IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 27, 2020, accepted December 12, 2020, date of publication December 15, 2020,
date of current version December 23, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3044961

Conditional Privacy-Preserving Authentication Scheme Without Using Point Multiplication Operations Based on Elliptic Curve Cryptography (ECC)

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 Existing conditional privacy-preserving authentication schemes utilized in Vehicular Ad-hoc Networks (VANETs) to satisfy security and privacy requirements essentially depend on point multiplication operations. Achieving repaid verification method of the message is commonly suffer performance efficiency from resulting overheads. We propose a conditional privacy-preserving authentication scheme to secure communication and perform better performance efficiency in this article. The proposed scheme only depends on an elliptic curve cryptography (ECC) based on a point addition operation instead of a point multiplication operation during signing and verifying messages. In the joining phase of the proposed scheme, the vehicle requires the joining process for the broadcasting traffic-related message to others or nearby RSU within its communication range. After obtaining the pseudonym and secret key from RSU, the vehicle is considered as a registered node in VANET. This article utilizes a Burrows-Abadi-Needham (BAN) logic to evidence that the proposed scheme fulfill successfully mutual authentication. The formal security phase shows that security and privacy requirements are satisfied by the proposed scheme. The performance efficiency shows that our proposed scheme has lower overhead in terms of computation cost compared with other recent schemes since a point multiplication operations based o ECC are not used. Therefore, the computation costs of the message signing, individual-authentication and batch-authentication in our proposed scheme are decreased by 99.3%, 99.7% and 98.1%, respectively.

INDEX TERMS Vehicular ad-hoc network (VANET), VANET storage, VANET elliptic curve, VANET security, VANET identity-based cryptography, VANET privacy-preserving.

I. INTRODUCTION

As a promising technology of intelligent transportation system (ITS), the vehicular ad-hoc network (VANET) has gained more and more support from the government sector, and both academia and industry in nowadays [1]–[3]. The major objective of VANET technology is to enhance the driving environment and immediately raise driver's awareness of the road management [4].

Basically, VANET is a subclass of the mobile ad-hoc networks (MANETs), where the vehicle represented as nodes of mobile [5], [6]. The structure of VANET contains the main three components, One trusted authority (TA), some roadside units (RSUs) and many vehicles which fitted to onboard units (OBUs), as shown in Figure 1. All the vehicle in VANET can exchange messages in vehicle-to-vehicle (V2V) and communicate directly with RSUs in vehicle-to-infrastructure (V2I) through the dedicated short-range communication (DSRC) technology [7], [8].

Due to inherent feature in openness nature of VANET, an attacker could impersonate any registered vehicle to send false messages. Furthermore, it's no difficult by the attacker to trace the particular vehicle by analyzing the captured message, which could be a dangerous thread in VANET

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

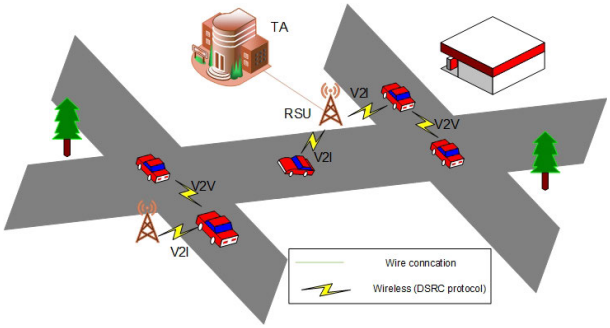


FIGURE 1. The structure of VANET.

system [9]. Security and privacy in VANET should be carefully considered [10]. Therefore, a conditional privacy-preserving authentication scheme should be supported in VANET system to provide security attacks resistance [11].

Many academic studies have been dedicated to conducting a conditional privacy-preserving authentication scheme to satisfy security and privacy requirements in VANETs. However, most of these schemes are high overhead in terms of performance efficiency. Besides, these schemes are not fully and also suffer high storage. Thus, an efficient conditional privacy-preserving authentication scheme is proposed to address these issues in VANET. More precisely, The following contributions of this article can be listed;

- A secure VANET communication by improving the conditional privacy-preserving authentication scheme to secure communication and perform better performance efficiency.
- The proposed scheme is only depending on elliptic curve cryptography (ECC) based on a point addition operation instead of a point multiplication operation during the signing and verifying messages.
- A security scheme that has lower computation cost compared with the existing schemes.

The remainder of the article is structured as follows. Section II introduced some the related work in this field, followed by Section III, which described the preliminary on the proposed scheme. Section IV describes the proposed scheme, and Section V shows its security analysis. Section VI evaluates the result of the performance efficiency to demonstrate the viability of our proposed scheme. Finally, Section VII is the conclusion of this work.

II. RELATED WORK

To fulfil security and privacy requirements in VANET, several schemes were proposed by researchers. Generally, existing work related to security and privacy is categorized into two main categories.

A. PUBLIC KEY INFRASTRUCTURE (PKI)

The main idea of schemes based on public key infrastructure (PKI) is that vehicles require to preload a large number of pair-keys and their respective anonymous certificates (about 43,800) on each OBU. The TA signs these anonymous certificates before preloading in vehicle.

Rajput *et al.* [12] introduced a hierarchical authentication scheme based on privacy-preserving pseudonymous which the valid period of their purpose to address several limitations of PKI-based schemes. Cincilla *et al.* [13] studied the scalability and uniformity of the replicated PKI-based schemes. Therefore, This scheme measures performance and scalability of PKI and emulates on machines hundreds. Joshi *et al.* [14] introduced an effective scheme utilizing event-triggered which sent messages to study security issues in the V2V communication. This scheme uses the authentication's sender based on the PKI to check the message. Asghar *et al.* [15] suggested a feasible PKI-based authentication protocol to address the authenticating requests process, which means that the CRL linear size. Therefore, this scheme support nodes to get services in good time and enhance scalability.

However, a large number of pair-keys and their respective anonymous certificates required to be preloaded on each the vehicle's OBU in advance, which will lead to increase huge burden of certification management for TA. Moreover, the vehicle also suffers from the burden of storage management since the storage capacity of the vehicle is limit. In addition, the verifying vehicle requires to check whether the certificate is valid during the authentication phase, which will cause to increase the computational complexity of the VANET system.

B. IDENTITY (ID)

The main idea of schemes based on identity (ID) is that utilizes identity information as the user's public key, while private keys are produced by the TA and then preloaded to users utilizing the same identity information. The receiver verifies the message with the public key of the sender and signs it with the private key of the sender. Therefore, the ID-based schemes tackle the problems arising on PKI-based schemes. The ID-based schemes could be further classified into two groups based on the cryptography used as follows,

1) BILINEAR PAIR

Lee and Lai [16] introduced improved ID-based schemes that support the batch authentication process. Jianhong *et al.* [17] pointed out various security weakness in scheme of Lee and Lai's [16]; for instance, it fails to fulfil the requirements of traceability and non-repudiation; and it does not withstand replay attacks. Lei Zhang *et al.* [18] suggested an authentication scheme based on privacy-preserving to cope with security attacks in the system. Zhong *et al.* [19] highlighted the Lei Zhang *et al.* scheme [18] that it did not indicate to who in the aggregation phase is the aggregator, and its authentication phase introduced a huge overhead. Pournagh *et al.* [20] suggested an authentication scheme based on conditional privacy-preserving, which integrates both schemes RSU-based and tamper proof device (TPD)-based for securing communication. Bayat *et al.* [21] introduced an authentication scheme by relying on RSU which the private key of the system and parameters are stored on the RSU's TPD.

However, the bilinear pair operations are one of the extreme time-consuming operations and are highly complicity cryptography. Thus, these operations cause massive computational complexity overheads in terms of performance efficiency during the message signing and authentication process.

2) ELLIPTIC CURVE CRYPTOGRAPHY (ECC)

Zhang *et al.* [22] design a chinese remainder theorem to propose an authentication scheme based on conditional privacy-preserving for V2V and V2I communications in VANET. This scheme utilizes fingerprints rather than original identity and password for the verification process. He *et al.* [23] design ID-based schemes to support mutual authentication and privacy-preserving, which could be utilized for securing communication in VANETs. The TA stores it's master secret key on OBU of the vehicle to sign message during the broadcasting process. Cui *et al.* [24] introduced the secure privacy-preserving authentication scheme for VANETs with Cuckoo Filter (SPACF) scheme using software without heavy hardware on a TPD that is fitted with each vehicle for secure communication. In addition, the scheme uses binary search and cuckoo filter methods to improve the process of batch verification. Azees *et al.* [25] proposed an anonymous authentication scheme for avoiding misbehaving vehicles joining into the system. This scheme provides a conditional tracking scheme for tracing the RSUs or vehicles that abuse the VANETs. Cui *et al.* [26] suggested a privacy-preserving data downloading scheme for securing cooperative downloading scenario of V2V and V2I communications; thus, they introduced an edge computing-based secure and privacy-preserving cooperative downloading scheme by using method of lightweight cryptography instead of time-consuming bilinear pairing. Alazzawi *et al.* [27] introduced conditional anonymity scheme based on authentication and integrity of message for V2V and V2I communications in VANET. This scheme address the insider attacker by proposed robust scheme utilizing a pseudonym instead of an original identity.

The operations of ECC are more efficient when compared with the operations of bilinear pair. However, in density areas, incremented numbers of ECC operations such as the point multiplication cause delays in the checking message for the receiver. In the scheme of Zhang *et al.* [22] consists of operations of two point multiplication during message signing, while operations of three point multiplication are included in the authentication process. In the scheme of He *et al.* [23] needs operations of three-point multiplication during message signing and authentication process. In the scheme of Alazzawi *et al.* [27] consists of one point multiplication operation during message signing, while two point multiplication operations are included in the authentication process.

III. PRELIMINARIES

A. NETWORK MODEL

The following components of the proposed scheme in VANETs are described.

- TA: is accountable for the storage, issuance and management in the whole system. Its a trusted third party with high capabilities compared with OBUs and RSUs. It is the only component in VANET that could reveal the vehicle's original identity from the suspect messages.
- RSU: The RSU is an infrastructure device deployed on the roadside. It can communicate with vehicles within its coverage range using a protocol of DSRC [28]. It could check the authenticity of received messages and process them locally or transmits them to TA for further use. Each RSU has a Tamper-Proof Device (TPD) for storing master private keys of the system. Thus, it is possible for an attacker to reveal it.
- vehicle: The vehicle is mounted with an OBU which enable the vehicle to receive and send the message within its coverage area. Each OBU has a TPD and its sensitive information is never revealed. The vehicle communicates wirelessly with others and nearby RSU utilizing DSRC protocol.

B. SECURITY OBJECTIVES

The proposed scheme for VANETs should fulfil the security and piracy requirements, as follow;

- Identity privacy-preserving: Registered components do not have the ability to reveal the original identity of the vehicle. The malicious vehicle cannot reveal the original identity of the vehicle by analyzing intercepted messages.
- Authentication and integrity: Registered components have the ability to check the authenticity of the received messages in VANET. Moreover, the registered components can detect any modification of the message sent by the vehicles.
- Traceability and revocability: The TA has the ability to reveal and revoke the original identity of the vehicle by analyzing its messages if it is necessary.
- Unlinkability: The malicious vehicle does not have the ability by cross-matching two or more received messages which sends by the same source.
- No storage burden: The proposed scheme should be not suffering from storage burden on OBU of vehicle.

IV. THE PROPOSED SCHEME

This section details the proposed scheme without using point multiplication during message signing and verification process. This section mainly includes four phases consisting of the initialization, joining, message signing and verification. These phases of our proposed scheme are based on the scheme of Bayat *et al.* [29]. However, the proposed scheme avoids the employ of the bilinear pairing operation and Map-To-Point hash function that are well-known to be time-consuming, unlike Bayat *et al.* [29].

A. INITIALIZATION

The initialization phase is done by the TA as follows,

- The TA selects a non-singular elliptic curve $E_p(a, b)$ $y^2 + x^3 + ax + b$ mode p, where $a, b \in F_p$, p is a large prime.
- The TA chooses a point P on $E_p(a, b)$ as an adaptive group G generator with order q.
- The TA chooses a key $s \in Z_q^*$ as it's master private key and computes $Pub = sP$ as its master public key.
- The TA selects some secure hash functions h^1, h^2 and h^3, where
  $-h^1 : G \rightarrow Z_q^*$
  $-h^2 : \{0, 1\}^* \times \{0, 1\}^* \times G \rightarrow Z_q^*$
  $-h^3 : \{0, 1\}^* \rightarrow Z_q^*$.
- The TA preloads the $parmas = \{p, q, a, b, P, Pub, h^1, h^2, h^3\}$ as public parameters of the system to each RSU and OBU.
- Finally, the TA saves its master private key s in each TPD on RSU.

B. JOINING

In this phase, vehicle requires the joining process for broadcasting traffic-related message M to others or nearby RSU within its communication range. After obtaining the pseudonym x_i and secret key S_{OID^i} from RSU, vehicle is considered as a registered node in VANET. Therefore, the vehicle broadcasts traffic-related message M to others or neighbor RSU. The joining process are done as the following steps,

- *Vehicle − to − RSU* vehicle chooses a key $z \in Z_q^*$ and calculates pseudonym $PID_{i,1} = zP$ and $PID_{i,2} = OID^i \oplus h^1(zPub)$, where OID_i is original identity of vehicle. Then the vehicle sends the *RSU* with $\{PID^v, T^1, \sigma_{OBU-RSU}\}$, where $PID^v = \{PID_{i,1}, PID_{i,2}\}$ and $\sigma_{OBU-RSU} = h^3(OID^i \| PID_{i,1} \| PID_{i,2} \| T^1)$.
- *RSU* Once receiving the message $\{PID^v, T^1, \sigma_{OBU-RSU}\}$, RSU first checks weather the timestamp T^1 is the freshness or not. Each timestamps are checked as the follow process: T^r is the receiving time, T^{∇} is the predefined time delay, and judgment that weather T^r is less than T^{∇}. If holds, that mean it is the freshness, than RSU calculates $OID^i = PID_{i,2} \oplus h^1(sPID_{i,1})$.
- *RSU − to − TA* The RSU tests whether $\sigma_{OBU-RSU}$=? $h^3(OID^i \| PID_{i,1} \| PID_{i,2} \| T^1)$. If not, it rejects the message, otherwise RSU chooses a key $w \in Z_q^*$ and calculates pseudonym $PID_{j,1} = wP$ and $PID_{j,2} = OID^j \oplus h^1(wPub)$, where OID_j is original identity of RSU. Then it sends message $\{PID^v, PID^r, T^2, \sigma_{RSU-TA}\}$ to the TA, where $PID^r = \{PID_{j,1}, PID_{j,2}\}$ and $\sigma_{RSU-TA} = h^3(OID^i \| OID^j \| T^2)$.
- *TA − to − RSU* Once receiving the message $\{PID^v, PID^r, T^2, \sigma_{RSU-TA}\}$, TA first checks weather the timestamp T^2 is the freshness or not. If so, TA discloses OID^i and OID^j from PID^v and PID^r, respectively. TA than tests whether OID^i and OID^j match the stored value. If so, TA sends message $\{PID^r, T^3, \sigma_{TA-RSU}\}$ to RSU, where $\sigma_{TA-RSU} = h^3(PID^r \| T^3 \| OID^j)$.
- *RSU* Once receiving the message $\{PID^r, T^3, \sigma_{TA-RSU}\}$, RSU tests whether σ_{TA-RSU} =?$h^3(PID^r \| T^3 \| OID^j)$. If so, RSU prepares the pseudonym x_i and secret key S_{OID^i} with its expiration time T_{exp} for the vehicle, as follows,
  RSU chooses random value r_i and then calculates the pseudonym $x_i = h^3(OID^i, r_i, T_{exp})$ and the corresponding secret key $S_{OID^i} = \frac{1}{x+x_i}P$.
- *RSU − to − Vehicle* By using XOR-operation, RSU computes $x_i^{enc} = x_i \oplus h^1(OID^i)$ and $S_{OID^i}^{enc} = S_{OID^i} \oplus h^1(OID^i)$. Then RSU sends message $\{x_i^{enc}, S_{OID^i}^{enc}, T_{exp}, T^4, \sigma_{RSU-OBU}\}$ to vehicle, where $\sigma_{RSU-OBU} = h^3(x_i \| S_{OID^i} \| T_{exp} \| T^4)$.
- *Vehicle* Once receiving the message $\{x_i^{enc}, S_{OID^i}^{enc}, T_{exp} \| T^4, \sigma_{RSU-OBU}\}$, vehicle first checks weather the timestamp T^4 is the freshness or not. If so, by using XOR-operation, it computes $x_i = x_i^{enc} \oplus h^1(OID^i)$ and $S_{OID^i} = S_{OID^i}^{enc} \oplus h^1(OID^i)$. Then checks whether $\sigma_{RSU-OBU}$ =?$h^3(x_i \| S_{OID^i} \| T^4)$. If so, it starts using x_i and S_{OID^i} within its expiration time T_{exp} to broadcast message.

To ensure the security of x_i and S_{OID^i} in VANETs, we advise a renewing method as introduced in [27] for our scheme. Via this process, the vehicle uses x_i and S_{OID^i} for a travelling short-time within VANET. Then, they updates freshen request to get new x_i and S_{OID^i} with new expiration time.

C. MESSAGE SIGNING

After x_i and S_{OID^i} are received, the vehicle first chooses random value $\eta \in Z_q^*$ and computes $R = w^{\eta}$, $T_{i1} = \eta P$, $T_{i2} = \eta \frac{1}{x_i} P$, $T_{i3} = \eta Pub$ and $PID_i = \eta x_i P$. The vehicle then executes the following steps for signing message M_i,

- The vehicle gets a timestamp ts_i and calculates $u = h^3(M_i, R, T_{i1}\ T_{i2}, T_{i3}, T_{exp}, ts_i)$.
- The vehicle generates signature on the message M_i as follows, $V = \frac{1}{\eta}(u + \eta)S_{OID^i}$.
- Finally, the vehicle broadcasts message-signature tuple $\{V, M_i, R, T_{i1}\ T_{i2}, T_{i3}, T_{exp}, PID_i, ts_i\}$ to the recipient.

D. VERIFICATION

Once receiving the message-signature tuple $\{V, M_i, R, T_{i1}\ T_{i2}, T_{i3}, T_{exp}, PID_i, ts_i\}$, the recipient (the RSU or OBU) first checks weather the timestamp ts_i and T_{exp} are the freshness or not. If so, it computes $u = h^3(M_i, R, T_{i1}\ T_{i2}, T_{i3}, T_{exp}, ts_i)$ and it then continues verifying message the following equations,

$$PID_i + T_{i2} = T_{i1} + T_{i2} \tag{1}$$

The proof of Equation 1 is as follows

$$\begin{aligned} &L.H.S \\ &PID_i + T_{i2} = T_{i1} + T_{i1} \\ &\eta x_i P + \eta \frac{1}{x_i} P \end{aligned}$$

$$\eta x_i P + \eta \frac{1}{x_i} P$$
$$\eta P + \eta P$$
$$T_{i1} + T_{i1}$$
$$= R.H.S$$

Then it uses the following equation,

$$T_{i3} + PID_i + V = Rw^u \quad (2)$$

The proof of Equation 2 is as follows

$$L.H.S$$
$$T_{i3} + PID_i + V = Rw^u$$
$$\eta Pub + \eta x_i P + \frac{1}{\eta}(u+\eta) S_{OID^i}$$
$$sP + x_i P + (u+\eta) S_{OID^i}$$
$$(s + x_i) P + (u+\eta) S_{OID^i}$$
$$(s + x_i) P + (u+\eta) S_{OID^i}$$
$$(P, P)^{u+\eta}$$
$$= R.H.S$$

IF the Equation 1 and 2 hold, the recipient accepts the message M_i.

V. SECURITY ANALYSIS

A. FORMAL SECURITY ANALYSIS

To check the validity of OBU and RSU in VANET, the Burrows-Abadi-Needham (BAN) tool is used by the proposed scheme to realize the specific security goals for the process of mutual authentication. [5], [30].

The main notations and meanings used of formal security analysis, as follows,

- §, Y: The original participants.
- X_M: Exchange-messages.
- K: share key.
- $\S| \equiv Y$: § believes Y.
- $\S| \lhd X_M$: § sees X_M.
- $\S| \sim X_M$: § sent X_M.
- $\#(X_M)$: Messages X_M are fresh.
- $\S \overset{K}{\leftrightarrow} Y$: § and Y communicate by K.
- $| \xrightarrow{\text{Pub}} Y$: Y has a public key Pub relevant with a private key Pri.
- $\S \Rightarrow Y$: § has the ability to control Y.
- $(X_M)_K$: The message X_M is hashing by K.

Rules: The essential rules of formal security analysis process are described as follows:

- R_1: $Message - meaning$: $\frac{\S| \equiv \S \overset{K}{\leftrightarrow} Y, \S \lhd (X_M)_K}{\S| \equiv Y| \sim X_M}$, $\frac{\S| \equiv \S \rightarrow \text{Pub} Y, \S \lhd (X_M)_{Pub^-}}{\S| \equiv Y| \sim X_M}$.
- R_2: $Freshness$: $\frac{\S| \equiv \#(X_M)}{\S| \equiv \#(X_M, Y_m)}$.
- R_3: $Nonce - verification$: $\frac{\S| \equiv \#(X_M), \S| \equiv Y| \sim X_M}{\S| \equiv Y| \equiv X_M}$.
- R_4: $Jurisdiction$: $\frac{\S| \equiv Y \Rightarrow (X_M), \S| \equiv Y \equiv X_M}{\S| \equiv X_M}$.

Security goals: The requirements of authentication for VANET should achieve the following security goals.

- $G_1 : TA| \equiv Vehicle| \equiv (OID^i)$.
- $G_2 : TA| \equiv (OID^i)$.
- $G_3 : TA| \equiv RSU| \equiv (OID^j)$.
- $G_4 : TA| \equiv (OID^j)$.
- $G_5 : RSU| \equiv TA| \equiv (\sigma_{TA-RSU})$.
- $G_6 : RSU| \equiv (\sigma_{TA-RSU})$.
- $G_7 : Vehicle| \equiv RSU| \equiv (x_i, S_{OID^i})$.
- $G_8 : Vehicle| \equiv (x_i, S_{OID^i})$.

Idealize the scheme phase: The proposed transformation is viewed in the following:

- The proposed scheme messages are:
  - $PSM_1 : Vehicle \rightarrow RSU : \{PID^v, T^1, \sigma_{OBU-RSU}\}$.
  - $PSM_2 : RSU \rightarrow TA : \{PID_i, PID_{RSU_j}, T_2, \sigma_{RSU-TA}\}$.
  - $PSM_3 : TA \rightarrow RSU : \{PID^r, T^3, \sigma_{TA-RSU}\}$.
  - $PSM_4 : RSU \rightarrow Vehicle$: $\{PID_i, PK_{enc}, \sigma_{RSU-OBU}\}$.
- Idealizing the proposed scheme messages are:
  - $IPSM_1 : Vehicle \rightarrow TA : (OID^i)_{(Pub)}$.
  - $IPSM_3 : RSU \rightarrow TA : (OID^j)_{(Pub)}$.
  - $IPSM_3 : TA \rightarrow RSU : (\sigma_{TA-RSU})_{(Pub)}$.
  - $IPSM_4 : RSU \rightarrow Vehicle : (x_i, S_{OID^i})_{h(OID^i)}$.

Assumptions: The proof of the proposed depends on some the following assumptions:

- $A_1 : TA| \equiv \#(T_2)$.
- $A_2 : RSU| \equiv \#(T_1, T_3)$.
- $A_3 : Vehicle| \equiv \#(T_4)$.
- $A_4 : TA| \equiv | \xrightarrow{Pub} OBU$.
- $A_5 : TA| \equiv | \xrightarrow{Pub} RSU$.
- $A_6 : Vehicle| \equiv Vehicle \overset{OID^i}{\longleftrightarrow} RSU$.
- $A_7 : TA| \equiv Vehicle \Rightarrow (OID^i)$.
- $A_8 : TA| \equiv RSU \Rightarrow (OID^j)$.
- $A_9 : Vehicle| \equiv RSU \Rightarrow (x_i, S_{OID^i})$.
- $A_{10} : RSU| \equiv | \xrightarrow{Pub} TA)$.
- $A_{11} : RSU| \equiv TA \Rightarrow (\sigma_{TA-RSU})$.

Proof: The proof is shown as follow.

Based on $IPSM_1$, we obtain:

$S_1 : TA \lhd (OID^i)_{(Pub)}$

Based on S_1, A_4, and by using **rule of message meaning**, we obtain:

Based on S_2 $TA| \equiv OBU| \sim (OID^i)$

Based on S_2, A_1, and by using **freshness and nonce-verification rules**, we obtain:

$S_3 : TA| \equiv OBU| \equiv (OID^i)$

Therefore, the security goal of (G_1) is achieved.

Based on S_3, A_7, and by using **jurisdiction rule**, we obtain:

$S_5 : TA| \equiv (OID_i)$

Therefore, the security goal of G_2 is achieved.

Based on $IPSM_2$, we obtain:

S_5 $TA \lhd (OID^j)_{(Pub)}$

Based on S_5, A_5, and by using **rule of message meaning**, we obtain:

$S_6 : TA| \equiv RSU| \sim (OID^j)$

Based on S_6, A_1, and by using **freshness and nonce-verification rules**, we obtain:

$S_7 : TA| \equiv RSU| \equiv (OID^j)$

Thus, the security goal of G_3 is achieved.

Based on S_7, A_8, and by using **rule of jurisdiction**, we obtain:

$S_8 : TA| \equiv (OID^j)$

Therefore, the security goal of G_4 is achieved.

Based on $IPSM_3$, we obtain:

$S_9 : RSU \triangleleft (\sigma_{TA-RSU})_{Pub}$

Based on S_9, A_{10}, and by using **rule of message meaning**, we obtain:

$S_{10} : RSU| \equiv TA| \sim (\sigma_{TA-RSU})$

Based on S_{10}, A_2, and by using **freshness and nonce-verification rules**, we obtain:

$S_{11} : RSU| \equiv |TA| \equiv (\sigma_{TA-RSU})$

Therefore, the security goal of G_5 is achieved.

Based on S_{11}, A_{11}, and by using **rule of jurisdiction**, we obtain:

$S_{12} : RSU| \equiv (\sigma_{TA-RSU})$ Thus, the security goal of G_6 is achieved.

Based on $IPSM_4$, we obtain:

$S_{13} : OBU \triangleleft (x_i, S_{OID^i})_{h(OID^i)}$

Based on S_{13}, A_6, and by using **rule of message meaning**, we obtain:

$S_{14} : OBU| \equiv RSU| \sim (x_i, S_{OID^i})$

Based on S_{14}, A_3 and by using **freshness and nonce-verification rules**, we obtain:

$S_{15} : OBU| \equiv RSU| \equiv (x_i, S_{OID^i})$ Therefore, the security goal of G_6 is achieved.

Based on S_{15}, A_9 and by using **jurisdiction rule**, we obtain:

$S_{16} : OBU| \equiv (x_i, S_{OID^i})$ Therefore, the security goal of G_8 is achieved.

Thus, the eight security goals collectively ensure that the RSU and OBU of the proposed scheme are mutually authenticated for V2V and V2I communications.

B. INFORMAL SECURITY ANALYSIS

- Identity privacy-preserving: The TA converts the original identity OID_i of vehicle to a pseudonym x_i. The main aim of this is to support identity privacy-preserving of vehicle concerned. In the proposes scheme, the pseudonym x_i is included in message-signature tuple $\{V, M_i, R, T_{i1}\ T_{i2}, T_{i3}, T_{exp}\ , PID_i, ts_i\}$. Therefore our scheme guarantees identity privacy-preserving requirement in VANET.
- Message integrity and authentication: Based on the signature $V = \frac{1}{\eta}(u + \eta)S_{OID^i}$ on the message M_i, calculating a legitimate signature requires the secret key S_{OID^i}. The attacker does not have the ability to issue a legitimate signature since he/she does not obtain the secret key. In addition, $S_{OID^i} = \frac{1}{x+x_i}P$ confirms that computing the secret keys of other vehicles is impossible for a misbehaving vehicle through its own secret key. Therefore, the attacker cannot forge a registered vehicle in the proposed scheme. Besides, a misbehaving vehicle cannot calculate the secret key of other vehicles through its secret key. Therefore, a vehicle cannot issue a legitimate signature rather than the other vehicles.
- Tractability and revocability: The main aim of the harmful vehicle is to disturb the VANET system by sending a false message to others. TA does not only have the ability to trace the harmful vehicle but also has the ability to revoke during travailing. For example, in V2V communication, vehicle V^i sends a false message to a recipient V^j. Once receiving a false message, vehicle V^j sends the report to the TA. The TA seeking all stored value x_i in its database and detect the pseudonym x_i fulfilling the following equation.

$$x_i T_{i2} = T_{i1} \tag{3}$$

The proof of Equation 3 is as follows

$$\begin{aligned} &L.H.S \\ &x_i T_{i2} = T_{i1} \\ &x_i \eta \frac{1}{x_i} P \\ &\eta P \\ &\quad = R.H.S \end{aligned}$$

After tracing pseudonym x_i on message M_i for vehicle V^i, the TA revokes it from continuing in VANET. The vehicle is no longer able to broadcast false message after the expiration time is expired. Thus, the proposed scheme can fulfil the traceability and revocability requirement in VANET.

- Unlinkability: After expiration time T_{exp} is expired for short time, the vehicle sends renewal request to update x_i and S_{OID^i}, which leads to compute new parameters as $\{V, R, T_{i1}\ T_{i2}, T_{i3}, T_{exp}\ , PID_i\}$ signing message. The vehicle broadcasts different message-signature tuple $\{V, M_i, R, T_{i1}\ T_{i2}, T_{i3}, T_{exp}\ , PID_i, ts_i\}$ during its travel. Therefore, it is no easy for an attacker to cross-link a correlation between the rapid-changing x_i and S_{OID^i} for the vehicle, and the malicious node cannot get vehicle's location. Therefore, the proposed scheme is satisfied unlinkability requirement.
- No storage burden: The vehicle equipped with OBU has to store public parameter of the system and a large of the number of different pseudonyms in its database, which leads to storage overhead is increased. For example, each pseudo ID includes an element in Z_q and G. According to literature, the size of Z_q is 20 bytes and G is 40 bytes. Assume there are 100 pseudo IDs, then the storage overhead of only pseudonym pool is 6 MB. The OBU in the proposed scheme only stores x_i and S_{OID^i} after obtaining from RSU during the mutual authentication process. Therefore, the proposed scheme is satisfied with no storage burden requirement.

TABLE 1. Running Time of Some Cryptographic Operations.

Operations.	The notation of operations	Time(ms)
T_{BP}	The running time of the bilinear pairing operation	5.811
T_{BP}^{SM}	The running time of scalar multiplication operation based on bilinear pairing	1.5654
T_{BP}^{SM-s}	The running time of small scalar point multiplication operation based on bilinear pairing	0.1829
T_{BP}^{PA}	The running time of point addition operation based on bilinear pairing	0.0106
T_{MTP}	The running time of map-to-point hash function	4.1724
T_{ECC}^{SM}	The running time of scalar multiplication operation based on ECC	0.6718
T_{ECC}^{SM-s}	The running time of small scalar point multiplication operation based on ECC	0.0665
T_{ECC}^{PA}	The running time of point addition operation based on ECC	0.0031
T_h	The running time of general hash function operation	0.001

VI. PERFORMANCE ANALYSIS AND COMPARISON

In this section, the comparison between the proposed scheme and existing schemes are analyzed in terms of computation and communication cost as follows.

A. COMPUNCTION COST ANALYSIS AND COMPARISON

In procedures of the existing proposed utilizing bilinear pair $G * G \rightarrow G_T$ such as Zhong *et al.* [19], Pournagh *et al.* [20] and Bayat *et al.* [21], the elliptic curve $y^2 = x^3 + x$ *modn* creates the group G_1, where the group order and n are the 160 and 512 bits prime, respectively. Nevertheless, in the existing proposal utilizing the elliptic curve such as Zhang *et al.* [22], He *et al.* [23] and Alazzawi *et al.* [27], the elliptic curve $y^2 = x^3 + ax + b$ *modn* is accountable for creating the group G_2, where the n and the order of G_2 are the 160 bit prime to realize the same level of secure compared with schemes based on the bilinear pair. For the simplicity of performance efficiency in terms of computation cost, some operations of cryptographic and the respective running time are presented in Table 1.

For simplicity, let *MS*, *SA* and *BA* denote the message signing, individual-verification and batch-verification, respectively.

During the *MS*, scheme of He *et al.* [23] needed three scalar point multiplication operations and three secure hash cryptography functions, thus the total cost is $3T_{ECC}^{SM} + 3T_h \approx 2.0184$. During the *SA*, He *et al.* [23] needed the three scalar point multiplication operations, two secure hash cryptography functions and two point addition operations during *SA*, therefore the total cost is $3T_{ECC}^{SM} + 2T_{ECC}^{PA} + 2T_h \approx 2.0236$. While this scheme needed $(n + 2)$ scalar multiplication operations, $(2n)$ small scalar point multiplication operations, $(2n - 1)$ point addition operations, and $(2n)$ secure hash cryptography functions during the *BA*, therefore the total cost is $(n + 2)T_{ECC}^{SM} + (2n)T_{ECC}^{SM-s} + (2n - 1)T_{ECC}^{PA} + (2n)T_h \approx 0.6718n + 1.3405$.

In the proposed scheme, *MS* consists a one point addition operation and one secure hash cryptography function, therefore the total cost is $1T_{ECC}^{PA} + 1T_h \approx 0.0041$. *SA* and *BA* of the proposed scheme include only one point addition operation and only n point addition operations, receptively. Therefore the total cost of *SA* and *BA* are $1T_h + 2T_{ECC}^{PA} \approx 0.0072$ and $nT_h + nT_{ECC}^{PA} \approx n0.0072$, respectively. The other schemes are also computed their *MS*, *SA* and *BA* in the same above method, as presented in Table 2.

As listed in Table 3, the computation cost of *MS* of the proposed scheme decreases by (2.0184 − 0.0041) / 2.0184 ≈ 99.7%, (2.0236 − 0.0031) / 2.0236 ≈ 99.8% and ((0.6718 * 50 +1.3405) − (0.0031 * 50)) / (0.6718 * 50 +1.3405) ≈ 99.5 % that *MS*, *SA* and *BA* of He *et al.* scheme [23],

TABLE 2. Comparison of Computation Cost.

Scheme	MS	SA	BA
Jianhong et al. [17]	$6T_{BP}^{SM} + 2T_{BP}^{PA} + 1T_{MTP} + 4T_h \approx 13.59$	$3T_{BP}+2T_{BP}^{SM}+1T_{BP}^{PA}+3T_h \approx 20.5774$	$3T_{BP} + (n+1)T_{BP}^{SM} + (2n)T_{BP}^{SM-s} + (3n-2)T_{BP}^{PA}+(3n)T_h \approx 1.966n + 18.9772$
Bayat et al. [21]	$1T_{MTP} \approx 4.1724$	$3T_{BP} + 1T_{BP}^{SM} + 1T_{MTP} \approx 23.1708$	$3T_{BP} + nT_{BP}^{SM} + nT_{MTP} \approx 5.7378n+17.4333$
Zhang et al. [22]	$2T_{ECC}^{SM} + 2T_h \approx 1.3446$	$(3)T_{ECC}^{SM} + 1T_h + 2T_{ECC}^{PA} \approx 2.0226$	$(n+2)T_{ECC}^{SM}+(n)T_{ECC}^{SM-s}+(n)T_{ECC}^{PA}+(2n)T_h \approx 0.7434n + 1.3436$
He et al. [23]	$3T_{ECC}^{SM} + 3T_h \approx 2.0184$	$3T_{ECC}^{SM} + 2T_{ECC}^{PA} + 2T_h \approx 2.0236$	$(n + 2)T_{ECC}^{SM} + (2n)T_{ECC}^{SM-s} + (2n - 1)T_{ECC}^{PA} + (2n)T_h \approx 0.6718n + 1.3405$
Alazzawi et al. [27]	$T_{ECC}^{SM} + 2T_h \approx 0.6738$	$(2)T_{ECC}^{SM} + 1T_h + T_{ECC}^{PA} \approx 1.3477$	$(2)T_{ECC}^{SM}+(2n)T_{ECC}^{SM-s}+(n+1)T_{ECC}^{PA}+(n)T_h \approx 0.1371n + 1.3467$
Our scheme	$1T_{ECC}^{PA} + 1T_h \approx 0.0041$	$1T_h + 2T_{ECC}^{PA} \approx 0.0072$	$nT_{ECC}^{PA} + nT_h \approx n0.0072$

TABLE 3. Improvement of Computation Cost Comparison.

Scheme	MS	SA	BA (50 messages)
Jianhong et al. [17]	99.9%	99.9%	99.9%
Bayat et al. [21]	99.9%	99.9%	99.9%
Zhang et al. [22]	99.6%	99.8%	99.5%
He et al. [23]	99.7%	99.8%	99.5%
Alazzawi et al. [27]	99.3%	99.7%	98.1%

TABLE 4. Comparison of Communication Cost.

Schemes	Single message	Batch messages
Jianhong et al. [17]	388 bytes	388n bytes
Bayat et al. [21]	348 bytes	348n bytes
Zhang et al. [22]	84 bytes	84n bytes
He et al. [23]	144 bytes	144n bytes
Alazzawi et al. [27]	148 bytes	148n bytes
Our scheme	208 bytes	208n bytes

respectively. The performance of the proposed scheme and the other schemes in terms of *MS*, *SA* and *BA* are listed in Table 3.

B. COMMUNICATION COST ANALYSIS AND COMPARISON

For the group G_1 utilizing the bilinear pairing, where the n is 512 bit prime, therefore each element size in G_1 is 128 bytes. Nevertheless, for the group G_2 utilizing the ECC, where n is 160 bit prime, therefore each element size in G_2 is 40 bytes. The output of timestamp, one-way hash and Z_q are 4 bytes, 20 bytes and 20 bytes respectively. As for the message size are excluded in our measurement.

The message size in the He *et al.* scheme [23] is $(40 * 3 + 20 + 4) = 144$ bytes, where the message comprises 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 proposed scheme, the vehicle broadcasts a message-signature tuple with size $(40*4 + 20 * 2 + 8) = 208$ bytes and the message-signature tuple content is four element in $\{T_{i1}, T_{i2}, T_{i3}, PID_i \in G\}$, two elements in $\{V, R \in z_q\}$, and two timestamps $\{T_{exp}, ts_i\}$. In the same method, the communication cost of other schemes are also computed. The overall communication cost is listed in Table 4.

VII. CONCLUSION

In this article, we propose an authentication scheme based on conditional privacy-preserving without using point multiplication operations of ECC. The main aim of the proposed scheme is to secure V2V and V2I communications and perform better performance efficiency. The proposed scheme only depends on ECC based on a point addition operation instead of a point multiplication operation during the signing and verifying messages. The security analysis shows that the security and privacy requirements for VANETs are fulfilled by the proposed scheme. In addition, the performance analysis proves that the computation cost of the proposed scheme is lower than other existing schemes. Lastly, for large-scale networks, the proposed scheme is more fitting.

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

[3] 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.

[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] S. A. Alfadhli, S. Lu, A. Fatani, H. Al-Fedhly, and M. Ince, "SD2PA: A fully safe driving and privacy-preserving authentication scheme for VANETs," *Hum.-Centric Comput. Inf. Sci.*, vol. 10, no. 1, pp. 1–25, Dec. 2020.

[6] M. A. Al-Shareeda, M. Anbar, I. H. Hasbullah, S. Manickam, and S. M. Hanshi, "Efficient conditional privacy preservation with mutual authentication in vehicular ad hoc networks," *IEEE Access*, vol. 8, pp. 144957–144968, 2020.

[7] Z. Lu, G. Qu, and Z. Liu, "A survey on recent advances in vehicular network security, trust, and privacy," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 2, pp. 760–776, Feb. 2019.

[8] 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.

[9] Z. Lu, Q. Wang, G. Qu, H. Zhang, and Z. Liu, "A blockchain-based privacy-preserving authentication scheme for VANETs," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 27, no. 12, pp. 2792–2801, Dec. 2019.

[10] 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.

[11] M. Azees, L. J. 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.

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

[13] 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.

[14] 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.

[15] 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.

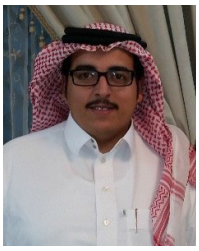
[16] C.-C. Lee and Y.-M. Lai, "Toward a secure batch verification with group testing for VANET," *Wireless Netw.*, vol. 19, no. 6, pp. 1441–1449, Aug. 2013.

[17] Z. Jianhong, X. Min, and L. Liying, "On the security of a secure batch verification with group testing for VANET," *Int. J. Netw. Secur.*, vol. 16, no. 5, pp. 351–358, 2014.

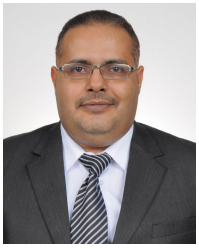
[18] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, and C. Hu, "Distributed aggregate privacy-preserving authentication in VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 3, pp. 516–526, Mar. 2017.

[19] H. Zhong, S. Han, J. Cui, J. Zhang, and Y. Xu, "Privacy-preserving authentication scheme with full aggregation in VANET," *Inf. Sci.*, vol. 476, pp. 211–221, Feb. 2019.

[20] S. M. Pournaghi, B. Zahednejad, M. Bayat, and Y. Farjami, "NECPPA: A novel and efficient conditional privacy-preserving authentication scheme for VANET," *Comput. Netw.*, vol. 134, pp. 78–92, Apr. 2018.
[21] 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. 1–16, Jun. 2019.
[22] 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.
[23] 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.
[24] 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.
[25] 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.
[26] J. Cui, L. Wei, H. Zhong, J. Zhang, Y. Xu, and L. Liu, "Edge computing in VANETs—An efficient and privacy-preserving cooperative downloading scheme," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 6, pp. 1191–1204, Jun. 2020.
[27] 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.
[28] J. B. Kenney, "Dedicated short-range communications (DSRC) standards in the united states," *Proc. IEEE*, vol. 99, no. 7, pp. 1162–1182, Jul. 2011.
[29] M. Bayat, M. Barmshoory, S. M. Pournaghi, M. Rahimi, Y. Farjami, and M. R. Aref, "A new and efficient authentication scheme for vehicular ad hoc networks," *J. Intell. Transp. Syst.*, vol. 24, no. 2, pp. 171–183, 2020.
[30] M. Burrows, M. Abadi, and R. M. Needham, "A logic of authentication," *Proc. Roy. Soc. A, Math., Phys. Eng. Sci.*, vol. 426, no. 1871, pp. 233–271, 1989.



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 Assistant Professor with the College of Computer Science and Engineering, University of Ha'il. His current research interests include wireless sensor networks, energy management & 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 Ha'il, Saudi Arabia. He is also an Assistant Professor with Hodeidah University, Yemen. In his research area, he has published many articles in reputed journals and conferences. (Based on document published on 25 May 2020). His research interests include wireless networks, mobile networks, vehicle networks, WSN, and image processing.

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 Ha'il, where he is also an Assistant 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.