symmetry

MDPI

Article

An Efficient Identity-Based Conditional Privacy-Preserving Authentication Scheme for Secure Communication in a Vehicular Ad Hoc Network

Mahmood A. Al-shareeda *, Mohammed Anbar *, Selvakumar Manickam and Iznan H. Hasbullah

National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia, Penang 11800 USM, Malaysia; selva@usm.my (S.M.); iznan@nav6.usm.my (I.H.H.)

* Correspondence: m.alshareeda@nav6.usm.my (M.A.A.-s.); anbar@nav6.usm.my(M.A.)

Received: 21 August 2020; Accepted: 12 October 2020; Published: 14 October 2020

Abstract: The security and privacy issues in vehicular ad hoc networks (VANETs) are often addressed with schemes based on either public key infrastructure, group signature, or identity. However, none of these schemes appropriately address the efficient verification of multiple VANET messages in high-density traffic areas. Attackers could obtain sensitive information kept in a tamper-proof device (TPD) by using a side-channel attack. In this paper, we propose an identity-based conditional privacy-preserving authentication scheme that supports a batch verification process for the simultaneous verification of multiple messages by each node. Furthermore, to thwart side-channel attacks, vehicle information in the TPD is periodically and frequently updated. Finally, since the proposed scheme does not utilize the bilinear pairing operation or the Map-To-Point hash function, its performance outperforms other schemes, making it viable for large-scale VANETs deployment.

Keywords: vehicular ad-hoc network (VANET); privacy-preserving; side-channel attack; random oracle model; identity-based cryptography

1. Introduction

In recent years, wireless communication technology's rapid advancement has made vehicular ad hoc networks (VANETs) gain considerable attention from researchers in the public and private sectors, especially those involved in intelligent transportation systems [1–3]. Some of the VANET technology goals are to improve transportation safety to help reduce road accidents and improve road traffic management. A VANET architecture comprises three main entities: a trusted authority (TA), several fixed roadside units (RSUs), and many mobile onboard units (OBUs), which are equipped in every VANET-enabled vehicle. By using dedicated short-range communication (DSRC) technology, the vehicle communicates with other vehicles or nearby RSU within its communication range. VANETs are known for their special characteristics, such as having randomly mobile vehicles as nodes and rapid network topology changes [4].

VANETs can provide safety and comfort services such as weather information, road-condition, and emergency warnings, intersection coordination, lane changing assistance, and etc. for the drivers and passengers [5]. Attacks on these services can be easily carried out without difficulties. Since the vehicles and fixed RSU in the VANET network make decisions based on the information that they receive, wrong decisions due to fake information from illegal nodes can lead to serious consequences. For instance, an attacker could impersonate an ambulance and request that traffic control allows it to pass by turning traffic lights green [6]. As a shared open medium, the wireless communication channel used by VANET transmits information that the users want to keep private without any protection [7,8].

All messages must always be authenticated by the recipient before further action is taken to avoid similar attacks.

Since the driver is usually the vehicle's owner, the lack of security on the VANETs communication could expose the driver's identity. For instance, an eavesdropper can infer a driver's residence and identity by gathering safety-related messages in VANET networks. This information leak may violate the user's privacy and may also lead to criminal acts. Therefore, the entities in the VANET networks have to communicate anonymously to prevent disclosure of the user identity via the message exchanges. However, preserving privacy should not be absolute but conditional. If there are disputes, then the sender's identity should be revealed by the authorities [9].

The existing authentication schemes that are based on conditional privacy-preservation are generally categorized into three main classes: PKI-based, group signature-based, and identity-based schemes. Furthermore, none of the existing schemes fully meets the security and privacy requirements, and thus not entirely secure. The contributions of this work are as follows:

- First, an identity-based conditional privacy-preserving authentication scheme for VANETs that satisfies the design goal in terms of the security and privacy requirements.
- Second, a scheme that prevents side-channel attacks by continuously updating the vehicle information kept in the tamper-proof device (TPD).
- Third, a scheme that outperforms other schemes and suitable for large scale deployment by avoiding the use of the bilinear pairing operation or the Map-To-Point hash function.

The rest of this paper is structured as follows. Section 2 reviews the related work in recent years. Section 3 presents the preliminary information related to our proposed scheme, followed by Section 4, which presents our proposed scheme in detail, including the six phases of the scheme. Section 5 gives an illustrative example for the proposed scheme. Section 6 describes an in-depth security analysis. Section 7 discusses the performance evaluation to demonstrate that the overall outlook of our scheme is reasonable. Finally, the conclusion of the paper and suggested future work are in Section 8.

2. Related Work

There are many schemes that have been proposed over the past few years to address the issues associated with the security and privacy of VANETs system. These schemes are commonly classified into three categories: (i) PKI-based conditional privacy-preserving authentication schemes, (ii) Group signature-based conditional privacy-preserving authentication schemes, and (iii) Identity-based conditional privacy-preserving authentication schemes. The existing schemes are clustered into their respective category and reviewed in the following sub-sections.

2.1. Pki-Based Conditional Privacy-Preserving Authentication Schemes

In PKI-based schemes [10–14], the safety-related message is signed with a pseudonym ID by the vehicle to preserve privacy. In order to demonstrate its validity, each message contains the corresponding pseudonym certificate. When a report about a malicious node is received, all of its pseudonym certificates will be revoked by the trust authority (TA) and added to the certificate revocation list (CRL). In this approach, the vehicle must carry out a revoked certificate check, and then check for each received message to ensure that both the certificate and the signature are valid. A large pseudonym certificate is provided by each vehicle to sign the message to preserve privacy. The increase in the number of revoked vehicles would cause the size of the CRL to increase as well. Since it is very time-consuming to check the CRL, it will greatly reduce the authentication performance.

Gamage et al. [15] proposed a signature-based scheme that can be used to hide the identity of the signer. However, the non-repudiation requirement will not be met if the sender is able to deny authorship of safety-related messages that it signs since no node in the VANET network knows the sender's identity. Raya et al. proposed a PKI-based scheme in 2007 to satisfy the integrity and non-repudiation requirements for safety-related messages. However, a large number of anonymous

certificates and the corresponding key pairs are required to be fitted in the OBU, which adds a huge management burden for the TA certification process. Moreover, the receiver needs to verify the validity of each and every certificate, which incurs additional cost to the system.

2.2. Group Signature-Based Conditional Privacy-Preserving Authentication Schemes

In the group signature-based scheme [16], anonymous authentication may be achieved by fulfilling the security and privacy requirements. In a group signature, any member of the group can sign the message on their behalf. The recipient then checks the validity of the group's public key without disclosing the identity of the signer. Regrettably, the group signature also suffers from the issue associated with the group member's revocation. Furthermore, the computation overhead to verify the group signature for VANETs is too high. Under the IEEE 802.11p technology, a vehicle in the VANETs system is required to broadcast a message for every 100 to 300 ms v. Any delay in the group signature verification process is highly intolerable and unacceptable, particularly if the traffic density is high.

The group signature-based authentication scheme for VANETs was first proposed in 2006 by [17] and followed by several other researchers [18–20]. In the GSIS scheme [20], only the group manager has the secret key of the group, so, none of the group members could disclose the signer's identity. This approach completely eliminates the burden of certificate management. However, when multiple vehicles are revoked, the size of the CRL also increases since there are two pairings involved in each CRL operation, which resulted in the computation overhead to increase. In addition, the computational overhead is higher than schemes in other categories (PKI-based and identity-based).

2.3. Identity-Based Conditional Privacy-Preserving Authentication Schemes

To address the known issues of PKI-based and group signature-based schemes for VANETs, several researchers have proposed identity-based conditional privacy-preserving authentication schemes [21].

These schemes use the identity information (such as name, ID card, etc.) as the public keys, while the TA generates private keys with the same ID and then passes them on to nodes. A public key is used to replace the certificate of the identity of the node. CRL and certificate verifications are avoided compared to PKI-based scheme. The receivers check the safety-related message using the sender's public key and the receiver's private key that was used to sign the message. However, several schemes in this identity-based system have huge overheads in terms of computation and communication costs.

The identity-based conditional privacy-preserving authentication schemes could be further categorized into two groups based on the cryptography used, such as bilinear pair and Elliptic curve cryptography (ECC).

2.3.1. Bilinear Pair Based

Zhang et al. [22,23] utilized the identity of a vehicle in an authentication scheme in which a vehicle is not required to store a large number of anonymous certificates and the corresponding key pairs. Additionally, their scheme avoids the burden of managing the certificates and the CRL.

Furthermore, their scheme supports the batch verification process that allows multiple messages in high-density areas to be verified by each node simultaneously. However, the signature verification process comprises both bilinear pairing and Map-To-Point hash function operations, which increase the verifier's computation overhead.

Jiang et al. [24] proposed a binary authentication tree (BAT) using the bilinear pairing operation for the VANET's vehicle-to-infrastructure (V2I) communication mode that satisfies the security and privacy requirements. However, the use of the bilinear pairing and Map-To-Point hash function operations lead to a large overhead in terms of computation cost. Sun et al. [25] also proposed an identity-based authentication scheme using the bilinear pairing operation. However, it does not support batch verification process.

To provide batch verification, Chim et al. [26] designed an identity-based authentication scheme based on bilinear pairing that uses the Map-To-Point hash function for the pseudonym generation in the message signing process. Since the batch verification process includes both operations of bilinear pairing and Map-To-Point hash function, it introduced a large computation overhead on the verifier.

For vehicle-to-vehicle (V2V) communication mode, Shim [27] proposed another authentication scheme using the bilinear pairing operation in the signature verification process that supports batch signature verification. However, the batch verification process comprises three bilinear pairing operations, which leads to high computation overhead.

Chim et al. [28] pointed out that the scheme by Jiang et al. [24] is vulnerable to security attacks such as replay and forgery attacks. Chim et al. [26] and Lee and Lai [29] indicated that the scheme by Zhang et al. [23] is vulnerable to replay attack and does not satisfy the non-repudiation requirement. Lee and Lai [29] proposed an improved identity-based authentication scheme using bilinear pairing operation to support the batch signature verification process. However, the verifier suffered high computation overhead because of the reliance on bilinear pairing operation and Map-to-Point hash function in the verification process.

Horng et al. [30] highlighted that Chim et al.'s scheme [26] is vulnerable to impersonation attack that allows a malicious or illegal vehicle to forge the identity of a legitimate vehicle in the VANETs system to send false safety-related messages. To overcome the vulnerability, they proposed a batch verification for secure pseudonymous authentication in VANET (b-SPECS+) scheme based on bilinear pairing. However, the batch verification process contains two bilinear pairing operations and a Map-to-Point hash function, which resulted in high computation overhead.

Jianhong et al. [31] pointed out various security limitations in Lee and Lai's [29] scheme; for example, it fails to satisfy the non-repudiation and traceability requirements; and it is vulnerable against replay attacks. To overcome the limitations in Lee and Lai's [29] scheme, Jianhong et al. [31] proposed an improved identity-based authentication scheme using bilinear pairing in VANETs system. However, the batch verification process includes both bilinear pairing operation and Map-To-Point hash function, which leads to a large overhead in terms of computation cost on the verifier.

A new scheme to withstand the side-channel attacker was suggested by Lei Zhang et al. [32]. In their scheme, the information kept in the TPD was continuously updated. Even if the attacker was able to access the information via a side-channel attack, the information was already out-of-date and thus prevented the exploitation of sensitive information. Zhong et al. [33] examined the scheme by Lei Zhang et al. [32] and found out that it did not refer to who in the aggregation phase is the aggregator, and its verification process introduced a large overhead. Bayat et al. [34] proposed an authentication scheme based on privacy-preserving that stores the private key of the system on TPD of RSU. Therefore, they introduced a new identity-based authentication scheme to resolve the flaws. Unfortunately, their new scheme utilizes the bilinear pairing operation and the Map-To-Point hash function in the verification process, which introduced large overhead in terms of computation cost for the verifier.

2.3.2. Elliptic Curve Cryptography (Ecc)-Based

He et al. [35] proposed an identity-based authentication scheme using the elliptic-curve cryptography (ECC) for VANETs system. In their scheme, the batch verification process in areas with high-density traffic is effective. Although they managed to solve some security issues in VANETs system, it is still vulnerable to the side-channel attack since the TA 's private master key is kept in the TPD of vehicle, which was supposed to be secure from compromise. However, a side-channel attack could still obtain some sensitive information stored in the TPD. The security of a VANET system will collapse once the attacker has obtained the secret master key. In addition, the operations of three-points multiplication on ECC cause a delay in the verification process.

Alazzawi et al. [36] proposed a robust identity-based ECC using a pseudonym rather than a real identity in the VANETs system. The batch verification process is supported and is more

efficient. Nevertheless, Alazzawi et al.'s [36] scheme requires two-point multiplication operations in its verification process. Furthermore, this scheme does not satisfy all of the privacy requirements, such as unlinkability. During the registration phase, the TA has to store all the pseudonyms in the vehicle's TPD for annual inspection. However, a side-channel attack would have enough time to obtain sensitive information before the next annual inspection to bring harm to the VANETs system.

3. Preliminary Information

3.1. Mathematical Tools

This section describes the elliptic-curve cryptography (ECC) and its respective mathematical problems.

3.1.1. ECC

Miller [37] introduced ECC in 1985, which has since become commonly utilized in many security algorithms designs. We assume that F_p denotes a finite field with prime order p. The following equation elliptic curve E with the non-singular definition $y^2 = x^3 + ax + b \bmod p$, where $4a^3 + 27b^2 \neq 0$ and $a, b \in F_p$. We assume that O denotes the point at infinity. The points of ECC make an additive group G with order q and generator P. The important features of the group G in ECC, as follow:

- Point addition: let P and S be two random points on ECC such that $(P, S) \in G$, where the point P calculates the group G with large prime order q. When $P \neq S$ then $R = P + S$ can be computed, where R denotes to the intersection point on ECC and the line which joins P and S. When $P = S$ then $R = P + S$, and when $P = -S$ then $P + S = O$.
- Scalar multiplication: the ECC definition as n$P = P + P + P.... + P$ for n times, where n $\in Z_q^*$ and n > 0.

3.1.2. Mathematical Problems

The mathematical problems of ECC are listed in Table 1.

Table 1. Mathematical problems of Elliptic curve cryptography (ECC).

Problem	Definition
Elliptic Curve Discrete Logarithm (ECDL) Problem	Given two points P and $Q = a$P $\in Z_q^*$ on E randomly, the main task of ECDL is to computes the unknown number a. Based on the assumption, it is hard to compute the points $Q = a$P and the probability of solving this problem is negligible.
Elliptic Curve Computational Diffie–Hellman (ECCDH) Problem	Given two points $Q = a$P and $R = b$P $\in Z_q^*$ on E randomly, the objective of ECCDH is to computes the unknown number a and b. According to the assumption, it is hard to calculate the points $Q = a$P and $R = b$P and the probability of solving this problem is negligible.

3.2. Network Model

In general, the architecture of a VANET system comprises three entities: TA, RSU, and OBU, as illustrated in Figure 1. TA is a third-party entity that is responsible for managing and generating the public system parameters on behalf of the other two entities. RSU is a fixed infrastructure typically deployed along the roadside, which acts as a proxy for communication between the vehicles and the TA via a wireless channel and wired channel, respectively. The OBU is equipped on every VANET-enabled vehicle, which allows the vehicle to process, receive, and broadcast safety-related messages for road traffic management. Each OBU is equipped with a TPD to keep personal identifiable information safe and secure.

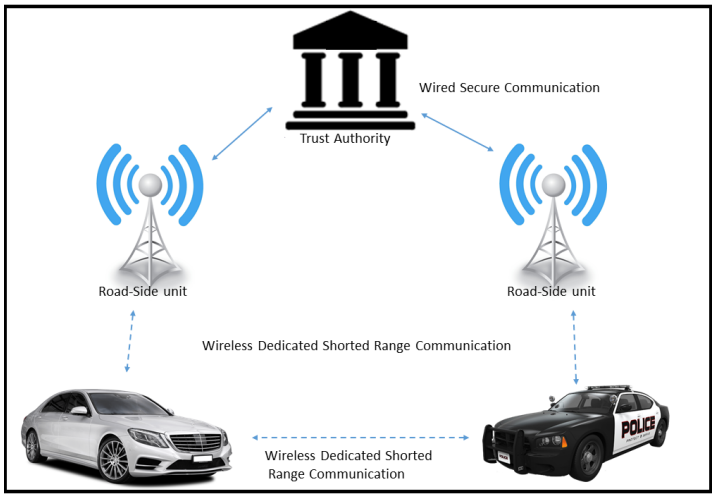

Figure 1. Typical structure of vehicular ad hoc network (VANET).

3.3. Thread Model

In VANETs, a good authentication scheme should be able to withstand common attacks, such as replay, impersonation, modification, and side-channel attacks. The description of the attacks are as follows:

- Replay attack: this is a type of attack where a malicious or illegal nodes replay the previously generated safety-related messages.
- Impersonation attack: impersonation attack happens when malicious user tries to assume the identity of a legitimate vehicle and poses as a legitimate node, either to cause disturbance or to obtain illegal access to network resources, which otherwise will not be accessible to the node under normal operation.
- Modification attack: this is a type of attack where malicious or illegal nodes try to modify or alter the content of safety-related messages between VANET participants.
- Side-channel attack: this is a type of attack that involves an attempt to gain sensitive information kept in the TPD using a side-channel attack. Once the malicious or illegal node obtains the master key of the system, the VANET structure will collapse.

3.4. Design Goals

The design goals of the proposed scheme are listed as below:

- Privacy preservation: the preservation of privacy in the VANETs system is an important objective for the vehicle's information and its owner. If the privacy is preserved, an attacker will not be able to disclose the vehicles' identity based on the published safety-related messages since only the TA knows the sender's identity.
- Message integrity and authentication: a verifier should be able to ensure that an attacker does not alter safety-related message (integrity) and a message was sent from an legitimate vehicle (authentication).
- Traceability and revocability: the TA is able to trace and revoke the identity of the attacker in the event there is a dispute or suspicion on the messages.
- Unlinkability: the malicious or illegal nodes should not be able to link two safety-related messages transmitted from the same source by inspecting the messages' content.
- Resistance against different types of attacks: identity-based conditional privacy-preserving authentication schemes should be able to resist different types of attacks, such as replay, impersonation, modification, and side-channel attacks.

4. The Proposed Scheme

In this paper, we propose an efficient identity-based conditional privacy-preserving authentication scheme to address some of the security issues of VANET, especially those related to the existing authentication schemes (refer to Section 2) to secure the V2V and V2I communications for managing all OBUs and RSUs in the VANETs system.

Our proposed scheme avoids the use of the bilinear pairing operation and Map-To-Point hash function that are well-known to be time-consuming. Instead, our scheme relies on ECC operation to resolve the issue of performance efficiency in terms of computation and communication cost prevalent in schemes such as [31,32,34]. Additionally, unlike scheme [35], the proposed scheme stores the system's master private key in the TPD of RSU during the registration process. The proposed scheme only keeps the vehicle's pseudonym in the TPD of OBU for a short time, unlike scheme [36] that stores the pseudonym indefinitely. Therefore, the proposed scheme introduces a TPD parameter renewing phase that continuously updates the sensitive information kept in the TPD to prevent malicious or illegal nodes from obtaining sensitive information via side-channel attacks. This preventive feature avoids the potential disruption of the whole VANETs system. The proposed scheme also supports the batch verification process that allows simultaneous verification of a large number of messages, especially in an area with high traffic density. The proposed scheme has six phases: initialization, registration, joining, broadcasting and verification, TPD parameters renewing, and vehicle revocation phases. Table 2 presents the notations used in the proposed scheme and their description. Figure 2 visualizes the phases of the proposed scheme, and the description of the phases are in the subsequent subsections.

Table 2. Notation and their description.

Notation	Descriptions
E	An elliptic curve
G	An additive group based on E
a, b	Two large prime number
p	large prime number
P	The base generator P$\in$ G
h_1, h_2, h_3	Three one-way hash function
$E_\pi(.)/D_\pi(.)$	Symmetric encryption and decryption function
λ_i	Symmetric key
s, P_{pub}	The private and public key of the system
OID_R, OID_v	Original identity RSU and OBU
PID_i, Ps	Pseudo-ID and pseudonym of vehicle
VP_{vi}	Valid period of Ps
PK_i	private key of vehicle
r, ζ_i, z_i	Random integer
σ_i	Signature on the safety-related message
δ_i	Sub-signature on the safety-related message
$\|\|$	Concatenation operation
$\oplus$	XOR operator

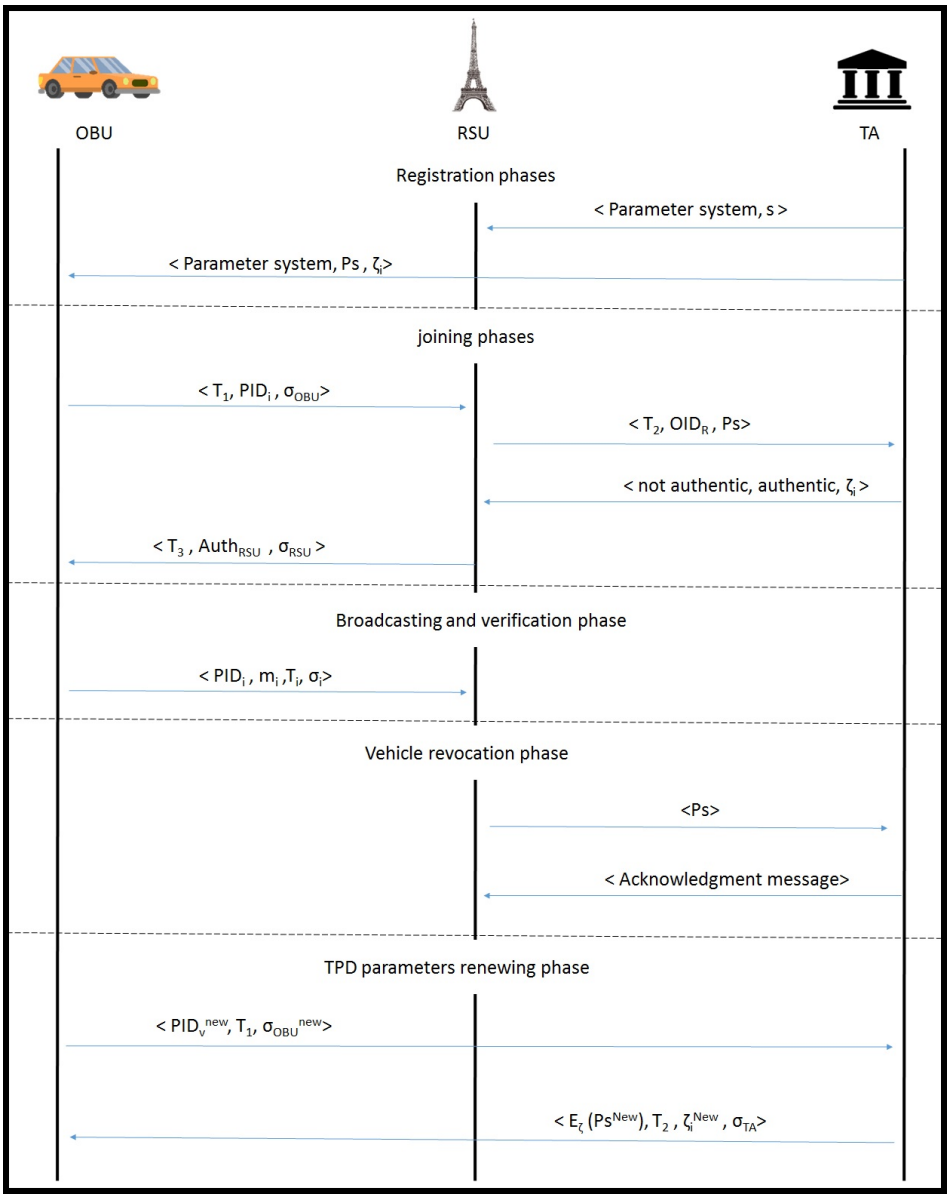

Figure 2. Sequence diagram of the proposed scheme.

4.1. Initialization Phase

In the proposed scheme, the TA generates the public parameters of the system. The VANET participants publish these parameters to facilitate the registration processes of other OBU and RSU. The details of the TA initialization phase are as follows:

- The TA selects two large prime p, q, the generator P of an additive group G with order q and non-singular elliptic curve E that are known by equation $y^2 = x^3 + ax + b \bmod p$, where $a, b \in F_p$.
- The TA selects a secret value $s \in Z_q^*$ randomly as the master private key of the TA, and it calculates $P_{pub} = s.P$ as its corresponding master public key.
- TA selects symmetric encryption function $E_\pi(.)/D_\pi(.)$ and three secure hash functions $h_1 : G \rightarrow Z_q^*$ $h_2 : \{0,1\}^* \times \{0,1\}^* \times G \rightarrow Z_q^*$ $h_3 : \{0,1\}^* \rightarrow Z_q^*$ as a cryptographic hash function.

4.2. Registration Phase

The new participant should be subjected to a registration process to authenticate its identity. There are two registration processes in this phase: registration of RSU and registration of OBU.

4.2.1. Registration of Rsu

The TA registers RSUs as follows:

- The TA selects the original identity of RSU OID_R according to its location.
- The TA preloads the public parameters $\Psi = \{p, q, a, b, P, P_{pub}, h_1, h_2, h_3\}$ in each RSU.
- The TA stores $<OID_R>$ in the registration list of RSUs and sends the master private key s to the RSUs.

4.2.2. Registration of Obu

The TA registers the OBUs following the steps below, as illustrated in Figure 3.

- The driver of the vehicle submits an original identity OID_v and password PW through a secure channel to the TA.
- The TA computes the pseudonym $Ps = h_3(OID_v || VP_{vi})$ after it checks the validity of the OID_v, where VP_{vi} is a valid period.
- The TA computes the encryption key of the vehicle by choosing a secret integer $\lambda_i \in Z_q^*$ and puts tuple $<\lambda_i$, Ps> into the TPD of vehicle.
- The TA preloads the public parameters $\Psi = \{p, q, a, b, P, P_{pub}, h_1, h_2, h_3\}$ in each OBU and stores tuple $<OID_v, Ps, VP_{vi}, \lambda_i>$ to the registration list of vehicles.

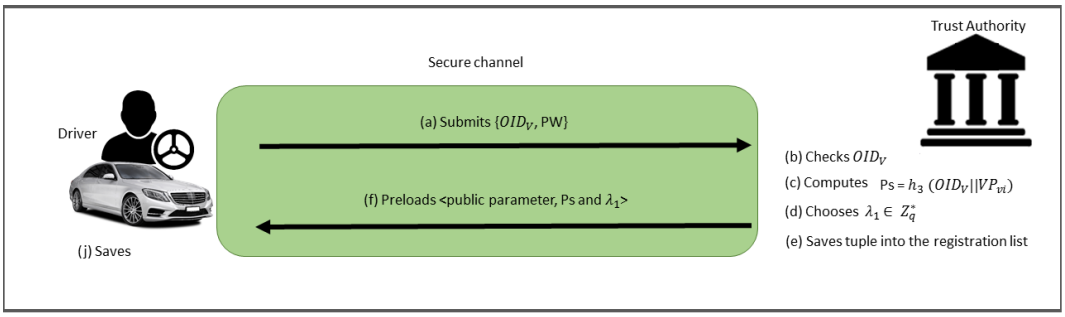

Figure 3. Onboard unit (OBU) registration process.

4.3. Joining Phase

The vehicle joins the RSU and should authenticate itself with the TA. Once the vehicle acquires private key PK from the RSU, the vehicle is regarded as an authentic vehicle and its messages can be broadcasted to nearby vehicles and RSUs, as shown in Figure 4. The joining phase is described as follows:

- $OBU_i \longrightarrow RSU_j$: the OBU randomly selects integer $r \in Z_q^*$ and computes its pseudo-ID $PID_i = <PID_i^1, PID_i^2>$, as follows:

$$\begin{aligned} PID_i^1 &= r.P \\ PID_i^2 &= Ps \oplus h_1(r.P_{pub}), \end{aligned} \tag{1}$$

where $r.P_{pub}$ displays the elliptic curve point's x-coordinate. Then, the OBU broadcasts to the RSU with message $<T_1, PID_i, \sigma_{OBU}>$, where $\sigma_{OBU} = h_3(T_1 || PID_i || Ps)$.

- $RSU_j \longrightarrow TA$: when the message <T_1, PID_i, σ_{OBU}> is received by RSU, the validity of the timestamp T_1 is checked first. If $T_r - T_1 < T_\triangle$. Then RSU continues the following process; otherwise, it dropped this message, where T_r depicts the message received-time and $T_\triangle$ is the predefined time delay. RSU calculates Ps, as follows:

$$Ps = PID_i^2 \oplus h_1(s.PID_i^1). \tag{2}$$

  Then, it is verified whether σ_{OBU} =? $h_3(T_1 || PID_i || Ps)$. If not, then the RSU drops the message; otherwise, it broadcasts to TA with message <T_2, OID_R, Ps>.
- $TA \longrightarrow RSU_j$: when the message <T_2, OID_R, Ps> is received by the TA, the validity of the timestamp T_2 is checked first. If fresh, then the TA verifies whether <OID_R, Ps> matches in the registration list. If not, then the TA drops the message and broadcasts to RSU with the message <not authentic>. Otherwise, it broadcasts message <authentic, λ_i>.
- $RSU_j \longrightarrow OBU_i$: when the message <not authentic/authentic, λ_i> is received by the RSU, it verifies whether the message content is <authentic, λ_i>. If not, then the RSU does not accept this message; otherwise, it selects a secret value $\zeta_i \in Z_q^*$ and calculates:

$$\mathrm{Y}_i = \zeta_i.P_{pub} \tag{3}$$

$$Sk_i = h_2(PID_i^1||PID_i^2||\mathrm{Y}_i||P_{pub}) \tag{4}$$

$$\omega_i = \mathrm{Y}_i + Sk_i.P \tag{5}$$

  The RSU Then computes

$$X_i = \left(\zeta_i + \frac{Sk_i}{s}\right) modq. \tag{6}$$

- $RSU_j \longrightarrow OBU_i$: when the RSU adjusts the private key as PK_i = <X_i, ω_i> for the OBU, it utilises the encryption key of vehicle to encrypt the private key to get $Auth_{RSU} = E_{\lambda_i}(PK_i)$ and broadcasts to OBU with message <T_3, $Auth_{RSU}$, σ_{RSU}>, where $\sigma_{RSU} = h_3(T_3 || PK_i || Ps)$.
- OBU_i: when the message <T_3, $Auth_{RSU}$, σ_{RSU}> is received by OBU, the validity of the timestamp T_3 is checked first. If it is fresh, then the OBU decrypts $PK_i = D_{\lambda_i}(Auth_{RSU})$ to get PK_i. It then verifies whether $\sigma_{RSU} = h_3(T_3 || PK_i || Ps)$. If it is okay, then it begins using PK_i to broadcast safety-related messages.

The RSU loads a pool of pseudo-IDs and private keys into each vehicle's OBU during its joining phase for a valid period. Whenever the available pseudo-IDs and private keys are close to expiry in the OBU traveling with VANETs, a new pool of pseudo-IDs and private keys are updated. Note that this is done between every vehicle and the TA when properly authenticated [38].

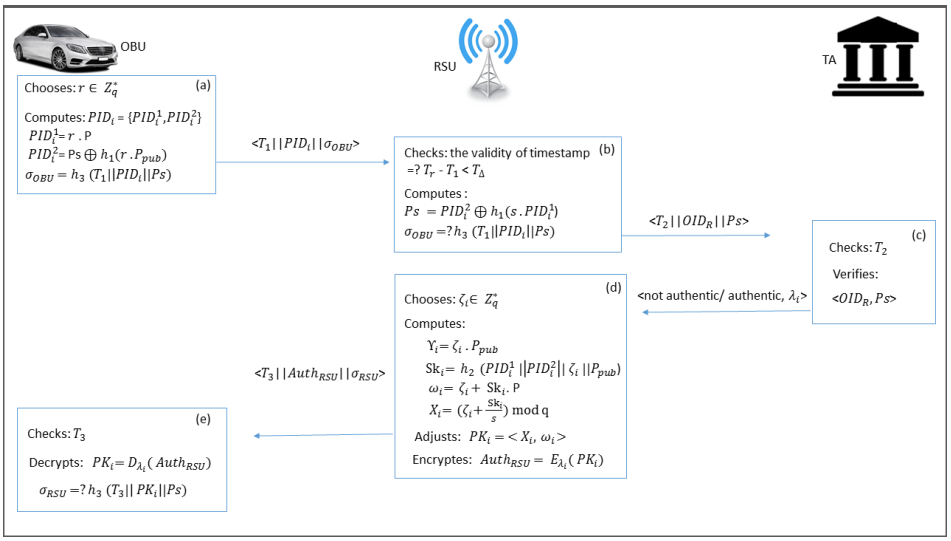

Figure 4. Joining phase.

4.4. Broadcasting and Verification Phase

In this phase, there are two processes, one for message signing and the other for verification; as shown in Figure 5.

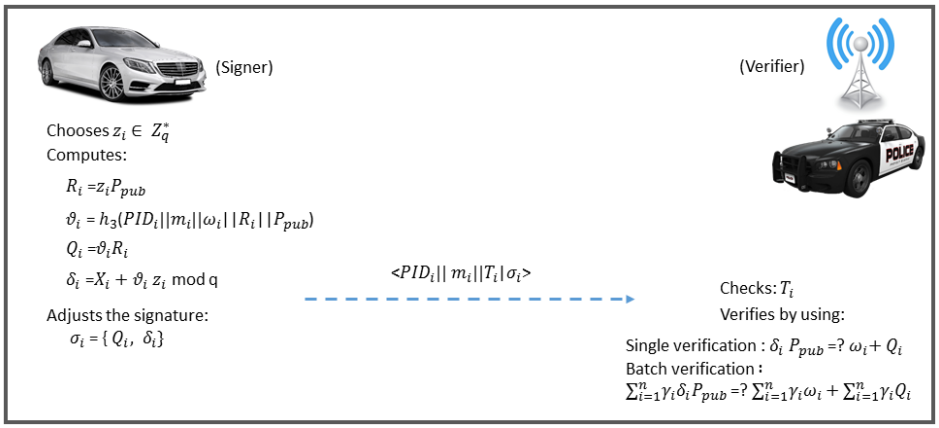

Figure 5. Broadcasting and verification phase.

4.4.1. Message Signing

In order to ensure security, all safety-related messages must be signed by the senders. This enables the recipients to check that the messages are not altered and verifies that the signature belongs to a valid vehicle. This process must be executed as follows:

- The OBU_i randomly chooses its pseudo-ID PID_i, and obtains the corresponding private key PK from the kept pseudo-IDs and the corresponding private keys.
- The OBU_i selects an integer value $z_i \in Z_q^*$ randomly and computes

$$R_i = z_i.P_{pub} \tag{7}$$

$$\vartheta_i = h_3(PID_i||m_i||T_i||\omega_i||R_i||P_{pub}) \tag{8}$$

$$Q_i = \vartheta_i.R_i. \tag{9}$$

- The OBU_i computes the sub-signature as follows

$$\delta_i = (X_i + \vartheta_i.z_i) mod q. \tag{10}$$

  Then, OBU_i adjusts the signature as σ_i = <Q_i, δ_i> on the safety-related message m_i.
- Finally, the message–signature $\{PID_i, m_i, T_i, \sigma_i\}$ is sent to the recipient.

4.4.2. Verification

Single Message Verification

Each vehicle only checks the signature of a safety-related message using this verification method. When the signed safety-related message arrives, the receiver must verify its authenticity and integrity before accepting it for further processing to ensure no malicious vehicles can pretend to be authentic vehicles, and prevent transmission of false safety-related messages. The details of the single message verification method are as follows:

- When the recipient (the RSU or OBU) received the message $\{PID_i, m_i, T_i, \sigma_i\}$, it first check the validity of the timestamp T_i first.
- Then, the verifying recipient uses σ_i of the message–signature tuple $\{PID_i, m_i, T_i, \sigma_i\}$ to verify safety-related message m_i, where σ_i = <Q_i, δ_i>. If Equation (11) holds, the message is accepted. Otherwise, the recipient will discard the message.

$$\delta_i.P_{pub} = \omega_i + Q_i \tag{11}$$

  The proof of Equation (11) is as follows:

$$\begin{aligned}
&L.H.S\\
&\delta_i.P_{pub}\\
&= (X_i + \vartheta_i.z_i).P_{pub}\\
&= \left(\left(\zeta_i + \frac{Sk_i}{s}\right) + \vartheta_i.z_i\right).P_{pub}\\
&= \left(\zeta_i + \frac{Sk_i}{s}\right).P_{pub} + \vartheta_i.z_i.P_{pub}\\
&= \zeta_i.P_{pub} + \left(\frac{Sk_i}{s}\right).s.P + \vartheta_i.\ R_i\\
&= \mathrm{Y}_i + (Sk_i).P + Q_i\\
&= \omega_i + Q_i\\
&= R.H.S
\end{aligned}$$

  Thus, Equation (11) is verified to be correct.

Batch Message Verification

Through this verification process, the verifier (the RSU or OBU) verifies multiple safety-related messages simultaneously. To minimize the time consumed, the proposed scheme utilities a batch verification method. To satisfy the requirement of non-repudiation in the proposed scheme, we utilize the small exponent test technique [31]. The verifier randomly generates an integer value γ = $\{\gamma_1, \gamma_2, ..., \gamma_n\}$, where $\gamma = \in [1, 2^t]$ and t is a small value, which does not increase the cost of the computation. In addition, consider that a recipient receives multiple safety-related messages $\{PID_i^1, m_i^1, T_i^1, \sigma_i^1\}$, $\{PID_i^2, m_i^2, T_i^2, \sigma_i^2\}$,...,$\{PID_i^n, m_i^n, T_i^n, \sigma_i^n\}$. Then, the verifying recipient uses σ_i^n of the

message–signature tuple $\{PID_i^n, m_i^n, T_i^n, \sigma_i^n\}$ to simultaneously verify safety-related messages min by using Equation (11), as follows:

$$\left(\sum_{i=1}^{n}(\gamma.\delta_i)\right).P_{pub} = \left(\sum_{i=1}^{n}(\gamma.\omega_i)\right) + \left(\sum_{i=1}^{n}(\gamma.Q_i)\right) \tag{12}$$

The proof of Equation (12) is as follows:

$$\begin{aligned}
&L.H.S\left(\sum_{i=1}^{n}\gamma_i.\delta_i\right).P_{pub}\\
&= \left(\sum_{i=1}^{n}\gamma_i.(X_i + \vartheta_i.z_i)\right).P_{pub}\\
&= \left(\sum_{i=1}^{n}(\gamma_i.\zeta_i) + \left(\sum_{i=1}^{n}(\gamma_i.Sk_i)\right).\frac{1}{s}\right).P_{pub} + \left(\sum_{i=1}^{n}(\gamma_i.\vartheta_i.z_i)\right).P_{pub}\\
&= \left(\sum_{i=1}^{n}.\gamma_i\zeta_i\right).P_{pub} + \left(\sum_{i=1}^{n}\gamma_i.Sk_i\right)\frac{1}{s}.s.P + \sum_{i=1}^{n}\gamma_i.(\vartheta_i.R_i)\\
&= \sum_{i=1}^{n}(\gamma_i.\mathrm{Y}_i) + \left(\sum_{i=1}^{n}(\gamma_i.Sk_i)\right).P + \sum_{i=1}^{n}(\gamma_i.Q_i)\\
&= \sum_{i=1}^{n}(\gamma_i.\omega_i) + \sum_{i=1}^{n}(\gamma_i.Q_i)\\
&= R.H.S
\end{aligned}$$

Thus, Equation (12) is verified to be correct. This process makes it easy for the receiver to verify multiple messages simultaneously.

4.4.3. Tpd Parameters Renewing Phase

In order to withstand the side-channel attack, the information kept (the pseudonym and encryption key) in the TPD should be continuously updated through an annual inspection and online mode. However, without updating the information kept for a short period of time or waiting for the next annul inspection mode, the attacker would have enough time to obtain information that can destroy the whole VANETs system. As shown in Figure 6, the specific steps to update the information kept in the TPD by using the online mode are as follows:

- The OBU_i chooses a random value $l \in Z_q^*$ and calculates $PID_i^1 = lP$ and $PID_i^2 = Ps \oplus h_1(l.P_{pub})$. Then, the OBU_i broadcasts message $\{PID_v^{new}, T_1, \sigma_{OBU_i^{new}}\}$ to the TA with the assistance of RSU, where $PID_v^{new} = \{PID_i^1 = lP, PID_i^2 = Ps \oplus h_1(l.P_{pub})\}$ and $\sigma_{OBU_i^{new}} = h_3(Ps\|PID_i^1\|PID_i^2\|T_1)$.
- The validity of timestamp T_1 is checked after the TA receives the message$\{PID_v^{new}, T_1, \sigma_{OBU_i^{new}}\}$. If T_1 is fresh, then TA computes old pseudonym of registered vehicle $Ps = PID_i^2 \oplus h_1(s.P_{pub})$. The TA verifies whether $\sigma_{OBU_i^{new}} =? h_3(Ps\|PID_i^1\|PID_i^2\|T_1)$ holds. TA checks whether the tuple $(OID_v, Ps, VP_{vi}, \lambda_i)$ exists in the registration list; else TA tests the VP_{vi} validity, where OID_v is original identity of vehicle and VP_{vi} is valid period.
- In case the VP_{vi} is expired, a new short period VP_{vi}^{New} is chosen by TA. Then, the TA computes a new pseudonym of registered vehicle $Ps^{New} = h_3(OID_i\|VP_{vi}^{New})$ and selects a new encryption key $\lambda_i^{New} \in Z_q^*$. It will abort if VP_{vi} is still valid.
- TA encrypts message $(Ps^{New}, \lambda_i^{New})$ by using the previous encryption key $E_{\lambda_i} \in Z_q^*$ to the vehicle and updates the new tuple $(OID_i, Ps^{New}, VP_{vi}^{New}, \lambda_i^{New})$ into the registration list of vehicles.

- TA sends a message to the vehicle with $(E_{\lambda_i}(Ps^{New}, \lambda_i^{New}) \| T_2 \| \sigma_{TA})$, where $\sigma_{TA} = h_2(Ps^{New} \| \lambda_i^{New} \| T_2)$.
- Finally, the vehicle decrypts $D_{\lambda_i}(Ps^{New}, \lambda_i^{New})$ to get the tuple $(Ps^{New}, \lambda_i^{New})$ as new pseudonym and encryption key.

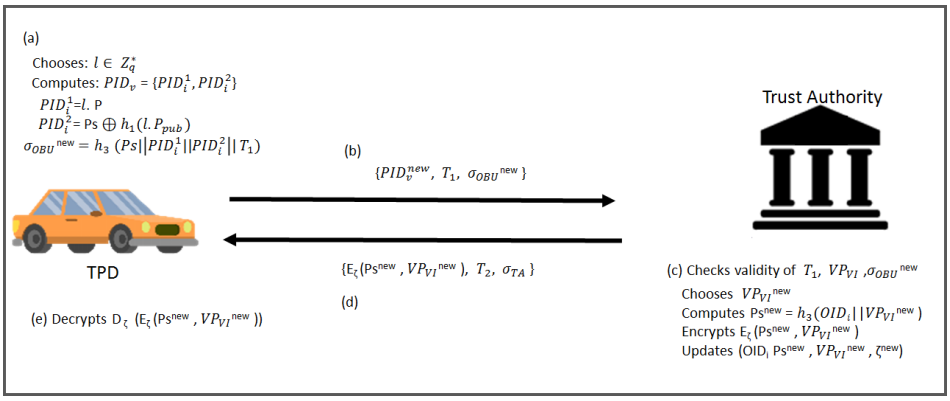

Figure 6. Update parameters process.

4.5. Vehicle Revocation Phase

As shown in Figure 7, when a report is received about a malicious or illegal vehicle, the TA traces this node and revokes it. The TA then discloses the vehicle's original identity from message–signature $\{PID_i, m_i, T_i, \sigma_i\}$, where $PID_i = <PID_i^1 = r.P, PID_i^2 = Ps \oplus h_1(r.P_{pub})>$, as follows:

$$Ps = PID_i^2 \oplus h_1(s.PID_i^1) \tag{13}$$

$$\begin{aligned} Ps &= PID_i^2 \oplus h_1(s.PID_i^1) \\ &= Ps \oplus h_1(r.P_{pub}) \oplus h_1(s.PID_i^1) \\ &= Ps. \end{aligned}$$

According to Ps, the original identity of the malicious or illegal vehicle is disclosed from the registration list. The TA adds the Ps to the CRL and broadcasts the last update to the RSUs. Therefore, the joining process fails whenever the pseudo-IDs and private keys on the OBU expire. Therefore, the malicious or illegal vehicle never authenticates itself with the RSU to get a new pool of pseudo-IDs and private keys. Therefore, no messages can be signed.

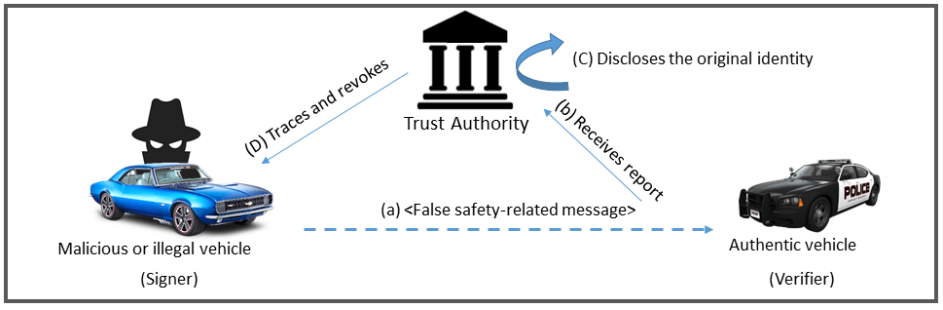

Figure 7. Vehicle revocation phase.

5. Illustrative Example

This section provides illustrative examples of the four phases of the proposed scheme: joining, signing, verifying, and revocation. Table 3 shows the parameters and their assigned values used in the illustrative examples.

Table 3. Input parameters and assigned values for illustrative examples.

Parameters	Assigned Value
a	-3
b	245515554600894381774029391519745178476910805816119123806 5
q	627710173538668076383578942320766641608390870039032496127 9
p	627710173538668076383578942320766641608390870039032496127 9
P	(606060575958698174522529830633150610660590643415807788118 0, 731059736642597018426628653347492645931119638401126465 27)
OID_v	Al-shareeda
VP_{vi}	1/10/2020-1/11/2020
Ps	575338844584270174718389643543398122480830084568
$T_\triangle$	0:00:59
OID_R	RSU-at-USM
m_i	Accident Zone

5.1. Joining Phase

Any vehicle that decides to join the VANET system first enters the joining phase by executing the following steps:

- $OBU_i \longrightarrow RSU_j$: After the OBU selects integer $r = 112$, it computes
  PID_i^1 = (537268550979458143092351915798392656784161062168980037634 6, 184358346550176987 847666348603008754532800063935891689112 3)

  PID_i^2 = 17252a1e7c5d2705773689bd03c4653bab4076c4c605e505a

  Then, the OBU broadcasts to the RSU with message <T_1, PID_i, σ_{OBU}>, where T_1 = 2020-1-10@3:50:00 pm and σ_{OBU} = 119626587889373751876040729907055448455231182888 7.
- $RSU_j \longrightarrow TA$: The validity of the timestamp T_1 is checked first. If $2020-1-10@3:50:08pm$ - $2020-1-10@3:50:00pm < T_\triangle$ where suppose $T_\triangle$ = 0:00:59. Then RSU calculates Ps, as follows:

  $Ps = 17252a1e7c5d2705773689bd03c4653bab4076c4c605e505a \oplus$
  $1250199638056575607191859587310833525244450561532$
  $= 575338844584270174718389643543398122480830084568$

  Then, the σ_{OBU} value is checked for whether it is equivalent to 119626587889373751876040729907055448455231182888 7. Then, the RSU broadcasts to the TA with the message <T_2, OID_R, Ps>, where T_2 = 2020-1-10@3:51:00 pm.
- $TA \longrightarrow RSU_j$: the validity of the timestamp T_2 is checked first. Then the TA verifies whether <RSU-at-USM, Al-shareeda> has a match in the registration list. Then the TA broadcasts to RSU with the message <not authentic>. Otherwise, it broadcasts message <authentic, λ_i>.
- $RSU_j \longrightarrow OBU_i$: The RSU selects a secret value $\zeta_i = 70$ and calculates:

  Y_i = (616896417072420023906096491673305396019724411656682534181 5, 5020579865249637335 390323875389858529392520706424450274958)

  Sk_i = 13447364013846897453172595856142478914538837771 11

  ω_i = (695964802647003559697395103815408855146214996023865488517, 3264385455095969240 554282193442456079956073210000018226187)

  Then, the RSU computes

  $X_i = (70 + \frac{1344736401384689745317259585614247891453883777111}{315}) mod q$

- $RSU_j \longrightarrow OBU_i$: after computing the X_i and ω_i, the RSU assigns the private key PK_i = <X_i, ω_i> for the OBU by utilising the vehicle's encryption key to encrypt the private key to get $Auth_{RSU} = E_{\lambda_i}(PK_i)$ and broadcasts to OBU with message <T_3, $Auth_{RSU}$, σ_{RSU}>, where $\sigma_{RSU} = h_3(T_3 \mid\mid PK_i \mid\mid Ps)$.
- OBU_i: the validity of the timestamp T_3 is checked first. Then, the OBU decrypts $D_{\lambda_i}(Auth_{RSU})$ to get PK_i. It then verifies whether $\sigma_{RSU} = h_3(T_3 \mid\mid PK_i \mid\mid Ps)$. If it is okay, then it begins using PK_i to broadcast safety-related messages.

5.2. Signing Messages

In signing phase, a vehicle signs the VANET messages by executing the following steps:

- The OBU_i selects an integer value $z_i = 222$ and computes

  R_i = (626151236438147419192537222499837442770391821811731825366 9, 495698213076377420701879862425132679568442421471184685719)

  ϑ_i = 307930924537994065473781821413919572502347505430

  Q_i = (247267479250158315543381241689317694302748111792610556834 8, 2066207338756896829801215631894887262859610071567012052768)
- The OBU_i computes the sub-signature as follows

  $\delta_i = (70 + \frac{1344736401384689745317259585614247891453883777111}{315})$
  + 307930924537994065473781821413919572502347505652) mod q

  Then, OBU_i assigns the signature as σ_i = <Q_i, δ_i> on the safety-related message m_i.
- Finally, the message–signature {PID_i, m_i, T_i, σ_i} is sent to the recipient, where suppose T_i is 2020-2-10@12:00:00 pm.

5.3. Verifying Messages

During the verifying messages process, vehicle executes the following steps;

- The validity of the timestamp T_i first.
- Then, the verifying recipient uses σ_i of the message–signature tuple {PID_i, m_i, T_i, σ_i} to verify safety-related message m_i, where σ_i = <Q_i, δ_i>. If the following holds, the message is accepted. Otherwise, the recipient will discard the message.

  $\delta_i.P_{pub}$ = (695964802647003559697395103815408855146214996023865488517, 3264385455095969240554282193442456079956073210000018226187) + (247267479250158315543381241689317694302748111792610556834 8, 2066207338756896829801215631894887262859610071567012052768)
- For batch message verification, the verifying recipient uses σ_i^n of the message–signature tuple {$PID_i{}^n$, $m_i{}^n$, $T_i{}^n$, $\sigma_i{}^n$} to simultaneously verify safety-related messages min by using the following:

  $(\sum_{i=1}^{n}(\gamma.\delta_i)).P_{pub} = (\sum_{i=1}^{n}(\gamma.(695964802647003559697395103815408855146214996023865488517, 3264385455095969240554282193442456079956073210000018226187))) + (\sum_{i=1}^{n}(\gamma.$ (247267479250158315543381241689317694302748111792610556834 8, 2066207338756896829801215631894887262859610071567012052768)))

$$\begin{aligned} Ps &= 17252a1e7c5d2705773689bd03c4653bab4076c4c605e505a \oplus \\ &\quad 125019963805657560719185958731083352524445056153 2 \\ &= 57533884458427017471838964354339812248083008456 8 \end{aligned}$$

According to Ps, the original identity of the malicious or illegal vehicle is removed from the registration list.

6. Analysis of the Proposed Scheme

In this section, we analyze the proposed scheme under the random oracle model to present the formal security proof and fulfill the stated design goals (Refer to Section 6.2) in terms of security and privacy requirements. We also analyze our scheme's resistance to some common attacks. Finally, a comparison between our proposed scheme and other existing schemes is presented.

6.1. Random Oracle Model Analysis

Theorem 1. *Our proposed scheme withstands an adaptively chosen message attack.*

Proof of Theorem 1. To analyze the authentication of the proposed scheme, we set up a game between a challenger Ch and an adversary Ad. Before the output is guessed in this game, the adversary Ad can make several queries.

- Proof: suppose an adversary Ad could forge a valid the message–signature $\{PID_i, m_i, T_i, \sigma_i\}$ for the safety-related message m_i. Then, the challenger Ch is able to solve the ECDLP with non-negligible probability by running Ad as a subroutine.
- Step-Oracle: the challenger Ch chooses a secret number $s \in Z_q^*$ randomly as the master private key, and calculates $P_{pub} = s.P$ as a master public key as $P_{pub} = s.P$ and generates the public parameters $\Psi = \{p, q, a, b, P, P_{pub}, h_1, h_2, h_3\}$. The challenger Ch sends the $\Psi = \{p, q, a, b, P, P_{pub}, h_1, h_2, h_3\}$ to Ad.
- h-$list_1$-Oracle: Ch keeps the list L_{h_1} as $(\xi, \tau h_1)$, where $\tau h_1 = h(\xi)$. Upon receiving Ad's query, Ch verifies whether the tuple $(\xi, \tau h_1)$ is in L_{h_1}. If it exists, then Ch sends τh_1 to Ad. Otherwise, Ch chooses random $\tau h_1 \in Z_q^*$, and puts $(\xi, \tau h_1)$ in L_{h_1}. Then, Ch sends $\tau h_1 = h(\xi)$ to Ad.
- h-$list_2$-Oracle: Ch keeps the list L_{h_2} as $(PID_i^1, PID_i^2, Y_i, P_{pub}, \tau h_2)$, where $\tau h_2 = h(PID_i^1, PID_i^2, Y_i, P_{pub})$. Upon receiving Ad's query, Ch checks whether the tuple $(PID_i^1, PID_i^2, Y_i, P_{pub}, \tau h_1)$ is in L_{h_2}. If it exists, then Ch sends τh_2 to Ad. Otherwise, Ch chooses random $\tau h_2 \in Z_q^*$, and puts $(PID_i^1, PID_i^2, Y_i, P_{pub}, \tau h_2)$ in L_{h_2}. Then, Ch sends $\tau h_2 = h(PID_i^1, PID_i^2, Y_i, P_{pub})$ to Ad.
- h-$list_3$-Oracle: Ch keeps the list L_{h_3} as $(PID_i, m_i, T_i, \omega_i, R_i, P_{pub}, \tau h_3)$, where $\tau h_3 = h(PID_i, m_i, T_i, \omega_i, R_i, P_{pub})$. Upon receiving Ad's query, Ch checks whether the tuple $(PID_i, m_i, T_i, \omega_i, R_i, P_{pub}, \tau h_3)$ is in L_{h_3}. If it exists, then Ch sends τh_3 to Ad. Otherwise, Ch chooses random $\tau h_3 \in Z_q^*$, and puts $(PID_i, m_i, T_i, \omega_i, R_i, P_{pub}, \tau h_3)$ in L_{h_3}. Then, Ch sends $\tau h_3 = h(PID_i, m_i, T_i, \omega_i, R_i, P_{pub})$ to Ad.
- Sign-Oracle: upon receiving Ad's query, Ch computes τh_1, τh_2, τh_3, δ_i and chooses a random PID_i, and Q_i. Then, Ch sends $\{PID_i, m_i, T_i, \sigma_i\}$ to Ad.

  Ad outputs $\{PID_i, m_i, T_i, \sigma_i\}$. Then, Ch checks Equation (14) as follows:

$$\delta_i^-.P_{pub} = ?\omega_i^- + Q_i, \tag{14}$$

  where, $\delta_i^- = (X_i^- + \vartheta_i^-.z_i) mod q$, $\delta_i = (X_i + \vartheta_i.z_i) mod q$, $\omega_i^- = Y_i^- + (Sk_i)^-.P$ and $Q_i = \vartheta_i.R_i$. This will lead us to:

$$\delta_i - \delta_i^-$$

$$(\omega_i + Q_i) - (\omega_i^- + Q_i),$$

where the modified *Ch*'s master public key $P_{pub} = s.P$, where $s \in Z_q^*$ is selected by A. Meanwhile, $\delta_i - \delta_i^-$ is an answer to the discrete logarithmic (DL) problem; that is, against the hardness of DL. Thus, the proposed scheme is resistant against forgery under an adaptively chosen message attack in a random oracle model.

□

6.2. Design Goal Analysis

In accordance with the design goals, as described in Section 3.4, we analyze the security and privacy requirements of the proposed scheme in the following sub-sections.

6.2.1. Message Integrity and Authentication

Consistent with Theorem 1, no ECDL problem can be solved and no signature can be forged by an attacker because of the complexity of ECDLP. In the proposed scheme, a verifying recipient can verify the message–signature tuple $\{PID_i, m_i, T_i, \sigma_i\}$ transmitted from a vehicle in terms of message integrity and node authenticity by checking whether equation $\delta_i.P_{pub} = \omega_i + Q_i$ holds. For example, after capturing the message–signature $\{PID_i, m_i, T_i, \sigma_i\}$ from registered vehicle V_j in the proposed scheme, a vehicle V_i alters the message m_i^A and broadcasts modified message–signature $\{PID_i, m_i^A, T_i, \sigma_i\}$ into the VANET system. The verifying vehicle V_v checks the validity of altered message–signature $\{PID_i, m_i^A, T_i, \sigma_i\}$ by checking whether Equations (11) or (12) hold. If true, then the proposed scheme satisfies the integrity and authenticity requirements.

6.2.2. Privacy Preservation

During the registration phase, the vehicle acquires the pseudonym Ps from TA, which is the only entity in VANETs that knows the vehicle's original identity OID_v, where $Ps = h_3(OID_v \| VP_{vi})$ and VP_{vi}. The vehicle utilities Ps to compute the PID_i that is contained within the message–signature $\{PID_i, m_i, T_i, \sigma_i\}$, where $PID_i^1 = r.P$, $PID_i^2 = Ps \oplus h_1(r.P_{pub})$ and $r \in Z_q^*$ is random value. Thus, the proposed scheme satisfies the identity privacy preservation requirement of the vehicle.

6.2.3. Traceability and Revocation

Although there is no information on OID_v in the message–signature tuple $\{PID_i, m_i, T_i, \sigma_i\}$ of the proposed scheme, as aforesaid in Section 4.5, a malicious or illegal vehicle can still be traced and revoked by the TA. For example, a vehicle V_i generates false message m_i^F and broadcasts it in the message–signature $\{PID_i, m_i^F, T_i, \sigma_i\}$ to a registered vehicle V_j in the proposed scheme. After V_j verifies and discovers false message m_i^F in the message–signature $\{PID_i, m_i^F, T_i, \sigma_i\}$ by using Equation (11) or (12), it sends a report to the TA by using Equation (13) for checking the pseudonym Ps of vehicle V_i. If the pseudonym Ps exists, then the TA traces and revokes the vehicle V_i in its registration list. Therefore, the proposed scheme satisfies the traceability and revocation requirements in VANETs.

6.2.4. Unlinkability

Malicious or illegal nodes are not able to successfully link two safety-related messages m_i and m_i^* originated from the same vehicle by inspecting the message content. This is because the vehicle signed these messages using different private keys $PK_i = <X_i, \omega_i>$ and pseudo-IDs PID_i for each vehicle, where $i = 1, 2, ..., n$, $X_i = (\zeta_i + \frac{Sk_i}{s}) mod q$, $\omega_i = Y_i + Sk_i.P$, $Y_i = \zeta_i.P_{pub}$ and $\zeta_i \in Z_q^*$ are random numbers. For example, after capturing a multiple message–signatures such as $\{PID_i^1, m_i^1, T_i^1, \sigma_i^1\}$, $\{PID_i^2, m_i^2, T_i^2, \sigma_i^2\}$, $\{PID_i^3, m_i^3, T_i^3, \sigma_i^3\}$,..., $\{PID_i^n, m_i^n, T_i^n, \sigma_i^n\}$ from the same sender vehicle. Due to the use of different parameters in every message–signature, malicious or illegal nodes cannot link between

them in the proposed scheme. Hence, the proposed scheme fulfills the unlinkability requirement among safety-related messages in VANETs.

6.3. Scheme Crypt-Analysis

Theorem 2. *Our Proposed scheme withstands the replay attack.*

Proof of Theorem 2. The message–signature tuple $\{PID_i, m_i, T_i, \sigma_i\}$ has the timestamps T_i. After the recipient receives the safety-related message *mi*, it first verifies whether the inequality $T_r - T_i < T_\triangle$ holds. If it is fresh, then the recipient accepts the safety-related message m_i for verification; otherwise, the message is rejected. In addition, according to message–signature tuple $\{PID_i, m_i, T_i, \sigma_i\}$, where $\sigma_i = <Q_i, \delta_i>$, $\delta_i = (X_i + \vartheta_i.z_i)$ mod q and $\vartheta_i = h_3(PID_i||m_i||T_i||\omega_i||R_i||P_{pub})$, another timestamp possibility cannot be used by an attacker because this attack results in different values of σ_i. In these procedures, replay of message m_i in VANETs system is detected. Without changing parameters, adversaries can intercept $\{PID_i, m_i, T_i, \sigma_i\}$, and replay the message to other vehicles. However, without fresh timestamp T, adversaries cannot perform a replay attack because the message will fail the verification process since a stale message will be dropped immediately by the receiver. For example, after capturing legitimate message–signature tuple $\{PID_i, m_i, T_i, \sigma_i\}$, the attacker rebroadcasts its at different time as as $\{PID_i{}^{old}, m_i^{old}, T_i^{old}, \sigma_i^{old}\}$ to other nodes in VANETs. A verifying vehicle checks the freshness of timestamp T_i included in the replayed message–signature tuple $\{PID_i{}^{old}, m_i^{old}, T_i^{old}, \sigma_i^{old}\}$ by checking whether the inequality $T_r - T_i^{old} < T_\triangle$ holds. If not, replay attack is detected and the message is rejected. Consequently, the proposed scheme successfully withstands the replay attack. □

Theorem 3. *Our proposed scheme withstands the modification attack.*

Proof of Theorem 3. According to the Theorem 1, the attacker cannot modify the message–signature tuple $\{PID_i, m_i, T_i, \sigma_i\}$ of the proposed scheme. This is because the verifying recipients can identify any modification in $\{PID_i, m_i, T_i, \sigma_i\}$ by checking whether equation $\delta_i.P_{pub} = \omega_i + Q_i$ holds. If true, then the recipients accept the message–signature; otherwise, it will be rejected. For example, after capturing the message–signature $\{PID_i, m_i, T_i, \sigma_i\}$ from an authentic vehicle, the attacker modifies the message m_i^M and rebroadcasts the modified message–signature $\{PID_i, m_i^M, T_i, \sigma_i\}$ into the VANET system. The verifying vehicle V_v checks the validity of modified message–signature $\{PID_i, m_i^M, T_i, \sigma_i\}$ by checking whether Equation (11) or (12) holds. If not, the modification attack is detected and the message is rejected. Therefore, the proposed scheme successfully withstands the modification attack. □

Theorem 4. *Our proposed scheme withstands the impersonation attack.*

Proof of Theorem 4. According to Theorem 1, no malicious or illegal node can impersonate a legitimate message–signature tuple $\{PID_i, m_i, T_i, \sigma_i\}$ in the proposed scheme. This is because the recipients can verify the authenticity of the tuple $\{PID_i, m_i, T_i, \sigma_i\}$ by checking whether equation $\delta_i.P_{pub} = \omega_i + Q_i$ holds. If true, then the recipients accept the message–signature; otherwise, it will be discarded. Thus, our scheme withstands the impersonation attack. To transmit a valid traffic-related message by impersonating a legitimate vehicle, the adversary must first acquire the identity of that vehicle's OID_i. For example, after capturing the legitimate message–signature $\{PID_i, m_i, T_i, \sigma_i\}$ from registered vehicle V_r, an attacker attempts to disclose the pseudonym Ps of V_r from PID_i by using Equation (13) to masquerade as a legitimate vehicle. According to Theorem 1, the adversary cannot obtain a real identity of a registered vehicle since the private key s of the system is not known to the adversary in the proposed scheme. □

Theorem 5. *Our proposed scheme withstands the side-channel attack.*

Proof of Theorem 5. Many schemes resort to storing the master secret key of the system in the vehicle's TPD since it almost never been compromised by any malicious or illegal node. However, an attacker could easily obtain sensitive information that is kept in the TPD through a side-channel attack. To address this issue, the proposed scheme continuously update the (Ps, λ_i) in the TPD, where $Ps = h_3(OID_v || VP_{vi})$ and $\lambda_i \in Z_q^*$. In the paper, it is stated that the vehicle's pseudonym Ps is utilizing repeatedly and frequently; so, if the Ps is not regularly updated, it will provide ample opportunity for the malicious or illegal node to disclose and exploit the pseudonyms associated with the messages. However, the Ps is already updated in the proposed scheme before it can be exploited by the attacker. The encryption key λ_i used in the authentication between the vehicle and other entities in the VANETs system is also updated concurrently. For example, after attacker accesses the TPD of OBU on vehicle directly, he/she discloses the authentic pseudonym Ps used for computing message–signature $\{PID_i, m_i, T_i, \sigma_i\}$. In the proposed scheme, the pseudonym is periodically and frequently updated (Refer to Section 4.4.3), thus making the attacker unable to exploit the disclosed old pseudonym. Therefore, the proposed scheme successfully withstands the side-channel attack. □

6.4. Security Comparison

Here, we compare the security and privacy requirement of the design goal of the proposed scheme with existing related schemes. The comparison of design goals is indicated in Table 4. Let DG-1, DG-2, DG-3, DG-4, DG-5, DG-6, DG-7, DG-8, denotes message integrity and authentication, identity privacy preservation, traceability and revocation, unlinkability, replay attack resistance, modification attack resistance, impersonation attack resistance and side-channel attack resistance, respectively.

According to Table 4, neither Jianhong et al.'s [31], Bayat et al.'s [34], He et al.'s [35] or Alazzawi et al.'s [36] schemes fulfill all of the design goals in VANETs. However, the design goals are fully achieved in the proposed scheme.

Table 4. Comparison of proposed scheme and the related schemes.

Scheme	DG-1	DG-2	DG-3	DG-4	DG-5	DG-6	DG-7	DG-8
Jianhong et al. [31]	✓	✓	✗	✓	✓	✓	✓	✗
Bayat et al. [34]	✓	✓	✗	✓	✓	✓	✓	✗
He et al. [35]	✓	✓	✗	✓	✓	✓	✓	✗
Alazzawi et al. [36]	✓	✓	✓	✗	✓	✓	✓	✗
Proposed	✓	✓	✓	✓	✓	✓	✓	✓

7. Performance Analysis

To address the issues related with the overhead of the system in terms of computation and communication costs, we analyze and compare the performance of the proposed scheme with the schemes proposed by Jianhong et al. [31], Lei Zhang et al. [32], Bayat et al. [34], He et al. [35] and Alazzawi et al. [36] for VANETs in this section. The computation cost is related to the number of cryptographic operations that have to be performed during the signing and verifying the message. While the communication cost is related to the size of a message–signature tuple, including the number of elements in the message–signature tuple. The details of the computation and communication costs are described in the following subsections.

7.1. Computation Cost Analysis

In a bilinear pairing, an additive group G_1 is generated with an 80-bit security level. Some of the parameters of the bilinear pair and ECC cryptography are presented in Table 5. MIRACL [39], a common and widely utilized cryptography library, is used in our experiment because it allows us to measure the computation cost in terms of running time of various cryptographic operations.

Table 5. Some parameters of bilinear pair and ECC cryptography.

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

The hardware platform used is powered by an Intel(R) Core™ 2 Quad 2.66 GHz processor with 4 GB memory running the Microsoft Windows™ 7 operating system. The running times for the cryptographic operations are listed in Table 6. In the analysis, the following cryptographic operations are taken into account.

- T_{bp}: the running time of the bilinear pair operation in G_1.
- T_{bp}^{pm}: the running time for the operation of a point multiplication in G_1.
- T_{mtp}: The running time for the operation of a Map-To-Point hash function in G_1.
- T_{ecc}^{pm}: the running time for the operation of a point multiplication in G.
- T_h: the running time for the operation of a general one-way hash function.

The cryptography operations in Jianhong et al. [31], Bayat et al. [34], Lei Zhang et al. scheme [32] are built on bilinear pairings, while those of He et al. [35] and Alazzawi et al. [36] and the proposed scheme utilize ECC. For simplicity, let GMS, VSM, and VMM denote generation of a message and a signature; verification of a single message; and verification of multiple messages, respectively.

Table 6. The running times for operation of cryptographic.

Cryptographic Operation:	T_{bp}	T_{bp}^{pm}	T_{mtp}	T_{ecc}^{pm}	T_h
Time (ms):	5.811	1.5654	4.1724	0.6718	0.001

In the Jianhong et al.'s [31] scheme, GMS consists of six multiplication operations, four general one-way hash functions and one Map-To-Point hash function. Thus, the overall computation cost of GMS is $6T_{bp} + 4T_h + T_{mtp}$. VSM in this scheme comprises three bilinear pairing operations, two multiplication operations and three general one-way hash functions. Hence, the overall computation cost of VSM is $3T_{bp} + 2T_{bp}^{pm} + 3T_h$. VMM in this scheme requires three bilinear pairing operations, (n +1) multiplication operations and 3n general one-way hash functions. In the proposed scheme, GMS includes two scalar multiplications and one general one-way hash function; so $2T_{ecc}^{pm} + 1T_h$ is the overall computation cost for GMS. VSM involves only one scalar multiplications; therefore, $1T_{ecc}^{pm}$ is the overall computation cost for VSM. VMM also requires only one scalar multiplication. Hence, T_{ecc}^{pm} is the overall computation cost for T_{ecc}^{pm}. The computation cost calculation is carried out in the same manner for other schemes.

Table 7 presents the comparison of the computation costs between the proposed scheme and five other identity-based schemes for GMS, VSM, and VMM. To analyze the batch verification of large number of messages, the computation costs of VMM for multiple messages in the proposed scheme are compared with five other identity-based schemes, as shown in Figure 8. Figure 9 shows the comparison between the proposed scheme and the Alazzawi et al. scheme [36].

Table 7. Comparison of computation cost.

Scheme	Generation of Message and Signature	Verification of the Single Message	Verification of Multiple Messages
Jianhong et al. [31]	$6T_{bp} + T_{mtp} + 4T_h$	$3T_{bp} + 2T_{bp}^{pm} + 3T_h$	$(n+1)T_{bp}^{pm} + 3T_{bp} + (3n)T_h$
Lei Zhang et al. [32]	$2T_{mtp} + 3T_h$	$2T_{mtp} + 3T_{bp} + 3T_h$	$(2n)T_{mtp} + 2T_{bp} + (3n)T_h$
Bayat et al. [34]	$5T_{bp} + T_{mtp} + 2T_h$	$3T_{bp} + T_{mtp} + T_{bp}^{pm} + T_h$	$3T_{bp} + (n)T_{mtp} + (n)T_{bp}^{pm} + (n)T_h$
He et al. [35]	$3T_{ecc}^{pm} + 3T_h$	$3T_{ecc}^{pm} + 2T_h$	$(n+2)T_{ecc}^{pm} + (2n)T_h$
Alazzawi et al. [36]	$T_{ecc}^{pm} + 2T_h$	$2T_{ecc}^{pm} + T_h$	$2T_{ecc}^{pm} + (n)T_h$
Proposed	$2T_{ecc}^{pm} + T_h$	T_{ecc}^{pm}	T_{ecc}^{pm}

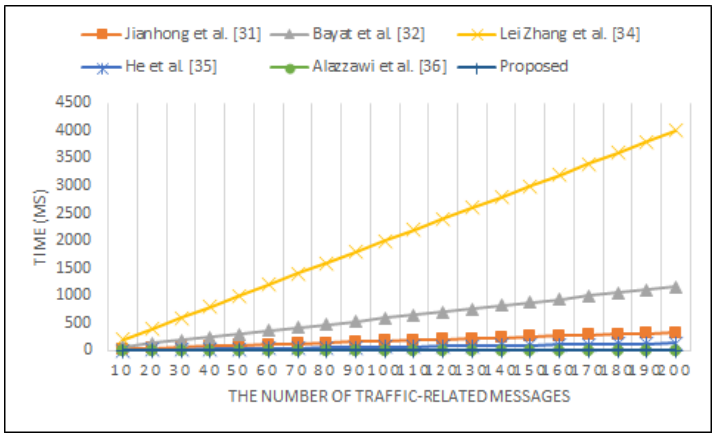

Figure 8. The computation costs of VMM for different numbers of messages.

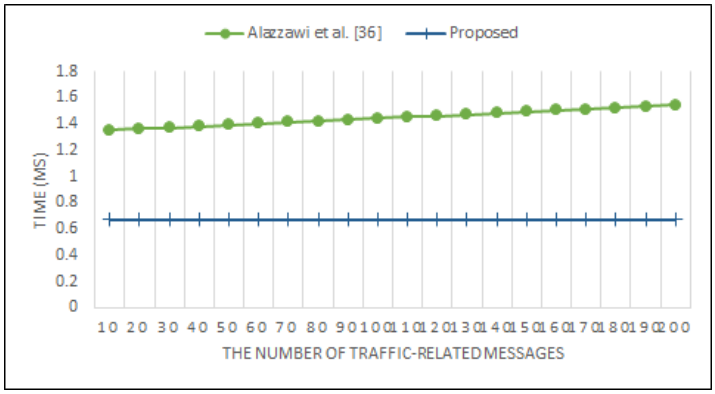

Figure 9. The computation costs of VMM between the proposed and Alazzawi et al. scheme [36].

7.2. Communication Cost Analysis

This subsection analyzes and compares the communication costs. For a fair evaluation, to satisfy the same security level in their scheme, we use the parameters indicated in Table 5. The assumptions made in our analysis are consistent across the schemes: the output sizes of the timestamp and secure hash function are 4 bytes and 20 bytes, respectively. The communication costs of each scheme are presented in Table 8.

In Jianhong et al.'s [31] scheme, the vehicle broadcasts a message–signature tuple $\{AID_i, M_i, S_i, T_i\}$, due to the AID_i, M_i, $S_i \in G_1$; therefore, the size of the tuple in their scheme is $128 \times 3 + 4 = 388$ bytes. In addition, the size of a message–signature tuple $\{PID_v, m, W, T, T_{sk}, \sigma_m\}$ in the Alazzawi et al.'s [36] scheme is $40 + 20 \times 3 + 8 = 108$ bytes, due to the $PID_{v1} \in G$ and the PID_{v2}, W, $\sigma_m \in Z_q^*$. The communication cost calculation is carried out in the same manner for other schemes. In the proposed scheme, the vehicle broadcasts a message–signature tuple $\{PID_i, m_i, T_i, \sigma_i\}$ with size $40 + 20 \times 3 + 8 = 104$ bytes.

Table 8. Comparison of communication cost.

Schemes	Message–Signature Tuple	Single Message	n Messages
Jianhong et al. [31]	$\{AID_i, M_i, S_i, T_i\}$	388 bytes	388 n bytes
Lei Zhang et al. [32]	$\{ID_{V_i}, VP_i, IPID_{V_i}, \sigma_i\}$	148 bytes	148 n bytes
Bayat et al. [34]	$\{M_i, pid_i, \sigma_m\}$	388 bytes	388 n bytes
He et al. [35]	$\{Mi, AID_i, T_i, R_i, \sigma_i\}$	144 bytes	144 n bytes
Alazzawi et al. [36]	$\{PID_v, m, W, T, T_{sk}, \sigma_m\}$	108 bytes	108 n bytes
Proposed	$\{PID_i, m_i, T_i, \sigma_i\}$	104 bytes	104 n bytes

8. Conclusions and Future Work

An identity-based conditional privacy-preserving authentication scheme for VANETs is proposed in this paper. In contrast to other schemes, the proposed scheme can withstand the side-channel attack by regularly updating the sensitive information kept on the TPD inside the vehicle's OBU. In areas with high-density traffic, the proposed scheme's batch verification process can efficiently verify multiple safety-related messages transmitted from different nodes in VANETs. The proposed scheme is also proven secure against forgery of adaptively chosen message attacks in the random oracle model. Security analysis shows that the proposed scheme satisfies all of the design goals in terms of the security and privacy of VANETs. Finally, since the proposed scheme does not use bilinear pairing operation and Map-To-Point hash function, the overhead costs of the proposed scheme are the lowest compared to five other identity-based conditional privacy-preserving authentication schemes. Therefore, the proposed scheme has better efficiency in terms of computation and communication overheads.

In future work, the experiment could be carried out using simulation platforms, such as OMNET++ and SUMO, to simulate VANET networks and road traffic, respectively, to verify and validate the proposed work, including the security resilience aspect of the proposed scheme. In addition, the data leakage issue does not only exist in VANET environment. It is also a big concern in emerging technology-based applications such as Internet of Things and cloud computing environments. Therefore, the proposed privacy-preserving authentication scheme could be applicable to a wide range of areas, and not just for VANET.

Author Contributions: Conceptualization, M.A.A.-s., M.A. and S.M.; Supervision, M.A. and S.M.; Writing—original draft, M.A.A.-s.; Writing—review and editing, I.H.H., M.A.A.-s. and S.M.; Funding acquisition, I.H.H. and M.A.; Investigation, M.A.A.-s.; Software, M.A.A.-s. All authors have read and agreed to the published version of the manuscript.

Funding: This work was partially funded by external agency U Mobile Sdn Bhd via Universiti Sains Malaysia (USM).

Acknowledgments: This work was partially supported by National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia and external grant from U Mobile Sdn Bhd [grant number: 304/PNAV/650958/U154].

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Al-Shareeda, M.A.; Anbar, M.; Hasbullah, I.H.; Manickam, S.; Hanshi, S.M. Efficient Conditional Privacy Preservation With Mutual Authentication in Vehicular Ad Hoc Networks. *IEEE Access* **2020**, *8*, 144957–144968. [CrossRef]
2. Al-Shareeda, M.A.; Anbar, M.; Manickam, S.; Yassin, A.A. VPPCS: VANET-Based Privacy-Preserving Communication Scheme. *IEEE Access* **2020**, *8*, 150914–150928. [CrossRef]
3. Wang, S.; Mao, K.; Zhan, F.; Liu, D. Hybrid conditional privacy-preserving authentication scheme for VANETs. *Peer-to-Peer Netw. Appl.* **2020**, *13*, 1600–1615. [CrossRef]
4. Sheikh, M.S.; Liang, J.; Wang, W. A Survey of Security Services, Attacks, and Applications for Vehicular Ad Hoc Networks (VANETs). *Sensors* **2019**, *19*, 3589. [CrossRef]
5. Ali, I.; Hassan, A.; Li, F. Authentication and privacy schemes for vehicular ad hoc networks (VANETs): A survey. *Veh. Commun.* **2019**, *16*, 45–61. [CrossRef]

6. Yang, X.; Yi, X.; Khalil, I.; Zeng, Y.; Huang, X.; Nepal, S.; Yang, X.; Cui, H. A lightweight authentication scheme for vehicular ad hoc networks based on MSR. *Veh. Commun.* **2019**, *15*, 16–27. [CrossRef]
7. Hao, Y.; Cheng, Y.; Zhou, C.; Song, W. A distributed key management framework with cooperative message authentication in VANETs. *IEEE J. Sel. Areas Commun.* **2011**, *29*, 616–629. [CrossRef]
8. Al-shareeda, M.A.; Anbar, M.; Hasbullah, I.H.; Manickam, S. Survey of Authentication and Privacy Schemes in Vehicular ad hoc Networks. *IEEE Sens. J.* **2020**. [CrossRef]
9. Ali, I.; Lawrence, T.; Li, F. An efficient identity-based signature scheme without bilinear pairing for vehicle-to-vehicle communication in VANETs. *J. Syst. Archit.* **2020**, *103*, 101692. [CrossRef]
10. Förster, D.; Kargl, F.; Löhr, H. PUCA: A pseudonym scheme with user-controlled anonymity for vehicular ad-hoc networks (VANET). In Proceedings of the 2014 IEEE Vehicular Networking Conference (VNC), Paderborn, Germany, 3–5 December 2014; IEEE: Piscataway, NJ, USA, 2014; pp. 25–32.
11. Huang, D.; Misra, S.; Verma, M.; Xue, G. PACP: An efficient pseudonymous authentication-based conditional privacy protocol for VANETs. *IEEE Trans. Intell. Transp. Syst.* **2011**, *12*, 736–746. [CrossRef]
12. Lu, R.; Lin, X.; Luan, T.H.; Liang, X.; Shen, X. Pseudonym changing at social spots: An effective strategy for location privacy in vanets. *IEEE Trans. Veh. Technol.* **2011**, *61*, 86–96. [CrossRef]
13. Sun, Y.; Zhang, B.; Zhao, B.; Su, X.; Su, J. Mix-zones optimal deployment for protecting location privacy in VANET. *Peer- Netw. Appl.* **2015**, *8*, 1108–1121. [CrossRef]
14. Thenmozhi, T.; Somasundaram, R. Pseudonyms based blind signature approach for an improved secured communication at social spots in VANETs. *Wirel. Pers. Commun.* **2015**, *82*, 643–658. [CrossRef]
15. Gamage, C.; Gras, B.; Crispo, B.; Tanenbaum, A. An identity-based ring signature scheme with enhanced privacy. In Proceedings of the 2006 Securecomm and Workshops, Baltimore, MD, USA, 28 August–1 September 2006; IEEE: Piscataway, NJ, USA, 2006; pp. 1–5.
16. Wasef, A.; Shen, X. Efficient group signature scheme supporting batch verification for securing vehicular networks. In Proceedings of the 2010 IEEE International Conference on Communications, Cape Town, South Africa, 23–27 May 2010; IEEE: Piscataway, NJ, USA, 2010; pp. 1–5.
17. Chaum, D.; Van Heyst, E. Group signatures. In *Workshop on the Theory and Application of of Cryptographic Techniques*; Springer: Berlin/Heidelberg, Germany, 1991; pp. 257–265.
18. Studer, A.; Shi, E.; Bai, F.; Perrig, A. TACKing together efficient authentication, revocation, and privacy in VANETs. In Proceedings of the 2009 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, Rome, Italy, 22–26 June 2009; IEEE: Piscataway, NJ, USA; 2009; pp. 1–9.
19. Lin, X.; Lu, R.; Zhang, C.; Zhu, H.; Ho, P.H.; Shen, X. Security in vehicular ad hoc networks. *IEEE Commun. Mag.* **2008**, *46*, 88–95.
20. Lin, X.; Sun, X.; Ho, P.H.; Shen, X. GSIS: A secure and privacy-preserving protocol for vehicular communications. *IEEE Trans. Veh. Technol.* **2007**, *56*, 3442–3456.
21. Shamir, A. Identity-based cryptosystems and signature schemes. In *Workshop on the Theory and Application of Cryptographic Techniques*; Springer: Berlin/Heidelberg, Germany, 1984; pp. 47–53.
22. Zhang, C.; Lu, R.; Lin, X.; Ho, P.; Shen, X. An efficient identity-based batch verification scheme for vehicular sensor networks. In Proceedings of the IEEE INFOCOM 2008-The 27th Conference on Computer Communications, Phoenix, AZ, USA, 13–18 April 2008; IEEE: Piscataway, NJ, USA, 2008; pp. 246–250.
23. Zhang, C.; Ho, P.H.; Tapolcai, J. On batch verification with group testing for vehicular communications. *Wirel. Netw.* **2011**, *17*, 1851. [CrossRef]
24. Jiang, Y.; Shi, M.; Shen, X.; Lin, C. BAT: A robust signature scheme for vehicular networks using binary authentication tree. *IEEE Trans. Wirel. Commun.* **2008**, *8*, 1974–1983. [CrossRef]
25. Sun, J.; Zhang, C.; Zhang, Y.; Fang, Y. An identity-based security system for user privacy in vehicular ad hoc networks. *IEEE Trans. Parallel Distrib. Syst.* **2010**, *21*, 1227–1239.
26. Chim, T.W.; Yiu, S.M.; Hui, L.; Li, V. SPECS: Secure and Privacy Enhancing Communications Schemes for VANETs. *Ad Hoc Netw.* **2011**, *9*, 189–203. [CrossRef]
27. Shim, K.A. CPAS: An Efficient Conditional Privacy-Preserving Authentication Scheme for Vehicular Sensor Networks. *IEEE Trans. Veh. Technol.* **2012**, *61*, 1874–1883. [CrossRef]
28. Shim, K.A. Reconstruction of a Secure Authentication Scheme for Vehicular Ad hoc Networks Using a Binary Authentication Tree. *IEEE Trans. Wirel. Commun.* **2013**, *12*, 5386–5393. [CrossRef]

29. Lee, C.C.; Lai, Y.M. Toward a Secure Batch Verification with Group Testing for VANET. *Wirel. Netw.* **2013**, *19*, 1441–1449. [CrossRef]
30. Horng, S.J.; Tzeng, S.F.; Pan, Y.; Fan, P.; Wang, X.; Li, T.; Khan, M.K. b-SPECS+: Batch Verification For Secure Pseudonymous Authentication in VANET. *IEEE Trans. Inf. Forensics Secur.* **2013**, *8*, 1860–1875. [CrossRef]
31. Jianhong, Z.; Min, X.; Liying, L. On The Security of a Secure Batch Verification With Group Testing for VANET. *Int. J. Netw. Secur.* **2014**, *16*, 351–358.
32. Zhang, L.; Wu, Q.; Domingo-Ferrer, J.; Qin, B.; Hu, C. Distributed aggregate privacy-preserving authentication in VANETs. *IEEE Trans. Intell. Transp. Syst.* **2016**, *18*, 516–526. [CrossRef]
33. Zhong, H.; Han, S.; Cui, J.; Zhang, J.; Xu, Y. Privacy-preserving authentication scheme with full aggregation in VANET. *Inf. Sci.* **2019**, *476*, 211–221. [CrossRef]
34. Bayat, M.; Barmshoory, M.; Rahimi, M.; Aref, M.R. A secure authentication scheme for VANETs with batch verification. *Wirel. Netw.* **2015**, *21*, 1733–1743. [CrossRef]
35. He, D.; Zeadally, S.; Xu, B.; Huang, X. An Efficient Identity-based Conditional Privacy-preserving Authentication Scheme for Vehicular Ad hoc Networks. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 2681–2691. [CrossRef]
36. Alazzawi, M.; Lu, H.; Yassin, A.; Chen, K. Efficient Conditional Anonymity with Message Integrity and Authentication in a Vehicular Ad hoc Network. *IEEE Access* **2019**, *7*, 71424–71435. [CrossRef]
37. Miller, V. Use of Elliptic Curves in Cryptography. In *Conference on the Theory and Application of Cryptographic Techniques*; Springer: Berlin/Heidelberg, Germany, 1985; pp. 417–426.
38. Lo, N.W.; Tsai, J.L. An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings. *IEEE Trans. Intell. Transp. Syst.* **2015**, *17*, 1319–1328. [CrossRef]
39. MIRACL, Inc. Multi Precision Integer and Rational Arithmetic Cryptographic Library (MIRACL). Available online: http://www.certivox.com (accessed on 13 August 2020).