IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 28, 2020, accepted January 18, 2021, date of publication January 20, 2021, date of current version January 27, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3053043

A Lightweight Authentication With Privacy-Preserving Scheme for Vehicular Ad Hoc Networks Based on Elliptic Curve Cryptography

JALAWI SULAIMAN ALSHUDUKHI, ZEYAD GHALEB AL-MEKHLAFI, AND BADIEA ABDULKAREM MOHAMMED, (Member, IEEE)

Department of Information and Computer Science, College of Computer Science and Engineering, University of Ha'il, Ha'il 81481, Saudi Arabia

Corresponding author: Zeyad Ghaleb Al-Mekhlafi (ziadgh2003@hotmail.com)

ABSTRACT Vehicle in vehicular ad hoc networks (VANETs) broadcasts beacons about their traffic status wirelessly for improving traffic safety and efficiency. Before deployment of the VANET system, problems related to security and privacy should be carefully addressed. In this article, we propose a lightweight authentication with conditional privacy-preserving scheme for guaranteeing secure communication in VANET. The proposed scheme is suitable for addressing issues related to security and privacy because it combines the tamper-proof device (TPD) based schemes with the roadside unit (RSU) based schemes. Based on elliptic curve cryptography, the proposed scheme preloads the initial public parameters and keys of the system in each TPD of RSU instead of the TPD of the on-border unit (OBU). Furthermore, the proposed scheme not only achieve security and privacy requirements but also resists common security attacks. The performance evaluation shows that the proposed scheme has a lower cost compared with other existing schemes in terms of computation cost and communication cost.

INDEX TERMS Authentication, tamper proof device (TPD), privacy-preserving, vehicular ad-hoc networks (VANETs).

I. INTRODUCTION

Recently, the intelligent transportation system (ITS) has attracted more deliberate attention from the motor industry, academia, and even government in recent years since it is reducing traffic congestion, enhancing driving efficiency, improving traffic safety, minimizing environmental pollution and providing convenience [1], [2]. Vehicular ad hoc networks (VANETs) are an entity of ITS with a fully a self-organizing wireless ad hoc communication system containing vehicles equipped with onboard unit (OBU), a trusted authority (TA) which preloads the initial public parameters of the VANET, and a road side unit (RSU) deployed at intersections in country, as presented in Figure 1. The communications types in VANETs contain two main modes: vehicle-to-vehicle (V2V) communication and vehicle-to-infrastructure (V2I) communication [3], [4].

Dedicated short-range communication (DSRC) protocol is an open wireless technology which allows the vehicle for processing, receiving, broadcasting and communicating with each other or nearby RSU and exchanging messages such as safety warnings, location, speed, direction, weather reports and movement of the vehicle to the network in a period from 100 ms until 300 ms, whereas RSUs and TA can exchange messages utilizing a secure wired channel [5]. According to

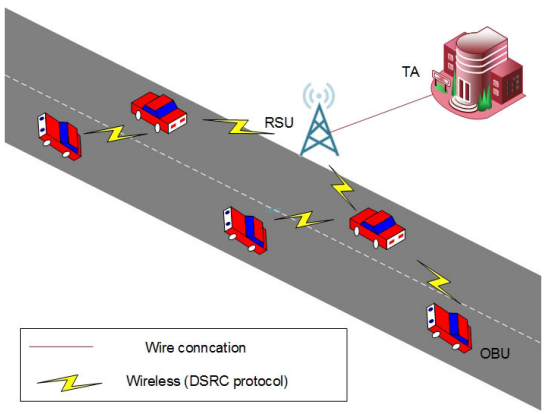

FIGURE 1. A typical VANET scenario.

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

these messages, other vehicles can take critical measures to utilize alternate paths during travel for avoiding traffic accident and congestion [6].

Based on the openness-nature of V2V and V2I communications in VANETs, it is possible that anyone could launch different security attacks for compromising the privacy of driver and obtaining sensitive information. Thus, before services and applications of VANETs are deployed, the issues related to security and privacy must be carefully considered in the system [7], [8].

Several researchers have been designed on the requirements of security and privacy. Although the other schemes have been able to satisfy most of these requirements. However, these schemes most also suffer from massive overhead regarding the burden storage and computation and communication costs. Thus, we propose a lightweight authentication with conditional privacy-preserving scheme in VANET. This article contains the major contributions can be listed as follows

- A lightweight authentication with conditional privacy-preserving scheme for securing V2V and V2I communications and carry out better efficient performance. The proposed scheme utilizes the Elliptic Curve Cryptography (ECC) algorithm and XOR operation with secure one-way hash functions during the mutual authentication and broadcasting process. Thus, lightweight security is satisfied by our scheme.
- A proposed scheme is suitable for addressing issues related to security and privacy, because it combines road side unit (RSU) based schemes with tamper proof device (TPD) based schemes. Based on elliptic curve cryptography, the proposed scheme preloads the initial public parameters and keys of the system in each TPD of RSU instead of TPD of on-border unit (OBU).
- After receiving secret key from TA, the RSU has the ability to generate multiple temporary private keys during various times. Therefor, the verifying receiver uses the RSU's public key instead of TA's public key to verify the signer authenticity and message validity.
- A performance evaluation shows that the proposed scheme has lower overhead compared with other existing schemes in terms of computation and communication costs.

The remainder of this article is organized as follows: Section II reviews the security schemes regarding VANETs. Section III introduced preliminaries of the proposed scheme. Section IV shows the five phases included in the proposed scheme. Section V shows security analysis and comparison of our work in details. Section VI indicates the performance efficiency. Conclusion and future work of this work are shown in Section VII.

II. RELATED WORK

A. PUBLIC KEY INFRASTRUCTURE (PKI)

The core concept of public key infrastructure (PKI) based schemes is that OBU needs to store a multiple of public-private keys and anonymous certificates (nearly 44,000) on each vehicle. These anonymous are signed by TA before storing on the vehicle in advance.

Rajput *et al.* [9] designed a privacy-preserving pseudonymous scheme based on hierarchical authentication which the legal interval of their aim to cope with some disadvantages of schemes based on PKI. Cincilla *et al.* [10] introduced the scalability and similarity of the replicated schemes based on PKI. Hence, their scheme computes efficiency of schemes based on PKI and emulates on tools hundreds. Joshi *et al.* [11] designed an efficient scheme using event-triggered which broadcasted beacons to address issues related to security in VANET. Their scheme utilizes the signer of verification based on the PKI to test the beacon validity. Asghar *et al.* [12] conducted a feasible scheme based on PKI to address the process of authenticating requests, which means that the amount of the certificate revocation list (CRL) linear. Hence, their scheme offers vehicles to get services in improve scalability and valid time.

Nevertheless, multiple of public-private keys and anonymous certificates needed to be stored on each the OBU of nodes, which will cause for increasing massive burden of anonymous management for TA. Furthermore, the node is vulnerable to the store management load due to the capacity of store of the node is small. Besides, the verifier needs to test whether the certificate is valid during the verification process, which will lead to increasing the computation overhead of the VANET system.

B. IDENTITY (ID)

To avoid the burden of multiple of public-private keys and certificates presenting from the approach of Public Key Infrastructure (PKI), Shamir interceded the identity approach in 1984 [13]. The core idea of IDentity (ID) is the public key is derived from identification data such as license, personal number and model. Thus, this approach is fully avoided from private-public keys and corresponding certificates with PKI, which leads the overhead created from the certificates of message containing is reduced. Thus, many types of research have proposed ID-based schemes in VANETs for providing secure V2V and V2I communications. We category these approaches as the following subsection,

1) TPD-BASED SCHEMES

The Tamper-Proof Device (TPD) is needed to ensure that the information collected has not been changed when they are transmitted to other nodes in VANETs. The main accountability of the TPD on on-border unit (OBU) is to possess capabilities of cryptographic processing to sign and verify messages. Due to it offers hardware protection, the attacker does not has the ability for penetrating.

Lee and Lai [14] suggested a group testing based on batch verification security to address the limitation of authentication schemes in securing communication. However, this scheme has an insecure against the impersonation attacks. Zhang *et al.* [15] conducted an authentication and privacy

scheme utilizing bilinear pairing to provide batch verification process which allowing multiple beacons received to be checked simultaneously. He *et al.* [16] conducted an authentication scheme based on conditional privacy-preserving to secure communication in VANET. Li *et al.* [17] proposed an efficient, provably-secure and anonymous conditional privacy-preserving authentication (EPA-CPPA) scheme to be used in safety-related applications of VANETs. However, in advance, TA preloads group of private keys and group of pseudonym-IDs to each vehicle, which will issue for increasing massive certification management burden for TA since the vehicle's storage capacity is limited. Al-shareeda *et al.* [18] introduced a new and efficient conditional privacy-preserving authentication (NE-CPPA) scheme to provide communication security in VANETs. Int their scheme, TA computes its private key and preloads in the TPD of the vehicle via a secure channel that given not to be compromised with any malicious node.

The major challenge of TPD-based schemes is the revocation process since the fact that the master keys and essential information are contained on TPD. Besides, the vehicle is also vulnerable to the burden of storage management. Hence the misbehaving vehicle should be revoked in the process of revocation requirement, TPD of it should be confiscated and the storage management burden is mitigated.

2) RSU-BASED SCHEMES

Road side units (RSUs) are infrastructure device which have sufficient power of processing, high rate of transmission and large capacities. RSUs are costly unites (particularly in VANET deployment's the early stages), which leads to it not be placed on all intersection in a country.

Huang *et al.* [19] designed leveraging RSU based scheme is called a pseudonymous authentication-based conditional privacy (PACP), which depends on using the pseudonym rather then the real identity to provide conditional privacy-preserving in VANETs. Xue *et al.* [20] designed the concept of a location to propose authentication with privacy-preserving scheme in VANETs to cope with the issue on conditional privacy preservation which a TA has the ability to trace the signer in a dispute case. Azees *et al.* [21] suggested a conditional privacy-preserving scheme based on anonymous authentication to avert misbehaving vehicle joining into V2V and V2I communications in VANETs system. In their work, before RSU provides location based safety information (LBSI) messages to vehicles, it could properly validate vehicles in an anonymous communication. Cui *et al.* [22] conducted an authentication scheme based on conditional privacy-preserving without utilizing a TPD that is fitted with each vehicle in VANETs. This scheme utilizes the cuckoo filter method and the binary search method for improving the batch authentication approach. Zhang *et al.* [23] used a method of Chinese Remainder Theorem in their work to suggest a conditional privacy-preserving scheme based on authentication for coping with problems of security and privacy in VANETs system. In their scheme, realistic TPD is only needed only requires realistic TPDs without storing the private key on to the TPD on OBU. Baya at al. [24] proposed an authentication scheme that preloads the list of pseudonym-IDs to the registered vehicle which vehicle uses them to sign and verify messages. Al-shareeda *et al.* [25] proposed VANET-based privacy-preserving communication (VPPCS) scheme to satisfy all requirements of privacy by injecting false information on anonymous communication during signing message process. It is possible for attacker to confirm weather vehicle switch on or not. Wei *et al.* [26] suggested a conditional privacy-preserving scheme based on authentication to satisfy message recovery and address side-channel attack methods by updating system secret key (SSK). This scheme is based on elliptic curve discrete logarithm supposition and SSK updating algorithm.

In RSU-based schemes, the vehicle authenticates each other by utilizing RSUs and then send the rogue vehicle list and authentic vehicle list with issues of the notification. Thus, the vehicle will wait for these issues before verifying the authenticity of the sender, which leads to an increase in the overhead of the system. Due to they do not provide the communication of V2V, therefore all communications must happen in the RSU's presence.

III. PRELIMINARIES

A. NETWORK MODEL

A typical VANETs contains three main components as follows,

- *OBU*:
  Each vehicle has a wireless device known as OBU to enable vehicle for processing, sending and receiving beacons through the DSRC protocol.
- *TA*:
  is trusted management accountable for generating system parameter and registering vehicle and RSU in VANETs. It is also accountable for executing the process of revocation.
- *RSU*:
  it is deployed along road side and it has the responsibility to manage each OBUs within its coveraged domain by utilizing the protocol of DSRC. The RSU exchange messages with OBUs and TA through a wireless and secure wired network, respectively. Each RSU has a Tamper-Proof Device (TPD) to save sensitive information and implement cryptography operations from the system. Thus, it is impossible for adversary to disclose it.

B. DESIGN GOALS

In this subsection, we briefly show that the design goals of the proposed scheme must satisfy the following requirements of security and privacy.

- *Integrity and Authentication:*
  A recipient must be ensured that received message content has not been altered or modified that it is an authentic vehicle.

- *Identity Privacy-Preserving:*
  An attacker should be unable to reveal the original identity of the vehicle from the beacons.
- *Unlinkability:*
  An attacker should not be capable of relating two or more beacons to the same sender.
- *Traceability and Revocation:*
  The TA should be capable to trace and revoke the original identity of the vehicle and take the necessary legitimate action.
- *Resistance to Security Attack:*
  A robustness scheme should withstand common attacks such as replay [27], modification [28], impersonation, and Man-In-The-Middle (MITM) attacks [29], [30].

IV. THE PROPOSED SCHEME

In this section, we propose a lightweight authentication with privacy-preserving scheme in VANETs. Functionally, RSU-based and TPD-based schemes are combined in this work. In the proposed, a TPD equipped with each vehicle and RSU in the system. Due to there being link security and rapid between RSU and TA, the process of authentication can be provided significantly more efficient. Therefore, it is accountable for storing the system's secret parameter and basic parameter in RSUs rather than OBUs.

Furthermore, unlike schemes reviewed in Subsection II-B1, the proposed scheme computes secret key and preloads it on TPD of RSU. So, the RSU has the ability to generate multiple temporary private key during various times. Also, the proposed scheme only keeps the RSU's temporary private key in the TPD of OBU for signing message, unlike schemes reviewed in Subsection II-B2 that stores the private key of the system. In the proposed, the TA's secret key is only equipped in the TPD of RSUs while the RSU's temporal secret key is saved in the TPD of OBUs. After the interval of timestamp (T_S) is expired, RSU's temporal secret key is updated regularly. The signer vehicle uses RSU's private key to generate signature key of message, while the verifying recipient uses RSU's public key rather than TA's public key to verify the authenticity of signer and validity of message by checking these signatures.

In the proposed, once a vehicle arrives at the RSU's coveraged domain, it must enter the RSU domain to obtain the RSU's temporal key. A pseudonym-ID with its original identity and TA's initial parameters are first generated by the OBU. Then OBU authenticates itself with the system by helping RSU via TA's secret key that is equipped with its TPD. After the shared secret key is computed, RSU sends its temporal key to OBU via a secure channel. Then OBU utilizes this RSU's temporal key for computing a pseudonym-ID and its relevant private key, which is useful until the end of the interval of (T_S). OBU utilizes this pseudonym-ID and its corresponding private key for signing the traffic-related messages that must be generated.

The following four phases are included in the proposed scheme: initialization of the system, mutual authentication, signing-message and verifying-messages. Table 1 lists The abbreviations and notations in this article.

TABLE 1. Notations Definition of the Proposed Scheme.

Notation	Descriptions
TPD	Tamper prof device
OBU	On-border unit
TA	Trusted authority
RSU	Roadside unit
P_{TA}^{pub}, X_{TA}	The public key and private key of the system
$P_{RSU_j}^{pub}, X_{TA}^{RSU_j}$	The public key and private key of the RSU_j
$ENC_x(.)/DEC_x(.)$	The encryption/decryption of symmetric function
h_1, h_2, h_3	One-way hash functions
$\|$	Operation of concatenation
$\oplus$	XOR operator
OID_i	The vehicle original identity
d, w	Random integer numbers
TS_i	Timestamp
$PsID_i, PID_i$	Vehicle Pseudonym-ID
PK_i	private key of signature message
k_{ij}	share secret key between RSU_j and OBU_i

A. INITIALIZATION OF SYSTEM

In this phase, we describe TA to generate initial parameters of the system and register the rest of the entity of VANETs in details.

- Let G be a generator of adaptive group of prime order q. Let E be an ECC determined by non-singular equation ($y^2 = x^3 + ax + b \bmod p$), where $a, b \in F_p$ and p is a large prime.
- TA selects a randomly value $X_{TA} \in Z_q^*$ as its secret key and computes $P_{TA}^{pub} = X_{TA}P$ to be its relevant public key.
- TA selects the encryption/decryption $ENC_x(.)/DEC_x(.)$ of symmetric function and three functions of one-way hash
  $-h_1 : G \rightarrow Z_q^*$,
  $-h_2 : \{0,1\}^* \times \{0,1\}^* \times G \rightarrow Z_q^*$,
  $-h_3 : \{0,1\}^* \rightarrow Z_q^*$.
- TA preloads the initial parameters $\{p, q, a, b, P, P_{TA}^{pub}, ENC_x(.), DEC_x(.), h_1, h_2, h_3\}$ in all RSUs and OBUs.
- TA computes X_{RSU_j} as a secret key for each RSU_j and then X_{TA} and X_{RSU_j} are stored on the TPD of RSU_j.

B. MUTUAL AUTHENTICATION

Once a vehicle reaches to the coveraged domain by RSU_j, OBU_i must be authorized itself with the system for obtaining the secret temporal key of RSU_j. The following steps should be done to achieve the process of OBU_i joining to the RSU domain.

- OBU_i chooses a random value $d \in Z_q^*$ and computes its pseudonym-ID to transmit it to RSU_j. This pseudonym-ID is generated by the original identity of vehicle and the TA's public key as bellow:

$$\begin{aligned} PID_i &= \{PID_{1,i}, PID_{2,i}\} \\ PID_{1,i} &= dP \\ PID_{2,i} &= OID_i \oplus h_1(dP_{TA}^{pub}) \end{aligned} \quad (1)$$

- After RSU_j receives the pseudonym-ID from OBU_i, RSU_j disclose the original identity of vehicle by utilizing the TA's secret key which is saved in the its TPD as bellow:

$$OID_i = PID_{2,i} \oplus h_1(X_{TA}PID_{1,i}) \tag{2}$$

- Then RSU_j verifies whether OID_i exists in the CRL which is sent by TA for ensuring that vehicle is not revoked. If vehicle is authenticated, the RSU computes symmetric secret key $k_{ij} = h_1(X_{TA}PID_{1,i})$.
- RSU_j generates the fresh temporal key (refresh in TS) as $X_{TS}^{RSU_j} = h_1(X_{RSU_j}||TS)$ with its secret key X_{RSU_j} which is saved in TPD of it. RSU_j then generates its relevant public key as $P_{RSU_j}^{pub} = X_{TS}^{RSU_j}P$. It then frequently sends public key ($P_{RSU_j}^{pub}$) of it with TS of it on the coveraged domain of it.
- RSU_j encrypts private key $X_{TS}^{RSU_j}$ of it as $ENC_{k_{ij}}(X_{TS}^{RSU_j})$ with the symmetric secret key k_{ij}, which RSU uses symmetric secret key k_{ij} to encrypt symmetric function of RSU's private key while the OBU_i uses it to decrypts function for obtaining RSU's private key, therefore, symmetric secret key is sharing secret key between RSU_j and OBU_i during mutual authentication process. It then sends $\{ENC_{k_{ij}}(X_{TS}^{RSU_j}), PID_{1,i}, PID_{2,i}\}$ to OBU_i.
- Once $\{ENC_{k_{ij}}(X_{TS}^{RSU_j}), PID_{1,i}, PID_{2,i}\}$ is received, OBU_i first decrypts $DEC_{k_{ij}} = ENC_{k_{ij}}(X_{TS}^{RSU_j})$ to obtain temporal key $X_{TS}^{RSU_j}$, where $k_{ij} = h_2(dP_{TA}^{pub}) = h_2(X_{TA}PID_{1,i})$.

C. SIGNING-MESSAGE

In order to the sake of vehicle's anonymity, beacon must be signed with a various private key. Therefore vehicle generates a pseudonym-ID and the corresponding private key for each beacon depends on the RSU_j temporal key within the interval of TS. To sign message (m_i), the following steps should be done by OBU_i.

- OBU_i first selects random value $w_i \in Z_q^*$ and computes its pseudonym-ID $PsID_i = <PsID_i^1, PsID_i^2>$ and its corresponding private key PK_i as follows:

$$\begin{aligned} PsID_i &= \{PsID_i^1, PsID_i^2\} \\ PsID_i^1 &= w_iP \\ PsID_i^2 &= OID_i \oplus h_1(w_iP_{RSU_j}^{pub}) \end{aligned} \tag{3}$$

$$PK_i = X_{TS}^{RSU_j}h_2(PsID_i^1||PsID_i^2||TS_i) \tag{4}$$

- OBU_i computes the signature of the message m_i as follows:

$$\sigma_{m_i} = PK_i + w_ih_3(PsID_i^1||PsID_i^2||m_i||TS_i) \tag{5}$$

- OBU_i broadcasts the beacon $\{PsID_i^1, PsID_i^2, m_i, TS_i, \sigma_{m_i}\}$ to receivers.

D. VERIFYING-MESSAGES

After the beacon $\{PsID_i^1, PsID_i^2, m_i, TS_i, \sigma_{m_i}\}$ is received, the receiver checks if Equation 6 holds and accepts the message m_i if it legitimate.

$$\begin{aligned} \sigma_{m_i}.P = {} & h_2(PsID_i^1||PsID_i^2||TS)P_{RSU_j}^{pub} \\ & + h_3(PsID_i^1||PsID_i^2||m_i||TS)PsID_i^1 \end{aligned} \tag{6}$$

Equation 6 proof is as below:

$$\begin{aligned} & = R.H.S \\ & = (PK_i + w_ih_3(PsID_i^1||PsID_i^2||m_i||TS_i)).P \\ & = (X_{TS}^{RSU_j}h_2(PsID_i^1||PsID_i^2||TS_i) \\ & \quad + w_ih_3(PsID_i^1||PsID_i^2||m_i||TS_i)).P \\ & = h_2(PsID_i^1||PsID_i^2||TS)X_{TS}^{RSU_j}.P \\ & \quad + h_3(PsID_i^1||PsID_i^2||m_i||TS_i)w_i.P \\ & = h_2(PsID_i^1||PsID_i^2||TS_i)P_{RSU_j}^{pub} \\ & \quad + h_3(PsID_i^1||PsID_i^2||m_i||TS_i)PsID_i^1 \\ & = R.H.S \end{aligned}$$

Hence, Equation 6 is checked to be true.

Furthermore, consider a verifying recipient who has received a large number of beacons such as $\{PsID_i^{1\,1}, PsID_i^{2\,1}, m_i^1, TS_i^1, \sigma_{m_i}^1\}, \{PsID_i^{1\,2}, PsID_i^{2\,2}, m_i^2, TS_i^2, \sigma_{m_i}^2\}, \ldots \{PsID_i^{1\,n}, PsID_i^{2\,n}, m_i^n, TS_i^n, \sigma_{m_i}^n\}$

By utilizing process of batch verification, the signatures can be checked at the simultaneous as bellow:

$$\begin{aligned} \left(\sum_{i=1}^{n}\sigma_{m_i}.P\right) = {} & \left(\sum_{i=1}^{n}h_2(PsID_i^1||PsID_i^2||TS)P_{RSU_j}^{pub}\right) \\ & + \left(\sum_{i=1}^{n}h_3(PsID_i^1||PsID_i^2||m_i||TS_i)PsID_i^1\right) \end{aligned} \tag{7}$$

If Equation 7 holds, all beacons are legitimate, all recipients are authenticated and the receivers accept all the message m_i. Otherwise, there is an unauthentic vehicle; therefore, a modern protocol is suggested in [31] to determine these unauthentic vehicles.

V. SECURITY ANALYSIS

Formal and informal analysis of the proposed scheme are briefly analyzed in this section as follows,

A. FORMAL ANALYSIS

According to the capability of the attacker, we analyze the security proof in this work by defining a game among an attacker A and the challenger C. If an attacker A wins the game, it is possible to return a legitimate forged signature. At the same time, the proposed scheme is secure in VANET when an attacker A is negligible for any attacks.

Theorem 1: Our proposed scheme under the random oracle model for VANETs is unforgeable against an adaptively chosen message attack.

Proof: Supposing an attacker A can forge legitimate beacon $\{PsID_i^1, PsID_i^2, m_i, TS_i, \sigma_{m_i}\}$ for the traffic-related message M_i, therefore a challenger C can be generated to resolve ECDL problem with probability of non-negligible to run A as a subroutine.

Setup initialization phase: Challenger C first selects randomly value $X_{TS}^{RSU_j} \in Z_q^*$ as the RSU's private key and computes $P_{RSU_j}^{pub} = X_{TS}^{RSU_j} P$ as the RSU's public key. Then C sends the public parameter and functions of the system to A.

$Lh-1$. C starts the $h-list_1$ with form of $(\alpha, \tau h_1)$. After A receives message with form of (α), C verify whether (α) is in $h-list_1$, if exist, C transmits $(\tau h_1 = h(\alpha))$ to A. Otherwise, C selects $\tau h_1 \in Z_q^*$ randomly and puts $(\alpha, \tau h_1)$ into $h-list_1$. Then, A sends $\tau h_1 = h(\alpha)$ to C.

$Lh-2$. C starts the h_{list_2} with form of $(PsID_i^1, PsID_i^2 \tau h_2)$. After A receives message with form of $(PsID_i^1, PsID_i^2)$, C verify whether $(PsID_i^1, PsID_i^2)$ is in $h-list_2$, if exist, C sends $(\tau h_2 = h(PsID_i^1 || PsID_i^2 || \tau h_2)$ to A. Otherwise, C selects $\tau h_2 \in Z_q^*$ at random and puts $(PsID_i^1, PsID_i^2 \tau h_2)$ into $h-list_2$. Then, A sends $\tau h_2 = h(PsID_i^1 || PsID_i^2 || \tau h_2)$ to C.

$Lh-3$. C starts the $h-list_3$ with form of $(M_i, TS_i, \tau h_3)$. After A receives message with form of $(M_i, TS_i, C$ verify whether (M_i, TS_i) is in h_{list_3}, if exist, C sends $(\tau h_3 = h(M_i || TS_i || \tau h_3)$ to A. Otherwise, C selects $\tau h_3 \in Z_q^*$ at random and puts $(M_i, TS_i, \tau h_3)$ into $h-list_3$. Then, A sends $\tau h_3 = h(M_i || TS_i || \tau h_3)$ to C.

Sign-Oracle: After receiving a sign request from A, C computes three randomly values, $h-i, 2; h-i, 3; \sigma_{m,i} \in Z_q^*$, and randomly point $PsID_i^2 \in G$. Then C computes $PsID_i^1 \in = (\sigma_{m,i} P - h - i, 2P_{RSU_j}^{pub} / h - i, 3)$. C puts $(PsID_i^1, PsID_i^2, \tau h_2)$ into $h-list_2$ and (M_i, TS_i) into $h-list_3$. Finally, C generates beacon $\{PsID_i^1, PsID_i^2, m_i, TS_i, \sigma_{m_i}\}$ and transmits it to A, where $PsID_i = \{PsID_i^1, PsID_i^2\}$. The reply is legitimate sign-oracle since the beacon $\{PsID_i^1, PsID_i^2, m_i, TS_i, \sigma_{m_i}\}$ fulfills the following Equation (2):

$$\begin{aligned} \sigma_{m_i}.P &= h-i, 2\, P_{RSU_j}^{pub} + h-i, 3PsID_i^1 \\ &= h-i, 2\, P_{RSU_j}^{pub} + (\sigma_{m_i} P - h-i, 2P_{RSU_j}^{pub}) = \sigma_{m_i}.P \end{aligned}$$

Output: Finally, A outputs the beacon $\{PsID_i^1, PsID_i^2, m_i, TS_i, \sigma_{m_i}\}$. C checks this message utilizing the Equation 8 as follows:

$$\sigma_{m_i} P = h-i, \quad 2P_{RSU_j}^{pub} + h-i,\ 3PsID_i^1 \tag{8}$$

When 8 does not hold, C finishes the game.

Based on the Cross Lemma, A can result another a the beacon $\{PsID_i^1, PsID_i^2, m_i, TS_i, \sigma_{m_i}^*\}$ that fulfills the Equation 9 as follows:

$$\sigma_{m_i} P = h-i, \quad 2^* P_{RSU_j}^{pub} + h-i,\ 3^* PsID_i^1 \tag{9}$$

Based on Equation 8 and 9, we can obtain

$$\begin{aligned} (\sigma_{m_i} - \sigma_{m_i}^*)P &= \sigma_{m_i} P - \sigma_{m_i}^* P \\ &= (h-i, 2P_{RSU_j}^{pub} + h-i, 3PsID_i^1) \\ &\quad - (h-i, 2^* P_{RSU_j}^{pub} + h-i, 3^* PsID_i^1) \\ &= h-i, 2P_{RSU_j}^{pub} - h-i, 2^* P_{RSU_j}^{pub} \\ &= (h-i, 2-h-i, 2^*) P_{RSU_j}^{pub} \\ &= (h-i, 2-h-i, 2^*) X_{TS}^{RSU_j} P \end{aligned}$$

Hence, we can get $(\sigma_{m_i} - \sigma_{m_i}^*) = (h-i, 2-h-i, 2^*) X_{TS}^{RSU_j}$ mod P. C solve the ECDL problem by computing $(\sigma_{m_i} - \sigma_{m_i}^*).(h-i, 2-h-i, 2^*)^{-1}$. Nevertheless, due to the difficulty of the ECDL problem with probability of non-negligible, the proposed scheme under random oracle model is resistant against an adaptively chosen message attack. Therefore, it is impossible to any attacker to join during mutual authentication process since he/she does not have the ability to solve the ECDL problem. Its mean that authenticated vehicle only can compute its pseudonym and RSU has the ability to reveal identity of vehicle.

B. INFORMAL ANALYSIS

This subsection analyses how our work fulfills the requirements of security and privacy as bellow,

- *Message Integrity and Authentication:*
  When receiving the beacon $\{PsID_i^1, PsID_i^2, m_i, TS_i, \sigma_{m_i}\}$ from signer vehicle, the verifying recipient (vehicle or RSU) checks the correctness of σ_{m_i}. $P = h_2(PsID_i^1 || PsID_i^2 || TS) P_{RSU_j}^{pub} + h_3(PsID_i^1 || PsID_i^2 || m_i || TS)$ $PsID_i^1$ in order to check the signer's authenticity and beacon's validity. Based on Theorem 1 in Section V-A, there is no attacker attacker that could fabricate a valid beacon when the ECDL problem hardness. Therefore, attacker cannot get the TA's private key and computes valid information for authentication and integrity of messages. Hence, the proposed scheme could fulfill the requirements of messages authentication and integrity.
- *Identity Privacy-Preservation:*
  In the signing-message phase, the original identity of vehicle is concealed in the $PsID_i = \{PsID_i^1, PsID_i^2\}$, where $PsID_i^1 = w_i P$ and $PsID_i^2 = OID_i \oplus h_1(w_i P_{RSU_j}^{pub})$. To disclose the original identity OID_i from $PsID_i^2 = OID_i \oplus h_1(w_i P_{RSU_j}^{pub})$, attacker requires to generate $w_i P_{RSU_j}^{pub} = w_i X_{TS}^{RSU_j} P = X_{TS}^{RSU_j} PsID_i^1$. However, this contradicts the CDH problem is hardness. Thus, the proposed scheme can fulfill the requirement of identity privacy preserving.
- *Unlinkability:*
  In the proposed scheme, vehicle selects random value $w_i \in Z_q^*$ in the pseudonym-ID $PsID_i = <PsID_i^1, PsID_i^2>$, where $PsID_i^1 = w_i P$ and $PsID_i^2 = OID_i \oplus h_1(w_i P_{RSU_j}^{pub})$ during signing-message phase. Based on the randomness of $w_i \in Z_q^*$, the vehicle could generate random pseudonym-ID $PsID_i$ and signatures from which the adversary cannot rotate two or more pseudonym-IDs and signatures by the same

signer vehicle. Hence, the proposed scheme could fulfill the requirement of unlinkability.

- *Traceability and Revocation:*
Once an adversary transmits a forged message, i.e. M_i to registered vehicles for leading disruption of the system in the driving environment, thus TA has the ability to revoke attacker after tracing he/she during travail. Assume, a vehicle Ve_j issues a forged message M_i and broadcasts it to a vehicle Ve_i. A report about the bogus message M_i is received by The TA from the vehicle Ve_j. The TA checks the pseudonym-ID $PsID_i$ on message M_i for vehicle Ve_i in the its list of registration. If the pseudonym-ID $PsID_i$ matched, then the TA utilizes RSU's private key $X_{TS}^{RSU_j}$ to disclose the identity ID_{vi} of vehicle Ve_j by calculating as below.

$$\begin{aligned} OID_i &= PsID_i^2 \oplus h_1(X_{TS}^{RSU_j} PsID_i^1) \\ &= OID_i \oplus h_1(w_i P_{RSU_j}^{pub}) \oplus h_1(X_{TS}^{RSU_j} PsID_i^1) \\ &= OID_i \end{aligned} \tag{10}$$

After the node's identity is traced, the TA could revoke its list of database registration, stores it in the Certificate renovation list (CRL). Hence, the proposed scheme could fulfil the requirements of traceability and revocation.

- *Resistance to Replay Attacks:*
Timestamp TS_i is included in the beacon $\{PsID_i^1, PsID_i^2, m_i, TS_i, \sigma_{m_i}\}$ and is also included in the calculation of σ_{m_i}. Therefore, the verifying recipient could discover a replay attack once TS_i no freshness. Hence, the proposed scheme has the ability to resist replay attacks.
- *Resistance to Impersonation Attacks:*
To lunch an impersonation attack, attacker has the ability to compute legitimate the beacon $\{PsID_i^1, PsID_i^2, m_i, TS_i, \sigma_{m_i}\}$, where $\sigma_{m_i} = PK_i + w_i h_3(PsID_i^1 || PsID_i^2 || m_i || TS_i)$. According to Theorem 1, attacker cannot fake beacons. The recipient can verify the beacon validity via checking the above equation correctness. Hence, the proposed scheme could be resisted impersonation attacks in VANETs system.
- *Resistance to Modification Attacks:* In the proposed scheme, each vehicle broadcasts a beacon to other components in VANETs with the format $\{PsID_i^1, PsID_i^2, m_i, TS_i, \sigma_{m_i}\}$. Attacker has the ability to modify the m_i content after capturing it on the open-access communication. In order to provide the beacon integrity, a signature of beacon on m_i is computed as $\sigma_{m_i} = PK_i + w_i h_3(PsID_i^1 || PsID_i^2 || m_i || TS_i)$, where TS_i is the current timestamp and $PsID_i^1 = w_i P$, $PsID_i^2 = OID_i \oplus h_1(w_i P_{RSU_j}^{pub})$ and $w_i \in Z_q^*$. Since the private key $PK_i = X_{TS}^{RSU_j} h_2(PsID_i^1 || PsID_i^2 || TS_i)$ is only known by the certain vehicle, no adversary cannot compute a legitimate signature. In addition, the private key PK_i is updated regularly. Hence, the proposed scheme has the ability to resist modification attacks.
- *Resistance to Man-in-the-Middle Attacks:*
Based on the above analysis for message integrity and authentication, it is not difficult for inferring that verification between signer and recipient is supported by the proposed scheme. Hence, the proposed scheme could be resisted man-in-the-middle attacks.

VI. PERFORMANCE EVALUATION

This section analyzes the computation cost and communication cost of other schemes and the proposed scheme. We implement the proposed utilizing a 2.66 GHz processor Intel(R) Core™ 2 Quad working the operating system of Microsoft Windows™ 7 with 4 GB memory. Schemes based on bilinear pair, we utilize the bilinear pair $y = x^3 + b \bmod q$ with establishing 12 of degree and the q is a number of prime 256-bit. Schemes based on ECC, we utilize an additive group G computed by a point p on the elliptic curve of $secp256r1$ with order q for achieving the 128 bits level of security in which p and q are two numbers of prime 256-bit.

TABLE 2. Performance Cost of Several Cryptographic Operations.

Notations.	The description of operations	Time(ms)
T^{BP}	The performance cost of operation of BP	5.811
T_{SM}^{BP}	The performance cost of operation of scalar multiplication related to BP	1.5654
T_{PA}^{BP}	The performance cost of operation of point addition related to BP	0.0106
T^{MTP}	The performance cost of map-to-point hash function	4.1724
T_{SM}^{ECC}	The performance cost of operation of scalar multiplication regrading ECC	0.6718
T_{PA}^{ECC}	The performance cost of operation of point addition regrading ECC	0.0031
T^h	The performance cost of general hash function operation	0.001

A. COMPUTATION OVERHEAD

In this article, we utilize MIRACL [32] that widely utilized cryptographic libraries, is used in our experiment since it provides the easy ability to measure the cost of computation related to performance cost of many operations of cryptographic, as presented in Table 2. Let *SMP*, *SVMP* and *BVMP* indicate the signing message phase, the single verifying-message phase, and the batch verifying-messages phase, respectively.

In the *SMP* of Al-shareeda *et al.* [18] scheme, the node requires to carry out three operations of scalar multiplication regarding the ECC, two cryptographic hash functions and one addition operation. Therefore, the computation cost of this phase is $3\ T_{SM}^{ECC} + 1\ T_{PA}^{ECC} + 2\ T^h \approx 2.0205$ ms. In the *SVMP*, the vehicle requires to execute four scalar multiplication operations related to the ECC, two cryptographic hash function operations and one addition operation. Hence, the

TABLE 3. A Comparative Summary of the Computation Overhead.

Schemes	SMP(ms)	$SVMP$(ms)	$BVMP$(ms)
He et al. [16]	$3T_{SM}^{ECC} + 3T^h \approx 2.0184$	$5T_{SM}^{ECC} + 1T_{PA}^{ECC} + 2T^h \approx 3.3641$	$(2+3n)T_{SM}^{ECC} + (2n)T_{PA}^{ECC} + (2n)T^h \approx 2.0236n + 1.3405$
Li et al. [17]	$2T_{SM}^{ECC} + 2T^h \approx 1.3456$	$4T_{SM}^{ECC} + 1T_{PA}^{ECC} + 2T^h \approx 2.6923$	$(2+2n)T_{SM}^{ECC} + (2n)T_{PA}^{ECC} + (2n)T^h \approx 1.3518n + 1.3405$
Al-shareeda et al. [18]	$3T_{SM}^{ECC} + 1T_{PA}^{ECC} + 2T^h \approx 2.0205$	$4T_{SM}^{ECC} + 1T_{PA}^{ECC} + 2T^h \approx 2.6923$	$(2+2n)T_{SM}^{ECC} + (2n-1)T_{PA}^{ECC} + (2n)T^h \approx 1.3518n + 1.3405$
Cui et al. [22]	$2T_{SM}^{ECC} + 1T_{PA}^{ECC} + 2T^h \approx 1.3487$	$4T_{SM}^{ECC} + 1T_{PA}^{ECC} + 7T^h \approx 2.0255$	$(4n+2)T_{SM}^{ECC} + (n+1)T_{PA}^{ECC} + (7n)T^h \approx 0.8149n + 1.3467$
Bayat et al. [24]	$5T^{BP} + 1T^{MTP} + 2T^h \approx 4.1724$	$3T^{BP} + T^{MTP} + 1T_{SM}^{BP} + 1T^h \approx 4.1724$	$3T^{BP} + (n)T^{MTP} + (n)T_{SM}^{BP} + (n)T^h \approx 5.7378n + 17.4333$
Al-shareeda et al. [25]	$2T_{SM}^{ECC} + 1T_{PA}^{ECC} + 4T^h \approx 1.3507$	$4T_{SM}^{ECC} + 1T_{PA}^{ECC} + 2T^h \approx 2.6923$	$(2n+3)T_{SM}^{ECC} + (n+1)T_{PA}^{ECC} + (2n)T^h \approx 1.3405n + 2.0236$
Proposed scheme	$2T_{SM}^{ECC} + 2T^h \approx 1.3456$	$3T_{SM}^{ECC} + 1T_{PA}^{ECC} + 2T^h \approx 2.0205$	$(n+2)T_{SM}^{ECC} + (n)T_{PA}^{ECC} + (2n)T^h \approx 0.6769n$

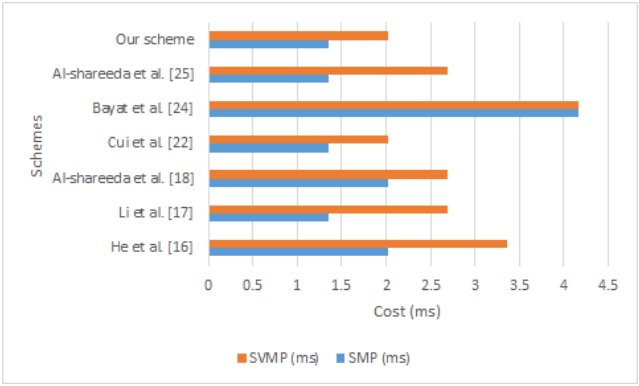

FIGURE 2. Computation cost.

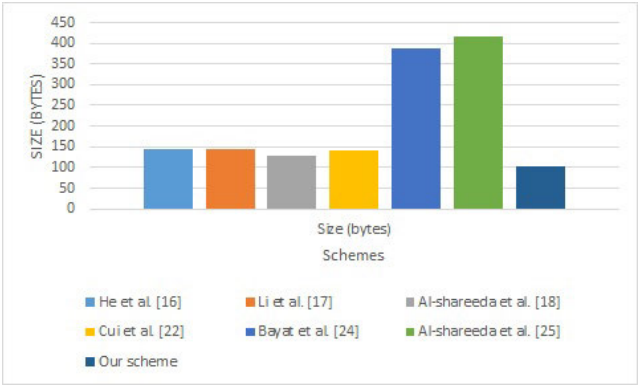

FIGURE 3. Communication cost.

computation cost of this phase is $4\ T_{SM}^{ECC} + 1\ T_{PA}^{ECC} + 2\ T^h \approx 2.6923$ ms. In the *BVMP*, the vehicle requires to carry out (2 + 2n) operations of scalar multiplication regarding the ECC, (2n) cryptographic hash functions and (2n − 1) operations of addition. Therefore, the computation cost of this phase is $(2+2n)T_{SM}^{ECC} + (2n-1)T_{PA}^{ECC} + (2n)T^h \approx 1.3518$ n + 1.3405 ms.

In the *SMP* of the proposed scheme, the vehicle requires to execute two operations of scalar multiplication regarding the ECC, two cryptographic hash functions and one addition operation. Therefore, the computation cost of this phase is $2\ T_{SM}^{ECC} + 1\ T_{PA}^{ECC} + 2\ T^h \approx 1.3456$ ms. In the *SVMP*, the vehicle requires to execute three scalar multiplication operations, two cryptographic hash function operations and one addition operation. Therefore, the computation cost of this phase is $3\ T_{SM}^{ECC} + 2\ T^h \approx 2.0205$ ms. In the *BVMP*, the vehicle requires to execute (n) operations of scalar multiplication, (2n) cryptographic hash functions and (2n − 1) addition operations. Thus, the computation cost of this *BVMP* is $(n)T_{SM}^{ECC} + (2n-1)T_{PA}^{ECC} + (2n)T^h \approx 0.6769$ n ms.

Similarity, the computation cost of the proposed scheme (i.e. *SMP*, *SVMP* and *BVMP*) are lower than those in [16], [17], [22], [24], [25] respectively. Table 3 lists a summary of the computation overhead. Figure 2 shows the computation cost of the proposed scheme and the existing schemes.

TABLE 4. A Comparative Summary of the Communication Overhead.

Schemes	Broadcasting one message	Broadcasting of n messages
He et al. [16]	144 bytes	144 n bytes
Li et al. [17]	144 bytes	144 n bytes
Al-shareeda et al. [18]	128 bytes	128 n bytes
Cui et al. [22]	140 bytes	140 n bytes
Bayat et al. [24]	388 bytes	388 n bytes
Al-shareeda et al. [25]	416 bytes	416 n bytes
Proposed scheme	104 bytes	104 n bytes

B. COMMUNICATION OVERHEAD

Consider the size of elements in G and G_1 are 40 bytes and 128 bytes, respectively. Furthermore, consider the timestamp size, hash function size and item in Z_q^* be 4 bytes, 20 bytes and 20 bytes respectively.

The beacon size in the Al-shareeda *et al.* scheme [18], is $(40 * 3 + 4) = 128$ bytes, where the beacon contains three items in $\{PsID_i^1, PsID_i^2, \sigma_i \in G\}$ and one timestamp. In the proposed scheme, the node broadcasts a beacons with size $(40 * 2 + 20 + 4) = 104$ bytes, where the beacon contains two items in $\{PsID_i^1, PsID_i^2 \in G\}$, one item $\{\sigma_m \in Z_q\}$, and one timestamp.

Similarity, the communication cost of the proposed scheme is lower than those in [16], [17], [22], [24], [25] respectively (see Figure 3). Table 4 lists a summary of the communication overhead.

VII. CONCLUSION AND FUTURE WORK

We have proposed a lightweight authentication with conditional privacy-preserving scheme that supports batch verification process in this article. The proposed scheme combines TPD based with RSU based schemes. The primary concept of the proposed scheme is to preload the initial public parameters and keys of the system in each TPD of RSU rather than of TPD of OBU on the vehicle. This proposed is based on ECC and secure hash function. The proposed scheme can satisfy the requirements of security and privacy and resists the common security attacks as shown in section of security analysis. Furthermore, due to the difficulty of the ECDL problem with the probability of non-negligible, the proposed scheme under the random oracle model is resistant against an adaptively chosen message attack. The result compared with existing schemes indicate a better performance evaluation in terms of computation and communication costs. In the future work, the mutual authentication process could be carried out using rules set of Burrows–Abadi–Needham logic (BAN logic) as well as simulation platforms, such as OMNET++ and SUMO to simulate VANET networks and road traffic, respectively.

REFERENCES

[1] M. A. Al-Shareeda, M. Anbar, I. H. Hasbullah, and S. Manickam, "Survey of authentication and privacy schemes in vehicular ad hoc networks," *IEEE Sensors J.*, vol. 21, no. 2, pp. 2422–2433, Jan. 2021.

[2] I. Ali, A. Hassan, and F. Li, "Authentication and privacy schemes for vehicular ad hoc networks (VANETs): A survey," *Veh. Commun.*, vol. 16, pp. 45–61, Apr. 2019.

[3] 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.

[4] M. A. Al-shareeda, M. Anbar, S. Manickam, and I. H. Hasbullah, "An efficient identity-based conditional privacy-preserving authentication scheme for secure communication in a vehicular ad hoc network," *Symmetry*, vol. 12, no. 10, p. 1687, Oct. 2020.

[5] M. A. Al-Shareeda, M. Anbar, M. A. Alazzawi, S. Manickam, and A. S. Al-Hiti, "LSWBVM: A lightweight security without using batch verification method scheme for a vehicle ad hoc network," *IEEE Access*, vol. 8, pp. 170507–170518, 2020.

[6] Sheikh, Liang, and Wang, "A survey of security services, attacks, and applications for vehicular ad hoc networks (VANETs)," *Sensors*, vol. 19, no. 16, p. 3589, Aug. 2019.

[7] X. Yang, X. Yi, I. Khalil, Y. Zeng, X. Huang, S. Nepal, X. Yang, and H. Cui, "A lightweight authentication scheme for vehicular ad hoc networks based on MSR," *Veh. Commun.*, vol. 15, pp. 16–27, Jan. 2019.

[8] S. O. Ogundoyin, "An autonomous lightweight conditional privacy-preserving authentication scheme with provable security for vehicular ad-hoc networks," *Int. J. Comput. Appl.*, vol. 42, no. 2, pp. 196–211, Feb. 2020.

[9] U. Rajput, F. Abbas, and H. Oh, "A hierarchical privacy preserving pseudonymous authentication protocol for VANET," *IEEE Access*, vol. 4, pp. 7770–7784, 2016.

[10] P. Cincilla, O. Hicham, and B. Charles, "Vehicular PKI scalability-consistency trade-offs in large scale distributed scenarios," in *Proc. IEEE Veh. Netw. Conf. (VNC)*, Dec. 2016, pp. 1–8.

[11] A. Joshi, P. Gaonkar, and J. Bapat, "A reliable and secure approach for efficient Car-to-Car communication in intelligent transportation systems," in *Proc. Int. Conf. Wireless Commun., Signal Process. Netw. (WiSPNET)*, Mar. 2017, pp. 1617–1620.

[12] M. Asghar, R. R. M. Doss, and L. Pan, "A scalable and efficient PKI based authentication protocol for VANETs," in *Proc. 28th Int. Telecommun. Netw. Appl. Conf. (ITNAC)*, Nov. 2018, pp. 1–3.

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

[14] 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.

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

[16] 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.

[17] J. Li, K.-K.-R. Choo, W. Zhang, S. Kumari, J. J. P. C. Rodrigues, M. K. Khan, and D. Hogrefe, "EPA-CPPA: An efficient, provably-secure and anonymous conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *Veh. Commun.*, vol. 13, pp. 104–113, Jul. 2018.

[18] M. A. Al-shareeda, M. Anbar, S. Manickam, I. H. Hasbullah, N. Abdullah, M. M. Hamdi, and A. S. Al-Hiti, "NE-CPPA: A new and efficient conditional privacy-preserving authentication scheme for vehicular ad hoc networks (VANETs)," *Appl. Math*, vol. 14, no. 6, pp. 1–10, 2020.

[19] 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.

[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] M. Azees, P. Vijayakumar, and L. J. Deboarh, "EAAP: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 9, pp. 2467–2476, Sep. 2017.

[22] 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.

[23] J. Zhang, J. Cui, H. Zhong, Z. Chen, and L. Liu, "PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks," *IEEE Trans. Depend. Sec. Comput.*, early access, Mar. 11, 2019, doi: 10.1109/TDSC.2019.2904274.

[24] 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.

[25] M. A. Al-Shareeda, M. Anbar, S. Manickam, and A. A. Yassin, "VPPCS: VANET-based privacy-preserving communication scheme," *IEEE Access*, vol. 8, pp. 150914–150928, 2020.

[26] L. Wei, J. Cui, Y. Xu, J. Cheng, and H. Zhong, "Secure and lightweight conditional privacy-preserving authentication for securing traffic emergency messages in VANETs," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 1681–1695, 2021.

[27] M. A. Al-shareeda, M. Anbar, I. H. Hasbullah, S. Manickam, N. Abdullah, and M. M. Hamdi, "Review of prevention schemes for replay attack in vehicular ad hoc networks (VANETs)," in *Proc. IEEE 3rd Int. Conf. Inf. Commun. Signal Process. (ICICSP)*, Sep. 2020, pp. 394–398.

[28] M. A. Al-shareeda, M. Anbar, S. Manickam, and I. H. Hasbullah, "Review of prevention schemes for modification attack in vehicular ad hoc networks," *Int. J. Eng. Manage. Res.*, vol. 10, no. 3, pp. 149–152, Jun. 2020.

[29] F. Ahmad, A. Adnane, V. Franqueira, F. Kurugollu, and L. Liu, "Man-in-the-middle attacks in vehicular ad-hoc networks: Evaluating the impact of attackers' strategies," *Sensors*, vol. 18, no. 11, p. 4040, Nov. 2018.

[30] M. A. Al-shareeda, M. Anbar, S. Manickam, and I. H. Hasbullah, "Review of prevention schemes for man-in-the-middle (MITM) attack in vehicular ad hoc networks," *Int. J. Eng. Manage. Res.*, vol. 10, no. 3, pp. 153–158, Jun. 2020.

[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.

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

JALAWI SULAIMAN ALSHUDUKHI received the B.Sc. degree in computer science from the University of Ha'il, Saudi Arabia, in 2002, the M.Sc. degree in computer networks from La Trobe University, Australia, in 2010, and the Ph.D. degree from Oxford Brookes University, U.K., in 2016. He is currently an Assistance Professor with the College of Computer Science and Engineering, University of Ha'il. His current research interests include wireless sensor networks, energy management and propagation models, WSNs MAC protocol, and intelligent transportation systems.

ZEYAD GHALEB AL-MEKHLAFI received the B.Sc. degree in computer science from the University of Science and Technology, Yemen, in 2002, the M.Sc. degree in computer science from the Department of Communication Technology and Network, Universiti National Malaysia (UKM), in 2011, and the Ph.D. degree from the Department of Communication Technology and Network, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, in 2018. He is currently a Lecturer with the University of Ha'il, where he is also an Assistance Professor with the Faculty of Computer Science and Engineering. His current research interests include wireless sensor networks, energy management and control for wireless networks, time synchronization, bio-inspired mechanisms, and emerging wireless technologies standard.

BADIEA ABDULKAREM MOHAMMED (Member, IEEE) received the B.Sc. degree in computer science from the University of Babylon, Iraq, in 2002, the M.Tech. degree in computer science from the University of Hyderabad, India, in 2007, and the Ph.D. degree from Universiti Sains Malaysia, Malaysia, in 2018. He is currently an Assistant Professor with the College of Computer Science and Engineering, University of Ha'il, Saudi Arabia. He is also an Assistant Professor with Hodeidah University, Yemen. His research interests include wireless networks, mobile networks, vehicle networks, WSN, and image processing. In his research area, he has published many articles in reputed journals and conferences.