IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received December 14, 2020, accepted December 16, 2020, date of publication December 18, 2020,
date of current version December 31, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3045940

An Efficient Conditional Privacy-Preserving Authentication Scheme for the Prevention of Side-Channel Attacks in Vehicular Ad Hoc Networks

JALAWI SULAIMAN ALSHUDUKHI, BADIEA ABDULKAREM MOHAMMED, (Member, IEEE), AND ZEYAD GHALEB AL-MEKHLAFI, (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: Badiea Abdulkarem Mohammed (b.alshaibani@uoh.edu.sa)

ABSTRACT Several group signature or identity schemes have been proposed for addressing the issues of security in a vehicular ad hoc network (VANET). Nonetheless, none of these schemes suitably cope with the performance efficient during the signing and verifying safety-messages. Furthermore, adversaries could acquire sensitive data stored in a tamper-proof device (TPD) by utilizing side-channel attacks. An efficient conditional privacy-preserving authentication scheme is proposed for the prevention of side-channel attacks and reducing the performance efficiency of the system in this paper. Moreover, to resist side-channel attacks, critical data stored in the TPD is frequently and periodically updated. Lastly, due to our work employs the one-way hash function and the elliptic curve cryptography, its performance evaluation has lower computation and communication cost compared to other schemes.

INDEX TERMS Identity-based cryptography, side-channel attack, privacy-preserving, vehicular ad-hoc networks (VANETs).

I. INTRODUCTION

Each year, more than 1 million person are caused to affect by a road incident. The harm of driving environment is the ninth causing of mortality universally and afford a loss at more than 2% or 1 USD trillion of the Gross Domestic Product (GDP) world [1], [2]. Besides, congestion waste massive fuel and time amount.

Intelligent transport systems (ITSs) play a highly significant role in the movement of the new human being in the digital world recently. To enhance the traffic road of vehicular in the future, ITSs provide innovative and comprehensive applications for controlling these unpleasant events [3]. It is being constructed for building smart vehicle via the fast development of wireless communication technology [4], [5]. New vehicle telcos and manufacturers have introduced the fact that wireless tools will be an integral part of each vehicle, allowing them for communicating with other vehicles and with infrastructures of road. This vehicle forms a specific kind of ad hoc network, where the vehicle is considered the network's node. Such networks are known as vehicular ad hoc networks (VANETs) that are a type of the mobile ad hoc networks (MANETs) that utilizes the technology of wireless for proximity and communication of vehicle for fixing infrastructures [6].

Communications of VANET are classified as either Vehicle-to-Infrastructure (V2I) or Vehicle-to-Vehicle (V2V). With these communications, each vehicle broadcasts a periodic safety-messages with their position, traffic events, speed and heading. Any vehicle within the coverage area, whether legal or not, will receive these safety-messages since the broadcasting in an openness communication of VANET. Nonetheless, this will also permit adversaries to change, alter and replay these safety-messages and broadcast them in the system. The broadcast of these changed and forged safety-messages could cause for situations such as road accidents, traffic disruption, etc., and therefore justify the call for modifies to be made for messaging security. Before they

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

become practical, the security issues in VANETs requires to be carefully addressed. In this paper, there are some following contributions for summarizing our proposed scheme,

- First, an efficient conditional privacy-preserving authentication scheme for securing vehicle-to-vehicle (V2V) and vehicle to infrastructure (V2I) communications. Besides, the proposed scheme shows that satisfies the requirements of security of design goal in VANETs.
- Second, a proposed that resists side-channel attacks by regularly updating the critical data stored in the tamper-proof device (TPD) of vehicle.
- Finally, a proposed is more efficient than existing schemes and appropriate for an area with high traffic density by using the one-way hash function and the elliptic curve cryptography (ECC).

The remainder of this paper is organized as follows: Section II deals with 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 presents the performance evaluation. Conclusions of the proposed scheme are shown in Section VII.

II. RELATED WORK

In this section, we review and discuss the related schemes since VANETs have suffered from issues of mutual authentication and conditional privacy-preserving. Existing scheme regarding security and privacy is commonly classified into two main categories as follows,

A. GROUP-SIGNATURE BASED SCHEMES

The core fundamental of group-signature based schemes is that each group member could be able for signing safety-message anonymously on behalf of the full group. The Chaum and van Heyst were first introduced group-signature [7]. Lin *et al.* [8] introduced a security scheme based on the group signature for securing V2V communication in vehicular systems. This scheme provides security and privacy without inducing the managing overhead regarding to multiple certificates at sides of the membership manager (MM). Zhang *et al.* [9] introduced a privacy-preserving scheme relies on a practical secure for applications of value-added. In their scheme, the vehicle only needs a member key for generating verifier-local revocation without violating the drivers' privacy. Shao *et al.* [10] designed a threshold anonymous authentication approach to address issues of security and privacy in VANETs. This scheme combines between the model of decentralized group and method of threshold authentication for obtaining threshold authentication. Lim *et al.* [11] introduced a key distribution scheme to propose secure and scalable by utilizing the domain concept with a number of RSUs for group signature-based authentication.

However, the main limitation of group-signature based schemes is growing the Certificate revocation list (CRL) size since the multiple revoked vehicle is increased. In addition, the vehicle uses two bilinear pairing operations for checking on CRL operation, which cause increasing of the verification computation overhead.

B. IDENTITY BASED SCHEMES

In order to address the limitation of group-signature based schemes, many scholars have proposed identity-based schemes. The core fundamental of identity-based schemes is that the identity information extracted by the public key, while TA computes the private key. Shamir has first proposed an identity in 1984 [18]. Zhang *et al.* [19], [20] conducts a security and privacy scheme based on bilinear pairing by supporting batch authentication process which allowing a large number of safety-messages received by rest of components to be verified simultaneously in VANETs. Lee and Lai [21] and Chim *et al.* [22] indicated that the proposed schemes by [19], [20] have drawbacks due to an OBU could utilize a false identity for eliminating the requirement of traceability. Besides, [19], [20] cannot withstand impersonation attack and replay attack. Jianhong *et al.* [23] indicates some limitations of security in the scheme of [21], for example that it cannot satisfy the requirements of non-repudiation and traceability and cannot withstands replay attack. To address the flaws in scheme of [21], a secure identity based scheme was conducted by Jianhong *et al.* [23]. Bayat *et al.* [14] pointed out the authentication scheme of Lee and Lai [21] have insecure against the attacks of impersonation. Therefore, they proposed an enhanced authentication scheme. He *et al.* [15] introduced an identity-based security and privacy scheme for securing communication in vehicular systems. This scheme does not utilization a bilinear pair in the process of signature verification since it is among the finest operations of time-consuming in cryptography. Instead, in their work, elliptic curve cryptography (ECC) is based on signing and verifying safety-messages. Azees *et al.* [24] suggested an authentication scheme to avert attackers entering into the V2V and V2I communications. Besides, the proposed scheme supports a conditional tracking scheme to trace the malicious components in the VANETs. Zhang *et al.* [12] proposed an authentication with conditional Privacy-preserving scheme based on chinese remainder theorem (CRT) in VANETs. This scheme utilizing fingerprints rather than a password and genuine identity for identity verification. Cui *et al.* [13] proposed an authentication with conditional Privacy-preserving scheme based on the binary search and cuckoo filter methods to satisfy the top success rate in the batch verification method. Bayat *et al.* [25] suggested an RSU based scheme in which a private key of TA is equipped to the TPD on RSUs since the communication channels between the TAs and RSUs are more faster and secure compared to put a private key to each OBUs. Al-shareeda *et al.* [16] proposed lightweight security without using batch verification method (LSWBVM) scheme for making single verification has the ability a large number of safety-messages during driving broadcasting. However, this scheme is vulnerable from various security attacks

TABLE 1. Summarizes the recent existing identity based schemes with their techniques applied, advantages, and limitations.

Schemes	Techniques	Advantages	Limitations
Zhang et al. [12]	ECC	uses chinese remainder theorem (CRT). Besides, its using fingerprints rather than a password and genuine identity.	High performance efficiency.
Cui et al. [13]	ECC	Uses binary search and cuckoo filter methods	V2V communication is only supported. Vehicle authenticates messages by helping RSU. Delay in the verification process.
Bayat et al. [14]	Bilinear pair	Address security limitations	Its vulnerable from side-channel attacks. Revocation requirement is not satisfied. complexes time-consuming operations are used.
He et al. [15]	ECC	ECC used instead of bilinear pair operations.	Its vulnerable from side-channel attacks. Besides, the revocation requirement is not satisfied.
Al-shareeda et al. [16]	ECC	Map-to-point function is totally ignored. Besides, its work without using batch verification.	Its vulnerable from various security attacks. Besides, its not satisfying authentication and integrity requirements in vehicular systems.
Al-shareeda et al. [17]	ECC	Complexes time-consuming operations are not included.	Its vulnerable from side-channel attacks. Besides, the revocation requirement is not satisfied.

such as impersonation and modification attacks due to the verifying vehicle uses only a one-way hash function for signature verification. Also, its vulnerable to replay attacks since the timestamp is not included on the safety-message tuple. Besides, this scheme is not satisfying authentication and integrity requirements in vehicular systems. Besides, it is suspect from side-channel attack due to the vehicle's identity stored on TPD is not update for a long time. Also, Al-shareeda *et al.* [17] suggested a new and efficient conditional privacy-preserving authentication (NE-CPPA) scheme for securing the V2V and V2I communications in vehicular systems. This scheme computes the private key of the system by TA and preloads in the TPD that assumed not to be compromised with any adversary. Nevertheless, an adversary also could obtain some data saved in the TPD through the attack of side-channel. When the TA's private key is obtained by the adversary, the vehicular system will be disturbed.

Table 1 summarizes the recent existing identity based schemes with their techniques applied, advantages, and limitations that proposed a mutual authentication and conditional privacy-preserving in VANETs. To overcome the aforementioned issues arising in the VANETs, we will propose an efficient conditional privacy-preserving authentication scheme for prevention of side-channel attacks, furthermore, by adding update parameter stored phase in our work for periodically changing in the TPD of the vehicle for preventing malicious adversaries from getting critical information via side-channel attacks for collapsing the VANETs system. Besides, the proposed scheme utilizes operations of ECC rather than operations of bilinear pairing; therefore, the proposed has lower performance efficiency regarding computation and communication cost compared others schemes.

III. PRELIMINARIES

In this section, we first define the structure of system model; this is followed by a presentation of the design goals in terms of security requirements and finally, the security attacks specified in this paper are defined. The major notations utilized in the proposed scheme are presented in Table 2.

TABLE 2. Definition of notations in this paper.

Notation	Descriptions
OBU	On-border unit
RSU	Roadside unit
TA	Trusted authority
TPD	Tamper prof device
Z_p^*	is the symbol used to represent integers
k, Pub	The private and public keys of the TA
h_1, h_2, h_3	Three function of one-way hash
ID_i, ID_{RSU_j}	The vehicle and the RSU identity
Pdm	Pseudonym of vehicle
SP_{vi}	Sort period of Pdm
z, r, w	Random integer
$PsID_i$	Pseudo-ID of vehicle
SK_i	Signature key of vehicle
PW_i	Password of driver
$\oplus$	XOR operator
$\|\|$	Operation of concatenation

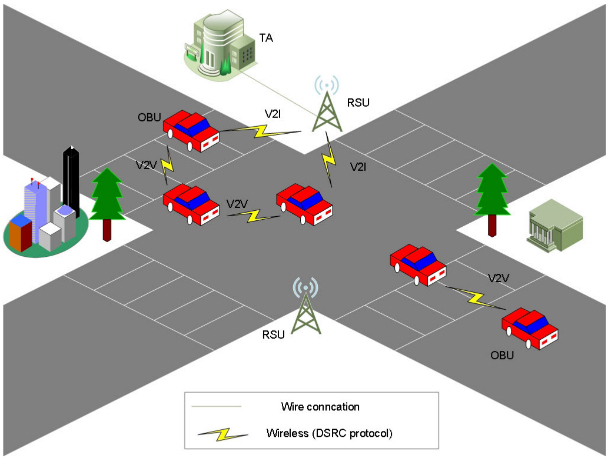


FIGURE 1. The structure of system model in VANETs.

A. SYSTEM MODEL

The proposed scheme's system model is included of three components, OBU, RSU and TA, as shown in Figure 1.

- OBU:
  Vehicles in VANET are equipped with an On-Board Unit (OBU) which allow the vehicles for processing,

receiving and broadcasting safety-messages. OBUs are fitted with a tamper-proof device (TPD) that using to save critical data.

- RSU:
  Roadside unit (RSU) is a wireless device located to the road as an infrastructure node. The RSU links with the TA by wired channel and links with vehicles in the wireless channel.
- TA:
  Trusted authority (TA) has high computation and communication resources. The responsibility of TA generates the system's public parameters and pseudo-ID for each vehicle.

B. DESIGN GOALS

In order to fulfil the security of V2V and V2I communications in the system, the proposed scheme should be to satisfy requirements of security, as follows.

- Integrity and authentication:
  The wireless components in VANETs must have the ability to determine any modification of the received safety-messages and must able to validate received safety-messages and authenticate nodes for ensuring the security of communications.
- Identity privacy preservation: An adversary must able to disclose the vehicle's identity by capturing a multiple safety-messages sent by it. Thus, the identity of the vehicle maintains anonymous to other legitimate and illegitimate vehicles for ensuring the driver's privacy.
- Traceability and revocation: The TA must be capable for disclosing the identity of the vehicle from its safety-messages to prevent malicious vehicles from denying their trust for the system's disruption by sending forge safety-messages to other authenticated vehicles.

C. SECURITY ATTACKS

Its easy by adversaries to be lunch certain security attacks since the nature openness of VANETs communication. In this subsection, we briefly present some vulnerabilities with the capabilities of an adversary in the VANETs.

- Replay attacks.
  The aim of misbehaving vehicles is to replay the old issued valid signature to the receiver for creating the illusion that accidents are happening.
- Modification attacks.
  The aim of misbehaving vehicles is to change the authentic safety-messages and send to other nodes [26]. For example, a malicious vehicle could feed forge messages to nearby vehicles. Thus, the verifying recipient cannot be executed with changed messages.
- Impersonation attacks.
  The aim of misbehaving vehicles is to impersonate a registered vehicle and transmit a proper safety-message to other vehicles in which the attacker attempts to masquerade as a registered vehicle.
- Man-In-The-Middle attacks.
  The aim of misbehaving vehicles is to implement information sniffing and tampering with intercept two communication sides [27], [28].
- Side-channel attacks.
  The aim of misbehaving vehicles is to obtain sensitive data stored in the TPD by utilizing a side-channel attack. When the misbehaving vehicles get the TA's private key, the structure of the system will collapse.

After the TA calculates the initial public parameters, it preloads them to the RSUs and OBUs in advance. Via the steps of mutual authentication, the vehicle must execute authenticating itself with the system for exchanging safety-message based on the RSU' parameters. Thus, the attacker does not have the ability to authorize access to the coverage region. After the vehicle is considered as to be registered vehicle, it calculates its signature of the message and the verifier will then check these signature.

We propose an efficient conditional privacy-preserving authentication scheme for prevention of side-channel attacks for ensuring secure communication in VANETs. The five phases included in the proposed scheme is presented as follows: phases of system initialization, mutual authentication, signing safety-message, verifying safety-message and update parameters. The phases of the proposed scheme are visualized in Figure 2.

D. PHASE OF SYSTEM INITIALIZATION

The phase of system initialization is included in the following subsection,

1) TA INITIALIZATION

In order to compute the initial public parameters of the system, the TA should execute the following steps.

- Two numbers of large prime q,p are chosen by TA, the generator P of an additive group G, which includes of each point on the non-singular with the order q by identifying elliptic curve E $(y^2 = x^3 + ax + b \bmod p$, where a, b $\in F_p)$.
- A random value $k \in Z_q^*$ are chosen by TA as TA's private key and then calculates $Pub = kP$ to be its corresponding public key.
- Lastly, three functions of one-way hash h_1, h_2 and h_3 are chosen by TA, where $-h_1 : G \to Z_q^*$, $-h_2 : \{0, 1\}^* \times \{0, 1\}^* \times G \to Z_q^*$ and$-h_3 : \{0, 1\}^* \to Z_q^*$.

IV. THE PROPOSED SCHEME

2) RSU AND VEHICLE REGISTRATION

In order to register the RSU and the vehicles at the TA, the following steps should be executed,

- Once the TA receives RSU's identity ID_{RSU_j}, the TA verifies the RSU's validity.
- The private key k is stored by the TA on the RSU's TPD.

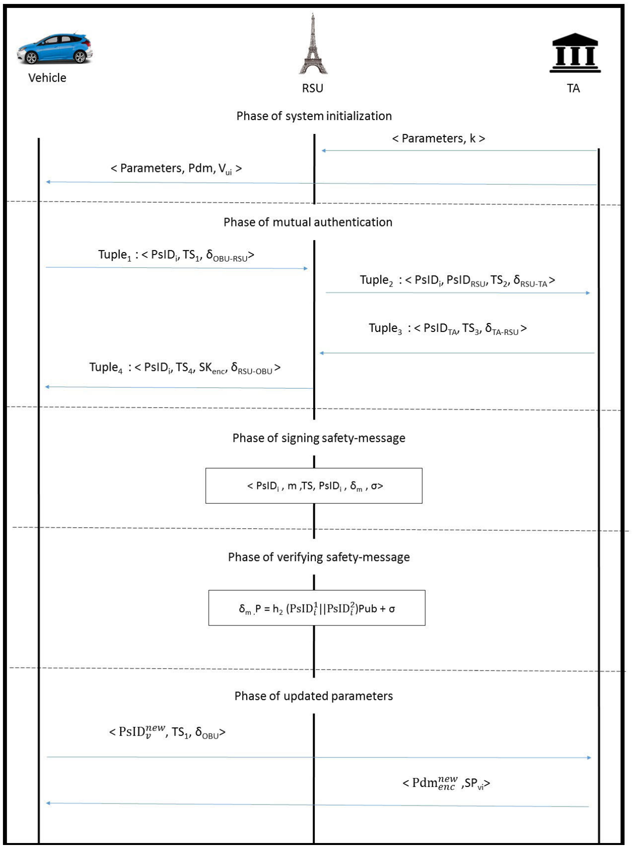

Vehicle
RSU
TA
Phase of system initialization
< Parameters, k >
< Parameters, Pdm, V_{ui} >
Phase of mutual authentication
$Tuple_1$: < $PsID_i$, TS_1, $\delta_{OBU\text{-}RSU}$>
$Tuple_2$: < $PsID_i$, $PsID_{RSU}$, TS_2, $\delta_{RSU\text{-}TA}$ >
$Tuple_3$: < $PsID_{TA}$, TS_3, $\delta_{TA\text{-}RSU}$ >
$Tuple_4$: < $PsID_i$, TS_4, SK_{enc}, $\delta_{RSU\text{-}OBU}$ >
Phase of signing safety-message
< $PsID_i$, m ,TS, $PsID_i$, δ_m , σ>
Phase of verifying safety-message
$\delta_m . P = h_2\ (PsID_i^1||PsID_i^2)Pub + \sigma$
Phase of updated parameters
< $PsID_v^{new}$, TS_1, δ_{OBU}>
< Pdm_{enc}^{new} ,SP_{vi}>

FIGURE 2. Sequence diagram of the proposed scheme.

- Once the driver submits identity ID_i and password PW_i via secure communication, the TA checks the driver's validity.
- The TA generates the pseudonym $Pdm = h_3(ID_i \| SP_{vi})$ after it verifies the ID_i validity, where V_{vi} is a short period.
- The TA preloads $<Pdm, V_{vi}>$ and k via a secure channel into the TPD of the vehicle and each RSU, respectively.
- Initial public parameters of the system $\psi = \{p, q, a, b, P, Pub, h_1, h_2, h_3\}$ are preloaded by TA in each vehicle's OBU and RSU.

A. PHASE OF MUTUAL AUTHENTICATION

The vehicle reaches in the RSU's communication range and performs the mutual authentication before it sends safety-messages to the nearby RSU or neighbour vehicle. Once the signature key SK received by the vehicle from the RSU, the vehicle's authenticity is considered as a registered, thus, this vehicle could broadcast safety-messages to the nearby RSU or neighbour vehicle. Figure 3 shows the top-level mutual authentication process of the proposed scheme. The following steps are utilized to perform the process of this phase.

- $OBU - TO - RSU$: Once the vehicle selects random value $w \in Z_q^*$, it generates its pseudo-ID $PsID_i = {<}PsID_i^1, PsID_i^2{>}$ as follows:
  $PsID_i^1 = wP$
  $PsID_i^2 = Pdm \oplus h_1(wPub)$
  Then, the vehicle transmits $Tuple_1$ to the RSU, where $Tuple_1 = \{PsID_i,\ TS_1\ \ \delta_{OBU-RSU}\}$, $\delta_{OBU-RSU} = h_3(PsID_i||TS_1||Pdm)$ and TS_1 is timestamp.
- $RSU - TO - TA$: Once the $Tuple_1$ is received by RSU from the OBU, RSU start to check the TS_1 freshness. Each timestamp is checks as follows. Subtract the present time TS with The TS_1 for judging the $Tuple_1$ freshness. If the result is less than the threshold of time, then TS_1 is fresh. Otherwise, the safety-message is dropped. Then, it calculates the $Pdm = PsID_i^2 \oplus h_1(kPsID_i^1)$ and verifies whether $\delta_{OBU-RSU} \overset{?}{=} h_3(PsID_i||Pdm||TS_1)$. The RSU rejects the $Tuple_1$ when it is not ok; otherwise, it selects random value $z \in Z_q^*$. It generates its pseudo-ID $PsID_{RSU_j} = {<}PsID_{RSU_j}^1, PsID_{RSU_j}^2{>}$ as bellow:
  $PsID_{RSU_j}^1 = zP$
  $PsID_{RSU_j}^2 = ID_{RSU_j} \oplus h_1(zPub)$
  Then, the RSU transmits $Tuple_2$ to TA, where $Tuple_2 = \{PsID_i,\ PsID_{RSU_j}, TS_2, \delta_{RSU-TA}\}$ and $\delta_{RSU-TA} = h_3(ID_{RSU_j}||Pdm||TS_2)$.
- $TA - TO - RSU$: Once the $Tuple_2$ is received by TA from the RSU, it first checks the TS_2 freshness. If TS_2 is fresh, then the TA does not reject the safety-message. Otherwise, the $Tuple_2$ is dropped. TA then calculates the $ID_i = PsID_i^2 \oplus h_1(kPsID_i^1)$ and $ID_{RSU_j} = PsID_{RSU_j}^2 \oplus h_1(kPsID_{RSU_j}^1)$ from $PsID_i$ and $PsID_{RSU_j}$, respectively. Then it verifies for confirming the $\delta_{RSU-TA} \overset{?}{=} h_3(Pdm||ID_{RSU_j}||TS_2)$. If is not ok, the TA rejects the $Tuple_2$; otherwise, it checks the identity authenticity of RSU and OBU through saved number ID_i, ID_{RSU_j}, respectively. If it is ok, then the TA does not reject safety-message and it chooses random value $r \in Z_q^*$, TA generates its pseudo-ID $PsID_{TA} = {<}PsID_{TA}^1,\ PsID_{TA}^2{>}$ as follows:
  $PsID_{TA}^1 = rP$
  $PsID_{TA}^2 = ID_{RSU_j}^* \oplus h_1(rPub)$
  Then, the TA transmits $Tuple_3$ to RSU, where $Tuple_3 = \{PsID_{TA}, TS_3, \delta_{TA-RSU}\}$, $\delta_{TA-RSU} = h_3(ID_{RSU_j}^*||TS_3)$ and $ID_{RSU_j}^*$ is the same RSU identity.
- $RSU - TO - OBU$: Once the $Tuple_3$ is received by RSU from the TA, it checks the TS_3 freshness. If TS_3 is fresh, then the RSU does not reject the safety-message. Otherwise, the $Tuple_3$ is dropped. RSU then generates the $ID_{RSU_j}^* = PsID_{TA}^2 = \oplus h_1(kPsID_{TA}^1)$ and verifies whether match of the $ID_{RSU_j}^* = ID_{RSU_j}$. It verifies whether $\delta_{TA-RSU} \overset{?}{=} h_3(ID_{RSU_j}^*||TS_3)$. The TA rejects the $Tuple_3$ when it is not ok; otherwise, RSU generates the signature key SK for the vehicle as follows:
  $SK = k.h_2(PsID_i^1||PsID_i^2)$
  Then, the RSU transmits $Tuple_4$ to OBU, where $Tuple_4 = \{PsID_i, TS_4, SK_{enc},\ \delta_{RSU-OBU}\}$, $SK_{enc} = SK \oplus h_1(Pdm)$ and $\delta_{RSU-OBU} = h_2(Pdm||SK||TS_4)$.
- OBU: Once the $Tuple_4$ is received by OBU from the RSU, it calculates the $SK = SK_{enc} \oplus h_1(Pdm)$ and

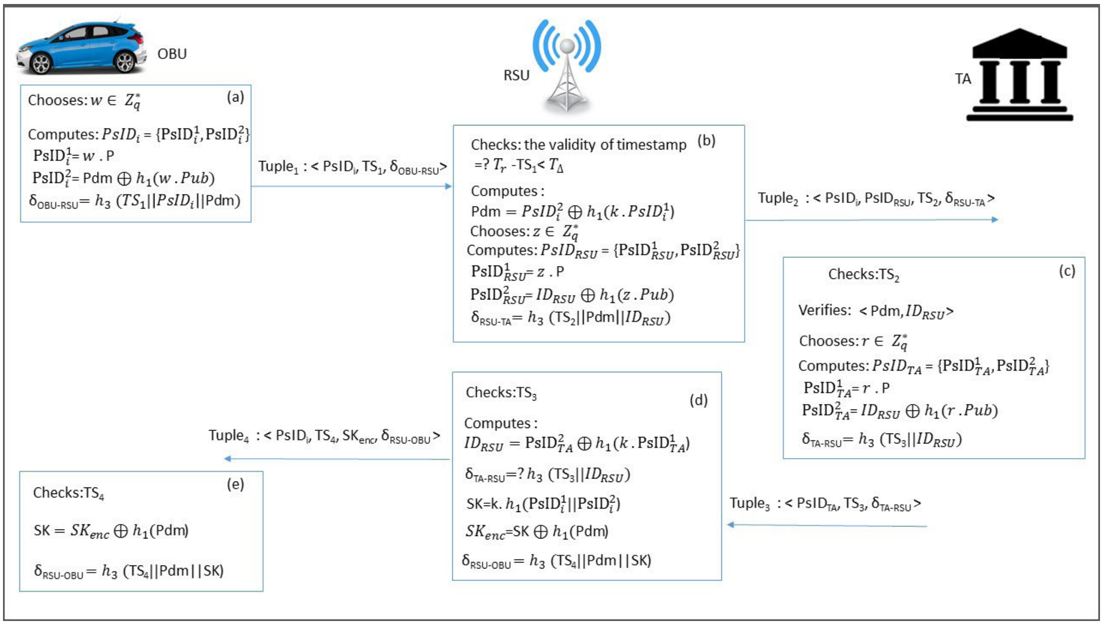

OBU
RSU
TA
Chooses: $w \in Z_q^*$
(a)
Computes: $PsID_i$ = {PsID_i^1, PsID_i^2}
$\mathrm{PsID}_i^1 = w$. P
PsID_i^2= Pdm $\oplus h_1(w\,.\,Pub)$
$\delta_{OBU\text{-}RSU} = h_3\ (TS_1||PsID_i||\mathrm{Pdm})$
Tuple$_1$: < PsID$_i$, TS$_1$, $\delta_{OBU\text{-}RSU}$>
Checks: the validity of timestamp
(b)
=? T_r -TS$_1$< T_Δ
Computes :
Pdm $= PsID_i^2 \oplus h_1(k\,.\,PsID_i^1)$
Chooses: $z \in Z_q^*$
Computes: $PsID_{RSU}$ = {PsID_{RSU}^1, PsID_{RSU}^2}
$\mathrm{PsID}_{RSU}^1 = z$. P
$\mathrm{PsID}_{RSU}^2 = ID_{RSU} \oplus h_1(z\,.\,Pub)$
$\delta_{RSU\text{-}TA} = h_3$ (TS$_2$||Pdm||ID_{RSU})
Tuple$_2$: < PsID$_i$, PsID$_{RSU}$, TS$_2$, $\delta_{RSU\text{-}TA}$ >
Checks:TS$_2$
(c)
Verifies: < Pdm, ID_{RSU}>
Chooses: $r \in Z_q^*$
Computes: $PsID_{TA}$ = {PsID_{TA}^1, PsID_{TA}^2}
$\mathrm{PsID}_{TA}^1 = r$. P
$\mathrm{PsID}_{TA}^2 = ID_{RSU} \oplus h_1(r\,.\,Pub)$
$\delta_{TA\text{-}RSU} = h_3$ (TS$_3$||ID_{RSU})
Tuple$_3$: < PsID$_{TA}$, TS$_3$, $\delta_{TA\text{-}RSU}$ >
Checks:TS$_3$
(d)
Computes :
$ID_{RSU} = \mathrm{PsID}_{TA}^2 \oplus h_1(k\,.\,\mathrm{PsID}_{TA}^1)$
$\delta_{TA\text{-}RSU}$=? h_3 (TS$_3$||ID_{RSU})
SK=k. $h_1(\mathrm{PsID}_i^1||\mathrm{PsID}_i^2)$
SK_{enc}=SK $\oplus h_1$(Pdm)
$\delta_{RSU\text{-}OBU} = h_3$ (TS$_4$||Pdm||SK)
Tuple$_4$: < PsID$_i$, TS$_4$, SK$_{enc}$, $\delta_{RSU\text{-}OBU}$ >
Checks:TS$_4$
(e)
SK $= SK_{enc} \oplus h_1$(Pdm)
$\delta_{RSU\text{-}OBU} = h_3$ (TS$_4$||Pdm||SK)

FIGURE 3. Process of mutual authentication phase.

verifies whether $\delta_{RSU-OBU} \overset{?}{=} h_2(Pdm||SK||TS_4)$ by assisting its Pdm. If it is ok, then the vehicle does not reject the PK as its corresponding signature key.

To ensure the pseudo-ID security and its corresponding signature key in the system, we advise a protocol of updating the signature key as demonstrated in [29] for our work. Over this protocol, the vehicle uses pseudo-ID and its corresponding signature key for a few periods of routing in the system.

B. PHASE OF SIGNING SAFETY-MESSAGE

Once the vehicle joins the communication range of the RSU during the mutual authentication process, it starts sending safety-message utilizing Sk as a signature for each safety-message. Figure 4 shows the process of signing safety-message phase.

- The vehicle calculates the signature of safety-message; $\delta_m = Sk + w.h_3(m||TS)$.
- The vehicle calculates $\sigma = h_3(m||TS)PsID_i^1$.
- The vehicle sets δ_m and σ are utilized to verifying safety-message for the recipient.
- Finally, the vehicle sends the tuple of safety-message-signature $\{PsID_i, m, TS, \delta_m, \sigma\}$ to neighbor vehicles and nearby RSUs.

C. PHASE OF VERIFYING SAFETY-MESSAGE

This section presents the single and batch verifying safety-messages, as shown in Figure 4.

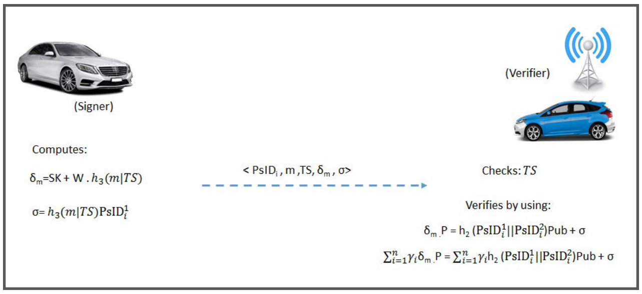

(Signer)
(Verifier)
Computes:
δ_m=SK + W . $h_3(m|TS)$
σ= $h_3(m|TS)\mathrm{PsID}_i^1$
< PsID$_i$, m ,TS, δ_m , σ>
Checks: TS
Verifies by using:
δ_m . P = h$_2$ ($\mathrm{PsID}_i^1||\mathrm{PsID}_i^2$)Pub + σ
$\sum_{i=1}^{n}\gamma_i\delta_m$. P = $\sum_{i=1}^{n}\gamma_i$h$_2$ ($\mathrm{PsID}_i^1||\mathrm{PsID}_i^2$)Pub + σ

FIGURE 4. The process of signing and verifying messages.

1) SINGLE VERIFYING SAFETY-MESSAGE

Each vehicle only verifies the safety-message signature utilizing this process of verification. Once the recipients receive signed safety-message, they should check its validity and authenticity. Ensuring no misbehaving vehicles can be considered to be legal vehicles before accepting the safety-message for further processing. Therefore, false safety-messages are preventing in the transmission. The single verifying safety-message method is presented in deeply as follows:

- Once the verifier received the tuple of safety-message-signature $\{PsID_i, m, TS, \delta_m, \sigma\}$, it verify the timestamp TS freshness first.
- Then, the verifier utilizes δ_m and σ of the tuple of safety-message-signature $\{PsID_i, m, TS, \delta_m, \sigma\}$ to check safety-message m, where $\sigma = h_3(m||TS)PsID_i^1$ and $\delta_m = Sk + w.h_3(m||TS)$. If Equation 1 holds, the safety-message does not reject. Otherwise, the verifier will drop the safety-message.

$$\delta_m.P = h_2(PsID_i^1||PsID_i^2)Pub + \sigma \tag{1}$$

Equation 1 proof is presented as follows:

$$L.H.S$$
$$\delta_m.P$$
$$= Sk + w.h_3(m||TS).P$$

$$
\begin{aligned}
&= \Big(k.h_2(PsID_i^1||PsID_i^2) + w.h_3(m||TS)\Big).P \\
&= h_2(PsID_i^1||PsID_i^2)k.P + h_3(m||TS)w.P \\
&= h_2(PsID_i^1||PsID_i^2)Pub + h_3(m||TS)PsID_i^1 \\
&= h_2(PsID_i^1||PsID_i^2)Pub + \sigma \\
&= R.H.S
\end{aligned}
$$

Therefore, Equation 1 is checked to be true.

2) BATCH VERIFYING SAFETY-MESSAGE

Via this batch verifying safety-message process, the recipient checks a multiple safety-messages at the same time. For reducing the time consumed, our work uses a batch verifying safety-message method. For satisfying the non-repudiation requirement in our work, we uses the technique of tiny exponent test [23]. The recipient randomly computes an integer number $\eta = \{\eta_1, \eta_2, \ldots, \eta_n\}$, where $\eta = \in [1, 2^t]$ and t is a tiny value, which the computation overhead is not increased. Besides, consider that a verifier receives a large number of the tuple of safety-message-signature $\{PsID_i^1, m^1, TS^1, \delta_m^1, \sigma^1\}, \{PsID_i^2, m^2, TS^2, \delta_m^2, \sigma^2\}, \ldots, \{PsID_i^n, m^n, TS^n, \delta_m^n, \sigma^n\}$. Then, the verifier utilizes δ_m^n of the tuple of safety-message-signature $\{PsID_i^n, m^n, TS^n, \delta_m^n, \sigma^n\}$ for simultaneously verifying the safety-message by utilizing Equation 1, as follows:

$$
\left(\sum_{i=1}^{n}(\gamma.\delta_m)\right).P = \left(\sum_{i=1}^{n}(\gamma.h_2(PsID_i^1||PsID_i^2)Pub)\right) + (\gamma.\sigma) \tag{2}
$$

Equation 2 proof is presented as follows:

$$
\begin{aligned}
&L.H.S\left(\sum_{i=1}^{n}\eta_i.\delta_m\right).P \\
&= \sum_{i=1}^{n}\eta_i.(Sk + w.h_3(m||TS)).P \\
&= \sum_{i=1}^{n}\eta_i.(k.h_2(PsID_i^1||PsID_i^2).P + w.h_3(m||TS)).P \\
&= \sum_{i=1}^{n}\eta_i.(h_2(PsID_i^1||PsID_i^2)k.P + h_3(m||TS))w.P \\
&= \sum_{i=1}^{n}\eta_i.(h_2(PsID_i^1||PsID_i^2)Pub + h_3(m||TS))PsID_i^1 \\
&= \sum_{i=1}^{n}\eta_i.(h_2(PsID_i^1||PsID_i^2)Pub + \sigma \\
&= R.H.S
\end{aligned}
$$

Therefore, Equation 2 is checked to be true.

D. PHASE OF UPDATE PARAMETERS

To prevent attacks of side-channel, the sensitive data stored (pseudonym of vehicle) in the TPD must be regularly updated via an online mode and annual inspection. Nonetheless, a few period, without updating the sensitive data stored for waiting for the mode of next annual inspection, the adversary could have enough period for obtaining sensitive data that can collapse the entire VANETs. The vehicle should execute the following specific steps for updating the sensitive data stored in the TPD by utilizing the online mode are as follows:

- The vehicle selects a random number $r \in Z_q^*$ and computes $PsID_i^1 = rP$ and $PsID_i^2 = Pdm \oplus h_1(r.Pub)$. Then, the vehicle sends message $\{PsID_v^{new}, TS_1, \delta_{OBU_i^{new}}\}$ to the TA, where $PsID_v^{new} = \{PsID_i^1 = rP, PsID_i^2 = Pdm \oplus h_1(r.Pub)\}$ and $\delta_{OBU_i^{new}} = h_3(Pdm\|PsID_i^1\|PsID_i^2\| TS_1)$.
- The freshness of timestamp TS_1 is verified, once the TA receives the message $\{PsID_v^{new}, TS_1, \delta_{OBU_i^{new}}\}$. If TS_1 is valid, then TA calculates old pseudonym of authenticated vehicle $Pdm = PsID_i^2 \oplus h_1(k.Pub)$. The TA checks whether $\delta_{OBU_i^{new}} =? h_3(Pdm\|PsID_i^1\|PsID_i^2\|TS_1)$ holds. TA verifies whether the tuple (ID_i, Pdm, SP_{vi}) presents in the its registration list of vehicle; else TA checks the SP_{vi} freshens.
- Once the SP_{vi} is expired, a modern short period SP_{vi}^{New} is selected by TA. Then, the TA calculates a new pseudonym of authenticated vehicle $Pdm^{New} = h_3(ID_i\|SP_{vi}^{New})$. It will drop if SP_{vi} is still freshness.
- TA encrypts message $(Ps^{New}, \lambda_i^{New})$ by using the previous encryption key $E_{\lambda_i} \in Z_q^*$ to the vehicle and updates the new tuple $(OID_i, Ps^{New}, VP_{vi}^{New}, \lambda_i^{New})$ into the registration list of vehicles.
  $K_{enc}, \delta_{RSU-OBU}\}$, $SK_{enc}^{new} = SK \oplus h_1(Pdm)$ and $\delta_{RSU-OBU} = h_2(Pdm||SK||TS_4)$.
- TA sends a message $(Pdm_{enc}^{new}, SP_{vi})$ to the vehicle, where $Pdm_{enc}^{new} = Pdm \oplus h_1(k.PsID_i^1)$.
- Lastly, the vehicle computes $Pdm = Pdm_{enc}^{new} \oplus h_1(k.PsID_i^1)$ to obtain new pseudonym.

V. SECURITY ANALYSIS AND COMPARISON

In this section, we first present the structure of formal analysis in terms of random oracle model and BAN logic; this is followed by a description of security requirements and finally, the security comparison between the proposed and other schemes.

A. FORMAL ANALYSIS

We use random oracle model and BAN logic to prove formal analysis of the proposed scheme as follows,

1) RANDOM ORACLE MODEL

This subsection lunches a game among adversary AY and challenger CR, where AY is a broker of the proposed scheme security and CR is the robustness of the proposed scheme.

Theorem 1: This work against an adaptive chosen message attack under the random oracle model is existentially unforgeable

Proof: Suppose CR could forge a legitimate the tuple of safety-message-signature $\{PsID_i, m, TS, \delta_m, \sigma\}$ in the proposed scheme. Besides, suppose that an instance of ECDLP

(P, Q = k.P) is specified for two points P, Q on E, and $k \in Z_q^*$. The *CR* then could overcome the unquestionably of ECDLP with *AY* like a subroutine.

Setup: *CR* calculates the private key and public parameters of the system $\psi = \{p, q, a, b, P, P_{pub}, h_1, h_2, h_3\}$ and then establishes three lists, namely, $LIST_{h^1}$ with form of $(\alpha, \tau h_1)$, $LIST_{h^2}$ with form of $(PsID_i^1, PsID_i^2, \tau h_2)$ and $LIST_{h^3}$ with form of $(m, TS, \tau h_3)$. *AY* is empty at first. Then, *CR* forwards ψ to *AY*.

Oracle of $LIST_{h^1}$: After *CR* receives message request α from *AY*, it first tests if tuple $(\alpha, \tau h_1)$ is $LIST_{h^1}$ exist. If right, then, *CR* sends $\tau h_1 = h(\alpha)$ to *AY*. Otherwise, *CR* chooses $\tau h_1 \in Z_q^*$ random and attaches $((\alpha, \tau h_1)$ into $LIST_{h^1}$. Then, *CR* forwards $\tau h_1 = h(\alpha)$ to *AY*.

Oracle of $LIST_{h^2}$: After *CR* receives message request $PsID_i^1, PsID_i^2$ from *AY*, it first tests if tuple $(PsID_i^1, PsID_i^2, \tau h_2)$ is $LIST_{h^2}$ exist. If right, then, *CR* sends $\tau h_2 = h(PsID_i^1 \| PsID_i^2)$ to *AY*. Otherwise, *CR* chooses $\tau h_2 \in Z_q^*$ random and attaches $((PsID_i^1, PsID_i^2, \tau h_2)$ into $LIST_{h^2}$. Then, *CR* forwards $\tau h_2 = h(PsID_i^1 \| PsID_i^2)$ to *AY*.

Oracle of $LIST_{h^3}$: After *CR* receives message request m, TS from *AY*, it first tests if tuple $(m, TS, \tau h_3)$ is $LIST_{h^2}$ exist. If right, then, *CR* sends $\tau h_3 = h(m||TS)$ to *AY*. Otherwise, *CR* chooses $\tau h_3 \in Z_q^*$ random and attaches $((PsID_i^1, PsID_i^2, \tau h_3)$ into $LIST_{h^3}$. Then, *CR* forwards $\tau h_3 = h(m||TS)$ to *AY*.

Sign: When receiving an *CR* request of sign from *AY* through message m, it computes $\{h^{i,2}, h^{i,3}, \delta_m \in Z_q^*, PsID_i^2 \in G\}$. *AY* generates $PsID_i^1 = (\delta_m P - h^{i,2} h^{i,3} Pub)$. *CR* inserts the $(PsID_i^1, PsID_i^2, \tau h_2)$ into $LIST_{h^2}$ and $(m, TS, \tau h^3)$ into $LIST_{h^3}$. Lastly, *CR* forwards the tuple of safety-message-signature $\{PsID_i, m, TS, \delta_m, \sigma\}$ to *AY*. The Oracle of Sign replay is legitimate due to the tuple of safety-message-signature $\{PsID_i, m, TS, \delta_m, \sigma\}$ complies with Equation (3):

$$\delta_m P = h^{i,2} Pub + \sigma$$

where $\sigma = h^{i,3} PsID_i^1$

$$= h^{i,2} Pub + \sigma + (\delta_m P - h^{i,2} Pub + \sigma) = \delta_m P \tag{3}$$

Output: *CR* ends up with the tuple of safety-message-signature $\{PsID_i, m, TS, \delta_m, \sigma\}$. *CR* tests this tuple utilizing Equation 4 as follows:

$$\delta_m P = h^{i,2} Pub + \sigma. \tag{4}$$

CR continues the game when Equation 4 does not hold.

Based on the forgery lemma in [21], *AY* could results another valid the tuple of safety-message-signature $\{PsID_i, m, TS, \delta_m, \sigma\}$. Hence, we obtain Equation 5 the following equation is obtained:

$$\delta_m^* P = h^{i,2^*} Pub + \sigma. \tag{5}$$

From the two 4 and 5, we can obtain

$$\begin{aligned}(\delta_m - \delta_m^*)P &= \delta_m P - \delta_m^* P\\ &= h^{i,2} Pub + \sigma - h^{i,2^*} Pub + \sigma\\ &= h^{i,2} Pub - h^{i,2^*} Pub = (h^{i,2} - h^{i,2^*}) Pub. \end{aligned} \tag{6}$$

Therefore, we could get $(\delta_m - \delta_m^*) = (h^{i,2} - h^{i,2^*}) Pub$ mod p.

AY results s $= (\delta_m - \delta_m^*) = (h^{i,2} - h^{i,2^*})^{-1}$

Hence, the proposed scheme in the random oracle model is resistant for choosing adaptive message attacks under the supposition that ECDLP is hardness.

2) BAN LOGIC

By using a generally formal logic as known BAN logic, the proposed scheme should achieve specific goals of security among the components in VANETs for mutual verification. The essential definition of the introduction of BAN logic is removed in this paper. We refer the reader for further details [30], [31].

Security goals

The main idea of these operations is to validate the session key among the components in the system. Thus, the proposed scheme requires for achieving the eight major goals as follows,

The proposed scheme's goals are as follows.

- **Goal-1.** $TA| \equiv OBU_i| \equiv (Pdm)$.
- **Goal-2.** $TA| \equiv (Pdm)$.
- **Goal-3.** $TA| \equiv RSU_j| \equiv (ID_{RSU_j})$.
- **Goal-4.** $TA| \equiv (ID_{RSU_j})$.
- **Goal-5.** $RSU_j| \equiv TA| \equiv (\delta_{TA-RSU_j})$.
- **Goal-6.** $RSU_j| \equiv (\delta_{TA-RSU_j})$.
- **Goal-7.** $OBU_i| \equiv RSU_j| \equiv (SK)$.
- **Goal-8.** $OBU_i| \equiv (SK)$.

Phase of idealize the proposed:

- The messages sharing between components in VANETs are idealized for the our work as follows
  M-1. $OBU_i \rightarrow RSU_j : \{PsID_i, TS_1\ \delta_{OBU-RSU}\}$.
  M-2. $RSU_j \rightarrow TA : \{PsID_i, PsID_{RSU_j}, TS_2, \delta_{RSU-TA}\}$.
  M-3. $TA \rightarrow RSU_j : \{PsID_{TA}, TS_3, \delta_{TA-RSU}\}$.
  M-4. $RSU \rightarrow OBU_i$: $\{PsID_i, SK_{enc}, \delta_{RSU-OBU}\}$.
- The messages of proposed are idealized as follows:
  SMI-1. $OBU_i \rightarrow TA : (ID_i)_{Pub}$.
  SMI-2. $RSU_j \rightarrow TA : (ID_{RSU_j})_{Pub}$.
  SMI-3. $TA \rightarrow RSU_j : (\delta_{TA-RSU_j})_{Pub}$.
  SMI-4. $RSU_j \rightarrow OBU_i : (SK)_{h(ID_i)}$.

Assumptions.

The following assumptions regarding to the initial situation of our work are made:

- **Ass-1.** $TA| \equiv \#(TS_2)$.
- **Ass-2.** $RSU_j| \equiv \#(TS_1, TS_3)$.
- **Ass-3.** $OBU_i| \equiv \#(TS_4)$.
- **Ass-4.** $TA| \equiv |\xrightarrow{Pub} OBU_i$.
- **Ass-5.** $TA| \equiv |\xrightarrow{Pub} RSU_j$.
- **Ass-6.** $OBU_i| \equiv OBU_i \overset{ID_i}{\longleftrightarrow} RSU_j$.
- **Ass-7.** $TA| \equiv OBU_i \Rightarrow (ID_i)$.
- **Ass-8.** $TA| \equiv RSU_j \Rightarrow (ID_{RSU_j})$.
- **Ass-9.** $OBU_i| \equiv RSU_j \Rightarrow (SK)$.
- **Ass-10.** $RSU_j| \equiv |\xrightarrow{Pub} TA)$.

- **Ass-11.** $RSU_j| \equiv TA \Rightarrow (\delta_{TA-RSU_j})$.

Proof.

In this part, the eight security goals included in the proposed scheme are accomplished.

From **SMI-1.**, we obtain:

S-1: $TA \triangleleft (ID_i)_{Pub}$

From **S-1, Ass-4**, and by using **rule of message meaning**, we obtain:

S-2: $TA| \equiv OBU_i| \sim (ID_i)$

From **S-2, Ass-1**, and by using **nonce-verification and freshness rules**, we obtain:

S3: $TA| \equiv OBU| \equiv (OID_i)$

Therefore, security **Goal-1** is accomplished.

From **S-3, Ass-7**, and by using **jurisdiction rule**, we obtain:

S-4: $TA| \equiv (ID_i)$

Therefore, security **Goal-2** is accomplished.

From **SMI-2.**, we obtain:

S-5: $TA \triangleleft (ID_{RSU_j})_{Pub}$

From **S-5, Ass-5**, and by using **rule of message meaning** , we obtain:

S-6: $TA| \equiv RSU_j| \sim (ID_{RSU_j})$

From **S-6, As-1**, and by using **nonce-verification and freshness rules**, we obtain:

S-7: $TA| \equiv RSU_j| \equiv (ID_{RSU_j})$

Therefore, security **Goal-3** is accomplished.

From **S-7, Ass-8**, and by using **rule of jurisdiction**, we obtain:

S-8: $TA| \equiv (ID_{RSU_j})$

Therefore, security **Goal-4** is accomplished.

From **SMI-3.**, we obtain:

S-9: $RSU_j \triangleleft (\delta_{TA-RSU_j})_{Pub}$

From **S-9, Ass-10**, and by using **rule of message meaning**, we obtain:

S-10: $RSU_j| \equiv TA| \sim (\delta_{TA-RSU_j})$

From **S-10, Ass-2**, and by using **nonce-verification and freshness rules**, we obtain:

S-11: $RSU_j| \equiv |TA| \equiv (\delta_{TA-RSU_j})$

Therefore, security **Goal-5** is accomplished.

From **S-11, As-11**, and by using **rule of jurisdiction**, we obtain:

S-12: $RSU| \equiv (\sigma_{TA-RSU})$

Therefore, security **Goal-6** is accomplished.

From **SMI-4.**, we obtain:

S-13: $OBU_i \triangleleft (SK)_{h(ID_i)}$

From **S-13, Ass-6**, and by using **rule of message meaning** , we obtain:

S-14: $OBU_i| \equiv RSU_j| \sim (SK)$

From **S-14, Ass-3**, and by using **nonce-verification and freshness rules**, we obtain:

S-15: $OBU_i| \equiv RSU_j| \equiv (SK)$

Therefore, security **Goal-7** is accomplished.

From **S-15, Ass-9**, and by using **jurisdiction rule**, we obtain:

S-16: $OBU_i| \equiv (SK)$

Thus, security **Goal-8** is accomplished.

Consequently, the eight security goals collectively guarantee that components of the proposed scheme are mutually validated.

B. SECURITY REQUIREMENTS

This subsection analyses how our work fulfills the requirements of security as follows,

- Message integrity and authentication:
  A receiver can check the tuple of safety-message-signature $\{PsID_i, m, TS, \delta_m, \sigma\}$ sent from a vehicle regarding to authenticity of node and integrity of message by verifying whether equation $\delta_m.P = h_2(PsID_i^1||PsID_i^2)Pub+\sigma$ holds. For instance, once capturing the tuple of safety-message-signature $\{PsID_i, m, TS, \delta_m, \sigma\}$ from authenticated vehicle AV_j in our work, a vehicle V_i changes the safety-message m_i^c and sends changed the tuple of safety-message-signature $\{PsID_i, m_i^c, TS, \delta_m, \sigma\}$ into the V2V and V2I communications. The verifying vehicle VV_v verifies the f changed the tuple of safety-message-signature $\{PsID_i, m_i^c, TS, \delta_m, \sigma\}$ validity by verifying whether Equation 1 or 2 hold. If ok, then our work is satisfied requirements of integrity and authentication.
- Identity privacy preservation:
  In the tuple of safety-message-signature $\{PsID_i, m, TS, \delta_m, \sigma\}$ of our work, a pseudo-ID $PsID_i$ includes two secret values (i.e., $(w, k) \in Z_q^*$), which are chosen at random by the broadcasting TA and vehicle, respectively. Its possible by an adversary to disclose the pseudonym Pdm of vehicle due to an attacker does not have the ability to compute $kPsID_i^1$ and wkP based on the ECCDH and ECDL problems, respectively. As $Pub = kP$, $PsID_i^1 = wP$ and $PsID_i^2 = Pdm \oplus h_1(wPub)$. The adversary has the ability to compute $kPsID_i^1$, wkP from $Pub = kP$ and $PsID_i^1 = wP$ for obtaining the pseudonym Pdm of vehicle. This process to prevent the attacker from disclosing the vehicle's Pdm from the aforesaid computation due to it is depended on hard problems. Therefore, requirement of identity privacy preservation is satisfied by our work.
- Traceability and revocation:
  In V2V and V2 communications, traceability and revocation are significant security requirements. If a forge safety-messages are transmitted from a malicious vehicle, the TA then can disclose the vehicle's identity from its pseudo-ID $PsID_i$. The TA's private key k in our work is utilized to disclose the identity ID_i via the following computations.

$$\begin{aligned} Pdm &= PsID_i^2 \oplus h_1(kPsID_i^1) \\ &= Pdm \oplus h_1(kPub) \oplus h_1(kPsID_i^1) \\ &= Pdm \end{aligned}$$

  Then, TA research the identity ID_i on the registration list of the vehicle which its match with Pdm. Besides, revocation is a serious security requirement for securing

V2V and V2I communications. After the process of traceability is done, the TA inserts the identity ID_i to the CRL and transmits the modern list of CRL. Thus, the RSU containing malicious vehicle broadcasts and updates the CRLs in the local. Hence, our work satisfies requirements of traceability and revocation due to they provide conditional anonymity

- Resistance to replay attacks
  This proposed scheme uses the current timestamp TS in the tuple of safety-message-signature $\{PsID_i, m, TS, \delta_m, \sigma\}$. During the process of verification by a receiver, an adversary can not alter TS in the tuple of safety-message-signature $\{PsID_i, m, TS, \delta_m, \sigma\}$. If TS was had expired or invalid, then the safety-message would be dropped. Hence, the proposed scheme successfully resists the replay attacks.
- Resistance to impersonation attacks
  The attacker should get a vehicle's identity if they want to send a true the tuple of safety-message-signature $\{PsID_i, m, TS, \delta_m, \sigma\}$ by impersonating the authenticated vehicle. Furthermore, based to previous knowledge, the attacker cannot discover an identity's vehicle in the proposed scheme. The impersonation attack in our work is therefore ineffective. Hence, the proposed scheme successfully resists the impersonation attacks.
- Resistance to modification attacks
  The signature δ_m is included in the tuple of safety-message-signature $\{PsID_i, m, TS, \delta_m, \sigma\}$ of the proposed scheme and ensures the security of the safety-message from the modification attacks. During the process of authentication by a receiver, if an adversary modifies or changes the safety-message, then it would be dropped. Therefore, the proposed scheme successfully resists the modification attacks.
- Resistance to man-in-the-middle attacks
  Mutual authentication among the signer and the receiver is executed in the proposed scheme. If the adversaries attempt a man-in-middle attack, they then should forge the signer message and receiver message for connecting with it. Nonetheless, an attacker cannot generate this attack type, based on the above analysis. Hence, our work successfully resists the man-in-the-middle attacks.
- Resistance to side-channel attacks
  Several scholars resort to saving the private key of the system in the TPD of OBU due to it is possible by misbehaving vehicle to be compromised. Nonetheless, an adversary can easily get critical data stored in the TPD via a side-channel attack. To cope with this attack, our work regularly update the (Pdm) in the TPD, where $Pdm = h_3(ID_i \| SP_{vi})$. It is stated that the pseudonym Psm of vehicle is using frequently and repeatedly; therefore, if the Pdm is not continuously updated, it will offer ample chance for the misbehaving vehicle for disclosing and exploiting the pseudonyms regarding the safety-messages. Nonetheless, in the proposed scheme, the Pdm is already updated before an adversary can be disclosed and exploited. For example, once adversaries reach the vehicle's TPD directly, they disclose the registered pseudonym Pdm utilized for calculating the tuple of safety message-signature $\{PsID_i, m, TS, \delta_m, \sigma\}$. In our work, the pseudonym is frequently and periodically updated (Indicate to Subsection IV-D), therefore making the adversary does not have the ability for exploiting the revealed previous pseudonym. Thus, our work successfully resists the side-channel attack.

TABLE 3. Comparison between other related schemes and the proposed scheme.

Schemes	SR-1	SR-2	SR-3	SR-4	SR-5	SR-6	SR-7
Jianhong et al. [23]	✓	✓	✗	✓	✓	✓	✗
He et al. [15]	✓	✓	✗	✓	✓	✓	✗
Bayat et al. [14]	✓	✓	✗	✓	✓	✓	✗
Al-shareeda et al. [16]	✗	✓	✓	✗	✗	✗	✗
Al-shareeda et al. [17]	✓	✓	✗	✓	✓	✓	✗
Our scheme	✓	✓	✓	✓	✓	✓	✓

C. SECURITY COMPARISON

This section compared the design goal in terms of requirements of security between the other related schemes and proposed scheme. Table 3 indicates the comparison of security requirements. Let SR-1, SR-2, SR-3, SR-4, SR-5, SR-6 and SR-7, refer message integrity and authentication, identity privacy preservation, traceability and revocation, resistance to replay attacks, resistance to impersonation attacks, resistance to modification attacks, and resistance to side-channel attacks, respectively.

According to Table 3, neither Jianhong *et al.*'s [23], He *et al.*'s [15], Bayat *et al.*'s [14], Al-shareeda *et al.* [16] or Al-shareeda *et al.* [17] schemes satisfy all of the security requirements in the system. Nonetheless, the security requirements are completely satisfied in the proposed scheme.

VI. PERFORMANCE EVALUATION

To overcome the issues regarding the system overhead in terms of computation cost and communication cost, we present the analysis and comparison of the performance evaluation between the proposed scheme and the schemes proposed by Jianhong *et al.* [23], Bayat *et al.* [14], He *et al.* [15], Al-shareeda *et al.* [16] and Al-shareeda *et al.* [17]. The cost of computation is regarding the multiple operations of cryptographic that have to be executed in the signing and verifying the messages. While the cost of communication regards to the tuple of safety-message-signature size, containing the multiple of elements in the tuple of safety-message-signature. The following subsections, we present the description of the computation cost and communication cost are described in detailed.

A. COMPUTATION COST ANALYSIS

A group G_1 of additive is computed with an 80 bit level of security in a bilinear pairing. Various parameters of the ECC and bilinear pair schemes are indicated in Table 5. In this paper, we use MIRACL [32] that widely used cryptographic

TABLE 4. The running times for operation of cryptographic [16].

Cryptographic operations:	BP_T	BP_T^{pm}	MTP_T	ECC_T^{pm}	h_T
Definitions:	The running time of the bilinear pair operation in G_1	The running time for the operation of a point multiplication in G_1	The running time for the operation of a Map-To-Point hash function in G_1	The running time for the operation of a point multiplication in G.	The running time for the operation of a general one-way hash function.
Time (ms):	5.811	1.5654	4.1724	0.6718	0.001

TABLE 5. Various cryptography operations cost.

Items	ECC	Bilinear pair
Curve type	E:$y^2 = x^3 + ax + b$ mod p, where $a, b \in Z_q^*$	E:$y^2 = x^3 + x$ mod p
Pairing	Pairing-free	$G_1 * G_1 \rightarrow G_2$
Cyclic Group	$G(p)$	$G_1(p)$
Size of p	160 bits	521 bits
Size of G	q = 160 bits	q = 160 bits
Length of group	$\|G\|$= 40 bytes	$\|G_1\|$= 128 bytes

TABLE 6. Computation cost comparison.

Schemes	$PSSM$	$SVSM$	$BVSM$
Jianhong et al. [23]	$6BP_T + MTP_T + 4h_T \approx 13.59$	$3BP_T + 2BP_T^{pm} + 3h_T \approx 20.5774$	$(n+1)BP_T^{pm} + 3BP_T + (3n)h_T \approx 1.966n + 18.9772$
Bayat et al. [14]	$5BP_T + MTP_T + 2h_T \approx 4.1724$	$3BP_T + MTP_T + BP_T^{pm} + h_T \approx 4.1724$	$3BP_T + (n)MTP_T + (n)BP_T^{pm} + (n)h_T \approx 5.7378n + 17.4333$
He et al. [15]	$3ECC_T^{pm} + 3h_T \approx 2.0184$	$3ECC_T^{pm} + 2h_T \approx 2.0236$	$(n+2)ECC_T^{pm} + (2n)h_T \approx 0.6718n + 1.3405$
Al-shareeda et al. [16]	$2h_T \approx 0.002$	$3ECC_T^{pm} + 2h_T \approx 2.0174$	$(3n+1)ECC_T^{pm} + (n)h_T \approx 2.0164n + 0.6718$
Al-shareeda et al. [17]	$3ECC_T^{pm} + 2h_T \approx 2.0174$	$3ECC_T^{pm} + 1h_T \approx 2.0164$	$(2n+1)ECC_T^{pm} + (n)h_T \approx 1.2446n + 0.6718$
Our work	$1ECC_T^{pm} + 2h_T \approx 0.6738$	$2ECC_T^{pm} + 1h_T \approx 1.3446$	$2ECC_T^{pm} + (n)T_h \approx 0.001n + 1.3436$

TABLE 7. Computation overhead comparison improvement.

Schemes	$PSSM$	$SVSM$	$BVSM$ (100 messages)
Jianhong et al. [23]	95%	93.5%	99.3%
Bayat et al. [14]	83.9%	67.8%	99.8%
He et al. [15]	66.7%	33.6%	97.9 %
Al-shareeda et al. [16]	0	33.3%	99.3%
Al-shareeda et al. [17]	66.6%	33.3%	98.8%

TABLE 8. Communication cost comparison.

Schemes	**A safety-message**	**n safety-messages**
Jianhong et al. [23]	388 bytes	388 n bytes
He et al. [15]	144 bytes	144 n bytes
Bayat et al. [14]	388 bytes	388 n bytes
Al-shareeda et al. [16]	120 bytes	120 n bytes
Al-shareeda et al. [17]	124 bytes	124 n bytes
Our work	104 bytes	104 n bytes

libraries, is utilized in our experiment due to it provides us for measuring the cost of computation regarding executing time of several cryptographic operations. Cryptography operations used in this work [16] employing in this paper- see Table 4. For simplicity, let $PSSM$, $SVSM$, and $BVSM$ denote phase of signing safety-message; single verifying safety-message; and batch verifying safety-messages, respectively.

In He *et al.* [15] scheme, $PSSM$ includes three operations of scalar multiplication and three functions of one-way hash, therefore $3ECC_T^{pm} + 3h_T$ is the whole computation overhead for $PSSM$. $SVSM$ includes three operations of scalar point multiplication and two functions of one-way hash, therefore the total cost is $3ECC_T^{pm} + 2h_T$. $BVSM$ $(n + 2)$ operations of scalar multiplication, and $(2n)$ functions of one-way hash, therefore $(n + 2)ECC_T^{pm} + (2n)h_T$. is the whole computation overhead for $BVSM$. In the same way, we perform the computation cost of other existing schemes. In the proposed scheme [17] scheme, $PSSM$ includes one operation of scalar multiplication and two functions of one-way hash, therefore $1ECC_T^{pm} + 2h_T$ is the whole computation overhead for $PSSM$. $SVSM$ includes two operations of scalar multiplications, one operation of point addition and one function of one-way hash, therefore $2ECC_T^{pm} + 1h_T$ is the whole computation overhead for $SVSM$. $BVSM$ (2) operations of scalar multiplication, (n+1) operations of point addition, and (2n) operations of one-way hash function, therefore $2ECC_T^{pm} + (n)h_T$ is the whole computation overhead for $BVSM$. In the same way, we perform the computation cost of other existing schemes.

As shown in Table 6, the computation cost of the proposed scheme improves by (2.0184 - 0.6738) / 2.0184 ≈ 66.7%, (2.0236 - 1.3446) / 2.0236 ≈ 33.6% and ((0.6718 * 100 +1.3405) - (0.001 * 100 + 1.3436)) / (0.6718 * 100 +1.3405) ≈ 97.9 % that $PSSM$, $SVSM$ and $BVSM$ of He *et al.* scheme [15], respectively. The improvement of performance of the proposed scheme compared with the other schemes regarding $PSSM$, $SVSM$ and $BVSM$ are listed in Table 7.

B. COMMUNICATION COST ANALYSIS

In this section, we present the performance evaluation in terms of the communication cost. In order to fulfil the same level of security in the proposed scheme and their schemes, we utilize the parameters presented in Table 5. The made of supposition in our work are consistent across the schemes: the size of the result of the timestamp is 4 bytes and the size of the result of the secure hash function is 20 bytes. Table 8 presents the cost of communication between the proposed scheme and other schemes.

The tuple of safety-message-signature in the He *et al.* scheme [15] is (40 * 3 + 20 + 4) = 144 bytes, where the tuple of safety-message-signature consists of three elements in $\{PID_{il}^1, PID_{il}^2, R_i \in G\}$, one element $\{\sigma_m \in Z_q\}$, and one timestamp. In our scheme, the vehicle sends a tuple of safety-message-signature with size (3 * 20 + 40 + 4) = 104 bytes and the content of tuple of safety-message-signature is one timestamp, one item in $\{PsID_1 \in G\}$ and two

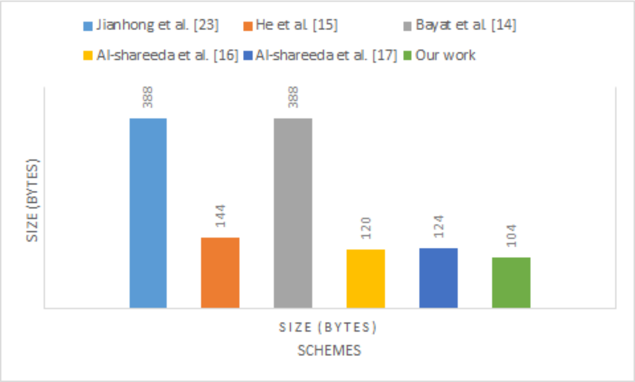


FIGURE 5. Communication costs.

items in $\{PsID_2, \delta_m, \sigma \in z_q\}$. In the same way, we perform the communication cost of other existing schemes. Table 8 illustrates the whole cost of communication between the proposed scheme and other schemes, and Figure 5 illustrates the corresponding outcome

VII. CONCLUSION AND FUTURE WORK

In this paper, An efficient conditional privacy-preserving authentication scheme is proposed. Compare with other schemes, and our scheme can resist the side-channel attack by periodically updating the critic data stored on the TPD on OBU of vehicle. Also, the proposed scheme is shown secure during authentication according to the rule of the BAN logic. Security analysis proves that the design goals regarding the security requirements are satisfied in our work. Finally, due to the proposed scheme uses the one-way hash function and ECC, the performance evaluation of our work are the lowest compared to other existing schemes regarding computation cost and communication cost.

In future work, the experiment could be executed utilizing platforms of network simulation, such as SUMO and OMNET++, to simulate road traffic and VANET networks, 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.*, early access, Sep. 4, 2020, doi: 10.1109/JSEN.2020.3021731.

[2] M. Azees, L. Jegatha Deborah, and P. Vijayakumar, "Comprehensive survey on security services in vehicular ad-hoc networks," *IET Intell. Transp. Syst.*, vol. 10, no. 6, pp. 379–388, Aug. 2016.

[3] *IEEE Trial-Use Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages*, IEEE Standard 1609.4-2006, Intelligent Transportation Systems Committee, 2006.

[4] I. Ali, M. Faisal, and S. Abbas, "A survey on lightweight authentication schemes in vertical handoff," *Int. J. Cooperat. Inf. Syst.*, vol. 26, no. 1, Mar. 2017, Art. no. 1630001.

[5] 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.

[6] 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.

[7] D. Chaum and E. Van Heyst, "Group signatures," in *Proc. Workshop Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer-Verlag, 1991, pp. 257–265.

[8] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: A secure and privacy-preserving protocol for vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 56, no. 6, pp. 3442–3456, Nov. 2007.

[9] L. Zhang, Q. Wu, B. Qin, J. Domingo-Ferrer, and B. Liu, "Practical secure and privacy-preserving scheme for value-added applications in VANETs," *Comput. Commun.*, vol. 71, pp. 50–60, Nov. 2015.

[10] 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.

[11] K. Lim, K. M. Tuladhar, X. Wang, and W. Liu, "A scalable and secure key distribution scheme for group signature based authentication in VANET," in *Proc. IEEE 8th Annu. Ubiquitous Comput., Electron. Mobile Commun. Conf. (UEMCON)*, Oct. 2017, pp. 478–483.

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

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

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

[19] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in *Proc. IEEE INFOCOM 27th Conf. Comput. Commun.*, Apr. 2008, pp. 246–250.

[20] 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.

[21] 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.

[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] 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.

[24] 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.

[25] M. Bayat, M. Pournaghi, M. Rahimi, and M. Barmshoory, "NERA: A New and Efficient RSU based Authentication Scheme for VANETs," *Wireless Netw.*, vol. 26, pp. 3083–3098, Jun. 2020.

[26] 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.

[27] F. Ahmad, A. Adnane, V. N. 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, 2018.

[28] 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.

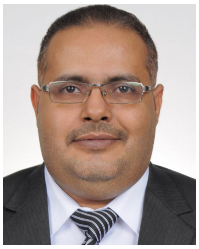
[29] M. A. Alazzawi, H. Lu, A. A. Yassin, and K. Chen, "Efficient conditional anonymity with message integrity and authentication in a vehicular ad-hoc network," *IEEE Access*, vol. 7, pp. 71424–71435, 2019.

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

[31] X. Li, M. H. Ibrahim, S. Kumari, A. K. Sangaiah, V. Gupta, and K.-K.-R. Choo, "Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks," *Comput. Netw.*, vol. 129, pp. 429–443, Dec. 2017.

[32] SS 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 working as an Assistance Professor with the College of Computer Science and Engineering, University of Ha'il. His main research interests are wireless sensor networks, energy management and Propagation models, WSNs MAC protocol, and intelligent transportation systems.



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 Hail, 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.

ZEYAD GHALEB AL-MEKHLAFI (Member, IEEE) 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 Hail, where he is also an Assistance Professor with the Faculty of Computer Science and Engineering. His main research interests include wireless sensor networks, energy management and control for wireless networks, time synchronization, bio-inspired mechanisms, and emerging wireless technologies standard.