IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 23, 2020, accepted August 2, 2020, date of publication August 6, 2020, date of current version August 19, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3014678

Efficient Conditional Privacy Preservation With Mutual Authentication in Vehicular Ad Hoc Networks

MAHMOOD A. AL-SHAREEDA[1], MOHAMMED ANBAR[1], (Member, IEEE), IZNAN HUSAINY HASBULLAH[1], SELVAKUMAR MANICKAM[1], AND SABRI M. HANSHI[2]

[1]National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia (USM), Gelugor 11800, Malaysia
[2]Computer Information System, Seiyun Community College, Seiyun, Yemen

Corresponding author: Mohammed Anbar (anbar@nav6.usm.my)

This work was supported in part by the National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia and External Grant from UMobile Sdn Bhd under Grant 304/PNAV/650958/U154.

ABSTRACT Vehicle Ad hoc Networks (VANETs) are an emergent wireless communication technology that has the potential to reduce the risk of accidents caused by drivers and provide a wide range of entertainment facilities. Because of the nature of VANETs' open-access environment, security attacks can affect the messages broadcast by a vehicle. VANET is therefore vulnerable to security and privacy issues. Recently, many schemes for addressing these problems of VANET have been proposed. However, most of them are affected by massive computation overhead and security issues. In this paper, we propose a scheme named efficient conditional privacy preservation with mutual authentication to address the problems mentioned above in VANET. This scheme depends on the division of geographical areas into a number domains and their distribution, where each domain stores the Certificate Revocation List (CRL) in all Road-side Units (RSUs) located inside the domain. During the mutual authentication phase, the vehicle should authenticate with the TA. After the vehicle obtains a pool of pseudo-identities and the corresponding secret keys from RSU, it is allowed to transmit a message to the other components in the VANET. Because our scheme does not use the bilinear pairing, the performance evaluation shows that our scheme has a lower system cost in terms of computation and communication than other existing methods. Meanwhile, the proposed scheme reduces the computation costs of signing the message and verifying the message by 99.85% and 99.93%, respectively. While the proposed scheme reduces the communication costs of the message size by 13.3%.

INDEX TERMS Vehicular ad-hoc network (VANET), privacy-preserving, elliptic curve, random oracle model, identity-based cryptography, domain public key.

I. INTRODUCTION

The aim of VANET is to improve road transportation. A study by the UK government on road accidents 2015 reveals that 1,732 people were killed and 22,137 were injured in road accidents [1]. VANET technology may therefore help to reduce the number of road accidents. VANETs use IEEE 802.11p technology, using the Dedicated Short Range Communication (DSRC) protocol [2]–[4]. There are three main components in a VANET system: a trusted authority (TA), a road-side unit (RSU), and an on-board unit (OBU). The TA is responsible for initializing and providing RSUs and vehicles with the system parameters, including public and private key pairs. The RSU is situated on the road and it is considered to be part of the network infrastructure, serving as a router between vehicles, whereas the radio OBU is used for the transmission and reception of security messages to other OBUs or RSUs [5]. In this case, Vehicle-To-Vehicle (V2V) and Vehicle-To-Infrastructure (V2I) can be established. The vehicles can then communicate with each other through RSU underlying the DSRC protocol [6].

In a limited area of several hundred meters, each equipped vehicle provides safe and traffic-related messages (called security messages), which include the vehicle's location, speed, heading and traffic events, more than three times a second [3]. Consequently, because of the nature of the

The associate editor coordinating the review of this manuscript and approving it for publication was Nabil Benamar.

open-access environment of VANET, whether the node is legitimate or not, they can receive the security message and manipulate it. Thus, to preserve the driver's privacy (e.g. their identity and location), the security issues (particularly on privacy requirements in VANET) need to be addressed. Malicious nodes can cause traffic jams and road accidents by sending illegal or fake messages. The VANET may be affected by illegal or fake messages, and this can lead to road incidents and traffic jams.

Several schemes have been suggested for secure authentication and privacy preservation in VANETs; however, they have huge overhead computation and communication costs. In addition, they have been unable to meet most of the requirements regarding security and privacy for VANETs, and thus they are not completely safe. Therefore, we propose a robust conditional privacy preservation scheme with mutual authentication that can address existing weaknesses in VANET schemes. Our paper's main contributions can be summarized as follows

- We propose efficient conditional privacy preservation with mutual authentication that depends on the division geographical areas into several domains, in which each domain stores the Certificate Revocation List (CRL) in all Road-side Units (RSUs) located inside the domain.
- The proposed scheme is based on Elliptic Curve Cryptography (ECC) and general one-way hash function without complex operations such as bilinear pairing and Map-To-Point function.
- A comprehensive security analysis is performed to demonstrate that the proposed scheme can withstand various attacks and satisfy all the VANET security requirements, especially on the driver's privacy.
- The achievements of the scheme are evaluated in terms of computation and communication costs. The scheme is better suited to VANET services than existing schemes.

The rest of this paper is structured as follows. A few current works are listed in Section II. Section III briefly discusses the vehicular system architecture and preliminaries. A detailed description of the proposed solution in Section IV. Sections V and VI describe the security and performance analyses, respectively. Section VII provides the conclusion.

II. RELATED WORK

In recent years, VANETs have suffered from privacy preservation and security authentication problems. Existing work on security and privacy is generally categorised into three major categories based on the methods presented in [5]:

A. PKI-BASED AUTHENTICATION SCHEME

To hide the real identity of the driver, Gamage *et al.* [7] introduced a ring signature scheme for the first time in 2006. Raya *et al.* [8] suggested an anonymous certification authentication scheme based on Public Key Infrastructure (PKI) in 2007 to ensure integrity and non-repudiation of message. In their scheme, several anonymous certifications and public-private keys are needed in advance and caused huge certification burdens for TA. However, because of a vehicle storage limit, the vehicle also suffers from the storage capacity. Therefore, during the verification process the verifier must check the message to ensure that the other vehicles are valid, which increases the system's costs.

B. GROUP-BASED AUTHENTICATION SCHEME

In 2006, several group-based authentication scheme [9]–[11] were introduced. In their schemes, the group member could create the signature anonymously on behalf of the whole group, and the group manager could resume the identity information on the group member's signature using the secret group key. In 2015, Shao *et al.* [12] proposed a threshold anonymous authentication scheme using a decentralized group model to minimize the overhead in terms of downloading and checking CRL. In this scheme, RSUs can trace the vehicle's position. This scheme uses bilinear pairing-based cryptography during the broadcasting process. Nevertheless, this scheme has some limitations, such as lack of forwarding and reversing security, collision control and unlinkability. In addition, it is also vulnerable to replay attack. In 2016, Wang *et al.* [13] investigated an efficient authentication scheme based on conditional privacy-preserving to provide the process of batch verification for V2V and V2I communications. Therefore, they proposed an Efficient Conditional Privacy-Preserving authentication scheme (ECPB) based on the group signature to enhance the efficiency of the authentication procedure in VANETs. However, the delay of average response in verification should be reduced further. In the GSIS scheme [11], only the private and public key created by the TA is stored by the vehicle rather than placing a large number of anonymous certifications and public-private keys within the vehicle's OBU, which reduces the burden of storage capacity. However, because only a group manager knows the group's secret key, no group member can resume information about signature identity. While the group signature scheme reduces a certified management burden, with the number of vehicles recovered the size of the Certificate Revocation List (CRL) increases. Due to the two bilinear pairings per operation of each CRL, the overhead computation will be increased by the signature verification. In addition, the approach of the general signature computational cost is also less than the group-based authentication scheme.

C. ID-BASED AUTHENTICATION SCHEME

To resolve the problems existing in these two authentication schemes, researchers have proposed Identity (ID)-based authentication schemes. In 1984, Shamir [14] first proposed the scheme for identity-based signature authentication. A public key is derived from identity information (e.g. name, ID card, etc.) in their scheme and a private institution generates a secret key. In 2008, in the scheme of Zhang *et al.* [15], a master TA secret key was stored in the Tamper-Proof Device (TPD), which assumes that the malicious attacker is not compromised. TA has avoided the burden of certification management and unlinkability of privacy is

achieved. In addition, an anonymous identity is used by a vehicle to hide its real identity instead of transmitting the message that attaches to its real identity during transmission. The conditional preservation of privacy is therefore accomplished. In the final phase, the authenticated batch method was used during the signature checked to verify multiple messages simultaneously transmitted from another vehicle, greatly reducing the overhead of the network. While the scheme in Zhang *et al.* [15] could achieve the preservation of privacy, other security issues must also be addressed in their scheme. Lee and Lai [16] found out in 2013 that Zhang *et al.*'s [15] scheme could not withstand some of the VANET security attacks. First, the verifier can check the previously verified signature to increase the overhead computation due to the lack of a corresponding unit. Therefore, the reply attack could not be resisted. Zhang *et al.* [15] could not further achieve non-repudiation. The singer can deny that a trustworthy institution has not sent identity information to the disputed messages. Lee and Lai [16] proposed an improved scheme for the protection of privacy to address security issues in Zhang *et al.* [15] scheme, the scheme satisfies all privacy requirements. The Lee and Lai [16] scheme later also pointed out by Zhang *et al.* [17] and Bayat *et al.* [18] were unable to withstand the impersonation attack. An attacker might spread some fake messages to gain a benefit and give themselves some convenience by simulating a legal vehicle. Therefore, there were two improved schemes for addressing the problems in Lee and Lai's [16] scheme. In 2014, Jianhong *et al.* [17] pointed out in the scheme proposed by Lee and Lai [16] that several security problems had been found, such as its failure to meet with the traceability requirement and resisting replay attacks. Nevertheless, He *et al.* [19] also found in 2015 that their scheme suffers from an attack of modification. In other words, during the broadcast message, a malicious attacker may alter the signature of the vehicle. They proposed a conditional scheme to preserve privacy to deal with security attacks and reduce the cost of the system. In 2017, Cui *et al.* [20] suggested the secure privacy-preserving authentication scheme for VANETs with Cuckoo Filter (SPACF) scheme. This scheme is based on software without heavily depending on any hardware on a Tamper-Proof Device (TPD) that is equipped in each vehicle for both V2V and V2I communication. Their scheme utilizes methods of cuckoo filter and binary search to improve the batch verification method. In 2019, Zhang *et al.* [21] proposed the Chinese remainder theorem (CRT)-based conditional privacy-preserving authentication scheme for VANETs. In their scheme, they eliminated the requirement for preloading the master key of the system into TPD of vehicle to secure communication. This scheme ensures that a fingerprint from a corrupted vehicle will not be authenticated. In the same year, Alazzawi *et al.* [22] proposed efficient anonymity with integrity and authentication of the message. This scheme based on the elliptic curve to achieve security and privacy requirement, where they use a pseudonym rather than a real identity. Moreover, the scheme [22] does not satisfy all privacy requirements, such as unlinkability, because the vehicle's anonymous identity is constant. In their scheme, the TA revokes the misbehaving vehicle when it receives a report about the malicious vehicle. It then adds the original identity of vehicle to CRL and the updated CRL sends this list to all RSUs in VANETs. After the new authentication process, the victim vehicle fails to join the system. However, with large scale networks, this approach may not have good efficiency because the number of revoked vehicles may be so large given that the size of local CRLs in all RSUs is increased. In the same year, a new RSU-based security and the privacy-preserving scheme was proposed in Bayat *et al.* [23]. In this scheme, the TA stored master keys in the tamper-proof device in the RSU. The verifier checks legitimated signature by using the public key of the RSU instead of the public key of the system. This means that the vehicle cannot check the signature of other vehicles on the road from the other RSU. Nevertheless, Bayat *et al.* [23] used the bilinear pairing and Map-To-Point operation, which caused extensive overhead computation. In addition, this scheme also affects the overhead computation with the size of CRL on all RSUs. In 2020, Cui *et al.* [24] introduced a privacy-preserving data downloading scheme to secure cooperative downloading scenario of VANETs; therefore, they proposed an edge computing-based secure and privacy-preserving cooperative downloading scheme. This scheme uses lightweight cryptography methods rather than time-consuming bilinear pairing.

We propose an efficient conditional privacy preservation with mutual authentication scheme to resolve the problems arising in the VANETs. In terms of geographical area, the scheme divides the system of VANETs into several domains, which stores one CRL in all RSUs per each domain. Therefore, the TA updated list of CRL into all RSUs inside one domain instead of all of the systems. The computation and communication cost of the proposed scheme is low because it does not use bilinear pairing in the design.

III. VEHICULAR SYSTEM ARCHITECTURE AND PRELIMINARY

This section describes the system model, types of attacks, security and privacy requirements and mathematical tools. Table 1 contains some notation and their description.

A. SYSTEM MODEL

According to Figure 1, the proposed scheme consists of three components: many vehicles running on the road, some roadside units fixed on the road and trusted authority. The details of those three components are described as follows:

1) OBU

An OBU is a radio that is equipped to transmit and received messages from other OBUs or RSUs in a vehicle operating in the DSRC protocol. Vehicles that drive along the roads exchange collective information about the environment or query for secret keys by the RSUs. Secure storage of private

TABLE 1. Notation and their description.

Notation	Descriptions
TA	The Trust Authority
RSU_i	the jth road side unit
OBU_i	The ith vehicle
E	An elliptic curve
G	An additive group based on E
a, b	Two large prime number
p	large prime number
P	The base generator P$\in$ G
h_1, h_2, h_3	Three one-way hash function
RID_r,RID_i	Real identity of the RSU and vehicle
PW_i	Password
x_{pri}^{TA}	The private master key of the system
P_{Pub}^{TA}	The public key of the TA
$s_{Pri}^{dom_i}$	The private master key of the $domain_i$
$P_{Pub}^{dom_i}$	The public key of the $domain_i$
r	Random integer
$\|$	Concatenation operation
$\oplus$	XOR operator
L_{PID_i}	List of OBU_i's local Pseudo identities
L_{SK_i}	List of OBU_i's local Private keys

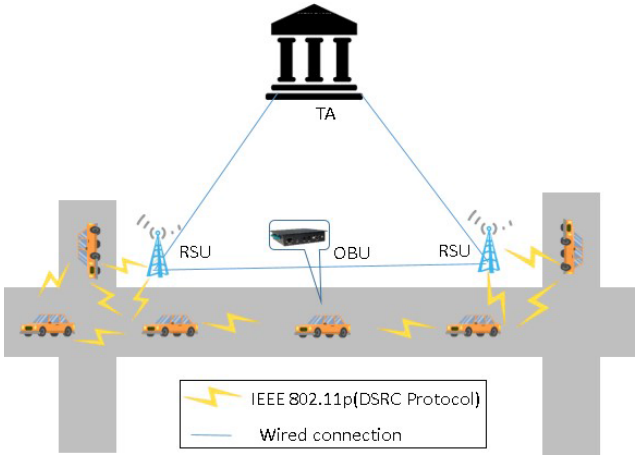

FIGURE 1. System model.

keys is embedded in OBUs. The security message is transmitted by the vehicle every 100 to 300 ms through the DSRC protocol.

2) RSU

RSUs are situated as routers among vehicles along the road and are considered to be part of the network infrastructure. An RSU administers all of the OBU's communication and publishes security messages within its area. It can also be used to exchange messages to other RSUs via a secure wired network. Each RSU has a Tamper-Proof Device (TPD) to store private keys from the system. Therefore, it is possible for anyone to disclose it. In addition, every RSU has its own identity RID_R.

3) TA

The TA is a completely trusted party in a VANET and is responsible for system parameters generation, communicates via wired and wireless communication with RSUs and vehicles, respectively. The TA is hard to compromise and has good computation and storage resources. In an emergency situation, the TA can identify a signer's real identity.

B. TYPES OF ATTACKS

VANETs are easily vulnerable to certain security threats because of their open communication environment. We will introduce some vulnerabilities in the VANETs under this subsection.

1) REPLY ATTACK

The attacker replays the legitimate signature previously received by the recipient.

2) IMPERSONATION ATTACK

An attacker could send fake signatures of a legitimate vehicle to other users.

3) MODIFICATION ATTACK

An attacker can edit and send a valid message to other users.

4) MAN-IN-THE-MIDDLE ATTACK

The attacker intercepts messages and allows sniffing and manipulation of data. The facts are not known on both sides of the communication.

C. SECURITY AND PRIVACY REQUIREMENTS

This paper focuses on the following security and privacy requirements:

1) MESSAGE INTEGRITY AND AUTHENTICATION

A receiver (vehicle or RSU) must be able to verify the receiving security message in a VANET to guarantee that it is legal.

2) IDENTITY PRIVACY PROTECTION

By analyzing multiple messages sent by the same vehicle, the attacker cannot obtain the identity

3) TRACEABILITY AND REVOCABILITY

An attacker can send malicious messages using anonymity to attack the VANET. However, the authentication scheme can get the identity of the malicious vehicle and revoke it from VANETs during malicious behaviors.

4) UNLINKABILITY

RSUs, vehicles, and participants from a third-party cannot track the actions of the vehicles by examination of its transmitted messages. In other words, they can not link and determine if two messages are sent from the same vehicles.

5) NO LARGE CRL

By increasing the number of revoked vehicles, the size of the CRL will be unlimited. The time-consuming checking of the certificate revocation list greatly reduces authentication performance. To improve the feasibility and effectiveness of

the VANET, the authenticity of the certificate must be reduced in all RSUs. Therefore, The scheme does not store the original identity of malicious vehicles on all RSUs of VANETs.

6) RESISTANCE AGAINST DIFFERENT TYPES OF ATTACKS

VANETs suffer from a number of security attacks. Therefore, their schemes must be able to resist attacks by attackers to guarantee security and reliability.

D. MATHEMATICAL TOOLS

In this subsection, we described the Elliptic Curve Cryptography (ECC) and the respective computationally difficult problems.

1) ECC

Let F_p represent a finite field of order p on E, where p is a large prime number and E is non-singular elliptic curve. Assume a set of an infinity point O on E over F_p utilizes an equation $y^2 = x^3 + ax + b \bmod p$, where the discriminant $\Theta = 4a^3 + 27b^2 \neq 0$ and a, b $\in F_p$. The elliptic curve E forms an additive cyclic group G under the operation of point addition $P + Q = R$. Scalar multiplication operation over F_p is expressed as $lP = P + P + \ldots + P$ for l times, where $l \in Z_q^*$ and $l > 0$.

2) COMPUTATIONALLY DIFFICULT PROBLEMS

The computationally difficult problems based on group G are considered as follows:

- **Elliptic Curve Discrete Logarithm (ECDL) problem:** Given two random points P and Q of group G on E. The primary task of ECDLP is to find an integer $s \in Z_q^*$ that satisfies $Q = sP$, where the unknown number s is difficult to compute. Thus, it is assumed that the problem of ECDL becomes computationally infeasible for any Probabilistic Polynomial Time (PPT) algorithms to solve with non-negligible probability.
- **Elliptic Curve Computational Differ-Hellman (ECCDH) problem:** Given two random points K and Q of group G on E, where $K = bP$, $Q = sP$ and $b, s \in Z_q^*$, the point $bsP \in G$ is difficult to calculate. Thus, it is assumed that the problem of ECCDH becomes computationally infeasible for any PPT algorithms to solve with non-negligible probability.

IV. THE PROPOSED SCHEME

VANET security attacks and privacy preservation are two important problems that are addressed in this paper. Numerous schemes to address the current issue of VANETs have been proposed in recent years. They are, however, affected by the high computational and communication cost. Without using a bilinear pair to address the security issue and reduce the overhead system, we propose an efficient conditional privacy preservation scheme with mutual authentication in VANETs. The architecture of the proposed scheme is described in Figure 2: the offline registration and the driving stage which consists of two main stages in the proposed scheme. The three phases of the offline registration stage are TA initialization, RSU and vehicle registration. The five phases of the driving stage are joining, signing of messages, verification of messages, renew lists and real identity tracking and revocation. The proposed scheme consists of two parts as follows:

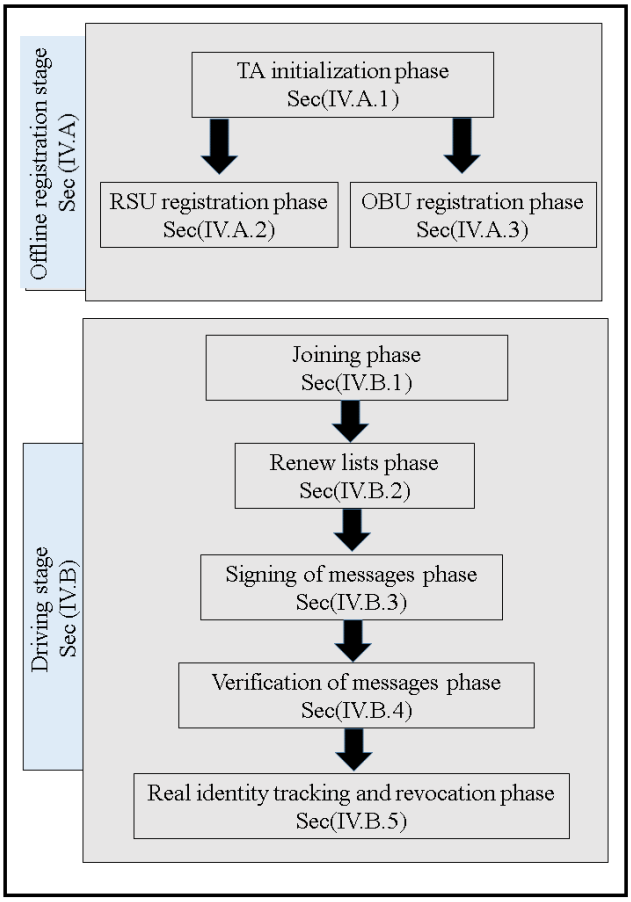

FIGURE 2. The architecture of proposed scheme.

A. OFFLINE REGISTRATION STAGE

The system initialisation phase is introduced in this section. During factory and annual inspections, OBU and RSU are registered offline.

1) TA INITIALISATION PHASE

Initial system parameters are generated by the TA and system parameters are updated to maintain the security of the system by using the following steps.

- The TA chooses two large numbers (p and q) at random. The TA then selects a non-singular elliptic curve E representing $y^2 = x^3 + ax + b \bmod p$, where $a, b \in F_p$ is defined.
- The TA selects a group of elliptic curve points with a prime order q and a generator P of G.

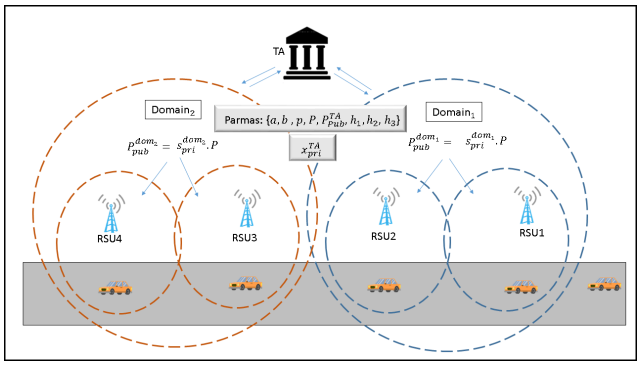

FIGURE 3. RSU registration in domain by TA.

- A random privacy key can be chosen for the number $x^{TA}_{pri} \in Z^*_q$ and a public key can be determined as $P^{TA}_{Pub} = x^{TA}_{pri}.\mathrm{P}$.
- TA chooses symmetric encryption function $E_\pi(.)/D_\pi(.)$.
- Finally, the TA chooses three cryptographic hash functions h_1, h_2 and h_3, where
  $-h_1 : G \rightarrow Z^*_q$
  $-h_2 : \{0, 1\}^* \times \{0, 1\}^* \times G \rightarrow Z^*_q$
  $-h_3 : \{0, 1\}^* \rightarrow Z^*_q$.

2) RSU REGISTRATION PHASE

As shown in Figure 3, RSU are registered by the TA as follows:

- According to the RSU deployment in area [2], the TA selects the number of RSUs located in a specific area as the domain. TA selects the RSU identity RID_r based on its location in this domain.
- The TA chooses $s^{dom_i}_{Pri} \in Z^*_q$ numbers randomly as the private key in $domain_i$ for all RSUs and determines $P^{dom_i}_{Pub} = x^{dom_i}_{Pri}.\mathrm{P}$ as its corresponding public key. The TA keeps the $s^{dom_i}_{Pri}$ private key in all RSUs within the $domain_i$ with x^{TA}_{pri} in all domains.
- The public parameters parmas $= \{p, q, a, b, \mathrm{P}, P^{TA}_{Pub}, h_1, h_2, h_3\}$ are preloaded by TA for each RSU.
- The TA preloads the private key x^{TA}_{pri} of the system to TPD of each RSU.

3) VEHICLE REGISTRATION PHASE

Vehicle are registered by the TA as follows:

- TA chooses the identity RID_i and password PW_i, which it then sends to OBU_i and the owner of vehicle.
- Public parameters parmas $= \{p, q, a, b, \mathrm{P}, P^{TA}_{Pub}, h_1, h_2, h_3\}$ are preloaded by the TA at each OBU.

B. DRIVING STAGE

The vehicle should perform the joining process using TA to be considered as authentic node. After the vehicle obtains a list of n local pseudo identities and the corresponding secret keys from the RSU, it creates a message signature which is checked by the verifier. Meanwhile, n is the anonymous level of security, which is the number of pseudo that a vehicle can use unrepeatably in an RSU area [25]. When the malicious attacker imitates the vehicle's legal identity, the TA should have the ability to retrieve the vehicle's identity information. The details follow:

1) JOINING PHASE

To start the OBU_i, a vehicle's owner should provide RID_i and PW_i input from the OBU_i to confirm that the owner is legitimate. If valid, then the OBU_i begins the process of joining. Figure 4 describes the top-level authentication process of the proposed scheme.

- A random integer $r \in Z^*_q$ is generated by OBU_i and computes $PID^1_i = rP$ and $PID^2_i = RID_i \oplus h_1(R_i)$, where $R_i = rP^{TA}_{Pub}$. Then the OBU_i transmits the RSU_j with $\{PID_v, T_1, \sigma_{OBU_i}\}$, where $PID_v = \{PID^1_i, PID^2_i\}$ and $\sigma_{OBU_i} = h_3(RID_i \| PID^1_i \| PID^2_i \| T_1)$.
- The first test on the validity of the timestamp T_1 will take place after RSU_j receives the $\{PID_v, T_1, \sigma_{OBU_i}\}$ message. The following is tested per timestamp T. Assume that T_r is the time of receipt, then T is valid if (T > T_r - T_∇), where T_∇ is the time delay predefined. Otherwise, a reply attack will occur and the message will be refused. If T_1 is valid, then RSU_j computes $RID_i = PID^2_i \oplus h_1(R_i)$, where $R_i = x^{TA}_{pri}.PID^1_i$. The RSU_j checks whether $\sigma_{OBU_i} =? h_3(RID_i \| PID^1_i \| PID^2_i \| T_1)$. If not, then the RSU does not accept the message, otherwise RSU_j transmits the TA with the $(RID_i \| RID_{R_j} \| T_2)$ message.
- The validity of timestamp T_2 is checked first, after the TA receives the $(RID_i \| RID_{R_j} \| T_2)$ message. If T_2 is valid, then the TA checks whether $RID_i$and RID_{R_j} matches the stored value in the OBU registration list. If not, then the TA does not accept the message and sends a message to RSU with {reject}. Send a {accepted} message otherwise.
- Once the message {reject|| accepted} is received by the RSU_j, it verifies if the message content is {$accepted$}. If not, then the message is dropped by RSU_j and the vehicle illegal. Otherwise, it prepares the secret keys for this pseudo identity of the vehicle which use to renew the process of pseudo identities and secret keys with its expiration time T^{Sk}_i. The RSU_j chooses n randoms $r_l \in Z^*_q$, l = 1: n, and family of unlinkable pseudo identities are calculated $L_{PID_i} = \{PID_{il}, \ldots.., PID_{in}\}$ as follows:
  $PID_{in} = \{PID^1_{il}, PID^2_{il}\}$
  $PID^1_{il} = r_l P$
  $R^1_i = r_l P^{TA}_{Pub}$
  $PID^2_{il} = RID_i \oplus h_1(R^1_i)$
  where, l = 1, 2, . . . , n.
- The RSU_j calculates the corresponding secret keys for each pseudo identity $L_{SK_i} = \{SK_{il}, \ldots.., SK_{in}\}$ with its expiration times for each pseudo identity as follows:
  $SK_{il} = s^{dom_i}_{Pri}.h_2(PID^1_{il} \| PID^2_{il} \| T_{SK_i})$
- The RSU_j computes $E_{x^{TA}_{pri}}(L_{PID_i}, L_{SK_i}, T_{SK_i})$. Then, RSU_j sends $\{E_{x^{TA}_{pri}}(L_{PID_i}, L_{SK_i}, T_{SK_i}) \| T_3 \| \sigma_{RSU_j}\}$ to OBU_i, where $\sigma_{RSU_j} = h_3(L_{PID_i} \| L_{SK_i} \| T_{SK_i} \| T_3 \| RID_i)$.

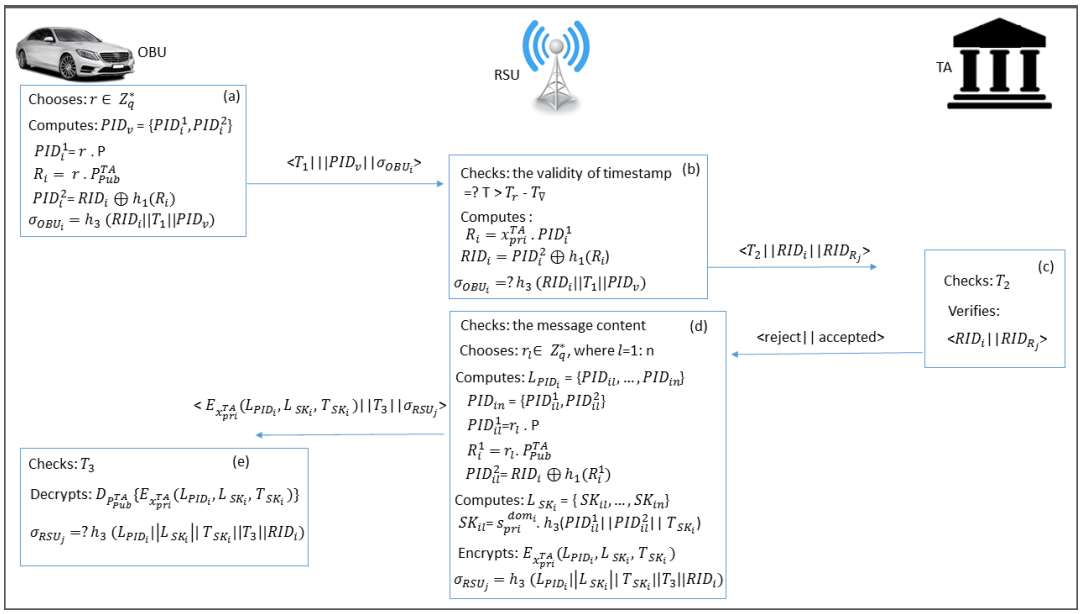

FIGURE 4. Description of the authentication process.

- The validity of timestamp T_3 is checked first, after the OBU_i receives the $\{E_{x_{pri}^{TA}}(L_{PID_i}, L_{SK_i}, T_{SK_i})\| T_3 \| \sigma_{RSU_j}\}$ message. If it is valid, then the OBU_i decrypts the message $D_{P_{Pub}^{TA}}(E_{x_{pri}^{TA}}(L_{PID_i}, L_{SK_i}, T_{SK_i})$ and checks $\sigma_{RSU_j} = ?h_3(L_{PID_i}\| L_{SK_i}\|T_{SK_i}\|T_3\|RID_i)$. If so, then it starts using L_{PID_i} and L_{SK_i} to sign messages anonymously in the RSU_j coverage area.

2) RENEW LISTS

The RSU preloads n of pseudo identities and the corresponding secret keys into each authentic vehicle's OBU during its joining phase for a valid short period. Whenever the available pseudo identities and the corresponding secret keys are close to expiry in the OBU traveling with VANETs, a modern n of pseudo identities and the corresponding secret keys are updated. Note that this is done between every vehicle and the TA when properly authenticated. If T_{SK_i} expires, the process of renew lists phase starts inside domain or outside domain for different times. We discuss these parts in the following

a: INSIDE Domain$_i$

If vehicle is still inside the domain, then the following is done:

- A new random integer $r^{new} \in Z_q^*$ is generated by OBU_i and computes $PID_{i:new}^1 = r^{new}P$ and $PID_{i:new}^2 = RID_i \oplus h_1(R^{new})$, where $R^{new} = r^{new}P_{Pub}^{TA}$. Then, the OBU_i transmits the RSU_j with $\{PID_v^{new}, PID_{in}, T_1, T_{SK_i}, \sigma_{OBU_i}^{new}\}$, where $PID_v^{new} = \{PID_{i:new}^1, PID_{i:new}^2\}$ and $\sigma_{OBU_i}^{new} = SK_i + r^{new}.h_2(PID_{i:new}^1\|PID_{i:new}^2\|T_1)$.
- The first test on the validity of the timestamp T_1 will take place after RSU_j receives the $\{PID_v^{new}, PID_{in}, T_1, T_{SK_i}, \sigma_{OBU_i}^{new}\}$ message. If valid, the time of expiration is verified for T_{SK_i}. If not valid, then the message is rejected by the RSU and the outside $Domain_i$ should be implemented. Otherwise, the following equation is used to check the validity of the vehicle:

$$\begin{aligned}\sigma_{OBU_i}^{new}.P &= \left(SK_i + r_{new}.h_2(PID_{i:new}^1\|PID_{i:new}^2\|T_1)\right).P \\ &= \left(s_{Pri}^{dom_i}.h_2(PID_i^1\|PID_i^2\|T_{Sk_i})\right. \\ &\quad \left. + r_{new}.h_2(PID_{i:new}^1\|PID_{i:new}^2\|T_1)\right).P \\ &= (h_2(PID_i^1\|PID_i^2\|T_{Sk_i})s_{Pri}^{dom_i}.P \\ &\quad + h_2(PID_{i:new}^1\|PID_{i:new}^2\|T_1))rnew.P \\ &= (h_2(PID_i^1\|PID_i^2\|T_{Sk_i})P_{Pub}^{dom_i} \\ &\quad + h_2(PID_{i:new}^1\|PID_{i:new}^2\|T_1))PID_{i:new}^1 \qquad (1)\end{aligned}$$

If Equation 1 is not held, then the message is rejected by RSU. It prepares the secret key for this new pseudo-identity of the vehicle and generates new $L_{PID_i^{new}}$ and $L_{SK_i^{new}}$ with new expired time. Then, the ''inside $domain_i$'' process is completed and OBU_i starts using new $L_{PID_i}^{new}$ and $L_{SK_i}^{new}$. An RSU may be used to perform the ''renew lists'' process. If a vehicle is leaving the RSU in the inside domain to renew its lists, then the new RSU must not be linked to the TA to ensure that the vehicle is authentic.

b: OUTSIDE Domain$_i$

The equation 1 is not held, when RSU in the other $domain$ receives $\{PID_v^{new}, PID_{in}, T_1, T_{Sk}, \sigma_{OBU_i}^{new}\}$ message because the public key different in that domain is being sent by RSU to authentically authenticate the vehicle with TA if it is legitimate to start generating a new list of pseudo identities and secret keys with new expired times.

3) SIGNING OF MESSAGE PHASE

Upon OBU joining the RSU, the message M_i is to be signed. The OBU_i must perform the following phases.

- OBU_i selects a pseudo identity PID_{in} from the L_{PID_i} list randomly and the corresponding secret keys SK_{il} from $L_{T_{SK_i}}$.
- OBU_i computes the signature of message as follows: $\sigma_m = h_3(M_i \| T \| PID_{in} \| SK_{il})$
- OBU_i broadcasts the traffic-related message $\{M_i, T, PID_{in}, SK_{il}, \sigma_m\}$ to the nearest RSU or another OBU.

4) VERIFICATION OF MESSAGE PHASE

The timestamp $[T_{exp}^{RSU_j}, T]$, are checked first after the traffic-related message has been received by the RSU or an OBU. If so, then it computes $\sigma_m^* = h_3(M_i \| T \| PID_{in} \| SK_{il})$. If $\sigma_m^* = \sigma_m$, the recipient accepts this messages; otherwise; it aborts.

5) REAL IDENTITY REVOCATION PHASE

In VANET communication, this step is very important because it not only allows the TA to trace a malicious authenticated vehicle and to disclose its identity but it also avoids further VANET involvement in this vehicle. The steps follow:

- If a complaint is issued about a misbehaving vehicle, then the RSU acquires the vehicle's real identity as follows:

$$RID_i = PID_{il}^2 \oplus h_1(x_{pri}^{TA}.PID_{il}^1) \tag{2}$$

- RID_i and RID_{r_j} are sent to the TA by the RSU.
- When TA receives the real identity of the malicious vehicle and transmitted RSU, the TA deletes RID_i from a list of registration and sends it to all RSU inside the domain with an {acknowledgment} message.
- All RSUs inside the domain prevent the vehicle from renewing lists after receiving the {acknowledgment} from the TA when $T_{SK_{il}}$ expires.
- When the malicious vehicle enters a new RSU in the outside domain, which revokes in renew the list, the TA cannot authenticate it with the joining process.

V. SECURITY ANALYSIS AND COMPARISON

This section aims to achieve the feature of non-forgery within a proposed identity-based scheme because of the difficulty in addressing the problem of the computerized Elliptic Curve Discrete Logarithm (ECDL). In addition, the security and privacy requirement of subsection III-C in the proposed scheme is provided. We compare our scheme and other related schemes according to the security requirements.

A. SECURITY ANALYSIS

The security model in our scheme is a game between the attacker and the challenger, which is based on the adversary's ability and a network model. The following can be described as the security model of the existential unforgeability against chosen-message attacks (EU-CMA):

Setup: Challenger C operates the key generation algorithm in this phase, which generates the system parameters and the secret system key. Challenger C then sends parameters of the system to the adversary A.

Query: Adversary A performs signature queries for the adversary's chosen messages. Challenger C performs the algorithm of the signature to calculate the signature in σ_m and sends it to adversary of A for a signature query within the message mi.

Forgery: Adversary A returns σ_m^- for a forged signature m^- for the game, and wins the game if

- σ_m^- is a valid message signature m^-.
- In the query phase, m^- signature was not queried.

The benefit of winning the game is the chance to return a valid forged signature. If a Polynomial adversary A is negligible, then our scheme is secure in VANET.

Theorem 1: The proposed scheme against an adaptive chosen message attack behind the random oracle model is existentially unforgeable.

Proof: Assume that A can fabricate a valid signature $\{M_i, T, PID_{in}, SK_{il}, \sigma_m\}$ for the message M_i. We can assume that an ECDLP instance (P, Q $= x_{Pri}^{TA}$.P) is given for two points P, Q on E/Ep, and $x_{Pri}^{TA} \in Z_q^*$. The challenger C can then address the ECDLP unquestionably with B as a subroutine.

Setup: A generates the system private key and establishes system parameters params $= \{p, q, \text{a}, \text{b}, \text{P}, P_{Pub}^{TA}, h_1, h_2, h_3\}$ and then builds and holds three lists, namely, $LIST_{h1}$ with $(\alpha, \tau h_1)$form, $LIST_{h2}$ with $(PID_{il}^1, PID_{il}^2, \tau h_2)$form and $LIST_{h3}$ with $(M_i, \text{T}, \tau h_3)$form. A is empty initially. Then, A transmits params to B.

$LIST_{h1}$**-Oracle:** After A receives a B message request with α, it initially verifies if tuple $(\alpha, \tau h_1)$ is in $LIST_{h1}$ or not. If so, then, A transmits $\tau h_1 = h(\alpha)$ to B. Otherwise, A randomly selects $\tau h_1 \in Z_q^*$ and appends $(\alpha, \tau h_1)$ into $LIST_{h1}$. Then, A transmits $\tau h_1 = h(\alpha)$ to B.

$LIST_{h2}$**-Oracle:** After A receives a B message request with $(PID_{il}^1, PID_{il}^2, T_{sk_{il}}))$, it initially verifies if tuple $(PID_{il}^1, PID_{il}^2, T_{sk_i}, \tau h_2))$ is in $LIST_{h2}$. If so, then A transmits $\tau h_2 = h(PID_{il}^1, PID_{il}^2, T_{sk_i})$ to B. Otherwise, A randomly chooses $\tau h_2 \in Z_q^*$ and appends $(PID_{il}^1, PID_{il}^2, T_{sk_i}, \tau h_2)$ into $LIST_{h2}$. Then, A transmits $\tau h_2 = h((PID_{il}^1 \| PID_{il}^2 \| T_{sk_i})$ to B.

$LIST_{h3}$**--Oracle:** After A receives a B message request with (M_i, T), it initially verifies if tuple $(Mi, T, \tau h_2)$ is in $LIST_{h3}$. If so, then A transmits $\tau h_3 = h(M_i \| T)$ to B. Otherwise, A randomly chooses $\tau h_3 \in Z_q^*$ and appends $(M_i, T, \tau h_2)$ into $LIST_{h3}$. Then, A transmits $\tau h_3 = h(M_i \| T)$to B.

Finally, adversary A outputs messages $\{M_i, T, PID_{in}, SK_{il}, \sigma_m\}$ and checks whether $R_i^1 = s_{Pri}^{TA} PID_{il}^1$ and $\sigma_m = h_3(M_i \| T \| PID_{in} \| SK_{il})$. Otherwise, challenger C will abort this game. According to the Cross-Lemma, another valid message $\{M_i^-, T^-, PID_{in}^-, SK_{il}^-, \sigma_m^-\}$ will be generated by adversary A and satisfies $R_i^{1-} = s_{Pri}^{TA} PID_{il}^{1-}$, $\sigma_m^- = h_3(M_i^- \| T^- \| PID_{in}^- \| SK_{il}^-)$ this process once again. Due to $R_i^{1-} - R_i^1 = s_{Pri}^{TA} PID_{il}^{1-} - s_{Pri}^{TA} PID_{il}^1$

It becomes computationally infeasible with the problem of ECDL for any Probabilistic Polynomial Time (PPT) algorithms to solve with non-negligible probability. Therefore, the proposed scheme is resistant against the chosen adaptive message attack under the random oracle model, which fulfill the security requirement in section III-C.

1) MESSAGE INTEGRITY AND AUTHENTICATION

We show in accordance with theorem 1 that an adversary cannot trump up a valid traffic-related message in our proposed solution, and recipients can verify that the message $\{M_i, T, PID_{in}, SK_{il}, \sigma_m\}$ has integrity and legality by verifying whether the $\sigma_m = h_3(M_i \| T \| PID_{in} \| SK_{il})$ holds. Therefore, the integrity and authenticity of the proposed VANET scheme are provided.

2) IDENTITY PRIVACY PRESERVATION

In the communication process, the vehicle's real identity of RID_i is involved in PID_{in} generated by OBU_i, where $P_{Pub}^{TA} = x_{Pri}^{TA}.\mathrm{P}$, $PID_{il}^1 = r_l P$, $R_i^1 = r_l P_{Pub}^{TA}$, $PID_{il}^2 = RID_i \oplus h_1(R_i^1)$, and $PID_{in} = \{PID_{il}^1, PID_{il}^2\}$. To retrieve RID_i from $PID_{il}^2 = RID_I \oplus h_1(R_i^1)$, the eavesdropper calculates $r_l P_{Pub}^{TA} = r_l x_{Pri}^{TA}.P$ from $P_{Pub}^{TA} = x_{Pri}^{TA}.\mathrm{P}$ and $PID_{il}^1 = r_l P$. Thus, no adversary can obtain the real identity RID_I of the vehicle through the PID_{il}^2. Therefore, the proposed scheme meets the identity privacy requirement. In other words, the proposed scheme satisfies the requirement for identity privacy preservation.

3) TRACEABILITY AND REVOCATION

The real identity of the vehicle RID_i is hidden in PID_{il}^2 created by the vehicle, where $P_{Pub}^{TA} = x_{Pri}^{TA}.\mathrm{P}$, $PID_{il}^1 = r_l P$, $R_i^1 = r_l P_{Pub}^{TA}$, $PID_{il}^2 = RID_i \oplus h_1(R_i^1)$ and $PID_{in} = \{PID_{il}^1, PID_{il}^2\}$. TA calculates $x_{Pri}^{TA}.\ PID_{il}^1 = x_{Pri}^{TA}.\ r_l.\mathrm{P} = r_l.\ x_{Pri}^{TA}.\mathrm{P} = r_l\ P_{Pub}^{TA}$ by using the system master key and retrieves the real identity by calculating $RID_i = PID_{il}^2 \oplus h_1(R_i^1)$. However, the proposed solution provides a traceability function.

4) UNLINKABILITY

During the message signing period, a pseudo-identity is used to create the signature. An anonymous description of the vehicle in the other message is rendered by the different random numerals r_l. The proposed scheme also used a current timestamp and expired time to calculate the signature. Any adversary who attempts to link two or more traffic-related messages may not succeed because of changes in their pseudo-identity, timestamp and expired time given that the content of the message varies each time. Consequently, neither message can be linked to a specific vehicle under the proposed scheme; however, no linkability issue arises.

5) NO LARGE CRL

In the proposed scheme for vehicles, every certification revocation list shares with all RSUs within the single domain. The RSUs do not need to manage any revoked certificate in any of the domains for VANETs, which reduces the number of misbehaving vehicles stored in the certificate revocation list.

6) RESISTANCE TO ATTACKS

We will now prove that our scheme is resistant to different attacks and show how secure our scheme is.

a: RESISTANCE REPLAY ATTACK

We use the current timestamp T in the message $\{M_i, T, PID_{in}, SK_{il}, \sigma_m\}$. In the verification process, an attacker can not modify or change T in a message. If T was invalid or had expired, then the message would be rejected. Thus, the replay attacks are resistant to our proposed identity-based scheme.

b: RESISTANCE IMPERSONATION ATTACK

The adversary must obtain a real identity of vehicles if they wish to transmit a valid traffic-related message by impersonating the legal vehicle. Moreover, according to previous knowledge, the adversary cannot find a vehicle with a real identity. The impersonation attack in the proposed solution is therefore ineffective. Thus, the impersonation attacks are resistant to our proposed identity-based scheme.

c: RESISTANCE MODIFICATION ATTACK

The signature σ_m is included in this scheme and guarantees the security of the message from the modifications. In the signature verification process, if an attacker changes or modifies the message, then it would be rejected. Thus, the modification attacks are resistant to our proposed identity-based scheme.

d: RESISTANCE MAN-IN-MIDDLE ATTACK

Mutual authentication between the sender and the verifier is carried out within our scheme. If the attacker tries a man-in-middle attack, then he/she must forge the sender and verifier messages to connect with it. However, an adversary cannot issue this kind of attack, according to Theorem 1. Thus, the man-in-middle attacks are resistant to our proposed identity-based scheme.

B. SECURITY COMPARISON

We perform a comparative analysis in terms of secure analysis between our system and other systems. Table 2 lists the result of the comparison where SR-1, SR-2, SR-3, SR-4, SR-5, SR-6, denotes message integrity and authentication, identity privacy protection, traceability and revocability, unlinkability, no large CRL and resistance to attacks respectively.

We know that the scheme proposed by [22], [23] for VANETs cannot fulfill all of the security requirements, as shown by Table 2. However, the proposed scheme could fulfill all of the security requirements.

VI. PERFORMANCE ANALYSIS

In this section, we will perform a comparative analysis between other schemes and our scheme in terms of the costs of computation and communication.

TABLE 2. Comparison of the secure requirement schemes.

	Alazzawi et al. scheme [22]	Bayat et al. scheme [23]	Proposed
SR-1	✓	✓	✓
SR-2	✓	✓	✓
SR-3	✓	✓	✓
SR-4	✗	✗	✓
SR-5	✗	✗	✓
SR-6	✓	✗	✓

✓: The secure requirement is satisfied
✗: The secure requirement is not satisfied

A. COMPUTATION COST ANALYSIS

By comparing our scheme with those of Zhang *et al.* [26], Bayat *et al.* [23], Alazzawi *et al.* [22], He *et al.* [19], we demonstrate its performance in terms of the cost of computations. The cryptography operations in [23], [26] are established on bilinear pairings, while those of [19], [22] and the proposed scheme are established on ECC.

This paper uses MIRACL's [27] cryptographic library to calculate the time required for various cryptographic operations. A 4 GB memory processor running the operating system Windows 7 The hardware platform is an Intel(R) Core(TM)2 Quad 2.66 GHz. Table 4 shows the definition of and execution times for associated cryptographic operations.

Let *GMS*, *VSM*, and *VMM* denote for simplicity the generation of message and signature, the verification of the single message, and verification of multiple messages, respectively.

In the scheme in [26], *MGS* comprises two map to point hash functions and three secure hash functions. Thus, the total computation time of *MGS* is 2 T_{mtp}+3 $T_h \approx 8.3478$ ms. This scheme has two map to point hash functions, two bilinear pairing operations and three secure hash functions, which gives the *SVM* an overall computation time of 2 T_{mtp}+2 T_{bp}+ 3 $T_h \approx 19.9698$ ms. *BVMM* in this scheme requires two bilinear pairing operations, $3n$ secure hash functions, and $2n$ map to point hash functions. The overall computation time for *BVMM* is $2\,T_{bp} + 3nT_h + 2nT_{mtp} \approx 8.3478$n+11.622 ms. The computation cost of other scheme are executed in the same method. In our scheme, *GMS* consists of five secure hash functions. so $1T_h = 0.001$ ms is the total computation time for *GMS*. *VSM* consists of a secure hash function. So 1 $T_h \approx 0.001$ ms is the total computation time for *VSM*. *VMM* (n) secure hash functions. so $(n)T_h =$ n0.001 ms is the total computation time for *VMM*.

Table 3 compares the cost of computation in the proposed scheme with the three other ID-based schemes for *MGS*, *SVM*, and *BVMM*. Figure 5 shows that our scheme has a significant advantage over *MGS* and *SVM* three scheme. Figure 6 and 7 indicate the costs of *BVMM* in measuring various traffic-related messages. Consequently, the proposed scheme is more productive and efficient than the schemes in [22], [23], [26] and [19] in terms of computation costs for *MGS*, *SVM*, and *BVMM*.

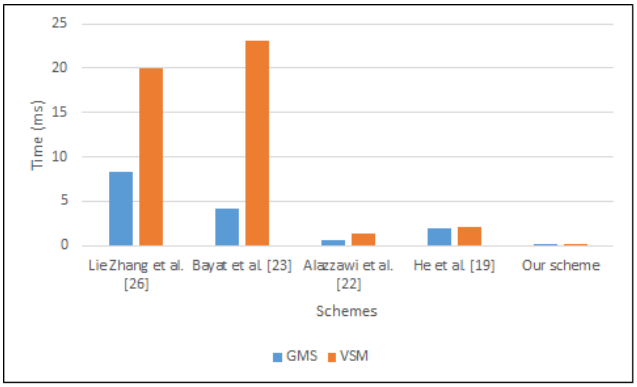

FIGURE 5. Computation costs of *GMS* and *VSM*.

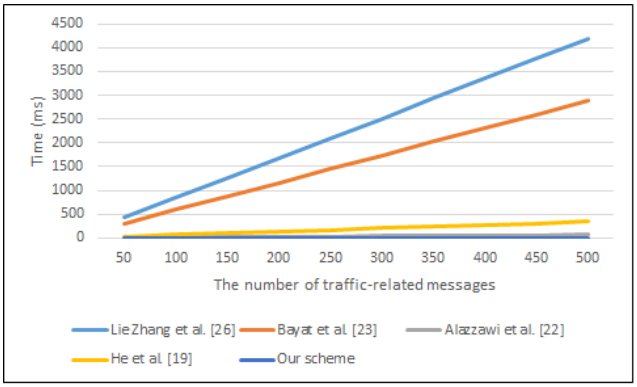

FIGURE 6. Computation costs of *BVMM* for different traffic-related messages.

B. COMMUNICATION COST ANALYSIS

The size of p^- is 64 bytes, so $G1$ is 128 bytes in size of each item, And the p size is 20 bytes, meaning that in G, every single item size is 40 bytes. We also assume that timestamp output sizes, secure hath function, and integer

TABLE 3. Cost of computation comparison.

Schemes	GMS(ms)	VSM(ms)	VMM(ms)
Lie Zhang et al. [26]	$2T_{mtp} + 3T_h \approx 8.3478$	$2T_{mtp} + 2T_{bp} + 3T_h \approx 19.9698$	$2T_{bp} + 3nT_h + 2nT_{mtp} \approx 8.3478$n+11.622
Bayat et al. [23]	$1T_{mtp} \approx 4.1724$	$3T_{bp} + 1T_{bp}^{sm} + 1T_{mtp} \approx 23.1708$	$3T_{bp} + nT_{bp}^{sm} + nT_{mtp} \approx 5.7378$n+17.4333
Alazzawi et al. [22]	$1T_{ecc}^{sm} + 2T_h \approx 0.6738$	$(2)T_{ecc}^{sm}+(1)T_h+(1)T_{ecc}^{pa} \approx 1.3477$	$(2)T_{ecc}^{sm} + (2n)T_{ecc}^{sm-s} + (n+1)T_{ecc}^{pa} + (n)T_h$ ≈ 0.1371n + 1.3467
He et al. [19]	$3T_{ecc}^{sm} + 3T_h \approx 2.0174$	$(3)T_{ecc}^{sm}+(2)T_h+(2)T_{ecc}^{pa} \approx 2.0236$	$(2)T_{ecc}^{sm} + (2n)T_{ecc}^{sm-s} + (n+1)T_{ecc}^{pa} + (n)T_h$ ≈ 0.6800n + 1.3405
Our scheme	$1T_h = 0.001$	$1\,T_h \approx 0.001$	$(n)T_h =$ n 0.001

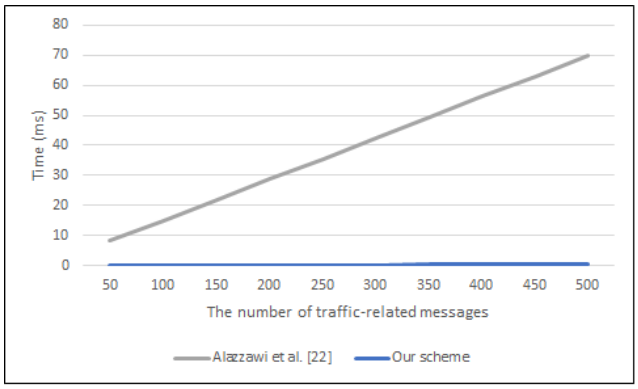

FIGURE 7. Computation costs of *BVMM* for different traffic-related messages.

TABLE 4. Definitions and time of cryptographic operation.

Abbr.	Execution time(ms)	Definition
T_{bp}	5.811	Bilinear pairing operation
T_{bp}^{sm}	1.5654	Scalar multiplication operation in a group based on bilinear pairing
T_{bp}^{sm-s}	0.1829	Small scalar point multiplication operation in a group based on bilinear pairing
T_{bp}^{pa}	0.0106	Point addition operation in a group based on bilinear pairing
T_{mtp}	4.1724	Map-to-point hash function
T_{ecc}^{sm}	0.6718	Scalar multiplication operation in a group based on ECC
T_{ecc}^{sm-s}	0.0665	Small scalar point multiplication operation in a group based on ECC
T_{ecc}^{pa}	0.0031	Point addition operation in a group based on ECC
T_h	0.001	General hash function operation

TABLE 5. Comparison of communication cost.

Schemes	One message(byte)	n messages(byte)
Lie Zhang et al. [26]	148	148 n
Bayat et al. [23]	120	120 n
Alazzawi et al. [22]	148	148 n
He et al. [19]	144	144 n
Our Scheme	104	104 n

item Z_q^* are, respectively, 4, 20, and 20 bytes, where the message content is excluded. The traffic-related message size in the scheme of [19] is $(40 * 3 + 20 + 4) = 144$ bytes, and the content of traffic-related message is three elements in G $\{PID_{il}^1, PID_{il}^2, R_i \in G\}$, one element $\sigma_m \in Z_q$, and one timestamp. The communication cost of other scheme are executed in the same method. In our proposed scheme, the vehicle sends a traffic-related message with size $(40 + 20 * 3 + 4) = 104$ bytes and the traffic-related message content is one element in $\{PID_{il}^1 \in G\}$, three elements in $\{PID_{il}^2, SK_{il}, \sigma_m \in z_q\}$, and one timestamp. The overall overhead communication is given in Table 5.

VII. CONCLUSION

In this paper, we propose an efficient conditional privacy preservation with mutual authentication scheme based domain, supporting V2V and V2I communication within VANET. Our proposal depends on the division geographical areas into several domains, in which each domain stores the CRL all RSUs located inside the domain. We perform a process of mutual authentication between TA and vehicles to ensure that the fabricated messages will not be sent out by the attacker with impersonating real vehicles. The phase of security analysis, security and privacy requirements for VANETs could be satisfied in our scheme. In terms of computation and communication costs, Our scheme outperforms others with low computation and communication costs. Finally, the proposed scheme is more suitable for large scale networks.

ACKNOWLEDGEMENT

This work was supported in part by the National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia and External Grant from UMobile Sdn Bhd under Grant 304/PNAV/650958/U154.

REFERENCES

[1] D. Lloyd, "Reported road casualties in Great Britain: Main results 2015," Dept. Transp. London, U.K., Tech. Rep., Sep. 2016.
[2] M. Al Shareeda, A. Khalil, and W. Fahs, "Realistic heterogeneous genetic-based RSU placement solution for V2I networks," *Int. Arab J. Inf. Technol.*, vol. 16, no. 3, pp. 540–547, 2019.
[3] J. B. Kenney, "Dedicated short-range communications (DSRC) standards in the United States," *Proc. IEEE*, vol. 99, no. 7, pp. 1162–1182, Jul. 2011.
[4] M. Al Shareeda, A. Khalil, and W. Fahs, "Towards the optimization of road side unit placement using genetic algorithm," in *Proc. Int. Arab Conf. Inf. Technol. (ACIT)*, Nov. 2018, pp. 1–5.
[5] I. Ali, A. Hassan, and F. Li, "Authentication and privacy schemes for vehicular ad hoc networks (VANETs): A survey," *Veh. Commun.*, vol. 16, pp. 45–61, Apr. 2019.
[6] Sheikh, Liang, and Wang, "A survey of security services, attacks, and applications for vehicular ad hoc networks (VANETs)," *Sensors*, vol. 19, no. 16, p. 3589, Aug. 2019.
[7] C. Gamage, B. Gras, B. Crispo, and A. S. Tanenbaum, "An identity-based ring signature scheme with enhanced privacy," in *Proc. Securecomm Workshops*, Aug. 2006, pp. 1–5.
[8] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *J. Comput. Secur.*, vol. 15, no. 1, pp. 39–68, 2007.
[9] A. Studer, E. Shi, F. Bai, and A. Perrig, "TACKing together efficient authentication, revocation, and privacy in VANETs," in *Proc. 6th Annu. IEEE Commun. Soc. Conf. Sensor, Mesh Ad Hoc Commun. Netw.*, Jun. 2009, pp. 1–9.
[10] X. Lin, R. Lu, C. Zhang, H. Zhu, P.-H. Ho, and X. Shen, "Security in vehicular ad hoc networks," *IEEE Commun. Mag.*, vol. 46, no. 4, pp. 88–95, Apr. 2008.
[11] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: A secure and privacy-preserving protocol for vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 56, no. 6, pp. 3442–3456, Nov. 2007.
[12] J. Shao, X. Lin, R. Lu, and C. Zuo, "A threshold anonymous authentication protocol for VANETs," *IEEE Trans. Veh. Technol.*, vol. 65, no. 3, pp. 1711–1720, Mar. 2016.
[13] Y. Wang, H. Zhong, Y. Xu, and J. Cui, "ECPB: Efficient conditional privacy-preserving authentication scheme supporting batch verification for VANETs," *IJ Netw. Secur.*, vol. 18, no. 2, pp. 374–382, 2016.
[14] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proc. Workshop Theory Appl. Cryptograph. Techn.* Cham, Switzerland: Springer, 1984, pp. 47–53.
[15] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in *Proc. 27th Conf. Comput. Commun. (INFOCOM)*, Apr. 2008, pp. 246–250.
[16] C.-C. Lee and Y.-M. Lai, "Toward a secure batch verification with group testing for VANET," *Wireless Netw.*, vol. 19, no. 6, pp. 1441–1449, Aug. 2013.
[17] Z. Jianhong, X. Min, and L. Liying, "On the security of a secure batch verification with group testing for VANET," *Int. J. Netw. Secur.*, vol. 16, no. 5, pp. 351–358, 2014.
[18] M. Bayat, M. Barmshoory, M. Rahimi, and M. R. Aref, "A secure authentication scheme for VANETs with batch verification," *Wireless Netw.*, vol. 21, no. 5, pp. 1733–1743, Jul. 2015.

[19] D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 12, pp. 2681–2691, Dec. 2015.
[20] J. Cui, J. Zhang, H. Zhong, and Y. Xu, "SPACF: A secure privacy-preserving authentication scheme for VANET with cuckoo filter," *IEEE Trans. Veh. Technol.*, vol. 66, no. 11, pp. 10283–10295, Nov. 2017.
[21] J. Zhang, J. Cui, H. Zhong, Z. Chen, and L. Liu, "PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks," *IEEE Trans. Dependable Secure Comput.*, early access, Mar. 11, 2019, doi: 10.1109/TDSC.2019.2904274.
[22] M. A. Alazzawi, H. Lu, A. A. Yassin, and K. Chen, "Efficient conditional anonymity with message integrity and authentication in a vehicular ad-hoc network," *IEEE Access*, vol. 7, pp. 71424–71435, 2019.
[23] M. Bayat, M. Pournaghi, M. Rahimi, and M. Barmshoory, "NERA: A new and efficient RSU based authentication scheme for VANETs," *Wireless Netw.*, vol. 5, pp. 1–16, Jun. 2019.
[24] J. Cui, L. Wei, H. Zhong, J. Zhang, Y. Xu, and L. Liu, "Edge computing in VANETs—An efficient and privacy-preserving cooperative downloading scheme," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 6, pp. 1191–1204, Jun. 2020.
[25] S. Biswas and M. M. Haque, and J. V. Misic, "Privacy and anonymity in VANETs: A contemporary study," *Ad Hoc Sensor Wireless Netw.*, vol. 10, nos. 2–3, pp. 177–192, 2010.
[26] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, and C. Hu, "Distributed aggregate privacy-preserving authentication in VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 3, pp. 516–526, Mar. 2017.
[27] (2018). *Multi Precision Integer and Rational Arithmetic Cryptographic Library (MIRACL)*. [Online]. Available: http://www.certivox.com/miracl/

MAHMOOD A. AL-SHAREEDA received the B.Sc. degree in communication engineering from the Iraq University College, and the M.Sc. degree in information technology from the Islamic University of Lebanon (IUL), in 2018. He is currently the Ph.D. Fellow with the School of National Advance IPv6 Centre (NAv6), Universiti Sains Malaysia (USM). His research interest includes security and privacy issues in vehicle ad hoc networks (VANETs).

MOHAMMED ANBAR (Member, IEEE) received the Ph.D. degree in advanced computer network from University Sains Malaysia (USM). He is currently a Senior Lecturer with the National Advanced IPv6 Centre (NAv6), USM. His current research interests include malware detection, Web security, intrusion detection systems (IDSs), intrusion prevention systems (IPSs), network monitoring, the Internet of Things (IoT), vehicular ad hoc network (VANET) security, and IPv6 security.

IZNAN HUSAINY HASBULLAH received the Bachelor of Science degree in electrical engineering from the Rensselaer Polytechnic Institute, Troy, NY, USA. He is currently pursuing the M.Sc. degree in advanced network security. He has experience working as a Software Developer, a Research and Development Consultant, and a Network Security Auditor prior to joining the National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia, in 2010, as a Research Officer. His research interests include unified communication, telematics, network security, network protocols, and next generation networks.

SELVAKUMAR MANICKAM is currently an Associate Professor working in Cybersecurity, the Internet of Things, Industry 4.0, and Machine Learning. He has authored and coauthored more than 160 articles in journals, conference proceedings, book reviews, and graduated 13 PhDs. He has ten years of industrial experience prior to joining the academia. He is a member of technical forums at national and international levels. He also has experience building IoT, embedded, server, and mobile and Web-based applications.

SABRI M. HANSHI received the B.Sc. degree in electronics and communications engineering from the Hadhramout University for Science and Technology, Yemen, in 2003, the M.Sc. degree in computer and information engineering from International Islamic University Malaysia, in 2010, and the Ph.D. degree from the National Advanced IPv6 Centre, Universiti Sains Malaysia. He was a Postdoctoral Fellow with the National Advanced IPv6 Centre, from 2017 to 2019. He is currently a Vice Dean for Academic Affairs with the Seiyun Community College, Yemen. His research interests include vehicular ad hoc networks, routing protocols over ad hoc networks, modeling and performance of wireless channels, and the Internet of Things.