required the execution of (n+2) scale multiplication operations related to elliptic curve cryptography, small-scale multiplication operations related to elliptic curve cryptography, (3n-1) point addition operations related to elliptic curve cryptography, and (2*n*) general hash function operations for a total execution time of $(n+2)T_{em}+2nT_{esm}+(3n-1)T_{ea}+2nT_{h}\approx(0.6382n+1.1216)$ ms. The proposed ESMAV scheme required the execution of execute (n+3) scale multiplication operations related to elliptic curve cryptography, (n) point addition operations related to elliptic curve cryptography, (2n+1) point addition operations related to elliptic curve cryptography, and (3*n*) general hash function operations for a total execution time of

$(n+3)T_{em}+nT_{esm}+(2n+1)T_{ea}+3nT_{h}\approx(0.602n+1.6894)$ ms. The present scheme exhibited the highest total execution time improvement. A comparison of the execution times for the batch verification of multiple messages is presented in **Fig. 2**, wherein the curve with the circle denotes Lee's scheme [21], the curve with the triangle denotes Zhang's scheme [22], the curve with the square represents Bayat's scheme [23], the curve with the asterisk denote He's scheme [24], and the curve with the line denotes the presented ESMAV. The ESMAV scheme exhibited an about 84.8% percentage improvement as compared to Lee's scheme [21] for the total execution time. In addition, an improvement of about 83%, 85.4%, and 0.05% was observed as compared to Zhang's [22], Bayat's [23], and He's schemes [24], respectively.

Therefore, based on the results shown in **Table 4** and **Fig. 2**, the proposed ESMAV scheme for LTE-V exhibited a lower computation overhead as compared to recent schemes.

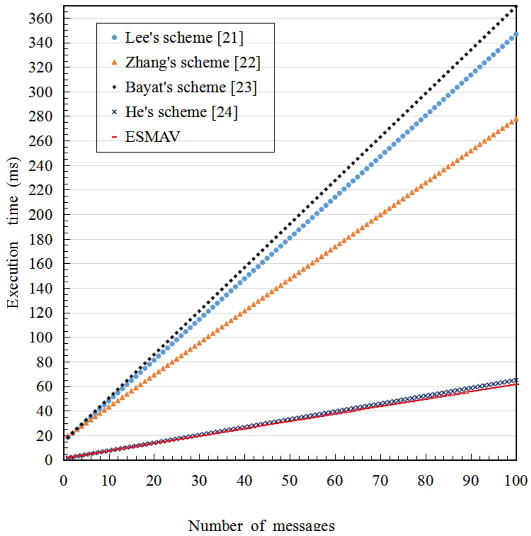


Fig. 2. Execution time for the batch verification of multiple messages

6.2 Computational Cost

The computational cost of the ESMAV was analyzed and compared with the other schemes. Given that the sizes of p and $\bar{p}$ were measured to be 20 bytes (160 bits) and 64 bytes (512 bits), respectively, the sizes of the elements in G1 and G were measured at $20\times2=40$ bytes and $64\times2=128$ bytes, respectively. Moreover, the sizes of the real ID, the general hash function's H output, and the timestamp T were measured to be 20 bytes, 20 bytes, and 4 bytes, respectively. The computational cost is presented in **Table 5**.

Table 5. Comparison of computational cost

	Sending a single message	**Sending n message**
Lee's scheme [21]	276 bytes	276 n bytes
Zhang's scheme [22]	388 bytes	388 n bytes
Bayat's scheme [23]	388 bytes	388 n bytes
He's scheme [24]	144 bytes	144 n bytes
ESMAV	124 bytes	124 n bytes

Lee's scheme [21] broadcasted $\{M_i, ID_i^1, ID_i^2, \sigma_i\}$ to the verifier, wherein $ID_i^1, \sigma_i \in G_1$ and $ID_i^2 = RID \oplus H(r \cdot P_{pub1})$. In addition, Lee's scheme presented a communication cost of 128*2+20=276 bytes. Zhang's [22] and Bayat's schemes [23] broadcasted $\{M_i, AID_i, T_i, U_i\}$ to the verifier, wherein $AID_i = \{AID_i^1, AID_i^2\}$, $AID_i^1, AID_i^2, U_i \in G_1$, and T_i is the timestamp. Zhang's and Bayat's schemes presented a communication cost of 128*3+4=388 bytes. He's scheme [24] broadcasted $\{M_i, AID_i, R_i, T_i, \sigma_i\}$ to the verifier, wherein $AID_i = \{AID_i^1, AID_i^2\}$, $AID_i^1, AID_i^2, R_i \in G$, $\sigma_i \in Z_q$, and T_i is the timestamp. He's scheme exhibited a communication cost of 40*3+20+4=144 bytes. The presented ESMAV scheme broadcasted the anonymous identity and signature $\{M_i, PID_i, R_i, U_i, T_i, \sigma_i\}$ to the verifier, where $U_i, R_i \in G$, $\sigma_i, PID_i \in Z_q$, $PID_i = RID_i \oplus H(r \cdot P_{pub1})$, and T_i is the timestamp for a communication cost of 40*2+20+20+4=124 bytes.

Therefore, the proposed ESMAV scheme exhibited a lower communication cost as compared to the recent schemes.

6.3 Simulation results and analysis

In this section, we evaluated the whole latency performance, including the computation and communication cost, to simulate the schemes on the LTE topology by the NS-3.25 network simulator on the 64-bit, 3.00 GHz, Intel Core E5-1607 processor. In the simulation, we enabled the execution of x2-based interface that was configured between the OBU and RSU. The values of the simulation parameters are presented in **Table 6**.

Fig. 3 presents the variations in the message delays with the number of the OBU, wherein the curve with the circle denotes Lee's scheme [21], the curve with the triangle denotes Zhang's scheme [22], the curve with the square denotes Bayat's scheme [23], the curve with the asterisk denotes He's scheme [24], and the curve with the line denotes the presented ESMAV. **Fig. 3** presents a comparison of the messages delay with the number of OBUs, wherein the presented scheme exhibited an obvious advantage as compared to Lee's, Zhang's, and Bayat's schemes. The ESMAV also exhibited a high vehicle density advantage as compared to He's scheme. In addition, the ESMAV provided robust privacy preservation, including anonymity, unlinkability, traceability, and non-frameability.

Table 6. The value of the simulation parameters

Parameters	**Values**
Road length	20 km
Multilane highway	4
RSU installation distance	1 km
RSU communication range	700 m
RSU transmission power	30 dB
OBU communication range	300 m
OBU broadcasts timespan	200 ms
OBU transmission power	10 dB
Connection bandwidth	100 Gps
Vehicle's speed	(30-90) km/h
Vehicle density	(1-30) pcu/ 100 m

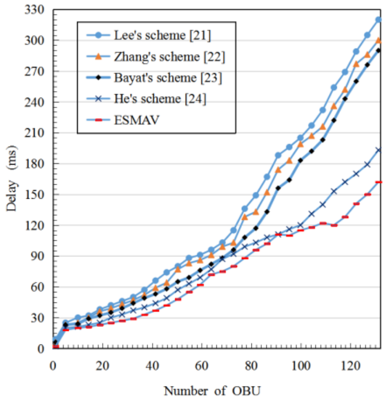


Fig. 3. Comparison of the message delays with the number of OBUs

The simulation results verified the applicability of the presented scheme in further reducing message delays, thereby improving the performance of the vehicular network.

Consideration of the performance of ESMAV can be achieved in the real environment. LTE-V is based on the cellular communication system, which does not require dedicated road side equipment and dedicated spectrum. The ESMAV in the LTE-V environment can reuse the existing honeycomb infrastructure and simplify the construction of the base station. In terms of application difficulty, the LTE-V can be conducted on existing cellular communication systems and an upgrade can be added on a small-scale environment, thereby eliminating the requirement of a large number of infrastructure communication modules. The ESMAV can provide a wide range of cellular application bases and operators to provide security. In terms of the scope of the application, the car network demand for communication technology is a short in terms of its low delay. In addition, more real-time wide coverage network can be guaranteed based on the existing cellular technology upgrade of LTE-V, which has more advantages.

7. Conclusion

The present study proposed an efficient identity-based message authentication scheme, which included the function on non-repudiation for simple and batch messages for enhanced performance. As compared to existing schemes, the proposed ESMAV scheme greatly reduced the amount of signal exchanges between massive vehicles and the network. The security evaluation and performance analysis also exhibited its robust security functions, which include privacy preservation, resistance to various attacks, non-frameability, and non-repudiation verification. In addition, the presented ESMAV exhibited outstanding performance as compared to existing solutions.

Acknowledgements

This work has been supported by Project U1603261 supported by Joint Funds of National Natural Science Foundation of China and Xinjiang, the National Natural Science Foundation of China (Grant No. 61602055) and the Project of High-level Teachers in Beijing Municipal Universities in the Period of 13th Five-Year Plan (IDHT20170511).

References

[1] J. Cao, M. Ma, H. Li, Y. Zhang, and Z. Luo, "A Survey on Security Aspects for LTE and LTE-A Networks," *Communications Surveys & Tutorials IEEE*, vol. 16, pp. 283-302, 2014. Article (CrossRef Link)

[2] J. Cheng, J. Cheng, M. Zhou, F. Liu, S. Gao, and C. Liu, "Routing in Internet of Vehicles: A Review," *IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS*, vol. 16, pp. 2339-2352, 2015. Article (CrossRef Link)

[3] M. H. Lin and Y. W. Chen, "Performance Analysis of Buffer Aware Scheduling for Video Services in LTE Network," *KSII Transactions on Internet & Information Systems*, vol. 9, pp. 3594-3610, 2015. Article (CrossRef Link)

[4] D. He, S. Chan and M. Guizani, "Securing software defined wireless networks," *IEEE Communications Magazine*, vol. 54, pp. 20-25, 2016. Article (CrossRef Link)

[5] G. Araniti, C. Campolo, M. Condoluci, A. Iera, and A. Molinaro, "LTE for Vehicular Networking: A Survey," *IEEE COMMUNICATIONS MAGAZINE*, vol. 51, pp. 148-157, 2013. Article (CrossRef Link)

[6] D. P. Van, B. P. Rimal, S. Andreev, and T. Tirronen, "Machine-to-Machine Communications Over FiWi Enhanced LTE Networks: A Power-Saving Framework and End-to-End Performance," *Journal of Lightwave Technology*, vol. 34, pp. 1062-1071, 2016. Article (CrossRef Link)

[7] K. Kanwal and G. A. Safdar, "Reduced Early Handover for Energy Saving in LTE Networks," *Communications Letters IEEE*, vol. 20, pp. 153-156, 2016. Article (CrossRef Link)

[8] M. Condoluci, M. Dohler, G. Araniti, and A. Molinaro, "Enhanced Radio Access and Data Transmission Procedures Facilitating Industry-Compliant Machine-Type Communications over LTE-Based 5G Networks," *IEEE Wireless Communications*, vol. 23, pp. 56-63, 2016. Article (CrossRef Link)

[9] R. Hemajanani, R. Perumalraja and S. Chowmya, "Software defined LTE vehicular network," *International Journal of Applied Engineering Research*, vol. 10, pp. 1812-1816, 2015. Article (CrossRef Link)

[10] T. H. Chuang, M. H. Tsai and C. Y. Chuang, "Group-Based Uplink Scheduling for Machine-Type Communications in LTE-Advanced Networks," in *Proc. of IEEE International Conference on Advanced Information NETWORKING and Applications Workshops*, 2015, pp. 652-657. Article (CrossRef Link)

[11] D. Choi, H. K. Choi and S. Y. Lee, "A group-based security protocol for machine-type communications in LTE-advanced," *Wireless Networks*, vol. 21, pp. 405-419, 2015. Article (CrossRef Link)

[12] C. Lai, H. Li, R. Lu, and X. Shen, "SE-AKA: A secure and efficient group authentication and key agreement protocol for LTE networks," *Computer Networks*, vol. 57, pp. 3492-3510, 2013. Article (CrossRef Link)

[13] C. Lai, H. Li, R. Lu, and R. Jiang, "LGTH: A lightweight group authentication protocol for machine-type communication in LTE networks," in *Proc. of GLOBECOM 2013 - 2013 IEEE Global Communications Conference*, 2013, pp. 832-837. Article (CrossRef Link)

[14] C. Lai, R. Lu, D. Zheng, H. Li, and X. Shen, "GLARM: Group-based Lightweight Authentication Scheme for Resource-constrained Machine to Machine Communications," *Computer Networks*, vol. 99, pp. 66-81, 2016. Article (CrossRef Link)

[15] P. Sindhuja, Y. Kuwahara, K. Kumaki, and Y. Hiramatsu, "A Design of Vehicular GPS and LTE Antenna Considering Vehicular Body Effects," *Ieice Transactions on Communications*, vol. 99, 2016. Article (CrossRef Link)

[16] W. Li, X. Ma, J. Wu, K. S. Trivedi, and X. L. Huang, "Analytically Modelling and Performance Evaluation of Long Term Evolution for Vehicle (LTE-V) Safety Services," *IEEE Transactions on Vehicular Technology*, 2016. Article (CrossRef Link)

[17] A. Fu, J. Song, S. Li, G. Zhang, and Y. Zhang, "A privacy-preserving group authentication protocol for machine-type communication in LTE/LTE-A networks," *Security & Communication Networks*, vol. 9, pp. 2002-2014, 2016. Article (CrossRef Link)

[18] Y. Qiu, M. Ma and X. Wang, "A proxy signature-based handover authentication scheme for LTE wireless networks," *Journal of Network & Computer Applications*, vol. 83, pp. 63-71, 2017. Article (CrossRef Link)

[19] Y. Xie, L. B. Wu, J. Shen, and A. Alelaiwi, "EIAS-CP: new efficient identity-based authentication scheme with conditional privacy-preserving for VANETs," *Telecommunication Systems*, pp. 1-12, 2016. Article (CrossRef Link)

[20] K. A. Shim, "CPAS:An Efficient Conditional Privacy-Preserving Authentication Scheme for Vehicular Sensor Networks," *IEEE Transactions on Vehicular Technology*, vol. 61, pp. 1874-1883, 2012. Article (CrossRef Link)

[21] C. C. Lee and Y. M. Lai, "Toward a secure batch verification with group testing for VANET," *Wireless Networks*, vol. 19, pp. 1441-1449, 2013. Article (CrossRef Link)

[22] Z. Jianhong, X. Min and L. Liying, "On the security of a secure batch verification with group testing for VANET," *International Journal of Network Security*, vol. 16, pp. 355-362, 2014. Article (CrossRef Link)

[23] M. Bayat, M. Barmshoory, M. Rahimi, and M. R. Aref, "A secure authentication scheme for VANETs with batch verification," *Wireless Networks*, vol. 21, pp. 1-11, 2015. Article (CrossRef Link)

[24] D. He, S. Zeadally, B. Xu, and X. Huang, "An Efficient Identity-Based Conditional Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks," *IEEE Transactions on Information Forensics & Security*, vol. 10, p. 1-1, 2015. Article (CrossRef Link)

[25] S. Chen, J. Hu, Y. Shi, and L. Zhao, "LTE-V: A TD-LTE based V2X Solution for Future Vehicular Network," *IEEE Internet of Things Journal*, vol. PP, p. 1-1, 2016. Article (CrossRef Link)

[26] Y. L. Tseng, "LTE-Advanced enhancement for vehicular communication," *IEEE Wireless Communications*, vol. 22, pp. 4-7, 2015. Article (CrossRef Link)

[27] C. K. Han and H. K. Choi, "Security Analysis of Handover Key Management in 4G LTE/SAE Networks," *IEEE Transactions on Mobile Computing*, vol. 13, pp. 457-468, 2014. Article (CrossRef Link)

[28] J. Calabuig, J. F. Monserrat, D. Gozalvez, and O. Klemp, "Safety on the Roads: LTE Alternatives for Sending ITS Messages," *Vehicular Technology Magazine IEEE*, vol. 9, pp. 61-70, 2014. Article (CrossRef Link)

[29] T. Yang, C. Lai, R. Lu, and R. Jiang, "EAPSG: Efficient authentication protocol for secure group communications in maritime wideband communication networks," *Peer-to-Peer Networking and Applications*, vol. 8, pp. 216-228, 2015. Article (CrossRef Link)

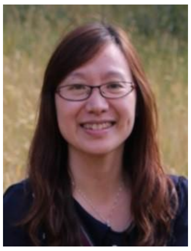
[30] X. Duan and X. Wang, "Authentication handover and privacy protection in 5G hetnets using software-defined networking," *IEEE Communications Magazine*, vol. 53, pp. 28-35, 2015. Article (CrossRef Link)

[31] A. G. Gotsis, A. S. Lioumpas and A. Alexiou, "M2M Scheduling over LTE: Challenges and new Perspectives," *IEEE Vehicular Technology Magazine*, vol. 7, pp. 34-39, 2012. Article (CrossRef Link)

[32] A. Fu, N. Qin, Y. Wang, Q. Li, and G. Zhang, "Nframe : A privacy-preserving with non-frameability handover authentication protocol based on (t , n) secret sharing for LTE/LTE-A networks," *Wireless Networks*, pp. 1-12, 2016. Article (CrossRef Link)

[33] MIRACL Library, 2017. Article (CrossRef Link)

Cheng Xu is currently a Ph.D. at the Institute of Network Technology in the Beijing University of Posts and Telecommunications (BUPT), China. His research interests include wireless security and the internet capacity of vehicles.



Xiaohong Huang, corresponding author, received her B.E. degree from Beijing University of Posts and Telecommunications (BUPT), Beijing, China, in 2000 and Ph.D. degree from the school of Electrical and Electronic Engineering (EEE), Nanyang Technological University, Singapore in 2005. Since 2005, Dr. Huang has joined BUPT and now she is an associate professor and director of Network and Information Center in Institute of Network Technology of BUPT. Dr. Huang has published more than 50 academic papers in the area of WDM optical networks, IP networks and other related fields. Her current interests are optimization of computer networks, network security and so on.

Maode Ma, received his Ph.D. degree in computer science from the Hong Kong University of Science and Technology, Hong Kong, China, in 1999. He is currently an Associate Professor with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore. He has extensive research interests, including network security and wireless networking. He has more than 300 international academic publications, including more than 130 journal papers and more than 160 conference papers. Dr. Ma is a Fellow of the IET and a senior member of the IEEE Communications and Education Societies. He is the Chair of the IEEE Education Society, Singapore Chapter.

Hong Bao, received his Ph.D. degree from the School of Computer and Information Technology, Beijing Jiao Tong University, Beijing, China. He is a professor at the Beijing Union University. His current research interests include intelligent control and intelligent vehicles.