IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 9, 2020, accepted August 4, 2020, date of publication August 17, 2020, date of current version August 27, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3017018

VPPCS: VANET-Based Privacy-Preserving Communication Scheme

MAHMOOD A. AL-SHAREEDA[1], MOHAMMED ANBAR[1], (Member, IEEE), SELVAKUMAR MANICKAM[1], AND ALI A. YASSIN[2]

[1]National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia (USM), Penang 11800, Malaysia
[2]Department of Computer Science, College of Education and Pure Science, University of Basrah, Basrah 61004, Iraq

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

ABSTRACT Over the past years, vehicular ad hoc networks (VANETs) have been commonly used in intelligent traffic systems. VANET's design encompasses critical features that include autonomy, distributed networking, and rapidly changing topology. The characteristics of VANET and its implementations for road safety have attracted considerable industry and academia interest, particularly in research involving transport systems enhancement that could potentially save lives. Message broadcasting in an open access system, such as VANET, is the main and utmost challenging problem with regard to security and privacy in VANETs. Various studies on VANET security and privacy have been proposed. Nevertheless, none has considered overall privacy requirements such as unobservability. In order to address these shortcomings, we propose a VANET based privacy-preserving communication scheme (VPPCS), which meets the requirements for content and contextual privacy. It leverages elliptic curve cryptography (ECC) and an identity-based encryption scheme. We have carried out a detailed security analysis (burrows–abadi–needham (BAN) logic, random oracle model, security of proof, and security attributes) to validate and verify the proposed scheme. The analysis has shown that our scheme is secure and also shown to be effective in a performance evaluation. The proposed scheme does not only meet the previously mentioned security and privacy requirements, but also impervious to various types of attacks such as replay, impersonation, modification, and man-in-the-middle attacks.

INDEX TERMS BAN logic, privacy-preserving, elliptic curve, random oracle model, identity-based cryptography.

I. INTRODUCTION

As the design of wireless communication technology and network systems is continuously and rapidly progressing, vehicular ad hoc networks (VANETs) have regained attention and interest in support of wireless vehicles in communicating with other vehicles and roadside units (RSUs) to guarantee traffic safety and improve driving experience [1]–[3]. VANETs also have the benefits of preventing collisions, lane-fusion, optimizing traffic, collecting toll, location-based services and infotainment [4]–[7]. VANET is basically Mobile ad hoc networks (MANETs) associated with vehicles and RSUs. In contrast to the nodes in a MANET, the power, storage, and computing capacity of vehicles are typically not resource constrained. Typical VANET contains trusted authorities (TAs), RSUs (e.g., road-side or other facilities), and onboard units (OBUs) equipped in vehicles [8], [9], as shown in Figure 1.

Using dedicated short-range communication (DSRC) protocol, the communication of VANET can be divided into vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) [8]. The OBU in the vehicle and the DSRC protocol will allow all vehicles to communicate on the roadside with adjacent vehicles and nearby RSUs. For example, traffic related messages on vehicle OBUs regularly broadcasts data on elements such as location, meteorological conditions, route, velocity, and traffic condition. The traffic-related message enables the participating vehicles in the region to take the necessary measures to prevent traffic accidents and avoid traffic congestion [10]. The traffic-related message (e.g., recent traffic incidents) may also be forwarded by the RSU and other vehicles to the traffic administration department and other relevant departments (e.g., the traffic police or fire department) to ensure necessary actions can be taken within

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

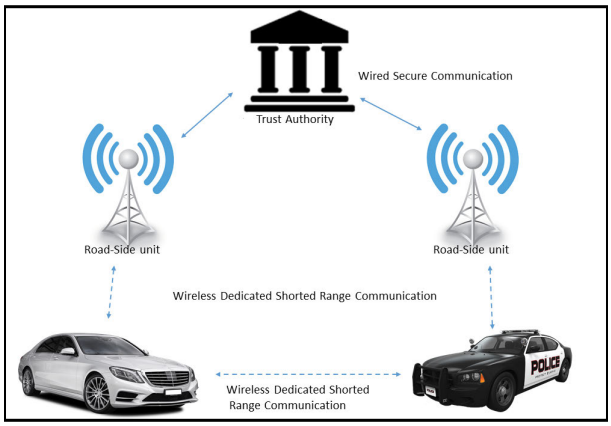

FIGURE 1. Typical structure of the VANET environment.

the stipulated time [4], [11]. However, any personal information of the user (e.g. identity or location) can expose to the drivers' to criminals(e.g., intercepting malicious attackers and replacing intercepted messages by modified messages to re-route victims' vehicles). The privacy protection should include content and contextual specifications. The privacy of content ensures that sensitive information associated with the vehicle against inappropriate and unauthorized disclosure. However, this alone is not sufficient because an attacker can still identify the vulnerabilities of the vehicle. This problem can be mitigated by introducing contextual confidentiality.

In turn, three sub requirements, namely,: anonymity, unlinkability, and unobservability, should be considered to ensure privacy is not tampered with [12], [13]. Anonymity is required when the driver has transmitted information regarding their identity to the RSU or other vehicles without masking. A malicious adversary can monitor driver's path by capturing these messages. Anonymity in VANETs is therefore another crucial feature [14]. Unlinkability is necessary to prevent the connection of the vehicle with the two or more messages from the same driver. Unobservability is crucial to ensure communication between vehicles and RSUs are not done by unauthorized entities.

In fact, by tapping into the communication of the vehicle, the broadcast message of the vehicle can be revealed. The communication should therefore be disguised [15]. In order to prevent message modification done for malicious intents from being transmitted to RSUs or near vehicles, VANET architecture should include traceability component, similar to the ones used by wireless network operators. Traceability is therefore an essential feature [11]. The trusted authority (TA) is the only party that can extract the true identity of the vehicle. However, as discussed in Section II, these current schemes have limitations, and none of them have considered the requirements of privacy. In order to meet these requirements, we propose a new V2V and V2I communicator-based privacy-preserving scheme that can address existing privacy preservation weaknesses that is inherent in existing VANET schemes. More specifically, the scheme describes the contributions of VPPCS as follows:

- A secure VANET based privacy preserving communication scheme called VPPCS, which protects privacy. Pseudonym-based identity verification signatures are used in the proposed scheme. In addition, batch verification is utilized to improve the computing efficiency of the scheme.
- Injecting fake messages during broadcasting, causing the attacker unable to discern if the message was sent.
- The proposed VPPCS uses a pseudonym set to sign the message which causes the attacker unable to identify the actual source of the message.
- A comprehensive security and privacy analysis is performed to demonstrate that the proposed scheme can withstand various attacks and satisfy the VANET security and privacy requirements.
- A security analysis that uses BAN logic, random oracle model, security of proof and security attributes are presented, which demonstrates that the proposed VPPCS is secure against various attacks such as (replay, impersonation, modification and man-in-middle).
- The balance between contextual privacy requirements and performance evaluation is provided and emphasized compared to existing related research
- The performance of the scheme are evaluated in terms of computational costs and overhead communication. The scheme is better suited to VANET services than existing schemes.

The rest of the paper is structured as follows. Most relevant existing works are listed in Section II. Section III briefly discusses the vehicular system architecture and preliminaries based on a detailed description of the proposed scheme in Section IV. Sections V and VI describe the security and performance assessments, respectively. Section VII provides the discussion. Some concluding remarks and future work are provided in Section VIII.

II. RELATED WORK

The problem of privacy occurs when sensitive and private traffic-related messages are available, which need to be shielded from misuse or disclosure. In From the vehicular communication context, privacy issues at all vehicle interaction levels, such as aggregation, and processing, collection, evaluation, and visualization, must be tackled. Privacy preservation is an important issue in this context given the sensitiveness sensitivity of the information exchanged [16]. This topic has been widely studied. The most relevant research is identified in below.

Ming and Shen [17] suggested a conditional privacy conservation scheme focused on a message recovery certificateless signature. The scheme promotes conditional privacy, and guarantees unlinkability since an adversary will not be able

to link a vehicle to its transmitted message. Nevertheless, the property of unobservability was not considered in this work.

Ming and Cheng [18] proposed a certificateless conditional privacy protection scheme based on elliptic curve. The scheme does not satisfy all privacy requirements, such as unobservability.

Hu *et al.* [19] proposed an HMAC-based security and privacy scheme that uses the revocation of vehicles instead of the certificate revocation list. It also provides anonymity. However, this scheme ignores the contextual privacy.

Xue and Ding [20] introduced location privacy-preserving authentication (LPA) scheme to address the issue of conditional privacy preserving in which safety messages can be anonymously authentication by peer vehicles. Also, the LPA scheme is supported by traceability features. However, unlinkability and unobservability requirements were not addressed.

An effective RSU-aided message (RAISE) scheme was proposed by Zhang *et al.* [21] based on K-anonymity method, authentication code, and hash message. Messages in the RAISE were checked by the RSU to provide low costs of communication and to maintain the privacy of the vehicle. The RAISE also assures that messages cannot be linked with an attack in the same vehicle. However, contextual privacy requirement is not met.

The VANET privacy enhancement communication schemes suggested by Chim *et al.* [22] defines a group communication protocol. A group of recognized vehicles can validate each other's signature without any other support of RSUs after simple handshaking to any RSU. For secure communication between group members, a typical group secret is established. The unlinkability of the message is also achieved; however, the remaining contextual requirements are ignored.

Shim [23] established an effective conditional privacy preservation scheme based on V2I communication architecture called CPAS. The proposed approach ensures a balance between privacy and traceability to achieve anonymity; however, the approach cannot provide unlinkability. As a result, conditional privacy and unobservability requirements are not fulfilled.

Recently, Alazzawi *et al.* [24] introduced a new robust pseudo identity privacy preservation based on the elliptic curve to achieve content privacy. This approach uses a pseudonym rather than a real identity to ensure privacy in VANET. The need for contextual privacy requirements is overlooked.

Under the same context, a new RSU-based security and privacy-preserving scheme was proposed by Bayat *et al.* [25]. In this method the RSUs are stored master keys in the tamper-proof device in the RSU. This approach assumes that drivers do not prefer (due to privacy concerns) being recognized and tracked by others. In addition, provided unlinkability because an adversary cannot connect a drivers to their transmitted message [25]. However, the unobservability property is overlooked in this scheme.

Based on the review of previous works, it is clear that contextual privacy requirement is not fully or partially fulfilled despite their importance in a VANET context. Moreover, the unobservability property is overlooked in these schemes. In order to meet these requirements, we propose VANET based privacy-preserving communication scheme that can address existing weaknesses in VANET schemes. More specifically, the contextual privacy requirements such as anonymity, unlinkability and unobservability are addressed in the proposed scheme. In addition, by using BAN logic and random oracle model, the proposed scheme resists the various types of attacks such as replay, impersonation, modification and man-in-middle. Thus, we design an effective VANET scheme that satisfies security and privacy requirements.

III. VEHICULAR SYSTEM ARCHITECTURE AND PRELIMINARIES

In the following parts, the necessary mathematical tools used in this study are introduced. Then, the model for vehicular communication and the adversary models are discussed. Finally, the security and privacy requirements for the proposed scheme are described. Table 1 contains some notation and their description.

TABLE 1. Notation and their description.

Notation	Descriptions
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∈ G
h_1, h_2, h_3	Three one-way hash function
RID_{RSU_j},RID_i	Real identity of the RSU and vehicle
PW_i	Password of driver
x_{pri}^{TA}, $s_{Pri}^{dom_i}$	The private master key of the system and $domain_i$
P_{Pub}^{TA}, $P_{Pub}^{dom_i}$	The public key of the TA and $domain_i$
r, z	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
R_1, L_1	Share secret key

A. MATHEMATICAL TOOLS REQUIREMENT

Miller [26] suggested ECC, an algorithm that is widely used to provide asymmetrical encryption in an elliptical curve. This algorithm has smaller key lengths than the same security level as other encryption algorithms.

Definition 1 (Elliptic Curve): Let F_p be a finite field, and a large prime number p is the order of F_p. E is an elliptic curve defined as: $y^2 = x^3 + ax + b \bmod p$. a, b $\in F_p$ are constants. A group G_q is defined on E, whose order is q and generator is P. The set contains an infinity point O.

- Scalar multiplication. Let P $\in Gq$, $n \in Z_q^*$, such that the scalar multiplication is x . P = P + P+P +P (x times).

Definition 2: Elliptic curve discrete logarithm problem (ECDLP): is computationally infeasible. E has two random

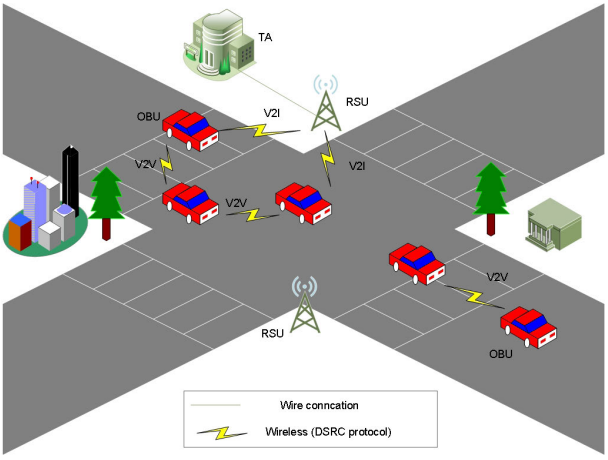

FIGURE 2. System model.

points P, Q from G, and Q = s.P. Computing s from Q in the polynomial time t is difficult.

B. SYSTEM MODEL

As illustrated in Figure 2, the proposed scheme consists of three entities: TA, RSU, and OBU. The three items are discussed below.

- TA
  TA is responsible for providing the principal parameter of RSUs and OBUs within its jurisdiction, with a reliable calculation and storage capacity. If false or malicious information is present in the system, then the TA can detect the actual identity of the information source. All entities consider TA be of absolute trust in the VANET system, and compromising TA is not feasible. TAs should be redundant to prevent a single point of failure or bottleneck caused by congestion.
- RSU
  An RSU is a stationary infrastructure distributed on the roadside. The RSU can communicates with OBU of the vehicle and TA through DSRC protocol and secure wired connections, respectively. The RSU can provide the driver with traffic-related conditions, such as traffic jams and accidents. Traffic-related messages from the signer, i.e. driver, can also be verified and forwarded to the TA or processed locally.
- OBU
  An OBU supporting the DSRC protocol is supplied to the vehicle. The OBU periodically transmits a traffic-related message about traffic statuses, such as speed, position and danger warning to the other OBU or RSU. Each OBU also has the public key of the system P_{Pub}^{TA}.

C. DESIGN GOALS

The following protection is the subject of this study, and the privacy objective should be met:

- Identity Privacy Preservation
  RSU, vehicles, and participants from third parties cannot extract the real vehicle identity from any traffic-related messages of the vehicle.
- Traceability
  The TA is the only party can extract a real vehicle identity if necessary (e.g., a complaint against a faulty vehicle).
- Unlinkability
  By linking some of the messaging signatures, the malicious vehicle or RSUs cannot successfully identify the anonymous entity.
- Unobservability
  A vehicle should be able to use a resource or service without being noticed in the use of support or service by others, particularly the third parties.
- Message Integrity and Authenticity
  Every vehicle message should be checked by RSUs and OBUs, and nodes should be allowed to detect any modifications or fabrications of the messages received.

IV. PROPOSED SCHEME

The proposed scheme has three phases: initialization, joining, and broadcasting. In this scheme, after TA generates the initial public parameters of the system, the TA calculates the private and public keys for the $domain_i$, which contains several registered RSUs from the registration list located nearby in a specific area (e.g.,city). The TA also stores the registered OBUs to the vehicle registration list.

In the second phase, after the OBU produces n pseudo ID list with its real identity and public TA parameters, the vehicle must establish a shared authentication with the nearest RSU in any domain to begin transmission and validate operations. Then, the TA will confirm the authenticity of the OBU via the private key of the system. Thereafter, the RSU generates a list of signatures that can be used in the selected timestamp, and then sends them securely to the OBU. n is a level of security anonymity, that is, the number of pseudo identities that a vehicle may unrepeatable in a region enclosed by the RSU [27]. Finally, the OBU uses the signature list until the time list expires. Figure 3 briefly describes the proposed scheme phases. The following subsection explains three phases in detail.

A. INITIALIZATION PHASE

During this phase, the TA creates system parameters to use the following steps:

- The TA selects two large prime numbers p, q and a non-singular elliptic curve E defined by the equation $y^2 = x^3 + ax + b \bmod p$, where a, b $\in F_p$.
- The TA selects a generator P with order q of the group G, which includes all points on the elliptic curve E and the point at infinity O.

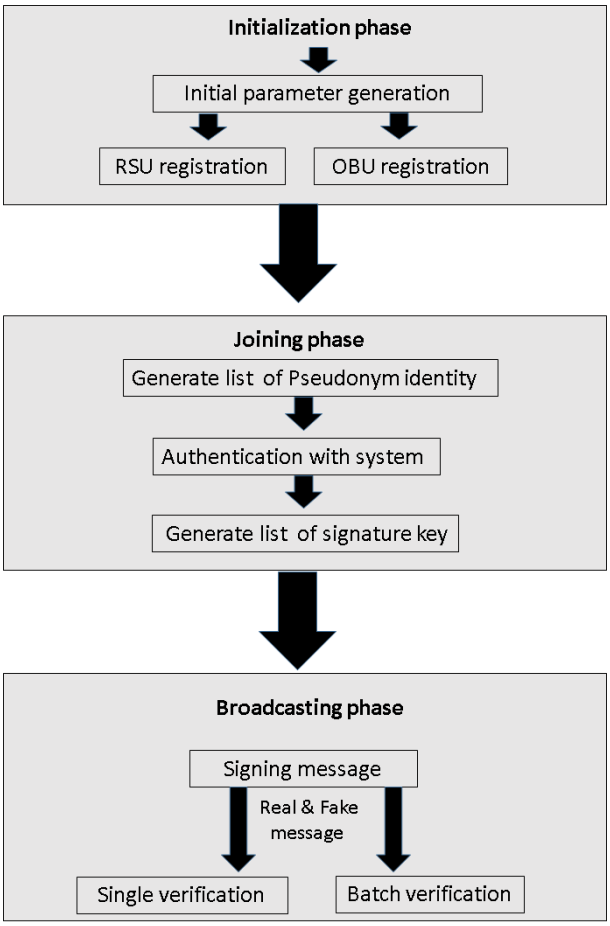

FIGURE 3. Proposed scheme architecture.

- The TA chooses a number $x_{Pri}^{TA} \in Z_q^*$ at random as the private key and computes $P_{Pub}^{TA} = x_{Pri}^{TA}$. P as its corresponding public key.
- Three secure cryptographic hash functions are selected by TA, $h_1 : G \rightarrow Z_q^*$, $h_2 : \{0, 1\}^* \times \{0, 1\}^* \times G \rightarrow Z_q^*$, $h_3 : \{0, 1\}^* \rightarrow Z_q^*$.

1) ROADSIDE UNIT REGISTRATION

The RSU registers with the TA as follows.

- The TA chooses the number of RSUs located in a specific area as $domain_i$.
- The TA randomly selects numbers $s_{Pri}^{dom_i} \in Z_q^*$ as a private key for all RSUs in $domain_i$ and calculates $P_{Pub}^{dom_i} = s_{Pri}^{dom_i}$.P as its related public key.
- The TA saves the private key $s_{Pri}^{dom_i}$ on all RSUs in the $domain_i$
- The TA preloads the public parameters parmas = $\{p, q,$ a, b, P, $P_{Pub}^{TA}, h_1, h_2, h_3\}$ in each RSU.
- The RSU_j familiar with $domain_i$ periodically broadcasts its public key $P_{Pub}^{dom_i}$ obtained from TA.

2) ONBOARD UNIT REGISTRATION

The vehicle registers with the TA as follows.

- By using the 4G/5G technology, the driver sends the registration request to TA with the messages $ENC_{P_{Pub}^{TA}}$ (RID_i, PW_i), where RID_i refers to its real identity and PW_i refers to its password.
- TA decrypts receiving message $DEC_{x_{Pri}^{TA}}(RID_i, PW_i)$. Then, after the validity of the RID_i is checked, TA preloads the public parameters parmas = $\{p, q,$ a, b, P, $h_1, h_2, h_3\}$ in each OBU.

B. JOINING PHASE

$domain_i$-based RSU category refers to that the exchange of data based on RSU parameters should be authenticated to that VANET system when a vehicle reaches an RSU coverage area. When an OBU arrives at the coverage area of a new domain or its pseudo IDs are disabled, it has to enter the RSU group and is issued with an RSU signing key. The process of joining the OBU is described with the RSU group in Figure 4. After arriving at RSU_j coverage area, the OBU_i takes the following steps to complete the joining phase:

- The OBU_j chooses n randoms $r_l \in Z_q^*$, $l = 1$: n, and family of unlinkable pseudo IDs is calculated: $L_{PID_i} = \{ PID_{i1},\ldots,PID_{in} \}$ as follows.

$$\begin{aligned} PID_{il} &= \{PID_{il}^1, PID_{il}^2\} \\ PID_{il}^1 &= r_l P \\ R_l &= r_l P_{Pub}^{TA} \\ PID_{il}^2 &= RID_i \oplus h_1(R_l) \end{aligned}$$

  where, $l = 1, 2,\ldots,$n.
- The OBU computes $ENC_{L_{PID_i}} = HMAC_{R_1}(L_{PID_i} \| T_1)$, where $R_1 = r_1 P_{Pub}^{TA}$ as the shared secret key. It sends $\{ENC_{L_{PID_i}}, PID_{i1}^1, PID_{i1}^2, T_1, \sigma_{Auth}^{OBU_i}\}$, where $\sigma_{Auth}^{OBU_i} = h_3(ENC_{L_{PID_i}} \| PID_{i1}^1 \| PID_{i1}^2 \| T_1)$ to the nearby RSU_j.
- After the RSU_j receives $\{ENC_{L_{PID_i}}, PID_{i1}^1, PID_{i1}^2, T_1, \sigma_{Auth}^{OBU_i}\}$ checks the validity of timestamp T_1. Each timestamp T is tested as follows: assume T_{Δ}^{delay} is the time delay estimation, and T_r is the receiving time. If $(T_{\Delta}^{delay} > Tr$ - T). If not, then it is not fresh. Otherwise, the message is accepted, and RSU checks whether $\sigma_{Auth}^{OBU_i} = ?h_3(ENC_{L_{PID_i}} \| PID_{i1}^1 \| PID_{i1}^2 \| T_1)$. If not, then RSU does not accept the message; otherwise, it chooses $z_j \in Z_q^*$ and computes:

$$\begin{aligned} PID_{RSU_j}^1 &= z_j P \\ L_j &= z_j P_{Pub}^{TA} \\ PID_{RSU_j}^2 &= RID_{RSU_j} \oplus h_1(L_j) \end{aligned}$$

  Finally, it sends $\{PID_{RSU_j}^1, PID_{RSU_j}^2, T_2, PID_{i1}^1, PID_{i1}^2\}$ to TA.
- After the message $\{PID_{RSU_j}^1, PID_{RSU_j}^2, T_2, PID_{i1}^1, PID_{i1}^2\}$ is send to the TA, it checks the validity of timestamp T_2.

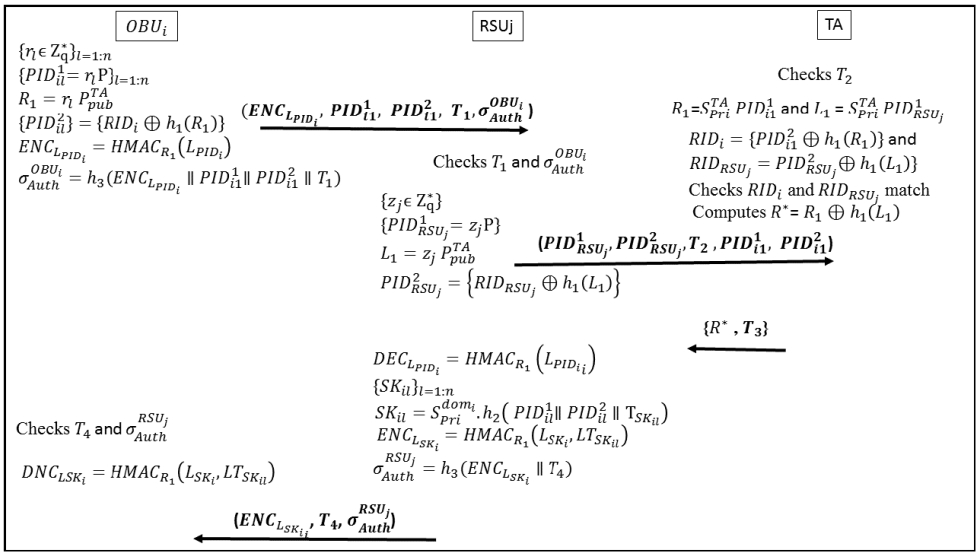

FIGURE 4. OBU joining to RSU phase.

By using private key (x_{Pri}^{TA}), the TA computes $L_j = x_{Pri}^{TA} PID_{RSU_j}^1$ and $R_1 = x_{Pri}^{TA} PID_{i1}^1$ to extracts the RID_{RSU_j} and RID_i, respectively as follows: $RID_{RSU_j} = PID_{RSU_j}^2 \oplus h_1(L_j)$ and $RID_i = PID_{i1}^2 \oplus h_1(R_1)$. Then, the TA checks whether RID_{RSU_j} and RID_i matches the stored value in the RSU registration list and vehicle registration list, respectively. If not, then the TA does not accept the message; Otherwise, TA sends $\{R*, T_3\}$ to TA, where $R* = R_1 \oplus h_1(L_j)$.

- Once the message $\{R*, T_3\}$ is received by the RSU, it checks the validity of timestamp T_3 and extracts $R_1 = R* \oplus h_1(L_j)$. Then RSU_j decrypts the list by using R_1 as $DEC_{L_{PID_i}} = HMAC_{R_1}(L_{PID_i} \| T_1)$ and prepares the $L_{SK_{il}}$ signature list with expiry time list $T_{SK_{il}}$ for the vehicle as follows and organizes $L_{SK_{il}}$ $\{SK_{i1}, \ldots, SK_{in}\}$ For each pseudo ID in L_{PID_i}, $l = 1{:}n$:

$$SK_{il}^1 = s_{Pri}^{dom_i} . h_2(PID_{il}^1 \| PID_{il}^2) \| T_{SK_{il}}).$$

Finally, it sends $\{ENC_{L_{SK_{il}}}, T_4, \sigma_{Auth}^{RSU_j}\}$ to OBU_i, where $ENC_{L_{SK_{il}}} = HMAC_{R_1}(L_{SK_{il}} \| T_{SK_{il}})$ and $\sigma_{Auth}^{RSU_j} = h_2(ENC_{L_{SK_{il}}} \| T_4 \| R_1)$.

- As the message $\{ENC_{L_{SK_{il}}}, T_4, \sigma_{Auth}^{RSU_j}\}$ is received, OBU_i checks the validity of T_4. If the timestamp is valid, then OBU_i verifies whether $\sigma_{Auth}^{RSU_j} = h_2(ENC_{L_{SK_{il}}} \| T_4 \| R_1)$. If not, OBU_i does not accept the message; otherwise, OBU_i decrypts the message $(ENC_{L_{SK_{il}}})$ by (R_1) to obtain the list of signature keys with list of expiration time $T_{SK_{il}}$ as $DEC_{L_{SK_{il}}} = HMAC_{R_1}(L_{SK_{il}} \| T_{SK_{il}})$. Now the OBU_i has a list of n signature keys, and pseudo ID that allows it to sign messages in an anonymity timestamp T_j in the RSU_j coverage area.

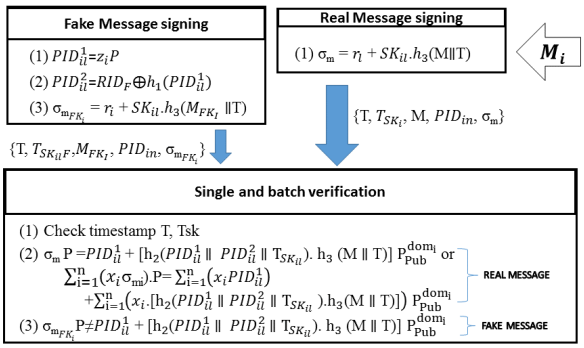

FIGURE 5. Message broadcasting procedure.

C. BROADCASTING PHASE

This phase involves two sub phases to sign and verify the message, as shown in Figure 5. These sub phases are explained in detail below.

1) MESSAGE SIGNING

If OBU_i wants a real message M_i to be signed, then the following steps must be executed, where T_i is the timestamp:

- $OBUi$ randomly selects a pseudo ID PID_i from the $L_{PID_{il}}$ list and obtains the corresponding private key sk_i from the $L_{SK_{il}}$ list.
- OBU_i signs the following message M_i: $\sigma_m = r_l + SK_{il}.h_3(M_i \| T)$
- OBU_i broadcasts the traffic-related message. $\{T, T_{SK_{il}}, M_i, PID_{in}, \sigma_m\}$ to the nearest RSU or another OBU.

To avoid the nodes from being observed by the attacker, the OBU_i injects a fake message M_{FK_i} during the broadcasting, then the following steps must be conducted:

- $z_i \in Z_q^*$ is chosen, and $PID_{il}^1 = z_i.P$, $PID_{il}^2 = RID_F \oplus h_1(PID_{il}^1)$ is computed, where RID_F is the fake real identity.
- The OBU computes the message signature $\sigma_{M_{FK_i}} = h_1(M_{FK_i}||PID_{il}^2||PID_{il}^1||T_i)$.
- The OBU broadcasts the fake message $\{T, T_{SK_{ilF}}, M_{FK_i}, PID_{in}, \sigma_{M_{FK_i}}\}$ periodically.

2) VERIFICATION

- Real Message:

The real message $\{T, T_{SK_{il}}, M_i, PID_{in}, \sigma_m\}$ is received once the RSU or one OBU checks the validity of the time stamps [T,$T_{SK_{il}}$]. If so, then one of the following is used to test the traffic-related message.

After the RSU or one OBU receives the real message $\{T, T_{SK_{il}}, M_i, PID_{in}, \sigma_m\}$. the validity of the timestamps [T,$T_{SK_{il}}$] is verified. If so, one of the following is used to verify the traffic-related message.

a: SINGLE VERIFICATION

The verifier (RSU or OBU) uses the following equation to verify the single traffic-related message.

$$\sigma_{M_i}P = PID_{il}^1 + [h_2(PID_{il}^1 \| PID_{il}^2 \| T_{SK_{il}})h_3(M_i \| T)]P_{Pub}^{dom_i} \quad (1)$$

The recipient rejects all traffic-related messages in case of Equation (1). Otherwise, the signature is valid, the transmitter is legal, and the recipient accepts the traffic-related message.

b: BATCH VERIFICATION

A batch validation approach is used in the proposed scheme to reduce the time spent in receiving a large number of traffic-related messages. We use a technique called the little test of exponents [28], [29] to satisfy the non-repudiation requirement. The verifier generates a random integer vector $x = \{x_1, x_2, \ldots, x_n\}$, where $x_i \in 2[1, 2^t]$and t is a small integer number, that does not increase the cost of computation. The following equation is used to verify traffic-related messages.

$$(\sum_{i=1}^{n}(x_i\sigma_{m,i}).P = (\sum_{i=1}^{n} x_i h_2([h_2(PID_{il}^1 \| PID_{il}^2 \| T_{SK_{il}} h_3(M_i \| T)])) + \sum_{i=1}^{n}(PID_{il}^1) \quad (2)$$

The recipient accepts all messages in the case of Equation (2). Otherwise, these vehicles contain at least one illegal vehicle. The illegal vehicle detection, which is a new algorithm proposed in [30], is adopted. The reader can refer to [30] for additional details.

- Fake Message:

If the RSU or one OBU receives the fake message $\{T, T_{SK_{ilF}}, M_{FK_i}, PID_{in}, \sigma_{M_{FK_i}}\}$,then the traffic-related message continues to be verified by:

$$\sigma_{M_{FK_i}}P \neq PID_{il}^1 + [h_2(PID_{il}^1 \| PID_{il}^2 \| T_{SK_{il}})h_3(M_i \| T)]P_{Pub}^{dom_i}. \quad (3)$$

When Equation (3) holds, signatures will not be valid, and the transmitters will be an illegal or fake message.

V. SECURITY ANALYSIS

A security analysis of the proposed scheme is provided in this section to clarify that our scheme is secure under a Burrows–Abadi–Needham (BAN) logic, random oracle model and proof of security. We also provide the requirements for security and privacy in this paper.

A. FORMAL VALIDATION

1) BAN-BASED FORMAL VALIDATION

To verify the legitimacy of both OBU and RSU, the proposed scheme uses a widely accepted tool BAN logic achieving the certain security goals for the mutual authentication and key agreement [31].

The following are the primary notations and meanings of BAN logic:

- S, R : The main participants in the proposed.
- X_m : Messages.
- SK : A shared key.
- $S| \equiv R$: S believes R.
- $S| \triangleleft X_m$: S sees X_m.
- $S| \sim X_m$: S sent X_m.
- $\#(X_m)$: Messages X_m are fresh.
- $S \overset{SK}{\longleftrightarrow} R$: S and R communicate by SK.
- $| \overset{\text{Pub}}{\longrightarrow} R$: R has a public key Pub corresponding to a private key Pri.
- $S \Rightarrow R$: S has the ability to control R.
- $(X_m)_{SK}$: The message X_m is hashing by SK.

Besides these, the main rules of BAN logic process are follows:

- $Message - meaning$: $\frac{S| \equiv S \overset{\text{SK}}{\longleftrightarrow} R, S \triangleleft (X_m)_{SK}}{S| \equiv R| \sim X_m}$, $\frac{S| \equiv S \rightarrow \text{Pub} R, S \triangleleft (X_m)_{Pub^-}}{S| \equiv R| \sim X_m}$.
- $Freshness$: $\frac{S| \equiv \#(X_m)}{S| \equiv \#(X_m, Y_m)}$.
- $Nonce - verification$: $\frac{S| \equiv \#(X_m), S| \equiv R| \sim X_m}{S| \equiv R| \equiv X_m}$.
- $Jurisdiction$: $\frac{S| \equiv R \Rightarrow (X_m), S| \equiv R \equiv X_m}{S| \equiv X_m}$.

a: SECURITY GOALS

The goal of this process is to authenticate the session key between OBU and RSU. Therefore, the proposed scheme need to achieve the following seven primary goals.

- **SG 1.** $TA| \equiv OBU| \equiv (R_1, RID_i)$.
- **SG 2.** $TA| \equiv (R_1, RID_i)$.
- **SG 3.** $TA| \equiv RSU| \equiv (L_J, RID_{RSU_j})$.

- **SG 4.** $TA| \equiv (L_J, RID_{RSU_j})$.
- **SG 5.** $RSU| \equiv (RSU \overset{R_1}{\longleftrightarrow} OBU)$.
- **SG 6.** $OBU| \equiv RSU \equiv (L_{PID_i})_{h(R_1)}$.
- **SG 7.** $OBU| \equiv (L_{SK_{il}})_{h(L_J)}$.

b: IDEALIZE THE SCHEME PHASE

- The messages for the scheme are:
  - **MS 1.** $OBU \rightarrow RSU : \{ENC_{L_{PID_i}}, PID^1_{i1}, PID^2_{i1}, T_1, \sigma^{OBU_i}_{Auth}\}$.
  - **MS 2.** $RSU \rightarrow TA : \{RID_{RSU_j}, T_2, PID^1_{il}, PID^2_{il}\}$.
  - **MS 3.** $TA \rightarrow RSU : \{Checked, R_1, T_3\}$.
  - **MS 4.** $RSU \rightarrow OBU : \{ENC_{L_{SK_{il}}}, T_4, \sigma^{RSU_j}_{Auth}\}$.
- The messages for the scheme are idealized as follows:
  - **MSI 1.** $OBU \rightarrow TA : (R_1, RID_i)_{h(P^{TA}_{Pub})}$.
  - **MSI 2.** $RSU \rightarrow TA : (L_j, RID_{RSU_j})_{h(P^{TA}_{Pub})}$.
  - **MSI 3.** $TA \rightarrow RAU : (RAU \overset{R_1}{\longleftrightarrow} OBU)_{h(L_j)}$.
  - **MSI 4.** $RSU \rightarrow OBU : (L_{SK_{il}})_{h(L_j)}$.

c: SUPPOSITIONS

The following Suppositions about the initial state of the proposed scheme as follows:

- **Sup 1.** $RSU| \equiv \#(T_1, T_3)$.
- **Sup 2.** $TA| \equiv \#(T_2)$.
- **Sup 3.** $OBU| \equiv \#(T_4)$.
- **Sup 4.** $TA| \equiv | \overset{P^{TA}_{pub}}{\longrightarrow} OBU$.
- **Sup 5.** $TA| \equiv | \overset{P^{TA}_{pub}}{\longrightarrow} RSU$.
- **Sup 6.** $RSU| \equiv TA \Rightarrow RSU \overset{R_1}{\longleftrightarrow} OBU$.
- **Sup 7.** $OBU| \equiv RSU \overset{R_1}{\longleftrightarrow} OBU$.
- **Sup 8.** $TA| \equiv OBU \Rightarrow (RID_i)$.
- **Sup 9.** $TA| \equiv RSU \Rightarrow (RID_{RSU_j})$.
- **Sup 10.** $RSU| \equiv RSU \overset{L_j}{\longleftrightarrow} TA$.
- **Sup 11.** $RSU| \equiv TA \rightarrow (RSU \overset{R_1}{\longleftrightarrow} OBU)$.
- **Sup 12.** $OBU| \equiv RSU| \Rightarrow (L_{SK_{il}})$.

Proof: We will proof that the proposed scheme achieves the above seven security objectives (Goal 1, Goal 2, Goal 3, Goal 4, Goal 5, Goal 6 and Goal 7) as follows.

From **MSI 1.**, we deduce:

AS1: $TA \triangleleft (R_1, RID_i)_{h(P^{TA}_{Pub})}$

From **AS1, Sup 5**, and by utilizing **message meaning rule**, we deduce:

AS2: $TA| \equiv OBU| \sim (R_1, RID_i)$

From **AS2, Sup 2**, and by utilizing **rule of freshness and nonce-verification**, we deduce:

AS3: $TA| \equiv OBU| \equiv (R_1, RID_i)$ Therefore, security goal 1 is achieved.

From **AS3, Sup 8**, and by utilizing **jurisdiction rule**, we deduce:

AS4: $OBU| \equiv (R_1, RID_i)$ Therefore, security goal 2 is achieved.

From **MSI 2.**, we deduce:

AS5: $TA \triangleleft (L_j, RID_{RSU_j})_{h(P^{TA}_{Pub})}$

From **AS5, Sup 5**, and by utilizing **message meaning rule**, we deduce:

AS6: $TA| \equiv OBU| \sim (L_j, RID_{RSU_j})$

From **AS6, Sup 2**, and by utilizing **rule of freshness and nonce-verification**, we deduce:

AS7: $TA| \equiv OBU| \equiv (L_j, RID_{RSU_j})$ Therefore, security goal 3 is achieved.

From **AS7, Sup 8**, and by utilizing **jurisdiction rule**, we deduce:

AS8: $OBU| \equiv (L_j, RID_{RSU_j})$ Therefore, security goal 4 is achieved.

From **MSI 3.**, we deduce:

AS9: $RSU \triangleleft (RSU \overset{R_1}{\longleftrightarrow} OBU)$ From **AS9, Sup 10**, and by utilizing **message meaning rule**, we deduce:

AS10: $RSU| \equiv TA| \sim (RSU \overset{R_1}{\longleftrightarrow} OBU)$

From **AS10, Sup 1**, and by utilizing **rule of freshness and nonce-verification**, we deduce:

AS11: $RSU| \equiv TA| \equiv (RSU \overset{R_1}{\longleftrightarrow} OBU)$

From **AS11, Sup 11**, and by utilizing **jurisdiction rule**, we deduce:

AS12: $RSU| \equiv (RSU \overset{R_1}{\longleftrightarrow} OBU)$ Therefore, security goal 5 is achieved.

From **MSI 4.**, we deduce:

AS13: $OBU \triangleleft (L_{SK_{il}})_{h(R_1)}$

From **AS13, Sup 7**, and by utilizing **message meaning rule**, we deduce:

AS14: $OBU| \equiv RSU| \sim (L_{SK_{il}})$

From **AS14, Sup 3**, and by utilizing **rule of freshness and nonce-verification**, we deduce:

AS15: $OBU| \equiv RSU| \equiv (L_{SK_{il}})$ Therefore, Goal 6 is achieved.

From **AS15, Sup 12**, and by utilizing **rule of jurisdiction**, we deduce:

AS16: $OBU| \equiv (L_{SK_{il}})$ Therefore, Goal 7 is achieved.

As a result, Goal 1, Goal 2, Goal 3, Goal 4, Goal 5, Goal 6 and Goal 7 collectively guarantee the mutual authentication between nodes of the proposed scheme in VANETs.

2) RANDOM ORACLE MODEL-BASED VALIDATION

We set up a game between challenger A and attacker B, where A is the proposed scheme and B is the one that can undermine the security of the proposed scheme.

Theorem 2: The proposed scheme against an adaptive chosen message attack behind the random oracle model is existentially unforgeable

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

Setup: A generates the system private key and establishes system parameters params $= \{p, q, a, b, P, P^{TA}_{Pub}, h_1, h_2, h_3\}$ and then builds and holds three lists, namely, $LIST_{h1}$ with $(\alpha, \tau h_1)$form, $LIST_{h2}$ with $(PID^1_{il}, PID^2_{il}, \tau h_2)$form and

$LIST_{h3}$ with (M_i, T, τh_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 (α, τh_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 ((α, τh_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, $T_{sk_{il}}$, τh_2)) is in $LIST_{h2}$. If so, then, A transmits $\tau h_2 = h(PID_{il}^1, PID_{il}^2, T_{sk_{il}})$ to B. Otherwise, A randomly chooses$\tau h_2 \in Z_q^*$and appends (PID_{il}^1, PID_{il}^2, $T_{sk_{il}}$, τh_2) into $LIST_{h2}$. Then, A transmits $\tau h_2 = h((PID_{il}^1 \| PID_{il}^2 \| T_{sk_{il}})$ to B.

$LIST_{h3}$-Oracle: After A receives a B message request with (M_i, T), it initially verifies if tuple (Mi, T, τh_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, τh_2) into $LIST_{h3}$. Then, A transmits $\tau h_3 = h(M_i \| T)$ to B.

Sign-Oracle: Upon receiving an A sign request from B via message m, it generates $h_{i,2}, h_{i,3}, \sigma_m \in Z_q^*$, $PID_{il}^2 \in G$. A randomly and computes $PID_{il}^1 = (\sigma_i P - h_{i,2}h_{i,3}P_{Pub}^{dom_i})$. A adds the (PID_{il}^1, PID_{il}^2, τh_2)into $LIST_{h2}$ and (M_i, T, τh_3) into $LIST_{h3}$. Finally, A transmits traffic-related message $\{T, T_{SK_{il}}, M_i, PID_{in}, \sigma_m\}$ to B. The Sign-Oracle answer is valid because the message $\{T, T_{SK_{il}}, M_i, PID_{in}, \sigma_m\}$ complies with Equation (2):

$$\begin{aligned}\sigma_m P &= PID_{il}^1 + h_{i,2}h_{i,3}P_{Pub}^{dom_i} \\ &= h_{i,2}h_{i,3}P_{Pub}^{dom_i} + (\sigma_m P - h_{i,2}h_{i,3}P_{Pub}^{dom_i}) = \sigma_m P \quad (4)\end{aligned}$$

Output: A ends up with a traffic-related message $\{T, T_{SK_{il}}, M_i, PID_{in}, \sigma_m\}$. A verifies this message using the following equation:

$$\sigma_m P = PID_{il}^1 + h_{i,2}h_{i,3}P_{Pub}^{dom_i}. \quad (5)$$

A completes the game if this equation does not hold.

According to the forgery lemma in [32], B can output another legitimate signature message $\{T, T_{SK_{il}}, M_i, PID_{in}, \sigma_m^*\}$. Thus, the following equation is obtained:

$$\sigma_m^* P = PID_{il}^1 + h_{i,2}^* h_{i,3}^* P_{Pub}^{dom_i}. \quad (6)$$

From the two equations above, we can deduce

$$\begin{aligned}(\sigma_m - \sigma_m^*)P &= \sigma_m P - \sigma_m^* P \\ &= PID_{il}^1 + h_{i,2}h_{i,3}P_{Pub}^{dom_i} \\ &\quad -(PID_{il}^1 + h_{i,2}^* h_{i,3}^* P_{Pub}^{dom_i}) \\ &= (h_{i,2}h_{i,3}P_{Pub}^{dom_i} - h_{i,2}^* h_{i,3}^* P_{Pub}^{dom_i}) \\ (h_{i,2}h_{i,3} - h_{i,2}^* h_{i,3}^*)P_{Pub}^{dom_i} &= (h_{i,2}h_{i,3} - h_{i,2}^* h_{i,3}^*)s_{Pri}^{dom_i} P \quad (7)\end{aligned}$$

Then, we can obtain$(\sigma_m - \sigma_m^*) = (h_{i,2}h_{i,3})s_{Pri}^{dom_i} \bmod p$.

B outputs s = $(\sigma_m - \sigma_m^*) = (h_{i,2}h_{i,3} - h_{i,2}^* h_{i,3}^*)^{-1}$

Therefore, the proposed scheme is resistant to the chosen adaptive message attacks in the random oracle model under the assumption that ECDLP is hard.

3) SECURITY OF PROOF

Theorem 1: A correct equation is present in the proposed scheme.

Proof of Equation (1): The recipient verifies the traffic-related message with Equation (1) in the single verification.

$$\begin{aligned}&L.H.S.\sigma_m P \\ &= (r_l + SK_{il}.h_3(M_i \| T))P \\ &= (r_l + s_{Pri}^{dom_i}.h_2(PID_{il}^1 \| PID_{il}^2) \| T_{SK_{il}}).h_3(M_i \| T))P \\ &= r_l.P + h_2(PID_{il}^1 \| PID_{il}^2) \| T_{SK_{il}}).h_3(M_i \| T)s_{Pri}^{dom_i}.P \\ &= PID_{il}^1 + [h_2(PID_{il}^1 \| PID_{il}^2 \| T_{SK_{il}})h_3(M_i \| T)]P_{Pub}^{dom_i} \\ &= R.H.S.\end{aligned}$$

Therefore, Equation (1) is accurately verified.

The Proof of Equation (2): The verifier tests the traffic-related messages with Equation (2) in the batch verification.

$$\begin{aligned}&L.H.S\left(\sum_{i=1}^{n}(x_i\sigma_{m,i})\right).P \\ &= \left(\sum_{i=1}^{n}\left(x_i(r_l + SK_{il}.h_3(M_i \| T)\right)\right).P \\ &= \left(\sum_{i=1}^{n}\left(x_i\left(r_l + s_{Pri}^{dom_i}.h_2(PID_{il}^1 \| PID_{il}^2) \| T_{SK_{il}}\right)\right.\right. \\ &\quad \left.\left.h_3(M_i \| T)\right)\right).P \\ &= \left(\sum_{i=1}^{n}\left(x_i r_l.P + x_i h_2(PID_{il}^1 \| PID_{il}^2) \| T_{SK_{il}}\right)\right. \\ &\quad \left.h_3(M_i \| T)s_{Pri}^{dom_i}.P\right) \\ &= \left(\sum_{i=1}^{n}x_i.PID_{il}^1\right) + \left(\sum_{i=1}^{n}\left(x_i h_2(PID_{il}^1 \| PID_{il}^2) \| T_{SK_{il}}\right.\right. \\ &\quad \left.\left.h_3(M_i \| T)\right).P_{Pub}^{dom_i}\right) \\ &= R.H.S.\end{aligned}$$

Therefore, Equation (2) is confirmed to be correct.

The Proof of Equation (3): The verifier checks traffic-related messages that use Equation (3) in a falsified message.

$$L.H.S.\sigma_{M_{FK_i}} P = h_1(M_{FK_i} || PID_{il}^2 || PID_{il}^1 || T_i)P$$

where,

$$\begin{aligned}\sigma_{M_{FK_i}} P &\neq \sigma_m P \\ h_1(M_{FK_i} || PID_{il}^2 || PID_{il}^1 || T_i)P &\neq PID_{il}^1 + [h_2(PID_{il}^1 \| PID_{il}^2 \| \\ &\quad T_{SK_{il}})h_3(M_i \| T)]P_{Pub}^{dom_i} \\ &\neq R.H.S.\end{aligned}$$

Therefore, Equation (3) is confirmed to be correct.

B. SECURITY ATTRIBUTES

This section shows that the proposed VPPCS scheme can satisfy the security and privacy requirements for vehicular communication mentioned in subsection design goals.

1) 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.

2) TRACEABILITY

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, proposed scheme provides a traceability function.

3) UNLINKABILITY

During the message signing period, an anonymous 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 VPPCS scheme also uses a current timestamp to calculate the signature. Any adversary who attempts to link two or more traffic-related messages may not succeed because of changes in their anonymous identity and timestamp 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.

4) UNOBSERVABILITY

Given that every vehicle real traffic and transmits probabilistically, global adversaries can only observe several transmissions and cannot distinguish the real traffic-related message from any vehicles. Furthermore, they cannot distinguish between real traffic and noise because false messages are injected randomly. Thus, unobservability occurs, which strengthens the anonymity of the vehicle.

5) MESSAGE INTEGRITY AND AUTHENTICITY

We show in accordance with theorem 1 that an adversary cannot trump up valid traffic-related message in our proposed scheme, and recipients can verify that the message $\{T, T_{SK_{il}}, M_i, PID_{in}, \sigma_m\}$ has integrity and legality by verifying whether the equation $\sigma_{M_i} P = PID_{il}^1 + [h_2(PID_{il}^1 \| PID_{il}^2 \| T_{SK_{il}}) h_3(M_i \| T)] P_{Pub}^{dom_i}$ holds. Therefore, the integrity and authenticity of the proposed scheme VANET scheme are provided.

6) RESISTANCE TO VARIOUS TYPES OF ATTACKS

- **Resistance to Replay Attack:**
  The timestamps T in the traffic-related message $\{T, T_{SK_{il}}, M_i, PID_{in}, \sigma_m\}$. After the recipient receives the message M_i, it first verifies whether the inequality $(T_{\Delta}^{delay} > Tr - \mathrm{T})$ hold. If it's fresh, the recipient accepts the message M_i to be verified further; otherwise, the message does not accept. In addition, according to traffic-related message $\{T, T_{SK_{il}}, M_i, PID_{in}, \sigma_m\}$, where $\sigma_m = r_l + SK_{il}.h_3(M_i \| T)$ and $SK_{il} = s_{Pri}^{dom_i}.h_2(PID_{il} \| PID_{il}) \| T_{SK_{il}})$. Thus, another timestamp cannot be used by attacker because this attack results in different values of σ_m. In these procedure, replay of message M_i in VANETs system is detected. Therefore, this proposed VPPCS scheme can resist replay attacks.
- **Resistance to Impersonation Attack:**
  According to the Theorem 2, the attacker cannot impersonate a valid traffic-related message $\{T, T_{SK_{il}}, M_i, PID_{in}, \sigma_m\}$ in the proposed VPPCS scheme. This is because the verifying recipients can verifies the authenticity of the tuple $\{T, T_{SK_{il}}, M_i, PID_{in}, \sigma_m\}$ by checking whether the equation $\sigma_{M_i} P = PID_{il}^1 + [h_2(PID_{il}^1 \| PID_{il}^2 \| T_{SK_{il}}) h_3(M_i \| T)] P_{Pub}^{dom_i}$ holds. If ok, the recipients accept the traffic-related message; otherwise, it does not accept it. The impersonation attack in the proposed VPPCS scheme is therefore ineffective.
- **Resistance to Modification Attack:**
  The adversary cannot easily tamper and modify a legal traffic-related message $\{T, T_{SK_{il}}, M_i, PID_{in}, \sigma_m\}$to $\{T, T_{SK_{il}}, M_i^*, PID_{in}, \sigma_m^*\}$, where $\sigma_i = \left(r_i + s_{Pri}^{dom_i} h_3 (M_i^* \| PID_{il}^1 \| PID_{il}^2 \| T_{SK_{il}})\right)$. The real identity of a vehicle $\{T, T_{SK_{il}}, M_i, PID_{in},$
  $\sigma_m\}$ is unknown. The VPPCS scheme can therefore resist the modification attack.
- **Resistance to Man-in-the-Middle Attack:**
  The study of message validity and authenticity above proves that it is necessary to check the relation between the sender and the verifier should be checked and that a genuine message cannot be changed and fabricated. Our proposed VPPCS scheme can thus be resisted by a man-in-the-middle attack.

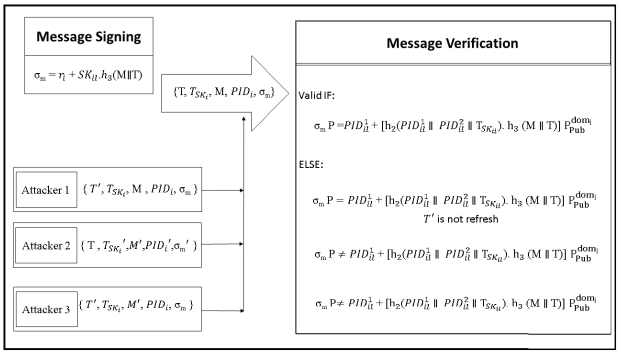

FIGURE 6. Process of system resisting attacks.

In Figure 6, we demonstrate the resistance of the system to three attacks. Attacker 1 can collect legal signatures and conduct replay attacks. Attacker 2 can impersonate a legitimate signature, and Attacker 3 can modify and tamper legal

TABLE 2. Cost of computation comparison.

schemes	MGS(ms)	SVM(ms)	$BVMM$(ms)
[17]	$1T_{ecc}^{sm} + 2T_h + 2T_{ecc}^{pa} \approx 0.6800$	$4T_{ecc}^{sm} + 3T_h \approx 2.6902$	$(4n)T_{ecc}^{sm} + (3n)T_h \approx 2.6902$n
[18]	$3T_{ecc}^{sm} + 3T_h \approx 2.0174$	$4T_{ecc}^{sm} + 3T_h + 2T_{ecc}^{pa} \approx 2.6964$	$(n+2)T_{ecc}^{sm} + (2n)T_{ecc}^{sm-s} + (2n-2)T_{ecc}^{pa} + (3n)T_h \approx 1.4858$n+1.3436
[20]	$3T_{bp}^{sm} + 2T_{mtp} \approx 13.041$	$4T_{bp} + 1T_{bp}^{sm} + 1T_{mtp} \approx 28.9818$	-
[22]	$3T_{bp}^{sm} + 1T_h + 2T_{bp}^{pa} \approx 4.7184$	$3T_{bp} + 2T_{bp}^{sm} + 2T_h + 1T_{bp}^{pa} \approx 23.5638$	$3T_{bp} + (n+1)T_{bp}^{sm} + (3n-3)T_{bp}^{pa} + 2nT_h \approx 3.5972$ n + 18.9666
[23]	$2T_{bp} + 6T_{bp}^{sm} + 1T_{mtp} + 4T_h + 2T_{bp}^{pa} \approx 22.0396$	$3T_{bp} + 2T_{bp}^{sm} + 3T_h + 1T_{bp}^{pa} \approx 23.5744$	$3T_{bp} + (n+1)T_{bp}^{sm} + 2nT_{bp}^{sm-s} + (3n-2)T_{bp}^{pa} + 3nT_h \approx 18.9772$ +4.9342 n
[24]	$1T_{ecc}^{sm} + 2T_h \approx 0.6728$	$2T_{ecc}^{sm} + 1T_h + 1T_{ecc}^{pa} \approx 1.3477$	$(2n+2)T_{ecc}^{sm} + (2n)T_{ecc}^{sm-s} + (2n)T_{ecc}^{pa} + (n)T_h \approx 1.4828$n + 1.3436
[25]	$1T_{mtp} \approx 4.1724$	$3T_{bp} + 1T_{bp}^{sm} + 1T_{mtp} \approx 23.1708$	$3T_{bp} + nT_{bp}^{sm} + nT_{mtp} \approx 5.7378$n+17.4333
VPPCS	$1T_{ecc}^{sm} + 3T_h \approx 0.6748$	$2T_{ecc}^{sm} + 2T_h + 1T_{ecc}^{pa} \approx 1.3487$	$(2)T_{ecc}^{sm} + (2n)T_{ecc}^{sm-s} + (n+1)T_{ecc}^{pa} + (2n)T_h \approx 0.1381$n+1.3467

message and transmits it to the recipient. Attacker 1 and attacker 3 are identical to an attacker of type 3, who cannot obtain partial user and master keys. Attacker 2 may be an attacker of type 3 or 2. However, neither can jeopardize the safety of the system. Attacker 1 and attacker 3 are similar to attackers of type 3 who access master keys. Attacker 2 can be either the type 3 attacker or the type 2 attacker. None of them may jeopardize the security of the system.

VI. PERFORMANCE EVALUATION

This section analyzes the performance of VPPCS and the methods in [17], [18], [20], [22]–[25] in terms of overhead computation and communication.

A. COMPUTATION OVERHEADS

The cryptography operation in [20], [22], [23], [25] are established on bilinear pairings, while those of [17], [18], [24] and the proposed scheme are established on ECC. This work uses MIRACL's cryptographic library [33] that calculates the time required for different cryptographic operations. The hardware platform comprises an Intel(R) Core(TM)2 Quad 2.66 GHz with a 4-gigabyte memory processor running the operating system Windows 7. Table 3 shows the definition of and execution times for associated cryptographic operations.

For flexibility, let *MGS*, *SVM*, and *BVMM* denote the message generation and signing, the single verification for a message, and the batch verification for multiple messages, respectively.

In the scheme in [17], *MGS* comprises one scalar multiplication, two secure hash functions and point additions. Thus, in this scheme, the overall calculation time of *MGS* is $1\ T_{ecc}^{sm} + 2\ T_h + 2\ T_{ecc}^{pa} \approx 0.6800$ ms. *SVM* comprises four scalar multiplications and three secure hash functions. Thus, it produces an overall computation time of $4T_{ecc}^{sm} + 3T_h \approx 2.6902$ ms. *BVMM* in this scheme requires (2n+2) scalar multiplications,(2n) small scalar point multiplications, (2n) point additions, and (3n) secure hash functions. The overall computation time for *BVMM* is therefore $(4n)T_{ecc}^{sm} + (3n)T_h \approx 2.6902$n ms.

TABLE 3. Cryptographic operation time and definitions.

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

In the scheme in [18], *MGS* comprises three scalar multiplications and two secure hash functions. Thus, in this scheme, the overall calculation time of *MGS* is $3T_{ecc}^{sm} + 2T_h \approx 2.0174$ ms. *SVM* comprises four scalar multiplications, three secure hash functions, and two point additions. Thus, it produces an overall computation time of $4T_{ecc}^{sm} + 3T_h + 2T_{ecc}^{pa} \approx 2.6964$ ms. *BVMM* in this scheme requires (2n+2) scalar multiplications,(2n) small scalar point multiplications, (2n) point additions, and (3n) secure hash functions. The overall computation time for *BVMM* is therefore $(2n+2)T_{ecc}^{sm} + (2n)T_{ecc}^{sm-s} + (2n)T_{ecc}^{pa} + (3n)T_h \approx 1.4858$n + 1.3436 ms.

In the scheme in [20], *MGS* comprises three scalar multiplications and two map to point hash functions. Thus, the total computation time of *MGS* is $3\ T_{bp}^{sm} + 2\ T_{mtp} \approx 13.041$ ms. This scheme has four bilinear pairing operations, one scalar multiplication and one map to point hash function, which gives the *SVM* an overall computation time of $4\ T_{bp} + 1\ T_{bp}^{sm} + 1\ T_{mtp} \approx 28.9818$ ms.

In the scheme in [22], *MGS* comprises three scalar multiplications, two point additions and one secure hash function. Thus, the total computation time of *MGS* is $3\ T_{bp}^{sm} + 1\ T_h + 2\ T_{bp}^{pa} \approx 4.7184$ ms. This scheme has three bilinear pairing operations, two scalar multiplications, two secure hash

functions and one point addition, which gives the *SVM* an overall computation time of 3 $T_{bp} + 2T_{bp}^{sm} + 2\ T_h + 1\ T_{bp}^{pa} \approx$ 23.5638 ms. *BVMM* in this scheme requires three bilinear pairing operations, $n + 1$ scalar multiplications, $2n$ small scalar multiplications, $3n - 3$ point additions and $2n$ secure hash functions. The overall computation time for *BVMM* is 3 $T_{bp} + (n + 1)T_{bp}^{sm} + (3n - 3)T_{bp}^{pa} + 2nT_h \approx 3.5972$ n + 18.9666 ms.

In the scheme in [23], *MGS* comprises two bilinear pairing operations, six scalar multiplications, one map to point hash function, four secure hash functions and two point additions. Thus, the total computation time of *MGS* is 2 $T_{bp} + 6\ T_{bp}^{sm} +$ 1 $T_{mtp} + 4\ T_h + 2\ T_{bp}^{pa} \approx 22.0396$ ms. This scheme has three bilinear pairing operations, two scalar multiplications, three secure hash functions and one point addition, which gives the *SVM* an overall computation time of 3 $T_{bp} + 2T_{bp}^{sm} +$ 3 $T_h + 1\ T_{bp}^{pa} \approx 23.5744$ ms. *BVMM* in this scheme requires three bilinear pairing operations, $n+1$ scalar multiplications, $2n$ small scalar multiplications, $3n - 2$ point additions and $3n$ secure hash functions. The overall computation time for *BVMM* is 3 $T_{bp}+(n+1)T_{bp}^{sm}+2nT_{bp}^{sm-s}+(3n-2)T_{bp}^{pa}+3nT_h \approx$ 4.9342n + 18.9772 ms.

In the scheme in [24], *MGS* comprises one scalar multiplication and two secure hash functions. Thus, in this scheme, the overall calculation time of *MGS* is $1T_{ecc}^{sm} +$ $2T_h \approx 0.6728$ ms. *SVM* comprises two scalar multiplications, two secure hash functions, and one point addition. Thus, it produces an overall computation time of $2T_{ecc}^{sm} +$ $1T_h + 1T_{ecc}^{pa} \approx 1.3477$ ms. *BVMM* in this scheme requires (2n+2) scalar multiplications,(2n) small scalar point multiplications, (2n+2) point additions, and (n) secure hash functions. The overall computation time for *BVMM* is therefore $(2n + 2)T_{ecc}^{sm} + (2n)T_{ecc}^{sm-s} + (2n)T_{ecc}^{pa} + (n)T_h \approx 1.4828$n + 1.3436 ms.

In the scheme in [25], *MGS* comprises one map to point hash function. Thus, the total computation time of *MGS* is 1 $T_{mtp} \approx 4.1724$ ms. This scheme has three bilinear pairing operations, a scalar multiplication, and a map to point hash function, which gives the *SVM* an overall computation time of 3 $T_{bp} + 1T_{bp}^{sm} + 1\ T_{mtp} \approx 23.1708$ ms. *BVMM* in this scheme requires three bilinear pairing operations, n scalar multiplications, and n map to point hash functions. The overall computation time for *BVMM* is 3 $T_{bp} + nT_{bp}^{sm} + nT_{mtp} \approx$ 5.7378n+17.4333 ms.

In VPPCS, *MGS* comprises only one multiplication and three secure hash functions. Therefore, in this scheme, the total computation time of *MGS* is$1T_{ecc}^{sm} + 3T_h \approx$ 0.6748 ms. *SVM* includes two scalar multiplications, two secure hash functions, and one point addition. Thus, it provides an overall computation time of *SVM* of $2T_{ecc}^{sm} + 2T_h +$ $1T_{ecc}^{pa} \approx 1.3487$ ms. *BVMM* in this scheme requires (2n+2) scalar multiplications,(2n) small scalar point multiplications, (n) point additions, and (2n) secure hash functions. The overall computation time for *BVMM* is therefore $(2)T_{ecc}^{sm} +$ $(2n)T_{ecc}^{sm-s} + (n + 1)T_{ecc}^{pa} + (2n)T_h \approx 0.1381$n + 1.3467 ms.

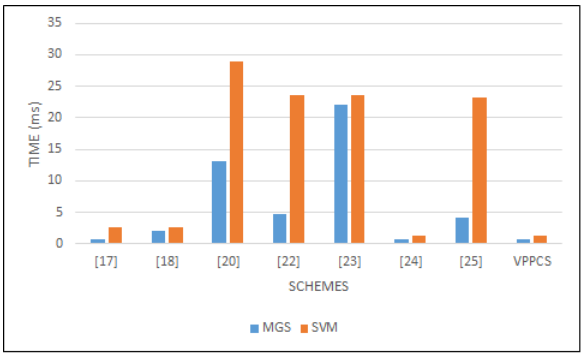

FIGURE 7. Computation costs of *MGS* and *SVM*.

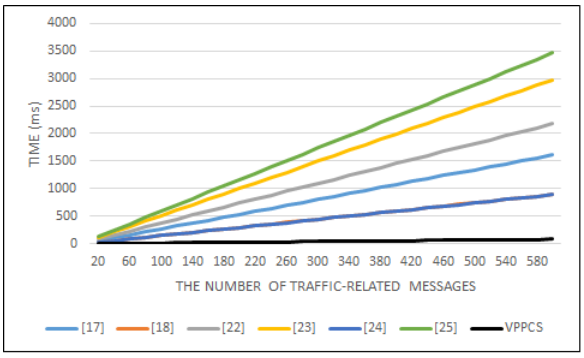

FIGURE 8. Computation costs of *BVMM* for different traffic-related messages.

Table 2 compares the cost of computing the proposed scheme with the three other ID-based schemes for *MGS*, *SVM*, and *BVMM*. Figure 7 shows that our scheme has a significant advantage over *MGS* and *SVM* tow schemes. Figure 8 indicates the costs of *BVMM* in measuring various traffic-related messages. Consequently, the proposed scheme is more productive and efficient than the methods in [17], [18], [20], [22], [23], [25] in terms of computation costs for *MGS*, *SVM*, and *BVMM*.

B. COMMUNICATION OVERHEADS

Communication overheads are now evaluated. The size of p^- is 64 bytes, which indicates that the size of each item in $G_1$is 128 bytes. The size of p is 20 bytes, which implies that the size of each item in G is 40 bytes. We also presume that the output sizes of the timestamp, secure hash function, and item in integer group Z_q^* are 4, 20, and 20 bytes, respectively, where the content of the message is omitted.

The traffic-related message contains two items in $\{PID_{il}^1, PK_i \in G\}$, three items in $\{PID_{il}^2, u_i, v_i \in Z_q\}$ and two timestamps. The size of the traffic-related message in the scheme [17] is (2*40 + 3*20 + 2*4) = 148 bytes.

The traffic-related message contains six items in G $\{PID_{i,1}, PID_{i,2}^2, R_i, P_i, D_i \in G\}$, one item in $\{\sigma_i \in Z_q\}$ and tow timestamps. The size of the traffic-related message in the scheme [18] is (4*2 + 20*5 + 40) = 148 bytes.

TABLE 4. Security analysis-based privacy properties.

Properties	[17]	[18]	[20]	[22]	[23]	[24]	[25]	VPPCS
Identity Privacy Preservation	✓	✓	✓	✓	✓	✓	✓	✓
Un-linkability	✓	✓	✓	✗	✗	✗	✓	✓
Un-observability	✗	✗	✗	✗	✗	✗	✗	✓
Traceability	✓	✓	✗	✓	✓	✓	✓	✓
Message Integrity and Authenticity	✓	✓	✗	✓	✓	✓	✓	✓
Resistance to Replay Attacks	✓	✓	✓	✗	✓	✓	✗	✓
Resistance to Impersonation Attacks	✓	✓	✓	✓	✓	✓	✓	✓
Resistance to Modification Attacks	✓	✓	✗	✓	✓	✓	✓	✓
Resistance to Man-in-the-Middle Attacks	✓	✓	✓	✓	✓	✓	✓	✓

The traffic-related message contains two items in $\{rx.P, Cert \in G_1\}$, four items in $\{L_i, U, V, W\sigma \in Z_q\}$ and two timestamps. The size of the traffic-related message in the scheme [20] is $(128 * 2 + 20 * 4) = 336$ bytes.

In G_1 $\{ID_{i1}, ID_{i2}, \sigma \in G_1\}$, the traffic-related message contents are three items. The size of the traffic-related message in scheme in [22] is $(128*3) = 384$ bytes.

The traffic-related message contains three items in $\{PID_{il}^1, PID_{il}^2, U_i \in G_1\}$, one item in $\{V_i \in Z_q\}$ and three timestamps. The size of the traffic-related message in the scheme [23] is $(20 + 3*128 + 2*4) = 412$ bytes.

The traffic-related message contains three items in $\{PID_{v1}, PID_{v2}, w \in G\}$, one item in $\{\sigma \in Z_q\}$ and two timestamps. The size of the traffic-related message in the scheme [24] is $(40 * 3 + 20 + 2*4) = 148$ bytes.

In G_1 $\{PID_i^1, PID_i^2, \sigma \in G_1\}$, the traffic-related message contents are three items. The size of the traffic-related message in scheme in [25] is $(128*3) = 384$ bytes.

TABLE 5. Overhead of communication comparison.

Schemes	Sending of single traffic-related message(byte)	Sending of multiple (n) traffic-related messages(byte)
[17]	148	148 n
[18]	148	148 n
[20]	336	336 n
[22]	384	384 n
[23]	412	412 n
[24]	148	148 n
[25]	384	384 n
VPPCS	88	88 n

In the proposed VPPCS, the vehicle broadcasts a traffic-related message with size $(40 + 20*2 + 8) = 88$ bytes. The traffic-related message contains one item in $\{PID_{il}^1 \in G\}$, two items in $\{PID_{il}^2, \sigma_m \in Z_q\}$, and two timestamps. Table 5 indicates the overall communication overhead, and Figure 9 illustrates the corresponding outcome. The overall communication overhead is relatively low for the proposed scheme.

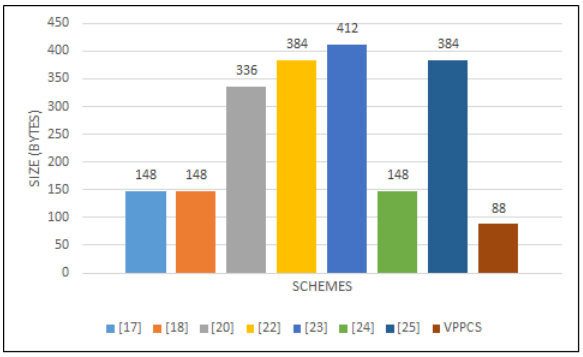

FIGURE 9. Communication costs.

VII. DISCUSSION

Privacy preservation is the main concern of drivers. Thus, we argue that vehicular communication systems should be resolved by complying with all privacy requirements. Compared with similar works [17], [18], [20], [22]–[25], our only scheme meets all of the requirements for security and privacy. VANET schemes [17], [18], [20], [22]–[25] compared with the proposed scheme are described in Table 4. Notably these schemes focus heavily on information privacy. However, the contextual privacy requirement is not fully fulfilled despite their importance in a VANET context. Only certain proposals satisfy the sender's and receiver's anonymity and the unlinkability. Unobservability is completely ignored because of the overhead. The communication with VANET fulfills all the requirements for privacy based on identity-based cryptography and the specific communication situation. We show the robustness and reliability of our VPPCS system through our privacy and performance analysis.

VIII. CONCLUSION AND FUTURE WORK

Intelligent Transport System (ITS) has been gaining momentum as more elements in a transport systems are becoming more connected. In line with this, VANETs are becoming popular and greatly contribute to ITS. The specifications for contents and contextual privacy must be met to protect privacy vehicles in terms of identity and location as susceptible information. In this paper, we have proposed a scheme to ensure these requirements are met. The scheme ensures privacy of data through signing and verifying traffic-related messages, which are protected by the proposed VPPCS scheme. It also meets the requirement of all contextual privacy on the grounds of the injection for fake traffic-related messages. Security and performance analyses were performed to validate the proposed scheme. The security

analysis shows that VPPCS can withstand model security attacks and satisfy all privacy requirements. The performance evaluation reveals that the scheme proposed by VPPCS is VANET compatible and that our VANET scheme is efficient in terms of computational cost and communication overhead. The balance between privacy and performance was also emphasized.

When the pseudonym set is expired, the vehicle removes the old set and then requests to obtain a new set. Consequently, there is no accumulated storage, which leads to the overhead increased. In future research, the main focus of the next paper is to address the overhead of storage in the VANET system. Besides, we will carry out simulation experiment through simulation platform such as OMNET++ and SUMO to demonstrate the performance of the work.

REFERENCES

[1] V. Hoa La and A. Cavalli, "Security attacks and solutions in vehicular ad hoc networks: A survey," *Int. J. AdHoc Netw. Syst.*, vol. 4, no. 2, pp. 1–20, Apr. 2014.

[2] F. Qu, Z. Wu, F. Wang, and W. Cho, "A security and privacy review of VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 6, pp. 2985–2996, Dec. 2015.

[3] 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.

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

[5] 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.

[6] M. R. Jabbarpour, H. Zarrabi, R. H. Khokhar, S. Shamshirband, and K.-K.-R. Choo, "Applications of computational intelligence in vehicle traffic congestion problem: A survey," *Soft Comput.*, vol. 22, no. 7, pp. 2299–2320, Apr. 2018.

[7] Z. Zhou, C. Gao, C. Xu, Y. Zhang, S. Mumtaz, and J. Rodriguez, "Social big-data-based content dissemination in Internet of vehicles," *IEEE Trans. Ind. Informat.*, vol. 14, no. 2, pp. 768–777, Feb. 2018.

[8] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETs): Status, results, and challenges," *Telecommun. Syst.*, vol. 50, no. 4, pp. 217–241, 2012.

[9] D. Jacobs, K.-K.-R. Choo, M.-T. Kechadi, and N.-A. Le-Khac, "Volkswagen car entertainment system forensics," in *Proc. IEEE Trustcom/BigDataSE/ICESS*, Aug. 2017, pp. 699–705.

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

[11] 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.

[12] A. Pfitzmann and M. Hansen, "Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management-a consolidated proposal for terminology," *Version V0*, vol. 31, p. 15, Feb. 2008.

[13] R. Boussada, M. E. Elhdhili, and L. A. Saidane, "A survey on privacy: Terminology, mechanisms and attacks," in *Proc. IEEE/ACS 13th Int. Conf. Comput. Syst. Appl. (AICCSA)*, Nov. 2016, pp. 1–7.

[14] 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.

[15] M. Razzazi, M. Jafari, S. Moradi, H. Sharifipanah, M. Damanafshan, K. Fayazbakhsh, and A. Nickabadi, "Common criteria security evaluation: A time and cost effective approach," in *Proc. 2nd Int. Conf. Inf. Commun. Technol.*, vol. 2, 2006, pp. 3287–3292.

[16] F. Dötzer, "Privacy issues in vehicular ad hoc networks," in *Privacy Enhancing Technologies* (Lecture Notes in Computer Science), vol. 3856, G. Danezis and D. Martin, Eds. Berlin, Germany: Springer, 2006. [Online]. Available: https://doi.org/10.1007/11767831_13

[17] 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.

[18] Y. Ming and H. Cheng, "Efficient certificateless conditional privacy-preserving authentication scheme in VANETs," *Mobile Inf. Syst.*, vol. 2019, pp. 1–19, Feb. 2019.

[19] C. Hu, T. W. Chim, S. M. Yiu, L. C. K. Hui, and V. O. K. Li, "Efficient HMAC-based secure communication for VANETs," *Comput. Netw.*, vol. 56, no. 9, pp. 2292–2303, Jun. 2012.

[20] X. Xue and J. Ding, "LPA: A new location-based privacy-preserving authentication protocol in VANET," *Secur. Commun. Netw.*, vol. 5, no. 1, pp. 69–78, Jan. 2012.

[21] 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.

[22] T. W. Chim, S. M. Yiu, L. C. K. 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.

[23] K.-A. Shim, "$\mathcal{CPAS}$: An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks," *IEEE Trans. Veh. Technol.*, vol. 61, no. 4, pp. 1874–1883, May 2012.

[24] 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.

[25] 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.

[26] V. S. Miller, "Use of elliptic curves in cryptography," in *Advances in Cryptology—CRYPTO* (Lecture Notes in Computer Science), vol. 218, H. C. Williams, Ed. Berlin, Germany: Springer, 1986. [Online]. Available: https://doi.org/10.1007/3-540-39799-X_31

[27] S. Biswas and J. Md. Mahbubul Haque, Misic, "Privacy and anonymity in VANETs: A contemporary study," *Ad Hoc Sensor Wireless Netw.*, vol. 10, nos. 2–3, pp. 177–192, 2010.

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

[29] 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.

[30] 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.

[31] M. Burrows, M. Abadi, and R. M. Needham, "A logic of authentication," *Proc. Roy. Soc. A, Math., Phys. Eng. Sci.*, vol. 426, no. 1871, pp. 233–271, 1989.

[32] 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.

[33] (2018). *Multi Precision Integer and Rational Arithmetic Cryptographic Library (MIRACL)*. [Online]. Available: http://www.certivox.com/miracl/

MAHMOOD A. AL-SHAREEDA received the B.S. degree in communication engineering from Iraq University College and the M.Sc. degree in information technology from the Islamic University of Lebanon (IUL), in 2018. He is currently pursuing the Ph.D. degree with the National Advanced IPv6 centre (NAv6), Universiti Sains Malaysia (USM). His research interests include security and privacy issues in vehicular ad hoc networks (VANETs) and network optimization.

MOHAMMED ANBAR (Member, IEEE) received the Ph.D. degree in advanced computer networks from University Sains Malaysia (USM). He is currently a Senior Lecturer with the National Advanced IPv6 centre (NAv6), Universiti Sains Malaysia. 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 networks (VANETs) security, and IPv6 security.

SELVAKUMAR MANICKAM is an associate professor working in cybersecurity, the Internet of Things, Industry 4.0, and machine learning. He has authored or coauthored more than 160 papers in journals, conference proceedings, and book reviews, and graduated 13 Ph.D. degree students. He has ten years of industrial experience prior to joining academia. He is a member of technical forums at national and international levels. He has also experience in building IoT, embedded servers, and mobile- and web-based applications.

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 of Science and Technology, Wuhan, China. He is currently an Assistant Professor with the Department of Computer Science, College of Education for Pure Science, University of Basrah. His research interests include the security of cloud computing, image processing, pattern recognition, biometrics, data integrity, DNA cryptography, steganography, sharing data, graphical password, QR code, and soft computing.