Received: 7 November 2017 | Revised: 21 December 2017 | Accepted: 22 December 2017

DOI: 10.1002/itl2.25

LETTER

WILEY

# Anonymous Group Message Authentication Protocol for LTE-based V2X Communications

**Dongxiao Liu**[1] | **Jianbing Ni**[1] | **Xiaodong Lin**[2] | **Xuemin (Sherman) Shen**[1]

[1]Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Canada N2L 3G1

[2]Department of Physics and Computer Science, Wilfrid Laurier University, Waterloo, Canada N2L 3C5

**Correspondence**

Dongxiao Liu, Department of Electrical and Computer Engineering, University of Waterloo, Waterloo Canada N2L 3G1

Email: dongxiao.liu@uwaterloo.ca

Cellular technologies, in particular the current long-term evolution (LTE) and future 5G, are suitable for implementing vehicle-to-everything (V2X) services, due to the existing network infrastructure, device-to-device (D2D) communication capability, and guaranteed end-to-end delay. In LTE-based V2X (LTE-V), vehicle grouping plays an important role for improving LTE spectrum utilization and providing group-oriented proximity-based services (ProSe). However, the flourishing of LTE-V group communications introduces unique privacy challenges. In this letter, the state-of-art standardization and research efforts are first reviewed, and their limitations are identified on achieving trajectory privacy for LTE-V group communications. Then, an efficient and anonymous group message authentication protocol is proposed to support message batch verification. Security analysis and performance evaluation demonstrate the feasibility of the proposed protocol.

**KEYWORDS**

group communications, long-term evolution (LTE), proximity-based services (ProSe), vehicle-to-everything (V2X)

## 1 | INTRODUCTION

Vehicle-to-everything (V2X) refers to a set of technologies that enables ubiquitous wireless connectivity between vehicles and: other vehicles (V2V), the infrastructure (V2I), pedestrians (V2P), and network (V2N). These technologies allow for a variety of vehicular applications, for example, forward collision warning, automated parking system, and realtime traffic monitoring, to enhance better road safety and reduce potential traffic congestion.[1] Due to the advantages, V2X has been attracting the attention of both industry and academia.

One of the main proposals for V2X communications is wireless access in vehicular environment (WAVE), which is based on the dedicated short-range communication (DSRC) protocol and the IEEE 802.11 standard, and operates in a spectrum of 75 MHz at 5.9 GHz.[2] Using WAVE, vehicles equipped with on-board units (OBUs) can communicate with roadside units (RSUs) and nearby vehicles to exchange realtime traffic messages. However, as a distributed communication solution, WAVE-based vehicular communication faces many problems and challenges when putting it into practice. First, the communication coverage of vehicles is limited and will be seriously affected by hidden terminal problem.[3] A vehicle with a high speed has short time for data transmission, thus leading to low data throughput.[4] Second, the performance of the IEEE 802.11 standard with the increased vehicle density is poor.[3] Third, deployment cost of RSUs is huge and the business model of WAVE is not clear.

To resolve these issues, automotive industry and academia are moving aggressively in the direction of cellular infrastructures for V2X communications. The 3rd Generation Partnership Project (3GPP) suggests long-term evolution (LTE) for V2X services,[5] which is well developed to support generalized mobile data services and reliable centralized control function in 4G networks.[6] LTE-based V2X, referred to as LTE-V, can dramatically enhance communication range with high capability on device density and data throughput, and reduce the deployment cost with ubiquitous vehicular communications. Recently, the 3GPP included proximity-based services (ProSe), which is based on ProSe device-to-device (D2D) direct communications and has been updated to its Release 15,[7] to support direct V2 V communications. Different from self-organized DSRC, ProSe uses

  

a dedicated spectrum, whose utilization and allocation are fully under the control of the LTE core network. LTE-V centralized and efficient bandwidth allocation and reuse is a good fit for V2X communication reliability and efficiency requirements. In order to improve overall LTE spectrum utilization, user equipment (UE) can form different groups for spectrum allocation. Moreover, by enabling direct communications within the same group, it can also open up new commercial opportunities and emerging group-oriented applications,[8] such as localized advertising and proximity-based social networking.

While LTE-V group communication brings tremendous benefits, there still remain many technical challenges to be addressed, in particular in the security and privacy space. Essential and well-recognized security features in V2X group communications are confidentiality, integrity, and accountability (nonrepudiation). In 3GPP specification,[9] after registered at a base station using international mobile subscriber identity (IMSI), all connected devices (referred to as UE in 3GPP terminology) within a same group will be assigned with a common group ID, carrier frequency, and group key for traffic encryption and decryption. In order to achieve anonymity for UE credential provisioning, each UE will be assigned with a pseudonym (referred as the group identity in Reference 10) based temporary credential, which is derived from a pseudonym-based certificate or using identity-based signature. Unfortunately, both the group ID and UEs' pseudonyms are transmitted in the clear, when UEs exchange messages with each other. As a result, an adversary can easily intercept transmitted messages in the wireless channel. By sniffing and linking messages with the same group identity in different sessions, an adversary can further detect trajectories of a targeted UE. That is, trajectory privacy of UE is not guaranteed in the proposed standard.

In this letter, the UE trajectory privacy in LTE-V group communications is carefully studied. Through identifying limitations of existing standardization and research efforts, an anonymous group message authentication protocol is proposed with efficient message batch verification. The contributions of this letter can be summarized as follows:

- Hybrid message authentication: By leveraging message authentication code (MAC) and short group signature, a versatile message authentication protocol is designed that can be applied to different group-oriented applications.
- Secure and efficient protocol: Compared with existing work[9,11] for LTE-V group communications, the proposed protocol first achieves UE trajectory privacy. Moreover, a newly designed batch verification technique is proposed to improve message verification efficiency. Security discussions and extensive experiment results demonstrate the feasibility of the proposed protocol.

The remainder of this letter is organized as follows. First, a comprehensive overview of 3GPP LTE-V group communications is presented and its key security and privacy challenges are identified. Then, some off-the-shelf privacy-preserving methods are reviewed from both the academia and industry to discuss their limitations when applied to LTE-V. At last, an anonymous and efficient group message authentication protocol is proposed for LTE-V and the feasibility of the proposed protocol is demonstrated.

## 2 | OVERVIEW OF LTE-V GROUP COMMUNICATIONS

### 2.1 | LTE-V architecture

LTE-V architecture mainly consists of 4 parts: vehicles, (ie, UEs), radio access networks (RAN), LTE core networks (referred to as evolved packet core, EPC), and application servers (AS), as shown in Figure 1. UEs can be OBUs on vehicles, or mobile devices carried by pedestrians with an IMSI for subscription services. RAN is the radio access interface between UEs and EPC. EPC has several main components: mobility management entity (MME), home subscriber server (HSS), serving gateway (S-GW), and Packet Data Network (PDN) gateway (P-GW). HSS is a database storing UE-related information. MME is the main signaling node in EPC. S-GW routes and forwards UE data packets and P-GW helps UE to establish connections with external IP networks, that usually refers to the Internet, to provide UEs with connectivity, through which they can access applications, provided by AS.

### 2.2 | Group communications in LTE-V

UE grouping is a basic and essential part for LTE-V group communications. From the perspective of spectrum utilization, UE grouping is for the design of efficient cellular radio resource management which is under control of EPC. There are 2 modes of radio resource management. In dedicated mode, UEs utilize some dedicated spectrum to avoid interference, which can be used by safety-related applications. In reuse mode, UEs reuse radio resources of the LTE air interface.

From perspective of applications, AS can provide a variety of applications for UEs, such as proximity-based social networking or information sharing. AS publish application information to EPC to apply for radio resources. Considering applications priority, EPC allocates radio resources to each application and builds a virtual secure group to manage the UEs who access the application. A UE can be assigned to several application groups according to its preferences. To join a service group, the UE

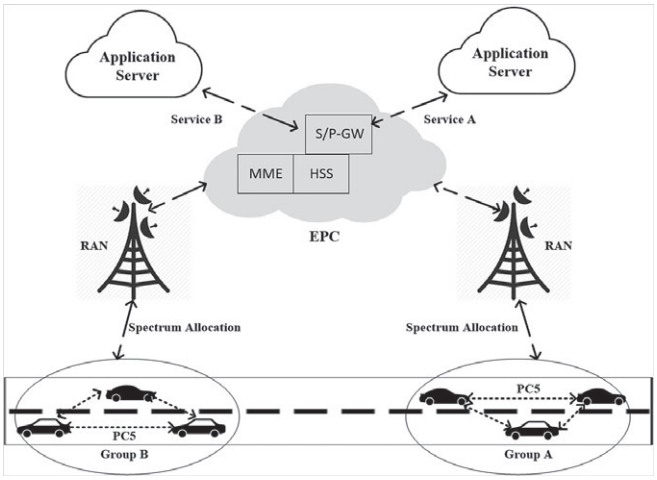


**FIGURE 1** Architecture of LTE-V

needs to be authorized by EPC and granted with group communication parameters. After that, UEs within the same application group can share a common carrier frequency to conduct direct group communications using PC5 interface as defined in 3GPP.[7] Generally speaking, UE grouping in LTE-V is logically controlled by AS, and EPC is in charge of radio resources management for overall system spectrum utilization for different application groups.

## 3 | SECURITY AND PRIVACY REQUIREMENTS

In this section, a general overview of security requirements in LTE-V and the unique privacy requirements are presented especially for group communications in LTE-V. By reviewing several off-the-shell privacy-preserving techniques for group communications, the limitations of existing solutions are presented when being applied to LTE-V group communications.

### 3.1 | Security requirements

In References 10 and 9, 3GPP summarizes essential security requirements for group communications in LTE-V. First, mutual authentication between UEs and RAN enables UE to be authorized and granted with necessary radio resources and communication parameters. Traffic protection between UEs requires *authenticity*, *confidentiality*, and *integrity* of exchanged messages.[12] Moreover, it is important to achieve source *accountability* (also referred as nonrepudiation) which means a sender cannot disprove having previously sent the message.

### 3.2 | Privacy enhancements

UE privacy is imperative for group communications in LTE-V. Exchanged messages among UEs are all through wireless communication channels, which can be easily intercepted by an attacker.[13] For example, an attacker can sniff all wireless packets within its communication range. Thus, UE anonymity should be guaranteed, which means UE's real identity should be concealed and kept secret. On achieving this, in 3GPP specification,[12] UEs within the same group are assigned with a unique group identity and a common group key. Combining this group key and UE group identity, UEs can further derive traffic encryption or decryption keys. Based on Reference 9, Ahmed and Lee[11] proposed a secure architecture for LTE-V services, in which a UE has 2 credentials: a long-term credential and a temporary credential. Specifically, a UE can first register herself or himself at a trusted authority to obtain her or his long-term credential. Then, when the UE accesses RAN using long-term credential, the UE can be authenticated and be assigned with a temporary credential, which is a pseudonym-based certificate for the UE to conduct group communications. However, both group identities and pseudonyms are directly transmitted in the clear in the proposed schemes. An attacker can intercept messages in the wireless channel and determine whether messages are sent from the same UE, which leads to exposure of a UE's *trajectory privacy*. A simple way to solve this problem is to frequently change the pseudonyms, which results in additional communication and storage overhead, and there is still possibility for an attacker to link UEs' pseudonyms by analyzing UEs' location information.[14]

## 4 | AN ANONYMOUS GROUP MESSAGE AUTHENTICATION PROTOCOL

In this section, an efficient and anonymous group message authentication protocol is proposed to protect UE trajectory privacy. By leveraging MAC and short group signature, a hybrid message authentication protocol is designed. Addition-

ally, the proposed protocol achieves batch verification and enjoys short signature size and is feasible for the deployment in LTE-V architecture.

## 4.1 | The detailed protocol

The anonymous and efficient group authentication protocol consists of 5 phases: Initialization, RAN access, service allocation, group message authentication, and misbehavior accounting.

### 4.1.1 | Initialization

EPC bootstraps the whole system and generates the public parameters for AS, UEs, and RANs. Let $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T)$ be 3 cyclic groups with a prime order $p$, where $p$ is $\lambda$ bits. In general, $\lambda$ is 160 or 320, which equals to the same security level of RSA 1024 or 5120, and can be set according to security requirements of different V2X applications. $g_1$ is a generator of $\mathbb{G}_1$ and $g_2$ is a generator of $\mathbb{G}_2$. $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ is a Type III bilinear pairing.[15] Thus, the system public parameter is $\{\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, e\}$.

### 4.1.2 | RAN access

Each UE is assigned with a universally international mobile equipment identity (IMEI) and shares a specific private key with HSS. Using this preshared key, the UE and EPC can authenticate each other and establish a secure communication channel. If the UE is eligible to access EPC, it will be issued with a temporary mobile subscriber ID (TMSI), which is used to apply for V2X services offered by AS.

### 4.1.3 | Service allocation

AS provide a variety of group-based applications, such as collaborative driving, proximity-based social networking, and location-based services. For a specific service $S_i$, AS randomly chooses $x_i, y_i \in Z_p^2$ to compute $X_i = g_2^{x_i}$, $Y_i = g_2^{y_i}$, and sends ($S_i$, $X_i$, $Y_i$) to EPC along with billing information.

A UE with an identifier $d$ and TMSI sends a request to AS to apply for group-based service $S_i$, in which several UEs form a group to access $S_i$. To do so, the UE randomly chooses a secret $k_d \in Z_p$ to compute a pair $(\alpha, \widehat{\alpha}) \leftarrow (g_1^{k_d}, Y_i^{k_d})$. Then, UE sends $(\alpha, \widehat{\alpha}, S_i)$ to AS along with a zero-knowledge proof of $k_d$ using a noninteractive $\Sigma$-protocol[16] through the established secure channel. Upon receiving the service request from the UE, AS verifies the knowledge of $k_d$ and checks if $e(\alpha, Y_i) = e(g_1, \widehat{\alpha})$. If both hold, AS randomly chooses $u \in Z_p$ to compute $\beta \leftarrow (\beta_1, \beta_2) \leftarrow (g_1^u, (g_1^{x_i} \cdot \alpha^{y_i})^u)$ and sends $\beta$ to the UE along with a secure session encryption key $K_s$ (eg, a 256-bit AES key) and a message authentication key $K_{MAC}$ (eg, a 256-bit HMAC key). Uniqueness and freshness of $K_s$ and $K_{MAC}$ can be guaranteed by periodically exchanging group control information between UEs and RAN.

### 4.1.4 | Group message authentication

Upon receiving ($K_s$, $K_{MAC}$, $\beta$), the UE can broadcast a message $m$ to other group members using $K_s$ to encrypt the data and $K_{MAC}$ to calculate MAC of the message, as such to realize message confidentiality and integrity. To achieve nonrepudiation, the UE firstly chooses a random value $t \in Z_p$ to compute $(\beta_1', \beta_2') \leftarrow ({\beta_1}^t, {\beta_2}^t)$. Then, the UE randomly chooses $l \in Z_p$ to compute $R \leftarrow e(\beta_1', Y_i)^l \leftarrow e(\beta_1, Y_i)^{lt}$. That is, the UE randomizes $\beta$ by choosing random values $t$, $l$ to compute $({\beta_1}', {\beta_2}')$. Finally, the UE computes $c \leftarrow H(\beta_1', \beta_2', R, m)$ and $s \leftarrow l + ck_d$, and the signature on the message $m$ is $\varrho = ({\beta_1}', {\beta_2}', c, s, R)$. Specifically, the message payload can be constructed as $GroupID||AES_{K_s}(m)||TimeStamp||MAC||\varrho$.

Upon receiving the message payload along with the signature, a UE within the same group first verifies the validity of the MAC. Then, the UE checks the signature by checking whether $R = (e({\beta_1}'^{-1}, X_i)e({\beta_2}', g_2))^{-c} e({\beta_1}'^s, Y_i)$ and $c \leftarrow H(\beta_1', \beta_2', R, m)$. It is noted that, the proposed protocol combines group signature and MAC in LTE-V to achieve both communication efficiency and message accountability. As for safety-related messages, UEs only need to check the validity of the MAC for low end-to-end delay. The message signature $\varrho$ can be used to recover the identity of a sending UE if there is any dispute occurred later.

Batch verification: Suppose that a UE receives a batch of messages $m_i \in \{m_1, \cdots, m_n\}$ along with their signatures $\{{\beta_{i1}}', {\beta_{i2}}', c_i, s_i, R_i\}_{i \in \{1, \cdots, n\}}$. Instead of verifying each signature separately, the UE checks $c_i \leftarrow H(\beta_{i1}', \beta_{i2}', R_i, m_i)$ and chooses random values $\delta_i$ from $Z_p$ for each signature, and checks the following equation to determine whether all the signatures are valid:

$$\prod_{i=1}^{n} (R_i)^{\delta_i} = e\left(\prod_{i=1}^{n} {\beta_{i1}'}^{c_i \delta_i}, X_i\right) \cdot e\left(\prod_{i=1}^{n} {\beta_{i2}'}^{-c_i \delta_i}, g_2\right) \cdot e\left(\prod_{i=1}^{n} {\beta_{i1}'}^{s_i \delta_i}, Y_i\right). \quad (1)$$

**TABLE 1** Comparison of privacy properties

| | Reference 11 | Reference 9 | Proposed protocol |
|---|---|---|---|
| Confidentiality and integrity | √ | √ | √ |
| Accountability | √ | √ | √ |
| Trajectory privacy | | | √ |

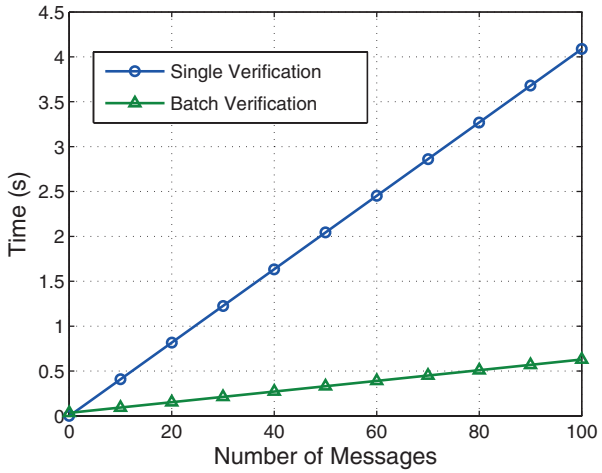


**FIGURE 2** Time cost on signature verification

#### 4.1.5 | Misbehavior accounting

Upon receiving a message from a misleading UE′, the UE uploads its signature $(\beta_1{}', \beta_2{}', c, s, R)$ to AS. After receiving the signature, AS can check $e(\beta_1' - 1, X_i)e(\beta_2', g_2) = e(\beta_1', \widehat{\alpha})$ for all $(\alpha, \widehat{\alpha})$ stored in the system until AS finds a match. Finally, AS sends the matched $(\alpha, \widehat{\alpha})$ to HSS to recover the identity of misbehaving UE′.

### 4.2 | Security analysis and performance evaluation

Using group key $K_s$ and MAC key $K_{MAC}$, the proposed protocol achieves message confidentiality and integrity. Meanwhile, the proposed protocol achieves message unlinkability to protect UE's trajectory privacy. Unlinkability means that an attacker cannot tell whether 2 messages are generated by the same UE. In signature generation phase, the UE selects 2 random numbers $l$, $t$ to compute the signature $\varrho = (\beta_1{}', \beta_2{}', c, s, R)$. The signatures are always randomized, which means that signatures generated by a UE are different even for the same message. This feature fits for the group communication scenario, where all group members can generate valid signatures that can be verified using the same group signature public key $(X_i, Y_i)$ instead of transmitting group identities or pseudonyms in References 3 and 13. Moreover, the security of the proposed protocol can be reduced to the modified LRSW assumption.[15] Specifically, a UE first needs to obtain a secret signing key $(\beta_1, \beta_2)$ from AS, which is a blind signature of the UE's randomly chosen secret $k_d$. The security of this blind signature can be reduced to the modified LRSW assumption 1. The unforgeability of the group signature under chosen message attack can be reduced to the modified LRSW assumption 2.[15] Therefore, if the modified LRSW assumption holds, an attacker cannot forge a signing key or a valid group signature. A comparison of privacy properties among the proposed protocol, 3GPP standardization[9] and Ahmed's work[11] is shown in Table 1.

Extensive simulations are conducted on an Intel Core i5 2.53GHz processer with 4.00GB memory to demonstrate the computational efficiency of the proposed protocol. The proposed protocol is implemented using MIRACL library.[17] The security parameter $p$ is 160-bit, and the elliptic curve is defined over $F_q$, where $q$ is 512-bit. SHA-256 is chosen as the cryptographic hash function. The batch verification is used to verify the validity of multiple signatures, in the way that the computational overhead on signature verification can be significantly reduced compared with the approach of separate verification. Expensive paring operations are replaced with more efficient exponential operations over $G_1$ and $G_2$ to achieve efficient batch verification. As shown in Figure 2, it can be seen that the proposed batch verification technique can increase verification efficiency, and total verification of 100 signatures takes less than 1 second.

In terms of storage overhead, UEs need to store key materials including a session encryption key $K_s$ (256 bits), a message authentication key $K_{MAC}$ (256 bits), and a group signature key $\beta$ (1024 bits). The total storage overhead of key materials is 1536 bits. In terms of communication overhead, a UE needs to calculate a MAC (256 bits) and a signature $\varrho = (\beta_1{}', \beta_2{}', c, s,$

*R*) (2368 bits) for each message. The proposed protocol has a short signature size and is feasible for practical LTE-V group communications.

**Remarks:** The proposed hybrid message authentication protocol combines MAC and group signature techniques. For safety-related messages that require guaranteed end-to-end delay (ie, 20 milliseconds), the receiving UE only needs to verify MAC, which is very efficient. However, MAC cannot provide accountability since all UEs within the same group share a common group MAC key. For secure provisioning of the shared group key $K_s$ and $K_{MAC}$ and efficient group rekeying, we refer readers to Reference 18.

## 5 | CONCLUSION

In this letter, key privacy requirements for LTE-V group communications have been investigated and an anonymous message authentication protocol has been proposed. By designing a hybrid authentication protocol, the proposed protocol can achieve UE anonymity, accountability, and trajectory privacy. Moreover, a newly designed batch verification mechanism for group signature has also been proposed to significantly improve verification efficiency. Security and performance evaluation have demonstrated that the proposed protocol is applicable for LTE-V group communications. For the future work, dynamic natures of LTE-V group communications will be taken into consideration, such as vehicle mobility model for group membership changing, to further improve the efficiency of the LTE-V group communications.

### ACKNOWLEDGEMENTS

The authors thank the Intel Security Research Team in Portland and the anonymous reviewers for their valuable comments and suggestions.

## ORCID

*Dongxiao Liu* http://orcid.org/0000-0003-2595-6757

### REFERENCES

1. [3GPP] Study on LTE Support for Vehicle to Everything (V2X) Services. *3GPP technical specification*. 2015; TR22.885,V14.0.0.
2. Jiang D, Delgrossi L. IEEE 802.11p: towards an international standard for wireless access in vehicular environments. Paper presented at: Proceedings of VTC-Spring; 2008:2036–2040 Singapore.
3. Abboud K, Omar HA, Zhuang W. Interworking of DSRC and cellular network technologies for V2X communications: a survey. *IEEE Trans Vehic Technol*. 2016;*65*(12):9457-9470.
4. Ploeg J, Scheepers BT, Van Nunen E, Van de Wouw N, Nijmeijer H. Design and experimental evaluation of cooperative adaptive cruise control. Paper presented at: Proceedings of IEEE ITSC, 2011:260-265 Washington, USA.
5. [3GPP] Architecture Enhancements for V2X Services. *3GPP technical specification*. 2016; TS23.285, V14.00.
6. Seo H, Lee KD, Yasukawa S, Peng Y, Sartori P. LTE evolution for vehicle-to-everything services. *IEEE Commun Mag*. 2016;*54*(6):22-28.
7. [3GPP] Proximity-based Services (ProSe). *3GPP technical specification*. 2017; TS23.303, V15.00.
8. [3GPP] Service Requirements for V2X Services. *3GPP technical specification*. 2017; TS22.185,V14.3.0.
9. [3GPP] Study on Security Aspects for LTE Support of V2X Services. *3GPP technical specification*. 2017; TR33.885, V2.0.0.
10. [3GPP] Proximity-based Services (ProSe); Security Aspects. *3GPP technical specification*. 2017; TS 33.303, V14.1.0.
11. Ahmed KJ, Lee MJ. Secure, LTE-based V2X service. *IEEE Internet Things J*. 2017. DOI: 10.1109/JIOT.2017.2697949.
12. Li G, Ma M, Liu C, Shu Y. An efficient authentication framework over heterogeneous vehicular networks. Paper presented at: IEEE International Conference on Communication Systems (ICCS) Shenzhen, China; 2016:1-6.
13. Lin X, Sun X, Ho PH, Shen X. GSIS: a secure and privacy-preserving protocol for vehicular communications. *IEEE Trans Vehic Technol*. 2007;*56*(6):3442-3456.
14. Mukisa SS, Rashid A. Challenges of privacy requirements modelling in V2X applications: a telematic insurance case study. Paper presented at: IEEE 25th International Requirements Engineering Conference Workshops (REW); 2017:97-103 Lisbon, Portugal.
15. Pointcheval D, Sanders O. Short randomizable signatures. Paper presented at: Cryptographers' Track at the RSA Conference; 2016:111-126 San Francisco, USA.
16. Bellare M, Goldreich O. On defining proofs of knowledge. Paper presented at: Annual International Cryptology Conference; 1992: 390-420; Heidelberg, Germany.
17. MIRACL Crypto SDK. https://libraries.docs.miracl.com/. accessed at October 2017.
18. Sun Y, Chen M, Bacchus A, Lin X. Towards collusion-attack-resilient group key management using one-way function tree. *Comput Network*. 2016;*104*:16-26.

**How to cite this article:** Liu D, Ni J, Lin X, Shen X (Sherman). Anonymous group message authentication protocol for long-term evolution-based vehicle-to-everything communications, *Internet Technology Letters*, 2018;e25. https://doi.org/10.1001/itl2.25