IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.DOI

A Realistic Distributed Conditional Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks

ZHI-CAI LIU[1], LING XIONG[1,3], TU PENG[2], DAI-YUAN PENG[3] AND HONG-BIN LIANG[4]

[1]School of Computer and Software Engineering, Xihua university, Chengdu. 610039, P.R. China
[2]School of Software, Beijing Institute of Technology, Beijing. 100081, P.R. China
[3]School of Information Science and Technology, Southwest Jiaotong University, Chengdu. 611756, P.R. China
[4]School of Transportation and Logistics, Southwest Jiaotong University, Chengdu. 611756, P.R. China

Corresponding author: Ling Xiong (e-mail: lingdonghua99@163.com).

This research was supported by National Science Foundation of China under Grant number (Grant No. 61502034 and 61571375) and the open research fund of key laboratory of intelligent network information processing, Xihua University (16224221)

ABSTRACT Nowadays, the research of tradeoff between reliance on the tamper-proof device(TPD) and storage space in authentication scheme has become an interesting topic for vehicular ad hoc networks(VANETs). Most recently, to minimize the dependencies of TPDs and reduce the storage space, Zhang et al. proposed a conditional privacy-preserving authentication scheme based on multiple trusted authority one-time identity-based aggregate signature technique. It is more practical than other related schemes due to not depending on ideal TPDs. However, Zhang et al.'s scheme requires a fully trusted third party to participate in the authentication and member secrets generate phase, which may suffer from security bottleneck. To overcome this weakness, in this work, we construct a realistic distributed conditional privacy-preserving authentication scheme for VANETs using identity-based cryptography and short lifetime region-based certificate. Comparing with Zhang et al.'s scheme, the proposed scheme has more security features but doesn't reduce computation and communication efficiency. The security analysis shows that our scheme is provably secure in the random oracle model.

INDEX TERMS Vehicular ad hoc networks, authentication, conditional privacy-preserving

I. INTRODUCTION

As a special case of mobile ad hoc networks, vehicular ad hoc networks (VANETs) has received a great deal of attention from researchers in the academic and industrial field [1]. Generally, VANETs consists of a trusted authority(TRA), some distributed roadside units(RSUs) and a large number of vehicles. All vehicles in the VANETs equipped with On-Board Units(OBUs) are moving on the road. To improve the driving experience and ensure driving safety, vehicles will broadcast real-time traffic conditions, such as traffic jams, traffic lights, and traffic signs, etc., to nearby vehicles or RSU [2]. These communications are divided into Vehicle-to-Vehicle (V2V) communication and vehicle-to-roadside unit (V2R) communication, which are controlled by short-range communications (DSRC) protocol [3].

Because DSRC operates in the wireless environments, a malicious adversary could control the communication channel easily, i.e., he/she can eavesdrop, insert, block, and alter the transmitted data. Thus, VANETs are subject to various types of attacks [4]. To ensure that the received messages are transmitted by a legitimate vehicle and to protect the integrity of messages, it is indispensable to achieve message authentication in VANETs [5].

Additionally, the leakage of vehicles' identities may reveal drivers' locations, movements, etc. The adversary can infer drivers' privacy from that information, which may cause serious consequences. For example, the attacker can infer the driver's actions trajectory and location information through vehicle social networks and burgles his home [6], [7]. Thus, it is of great concern to protect vehicles' identities in VANETs. Although vehicle anonymity is a key issue in VANETs, it should still be conditional anonymity in the sense that a trusted authority should extract the real identity form the transmitted message. Because a malicious vehicle may send a fake message, which will misguide other vehicles into accidents [4], [8].

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2018.2834224, IEEE Access

In the past several years, a series of remarkable conditional privacy-preserving authentication scheme for VANETs(e.g. [4], [8], [9]) have been proposed. He et al.'s [4] designed an identity-based conditional privacy-preserving authentication scheme with batch verification for VANETs without using bilinear pairing, which could satisfy various security requirements. This scheme assumes that the OBU is a tamper-proof device(TPD) and its secret keys are never disclosed. Obviously, it relies heavily on the TPD. Since the system private key is stored in all vehicles' TPD. Once key leakage occurs in any TPDs among these vehicles, the whole system will be compromised. Subsequently, Lo and Tsai [9] constructed a novel conditional privacy-preserving authentication scheme without the dependencies of TPD. But it requires a large storage space to preload secret parameters. The reason is that each vehicle in VANETs broadcasts traffic-related messages to nearby vehicles or RSUs frequently in practice. (e.g. in a short time interval, such as 1 minute [10], [11]). Hence, the storage capacity is impeded by limited resources of TPD. To address these issues, Zhang et al. [8] proposed an authentication protocol based on multiple trusted authority one-time identity-based aggregate signature technique. It does not require strong realistic on TPDs. Furthermore, a huge pool of secret parameters is avoided in TPDs. It is more practical than the other two schemes [4], [9]. However, it requires a fully trusted third party to participate authentication when the vehicle enters into a range area of a new RSU, which may make the trusted third party being a bottleneck of security.

Motivated by the above facts, in this work, we design a realistic distributed conditional privacy-preserving authentication scheme for VANETs without the strong reliance on TPD, which also does not need ample space. Meanwhile, our scheme achieves authentication in authentication, and member secrets generate phase without the help of TRA. Besides, the proposed scheme can provide message authentication, vehicle anonymity, conditional traceability, and resistance to various attacks.

A. RELATED WORK

Until now authentication schemes based on cryptography techniques in VANETs can be divided into five categories: 1) ones based on the pseudonymous certificate; 2)ones based on group signatures; 3)ones based on symmetric cryptography; 4) ones based on identity-based cryptography(IBC); 5) ones based on hybrid methods [8], [11], [12].

1) Pseudonymous certificate based classification

The authentication schemes based on pseudonymous certificate mainly utilize public key infrastructure(PKI). Raya and Hubaux proposed a typical authentication scheme based on anonymous certificate [10], [13]. This scheme can provide message authentication and non-repudiation. To achieve unlinkability, the transmitted anonymous certificate must be changed at every session. Consequential, each vehicle in VANETs needs to preload a huge number of anonymous certificates. Besides, with time growing, the size of certificate revocation lists(CRLs) are getting longer, which will cause the problem of efficiency. Furthermore, every signature verification based this classification is independent. So the computation cost of verification is high.

2) Group signature based classification

Group signature is commonly used in VANETs to achieve vehicle anonymous. In 2007, Lin et al. [14] proposed a privacy-preserving authentication scheme based on group signature. The group manager who has the group master key can trace the real identity. However, the size of CRL is linear with the revoked vehicles. As a result, the running time of checking operation will take a long time. Subsequently, several authentication schemes [15]–[17] based on group signature have been proposed. Although these schemes [15]–[17] have much better performance than Lin et al. scheme [14], they are still cost a lot of communication energy and computation resource of the group leader, which may make the group leader become the bottleneck of the system. Besides, the computation cost of verification using group signature is higher than those of the traditional signature.

3) Symmetric cryptography based classification

The symmetric cryptography based schemes are subcategorized into three groups. The first group utilizes message authentication code (MAC) to achieve message authentication(e.g. [18], [19]). The second group uses hash function(e.g. [20], [21]) and the third group employs timed efficient stream loss-tolerant authentication(e.g. [22], [23]). Symmetric cryptography based schemes are more efficient than ones based on asymmetric cryptography. However, they have several inherent drawbacks like the problem of non-repudiation and key management. Although Wang et al. claimed that their scheme [11] cam achieve non-repudiation only using MAC and hash function, it has a strong reliance on TPDs. Since Wang et al.'scheme assumes that the TPD is fully trusted and the signature messages include the current timestamp, a vehicle cannot deny the act of broadcasting message. Besides, like He et al.'s scheme [4], every vehicle in VANETs stores the system key, the whole system will be in danger of occurring key leakage.

4) Identity-based cryptography based classification

To address the problem of certificate management, identity-based cryptography (IBC) has been utilized in VANETs for authentication, which greatly increases the computation and communication efficiency. In 2006, Kamat et al. [24] presented an identity-based security framework for VANETs to provide authentication, non-repudiation, confidentiality and message integrity. However, this framework is the strong reliance on the infrastructure, which causes the signaling overhead overwhelming. To resolve this problem, Sun et al. [17] proposed an authentication scheme using identity-based encryption(IBE), which can achieve vehicle privacy and vehicle traceability. In 2012, Shim et al. [25] designed an conditional privacy-preserving authentication(CPAS) scheme us-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2018.2834224, IEEE Access

ing pseudo IBC for VANETs. The efficiency of signature verification in CPAS is increased due to the batch verification. Later on, a series of authentication schemes for VANETs using IBC have been proposed(e.g. [26]–[28]). These schemes still exist some limitations, such as impersonation attack and modification attack. Consequently, He et al. [4] constructed an efficient identity-based conditional privacy-preserving authentication(CPPA) scheme for VANETs without using heavy bilinear pairings, which supports both authentication and privacy protection simultaneously. But the CPPA scheme has strong dependencies on TPD. Once key leakage occurs in any TPDs of vehicles, the whole system will be compromised. In 2016, Lo and Tsai [9] developed an efficient conditional privacy-preserving authentication scheme without reliance on TPDs. However, it needs a vast storage space to store its pseudo-IDs and the corresponding private keys.

5) Hybrid methods based classification

Calandriello et al. [29] put forwarded a scheme combining pseudonym scheme with group signature, which generates pseudonyms on-the-fly. However, it still requires a large storage capacity for CRLs, and the expensive CRL checking remains a problem. Subsequently, a series of improved schemes [30]–[32] have been introduced to minimize the size of CRL. Although these schemes have reduced the broadcast CRL size, they still suffer from the expected significant size. In 2013, Wasef et al. [33] designed an expedite message authentication(EMAP) protocol using PKI and HMAC. Since utilizing HMAC instead of CRL, the main advantage of the EMAP reduces the computation and storage cost compared to the previous schemes employing CRL [30]–[32]. However, this work still exists a limitation, which causes high packet verification overhead for the batch authentication scheme. Most recently, Zhang et al.'s scheme [8], based on the approach of a trade-off between reliance on TPDs and storage space, combined one-time identity-based aggregate signature technique and certificate. This scheme issues short lifetime region-based certificate, which is valid only within the coverage range of the RSU. Obviously, it is more practical than the other schemes. However, it requires a TRA to participate authentication, which may make the TRA being a bottleneck of security.

B. CONTRIBUTIONS

In this paper, to balance the reliance on TPDs and storage space, we present a realistic distributed conditional privacy-preserving authentication scheme for VANETs without the help of online TRA. The major contributions of the work are summarized as follows.

(1) Based on identity-based cryptography and short lifetime region-based certificate, the authentication and member secrets generate phase of our proposed scheme does not require the participation of trusted third party.
(2) Since each vehicle's TPD only stores secret key within the coverage range of the RSU, which will update at a short period. So, the proposed scheme achieves various security requirements without strong reliance on TPDs.
(3) Security analysis shows that our scheme does not only meet a variety of security requirements for VANETs but also resist various kinds of known attacks.
(4) Compared with the previously related schemes, our scheme provides more security features but doesn't reduce computation and communication efficiency.

C. ORGANIZATION OF THE PAPER

The rest of this paper is organized as follows. Section II introduces security requirements for VANETs. Section III presents the detailed procedure of our proposed scheme. Section IV gives security analysis of the proposed scheme. The computation and communication costs analysis of the proposed scheme are discussed in section V. Finally, section VI concludes this paper. All the notations mentioned in our proposed scheme are defined in Table 1.

TABLE 1. Notations

Notation	Descriptions
V_i	A vehicle user
R_j	A RSU
TPD_i	The tamper-proof device of a vehicle user
RID_{Vi}	Unique real identity of V_i
PID_{Vi}	Pseudo-IDs of V_i
G_1	An elliptic curve additive group with order q
G_2	A cyclic multiplicative group
P	A generator of G_1
sk	The system private key
PK	The system public key
T_1, T_2	Current time stamp values
$h_i(i = 0, 1, ..., 4)$	One-way hash function
$X\|\|Y$	Concatenate operation
$\oplus$	XOR operation

II. SECURITY REQUIREMENTS

He et al. [4] pointed out VANETs should meet many security requirements, including message authentication, identity privacy preservation, traceability, un-linkability and resistance to various known attacks. In addition to the security requirements mentioned above, we believe that an authentication scheme for VANETs should also satisfy the following security properties.

(1) **Not strong reliance on TPDs**: Although TPD is a tamper-proof device in VANETs, the security properties should not be a strong reliance on TPDs. Even if a vehicle is compromised, the whole system should not be in danger.
(2) **Efficient storage space**: Because the vehicle's TPD is limited in computing power and storage. Meanwhile, the communications within V2V or V2R are frequently. The authentication scheme for VANETs should consider the storage space. Ample storage space may be not suitable for constrained TPDs.
(3) **Key escrow freeness**:Any legitimate vehicle cannot sign messages to forge another vehicle. The TRA can sign messages on behalf of any vehicle [8].

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2018.2834224, IEEE Access

III. THE PROPOSED SCHEME

This section will describe the details of the proposed anonymous authentication scheme. Our proposed scheme consists of six phases: initialization phase, vehicle registration phase, RSU registration phase, authentication and member secrets generate phase, anonymous identity generation and message signing phase, and message verification phase. Each phase in detail will be introduced as follows.

A. INITIALIZATION PHASE

In the initialization phase, the root TRA choose an additive group of point G_1 with order q, and P is a generator of G_1. TRA generates the system private key $sk \in Z_q^*$ and calculates the system public key $PK = sk \cdot P$. Then TRA chooses five secure hash functions $h_i : \{0,1\}^* \rightarrow Z_q^*$, $(i = 0, 1, ..., 4)$. The TRA stores sk into its memory as secret and publishes the system parameters $\{G_1, P, PK, h_0, h_1, h_2, h_3, h_4\}$. Notice that the system parameters are preloaded into the TPD of all vehicles and RSU.

B. VEHICLE REGISTRATION PHASE

When a new vehicle user V_i wants to join a VANET, he/she needs to register for the TRA first. After registration, the TPD of V_i must be initialized. The procedure of vehicle registration is described as follows.

(1) A new vehicle user V_i submits the real identity RID_{Vi} to TRA through a secure channel.

(2) Upon receipt of the message, the TRA at first checks whether RID_{Vi} exists in the vehicle information table. If it exists, TRA rejects the registration request. Otherwise, the TRA generates a set of random numbers named pseudo-IDs $PID_{Vi} = \{PID_{Vi0}, PID_{Vi1}, ..., PID_{Vin-1}\}$, a set of its corresponding private keys $(TVP_i, KV_i) = \{(TVP_{i0}, KV_{i0}), ..., (TVP_{in-1}, KV_{in-1})\}$, where n is the number of elements in each set. Each element are generated as follows. First, the TRA generates n random numbers r_0,r_1,...r_{n-1}, and computes

$$TVP_{ij} = r_j \cdot P \quad (1)$$

$$KV_{ij} = r_j + h_2(PID_{Vij}||TVP_{ij}||L_t) \times skmodq \quad (2)$$

Where $0 \leq j \leq n-1$. Next, the TRA updates the vehicle identity information table with the new entry $\{RID_{Vi}, PID_{Vi}, L_t\}$, and preloaded $\{PID_{Vi}, (TVP_i, KV_i), L_t\}$ into the TPD of V_i.

C. RSU REGISTRATION PHASE

When an RSU R_j is deployed, R_j is required to register in TRA. The procedure of sensor node registration is described as follows.

(1) A new RSU R_j selects the identity ID_{Rj} and transmits it to TRA via a secure channel.

(2) After receiving the identity ID_{Rj}, TRA first checks whether ID_{Rj} exists in the RSU information table. If it exists, TRA refuses the RSU registration request. Otherwise, TRA generates two random numbers $r_{Rj}, k_{Rj} \in Z_q^*$, and computes $TRP_i = r_{Rj} \cdot P$, $TKP_i = k_{Rj} \cdot P$, $S_{Rj} = sig(ID_{Rj}, TRP_i, TKP_i)$, where sig is a signature on (ID_{Rj}, TRP_i, TKP_i). Then TRA broadcast the certificate $cert_{Rj} = (ID_{Rj}, TRP_i, TKP_i, S_{Rj})$ to vehicle within R_j's communication range. After that, TRA stores $\{ID_{Rj}\}$ into the RSU table and sends $\{r_{Rj}, k_{Rj}, TRP_i, TKP_i\}$ to R_j via a private channel. Note: r_{Rj} is used to generate signature value for the vehicle in R_j's communication range, which is updated in a short period, such as a day or a week. k_{Rj} is used to generate a secure communication between a vehicle and R_j. $cert_{Rj}$ is updated as the value of r_{Rj}.

(3) After receiving the message $\{r_{Rj}, k_{Rj}, TRP_i, TKP_i\}$ from TRA, R_j stores them into its memory secretly.

D. AUTHENTICATION AND MEMBER SECRETS GENERATE PHASE

When a vehicle V_i enters into the communication range of R_j, it requests to join the subgroup of R_j. If V_i has joined this subgroup, and the authorized period is not expired, it does nothing. As shown in Fig. 1, the process of mutual authentication and member secrets generate is described as follows.

(1) The TPD_i first checks the correctness of R_j's certificate $cert_{Rj}$. If it is invalid, V_i abotrts. Otherwise, TPD_i extracts (ID_{Rj}, TRP_i, TKP_i) from $cert_{Rj}$. Next, TPD_i randomly selects a pseudo-ID PID_{Vik} and its corresponding private key (TVP_{ik},KV_{ik}) form the set of pseudo-IDs and its corresponding set of private keys, generates a random number $x \in Z_q^*$, and computes $X = x \cdot P$, $CT_1 = (PID_{Vik}||TVP_{ik}||L_t) \oplus h_0(x \cdot TKP_i||T_1)$, $V_1 = h_3(X||PID_{Vik}||TVP_{ik}||T_1) \times x + KV_{ik} modq$, where T_1 is current timestamp. Finally, TPD_i sends $\{X, CT_1, V_1, T_1\}$ to R_j.

(2) After receiving the authentication messages, R_j at first checks the timestamp T_1. After that, R_j decrypts the ciphertext using the secret key k_{Rj} by computing $PID_{Vik}||TVP_{ik}||L_t = CT_1 \oplus h_0(k_{Rj} \cdot X||T_1)$. Then R_j checks the validity of period L_t and verifies whether the following equation holds.

$$V_1 \cdot P = h_3(X||PID_{Vik}||TVP_{ik}||T_1) \cdot X + TVP_{ik} + h_2(PID_{Vik}||TVP_{ik}||L_t) \cdot PK \quad (3)$$

If the equation (3) holds, it means that TPD_i is a legitimate vehicle. Then R_j computes $CT_2 = (r_{Rj}||LR_t) \oplus h_0(k_{Rj} \cdot X||T_2)$, $V_2 = h_4(PID_{Vik}||r_{Rj}||LR_t||T_2)$ and sends $\{CT_2, V_2, T_2\}$ to TPD_i through a public channel.

(3) Upon receipt of the messages from R_j, TPD_i checks the validity of the timestamp T_2 firstly. Then, TPD_i computes $r_{Rj}||LR_t = CT_2 \oplus h_0(x \cdot TKP_i||T_2)$,

$V_2 = h_4(PID_{Vik}||r_{Rj}||LR_t||T_2)$ and compares V_2' with the received value V_2. If they are not equal, TPD_i terminates this session. Otherwise, TPD_i believes the legitimate of R_j. Finally, TPD_i stores $\{r_{Rj}, LR_t\}$ into its secret memory.

E. ANONYMOUS IDENTITY GENERATION AND MESSAGE SIGNING PHASE

If a vehicle V_i wants to broadcast traffic-related messages to the nearby vehicle and R_j, these messages should be signed to meet authentication and conditional privacy-preserving. Suppose the TPD_i has joined the subgroup of R_j and obtained the member secrets $\{r_{Rj}, LR_t\}$. Details of the signature are generated as follows.

(1) The vehicle V_i first generates traffic-related messages M_i and request TPD_i to generate pseudo-ID and its corresponding private key.

(2) After receiving the signature request, TPD_i randomly selects a pseudo-ID PID_{Vik} the set of pseudo-IDs, generates a random number $u_i \in Z_q^*$ and computes

$$TP_{ui} = u_i \cdot P \tag{4}$$

$$PPID_i = PID_{Vik} \oplus h_1(u_i \cdot PK||t_i) \tag{5}$$

$$V_{ui} = u_i + h_2(PPID_i||TP_{ui}||t_i) \times r_{Rj} mod q \tag{6}$$

Then, TPD_i gives $\{TP_{ui}, PPID_i, V_{ui}, t_i\}$ to V_i.

(3) V_i generates a random number $w_i \in Z_q^*$ and computes

$$TP_{wi} = w_i \cdot P \tag{7}$$

$$\sigma_i = V_{ui} + h_3(TP_{ui}||TP_{wi}||PPID_i||t_i||M_i) \times w_i mod q \tag{8}$$

At last, V_i broadcasts $\{M_i, TP_{ui}, PPID_i, t_i, TP_{wi}, \sigma_i\}$ to nearby vehicles or RSU.

F. MESSAGE VERIFICATION PHASE

After receiving n traffic-related signature tuples $\{M_i, TP_{ui}, PPID_i, t_i, TP_{wi}, \sigma_i\}$ $(i = 1, 2..., n)$, the verifier employs the system parameters $\{G_1, P, PK, h_0, h_1, h_2, h_3, h_4\}$ and R_j's certificate $cert_{Rj}$ to verify the validity of signatures. The batch verification of n signatures are described as follows.

(1) The verifier checks the validity of t_i $(i = 1, 2..., n)$. If it is invalid, the verifier rejects the signature.

(2) The verifier chooses n random number $a_i \in \{0,1\}^l$, where usually $l = 80$ and $i = 1, 2..., n$. Then the verifier computes

$$(\sum_{i=1}^{n} a_i \sigma_i) \cdot P = \sum_{i=1}^{n} a_i \cdot TP_{ui} + (\sum_{i=1}^{n} a_i h_{i2}) \cdot TRP_i + (\sum_{i=1}^{n} a_i h_{i3}) \cdot TP_{wi} \tag{9}$$

where $h_{i2} = h_2(PPID_i||TP_{ui}||t_i)$, $h_{i3} = h_3(TP_{ui}||TP_{wi}||PPID_i||t_i||M_i)$. If the equation (9) holds, the verifier accepts the signatures. Otherwise, the verifier rejects the signatures.

IV. SECURITY ANALYSIS OF THE PROPOSED SCHEME

In this section, we will show our proposed scheme meets all the security requirements in section II. Because the initialization phase, vehicle registration phase, and RSU registration phase are executed in the secure channel. The proposed scheme may suffer security and privacy threats in the authentication and member secrets generate phase, anonymous identity generation and message signing phase, and message verification phase. The security of the anonymous identity generation and message signing phase and message verification phase are consistent with the reference [4]. Therefore, in this section, we demonstrate the authentication and member secrets generate phase is secure.

Protocol participant. The proposed scheme involves four participants, the trusted authority TRA, the RSU R_j, the vehicle V_i, and the V_i's tamper-proof device TPD_i. TRA is a trusted third party and it generates secure parameters. R_j is located at roadside who is used to connect V_i and TRA. TPD_i is a trusted device and the secret information is hard to hack into.

Adversary model. The goal of an adversary A has three goals. One is that A can successfully forge a valid TPD_i's signature to R_j. The other is that A can successfully impersonate R_j authenticating to TPD_i. And the last is that A can obtain the private signature key r_{Rj} and forge the signature of V_i. We assume that A is a probabilistic polynomial time attacker, and the feasible attacks are summarized as follows:

(1) A can control the channel between the vehicle and the RSU. It means that A can obtain, inject and modify messages transmitted on the channel.

(2) Assume that RSU is semi-trusted, and A can compromise small part of RSU.

(3) A may be another legitimate but malicious driver of the vehicle in the system.

(4) A may stole the V_i's tamper-proof device TPD_i.

Security Model. Based on the literature [4], we proposed a security model for our scheme. The security model of our scheme is defined by a game played by the adversary A and a challenger ζ. A can make following oracle queries.

(1) $h_i - Oracle$: This query simulates the hash function. When A ask the query m_i, ζ generates a random $h_i \in Z_q^*$ and returns h_i to A.

(2) $Register - Oracle$: This query simulates A registration as a legitimate vehicle. A issues inquiry and receives pseudo-ID of the vehicle.

(3) $Setup{-}Oracle$: This query simulates that ζ initials the system parameters and the private key of the system. Then, ζ sends the system parameters to A.

(4) $TSend - Oracle$: This query simulates ζ generates a request message $\{X, CT_1, V_1, T_1\}$ when ζ receives the a null message. Then, ζ outputs a $\{X, CT_1, V_1, T_1\}$ to A.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2018.2834224, IEEE Access

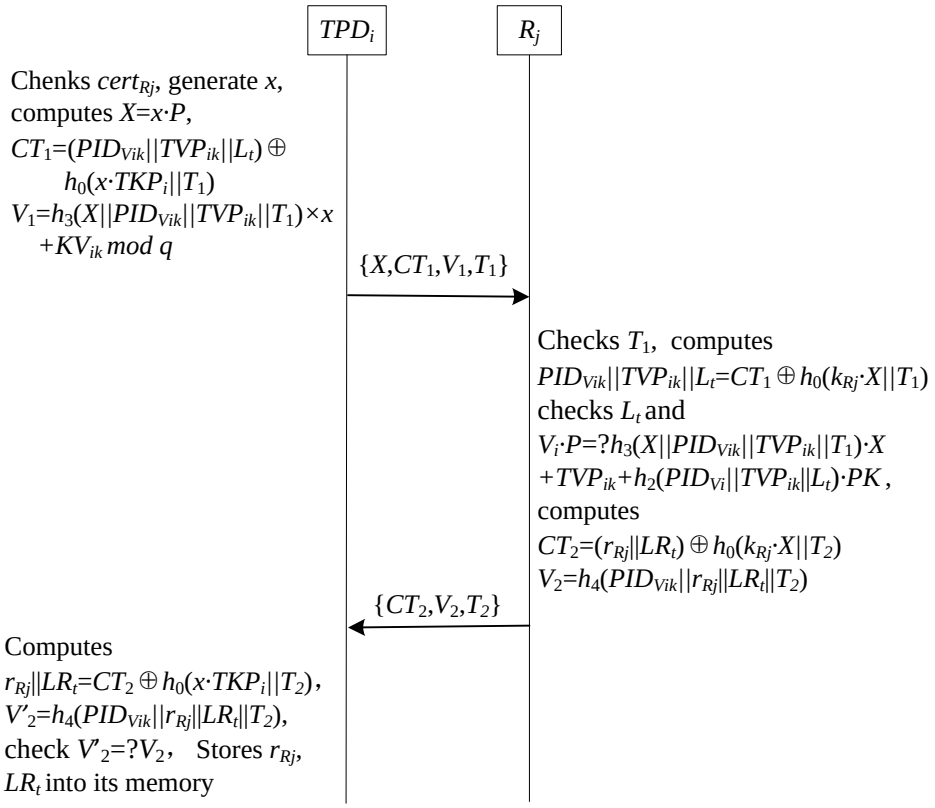

FIGURE 1. Authentication and member secrets generate phase of our scheme.

(5) $RSend-Oracle$: In this query, ζ generates message $\{CT_2, V_2, T_2\}$ upon receiving the message $\{X, CT_1, V_1, T_1\}$. ζ will output $\{X, CT_1, V_1, T_1\}$ to A.

(6) $Test-Oracle$: This query simulates the semantic security of the pseudo-ID PID_{Vik}. ζ chooses a random bit $b \in 0, 1$. If $b = 1$, ζ returns the pseudo-ID PID_{Vik} to A, otherwise ζ returns a random number to A.

Definition 1: Matching sessions: The session in instance $\prod_V^s$ and the session in instance $\prod_R^{s'}$ are said to be matching if $s = s'$, $pid_V = S$, $pid_R = U$ and both have accepted, where pid_V and pid_R denote as a peer identity.

Definition 2: Security protocol: We say that our scheme is secure if the following properties hold:

- $\prod_V^s$ and $\prod_R^s$ are matching session, and they accept each other.
- The probability of $\prod_V^s$ accepted A as $\prod_R^s$ is negligible.
- The probability of $\prod_R^s$ accepted A as $\prod_V^s$ is negligible.
- The probability of distinguishing the pseudo-ID from a random number is negligible.

A. PROVABLE SECURITY

To prove the security of our proposed scheme, we assume that our scheme is defined by a game played between an adversary A and a challenger ζ. At first, we give two mathematical problems used for our security analysis.

Definition 3: Discrete Logarithm (DL) Problem: Given $X = xP$, where $x \in Z_q^*$, $X \in G_1$, it is infeasible to compute x.

Definition 4: The Computational Diffie-Hellman(CDH) Problem: Given $X = xP$, $Y = yP$, where $x, y \in Z_q^*$, $X, Y \in G_1$, it is infeasible to compute xyP.

Lemma 1: (Secure vehicle authentication): In the proposed scheme, if h_0, h_1, h_3 are ideal random functions and $\prod_S^R$ has been accepted, then there is no polynomial adversary against our proposed scheme who can forge a legal vehicle authentication message with a non-negligible probability.

Proof. We assume that the adversary A can forge a legitimate authentication message with a non-negligible probability ϵ. Then there is a challenger ζ who can solve the DL problem with a non-negligible probability.

Given an instance $(P, PK = sk \cdot P)$ of DL problem, the task of ζ is to compute sk. ζ sends the system parameters $\{G_1, P, PK, h_0, h_1, h_2, h_3, h_4\}$ to A. ζ randomly selects a vehicle's identity RID_{VC} as the challenge identity and answers A's queries as follows:

- $h_i - Oracle$: This query h_i, $i = 0, 1, 2, 3, 4$ maintains a list L_{hi} with initialized empty. ζ checks whether the message m_i exists in L_{hi}. If it exists, ζ returns its value h_i to A. Otherwise, ζ generates a random number h_i,

and stores the tuple (m_i, h_i) into L_{hi} and returns h_i to A.

- $Register - Oracle$: In this query, ζ maintains a list L_R with initialized empty. When A asks this query with identity RID_{Vi}, ζ checks whether the tuple of RID_{Vi} exists in L_R. If it exists, ζ returns RID_{Vi} to A.Otherwise, ζ operates as follows:
  - ◇ If $RID_{Vi} = RID_{VC}$, ζ generates three random numbers $r_i, \varepsilon_i, c_i \in Z_q^*$, computes $TVP_{ij} = r_i \cdot P$, sets $h_1(r_i \cdot PK||L_t) = \varepsilon_i$, $PID_{Vij} = RID_{Vi} \oplus \varepsilon_i$, $h_2(PID_{Vij}||TVP_{ij}||L_t) = c_i$, $KV_{ij} = \perp$, and stores $(PID_{Vij}, r_i, TVP_{ij}, c_i, KV_{ij}, L_t)$ into L_R, $(r_i \cdot PK||L_t, \varepsilon_i)$ into L_{h1}, and $(PID_{Vij}||TVP_{ij}||L_t, c_i)$ into L_{h2}. ζ returns PID_{Vij} to A.
  - ◇ If $RID_{Vi} \neq RID_{VC}$, ζ generates three random numbers $r_i, \varepsilon_i, c_i \in Z_q^*$, computes $TVP_{ij} = r_i \cdot P - c_i \cdot PK$, sets $h_1(r_i \cdot PK||L_t) = \varepsilon_i$, $PID_{Vij} = RID_{Vi} \oplus \varepsilon_i$, $h_2(PID_{Vij}||TVP_{ij}||L_t) = c_i$, $KV_{ij} = r_i$, and stores $(PID_{Vij}, r_i, TVP_{ij}, c_i, KV_{ij}, L_t)$ into L_R, $(r_i \cdot PK||L_t, \varepsilon_i)$ into L_{h1}, and $(PID_{Vij}||TVP_{ij}||L_t, c_i)$ into L_{h2} respectively. ζ returns PID_{Vij} to A.
- $TSend - Oracle$: After ζ receiving A's query with PID_{Vij}, ζ checks whether PID_{Vij} exists in the list L_R. If not, ζ operates $Register - Oracle$, generates a tuple $(PID_{Vij}, r_i, TVP_{ij}, c_i, KV_{ij}, L_t)$ and stores it into L_R. Otherwise, ζ generates two random numbers $\alpha_i, \beta_i \in Z_q^*$, computes $X = \alpha_i \cdot P$, $V_1 = \alpha_i \times \beta_i + r_i$, sets $h_3(X||PID_{Vij}||TVP_{ij}||T_1) = \beta_i$, and stores $(X||PID_{Vij}||TVP_{ij}||T_1, \beta_i)$ into L_{h3}. Then, ζ returns $\{PID_{Vij}, TVP_{ij}, X, T_1, V_1\}$ to A.
- $RSend - Oracle$: ζ operates according to the specification of the proposed scheme and returns the result of response to A.

Based on above queries, A outputs the message $\{PID_{Vij}, TVP_{ij}, X, T_1, V_1\}$. ζ checks whether the following equation holds.

$$V_1 \cdot P = \beta_i \cdot X + TVP_{ij} + c_i \cdot PK \tag{10}$$

If it does not hold, ζ aborts this process. if A can forge the message $\{PID_{Vij}, TVP_{ij}, X, T_1, V_1'\}$, A is able to successfully authenticate to the RSU. According to the forgery lemma [4], [34], the following equation can be got.

$$V_1' \cdot P = \beta_i \cdot X + TVP_{ij} + c_i' \cdot PK \tag{11}$$

According to the equation (11) and (12), we can get

$$(V_1 - V_1') \cdot P = (c_i - c_i') \cdot PK = (c_i - c_i') \times sk \cdot P \tag{12}$$

and

$$(V_1 - V_1') = (c_i - c_i') \times skmodq \tag{13}$$

Thus, $(c_i - c_i')^{-1}(V_1 - V_1')$ is the answer of DL problem. Obviously, it is a contradictory assumption. Therefore, there is no polynomial adversary can forge a legitimate vehicle's authentication message with a non-negligible probability.

Lemma 2: (Secure RSU authentication): In our proposed scheme, if h_0, h_1, h_2, h_3, h_4 are ideal random functions and $\prod_V^s$ has been accepted, then there is no polynomial adversary against the proposed scheme who can forge a legal RSU authentication message with a non-negligible probability.

Proof. We assume that the adversary A can forge a legal RSU authentication message with a non-negligible probability ϵ. Then there is a challenger ζ who can resolve the CDH problem with a non-negligible probability. Given an instance $(P, TKP_i = k_{Rj} \cdot P, B = x \cdot P)$ of CDH problem, the task of ζ is to compute $xk_{Rj} \cdot P$. ζ sends the system parameters $\{G_1, P, PK, h_0, h_1, h_2, h_3, h_4\}$ and TKP_i to A. Assume that ID_{R0} is the identity of challenge. ζ answers the $h_i(i = 0, 1, 2, 3, 4)$ query, Register query as he does in the proof of Lemma 1. Then ζ answers other queries as follows:

- $TSend - Oracle$:ζ operates according to the specification of the proposed scheme and returns $\{X, CT_1, V_1, T_1\}$ to A.
- $RSend - Oracle$:ζ checks whether $ID_{Rj} = ID_{R0}$ holds. If not,ζ operates according to the specification of the proposed scheme and returns $\{CT_2, V_2, T_2\}$ to A. Otherwise,ζ aborts the game.

Based on above queries, if A can forge the message $\{CT_2, V_2, T_2\}$, A is able to successfully authenticate to the vehicle. There may be two cases to forge $\{CT_2, V_2, T_2\}$.

- ◇ A can guesses V_2 correctly without knowing k_{Rj}. The probability of this case is equal to the probability of the hash collision. That is $1/2^{l/2}$, where l is the output bit length of h_0. Obviously, it is negligible.
- ◇ A gets k_{Rj} and asks the h_0 query. It means that $k_{Rj} \cdot X$ is the solution to the CDH problem. Obviously, it is a contradictory assumption.

Therefore, there is no polynomial adversary can forge a legal RSU's authentication message with non-negligible probability.

Lemma 3: (Secure anonymous pseudo-ID): In our scheme, if h_0, h_1, h_2, h_3, h_4 are ideal random functions and $\prod_V^s$ and $\prod_R^s$ have been accepted, then there is no polynomial adversary against the proposed scheme who can distinguish the pseudo-ID and a random number with a non-negligible probability.

Proof. The adversary A asks the $h_i(i = 0, 1, 2, 3, 4)$ query, $TSend - Oracle$, $RSend - Oracle$ and $Test - query$. ζ chooses a random bit $b \in \{0, 1\}$. If $b = 1$,ζ returns the pseudo-ID PID_{ik} to A, otherwise, ζ returns a random number to A. If A can distinguish the pseudo-ID PID_{ik} with a random number, he must know x or k_{Rj}. According to the proof of Lemma 1 and Lemma 2, if A obtains x or k_{Rj}, he must know the solution of the CDH problem. Obviously, it is a contradictory assumption. Therefore, there

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2018.2834224, IEEE Access

is no polynomial adversary against the proposed scheme who can distinguish the pseudo-ID and a random number with a non-negligible probability.

Theorem 1: Our proposed scheme is secure protocol, if: (A)$\prod_V^s$ and $\prod_R^s$ have been accepted; (B)h_0, h_1, h_2, h_3, h_4 are ideal random functions; (C) the DL problem is hard; (D) the CDH problem is hard.

Proof. Based on Lemma 1 and Lemma 2, we can know that there is no polynomial adversary can forge a legal vehicle or RSU if DL and CDH problem are hard. According to the definition 2, the proposed scheme is a secure protocol.

B. FURTHER SECURITY ANALYSIS OF THE PROPOSED SCHEME

1) Mutual authentication

According to Theorem 1, we can know that there is no polynomial adversary can forge a legal vehicle or RSU if DL and CDH problem are hard. Therefore, the vehicle and the RSU can successfully authenticate each other.

2) Resistance to forgery or modification of message

In our scheme, traffic-related messages are protected by signature value σ_i. When the vehicle or the RSU receives the traffic-related messages $\{M_i, TP_{ui}, PPID_i, t_i, TP_{wi}, \sigma_i\}$, he/she can verify the validity and integrity by checking whether the equation $\sigma_i \cdot P = TP_{ui} + h_{i2} \cdot TRP_i + h_{i3} \cdot TP_{wi}$ holds, where $h_{i2} = h_2(PPID_i||TP_{ui}||t_i)$, $h_{i3} = h_3(TP_{ui}||TP_{wi}||PPID_i||t_i||M_i)$. Therefore, the adversary cannot forge or modify traffic-related messages, the proposed scheme can provide message integrality authentication.

3) Identity privacy preserving

In the proposed scheme, the vehicle's real identity is encoded into pseudo-ID. Thus, no one, except for TRA, is able to get the real identity of the vehicle without the system private key sk. Besides, in the authentication and member secrets generate phase, the pseudo-ID of the vehicle is transmitted in the form of a cipher, which is changed with the timestamp. So, the adversary never even extract pseudo-ID without the secret x or k_{Rj}. In this case, the RSU still get the vehicle's real identity even if he/she receives the pseudo-ID of the vehicle. In the anonymous identity generation and message signing phase, the pseudo-ID of the vehicle is protected by $h_1(u_i \cdot PK||t_i)$. The adversary has to solve the CDH problem if he/she want to get the pseudo-ID of the vehicle. Therefore, this proposed scheme can provide identity privacy.

4) Non-repudiation

Every message the vehicle broadcasted is bound to the protected pseudo-ID, timestamp and identity-based signature. Upon receiving the broadcast message, the vehicle or RSU will verify the correctness of the message. Anyone cannot forge the signature of the message without secret key r_{Rj}. Besides, r_{Rj} is updated in a short period. Therefore, if the TPD of the vehicle is compromised, the whole system cannot damage.

5) Traceability

In our scheme, TRA can trace the vehicle by extracting real identity from every broadcast messages $\{M_i, TP_{ui}, PPID_i, t_i, TP_{wi}, \sigma_i\}$, where $TP_{ui} = u_i \cdot P$, $PPID_i = PID_{Vik} \oplus h_1(u_i \cdot PK||t_i)$. TRA computes $PID_{Vik} = PPID_i \oplus h_1(sk \cdot TP_{ui}||t_i)$, and extracts the real identity through the the vehicle identity information table. Therefore, the proposed scheme can provide traceability.

6) Unlinkability

The proposed scheme adopts two random numbers(u_i and w_i) and timestamp to support unlinkability for the vehicle. If the adversary has intercepted multiple broadcast messages $\{M_i, TP_{ui}, PPID_i, t_i, TP_{wi}, \sigma_i\}$ of the vehicle, he/she still cannot link them generated by the same vehicle, where $TP_{ui} = u_i \cdot P$, $PPID_i = PID_{Vik} \oplus h_1(u_i \cdot PK||t_i)$, $TP_{wi} = w_i \cdot P$, $\sigma_i = V_{ui} + h_3(TP_{ui}||TP_{wi}||PPID_i||t_i||M_i) \times w_i mod q$. The reason is that two random numbers and timestamp is fresh and different at every broadcast. Therefore, our scheme for VANETs can provide unlinkability.

7) Resistance to impersonation attack

To impersonate a vehicle in the authentication and member secrets generate phase, the adversary must generate legitimate authentication messages V_1. According to Lemma 1, there is no polynomial adversary can forge a legitimate vehicle's authentication message with a non-negligible probability if DL problem is hard. So the adversary cannot impersonate a legitimate vehicle in the authentication and member secrets generate phase. Similarly, it is concluded that the adversary cannot impersonate a legitimate RSU in the authentication and member secrets generate phase based on Lemma 2. For the anonymous identity generation and message signing phase, every broadcast message $\{M_i, TP_{ui}, PPID_i, t_i, TP_{wi}, \sigma_i\}$ is protected signature value, where $\sigma_i = V_{ui} + h_3(TP_{ui}||TP_{wi}||PPID_i||t_i||M_i) \times w_i mod q$. According to the proof of reference [4], the adversary cannot forge the legitimate signature without the private key. Therefore, our proposed scheme can be security in impersonation attack.

8) Resistance to reply attack

The proposed scheme adopts timestamp to withstand reply attack. In the authentication and member secrets generate phase, the current timestamps T_1 and T_2 are included in the transmitted messages X, CT_1, V_1, T_1 and CT_2, V_2, T_2. Thus, the receiver can verify whether the message is replyed by checking the freshness of T_1 and T_2. In the anonymous identity generation and message signing phase, every broadcast message $\{M_i, TP_{ui}, PPID_i, t_i, TP_{wi}, \sigma_i\}$ also contain current timestamp. The adversary cannot forge the legitimate signature value using t_i binding without the private key. Therefore, our proposed scheme can resist against replying attack.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2018.2834224, IEEE Access

V. COMPARISONS

This section compares the qualitative property, computational costs and communication overheads of our proposed scheme with other related schemes such as He et al.'s scheme [4], Lo and Tsai's scheme [9] and Zhang et al.'s scheme [8]. To measure the effectiveness of our proposed scheme, we present the comparison results in different tables.

A. QUALITATIVE COMPARISONS

The analysis of qualitative property includes TPD compromised, storage cost, using online TRA. In Table 2, we summarize the qualitative property of the proposed scheme with other related schemes.

The purpose of TPD compromised is to evaluate the reliance on TPD, which states the security level of the whole system under the TPD compromised. In our proposed scheme, the TPD of the vehicle only stores local RSU's secret key. If this secret key is revealed by an adversary, only a limited number of vehicles who are in the same cover range of RSU can be affected. Besides, the secret key in the TPD will be updated in a short period. After this short period, the cover range of RSU has a new secret key, and the adversary may not extract sufficient secret information [8]. So, our scheme is the local danger under the TPD compromised. In He et al.'s scheme [4], the master system secret key is stored in vehicle's TPD. Obviously, when a vehicle is corrupted, the whole system will be in damage. In Lo and Tsai's scheme [9], the TPD of the vehicle stores only its own pseudo-IDs and corresponding private key. It does not affect system security if its own secret leaked. Similarly, Zhang et al.'s scheme [8] is the local danger. Because the vehicle's TPD stores local RSU's secret key, which updates in a short period.

The storage cost includes the secret parameters stored in vehicle's TPD prior to development. To achieve convincing comparisons in storage cost, assume that the bit length of hash output, the validity lifetime L_t and authentication key are 160, 64 and 256 bits, the bit length of the element in G_1 and G_2 are 160 and 1024 bits (because the security strength of the 160 bits elliptic curve is approximately equal to the 1024 bits RSA [12]), respectively. In our scheme, the TPD of a vehicle needs to store pseudo-IDs $PIDV_i$, corresponding private keys (TVP_i, KV_i), validity lifetime L_t and member secres (r_{Rj}, L_{Rt}), which need $(64n + 320n + 320n + 64 + 320 + 64) = 740n + 448$, where n is the number of element in set pseudo-IDs. Similarly, the total storage cost of the other related schemes can be computed in Table 2. Note, the storage cost of Lo and Tsai's scheme [9] in Table 2 uses a parameter m, which is similar to n and denotes the number of elements in set pseudo-IDs. Since the pseudo-ID in our scheme is used for authentication and member secrets generate phase, while one in Lo and Tsai's scheme [9] is used for the broadcasting message. Besides, the pseudo-ID in our scheme is communicated in ciphertext form, which can be reused again. Therefore, m is much greater than n.

When the vehicle enters into the cover range maintained by an RSU, it must achieve mutual authentication between the vehicle and the RSU. All of the above-mentioned schemes except for Zhang et al.'s scheme [8] do not need online TRA to achieve authentication. In Zhang et al.'s scheme [8], the RSU has to complete authentication with the help of online TRA, which may make the trusted third party being a bottleneck of security.

TABLE 2. Qualitative comparisons between our proposed scheme and other related schemes

Qualitative property	He [4]	Lo [9]	Zhang [8]	Ours
TPD compromised	danger	security	local danger	local danger
Storage cost	448	$1088m$	1504	$740n$+448
Using online TRA	no	no	Yes	no

From comparison in Table 2, it can be concluded that the proposed scheme is superior qualitative property among the above schemes, which balances these three qualitative properties. Compared with He et al.'s scheme [4], this proposed scheme is less dependent on TPD. If the vehicle's TPD is compromised, only the cover range of the same RSU cloud be affected. Meanwhile, our scheme needs less storage than Lo and Tsai's scheme [9]. Although Lo and Tsai's scheme [9] has the advantage in TPD compromised, it requires a vast amount of storage space for secret parameters. The reason is that a vehicle in VANETs may broadcast message frequently. So the number m in Table 2 is much greater than n in our scheme. Furthermore, Zhang et al.'s scheme [8] seems to be efficient in TPD compromised and storage cost. But in practice, it requires a fully trusted third party to participate in each vehicle authentication and member secrets generate phase, which may make the trusted third party being a bottleneck of security. Therefore, our proposed scheme is more suit for the realistic VANETs environment.

B. COMPUTATION ANALYSIS

For efficiency analysis, we compare the computation cost of our proposed scheme with the prior related schemes [4], [8], [9]. Because the initialization phase, registration phase and authentication and member secrets generate phase are not used frequently, we only compare anonymous identity generation and message signing phase, message verification phase. Almost all of the operations in our scheme and prior related schemes have appeared in He et al.'s scheme [4], we continue to follow the running time of all operations in their scheme. To facilitate analysis, we use the following notations and their running time to measure the computation cost.

(1) T_{bp}: The execution time of bilinear pairing operation, which takes about 4.2110ms;
(2) T_{sm}: The execution time of point multiplication operation in G_1, which takes about 0.4420ms;
(3) T_{pa}: The execution time of point addition operation in G_1, which takes about 0.0018ms;
(4) T_{exp}: The execution time of exponentiation operation in G_2, which takes about 0.0050ms;
(5) T_h: The execution time of general hash function, which takes about 0.0001ms.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2018.2834224, IEEE Access

The results of computation cost comparisons are summarized in Table 3. From Table 3, we can see that the computation cost of our scheme is as efficient as He et al.'s scheme [4]. Although the computation cost in Lo and Tsai's scheme [9] and Zhang et al.'s scheme [8] is less than our scheme, they achieve at the price of storage cost or heavy bilinear pairings operations.

TABLE 3. Computation comparisons between our proposed scheme and other related schemes

Scheme	Signature generate	Signature verification	n Batch verification
He [4]	$3T_{sm}+3T_h \approx 1.3263ms$	$3T_{sm} + 2T_h + 2T_{pa} \approx 1.3298ms$	$(n+2)T_{sm} + (n+2)T_{pa} + (2n)T_h \approx 0.444n + 0.8876ms$
Lo [9]	$T_{sm} + T_h \approx 0.4421ms$	$3T_{sm} + 2T_h + 2T_{pa} \approx 1.3298ms$	$(n+2)T_{sm} + (n+2)T_{pa} + (2n)T_h \approx 0.444n + 0.8876ms$
Zhang [8]	$5T_{exp}+3T_h \approx 0.0253ms$	$2T_{bp} + T_{exp} + 3T_h \approx 8.4273ms$	$(n+1)T_{bp} + nT_{exp} + 3nT_h \approx 4.2161n + 4.211ms$
Ours	$3T_{sm}+3T_h \approx 1.3263ms$	$3T_{sm} + 2T_h + 2T_{pa} \approx 1.3298ms$	$(n+2)T_{sm} + (n+2)T_{pa} + (2n)T_h \approx 0.444n + 0.8876ms$

C. COMMUNICATION ANALYSIS

In this section, we compare communication cost of our proposed scheme with the two prior related schemes [4], [8], [9]. To achieve convincing comparisons, we assume that the bit length of hash output and the timestamp t_i are 20 and 4 bytes, the bit length of the elements in G_1 and G_2 are 20 and 128 bytes, respectively. Furthermore, assume that the size of signature messages are same in all comparison schemes. The results of communication efficiency comparisons are summarized in Table 4.

In the proposed scheme, the signature messages $\{TP_{ui}, PPID_i, t_i, TP_{wi}, \sigma_i\}$ require (40+20+4+40+40)=144 bytes. For He et al.'s scheme [4], the signature messages $\{AID_i, T_i, R_i, \sigma_i\}$ require (40+20+4+40+40)=144 bytes, where $AID_i = (AID_{i1}, AID_{i2})$, $AID_{i1}, R_i \in G_1$, $\sigma_i \in Z_q$, t_i is the timestamp, AID_{i2} is pseudo-ID. For Lo and Tsai's scheme [9], the signature messages $\{PID_{ik}, tt_i, \sigma\}$ require (40+20+4+4+40+40+40)=188 bytes, where $PID_{ik} = (PID_{i1}, PID_{i2}, t_i)$, $\sigma = (K_i, R_i, V_i)$, $PID_{i1}, K_i, R_i \in G_1$, $V_i \in Z_q$, tt_i and t_i is the timestamp, PID_{i2} is pseudo-ID. For Zhang et al.'s scheme [8], the signature messages $\{PPID_{i,t}, \sigma_{i,t}\}$ require (20+128)=148 bytes, where $PPID_{i,t}$ is the timestamp, $\sigma_{i,t} \in G_2$.

From comparison in Table 4, we conclude that the proposed scheme is more efficient than Lo and Tsai's scheme [9], Zhang et al.'s scheme [8], and as efficient as He et al.'s scheme [4] in communication overhead.

TABLE 4. Computation comparisons between our proposed scheme and other related schemes

Scheme	Sending a signature message	Sending n signature messages
He [4]	144 bytes	$144n$ bytes
Lo [9]	188 bytes	$188n$ bytes
Zhang [8]	148 bytes	$148n$ bytes
Ours	144 bytes	$144n$ bytes

VI. CONCLUSION

In this paper, we propose a realistic distributed conditional privacy-preserving authentication scheme for VANETs. The proposed scheme can provide various kinds of security requirements without an ideal TPD, such as privacy-preserving, conditional unlinkability, and non-repudiation, etc. Besides, in comparison with Zhang et al.'s scheme [8], the proposed scheme does not require a trusted third party to participate in each vehicle authentication and member secrets generate phase. The security analysis demonstrates that our scheme is secure against active and passive attacks. Performance analysis shows that the proposed scheme can be deployed in practice for VANETs while achieving a balance between security and efficiency.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers and the Associate Editor for providing constructive and generous feedback.

REFERENCES

[1] Y. Toor, P. Muhlethaler, and A. Laouiti, "Vehicle ad hoc networks: Applications and related technical issues," IEEE communications surveys & tutorials, vol. 10, no. 3, 2008.

[2] F. Qu, Z. Wu, F.-Y. Wang, and W. Cho, "A security and privacy review of vanets," IEEE Transactions on Intelligent Transportation Systems, vol. 16, no. 6, pp. 2985–2996, 2015.

[3] J. B. Kenney, "Dedicated short-range communications (dsrc) standards in the united states," Proceedings of the IEEE, vol. 99, no. 7, pp. 1162–1182, 2011.

[4] 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 and Security, vol. 10, no. 12, pp. 2681–2691, 2015.

[5] J.-P. Hubaux, S. Capkun, and J. Luo, "The security and privacy of smart vehicles," IEEE Security & Privacy, vol. 2, no. 3, pp. 49–55, 2004.

[6] A. Rahim, X. Kong, F. Xia, Z. Ning, N. Ullah, J. Wang, and S. K. Das, "Vehicular social networks: A survey," Pervasive and Mobile Computing, 2017.

[7] X. Kong, F. Xia, Z. Ning, A. Rahim, Y. Cai, Z. Gao, and J. Ma, "Mobility dataset generation for vehicular social networks based on floating car data," IEEE Transactions on Vehicular Technology, 2018.

[8] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, and C. Hu, "Distributed aggregate privacy-preserving authentication in vanets," IEEE Transactions on Intelligent Transportation Systems, vol. 18, no. 3, pp. 516–526, 2017.

[9] N.-W. Lo and J.-L. Tsai, "An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings," IEEE Transactions on Intelligent Transportation Systems, vol. 17, no. 5, pp. 1319–1328, 2016.

[10] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," Journal of Computer Security, vol. 15, no. 1, pp. 39–68, 2007.

[11] F. Wang, Y. Xu, H. Zhang, Y. Zhang, and L. Zhu, "2flip: A two-factor lightweight privacy-preserving authentication scheme for vanet," IEEE Transactions on Vehicular Technology, vol. 65, no. 2, pp. 896–911, 2016.

[12] S. S. Manvi and S. Tangade, "A survey on authentication schemes in vanets for secured communication," Vehicular Communications, vol. 9, pp. 19–30, 2017.

[13] M. Raya and J.-P. Hubaux, "The security of vehicular ad hoc networks," in Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks, pp. 11–21, ACM, 2005.

[14] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "Gsis: A secure and privacy-preserving protocol for vehicular communications," IEEE Transactions on vehicular technology, vol. 56, no. 6, pp. 3442–3456, 2007.

[15] L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer, "A scalable robust authentication protocol for secure vehicular communications," IEEE Transactions on vehicular Technology, vol. 59, no. 4, pp. 1606–1617, 2010.

[16] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, "Amoeba: Robust location privacy scheme for vanet," IEEE Journal on Selected Areas in communications, vol. 25, no. 8, 2007.

[17] J. Sun, C. Zhang, Y. Zhang, and Y. Fang, "An identity-based security system for user privacy in vehicular ad hoc networks," IEEE Transactions on Parallel and Distributed Systems, vol. 21, no. 9, pp. 1227–1239, 2010.

[18] X. Lin, X. Sun, X. Wang, C. Zhang, P.-H. Ho, and X. Shen, "Tsvc: Timed efficient and secure vehicular communications with privacy preserving," IEEE Transactions on Wireless Communications, vol. 7, no. 12, pp. 4987–4998, 2008.

[19] C. Zhang, X. Lin, R. Lu, P.-H. Ho, and X. Shen, "An efficient message authentication scheme for vehicular communications," IEEE Transactions on Vehicular Technology, vol. 57, no. 6, pp. 3357–3368, 2008.

[20] L. He and W. T. Zhu, "Mitigating dos attacks against signature-based authentication in vanets," in Computer Science and Automation Engineering (CSAE), 2012 IEEE International Conference on, vol. 3, pp. 261–265, IEEE, 2012.

[21] M.-C. Chuang and J.-F. Lee, "Team: Trust-extended authentication mechanism for vehicular ad hoc networks," IEEE systems journal, vol. 8, no. 3, pp. 749–758, 2014.

[22] A. Studer, F. Bai, B. Bellur, and A. Perrig, "Flexible, extensible, and efficient vanet authentication," Journal of Communications and Networks, vol. 11, no. 6, pp. 574–588, 2009.

[23] M. H. Jahanian, F. Amin, and A. H. Jahangir, "Analysis of tesla protocol in vehicular ad hoc networks using timed colored petri nets," in Information and Communication Systems (ICICS), 2015 6th International Conference on, pp. 222–227, IEEE, 2015.

[24] P. Kamat, A. Baliga, and W. Trappe, "An identity-based security framework for vanets," in Proceedings of the 3rd international workshop on Vehicular ad hoc networks, pp. 94–95, ACM, 2006.

[25] K.-A. Shim, "Cpas: An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks," IEEE Transactions on Vehicular Technology, vol. 61, no. 4, pp. 1874–1883, 2012.

[26] J. Li, H. Lu, and M. Guizani, "Acpn: a novel authentication framework with conditional privacy-preservation and non-repudiation for vanets," IEEE Transactions on Parallel and Distributed Systems, vol. 26, no. 4, pp. 938–948, 2015.

[27] 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, no. 5, pp. 351–358, 2014.

[28] M. Bayat, M. Barmshoory, M. Rahimi, and M. R. Aref, "A secure authentication scheme for vanets with batch verification," Wireless networks, vol. 21, no. 5, pp. 1733–1743, 2015.

[29] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in vanet," in Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks, pp. 19–28, ACM, 2007.

[30] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, "Eviction of misbehaving and faulty nodes in vehicular networks," IEEE Journal on Selected Areas in Communications, vol. 25, no. 8, 2007.

[31] K. P. Laberteaux, J. J. Haas, and Y.-C. Hu, "Security certificate revocation list distribution for vanet," in Proceedings of the fifth ACM international workshop on VehiculAr Inter-NETworking, pp. 88–89, ACM, 2008.

[32] J. J. Haas, Y.-C. Hu, and K. P. Laberteaux, "Design and analysis of a lightweight certificate revocation mechanism for vanet," in Proceedings of the sixth ACM international workshop on VehiculAr InterNETworking, pp. 89–98, ACM, 2009.

[33] A. Wasef and X. Shen, "Emap: Expedite message authentication protocol for vehicular ad hoc networks," IEEE transactions on Mobile Computing, vol. 12, no. 1, pp. 78–89, 2013.

[34] D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures," Journal of cryptology, vol. 13, no. 3, pp. 361–396, 2000.