IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 3, 2019, accepted May 22, 2019, date of publication May 30, 2019, date of current version June 12, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2919973

Efficient Conditional Anonymity With Message Integrity and Authentication in a Vehicular Ad-Hoc Network

MURTADHA A. ALAZZAWI[1,2], HONGWEI LU[1], ALI A. YASSIN[3], AND KAI CHEN[1]

[1]School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074, China
[2]Department of Computer Techniques Engineering, Imam Al-Kadhum College (IKC), Baghdad 10001, Iraq
[3]Computer Science Department, Education College for Pure Science, University of Basrah, Basrah 61004, Iraq

Corresponding authors: Murtadha A. Alazzawi (murtadhaali@alkadhum-col.edu.iq) and Kai Chen (kchen@hust.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61572222, Grant 61272405, and Grant 61272033, and in part by the Provincial Teaching Research Projects of Higher Institutions in Hubei Province.

ABSTRACT Vehicles in a vehicular ad-hoc network (VANET) broadcast beacons giving safety-related and traffic information. In an open-access environment, this means that the VANET is susceptible to security and privacy issues. In this paper, we propose a new pseudo-identity-based scheme for conditional anonymity with integrity and authentication in a VANET. The proposed scheme uses a pseudonym in the joining process with the road-side unit (RSU) to protect the real identity even from the RSU, in case it is compromised. All previous identity-based schemes have been prone to insider attackers, and have not met the revocation process. Our scheme resolves these drawbacks as the vehicle signs the beacon with a signature obtained from the RSU. Our scheme satisfies the requirements for security and privacy, and especially the requirements for message integrity and authentication, privacy preservation, non-repudiation, traceability, and revocation. In addition, it provides conditional anonymity to guarantee the protection of an honest vehicle's real identity, unless malicious activities are detected. It is also resistant to common attacks such as modification, replay, impersonation, and man-in-the-middle (MITM) attacks. Although the numerous existing schemes have used a bilinear pairing operation, our scheme does not depend on this due to the complex operations involved, which cause significant computation overhead. Furthermore, it does not have a certification revocation list, giving rise to significant costs due to storage and inefficient communication. Our analysis demonstrates that our scheme can satisfy the security and privacy requirements of a VANET more effectively than previous schemes. We also compare our scheme with the recently proposed schemes in terms of communication and computation and demonstrate its cost-efficiency and appropriateness in working with the VANET. Meanwhile, the computation costs of the beacon signing and verification in our scheme are reduced by 49.9% and 33.3%, respectively.

INDEX TERMS VANET, elliptic curve, anonymity, authentication, revocation, pseudonym.

I. INTRODUCTION

The principal aim of a VANET is to improve the safety of transportation. A UK Government Road Casualties Report of 2015 reveals that 1,732 persons have died and 22,137 were injured in road accidents [1]. Hence, VANET technology can help to decrease the number of accidents on the road. VANETs use IEEE 802.11p technology, via a protocol called Dedicated Short-Range Communication (DSRC) [2]. A VANET environment is mainly composed of three components [3]: a trusted authority (TA), a road-side unit (RSU), and an on-board unit (OBU). The TA is responsible for initialising and providing system parameters, including public and private key pairs, to RSUs and vehicles. The RSU is located along the road as a router between vehicles and is considered to be part of the network infrastructure, while the OBU is a radio device installed in a vehicle and used to broadcast and receive beacons to other OBUs or RSU [4]. Using the DSRC protocol, vehicles can communicate with each other via vehicle-to-vehicle (V2V) communication and with the RSU by vehicle-to-infrastructure (V2I) communication [5].

Each OBU-equipped vehicle broadcasts safety- and traffic-related messages called beacons, containing

The associate editor coordinating the review of this manuscript and approving it for publication was Md. Abdur Razzaque.

its location, velocity, heading and traffic events, more than three times per second over a limited range of a few hundred meters [6]. Hence, each node (legal or illegal) located within this range receives these beacons, due to the nature of broadcasting in an open access environment. The security and privacy requirements in a VANET are therefore challenges that should be resolved before releasing it, both in order to avoid illegal and forged messages and to protect the privacy of drivers in terms of their identity and location. Illegal or forged messages may damage the VANET, and lead to road incidents and traffic jams.

Numerous academic studies have been conducted of the security and privacy requirements in VANETs. Although previous works have been able to meet most of these requirements for VANETs, they are not fully safe, and most also suffer from low performance in terms of computation and communication overhead and high storage. We therefore propose a robust scheme for conditional anonymity with integrity and authentication in VANET. The main contributions of our paper can be summarised as follows:

- We propose a new robust pseudo-identity-based scheme using a pseudonym rather than a real identity. The new scheme meets the security and privacy requirements of a VANET and is resistant to common attacks.
- The vehicle signs its beacons using a signature obtained from the RSU in order to meet the revocation requirement and to protect the vehicle's real identity from an insider attacker.
- The scheme supports a batch verification process to improve computational efficiency.
- The RSU only knows the vehicle's pseudonym, and is not able to acquire the vehicle's real identity.
- Our scheme provides conditional anonymity that guarantees protection of an honest vehicle's real identity, unless malicious activities are detected.

The rest of the paper is structured as follows: Section II describes some previous related works. Section III gives the preliminaries of the proposed scheme, and this is followed by a detailed description of our proposed scheme in Section IV. Sections V and VI present a security analysis and a performance analysis, respectively. Our paper is concluded in Section VII.

II. RELATED WORKS

In recent years, many researchers have focused on the security and privacy issues of VANETs. We can class these works into two categories: public key infrastructure (PKI)-based and identity (ID)-based schemes.

In a PKI-based approach, the vehicle's real identity is hidden using anonymous certificates, and each vehicle obtains many certificates with their key pairs during the registration process. In 2004, Hubaux et al. [7] claimed that PKI technology could be suitable for handling security and privacy issues in VANETs. In 2007, Raya and Hubaux [8] used PKI and anonymous certificates to propose an anonymous authentication scheme that aimed to resolve the security and privacy issues in VANETs. The methodology of this scheme [8] requires preloading the vehicle with numerous certificates and the corresponding anonymous public/private key pairs. In this case, OBUs suffer from a massive verification overhead and large storage requirements. Moreover, the TA generates a large certification revocation list (CRL), making the revocation processing ineffective. In 2008, Lu et al. [9] proposed a protocol for security in VANETs called ECPP to solve the increase in the CRL and the storage space limitations. In ECPP, the vehicle depends on the RSU to obtain a short-term pseudonym. In 2008, Zhang et al. [10] suggested a scheme known as efficient RSU-aided message authentication (RAISE), based on a k-anonymity approach and a hash message authentication code. In RAISE, messages are verified by the RSU to give low communication costs and to preserve the privacy of the vehicles. In 2016, Rajput et al. [11] suggested a protocol known as hierarchical privacy-preserving pseudonymous authentication to resolve these PKI-based drawbacks. This protocol does not require the management of a CRL, and the vehicle obtains only two pseudonyms with the corresponding key pairs. However, PKI-based schemes in VANETs encounter problems with the storage of certificates and key management.

To resolve the problems arising in PKI-based schemes, many researchers have proposed ID-based schemes for VANETs. The first work that used an ID-based signature was put forward in 1984 by Shamir [12]. In this scheme, the identity information is used as the node's public key, while private keys are generated by a TA using the same identity information and then distributed to nodes. The recipients verify the message using the sender's public key, and the message is signed using the sender's private key. Zhang et al. [13], [14] used the vehicle user's identity in an ID-based scheme in which a vehicle does not need to save a large number of public and private keys and their certificates. This scheme therefore mitigates the amount of storage needed as well as the communication and computation costs. Additionally, it avoids the need for certificate management and a CRL. The schemes proposed by Zhang et al. [13], [14] support batch verification based on bilinear pairing for the messages received by a vehicle and an RSU, and thus achieve low verification costs, allowing several messages to be verified concurrently. In 2009, Jiang et al. [15] used an ID-based scheme to propose the binary authentication tree (BAT) for V2I communication. BAT achieves high efficiency and meets the security and privacy requirements in VANETs. In 2011, Huang et al. [16] proposed a new authentication scheme termed PACP, which depends on using pseudonyms rather than real identities, providing conditional privacy and efficiency in performance. Chim et al. [17] and Lee and Lai [18] pointed out, in 2011 and 2013 respectively, that the schemes proposed in [13], [14] have flaws that mean that an OBU can use a fake identity to eliminate the traceability requirement. In addition, these schemes cannot resist replay and impersonation attacks.

In 2013, Lee and Lai [18] suggested an improved ID-based scheme to enhance security in VANETs and to achieve much higher effectiveness. In 2013, Horng et al. [19] demonstrated that the scheme in [17] was susceptible to impersonation attacks, and that a malicious vehicle was able to force another vehicle to broadcast bogus messages to other vehicles. Horng et al. [19] then proposed a scheme named SPECS to improve the flaws of the scheme [17]. In 2014, Jianhong et al. [20] highlighted several security drawbacks in the scheme proposed by Lee and Lai [18], for example that it cannot meet the traceability and non-repudiation requirements and cannot resist replay attacks. To resolve the flaws in Lee and Lai's [18] scheme, an improved ID-based scheme was suggested by Jianhong et al. [20]. Recently, several researchers [21]–[28] have proposed ID-based authentication schemes that use elliptic curve cryptography (ECC) instead of bilinear pairing operations. These achieve high productivity in terms of computation and communication overhead.

Although existing ID-based authentication schemes have simplified key management, reduced the number of certificates and the storage overhead, and mitigated the computation and communication costs, they still suffer from certain challenges. We can categorise the previous ID-based schemes into three groups, each of which faces its own challenges that make it unsuitable for use in a VANET. Bilinear pairing operations are used in the first group [13]–[20]; these schemes suffer from high computation and communication cost, and the same issues as those found in the second group [21]–[26]. In the second group, when a vehicle is broadcasting bogus information, a TA can track this vehicle but cannot stop it from continuing to send these messages. In addition, an insider attacker can easily reveal the real identity of any vehicle, since this attacker has the TA's private and public key pairs. Consequently, these schemes do not meet the requirements for revocation and privacy preservation. The schemes in the third group [27], [28] depend on RSUs to verify beacons, and then publish lists of legal and illegal vehicles with the notification messages. The OBU will therefore wait for a notification message before verifying the legitimacy of the sender, and this process may be time-consuming. Moreover, in the case where there are two nearby vehicles that are connected to different RSUs, in [27], [28], each RSU is responsible for verifying beacons and dealing only with the vehicles that are within its range and registered with it. Thus, these two vehicles cannot trust each other.

In this paper, we propose a new pseudo-ID-based scheme to address the aforementioned issues. Our scheme uses ECC instead of the bilinear pairing operations to resolve the communication and computation cost issue in [13]–[20]. Additionally, the vehicle signs the beacon by using a signature issued by the RSU, and this feature helps to overcome the flaws in [21]–[26]. Unlike the schemes in [27], [28], our scheme depends on each vehicle verifying the received beacons as well as providing mutual authentication between two vehicles within the ranges of different RSUs.

III. PRELIMINARIES

This section first demonstrates the system model; this is followed by a description of the security and privacy requirements of a VANET and lastly, the mathematical tools used in this work are explained.

A. THE SYSTEM MODEL

Our proposed scheme comprises three components, as shown in Fig. 1:

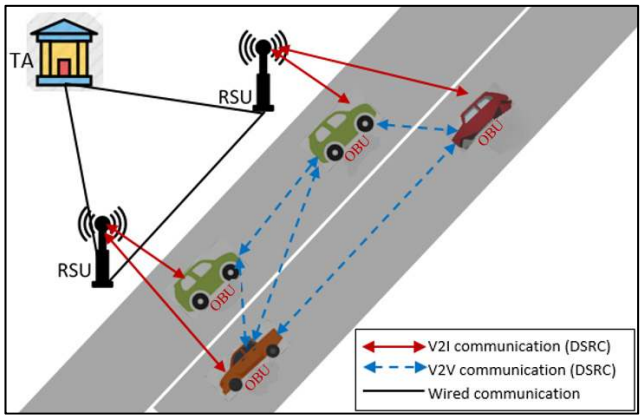

FIGURE 1. The system model.

1) A TA is a fully trusted party in a VANET and is accountable for initialising and providing the system parameters, including public and private key pairs, to RSUs and vehicles (we assume that a TA has complete knowledge of the location of all RSUs and connects with them via secure wire network).
2) RSUs are located along the road as routers between vehicles, and are considered part of the network infrastructure. An RSU manages the communication of all OBUs within its area and publishes traffic-related messages. It also connects to other RSUs to exchange traffic messages via secure wire network. Each RSU also has a unique real identity, RID_R.
3) An OBU is a radio device installed in a vehicle that operates on the DSRC protocol to broadcast and receive beacons from other OBUs or RSUs. Each OBU has a tamper-proof device (TPD) that is accountable for storing secret parameters and implementing cryptographic operations.

B. SECURITY AND PRIVACY REQUIREMENTS

1) MESSAGE INTEGRITY AND AUTHENTICATION

In a VANET, a recipient (vehicle or RSU) should have the ability to verify the receiving beacon and to ensure that the sender is legal. Moreover, the content of the beacon should be verified to ensure that it has been transported without being corrupted.

2) PRIVACY PRESERVATION

In a VANET, the scheme must meet the requirement of privacy preservation, which means that private information

about vehicles such as their location and identity should be secure, and should not be revealed by the broadcast beacons.

3) TRACEABILITY AND REVOCATION

These are important requirements in a VANET, as they offer conditional anonymity. This means that a TA should have the ability to trace a malicious vehicle, to reveal its real identity and to prevent it from continuing to take part in VANET.

4) NON-REPUDIATION

This means that the senders of beacons should not be able to deny that they have sent beacons.

5) CONDITIONAL ANONYMITY

In a VANET, the scheme should offer conditional anonymity. This means guaranteeing the anonymity of an honest vehicle's real identity, unless malicious activities are detected.

6) RESISTANCE TO ATTACKS

In a VANET, an effective scheme should resist general attacks such as impersonation, replay, modification and MITM attacks.

C. MATHEMATICAL TOOLS

In 1985, Miller [29] proposed ECC, which has since become a widely used tool in the design of security algorithms and digital signatures. We assume that F_p represents a finite field where p is a large prime number, E denotes an elliptic curve over F_p that is based on the equation $y^2 = x^3 + ax + b \; mod \; p$, where $\left(4a^3 + 27b^2\right) mod \; p \neq 0$ and $x, y, a, b \in F_p$. Let O be an infinite point, and G an additive group with order q and generator P. An additive group G includes all points on the elliptic curve E. Let P and Q be two points on the elliptic curve E; the operation of point addition in G is then defined as $P + Q = R$. Scalar point multiplication in G is defined as $s.P = P + P + \ldots\ldots + P(s \; times)$.

The elliptic curve discrete logarithm problem (ECDLP) [30] is computationally infeasible. Based on E, and given two points P and Q from G, the main task of ECDLP is to find an integer s that satisfies $Q = sP$.

IV. PROPOSED SCHEME

Our proposed scheme has six phases: in the first and second phases, the system parameters are initialised and broadcast by the TA and the vehicle is registered. In the subsequent three phases, the vehicle will create a mutual authentication with the nearest RSU to start broadcasting and verifying operations, and at the same time will renew the signature if it expires, using any RSU for which the vehicle is in range. Fig. 2 illustrates an example to explain how the vehicle works during these three phases. In this example, the vehicle undergoes a five-stage process. In stage (A), the vehicle sends a 'joining request' message to the nearest RSU. In this state, the RSU needs to open a session with the TA to ensure the vehicle's legitimacy. In stage (B), when the vehicle has obtained agreement and a signature from the RSU, it starts

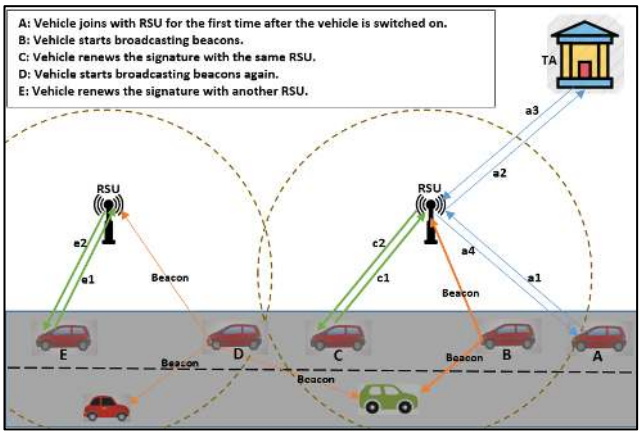

FIGURE 2. An example explains the mutual authentication between the vehicle and RSUs.

broadcasting and verifying operations. When the signature expires, stage (C) renews it by sending a 'renew signature' message to the RSU. Then, in stage (D), the vehicle restarts broadcasting and verifying operations and will continue even within the range of another RSU. In stage (E), the vehicle can renew the signature, even using other RSUs, simply by sending a 'renew signature' message. Thus, the vehicle can start the broadcasting operation with a signature that can be relied on by others. Each signature has a set time period of validity, and once this expires, the vehicle needs to renew the signature. If a trusted vehicle begins broadcasting fake or bogus information in a VANET, the sixth phase of our proposed scheme allows us to trace this vehicle and revoke its permissions. Fig. 3 illustrates the operation of the proposed

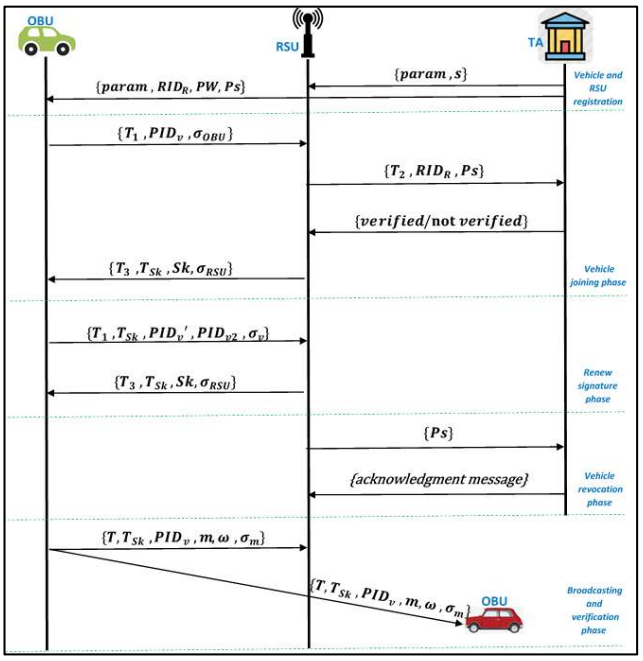

FIGURE 3. The operation of the proposed scheme.

scheme, while Table 1 gives the main notations used and their descriptions.

TABLE 1. Notations and their descriptions.

Notation	Descriptions
E	An elliptic curve
G	An additive group based on E
P	A generator of G
p, q	Large prime numbers
s, Pub	Private and public key pairs
h_1, h_2, h_3	Three secure hash functions
RID_R, RID_v	Real identities of the RSU and vehicle
PID_{v1}, PID_{v2}	Pseudonyms of the vehicle for broadcasting
Ps	Pseudonym of the vehicle to hide its real identity
r	Random integer
PW	Password
$\|$	Concatenation operator
$\oplus$	Exclusive OR (XOR) operation
Sk	The signature of the beacon issued from the RSU
m	Traffic-related message
T_{Sk}	The timestamp of the signature
$T, T_r, \Delta T$	Timestamp, receiving time and time delay values

A. INITIALISATION PHASE

In this phase, the TA generates the initial system parameters using the following steps, and updates the system parameters to maintain the security of the system.

1) The TA selects two large prime numbers p, q and an additive group G with order q and generator P. An additive group G includes all points on the elliptic curve E that are defined by the equation $y^2 = x^3 + ax + b \ mod \ p$, where, $a, b \in F_p$.
2) The TA generates a random number $s \in Z_q^*$ as the private key, and computes the public key $Pub = s.P$.
3) The TA selects three secure hash functions $h_1 : G \rightarrow Z_q^*$, $h_2 : \{0,1\}^* \times \{0,1\}^* \times G \rightarrow Z_q^*$, $h_3 : \{0,1\}^* \rightarrow Z_q^*$ as a cryptographic hash function.
4) The TA preloads the private key s for each legal RSU.
5) The TA broadcasts the system parameters $param = \{q, Pub, P, h_1, h_2, h_3\}$.

B. VEHICLE REGISTRATION PHASE

This phase happens when a new vehicle's user is willing to join the VANET, therefore, he/she should register for the TA. The procedure of this phase starts by submitting a real identityRID_v and a password PW from the user to the TA via a secure channel. The TA checks the validity of the RID_v and then computes the pseudonym $Ps = h_3(RID_v \| s)$. Finally, it saves $< RID_R, PW, Ps >$ to the registration list and preloads $Ps$to the vehicle's TPD.

C. VEHICLE JOINING PHASE

In this phase, the vehicle joins the RSU and creates a mutual authentication. To start the OBU, the driver of a vehicle should feedback TPD with RID_v and PW to check the validity of the driver. If valid, the OBU starts the joining process as follows.

1) The OBU generates a random integer $r \in Z_q^*$ and computes $PID_{v1} = r.P$ and $PID_{v2} = Ps \bigoplus h_1(r.Pub)$. Then, the OBU sends $\{T_1, PID_v, \sigma_{OBU}\}$ to the RSU, where, $PID_v = \{PID_{v1}, PID_{v2}\}$ and $\sigma_{OBU} = h_3(T_1 \| Ps)$.
2) After the RSU receives the message $\{T_1, PID_v, \sigma_{OBU}\}$, it first checks the validity of timestamp T_1. Each timestamp T is checked as follows. Suppose T_r is the receiving time and T is the predefined time delay. If $(T > T_r - T)$, then T is valid. Otherwise, the message is rejected. If T_1 is valid, RSU computes $Ps = PID_{v2} \bigoplus h_1(s.PID_{v1})$ and checks whether $\sigma_{OBU} = ?h_3(T_1 \| Ps)$. If not, RSU rejects the message; otherwise, it sends $\{T_2, RID_R, Ps\}$to TA.
3) After the TA receives the message $\{T_2, RID_R, Ps\}$, it first checks the validity of timestamp T_2. If valid, then the TA checks whether $\{Ps, RID_R\}$ match the stored values. If not, then the TA rejects the message and sends a $\{not\ verified\}$ message to RSU. Otherwise, it sends a $\{verified\}$ message.
4) After the RSU receives the message $\{verified/not\ verified\}$, it checks whether the content of the message is $\{verified\}$. If not, the RSU drops the message and the vehicle is identified as illegal. Otherwise, it prepares the signature Sk with its expiration time T_{Sk} for the vehicle, where $Sk = s.h_2(PID_{v1} \ \| \ PID_{v2} \ \| \ T_{Sk})$. Finally, the RSU sends $\{T_3, T_{Sk}, Sk\_enc, \sigma_{RSU}\}$ to the OBU, where $\sigma_{RSU} = h_2(Sk \ \| \ T_3 \ \| \ T_{Sk})$ and $Sk\_enc = Sk \bigoplus h_1(s.PID_{v1})$.
5) After the OBU receives the message $\{T_3, T_{Sk}, Sk\_enc, \sigma_{RSU}\}$, it first checks the validity of timestamp T_3. If it is valid, then the OBU computes $Sk = Sk\_enc \bigoplus h_1(r.Pub)$. It then checks whether $\sigma_{RSU} = ?h_2(Sk \ \| \ T_3 \ \| \ T_{Sk})$. If so, it starts using Sk to broadcast beacons.

D. RENEW SIGNATURE PHASE

When T_{Sk} expires, the OBU needs to renew the Sk. This is done as follows:

1) The OBU randomly generates a new integer $r^{new} \in Z_q^*$ and computes a new PID_v^{new}, where $PID_{v1}^{new} = r^{new}.P$ and $PID_{v2}^{new} = Ps \bigoplus h_1(r^{new}.Pub)$. The OBU then sends $\{T_1, T_{Sk}, PID_v^{new}, PID_v, \sigma_v\}$ to the RSU, where $\sigma_v = Sk + r.h_2(PID_{v1}^{new} \| PID_{v2}^{new} \| T_1)$.
2) After the RSU receives the message $\{T_1, T_{Sk}, PID_v^{new}, PID_v, \sigma_v\}$, it first checks the validity of timestamp T_1. If it is valid, it checks the expiration time T_{Sk} (the OBU has determined by the period time to request new Sk). If not valid, RSU rejects the message and OBU should implement the vehicle joining phase.

Otherwise, it checks the validity of the vehicle using the following equation:

$$\sigma_v P = h_2\left(PID_{v1} \parallel PID_{v2} \parallel T_{Sk}\right).Pub + h_2\left(PID_{v1}^{new} \parallel PID_{v2}^{new} \parallel T_1\right) PID_{v1} \quad (1)$$

If Equation (1) is not valid, the RSU rejects the message; otherwise, it prepares a new $Sk^{new} = s.h_2(PID_{v1}^{new} \parallel PID_{v2}^{new} \parallel T_{Sk})$ where, T_{Sk} is the new expiration time. Finally, RSU sends $\{T_2, T_{Sk}, Sk\_enc, \sigma_{RSU}\}$ to the OBU, where $Sk_{enc} = Sk^{new} \bigoplus h_1(s.PID_{v1}^{new})$ and $\sigma_{RSU} = h_2(Sk^{new} \parallel T_2 \parallel T_{Sk})$.

3) After the OBU receives the message $\{T_2, T_{Sk}, Sk\_enc, \sigma_{RSU}\}$, it first checks the validity of timestamp T_2. If this is valid, it computes $Sk^{new} = Sk\_enc \bigoplus h_1(r^{new}.Pub)$. Finally, the OBU checks whether $\sigma_{RSU} = ?h_2(Sk^{new} \| T_2 \| T_{Sk})$. If this holds, then the 'renew signature' process is completed and the OBU starts broadcasting beacons with a new Sk.

The 'renew signature' process can be carried out with any RSU. This means when a vehicle leaves the first RSU and needs to renew the signature, the new RSU does not need to connect to the TA to ensure the legitimacy of the vehicle, since the previous signature Sk was signed by the first RSU with the private key s.

E. BROADCASTING AND VERIFICATION PHASE

1) BROADCASTING

After the OBU joins the RSU, it starts broadcasting beacons using Sk as a signature for each beacon, as follows:

- The OBU computes the message signature $\sigma_m = Sk + r.h_3(m \parallel T)$.
- The OBU computes $\omega = h_3(m \parallel T) PID_{v1}$, which is used to mitigate the verification time for the receptor.
- The OBU broadcasts the beacon $\{T, T_{Sk}, PID_v, m, \omega, \sigma_m\}$.

2) VERIFICATION

After the RSU or one OBU receives the beacon $\{T, T_{Sk}, PID_v, m, \omega, \sigma_m\}$, it first checks the validity of the timestamps $\{T, T_{Sk}\}$. If so, it continues verifying the beacon by one of the following:

a: SINGLE VERIFICATION

The recipient (the RSU or OBU) verifies the single beacon using the following equation:

$$\sigma_m P = h_2\left(PID_{v1} \parallel PID_{v2} \parallel T_{Sk}\right) Pub + \omega \quad (2)$$

If Equation (2) does not hold, the recipient rejects the beacon. Otherwise, the signature is valid, the sender is legal and the recipient accepts the beacon.

b: BATCH VERIFICATION

When the recipient (the RSU or OBU) receives a large number of beacons, the proposed scheme uses a batch verification method to mitigate the amount of time consumed. To meet the non-repudiation requirement, we use a technique called the small exponent test [19], [20]. The recipient generates a vector of random integers $x = \{x_1, x_2, \ldots x_n\}$, where $x_i \in [1, 2^t]$ and t is a small number, which does not increase the computational cost. Then, it verifies the beacons using the following equation:

$$\left(\sum_{i=1}^{n}\left(x_i \sigma_{m,i}\right)\right).P = \left(\sum_{i=1}^{n}\left(x_i h_2(PID_{i,v1} \parallel PID_{i,v2} \parallel T_{i,Sk})\right)\right).Pub + \sum_{i=1}^{n}(x_i \omega_i) \quad (3)$$

If Equation (3) holds, all signatures are valid, all senders are legal and the recipient accepts all beacons. Otherwise, one or more vehicles are illegal. A new algorithm is proposed in [31] to identify these illegal vehicles. For more details, the reader is referred to [31].

F. VEHICLE REVOCATION PHASE

This phase is very important in a VANET to allow the TA not only to trace a malicious authenticated vehicle and reveal its identity, but also to prevent this vehicle from taking further part in a VANET. This phase is as follows.

1) If a malicious authenticated vehicle is broadcasting bogus beacons, the RSU computes its pseudonym according to PID_v, where $Ps = PID_{v2} + h_1(s.PID_{v1})$.
2) The RSU sends Ps to the TA.
3) The TA reveals the real identity of the culprit vehicle, according to Ps in the registration list, and then deletes it from the registration list and sends an $\{acknowledgement\ message\}$ to the RSU.
4) After receiving the $\{acknowledgement\ message\}$ from the TA, the RSU prevents this vehicle from renewing the signature and adds all its information to a temporary list. At the same time, it sends this list to the nearby RSUs to prevent the vehicle from renewing the signature with other RSUs, in case the vehicle moves out of range of the current RSU. When T_{SK} expires, the OBU cannot renew the signature. However, a revoked OBU may have the ability to broadcast beacons until T_{Sk} expires.

V. SECURITY ANALYSIS AND COMPARISON

This section presents a security analysis of our proposed scheme, in order to demonstrate that our scheme is strongly secured under a random oracle model and to ensure that it meets the security and privacy requirements mentioned in Section III-B. We also present a comparison of our scheme with existing methods.

A. SECURITY PROOF

Theorem 1:The equations used in the proposed scheme are correct.

Proof of Equation (1): In the 'renew signature' phase, the RSU checks the validity of the vehicle according to

Equation (1).

$$
\begin{aligned}
&L.H.S.\sigma_v P \\
&= \left(Sk + r.h_2\left(PID_{v1}^{new} \parallel PID_{v2}^{new} \parallel T_1\right)\right).P \\
&= (\, s.h_2(\, PID_{v1} \parallel PID_{v2} \parallel T_{Sk}\,) + r.h_2(\, PID_v^{new} \parallel PID_{v2}^{new} \\
&\quad \parallel T_1\,)\,).P \\
&= (\, h_2\,(PID_{v1} \parallel PID_{v2} \parallel T_{Sk})\,.s.P + h_2\,(\, PID_{v1}^{new} \parallel PID_{v2}^{new} \\
&\quad \parallel T_1\,)\,.r.P\,) \\
&= (\, h_2\,(PID_{v1} \parallel PID_{v2} \parallel T_{Sk})\,.Pub + h_2\,(\, PID_{v1}^{new} \parallel PID_{v2}^{new} \\
&\quad \parallel T_1\,)\,.PID_{v1}\,) \\
&= R.H.S.
\end{aligned}
$$

Thus, it is verified that Equation (1) is accurate.

Proof of Equation (2): In single verification, the recipient verifies the beacon using Equation (2).

$$
\begin{aligned}
&L.H.S.\sigma_m P \\
&\quad = (Sk + r.h_3\,(m \parallel T))\,.P \\
&\quad = (s.h_2\,(PID_{v1} \parallel PID_{v2} \parallel T_{Sk}) + r.h_3\,(m \parallel T))\,.P \\
&\quad = h_2\,(PID_{v1} \parallel PID_{v2} \parallel T_{Sk})\,.s.P + h_3\,(m \parallel T)\,.r.P \\
&\quad = h_2\,(PID_{v1} \parallel PID_{v2} \parallel T_{Sk})\,.Pub + h_3\,(m \parallel T)\,.PID_{v1} \\
&\quad = h_2\,(PID_{v1} \parallel PID_{v2} \parallel T_{Sk})\,.Pub + \omega \\
&\quad = R.H.S.
\end{aligned}
$$

Thus, Equation (2) is verified as accurate.

Proof of Equation (3): In batch verification, the recipient verifies the beacons using Equation (3).

$$
\begin{aligned}
&L.H.S\left(\sum_{i=1}^{n}\left(x_i\sigma_{m,i}\right)\right).P \\
&= \left(\sum_{i=1}^{n}\left(x_i(Sk + r.h_3\,(m \parallel T))\right)\right).P \\
&= (\sum_{i=1}^{n}(\, x_i\,(\, s.h_2(PID_{i,v1} \parallel PID_{i,v2} \parallel T_{i,Sk}) + r_i.h_3\,(\, m_i \\
&\quad \parallel T_i\,)\,)\,)\,).P \\
&= (\sum_{i=1}^{n}(\, x_i h_2(PID_{i,v1} \parallel PID_{i,v2} \parallel T_{i,Sk}).s.P + x_i h_3\,(\, m_i \\
&\quad \parallel T_i\,)\,.r_i.P\,)\,) \\
&= (\sum_{i=1}^{n}(\, x_i h_2(PID_{i,v1} \parallel PID_{i,v2} \parallel T_{i,Sk}).Pub + x_i h_3\,(\, m_i \\
&\quad \parallel T_i\,)\,.PID_{i,v1}\,)\,) \\
&= \left(\sum_{i=1}^{n}\left(x_i h_2(PID_{i,v1} \parallel PID_{i,v2} \parallel T_{i,Sk}).Pub + x_i\omega_i\right)\right) \\
&= \left(\sum_{i=1}^{n}\left(x_i h_2(PID_{i,v1} \parallel PID_{i,v2} \parallel T_{i,Sk})\right)\right).Pub + \sum_{i=1}^{n}(x_i\omega_i) \\
&= R.H.S.
\end{aligned}
$$

Thus, Equation (3) is verified as accurate.

To analyse the security proof in the proposed scheme, we construct a game between a challenger *Ch* and an adversary *Ad* based on the network model of a VANET and an adversary.

Theorem 2: Our proposed scheme is unforgeable against an adaptively chosen message attack under the random oracle model.

Proof: We assume that *Ad* can forge a legitimate signature $\{T, T_{Sk}, PID_v, m, \omega, \sigma_m\}$ for the message m, and that a ECDLP instance $(P, Q = sP)$ is given for two points P, Q on E/E_p and $s \in Z_q^*$. Then, by running *Ad* as a subroutine, the challenger *Ch* can solve the ECDLP with non-negligible probability.

Setup: Challenger *Ch* sets $Pub = Q = sP$ as a public key and produces public parameters $param = \{q, Pub, P, h_1, h_2, h_3\}$. *Ch* then builds and maintains three lists: $(h\_list_1, h\_list_2, h\_list_3)$. Finally, *Ch* sends *param* to *Ad*.

h_list_1-Oracle: Ch maintains h_list_1 in the form $\langle \alpha, \tau h_1 \rangle$ and initialises it to empty. After *Ch* receives a request from *Ad* with a message α, it first checks whether the tuple $\langle \alpha, \tau h_1 \rangle$ is in h_list_1. If so, *Ch* sends $\tau h_1 = h(\alpha)$ to *Ad*. Otherwise, *Ch* randomly selects $\tau h_1 \in Z_q^*$ and inserts $\langle \alpha, \tau h_1 \rangle$ into h_list_1. Then *Ch* sends $\tau h_1 = h(\alpha)$ to *Ad*.

h_list_2-Oracle: Ch maintains h_list_2 in the form $\langle PID_{v1}, P\ ID_{v2}, T_{Sk}, \tau h_2 \rangle$ and initialises it to empty. After *Ch* receives a request from *Ad* with the message $(PID_{v1}, PID_{v2}, T_{Sk})$, it first checks whether the tuple $\langle PID_{v1}, P\ ID_{v2}, T_{Sk}, \tau h_2 \rangle$ is in h_list_2. If so, *Ch* sends $\tau h_2 = h((PID_{v1} \| PID_{v2} \| T_{Sk})$ to *Ad*. Otherwise, *Ch* randomly selects $\tau h_2 \in Z_q^*$ and inserts $\langle PID_{v1}, P\ ID_{v2}, T_{Sk}, \tau h_2 \rangle$ into h_list_2. Then *Ch* sends $\tau h_2 = h((PID_{v1} \| PID_{v2} \| T_{Sk})$ to *Ad*.

h_list_3-Oracle: Ch maintains h_list_3 in the form $\langle m, T, \tau h_3 \rangle$ and initialises it to empty. After *Ch* receives a request from *Ad* with the message (m, T), it checks whether the tuple $\langle m, T, \tau h_3 \rangle$ is in h_list_3. If so, *Ch* sends $\tau h_3 = h(m \parallel T)$ to *Ad*. Otherwise, *Ch* randomly selects $\tau h_3 \in Z_q^*$ and inserts $\langle m, T, \tau h_3 \rangle$ into h_list_3. Then *Ch*sends $\tau h_3 = h(m \parallel T)$ to *Ad*.

Sign-Oracle: After *Ch* receives a sign request via message m from *Ad*, it generates three random numbers, $h_{i,2}, h_{i,3}, \sigma_m \in Z_q^*$, and one random point $PID_{v2} \in G$. Then *Ch* calculates $PID_{v1} = (\sigma_m P - h_{i,2}Pub)/h_{i,3}$. *Ch* inserts $\langle PID_{v1}, P\ ID_{v2}, T_{Sk}, \tau h_2 \rangle$ into h_list_2 and $\langle PID_{v1}, P\ ID_{v2}, T_{Sk}, \tau h_2 \rangle$ into h_list_3. Finally, *Ch* builds a beacon, $\{T, T_{Sk}, PID_v, m, \omega, \sigma_m\}$ and sends it to *Ad*, where $PID_v = \{PID_{v1}, PID_{v2}\}$. The response to the Sign-Oracle is valid since the beacon $\{T, T_{Sk}, PID_v, m, \omega, \sigma_m\}$ satisfies Equation (2) as follows:

$$
\begin{aligned}
\sigma_m P &= h_{i,2}Pub + \omega \quad \text{where } \omega = h_{i,3}PID_{v1} \\
\sigma_m P &= h_{i,2}Pub + h_{i,3}PID_{v1} \\
&= h_{i,2}Pub + \left(\sigma_m P - h_{i,2}Pub\right) = \sigma_m P
\end{aligned} \tag{4}
$$

Output: Finally, *Ad* outputs a beacon $\{T, T_{Sk}, PID_v, m, \omega, \sigma_m\}$. *Ch* verifies this beacon using the following

equation:

$$\sigma_m P = h_{i,2} Pub + \omega \tag{5}$$

where $\omega = h_{i,3} PID_{v1}$

If this equation does not hold, *Ch* terminates the game.

According to the forgery lemma in [18], *Ad* can output another valid beacon $\{T, T_{Sk}, PID_v, m, \omega, \sigma_m^*\}$ that satisfies the following equation:

$$\sigma_m^* P = h_{i,2}^* Pub + \omega \tag{6}$$

where $\omega = h_{i,3} PID_{v1}$

Based on Equations (5) and (6), we can deduce

$$\begin{aligned}\left(\sigma_m - \sigma_m^*\right) P &= \sigma_m P - \sigma_m^* P \\ &= h_{i,2} Pub + \omega - \left(h_{i,2}^* Pub + \omega\right) = h_{i,2} Pub - h_{i,2}^* Pub \\ &= \left(h_{i,2} - h_{i,2}^*\right) Pub = \left(h_{i,2} - h_{i,2}^*\right) s.P \end{aligned} \tag{7}$$

Then, we can obtain $\left(\sigma_m - \sigma_m^*\right) = \left(h_{i,2} - h_{i,2}^*\right) s \ mod \ p$. *Ch* outputs $s = \left(\sigma_m - \sigma_m^*\right) . \left(h_{i,2} - h_{i,2}^*\right)^{-1}$ as a solution to the given ECDLP instance. However, this contradicts the hardness of ECDLP. Thus, our proposed scheme under the random oracle model is resistant against a chosen adaptive message.

B. SECURITY ANALYSIS

1) MESSAGE INTEGRITY AND AUTHENTICATION

Consistent with Theorem 2, the ECDLP is hard. Thus, the adversary cannot forge a valid beacon in our proposed scheme, and recipients can examine the integrity and validity of the beacon $\{T, T_{Sk}, PID_v, m, \omega, \sigma_m\}$ by checking whether the equation $\sigma_m P = h_2 \left(PID_{v1} \parallel PID_{v2} \parallel T_{Sk}\right) Pub + \omega$ holds. Hence, our proposed scheme satisfies the message integrity and authentication requirement.

2) PRIVACY PRESERVATION

In our scheme, the vehicle obtains the pseudonym *Ps* during the registration process from the TA, which is the only element that knows the real identity RID_v of the vehicle, where $Ps = h_3(RID_v \| s)$. The vehicle uses *Ps* to generate the PID_v that is included with the beacons, where $PID_{v1} = r.P$, $PID_{v2} = Ps \bigoplus h_1(r.Pub)$, and $r \in Z_q^*$ is a random integer number. Hence, the adversary cannot acquire the real identity even if the RSU is compromised. In our scheme, the vehicle also renews the signature and updates PID_v after the T_{Sk} expires, meaning that after a short time, an adversary receives a beacon message containing a different PID_v and signed with a new *Sk*. It is therefore very difficult for an adversary to generate a correlation between the fast-changing pseudonyms for the vehicle, and the adversary cannot acquire the location of the vehicle. Thus, our proposed scheme satisfies the requirement for privacy preservation.

3) TRACEABILITY AND REVOCATION

In the proposed scheme, although a beacon does not contain any information about RID_v, the TA can trace and revoke the bogus vehicle, as mentioned in Section IV-F. Thus, our proposed scheme satisfies the traceability and revocation requirements.

4) NON-REPUDIATION

In our scheme, once the TA has traced the RID_v of a beacon sent to the VANET, the beacon sender will not be able to deny he/she sent this beacon since the OBUs broadcast dissimilar beacons based on their own unique *Ps*. In addition, in the process of batch verification of beacons, we use a random integer vector $x = \{x_1, x_2, \ldots x_n\}$ to exam any exchanges of the beacons. Thus, our proposed scheme satisfies the non-repudiation requirement.

5) CONDITIONAL ANONYMITY

The real identity of the offender vehicle in our scheme is traced and revoked from the VANET when malicious activity is detected, as mentioned in Section IV-F. However, the anonymity of honest vehicles is guaranteed in the scheme. Thus, our proposed scheme satisfies the conditional anonymity requirement.

6) RESISTANCE TO IMPERSONATION ATTACK

- In the case where an attacker attempts to impersonate the vehicle in the joining phase: In the proposed scheme, the joining message $\{T_1, PID_v, \sigma_{OBU}\}$ that is sent by the vehicle to the RSU contains $\sigma_{OBU} = h_3(T_1 \parallel Ps)$. Therefore, an attacker cannot impersonate any vehicle because he/she does not have the vehicle's pseudonym *Ps*.
- In the case where an attacker attempts to impersonate the vehicle while renewing the signature: The message $\{T_1, T_{Sk}, PID_v^{new}, PID_v, \sigma_v\}$ sent by the vehicle to the RSU to renew the signature *Sk* contains$\sigma_v = Sk + r.h_2(PID_{v1}^{new} \parallel PID_{v2}^{new} \parallel T_1)$. Hence, an attacker must have the old *Sk* and the random number *r* to be able to impersonate the vehicle that wants to renew the signature.
- In the case where an attacker attempts to impersonate the vehicle while broadcasting beacons: In the proposed scheme, the beacon message $\{T, T_{Sk}, PID_v, m, \omega, \sigma_m\}$, has the signature σ_m, signed with *Sk* and the random number *r*. Therefore, the attacker must acquire *r* and *Sk* to impersonate the vehicle. This is difficult, because *r* is a random number generated by the vehicle and *Sk* is a signature that has a limited period of validity and is generated by the RSU for the vehicle.

Thus, an impersonation attack is ineffective in our scheme.

7) RESISTANCE TO A REPLAY ATTACK

In the beacon message $\{T, T_{Sk}, PID_v, m, \omega, \sigma_m\}$, we use the current timestamp *T*. An attacker cannot modify *T* in a beacon since in the verification process, the beacon would be rejected if *T* was invalid or had expired. Thus, the replay attack is ineffective in the proposed scheme.

8) RESISTANCE TO A MODIFICATION ATTACK

In this scheme, the beacon contains the signature σ_m, which ensures the safety of the message from modification. If an attacker modifies the beacon, it would be rejected in the signature verification process. Thus, the modification attack is ineffective in the proposed scheme.

9) RESISTANCE TO A MITM ATTACK

In our scheme, mutual authentication is carried out between the sender and the verifier. If an adversary attempts an MITM attack, he/she needs to forge beacons to connect with the sender and the verifier. However, according to Theorem 2, it is impossible for an adversary to issue this type of attack. Thus, the MITM attack is ineffective in our scheme.

C. COMPARISION WITH EXISTING SCHEMES

This subsection presents a comparison of our scheme with prior approaches regarding issues found in groups [13]–[20], [21]–[26], and [27], [28]. The proposed scheme does not depend on a bilinear pairing operation and satisfies the requirements for revocation and privacy. It also does not depend on the RSU to verify beacons. Table 2 presents the results of comparison.

TABLE 2. Comparison with existing schemes.

Feature	[13-20]	[21-26]	[27-28]	Our scheme
Uses a bilinear pairing operation	Yes	No	No	No
Does not meet the revocation requirement and an insider attack can obtain RID	Yes	Yes	No	No
Beacons verified by the RSU	No	No	Yes	No

VI. PERFORMANCE EVALUATION

This section explains the computation and communication costs.

A. COMPUTATION COST

In this subsection, we demonstrate the performance of our scheme by comparing it with those of Jianhong et al. [20], Debiao et al. [22], Libing et al. [25], and Jie et al. [27] in terms of computation cost. The cryptography operation in [20] is built on bilinear pairings, while those of [22], [25], [27] and our scheme use ECC. In a bilinear pairing with an 80-bit security level, the additive group $\bar{G}$ is generated based on an elliptic curve $\bar{E}: y^2 = x^3 + x \ mod \ \bar{p}$, where $\bar{p}$ is a 512-bit prime number. However, in ECC with the same security level, the additive group G is generated based on an elliptic curve $E: y^2 = x^3 + ax + b \ mod \ p$, where p is a 160-bit prime number. The execution times for the cryptographic operations used in [22] are adopted in this paper, as shown in Table 3 (where Abbr. means the abbreviations of cryptographic operations). Since the execution time of the concatenate and XOR operations is much lower than the execution time for a hash function, these are considered negligible and are excluded from the analysis of computation cost.

TABLE 3. Execution time and descriptions of cryptographic operations[22].

Abbr.	Execution time (ms)	Description
T_{bp}	4.211	Bilinear pairing operation
T_{sm-bp}	1.709	Scalar multiplication operation in a group based on bilinear pairing
$T_{sm-bp-s}$	0.0535	Small scalar point multiplication operation in a group based on bilinear pairing
T_{pa-bp}	0.0071	Point addition operation in a group based on bilinear pairing
T_{mtp}	4.406	Map-to-point hash function
T_{sm-ecc}	0.442	Scalar multiplication operation in a group based on ECC
$T_{sm-ecc-s}$	0.0138	Small scalar point multiplication operation in a group based on ECC
T_{pa-ecc}	0.0018	Point addition operation in a group based on ECC
T_h	0.0001	General hash function operation

For simplicity, let *BGS*, *SVOB* and *BVMB* denote the generation and signing of the beacon, the single verification for a beacon, and the batch verification for multiple beacons, respectively. In the scheme of Jianhong et al. [20], *BGS* comprises the following operations: six scalar multiplications; two point additions; one map-to-point hash function; and four secure hash functions. Hence, the total computation time of *BGS* is $6T_{sm-bp} + 2T_{pa-bp} + 1T_{mtp} + 4T_h \approx 14.6746$. *SVOB* for this scheme involves the following operations: three bilinear pairings; two scalar multiplications; one point addition; and three secure hash function. Thus, the overall computation time of *SVOB* is $3T_{bp} + 2T_{sm-bp} + 1T_{pa-bp} + 3T_h \approx 16.0584$. *BVMB* for this scheme involves the following operations: three bilinear pairings; (n+1) scalar multiplications; ($2n$) small scalar point multiplications; ($3n-2$) point additions; and ($3n$) secure hash functions. This means that the total computation time of the *BVMB* is $3T_{bp} + (n+1)\,T_{sm-bp} + (2n)\,T_{sm-bp-s} + (3n-2)\,T_{pa-bp} + (3n)\,T_h \approx 1.8376n + 14.3267$.

In the scheme of Debiao et al. [22], *BGS* comprises three scalar multiplications and three secure hash functions. Hence, the total computation time of *BGS* is $3T_{sm-e} + 3T_h \approx 1.3263$. *SVOB* in this scheme involves three scalar multiplications, two secure hash functions and two point additions, giving an overall computation time for *SVOB* of $3T_{sm-ecc} + 2T_h + 2T_{pa-ecc} \approx 1.3298$. *BVMB* in this scheme requires ($n+2$) scalar multiplications; ($2n$) small scalar point

multiplications; $(2n-1)$ point additions; and $(2n)$ secure hash functions. The overall computation time for *BVMB* is therefore $(n+2)\,T_{sm-ecc} + (2n)\,T_{sm-ecc-s} + (2n-1)\,T_{pa-ecc} + (2n)\,T_h \approx 0.4734n + 0.8822$.

In the scheme of Libing et al. [25], *BGS* comprises two scalar multiplications and two secure hash functions, giving an overall computation time for *BGS* of $2T_{sm-ecc} + 2T_h \approx 0.8841$. *SVOB* for this scheme is comprises four scalar multiplications, two secure hash functions, and two point additions. Hence, the overall computation time for *SVOB* is $4T_{sm-ecc} + 2T_h + 2T_{pa-ecc} \approx 1.7718$. *BVMB* involves the following operations: $(2n+2)$ scalar multiplications; $(2n)$ small scalar point multiplications; $(2n+2)$ point additions; and $(2n)$ secure hash functions, giving an overall computation time for *BVMB* of $(n+2)\,T_{sm-ecc} + (2n)\,T_{sm-ecc-s} + (2n-1)\,T_{pa-ecc} + (2n)\,T_h \approx 0.9154n + 0.8876$.

In the scheme of Jie et al. [27], *BGS* comprises two scalar multiplications and two secure hash functions, giving an overall computation time for the *BGS* of $2T_{sm-ecc} + 2T_h \approx 0.8841$. *SVOB* and *BVMB* for this scheme are achieved using the RSU, and involve four steps, as follows:

- **In the first step**, the RSU verifies the public keys with the shared secrets. This requires one scalar multiplication and one secure hash function for each beacon.
- **In the second step**, the RSU checks the validity of beacons. Here, *SVOB* comprises two scalar multiplications, one secure hash function, and one point addition. *BVMB* involves two scalar multiplications, $(2n)$ small scalar point multiplications, $(n+1)$ point additions, and (n) secure hash functions.
- **In the third step**, the RSU fills the cuckoo filter with the valid and invalid signatures to generate the notification message. Here, the RSU carries out only three secure hash functions for each beacon.
- **In the last step**, when a vehicle receives the notification message and beacons, it uses three secure hash functions to verify whether the beacon's signature appears in the positive or negative list.

Hence, the total computation times of *SVOB* and *BVMB* in the scheme of Jie et al. [27] are $3T_{sm-e} + 7T_h 1T_{pa-ecc} \approx 1.3285$ and $(n+2)2T_{sm-ecc} + (2n)\,T_{sm-ecc-s} + (n1)\,T_{pa-ecc} + (7n)T_h \approx 0.4721n + 0.8838$, respectively.

In our proposed scheme, *BGS* involves one scalar multiplication and two secure hash functions. Thus, the total computation time of *BGS* is $1T_{sm-ecc} + 2T_h \approx 0.4422$. *SVOB* involves two scalar multiplications, one secure hash function, and one point addition, giving an overall computation time for the *SVOB* of $2T_{sm-ecc} + 1T_h + 1T_{pa-ecc} \approx 0.8859$. *BVMB* involves two scalar multiplications, $(2n)$ small scalar point multiplications, $(n+1)$ point additions and (n) secure hash functions, giving a total computation time for *BVMB* of $(n+2)\,T_{sm-ecc} + (2n)\,T_{sm-ecc-s} + (2n-1)\,T_{pa-ecc} + (2n)\,T_h \approx 0.0295n + 0.9153$. Table 4 presents a comparison of the computation cost of the proposed scheme with other four ID-based schemes in terms of *BGS, SVOB* and *BVMB*.

TABLE 4. Computation cost of five ID-based schemes.

Schemes	*BGS (ms)*	*SVOB (ms)*	*BVMB (ms)*
Jianhong et al. [20]	$6T_{sm-bp} + 2T_{pa-bp} + 1T_{mtp} + 4T_h \approx$ **14.6746** .	$3T_{bp} + 2T_{sm-bp} + 1T_{pa-bp} + 3T_h \approx$ **16.0584**	$3T_{bp} + (n+1)T_{sm-bp} + (2n)T_{sm-bp-s} + (3n-2)T_{pa-bp} + (3n)T_h \approx$ $\mathbf{1.8376n + 14.3267}$
Debiao et al. [22]	$3T_{sm-ecc} + 3T_h \approx$ **1.3263**	$3T_{sm-ecc} + 2T_h + 2T_{pa-ecc} \approx$ **1.3298**	$(n+2)T_{sm-ecc} + (2n)T_{sm-ecc-s} + (2n-1)T_{pa-ecc} + (2n)T_h \approx$ $\mathbf{0.4734n + 0.8822}$
Libing et al. [25]	$2T_{sm-ecc} + 2T_h \approx$ **0.8841**	$4T_{sm-ecc} + 2T_h + 2T_{pa-ecc} \approx$ **1.7718**	$(2n+2)T_{sm-ecc} + (2n)T_{sm-ecc-s} + (2n+2)T_{pa-ecc} + (2n)T_h \approx$ $\mathbf{0.9154n + 0.8876}$
Jie et al. [27]	$2T_{sm-ecc} + 2T_h \approx$ **0.8841**	$3T_{sm-ecc} + 7T_h + 1T_{pa-ecc} \approx$ **1.3285**	$(n+2)T_{sm-ecc} + (2n)T_{sm-ecc-s} + (n+1)T_{pa-ecc} + (7n)T_h \approx$ $\mathbf{0.4721n + 0.8838}$
Our scheme	$1T_{sm-ecc} + 2T_h \approx$ **0.4422**	$2T_{sm-ecc} + 1T_h + 1T_{pa-ecc} \approx$ **0.8859**	$2T_{sm-ecc} + (2n)T_{sm-ecc-s} + (n+1)T_{pa-ecc} + nT_h \approx$ $\mathbf{0.0295n + 0.9153}$

As shown in Table 4, the computation time for *BGS* in the proposed scheme is 0.4422 ms, which is 96.9%, 66.7%, 49.9% and 49.9% lower than the schemes of Jianhong et al. [20], Debiao et al. [22], Libing et al. [25], and Jie et al. [27], respectively. The computation time for *SVOB* in our scheme is 0.8859 ms, i.e. 94.5%, 33.4%, 50% and 33.3% lower than in the above schemes, while the computation time for *BVMB* in our scheme for 50 beacons is 2.3903 ms, which is 97.8%, 90.3%, 94.9% and 90.2% lower than in the above schemes. Table 5 shows the improvement of our proposed scheme over the other schemes in terms of computation cost. Fig. 4 demonstrates that our scheme has a large advantage over the other four schemes with respect to *BGS* and *SVOB*. Fig. 5 shows the computation costs for *BVMB* for different numbers of beacons. Consequently, the proposed scheme is more efficient and effective than those of Jianhong et al. [20], Debiao et al. [22], Libing et al. [25], and Jie et al. [27] in terms of the computation cost for *BGS*, *SVOB* and *BVMB*.

TABLE 5. Improvement of our proposed scheme over other schemes in terms of computation cost.

Scheme	*BGS*	*SVOB*	*BVMB* (50 beacon)
Jianhong et al. [20]	96.9%	94.5%	97.8%
Debiao et al. [22]	66.7%	33.4%	90.3%
Libing et al. [25]	49.9%	50%	94.9%
Jie et al. [27]	49.9%	33.3%	90.2%

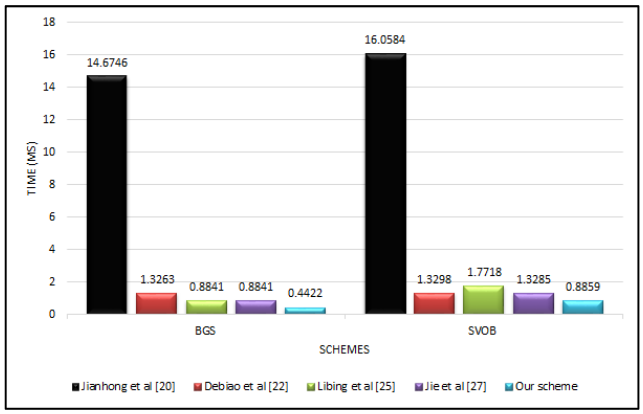

FIGURE 4. The computation costs of PGS and SVOB.

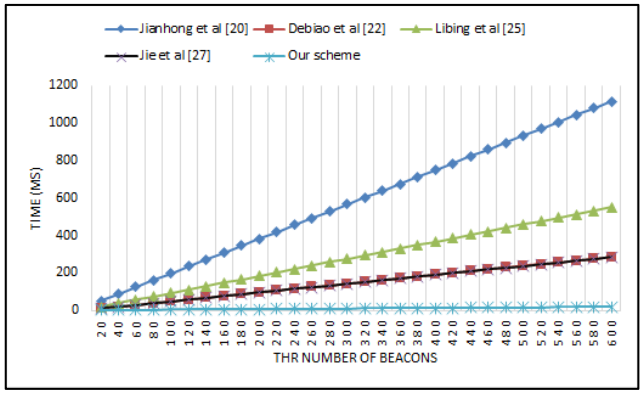

FIGURE 5. The computation costs of BVMB for the different number of beacons.

B. COMMUNICATION COST

We now compare our scheme with those of Jianhong et al. [20], Debiao et al. [22], Libing et al. [25], and Jie et al. [27] in terms of communication cost. As mentioned in the previous subsection, the size of $\overline{p}$ is 64 bytes, meaning that the size of each element in $\overline{G}$ is 128 bytes, and the size of p is 20 bytes, meaning that the size of each element in G is 40 bytes. We also assume that the output sizes of the timestamp, secure hash function and element in integer group Z_q^* are 4, 20 and 20 bytes, respectively. The comparative results of our scheme with prior schemes are listed in Table 6, where the content of the message is excluded.

TABLE 6. Comparison of communication cost.

Scheme	Message size (*bytes*)
Jianhong et al. [20]	388
Debiao et al. [22]	144
Libing et al. [25]	148
Jie et al. [27]	84
Our scheme	108

As shown in Table 6, the size of the beacon in the scheme of Jianhong et al. [20] is $(128 \times 3 + 4) = 388$ bytes, and the content of the beacon is three elements in $\bar{G}$ $\{ID_1, ID_2, \sigma \in \bar{G}\}$ and one timestamp. The beacon size in the scheme of Debiao et al. [22] is $(40 \times 3 + 20 + 4) = 144$ bytes, and the content of beacon is three elements in G $\{AID_i^1, AID_i^2, R_i \in G\}$, one element $\sigma_i \in Z_q$, and one timestamp. The beacon size in the scheme of Libing et al. [25] is $(40 \times 3 + 20 + 8) = 148$ bytes and the content of the beacon is three elements in $\{PID_{vi}, h_{ki}, R_i \in G\}$, one hash function $\delta_i \in Z_q$, and two timestamps. The beacon size in the scheme of Jie et al. [27] is $(40 + 20 \times 2 + 4) = 84$ bytes, and the content of beacon is one element in $ID_{i1} \in G$, two elements in $\{Z_q ID_{i2}, \sigma_i \in Z_q$, and one timestamp. In our proposed scheme, the vehicle broadcasts a beacon with size $(40 + 20 \times 3 + 8) = 108$ bytes and the content of beacon is one element in $\{PID_{v1} \in G\}$, three elements in $\{Z_q PID_{v2}, \sigma_m, \omega \in Z_q\}$, and two timestamps.

Table 6 shows that the overall communication overhead of our proposed scheme is relatively low. Here, the communication overhead in the scheme of Jie et al. [27] is slightly lower than ours, since the proposed scheme mitigates the computation cost for the recipient, where the sender of the beacon calculates part of Equations (2) and (3) by implement $\omega = h\,(m \parallel T)\, PID_{v1}$, and inserts ω into the beacon.

VII. CONCLUSION

This paper proposes a new pseudo-ID-based scheme for a VANET with conditional anonymity, message authentication and integrity. The proposed scheme depends on using a pseudonym instead of the real identity, and satisfies all the security and privacy requirements of a VANET as well as resisting common attacks. Our scheme can provide conditional anonymity in which only the real identity of a vehicle conducting malicious activity is revealed. We were able to overcome the previous drawbacks of ID-based schemes, and our scheme does not require the complex operations that are produced by a bilinear pairing operation. It can also preserve privacy in terms of the vehicle's real identity, even from an insider attacker. Furthermore, the TA can trace a bogus vehicle and revoke it as a member of the VANET. A security analysis shows that our scheme is secure under the random oracle module and can meet the security and privacy requirements of a VANET. We compare our scheme with recent proposed ID-based schemes and show that it has computation costs that are lower than previous schemes and lightweight communication. Our scheme resolves these challenges positively and is suitable for VANETs.

ACKNOWLEDGMENT

The authors are very grateful to the anonymous reviewers and the Associate Editor for providing constructive and generous feedback.

REFERENCES

[1] D. Lloyd. 2016. *Reported Road Casualties in Great Britain: Main Results 2015*. [Online]. Available: https://www.gov.uk/government/statistics/reported-road-casualties-in-great-britain-main-results-2015

[2] S. Bao, W. Hathal, H. Cruickshank, Z. Sun, P. Asuquo, and A. Lei, "A lightweight authentication and privacy-preserving scheme for VANETs using TESLA and Bloom Filters," *ICT Express*, vol. 4, no. 4, pp. 221–227, Dec. 2017.

[3] Y. Ming and X. Shen, "PCPA: A practical certificateless conditional privacy preserving authentication scheme for vehicular ad hoc networks," *Sensors*, vol. 18, no. 5, p. 1573, May 2018.

[4] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "VANET security surveys," *Comput. Commun.*, vol. 44, pp. 1–13, May 2014.

[5] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANet security challenges and solutions: A survey," *Veh. Commun.*, vol. 7, pp. 7–20, Jan. 2017.

[6] J. B. Kenney, " Dedicated short-range communications (DSRC) standards in the United States," *Proc. IEEE*, vol. 99, no. 7, pp. 1162–1182, Jul. 2011.

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

[8] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *J. Comput. Secur.*, vol. 15, no. 1, pp. 39–68, Jan. 2007.

[9] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in *Proc. 27th Conf. Comput. Commun. (INFOCOM)*, Apr. 2008, pp. 1229–1237.

[10] C. Zhang, X. Lin, R. Lu, and P.-H. Ho, "RAISE: An efficient RSU-aided message authentication scheme in vehicular communication networks," in *Proc. IEEE Int. Conf. Commun.*, May 2008, pp. 1451–1457.

[11] U. Rajput, F. Abbas, and H. Oh, "A Hierarchical Privacy Preserving Pseudonymous Authentication Protocol for VANET," *IEEE Access*, vol. 4, pp. 7770–7784, 2016.

[12] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proc. Workshop Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, Nov. 1984, pp. 47–53.

[13] 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. IEEE 27th Conf. Comput. Commun. (INFOCOM)*, Apr. 2008, pp. 246–250.

[14] C. Zhang, P.-H. Ho, and J. Tapolcai, "On batch verification with group testing for vehicular communications," *Wireless Netw.*, vol. 17, no. 8, pp. 1851–1865, Nov. 2011.

[15] Y. Jiang, M. Shi, X. Shen, and C. Lin, "BAT: A robust signature scheme for vehicular networks using binary authentication tree," *IEEE Trans. Wireless Commun.*, vol. 8, no. 4, pp. 1974–1983, Apr. 2009.

[16] D. Huang, S. Misra, M. Verma, and G. Xue, "PACP: An efficient pseudonymous authentication-based conditional privacy protocol for VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 12, no. 3, pp. 736–746, Sep. 2011.

[17] T. W. Chim, S. M. Yiu, L. C. Hui, and V. O. K. Li, "SPECS: Secure and privacy enhancing communications schemes for VANETs," *Ad Hoc Netw.*, vol. 9, no. 2, pp. 189–203, Mar. 2011.

[18] 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.

[19] S.-J. Horng, , Y. Pan, X. Wang, K. Khan, S.-F. Tzeng, P. Fan, T. Li "B-Specs+: Batch verification for secure pseudonymous authentication in VANET," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 11, pp. 1860–1875, Nov. 2013.

[20] 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, Sep. 2014.

[21] 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.

[22] 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.

[23] H. Zhong, J. Wen, J. Cui, and S. Zhang, "Efficient conditional privacy-preserving and authentication scheme for secure service provision in VANET," *Tsinghua Sci. Technol.*, vol. 21, no. 6, pp. 620–629, 2016.

[24] N.-W. Lo and J.-L. Tsai, "An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 5, pp. 1319–1328, May 2016.

[25] L. Wu, J. Fan, Y. Xie, J. Wang, and Q. Liu, "Efficient location-based conditional privacy-preserving authentication scheme for vehicle ad hoc networks," *Int. J. Distrib. Sensor Netw.*, vol. 13, no. 3, Mar. 2017, pp. 1–13.

[26] Y. Xie, L. Wu, J. Shen, and A. Alelaiwi, "EIAS-CP: New efficient identity-based authentication scheme with conditional privacy-preserving for VANETs," *Telecommun. Syst.*, vol. 65, no. 2, pp. 229–240, Jun. 2017.

[27] 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.

[28] H. Zhong, B. Huang, J. Cui, Y. Xu, and L. Liu, "Conditional privacy-preserving authentication using registration list in vehicular ad hoc networks," *IEEE Access*, vol. 6, pp. 2241–2250, 2018.

[29] V. S. Miller, "Use of elliptic curves in cryptography," in *Proc. Conf. Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, Dec. 1985, pp. 417–426.

[30] N. P. Smart, "The discrete logarithm problem on elliptic curves of trace one," *J. Cryptol.*, vol. 12, no. 3, pp. 193–196, Jun. 1999.

[31] J.-L. Huang, L.-Y. Yeh, and H.-Y. Chien, "ABAKA: An anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 60, no. 1, pp. 248–262, Jan. 2011.

MURTADHA A. ALAZZAWI received the bachelor's and master's degrees in computer science from Science College, Basra University, Iraq, in 2010 and 2013, respectively. He is currently pursuing the Ph.D. degree in computer science and technology with the Huazhong University of Science and Technology, China. He has five years of teaching experience and was working with the Imam Al-Kadhum College (IKC), before taking study leave and coming to China. His research interests are security and privacy issues in VANETS.

HONGWEI LU received the B.Sc., M.Sc., and Ph.D. degrees from the Huazhong University of Science and Technology (HUST), Wuhan, China, where he is currently a Professor with the School of Computer Science and Technology. His research interests are in security and privacy in ubiquitous computing and electronic commerce, with a focus on security protocol analysis, access control, and trust negotiation.

ALI A. YASSIN received the bachelor's and master's degrees from the University of Basrah, Basrah, Iraq, and the Ph.D. degree from the Huazhong University for Science and Technology, Wuhan, Hubei, China. He is currently an Assistant Professor with the Computer Science Department, Education College for Pure Science, University of Basrah, Iraq. His research interests include security of cloud computing, image processing, pattern recognition, biometrics, data integrity, DNA cryptography, steganography, sharing data, graphical password, QR code, and soft computing.

KAI CHEN received the M.S. and Ph.D. degrees from the School of Computer Science and Technology, Huazhong University of Science and Technology, in 2008 and 2012, respectively. His current research interests include computer network application, computer network security, and computer network protocol analysis.