IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received July 27, 2021, accepted August 9, 2021, date of publication August 11, 2021, date of current version August 19, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3104148

Towards Identity-Based Conditional Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks

MAHMOOD A. AL-SHAREEDA, MOHAMMED ANBAR, SELVAKUMAR MANICKAM, AND IZNAN HUSAINY HASBULLAH

National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia (USM), Gelugor, Penang 11800, Malaysia

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

This work was supported by Universiti Sains Malaysia (USM) external grant number 304/PNAV/650958/U154.

ABSTRACT Vehicular ad hoc networks (VANETs) have become increasingly common in the past decades and provides essential and efficient communication for vehicles within intelligent transportation systems. Securing the VANETs wireless communication channel is one of the principal challenges in VANETs since existing security schemes are still vulnerable to security and privacy issues and have substantial computational and communicational overheads. To overcome these issues, this paper focuses on enhancing an authentication scheme based on conditional privacy-preserving and improving its performance efficiency. This paper reviews the security vulnerabilities of the existing schemes. It also proposes enhancements to the identity-based conditional privacy-preserving authentication scheme to secure and improve the efficiency of VANETs communications. The proposed scheme not only satisfies the security and privacy requirements but also has been proven secure under the random oracle model. Finally, the performance evaluation shows that the proposed scheme is more efficient computationally and communicational than the existing schemes in signing and verifying VANETs messages.

INDEX TERMS Vehicular ad-hoc network (VANET), side-channel attacks, unlinkability, random oracle model, privacy preserving.

I. INTRODUCTION

Recently, vehicular ad hoc networks (VANETs) [1] have become more promising, along with the rapid development of wireless technology (e.g., GSM, WiMAX and 5G) and intelligent transportation systems (ITSs) [2], [3], which enable convenient and integrated services for mobile devices. As [4] indicated, there are different forms of application in various fields of the Internet of Things, such as vehicular communications. Vehicles are commonly fitted with wireless communication devices (e.g., OBU, Wi-Fi, Bluetooth), processors, and sensors (e.g., position, axle weight and spacing, deceleration, speed) to complete all the tasks of computation, communication and terminal perception [5]. Vehicles can share and communicate information between each other, because VANETs are a node wireless environment [6]. Police may request information from drivers, however, when drivers communicate in a VANET environment that has security threats, drivers must pay particular attention to their own sensitive personal information (e.g., movements, history, and identity of location). In such a communication process, it is possible that this useful data can be stolen by an attacker. This is why governments, mobile users, and even researchers, are focussing more on security problems in order to improve the implementation of smart applications in real-time [7], [8].

The technology of Dedicated Short-Range Communications (DSRC) is a wireless communication protocol that enables vehicles to communicate with each other and other infrastructure via vehicle-to-vehicle (V2V) communication and Vehicle-to-infrastructure (V2I), respectively. As shown in Fig. 1, the trusted authority (TA), roadside unit (RSU) and on-board unit (OBU) are the three major units in a VANET. In a VANET, the vehicles are considered as mobile devices fitted with OBUs that include vehicular sensors, protocols of IEEE 802.11p, and a GPS receiver [9]. It is the OBU's responsibility to record information (e.g., location, velocity) during

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

the drive and to match other nodes in VANETs. The RSU is located on the side of road and is used as a roadside infrastructure for connected vehicles via secure communication channels. In addition, the RSU can exchange traffic-related messages and collect messages by equipping it with wireless devices to find out about the local situation [10].

VANETs face serious security challenges, such as confidentiality and information integrity, because of the features above and their inherent transparency. Therefore, it is increasingly important for protocols to provide secure and user-friendly drivers authentication in order to ensure secure communications [11]. VANETs, like any other wireless network, are vulnerable to malicious attacks [12]–[15], which means that more and more researchers are watching and participating in conditional privacy-preserving authentication.

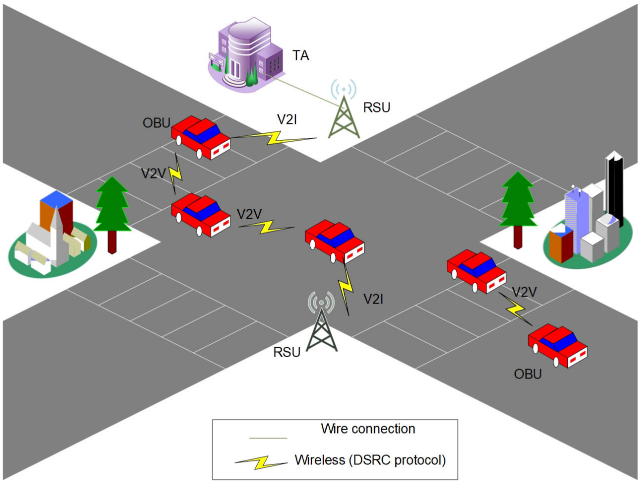


FIGURE 1. A typical VANET scenario.

Many researchers have improved conditional privacy-preserving authentication schemes for VANETs, including those proposed during the communication period in order to preserve privacy, and those proposed for reducing the cost of communication/computation. Nevertheless, current conditional privacy-preserving authentication schemes usually have deficiencies against an external attacker. VANETs still need a safe and efficient security scheme based on conditional privacy-preserving. This research aims to propose an efficient and secure security scheme based on conditional privacy-preservation to address the security vulnerabilities and privacy issues of the existing schemes.

The important contributions of this paper include the following:

- A secure VANET communication by improving the conditional privacy-preserving authentication scheme to overcome the shortcomings of the existing schemes,
- An in-depth analysis of the existing scheme vulnerabilities,
- A comprehensive security analysis on the proposed scheme to prove its security and fulfillment of the VANETs security and privacy requirements,
- A security scheme that has lower computation and communication overheads compared to the existing schemes.

The remainder of the framework for this paper is structured as follows to present our work and contributions. Section II introduces the related work in recent years. In Section III, we present preliminary information on the proposals of this paper. We review the scheme of Alazzawi *et al.* [16] in Section IV. Section V also highlights its current security vulnerabilities. Section VI describes the principal improvements made by our proposal and Section VII provides an analysis of its security. In Section VIII, we present a performance evaluation to demonstrate that the overall outlook of our scheme is reasonable. Finally, in the last section, we provide some conclusions.

II. RELATED WORK

A wide range of research in the recent past has focused on an efficient and secure security scheme based on conditional privacy-preservation in VANETs.

In 2008, Zhang *et al.* [17] proposed a batch authentication system based on identity with bilinear pairing mapping. Shamir [18] first proposed an identity-based authentication system in 1984, which extracts the public key from the information (e.g. name, ID card, etc.) about the identity and creates a TA's secret key. The TA certification burden is avoided in Zhang *et al.* [17] and a privacy unlinkability is successfully accomplished because the TA has a secret TA master key, which is supposed to not be compromised by a malicious attacker. Besides, the vehicle uses an anonymous identity during transmission to hide the original identity rather than broadcasting the message attached to the vehicle's original identity. Finally, during the phase of signature verification, many messages broadcast simultaneously from other vehicles using a batch-authenticated method, which greatly reduces the system overhead. Zhang *et al.* [17] could not satisfy conditional privacy preservation, and they also needed to address other secure problems in their scheme.

In 2013, Lee and Lai [19] pointed out that Zhang *et al.* [17] couldn't withstand a certain number of VANET security attacks. Firstly, the verifier may verify a signature previously verified, because of the lack of equipment, to increase the overhead for the computation. They therefore could not withstand the reply attack. Moreover, the scheme of Zhang *et al.* [17] could not satisfy non-repudiation. The signer could deny that a trusted institution had sent the disputed messages, by tracing identity information. Lee and Lai [19] proposed an improved scheme for privacy preservation to eliminate the security problems that exist in the scheme of Zhang *et al.* [17].

In 2014 and 2015, it was found that the scheme of Lee and Lai [19] was not able to withstand impersonation attack, see Zhang *et al.* [20] and Bayat *et al.* [21]. An attacker could advantageously transmit a false message by simulating a legal vehicle. Therefore, two improved schemes have been proposed to eliminate the difficulties with the scheme of

Lee and Lai [19]. Nevertheless, He *et al.* [22] also indicated, in 2015, that a modification attack could affect their scheme. In other words, during the broadcast message, a malicious attacker could change the vehicle signature. There is therefore a conditional system of privacy protection that addresses security attacks and reduces system costs.

Although the scheme of He *et al.* [22] is able to tackle a certain number of the VANETs' security issues, the side-channel attack also affects them. The TA master secret key was saved in the Tamper Proof Device (TPD) of the vehicle in their scheme, and assumed that no attacker could compromise it. However, certain information saved in the TPD could also be obtained through a side channel from an attacker. The VANET system collapses after the attacker has obtained the master secret key.

In 2016, a side channel attacker resistance scheme was proposed by Zhang *et al.* [23]. They updated periodically information from a TPD, so that even if the attacker could acquire useful information via a side channel attack, it would be updated and would be unable to provide the attacker with certain useful information.

In 2019, Zhong *et al.* [24] indicated that in Lei Zhang *et al.* [23] it was not specified who is the aggregator in the aggregation phase, with a huge overhead of verification signatures. They therefore proposed a better scheme to deal with these problems. But Zhong *et al.* [24] uses bilinear pair combinations and map-to-point operations, which leads to high computational overhead.

Recently, Chen *et al.* [25] performed the security analysis of the emerging technology of Connected Vehicle (CV) by finding the current algorithms of signal control system that are strongly susceptible for congestion attacks. Feng *et al.* [26] investigated the traffic control systems susceptibility in a connected environment including OBUs, RSUs vehicle detectors and signal controllers that are attack surfaces by sending falsified data. Azees *et al.* [27] offered a conditional tracking mechanism by proposing a anonymous authentication scheme for avoiding the adversaries entering into the VANET. Zhang *et al.* [28] addressed the performance constraints of vehicular authentication by introducing a conditional privacy-preserving authentication scheme that is based on Chinese remainder theorem (CRT). Cui *et al.* [29] addressed a data downloading requests by designing the concept of edge computing for the resource allocation efficiency of the VANET. Lai *et al.* [30] proposed a several solutions namely a cooperative message authentication, secure group setup with privacy preservation and distributed group key management for addressing issues regarding security and privacy in a 5G-enabled vehicular networks. Cui *et al.* [31] proposed a content sharing scheme for the fast-moving character of vehicles in 5G-enabled vehicular networks. Alazzawi *et al.* [16] proposed an improved authentication scheme with conditional anonymity based on elliptic curve cryptography (ECC) to make secure, efficient, and practical applications of the VANET. Nevertheless, according to our analysis, that scheme cannot resist side channel attacks and has weaker privacy-preserving in term of unlinkability as well as has no flexibility to modify the passwords.

For an improved security scheme based on conditional privacy-preserving in VANETs, we also use an ECC algorithm to conduct a new conditional privacy-preserving authentication scheme. A formal and informal security analysis of our scheme shows its security and demonstrates that it can overcome the shortcomings of the scheme of Alazzawi *et al.* An analysis of the performance of our proposal shows that it offers a lower overhead for communication and computational cost.

III. BACKGROUND AND PRELIMINARIES

In this section, the necessary mathematical tools used in this study are introduced. Then, the network model for vehicular communication and the thread models are discussed. Finally, the security and privacy requirements in the proposed scheme are described. Table 1 describes some notation.

TABLE 1. Notation and their descriptions.

Notation	Descriptions
E	An elliptic curve
G	An additive group based on E
a, b	Two large prime numbers
p	large prime number
P	The base generator P∈ G
h_1, h_2, h_3	Three one-way hash functions
RID_r,RID_v	Original identity of the RSU and vehicle
PW	Password
s	The private master key of the system
Pub	The public key of the TA
Ps	pseudonym of vehicle
r	Random integer
E(.)/D(.)	Secure symmetric encryption and decryption function
k_{ij}	Key of symmetric function
$\|\|$	Concatenation operation
$\oplus$	XOR operator
L_{PID_v}	List of OBU's local Pseudo identities
PID_v	Pseudo identity of vehicle
Sk	signature key of vehicle
T	Timestamp
T_{sk}	Timestamp of signature key
M_i	safety-related message
σ	signature of sent message
GMS	The generation of a message and signature
VSM	The verification of the single message
VMM	The verification of multiple messages

A. MATHEMATICAL TOOLS

Miller [32] proposed ECC in 1985 and it has since been widely employed in the design of digital signatures and security algorithms. An elliptic curve over a finite field F_p is represented by the equation $y^2 = x^3 + ax + bmodp$, where $(4a_3+27b^2)$ mod p$\neq 0$ and x, y, a, b $\in F_p$. Let O be an infinite point, and G an additive group of order q and generator P. All the points on the elliptic curve E are contained in the additive group G. Let P and Q be two points on the elliptic curve E. then $P + Q = R$ is defined by the operation of addition in G. The scalar multiplication of points in G is defined by $s.P = P + P + \ldots\ldots + P$ (s times).

The discrete logarithm problem in an elliptical curve (ECDLP) is computationally impossible [33]. The main use of the ECDLP is to find an integer s that fulfills $Q = sP$ based on E, with two points P and Q of G.

B. NETWORK MODEL

Generally, the components of an VANET are classified into two layers. The TA runs on the top layer, while the vehicle and RSU work on the bottom layer. In the network model, we use three components of our proposed scheme. The description of each component of the VANET is provided in the following:

1) TA

The TA is fully trusted authority in the VANET system. The TA has significant computing power and storage capacity compared with RSUs and OBUs. The TA is responsible for registering the rest of the components in the VANET. When a dispute occurs, the TA can further trace and disclose the vehicle's original identity from the transmitted message [34].

2) RSU

The RSU in a VANET is a base station that runs as an intermediate component along the roadside between the vehicles and the TA. It has less computational power and storage capacity than the TA. The DSRC 5.9-GHz Protocol [35], [36] communicates with and handles vehicles in its communication field. The RSU checks the authenticity of messages sent from different sources and transmits them for further analysis to the TA or distributes them to vehicles in its communications range.

3) OBU

Each vehicle in a VANET has a wireless communication device, an OBU, which allows the communication of messages with other nodes by using the DSRC 5.9-GHz protocol [35], [36]. TPD is provided in each OBU. There is a Graphical User Interface (GUI) for drivers to interact with. A OBU has less computing power and storage capacity than the RSU and TA.

C. THREAD MODEL

The VANETs are easily vulnerable to some security attacks due to the openness of the communications environment of a VANET. In this subsection, some security attacks that can be mounted against VANETs are introduced:

1) REPLAY ATTACK

The attacker replays a legitimate signature previously received by the recipient, which will raise the computational overhead of the system because the corresponding device is not available.

2) IMPERSONATION ATTACK

An adversary could impersonate a legitimate vehicle in order to transmit fake messages and gain a benefit. One attacker could, for instance, imitate an ambulance in a traffic jam for green channels.

3) MODIFICATION ATTACK

If the recipient receives a message from another vehicle, the verifier must test whether an attacker has modified the message.

4) SIDE CHANNEL ATTACK

In the TPD, information can be obtained through a side channel attack by an attacker. When the system master key or original identity of a vehicle has been identified by malicious attackers, the VANET structure collapses.

D. SECURITY AND PRIVACY REQUIREMENTS

A conditionally privacy-preserving security scheme should fulfill the security and privacy requirements for VANETs as follows:

1) MESSAGE CONFIDENTIALITY

In a VANET system, the scheme should be satisfied the message confidently requirement, which means that vehicle's sensitive information must be secure, and must not be retrieved by the adversary.

2) TRACTABILITY AND REVOCATION

The TA should be able to disclose the original identity of a malicious vehicle so that the TA can trace and revoke it from further participation in the VANET.

3) NON-FORGERY

The vehicle's signature is unique and the attacker can not generate another valid signature on behalf of the vehicle.

4) FREE FROM SIDE CHANNEL ATTACK

The attacker can not obtain useful information stored in the TPD of a vehicle via a side channel.

5) UNLINKABILITY

The adversary should not be able to decide whether various messages have been signed by the same vehicle.

6) MODIFICATION OF PASSWORD

The vehicle owner should be able to modify the password anywhere anytime.

IV. REVIEWS OF THE SCHEME OF ALAZZAWI *et al.* FOR VANETs

There are six subsections in Alazzawi *et al.*'s scheme [16], including (a) initialization phase, (b) vehicle registration phase, (c) vehicle joining phase, (d) broadcasting and verification phase, (e) vehicle revocation phase and (f) renewal phase. All the notions in that paper are presented in Table 1. We briefly describe them as follows:

A. INITIALIZATION PHASE

The four steps that follow are the TA initialization procedures, when the system parameters are set.

- Let G be the group of an elliptic curve determined by a prime number p and a generator P.
- The TA generates s at random from Z_q^* as its private key, and calculates the public key Pub $= s.P$.
- Three secure cryptographic hash functions are selected by the TA: $h_1 : G \to Z_q^*, h_2 : \{0, 1\}^* \times \{0, 1\}^* \times G \to Z_q^*$, and $h_3 : \{0, 1\}^* \to Z_q^*$.
- Finally, TA preloads for each legal RSU the private key s of the system. Moreover, the system parameters {q, Pub, P, h_1, h_2, h_3} are broadcast by the TA.

B. VEHICLE REGISTRATION PHASE

If the driver of a new vehicle is ready for VANET membership, he/she has to execute the following steps, as shown in Fig. 2.

- (a) The driver first submits to the TA, via a secure channel, with their original identity RID_v and password PW.
- (b) After the TA tests the the validity of RID_v, (c) it calculates the pseudonym Ps=$h_3(RID_v \| \text{s})$.
- Finally, (d) the TA saves the tuple <RID_v, PW, Ps> to the registration list and (e) preloads Ps to the TPD of the vehicle.

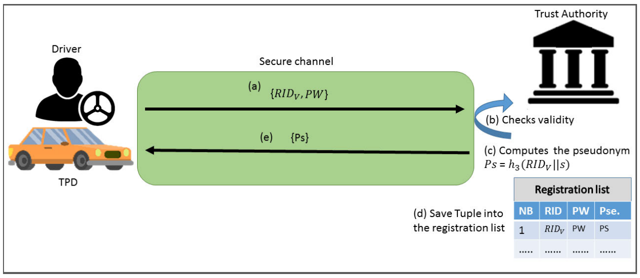


FIGURE 2. TA registers OBU by Alazzawi *et al.*'s scheme.

C. VEHICLE JOINING PHASE

In order to begin the OBU, the vehicle driver should provide TPD feedback with RID_v and PW to check the driver's validity. If valid, the OBU begins the process of joining and creates a mutual authentication as shown in Fig. 3. The following steps complete the OBU joining phase:

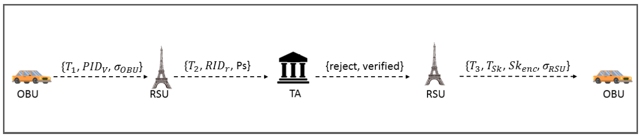

$\{T_1, PID_V, \sigma_{OBU}\}$
$\{T_2, RID_r, \text{Ps}\}$
{reject, verified}
$\{T_3, T_{Sk}, Sk_{enc}, \sigma_{RSU}\}$
OBU
RSU
TA
RSU
OBU

FIGURE 3. OBU joining to RSU phase by Alazzawi *et al.*'s scheme.

- $OBU_i \longrightarrow RSU_j$: The OBU generates r at random from Z_q^* and calculates:

$$PID_{v1} = rP$$
$$PID_{v2} = Ps \oplus h_1(rPub)$$

  Then, the OBU transmits to the RSU with the message $\{T_1, PID_v, \sigma_{OBU}\}$, where PID_v=$\{PID_{v1}, PID_{v2}\}$ and $\sigma_{OBU} = h_3(T_1 \| \text{Ps})$.
- $RSU_j \longrightarrow TA$: The RSU firstly checks the timestamp validity T_1 after it receives the message $\{T_1, PID_v, \sigma_{OBU}\}$ from the OBU. If T_1 is not valid, the RSU rejects this message. Otherwise, RSU calculates Ps $= PID_{v2} \oplus h_1(s.PID_{v1})$ and tests whether $\sigma_{OBU} \overset{?}{=} h_3(T_1 \| \text{Ps})$. If not, the message is rejected by the RSU; otherwise, it transmits $\{T_2, RID_r, \text{Ps}\}$ to the TA.
- $TA \longrightarrow RSU_j$: The TA firstly checks the timestamp validity T_2 after it receives $\{T_2, RID_r, \text{Ps}\}$ from the RSU. If T_2 is not valid, the TA does not accept the message. Otherwise, the TA tests whether the values stored for $RIDr$ and ps match. Finally, the TA transmits {reject, verified} to the RSU.
- $RSU_j \longrightarrow OBU_i$: After the RSU checks whether the message content is {verified}, the signature Sk prepares it for the vehicle with its expiry time T_{Sk}, where Sk= $s.h_2$ $(PID_{v1} \| \; PID_{v2} \| \; T_{Sk})$. Finally, the RSU transmits $\{T_3, T_{Sk}, Sk_{enc}, \sigma_{RSU}\}$ to the OBU, where Sk_{enc} = Sk $\oplus h_1(s.PID_{v1})$ and $\sigma_{RSU} = h_2(\text{Sk} \, \| T_3 \| \; T_S)$.
- OBU_i: The OBU firstly checks the timestamp validity T_3 after it receives the message $\{T_3, T_{Sk}, Sk_{enc}, \sigma_{RSU}\}$ from the RSU. Then the OBU calculates Sk $= Sk_{enc} \oplus h_1(r.\text{Pub})$. It then tests whether $\sigma_{RSU} \overset{?}{=} h_2(\text{Sk} \, \| T_3 \| \; T_{Sk})$. If it is right, the OBU accepts Sk as its corresponding private key.

D. BROADCASTING AND VERIFICATION PHASE

1) BROADCASTING

If the OBU wishes to sign message M_i, the following steps must be executed:

- The OBU calculates the signature of the message as followas: $\sigma_m = \text{Sk} + r.h_3(M_i \| \text{T})$.
- The OBU calculates $w = h_3(M_i \| \text{T}).PID_{v1}$; this is used for mitigating the time of recipient verification.
- Finally, the message $\{M_i, \text{T}, T_{Sk}, PID_{v1}, \text{w}, \sigma_m\}$ is sent to the recipient.

2) VERIFICATION

Alazzawi *et al.*'s scheme has two versions of the message verification process: single message verification and batch message verification. We will describe them briefly.

a: SINGLE MESSAGE VERIFICATION

The recipient checks Equation 1 when the message is received and accepts the message if it holds.

$$\sigma_m P = h_2(PID_{v1}||PID_{v2}||T_{Sk})Pub + w \qquad (1)$$

The proof of Equation 1 is as follows:

$$\begin{aligned}
&= (\mathrm{Sk} + r.h_3(M_i||T)).P \\
&= (s.h_2(PID_{v1}||PID_{v2}||T_{Sk}) + r.h_3(M_i||T)).P \\
&= h_2(PID_{v1}||PID_{v2}||T_{Sk})s.P + h_3(M_i||T)r.P \\
&= h_2(PID_{v1}||PID_{v2}||T_{Sk})\mathrm{Pub} + h_3(M_i||T)PID_{v1} \\
&= h_2(PID_{v1}||PID_{v2}||T_{Sk})\mathrm{Pub} + w.
\end{aligned}$$

b: BATCH MESSAGE VERIFICATION

If a recipient receives a large number of messages $\{M_i{}^1$, T^1, $T_{Sk}{}^1$, $PID_{v1}{}^1$, w^1, $\sigma_m{}^1\}$, $\{M_i{}^2$, T^2, $T_{Sk}{}^2$, $PID_{v1}{}^2$, w^2, $\sigma_m{}^2\} \ldots \{M_i{}^n, T^n, T_{Sk}{}^n, PID_{v1}{}^n, w^n, \sigma_m{}^n\}$, the signatures can be simultaneously verified as follows:

$$\left(\sum_{i=1}^{n}(x_i\sigma_{m,i})\right).P = \left(\sum_{i=1}^{n}\left(x_i h_2(PID_{v1}||PID_{v2}||T_{Sk})\right)\right)Pub + \sum_{i=1}^{n}(x_i w) \quad (2)$$

E. VEHICLE REVOCATION PHASE

If a report is received about a misbehaving vehicle, the TA and RSU can trace and revoke a malicious vehicle cooperatively. The TA acquires the pseudonym of the vehicle as follows:

$$\mathrm{Ps} = PID_{v2} \oplus h_1(s.PID_{v1})$$

The Ps is added by the TA to the certificate revocation list (CRL) and this is then sent to the RSUs.

F. RENEWAL PHASE

The OBU must renew the Sk when T_{Sk} expires, which is done as follows.

- $OBU_i \longrightarrow RSU_j$: The OBU generates r^{new} at random from Z_q^* and calculates

  $$\begin{aligned} PID_{v1}^{new} &= r^{new}P \\ PID_{v2}^{new} &= Ps \oplus h_1(r^{new}Pub) \end{aligned}$$

  Then, the OBU transmits $\{T_1, T_{Sk}\ PID_v^{new}, PID_v, \sigma_v\}$ to the RSU, where $PID_v^{new} = \{PID_{v1}^{new}, PID_{v2}^{new}\}$ and $\sigma_v = \mathrm{Sk} + r.h_3(T_1||PID_{v1}^{new}||PID_{v1}^{new})$.
- $RSU_j \longrightarrow OBU_i$: The RSU firstly checks the timestamp validity T_1 after it receives the message $\{T_1, T_{Sk}\ PID_v^{new}$, $PID_v, \sigma_v\}$ from the OBU. If it is found to be valid, it then tests the expiration time T_{Sk} (the time to apply for a new Sk was set by the OBU). If it is not valid, the RSU does not accept the message, and a vehicle join phase must be implemented by the OBU. Otherwise, the following equation is used to check the validity of the vehicle.

  $$\begin{aligned} \sigma_v.P = h_2(&PID_{v1}||PID_{v2}||T_{Sk}) \\ &+ h_2(PID_{v1}^{new}||PID_{v2}^{new}||T_1)PID_{v1} \quad (3) \end{aligned}$$

  If Equation 3 does not hold, the RSU does not accept the message; otherwise, the RSU prepares a new signature and completes the process as in the previous phase.

V. SECURITY ANALYSIS OF THE SCHEME OF ALAZZAWI *et al.*

For the sake of secure, efficient, and practical use of VANETs, the scheme of Alazzawi *et al.* proposed an improved authentication scheme with conditional anonymity based on ECC. However, this scheme has three weaknesses: (a) it is vulnerable to the side channel attack, (b) it fails to ensure the unlinkability of messages, and (c) it also fails to allow modifying passwords. Details of these three weaknesses are presented in what follows.

A. SIDE CHANNEL ATTACK

The scheme of Alazzawi *et al.* is vulnerable to a side channel attack. To authenticate with a VANET, a vehicle may need to prove its own pseudonym, which is usually stored on the vehicle in the TPD. Besides the storage of pseudonyms, TPD also offers computational services, where the pseudonym of vehicle is concerned. The scheme of Alazzawi *et al.* is designed to use the TPD to securely store the pseudonym of the vehicle and to carry out the associated calculations, which they assume can never be compromised by adversaries. However, this assumption could be too strong in practice to be realistic. In particular, the TPD may confuse vehicle shocks caused by uneven road surfaces under VANET and erase secrets in VANET conditions [37]. Adversaries can also collect enough TPD secret information by side channel attacks such as electromagnetic radiation [38] and an analysis of power consumption [39].

After obtaining the pseudonym from the TPD of a legitimate vehicle, the adversary could execute the following steps:

- The adversary $\longrightarrow RSU_j$: The adversary generates r^F at random from Z_q^* and calculates

  $$\begin{aligned} PID_{v1}{}^F &= r^F P \\ PID_{v2}{}^F &= Ps \oplus h_1(r^F Pub) \end{aligned}$$

  Then, the adversary transmits $\{T_1, PID_v{}^F, \sigma_F\}$ to the RSU, where $PID_v{}^F = \{PID_{v1}{}^F, PID_{v2}{}^F\}$ and $\sigma_F = h_3(T_1||\mathrm{Ps})$.
- $RSU_j \longrightarrow TA$: The RSU firstly checks the timestamp validity T_1 after it receives the message $\{T_1, PID_v{}^F, \sigma_F\}$ from the adversary. If T_1 is not valid, the RSU rejects this message. Otherwise, RSU calculates $\mathrm{Ps} = PID_{v2}{}^F \oplus h_1(s.PID_{v1}{}^F)$ and tests whether $\sigma_F \overset{?}{=} h_3(T_1||\mathrm{Ps})$. If not, the message is rejected by the RSU; otherwise, it transmits the message $\{T_2, RID_r, \mathrm{Ps}\}$ to the TA.
- $TA \longrightarrow RSU_j$: The TA firstly checks the timestamp validity T_2 after it receives the message $\{T_2, RID_r, \mathrm{Ps}\}$ from the RSU. If T_2 is not valid, the TA does not accept the message. Otherwise, the TA tests whether the values stored for *RIDr* and ps match. Finally, the TA transmits the message {reject, verified} to the RSU.
- $RSU_j \longrightarrow$ The adversary: After the RSU checks whether the message content is {verified}, the signature Sk prepares it for the vehicle with its expiry time T_{Sk}, where $\mathrm{Sk} = s.h_2(PID_{v1}{}^F||PID_{v2}{}^F||T_{Sk})$. Finally, the RSU

transmits $\{T_3, T_{Sk}, Sk_{enc}, \sigma_{RSU-F}\}$ to the adversary, where $Sk_{enc} = \text{Sk} \oplus h_1(s.PID_{v1}{}^F)$ and $\sigma_{RSU-F} = h_2(\text{Sk} \,||T_3||\, T_S)$.

- The adversary: The adversary firstly checks the timestamp validity T_3 after it receives the message $\{T_3, T_{Sk}, Sk_{enc}, \sigma_{RSU-F}\}$ from the RSU. Then the adversary calculates $\text{Sk} = Sk_{enc} \oplus h_1(r^F.\text{Pub})$. It then tests whether $\sigma_{RSU-F} \overset{?}{=} h_2(\text{Sk} \,||T_3||\, T_{Sk})$. If so, the adversary uses it to sign a fake message.

B. NOT ACHIEVING UNLINKABILITY

The scheme of Alazzawi *et al.*'s conditional anonymity is very efficient. It generates r at random from Z_q^* and calculates $PID_{v1} = rP$ and $PID_{v2} = Ps \oplus h_1(rPub)$. Then the scheme uses this to sign many transmitted messages, leading to the possiblity that an adversary can link them, i.e., determine if many messages have been sent from the same vehicle. However, any tracking of information that is sensitive, such as an identity or a location, can lead to physical harassment of a driver, kidnapping, and murder (e.g., intercepting malicious opponents and replacing intercepted messages by fabricated messages to re-route victims' vehicles). Preserving privacy is an important issue in this context, given the sensitiveness of the information exchanged [40].

C. NOT ENABLING MODIFIABILITY OF PASSWORDS

The TPD of the scheme of Alazzawi *et al.* holds a lot of valuable sensitive data, such as Ps, PID_{v1}, PID_{v2}, r, Sk. During the vehicle registration phase, the TA saves the PW of the vehicle to the registration list. However, the owner of the vehicle can not change the password anywhere, whenever, and anytime. One security tip is to modify passwords constantly, so this is a big priority for keeping work data secure. Modifying passwords removes a variety of threats.

VI. THE PROPOSED SCHEME

We propose an improved efficient and secure security scheme with conditional privacy-preservation in VANETs to overcome the shortcomings of Alazzawi *et al.*'s scheme [16]. In our proposal, we extend the framework of their scheme. As shown in Fig. 4, the proposed scheme' sequence diagram, and the description of the phases are in the next subsections. Our proposed scheme also has six phases: initialization, vehicle registration, vehicle joining, broadcasting and verification, vehicle revocation, and a renewal phase. A description of our proposed scheme follows.

A. INITIALIZATION PHASE

The TA mainly uses this procedure to set up device parameters, and it is the same as in Alazzawi *et al.* In this phase, the difference between their scheme and ours is that the TA also chooses a symmetric encryption function E(.)/D(.).

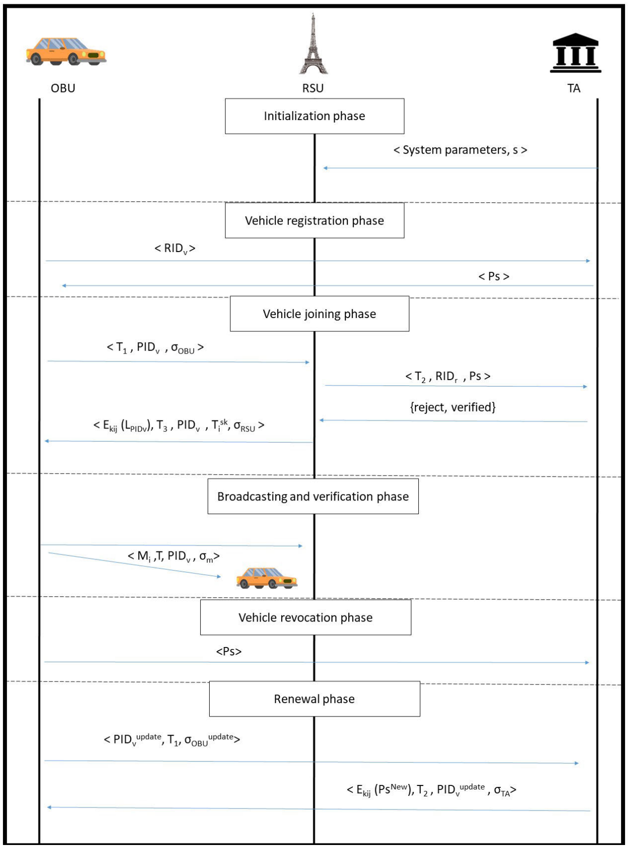

OBU
RSU
TA
Initialization phase
< System parameters, s >
Vehicle registration phase
$< RID_v >$
< Ps >
Vehicle joining phase
$< T_1 , PID_v , \sigma_{OBU} >$
$< T_2 , RID_r , Ps >$
{reject, verified}
$< E_{kij} (L_{PIDv}), T_3 , PID_v , T_i^{sk}, \sigma_{RSU} >$
Broadcasting and verification phase
$< M_i ,T, PID_v , \sigma_m>$
Vehicle revocation phase
<Ps>
Renewal phase
$< PID_v^{update}, T_1, \sigma_{OBU}^{update}>$
$< E_{kij} (Ps^{New}), T_2 , PID_v^{update} , \sigma_{TA}>$

FIGURE 4. The proposed scheme's sequence diagram.

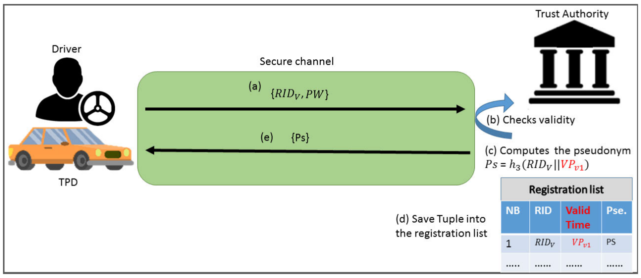


FIGURE 5. TA registers OBU by the proposed scheme.

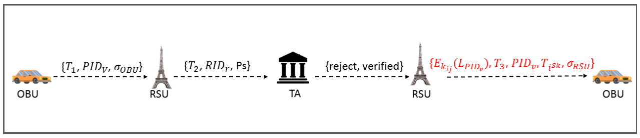
B. VEHICLE REGISTRATION PHASE

If a driver of new vehicle is ready for VANET membership, he/she has to execute the following steps, as shown in Fig. 5.

- (a) The driver first submits to the TA, via a secure channel, the original identity RID_v and password PW.
- (b) After the TA tests the validity of RID_v, (c) it calculates the pseudonym Ps=$h_3(RID_v||VP_{v1})$, where VP_{v1} is the period of validity, such as 01.07.2020–01.08.2020.
- Finally, (d) the TA saves the tuple $<RID_v, VP_{v1}$, Ps> to the registration list and (e) preloads Ps to the TPD of the vehicle.

C. VEHICLE JOINING PHASE

In order to begin the OBU, the vehicle driver should provide the TPD feedback with RID_v and PW to check the driver's validity. If valid, the OBU begins the process of joining and creates a mutual authentication as shown in Fig. 6. The following steps constitute the OBU joining phase:



OBU
$\{T_1, PID_V, \sigma_{OBU}\}$
RSU
$\{T_2, RID_r, \text{Ps}\}$
TA
{reject, verified}
RSU
$\{E_{k_{ij}}(L_{PID_v}), T_3, PID_v, T_{i^{Sk}}, \sigma_{RSU}\}$
OBU

FIGURE 6. OBU joining to RSU phase by the proposed scheme.

- $OBU_i \longrightarrow RSU_j$: The OBU generates r at random from Z_q^* and calculates
$$PID_{v1} = rP$$
$$PID_{v2} = Ps \oplus h_1(rPub)$$
Then, the OBU transmits the message $\{T_1, PID_v, \sigma_{OBU}\}$ to the RSU, where $PID_v = \{PID_{v1}, PID_{v2}\}$ and $\sigma_{OBU} = h_3(T_1 || \text{Ps})$.
- $RSU_j \longrightarrow TA$: The RSU firstly checks the timestamp validity T_1 after it receives the message $\{T_1, PID_v, \sigma_{OBU}\}$ from the OBU. If the T_1 is not valid, the RSU rejects this message. Otherwise, RSU calculates Ps $= PID_{v2} \oplus h_1(s.PID_{v1})$ and tests whether $\sigma_{OBU} \overset{?}{=} h_3(T_1 || \text{Ps})$. If not, the message is rejected by the RSU; otherwise, it transmits $\{T_2, RID_r, \text{Ps}\}$ to the TA.
- $TA \longrightarrow RSU_j$: The TA firstly checks the timestamp validity T_2 after it receives the message $\{T_2, RID_r, \text{Ps}\}$ from the RSU. If T_2 is not valid, the TA does not accept the message. Otherwise, the TA tests whether the values stored for *RIDr* and ps match. Finally, the TA transmits the message {reject, verified} to the RSU.
- $RSU_j \longrightarrow OBU_i$: Once the message {reject|| verified} is received by the RSU, it verifies if the message content is {*accepted*}. If not, the message is dropped by RSU_j and the vehicle is illegal. Otherwise, it prepares the pseudo-ID sets with its expiration time T_i^{Sk}. The RSU chooses n random draws $z_l \in Z_q^*$, where l=1:n and n is an anonymous level of security that is the pseudo-ID sets in an area covered by an RSU, a vehicle may not be used repeatably [41]. Then the RSU calculates L_{PID_v}=$\{PID_{vl}, \ldots.., PID_{vn}\}$ as follows:
$$PID_{vn} = \{PID_{v1}^l, PID_{v2}^l\}$$
$$PID_{v1}^l = z_l P$$
$$PID_{v2}^l = Ps \oplus h_1(z_l Pub)$$
Then, the RSU_j encrypts $E_{k_{ij}}(L_{PID_v})$ and sends the message $\{E_{k_{ij}}(L_{PID_v}), T_3, PID_v, T_i^{Sk}, \sigma_{RSU}\}$ to the OBU_i, where $k_{ij} = h_3(\text{Ps}||sPID_{v1})$ as the key of the symmetric function and $\sigma_{RSU} = h_2(L_{PID_v}||T_3||T_i^{Sk}||PID_v)$.
- OBU_i: The OBU firstly checks the timestamp validity T_3 after it receives the message $\{E_{k_{ij}}(L_{PID_v}), T_3, PID_v, T_i^{Sk}, \sigma_{RSU}\}$ from the RSU. Then the OBU calculates $k_{ij} = h_3(\text{Ps}|| \, rPub)$. Then the OBU decryptes $D_{k_{ij}}(E_{k_{ij}}(L_{PID_v}))$ and checks $\sigma_{RSU} \overset{?}{=} h_2(L_{PID_v}||T_3||T_i^{Sk}||PID_v)$. If so, it starts using L_{PID_v} to sign messages anonymously in the RSU coverage area.

D. BROADCASTING AND VERIFICATION PHASE

1) BROADCASTING

If the OBU wishes to sign a message M_i, the following steps must be executed:

- The OBU randomly chooses a pseudo-ID PID_v from the list L_{PID_v}.
- The OBU calculates the signature of the message as follows: $\sigma_m = h_3(M_i|| \text{ T}|| \, PID_v)$.
- Finally, the message $\{M_i$, T, PID_v, $\sigma_m\}$ is sent to the recipient.

2) VERIFICATION

When any message is finally received from each receipt, such as $\{M_i$, T, PID_v, $\sigma_m\}$, it will be checked for T. If (T_r - T $< T_\nabla$), the check process continues with receipt, otherwise, the final message is rejected. Here, T_r denotes the time of receipt of the message and T_∇ denotes the predefined endurable transmission delay. There are two versions of our message verification process: single message verification and batch message verification. These are describe in detail in the following:

a: SINGLE MESSAGE VERIFICATION

The recipient checks when the message is received and accepts the message if

$$\sigma_m^* = \sigma_m$$
$$\sigma_m^* = h_3(M_i||T||PID_v)$$

b: BATCH MESSAGE VERIFICATION

If a recipient receives a number of large message, denoted by $\{{M_i}^1$, T, ${PID_v}^1$, ${\sigma_m}^1\}$, $\{{M_i}^2$, T, ${PID_v}^2$, ${\sigma_m}^2\}$, $\ldots.\{{M_i}^n$, T, ${PID_v}^n$, ${\sigma_m}^n\}$, the signatures can be simultaneously verified as follows:

$$\Big(\sum_{i=1}^{n}(\sigma_m^*)\Big) = \Big(\sum_{i=1}^{n}(\sigma_m)\Big)$$

When there is a suspect vehicle in VANET, the registered vehicle verifies the message signature before accepting the message as follows,

- For single message verification: $\sigma_m.Pub = h_3(M_i|| \text{ T}|| \, PID_v).Pub$
- For batch message verification: $\Big(\sum_{i=1}^{n}(\sigma_m^*).Pub\Big) = \Big(\sum_{i=1}^{n}(\sigma_m).Pub\Big)$

E. VEHICLE REVOCATION PHASE

This phase is primarily used to trace and revoke a malicious vehicle by the TA and RSU and is the same as that used by Alazzawi *et al.*

F. RENEWAL PHASE

To withstand a side channel attack, we should update the Ps saved within the TPD periodically through offline and online mode. Nevertheless, pending the next annual inspection, the attacker could have enough time to obtain sensitive information that would collapse the VANET system. The first mode could be to perform an official inspection such as an annual inspection to update the Ps. We therefore update sensitive information saved within the TPD by using the online mode. The following are the specific steps in the update process:

- The OBU generates a random integer $r_{update} \in Z_q^*$ and computes $PID_i^1 = r_{update}P$ and $PID_i^2 = PS \oplus h_1(r_{update}Pub)$. Then the OBU transmits $\{PID_v^{update}$, T_1, $\sigma_{OBU_i^{update}}\}$ the TA with the aid of the RSU, where $PID_v^{update} = \{PID_i^1, PID_i^2\}$ and $\sigma_{OBU_i^{update}} = h_3(Ps \| PID_i^1 \| PID_i^2 \| T_1)$.
- The validity of the timestamp T_1 is checked after the TA receives the message $\{PID_v^{update}, T_1, \sigma_{OBU^{update}}\}$. If T_1 valid, the TA computes $Ps = PID_i^2 \oplus h_1(s.PID_i^1)$. The TA checks whether $\sigma_{OBU^{update}} \overset{?}{=} h_3(Ps \| PID_i^1 \| PID_i^2 \| T_1)$. The TA searches for whether the registration list includes the tuple <RID_v, VP_{v1}, Ps>; else the TA tests the VP_{v1} validity.
- In case the VP_{v1} is invalid, a new period of validity VP_{v1}^{New} is chosen by the TA. Then the TA computes $Ps^{New} = h_3(RID_v \| VP_{v1}^{new})$. It will abort if VP_{v1} is valid.
- The TA encrypts the message using a symmetric encryption key as $E_{kij}(Ps^{New})$ to the OBU and puts the new tuple <RID_v, VP_{v1}^{new}, Ps^{new} > into the registration list. Then, the TA sends the message $(E_{kij}(Ps^{New}))||T_2||PID_v^{update}||\sigma_{TA})$ to the OBU, where $\sigma_{TA} = h_2(Ps^{New}||PID_v^{update}||T_2)$.
- Finally, the OBU decrypts to get Ps^{New} as the new pseudonym.

VII. SECURITY ANALYSIS

The model of security in a conditional privacy-preserving authentication scheme is a game between the attacker and the challenger, which is based on the adversary's ability and a network model. The following can be described as the security model of the existential unforgeability against chosen-message attacks:

Theorem 1: The proposed scheme is existentially unforgeable against an adaptive chosen message attack under the random oracle model.

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

Setup: A generates the system private key and sets the system parameters parameters = {q, Pub, P, h_1, h_2, h_3} and then builds and holds three lists, namely, $LIST_{h1}$ with $(\alpha, \tau h_1)$form, $LIST_{h2}$ with $(PID_{v1}, PID_{v2}, T_i^{Sk}, \tau h_2)$form and $LIST_{h3}$ with (M_i, T, τh_3)form. A is empty initially. Then, A transmits the parameters to B.

$LIST_{h1}$-Oracle: After A receives a message request from B with α, it initially verifies if the tuple $(\alpha, \tau h_1)$ is in $LIST_{h1}$ or not. If so, then, A transmits $\tau h_1 = h(\alpha)$ to B. Otherwise, A randomly chooses $\tau h_1 \in Z_q^*$ and appends $((\alpha, \tau h_1)$ into $LIST_{h1}$. Then, A transmits $\tau h_1 = h(\alpha)$ to B.

$LIST_{h2}$-Oracle: After A receives a B message request with $(PID_{v1}, PID_{v2}, T_i^{Sk}$, it initially verifies if $(PID_{v1}, PID_{v2}, T_i^{Sk}, \tau h_2))$ is in $LIST_{h2}$. If so, then, A transmits $\tau h_2 = h(PID_{v1}, PID_{v2}, T_i^{Sk})$ to B. Otherwise, A randomly chooses $\tau h_2 \in Z_q^*$ and appends $(pID_i^1, pID_i^2, T_s^{sub_j}, \tau h_2)$ into $LIST_{h2}$. Then, A transmits $\tau h_2 = h(PID_{v1}, PID_{v2}, T_i^{Sk})$ to B.

$LIST_{h3}$-Oracle: After A receives a B message request with (M_i, T), it initially verifies if $(M_i, T, \tau h_2)$ is in $LIST_{h3}$. If so, then, A transmits $\tau h_3 = h(M_i \| T)$ to B. Otherwise, A randomly chooses $\tau h_3 \in Z_q^*$ and appends $(M_i, T, \tau h_2)$ into $LIST_{h3}$. Then, A transmits $\tau h_3 = h(M_i \| T)$ to B.

Finally, attacker A outputs the messages {M_i, T, PID_v, σ_m} and checks whether s PID_{v1} and $\sigma_m = h_3(M_i \|$ T$\|$ $PID_v)$. Otherwise, challenger C will abort this game. According to the Cross-Lemma, another valid message $\{M_i^-, T^-, PID_v^-, \sigma_m^-\}$ will be generated by attacker A, satisfying $sPID_{v1^-}$, $\sigma_m^- = h_3(M_i^- \|$ T$\|$ PID_v^- this process once again, Due to the fact that s PID_{v1}^- - s PID_{v2}^-

Because of the difficulty of dealing with the ECDL and its irreversibility, under a random oracle model in the adaptively chosen message attack our scheme satisfies non-forgery. This fulfills the security requirement of Section III-D.

1) MESSAGE CONFIDENTIALITY

During the TA registration process, the vehicle gets the pseudonym Ps, which is the only element which knows the vehicle's original identity RID_v, where Ps=$h_3(RID_v \| VP_{v1})$. The vehicle uses Ps to create PID_v which is included by traffic-related messages, where $PID_{v1} = rP$, $PID_{v2} = Ps \oplus h_1(rPID_{v1})$, and $r \in Z_q^*$ is a random integer. It is very difficult for an adversary to create a link between the rapidly changing pseudonyms for the vehicle, and it is not possible for the adversary to obtain the vehicle's location. Therefore, the proposed scheme meets the identity privacy requirement. In other words, the proposed scheme satisfies the requirement for message confidentiality.

2) SECURITY OF MESSAGE CONFIDENTIALITY

After RSU generates sets of pseudo-ID for each vehicle, it encrypts sets by using the key of the symmetric function. Once specific vehicle is received, it decrypts sets after checking timestamp validly. Since sets are saved securely therefore, the adversary does not have the ability to retrieve sets for generating forge message. In addition, when there is a suspect vehicle in VANET, the registered vehicle verifies the message signature before accepting the message. Hence, the proposed scheme satisfies the security of Message confidentiality.

3) TRACTABILITY AND REVOCATION

As specified in Section VI-E, the TA must be able to trace and revoke a malicious vehicle. Although is no information about RID_i in the proposed scheme, the proposed scheme provides a traceability function.

4) NON-FORGERY

The complexity of the ECDL problem and the continual use of a one-way hash implies that the attacker can not produce the legal signature of one-half of the vehicles during a message attack adapted to a random oracle model. The non-forgery of signatures is therefore not falsified.

5) RESISTS SIDE CHANNEL ATTACK

Many schemes choose to put the pseudonym in a TPD, which no attacker has ever compromised. However, by performing a side channel attack, the sensitive information contained in the TPD could be accessed. In our proposal, we can update the (Ps) saved in the TPD regularly to withstand attacks by side channels. Several times in the present paper, the pseudonym Ps is used. If the Ps is not updated, the attacker can resume message identity information. The Ps has been modified in the proposed scheme before an assailant monitors it through the side channel.

6) UNLINKABILITY

During the message signing period, an anonymous description of the vehicle in the other message is rendered by the different random numerals z_l. The proposed scheme also uses a current timestamp and expiration time to calculate the signature. Any adversary who attempts to link two or more traffic-related messages can not succeed because of changes in their pseudo-ID sets, timestamp, and expiration times, given that the content of the message varies each time. Consequently, neither message can be linked to a specific vehicle under the proposed scheme; so, no linkability issue arises.

7) MODIFICATION OF PASSWORD

If a vehicle owner finds a password to be dangerous, it can be modified anywhere anytime. The following are the details for this. The owner inputs RID_v, PW old, and PW new, to start the OBU. the OBU will check whether RID_v and PW old are identical to the stored ones. If so, the password is modified. Therefore, the modifiability of the passwords of the proposed VANET scheme is provided.

A. SECURITY COMPARISON

We perform a comparative analysis in terms of security and privacy requirements between the scheme of Alazzawi *et al.* and our proposal. Table 2 lists the results of the comparison, where SPR-1, SPR-2, SPR-3, SPR-4, SPR-5, and SPR-6 denote message confidentiality, traceability, Non-forgery, resistance to side-channel attack, unlinkability, and modifiability of passwords, respectively.

We know that the scheme proposed by [16] for VANETs can not fulfill all the security and privacy requirements shown in Table 2. However, the proposed scheme fulfills all these security and privacy requirements.

TABLE 2. Comparison in Alazzawi *et al.* scheme for security and privacy requirements.

	Alazzawi et al. scheme [16]	Our scheme
SPR-1	✓	✓
SPR-2	✓	✓
SPR-3	✓	✓
SPR-4	✗	✓
SPR-5	✗	✓
SPR-6	✗	✓

✓: The requirement is satisfied

✗: The requirement is not satisfied

VIII. PERFORMANCE ANALYSIS

The main reason behind in the comparison of only one scheme since Alazzawi *et al.* scheme is more efficient compared to the existing schemes Jianhong *et al.* [20], He *et al.* [22], Wu *et al.* [42] and Cui *et al.* [43] in terms of computation cost and communication cost. Therefore, we will present a comparison of the scheme of Alazzawi *et al.* and our proposed scheme for proving the proposed scheme are more efficient compared to the existing schemes.

A. COMPUTATIONAL COST ANALYSIS

We describe the performance of our scheme in terms of the cost of the computations. This has been done using MIRACL's [44] cryptographic library to calculate the time required for various cryptographic operations. A 4 GB memory processor was running the operating system Windows 7. The hardware platform was an Intel(R) Core(TM)2 Quad 2.66 GHz. Table 3 shows the definition of and execution times for the associated cryptographic operations.

For simplicity, let GMS, VSM, and VMM denote the generation of a message and signature, the verification of the

TABLE 3. Definitions and time of cryptography operation.

Abbr.	Execution time(ms)	Definition
T_{ecc}^{sm}	0.6718	Scalar multiplication operation in a group based on ECC
T_{ecc}^{sm-s}	0.0665	Small scalar point multiplication operation in a group based on ECC
T_{ecc}^{pa}	0.0031	Point addition operation in a group based on ECC
T_h	0.0001	General hash function operation

TABLE 4. Cost of computation comparison.

Schemes	GMS(ms)	VSM(ms)	VMM(ms)
Alazzawi et al. [16]	$T^{sm}_{ecc} + 2T_h \approx 0.6738$	$(2)T^{sm}_{ecc} + T_h + T^{pa}_{ecc} \approx 1.3477$	$(2)T^{sm}_{ecc} + (2n)T^{sm-s}_{ecc} + (n+1)T^{pa}_{ecc} + (n)T_h \approx 0.1371\text{n} + 1.3467$
Our scheme	$T_h \approx 0.0001$	$T_h \approx 0.0001$	$nT_h \approx 0.0001\text{n}$

single message, and the verification of multiple messages, respectively.

In the scheme in [16], *GMS* comprises one scalar multiplication and two secure hash functions. Thus, the total computation time of *GMS* is $T^{sm}_{ecc} + 2\ T_h \approx 0.6720$ ms. This scheme has two scalar multiplications, one secure hash function and one point additions, which gives the *VSM* an overall computation time of $2\ T^{sm}_{ecc} + 1T_h + T^{pa}_{ecc} \approx 1.3468$ ms. *VMM* in this scheme requires two scalar multiplications, $2n$ small scalar multiplications, $n + 1$ point additions, and n secure hash functions. The overall computation time for *VMM* is $(2)T^{sm}_{ecc}+(2n)T^{sm-s}_{ecc}+(n+1)T^{pa}_{ecc}+(n)\ T_h \approx 0.1371\text{n}+1.3467$ ms. In our scheme, GMS consists of one secure hash function, so $1T_h = 0.0001$ ms is the total computation time for GMS. *VSM* consists of a secure hash function, so $1\ T_h \approx 0.0001$ ms is the total computation time for *VSM*. *VMM* uses n secure hash functions, so $(n)T_h = \text{n}\ 0.0001$ ms is the total computation time for *VMM*.

Table 4 compares the computational costs of the proposed scheme with those of Alazzawi *et al.*, for *GMS*, *VSM*, and *VMM*. Fig. 7 shows that our scheme has a significant advantage with *GMS* and *VSM*. Fig. 8 indicates the costs of *VMM* in measuring various traffic-related messages.

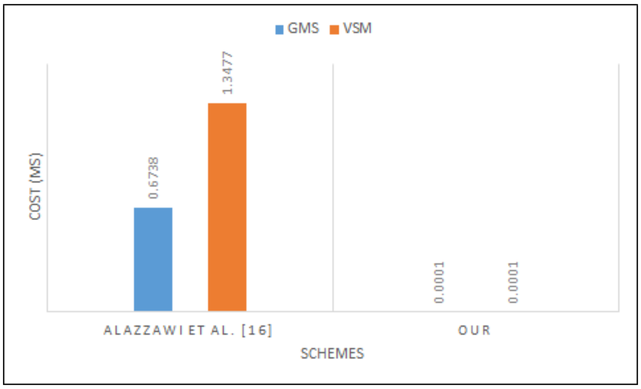


FIGURE 7. Computation costs of *GMS* and *VSM*.

As can be seen from the simulation results and Fig. 7, our proposed scheme has lower computational costs than those of the recently proposed scheme of Alazzawi *et al.*. Our proposed scheme only needs 0.0001 ms to generate a single message, compared with the 0.6720 s needed by the scheme proposed by Alazzawi *et al.* Our proposed scheme outperforms that of Alazzawi *et al.* by (0.6720 - 0.001)/0.6720 = 99.9%. Our proposed scheme highly outperforms that of Alazzawi *et al.*: by 99.5% in terms of single message verification. Additionally, our proposed scheme has better a computation cost performance in batch verification. Our computation cost is 99.2% less than that of Alazzawi *et al.* Consequently, the proposed scheme is more productive and efficient than the schemes in [16] in terms of the computational costs for *GMS*, *VSM*, and *VMM*.

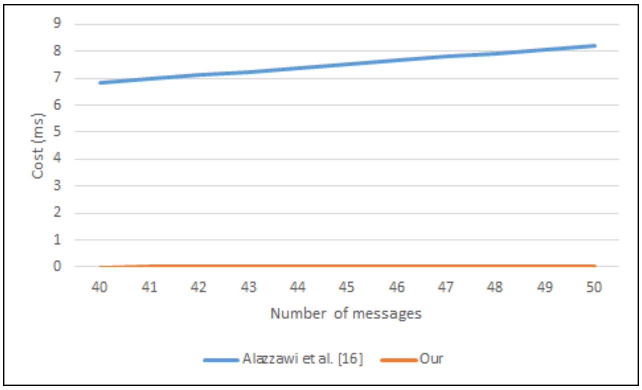


FIGURE 8. Computation costs of *VMM* for different traffic-related messages.

B. COMMUNICATION COST ANALYSIS

The size of p^{-} is 64 bytes, so $G1$ is 128 bytes in size of each item, and the p size is 20 bytes, meaning that in G, every single item size is 40 bytes. We also assume that timestamp output sizes, secure hash function, and integer item Z^{*}_{q} are respectively 4, 20, and 20 bytes, where the message content is excluded.

The traffic-related message size in the scheme of [16] is $(40+3*20+8) = 108$ bytes, and the content of traffic-related message is one element in G $\{PID_{v1}, \in\ G\}$, three elements $PID_{v2}, W, \sigma_m \in Z_q$, and two timestamps. In our proposed scheme, the vehicle sends a traffic-related message with size $(40 + 20 * 2 + 4) = 84$ bytes and the traffic-related message includes only one element in $\{PID_{v1} \in G\}$, two elements in $\{PID_{v2}, \sigma_m \in z_q\}$, and one timestamp. The overall communication overhead is shown in Table 5.

TABLE 5. Comparison of communication cost.

Schemes	One message	n messages
Alazzawi et al. [16]	108 bytes	108 n bytes
Our Scheme	84 bytes	84 n bytes

As can be seen from Table 5, a vehicle needs 84 bytes to submit a single status message, compared with 108 bytes in the proposal by Alazzawi *et al.* [16]. Our proposed scheme provides a 22% improvement in communication cost compared with that of Alazzawi *et al.* The number of bytes needed to submit n messages is linearly proportional to the number of messages. Our proposed scheme outperforms that of Alazzawi *et al.* by $(108 - 84)/108 = 22\%$ per single message. This improvement will greatly reduce the communication cost.

IX. CONCLUSION

We have reviewed the finding that the scheme of Alazzawi *et al.* cannot satisfy some vital requirements for security and privacy due to the fact that it is vulnerable to the side channel attack, it fails to provide unlinkability of the messages, and its also fails to allow modifications of the passwords. In addition, based on elliptic curve cryptography, a new security scheme based on conditional privacy-preservation has been proposed to overcome these shortcomings. A performance evaluation of the results of some measurements has shown that our proposed scheme is acceptable because it has lower overhead in term of computational and communication cost than the scheme of Alazzawi *et al.* That is why our improvements for VANETs make them stronger and more stable.

REFERENCES

[1] M. A. Al-Shareeda, M. Anbar, I. H. Hasbullah, and S. Manickam, "Survey of authentication and privacy schemes in vehicular ad hoc networks," *IEEE Sensors J.*, vol. 21, no. 2, pp. 2422–2433, Jan. 2020.

[2] F.-Y. Wang, D. Zeng, and L. Yang, "Smart cars on smart roads: An IEEE intelligent transportation systems society update," *IEEE Pervas. Comput.*, vol. 5, no. 4, pp. 68–69, Oct. 2006.

[3] M. A. Alazzawi, H. A. Al-behadili, M. N. S. Almalki, A. L. Challoob, and M. A. Al-shareeda, "ID-PPA: Robust identity-based privacy-preserving authentication scheme for a vehicular ad-hoc network," in *Proc. Int. Conf. Adv. Cyber Secur.* Singapore: Springer, 2020, pp. 80–94.

[4] K. Hwang and M. Chen, *Big-Data Analytics for Cloud, IoT and Cognitive Computing*. Hoboken, NJ, USA: Wiley, 2017.

[5] Y. Liu, Y. Wang, and G. Chang, "Efficient privacy-preserving dual authentication and key agreement scheme for secure V2V communications in an IoV paradigm," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 10, pp. 2740–2749, Oct. 2017.

[6] S. Kumari, M. Karuppiah, X. Li, F. Wu, A. K. Das, and V. Odelu, "An enhanced and secure trust-extended authentication mechanism for vehicular ad-hoc networks," *Secur. Commun. Netw.*, vol. 9, no. 17, pp. 4255–4271, 2016.

[7] M. Chen, Y. Hao, K. Lin, L. Hu, and Z. Yuan, "Label-less learning for traffic control in an edge network," *IEEE Netw.*, vol. 32, no. 6, pp. 8–14, Nov. 2018.

[8] M. A. Al-shareeda, M. Anbar, S. Manickam, I. H. Hasbullah, A. Khalil, M. A. Alazzawi, and A. S. Al-Hiti, "Proposed efficient conditional privacy-preserving authentication scheme for V2V and V2I communications based on elliptic curve cryptography in vehicular ad hoc networks," in *Proc. Int. Conf. Adv. Cyber Secur.* Singapore: Springer, 2020, pp. 588–603.

[9] B. Liu, D. Jia, J. Wang, K. Lu, and L. Wu, "Cloud-assisted safety message dissemination in VANET–cellular heterogeneous wireless network," *IEEE Syst. J.*, vol. 11, no. 1, pp. 128–139, Mar. 2015.

[10] B. Liu, D. Jia, K. Lu, H. Chen, R. Yang, J. Wang, Y. Barnard, and L. Wu, "Infrastructure-assisted message dissemination for supporting heterogeneous driving patterns," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 10, pp. 2865–2876, Oct. 2017.

[11] M. M. Hamdi, L. Audah, S. A. Rashid, and M. A. Al-shareeda, "Techniques of early incident detection and traffic monitoring centre in VANETs: A review," *J. Commun.*, vol. 15, no. 12, pp. 896–904, 2020.

[12] 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.

[13] L. Wu, Y. Xia, Z. Wang, and H. Wang, "Be stable and fair: Robust data scheduling for vehicular networks," *IEEE Access*, vol. 6, pp. 32839–32849, 2018.

[14] 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.

[15] Q. Jiang, J. Ma, G. Li, and X. Li, "Improvement of robust smart-card-based password authentication scheme," *Int. J. Commun. Syst.*, vol. 28, no. 2, pp. 383–393, 2015.

[16] 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.

[17] 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. 27th Conf. Comput. Commun. (IEEE INFOCOM)*, Apr. 2008, pp. 246–250.

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

[19] 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, 2013.

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

[21] M. Bayat, M. Barmshoory, M. Rahimi, and M. R. Aref, "A secure authentication scheme for VANETs with batch verification," *Wireless Netw.*, vol. 21, no. 5, pp. 1733–1743, 2015.

[22] D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 12, pp. 2681–2691, Dec. 2015.

[23] 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. 2016.

[24] 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.

[25] Q. A. Chen, Y. Yin, Y. Feng, Z. M. Mao, and H. X. Liu, "Exposing congestion attack on emerging connected vehicle based traffic signal control," in *Proc. Netw. Distrib. Syst. Secur. Symp. (NDSS)*, 2018, pp. 1–15.

[26] Y. Feng, S. Huang, Q. A. Chen, H. X. Liu, and Z. M. Mao, "Vulnerability of traffic control system under cyberattacks with falsified data," *Transp. Res. Rec., J. Transp. Res. Board*, vol. 2672, no. 1, pp. 1–11, Dec. 2018.

[27] 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.

[28] 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.*, vol. 18, no. 2, pp. 722–735, Mar. 2021.

[29] 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.

[30] C. Lai, R. Lu, D. Zheng, and X. Shen, "Security and privacy challenges in 5G-enabled vehicular networks," *IEEE Netw.*, vol. 34, no. 2, pp. 37–45, Mar. 2020.

[31] J. Cui, J. Chen, H. Zhong, J. Zhang, and L. Liu, "Reliable and efficient content sharing for 5G-enabled vehicular networks," *IEEE Trans. Intell. Transp. Syst.*, early access, Sep. 24, 2020, doi: 10.1109/TITS.2020.3023797.

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

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

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

[35] D. Jiang, V. Taliwal, A. Meier, W. Holfelder, and R. Herrtwich, "Design of 5.9 GHz DSRC-based vehicular safety communication," *IEEE Wireless Commun.*, vol. 13, no. 5, pp. 36–43, Oct. 2006.

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

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

[38] J.-J. Quisquater and D. Samyde, "Electromagnetic analysis (EMA): Measures and counter-measures for smart cards," in *Proc. Int. Conf. Res. Smart Cards*. Berlin, Germany: Springer, 2001, pp. 200–210.

[39] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proc. Annu. Int. Cryptol. Conf.* Berlin, Germany: Springer, 1999, pp. 388–397.

[40] D. B. Rawat, G. Yan, B. B. Bista, and M. C. Weigle, "Trust on the security of wireless vehicular ad-hoc networking," *Ad Hoc Sensor Wireless Netw.*, vol. 24, nos. 3–4, pp. 283–305, 2015.

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

[42] L. Wu, J. Fan, Y. Xie, J. Wang, and Q. Liu, "Efficient location-based conditional privacy-preserving authentication scheme for vehicle ad hoc networks," *Int. J. Distrib. Sensor Netw.*, vol. 13, no. 3, 2017, Art. no. 1550147717700899.

[43] 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.

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

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

MOHAMMED ANBAR received the Ph.D. degree in advanced computer network from University Sains Malaysia (USM). He is currently a Senior Lecturer with the National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia. His current research interests include malware detection, web security, intrusion detection systems (IDS), intrusion prevention systems (IPS), network monitoring, the Internet of Things (IoT), vehicular *ad hoc* network (VANET) security, and IPv6 security.

SELVAKUMAR MANICKAM is currently working as an Associate Professor with the National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia. He has authored and coauthored more than 160 articles in journals, conference proceedings, and book reviews, and graduated 13 Ph.D. students. He has ten years of industrial experience prior to joining academia. He also has experience building the IoT, embedded, server, mobile, and web-based applications. His research interests include cybersecurity, the Internet of Things, industry 4.0, and machine learning. He is a member of technical forums at national and international levels.

IZNAN HUSAINY HASBULLAH received the B.Sc. degree in electrical engineering from Rensselaer Polytechnic Institute, Troy, NY, USA. He is currently pursuing the M.Sc. degree in advanced network security. He has experience working as a software developer, a research and development consultant, and a network security auditor prior to joining the National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia, in 2010, as Research Officer. His research interests include unified communication, telematics, network security, network protocols, and next generation networks.