sensors

MDPI

Article

A Secure Pseudonym-Based Conditional Privacy-Preservation Authentication Scheme in Vehicular Ad Hoc Networks

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

National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia, USM, Gelugor 11800, Penang, Malaysia; m.alshareeda@nav6.usm.my (M.A.A.-S.); selva@usm.my (S.M.); iznan@nav6.usm.my (I.H.H.)
* Correspondence: anbar@nav6.usm.my; Tel.: +604-653-4633

Abstract: Existing identity-based schemes utilized in Vehicular Ad hoc Networks (VANETs) rely on roadside units to offer conditional privacy-preservation authentication and are vulnerable to insider attacks. Achieving rapid message signing and verification for authentication is challenging due to complex operations, such as bilinear pairs. This paper proposes a secure pseudonym-based conditional privacy-persevering authentication scheme for communication security in VANETs. The Elliptic Curve Cryptography (ECC) and secure hash cryptographic function were used in the proposed scheme for signing and verifying messages. After a vehicle receives a significant amount of pseudo-IDs and the corresponding signature key from the Trusted Authority (TA), it uses them to sign a message during the broadcasting process. Thus, the proposed scheme requires each vehicle to check all the broadcasting messages received. Besides, in the proposed scheme, the TA can revoke misbehaving vehicles from continuously broadcasting signed messages, thus preventing insider attacks. The security analysis proved that the proposed scheme fulfilled the security requirements, including identity privacy-preservation, message integrity and authenticity, unlinkability, and traceability. The proposed scheme also withstood common security attacks such as man-in-the-middle, impersonation, modification, and replay attacks. Besides, our scheme was resistant against an adaptive chosen-message attack under the random oracle model. Furthermore, our scheme did not employ bilinear pairing operations; therefore, the performance analysis and comparison showed a lower resulting overhead than other identity-based schemes. The computation costs of the message signing, individual signature authentication, and batch signature authentication were reduced by 49%, 33.3%, and 90.2%, respectively.

Keywords: Vehicular Ad hoc Networks (VANETs); security and privacy requirements; random oracle model; pseudonym identity scheme; Elliptic Curve Cryptography (ECC)

Citation: Al-shareeda, M.A.; Anbar, M.; Manickam, S.; Hasbullah, I.H. A Secure Pseudonym-Based Conditional Privacy-Preservation Authentication Scheme in Vehicular Ad Hoc Networks. *Sensors* **2022**, *22*, 1696. https://doi.org/10.3390/s22051696

Academic Editor: Paolo Bellavista

Received: 20 January 2022
Accepted: 16 February 2022
Published: 22 February 2022

1. Introduction

In recent years, the Vehicular Ad hoc Network (VANET) has been attracting more and more attention from academia and industry [1,2]. According to a report published in 2015 [3,4], around 1800 fatalities and more than 20,000 injuries were due to road accidents annually in the United Kingdom. Therefore, the VANET, one of the cornerstone technologies of the Intelligent Transport System (ITS), is expected to help reduce traffic accidents [5,6].

VANETs are an emerging type of Mobile Ad hoc Network (MANET), where the vehicle is considered a mobile node [7]. The VANET typically comprises three components; a Trusted Authority (TA), some fixed Roadside Unit (RSU), and many mobile Onboard Units (OBUs). As presented in Figure 1, a vehicle equipped with an OBU communicates with others via Vehicle-to-Vehicle (V2V) or with the RSU via Vehicle-to-Infrastructure (V2I) communications.

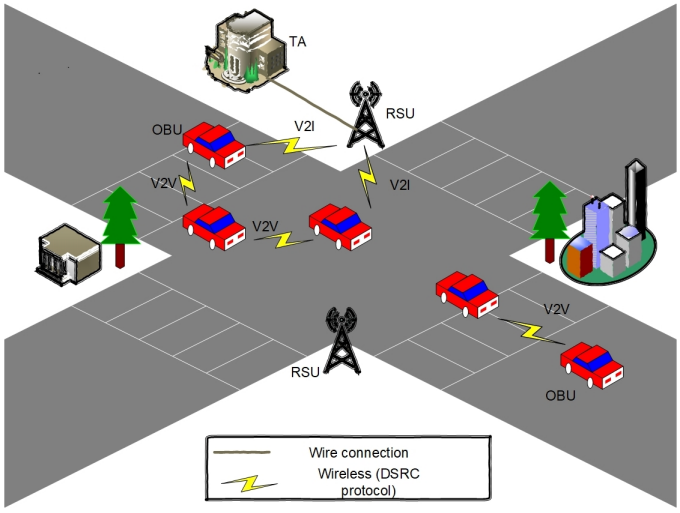

Figure 1. The structure of the VANET.

More specifically, driving safety and efficiency improvement are the main goals of ITS research, making VANETs a promising technology. Nevertheless, the advantages are out-weight by issues with security, privacy-preservation, and performance efficiency. Therefore, these challenges should be carefully considered in VANETs [8–12]. The security issue is crucial in V2V and V2I communications. The open nature of the transmission medium in VANETs is susceptible to security attacks [13–15], i.e., attackers can replay, modify, intercept, and impersonate transmitted messages in VANETs. Therefore, every receiver must check the authenticity and integrity of all received messages before accepting them. In addition, privacy preservation is also a fundamental requirement. In VANETs, attackers may discover the vehicle's identity and trace its journey paths by dissecting captured messages. Therefore, anonymous communication is needed to preserve privacy and support drivers' unlinkability requirements. Finally, performance efficiency is vital in V2V and V2I communications, apart from the security and privacy requirements.

Several scholars have proposed to address the security, privacy, and performance efficiency for the VANET system. However, some existing identity schemes have several limitations: (i) using time-consuming operations based on the bilinear pair; (ii) susceptible to an insider attack; (iii) only the vehicle's message is verified by the RSU. As a result, this renders the whole system to be exposed and insecure.

Therefore, this paper aimed to cope with these three limitations arising from the existing identity schemes by generating lists of pseudonym-IDs and the corresponding signature keys by the TA. The main contribution of this paper is a secure pseudonym-based conditional privacy-preservation authentication scheme based on Elliptic Curve Cryptography (ECC).

The proposed scheme's novelty is that: (i) it can sign and verify messages without relying on the online RSU for verification; (ii) the proposed scheme does not use the RSU during the mutual authentication process, thereby the TA issues and preloads the pool of pseudonym-IDs and the corresponding signature keys into the vehicle; (iii) the TA can revoke attackers' certificates to prevent the continuous broadcast of fake signed messages.

The rest of the paper is structured as follows. The review of existing works is in Section 2. Section 3 presents the design of our scheme. Section 5 gives an illustrative example of the proposed scheme, followed by an in-depth discussion of the proposed scheme for VANETs in Section 4. Section 6 presents the security proof and analysis of the proposed scheme. In Section 7, we discuss the performance of the proposed scheme and a comparison with several existing schemes. Finally, Section 8 concludes this paper.

2. Related Work

In order to mitigate the burden of preloading several key pairs and their corresponding certificates from the common Public Key Infrastructure (PKI), in 1984, Shamir introduced the Identity (ID) approach [16]. This ID eliminated the need for key pairs and their corresponding certificates with the PKI due to not utilizing any certificate for verifying messages, thus decreasing the overhead generated from the messages containing certificates. Consequently, several studies have proposed ID-based schemes for communication security. In the following subsection, we classify the ID-based schemes in three ways.

2.1. ID Bilinear Pair Based

Zhang et al. [17,18] utilized the vehicle's identity in which a vehicle is not required to preload a pool of key pairs and the corresponding certificates, eliminating the need for large storage, therefore reducing the overall processing overhead. Additionally, it mitigates the need to manage certificates and a CRL. Jiang et al. [19] suggested a Binary Authentication Tree (BAT) by using an ID-based scheme for V2I communication in VANETs. Huang et al. [20] suggested leveraging an ID-based scheme, called PACP, which relies on utilizing pseudonyms instead of the original identities, providing conditional privacy-preservation in VANETs. Chim et al. [21] and Lee and Lai [22] highlighted that the schemes proposed in [17,18] are not able to satisfy the traceability requirement. Besides, these schemes are vulnerable to impersonation and replay attacks. Lee and Lai [22] proposed an enhanced authentication scheme to secure communication and fulfill high-performance efficiency in VANETs. Horng et al. [23] pointed out that the scheme in [21] is vulnerable to security attacks such as impersonation and that an attacker can mimic an authorized vehicle for broadcasting bogus messages in VANETs. Therefore, Horng et al. [23] suggested a scheme named SPECS to enhance the scheme's limitations [21]. Jianhong et al. [24] pointed out many security limitations in the scheme by Lee and Lai [22]. For instance, it cannot satisfy the requirements of non-repudiation and traceability and it cannot withstand attacks, such as replay attacks. In order to address the limitations in the scheme of Lee and Lai [22], Jianhong et al. [24] proposed an enhanced authentication scheme for communication security in VANETs.

ID-bilinear-pair-based schemes [17–24] utilize the bilinear pairing operations in their schemes. However, these schemes have a high overhead in terms of performance efficiency, owing to the time-consuming operation of the bilinear pair in VANETs.

2.2. ID Vulnerable to Insider Attack Based

He et al. [25] suggested an authentication scheme established on conditional privacy preservation for communication security in VANETs that does not utilize bilinear pairing operations during message signing and verification. For instance, in the scheme of He et al. [25], the system's master key (TA) is preloaded and saved on the TPD of the vehicle and remains there for a long time. However, if an insider attacker compromises one vehicle, the entire VANET system will be vulnerable and insecure. The TA cannot revoke the compromised vehicle's certificate to prevent it from being in the system. Therefore, the scheme by He et al. [25] does not satisfy the revocation requirement. Zhong et al. [26] structured a security and privacy scheme for secure service provision, accounting for messages' security and users' privacy in VANETs. Lo and Tasi [27] proposed an authentication scheme based on conditional privacy preservation for communication security in VANETs by adopting an ID-based scheme using ECC. Wu et al. [28] designed the concept of location to propose an authentication scheme based on conditional privacy preservation without using the operation of the bilinear pairing and TPD in VANETs. Xie et al. [29] proposed an authentication scheme based on conditional privacy preservation, which utilizes ID-based signatures to guarantee messages' reliability and integrity in VANETs.

In ID vulnerable-to-insider-attack-based schemes [25–29], when a vehicle is transmitting false messages, the TA has the ability to trace this vehicle, but does not have the ability to revoke it for broadcasting these messages. Furthermore, an insider attacker has

the ability to possibly disclose the vehicle's identity, since the attacker has the key pairs of the TA. Thus, none of these schemes satisfy the revocation and privacy-preservation requirements in VANET.

2.3. ID RSU Authentication Based

Cui et al. [30] introduced a secure privacy-preservation authentication scheme based on ECC in VANETs. A cuckoo filter and binary search methods were used in this scheme to enhance the success rate of batch signature authentication. Zhong et al. [31] suggested an authentication scheme based on conditional privacy preservation, which utilizes the list of registration rather than the list of revocation to decrease the overhead of the system in terms of communication cost.

ID-RSU-authentication-based schemes [30,31] rely on RSUs to authenticate the traffic-related messages and then broadcast authentic and rogue vehicles lists with the notification issues. Therefore, the vehicle will wait for these issues before checking the validity of the signer, which increases the overhead.

In this paper, we propose a secure pseudonym-based conditional privacy-preservation authentication scheme to cope with the above-mentioned issues. It utilizes ECC rather than the bilinear pair operations to reduce the overhead of the system in terms of performance efficiency in ID-bilinear-pair-based schemes [17–24]. In addition, the authentic sender signs the message by utilizing a signature generated by the TA during the registration phase, and this process assists in coping with the flaws in ID vulnerable-to-insider-attack-based schemes [25–29]. Unlike the ID-RSU-authentication-based schemes [30,31], the proposed scheme relies on each vehicle checking the received messages.

3. Preliminaries

In this section, the network model, as well as the security requirements of the proposed scheme are presented. Besides, the mathematical tool used in this work is described as well.

3.1. Network Model

The network model of the proposed scheme consisted of three components, the TA, RSU, and OBU:

- TA: The TAs are trusted parties in VANETs with high resources such as computation and communication. The TA issues the system's public parameters, pseudo-ID, and the private keys for each vehicle and transmits them to each respective vehicle;
- RSU: The RSU is a wireless base station deployed on the road as a brigade interface between the TA and OBUs. The RSU connects with the TA by wired technology and connects with vehicles by wireless technology;
- OBU: Each vehicle is fit with an On-Board Unit (OBU), enabling the vehicle to process, receive, and broadcast messages in the VANET. Each OBU is equipped with a Tamper-Proof Device (TPD) that is usually utilized to keep secrets. Therefore, it is difficult for any adversary to obtain the information stored in the TPD.

3.2. Security Requirements

The proposed scheme must fulfill all security and privacy requirements to achieve V2V and V2I communication security in VANETs. The security and privacy requirements are as follows:

- Authentication and integrity: The vehicle or RSU must be able to identify any alteration of the received message and must have the ability to authenticate the integrity and validity of the received messages to ensure communication security;
- Identity privacy preservation: An attacker must not have the ability to reveal the vehicle's identity by capturing multiple messages transmitted by it. Therefore, the vehicle's identity must remain anonymous to other legal and illegal nodes to ensure users' privacy;

- Traceability: The TA must have the ability to reveal the vehicle's identity from its message in case of any misbehavior to prevent misbehaving vehicles from denying their responsibility for disrupting the system by broadcasting false messages to other registered vehicles;
- Unlinkability: The misbehaving vehicles and RSUs cannot link two or more messages transmitted by the same source to ensure privacy preservation.

3.3. Adversary Model

A better understanding of adversity attacks against VANETs is needed. The following attack types should be resisted in the proposed scheme on VANETs:

- Replay attacks. Malicious nodes replay the previously generated legitimate signature to the recipient;
- Modification attacks. Malicious nodes alter authentic messages and broadcast them to other users [32];
- Impersonation attacks. Malicious nodes impersonate an authentic node and broadcast a legitimate message to other nodes;
- Man-in-the-middle attacks. Malicious nodes intercept two sides of the communication and perform data tampering and sniffing [33,34].

3.4. Elliptic Curve Cryptography

Elliptic Curve Cryptography (ECC) [35] is a tool used in the security algorithms' design and digital signatures to secure communications. Due to the length of the smaller key and the same security level contrast with other encryption tools, ECC is commonly utilized in cryptography.

Definition 1. *Elliptic curve: Consider that the large prime value p is the order of F_p and F_p is a finite field. The equation of an elliptic curve E is determined as $y^2 = x^3 + ax + b \bmod p$, where $a, b \in F_p$.*

There is an additive group G_q identified on E, the order of which is q, and the generator is P. Let O be an infinity point:

– *Scalar multiplication. Denote $P \in G_q$, $n \in Z_q^*$, then the scalar multiplication is $L \cdot P = P + P + P + \ldots + P$ (for all the L times).*

Definition 2. *Computational Diffie–Hellman Problem (CDHP): There are two random points P, $Q \in G$, where $P = yP$, $Q = xP$, x, y are unknown integers, and it is impossible to calculate xyP.*

Definition 3. *Elliptic Curve Discrete Logarithm (ECDL) problem: Given two random points P, $Q \in G$, and $Q = xP$, it is impossible to calculate x from Q in the polynomial time t.*

4. The Proposed Scheme

Security and privacy are significant challenges that need to be carefully faced in VANET communication. This paper proposes a conditional privacy persevering based on mutual authentication scheme to fulfill the security and privacy requirements and reduce the system's overhead. The secure pseudonym-based scheme means that the proposed scheme satisfies all security and piracy requirements mentioned (Section 3.2) and resists common security attacks, especially insider attacks. The proposed scheme consists of five phases: initialization, vehicle registration, message signing, individual signature authentication, and batch signature authentication, as shown in Figure 2.

The behavior of the overall system is as follows. The first phase is initialization, where the TA is responsible for generating and preloading the public parameters of the system based on an elliptic curve. The second phase is vehicle registration, where the TA is responsible for generating and preloading the list of pseudonym-IDs and signature keys to each participating registered vehicle in the VANET. The third phase is message signing, where the registered vehicle signs each traffic message by using randomly the pseudonym-

ID and the signature key before broadcasting. The fourth phase is individual signature authentication, where the receiving vehicle should verify the validity and authenticity of the message before accepting. The fifth phase is batch signature authentication, where the verified vehicle has the ability to check a large number of messages simultaneously. Furthermore, when receiving a report about a malicious vehicle, the TA is responsible for tracing and revoking it. After all pseudonym-IDs have expired, the TA does not update the new pseudonym-ID list to avoid it being utilized for additional applications and services in the VANET. Table 1 presents the notation utilized and their definitions in the following phases.

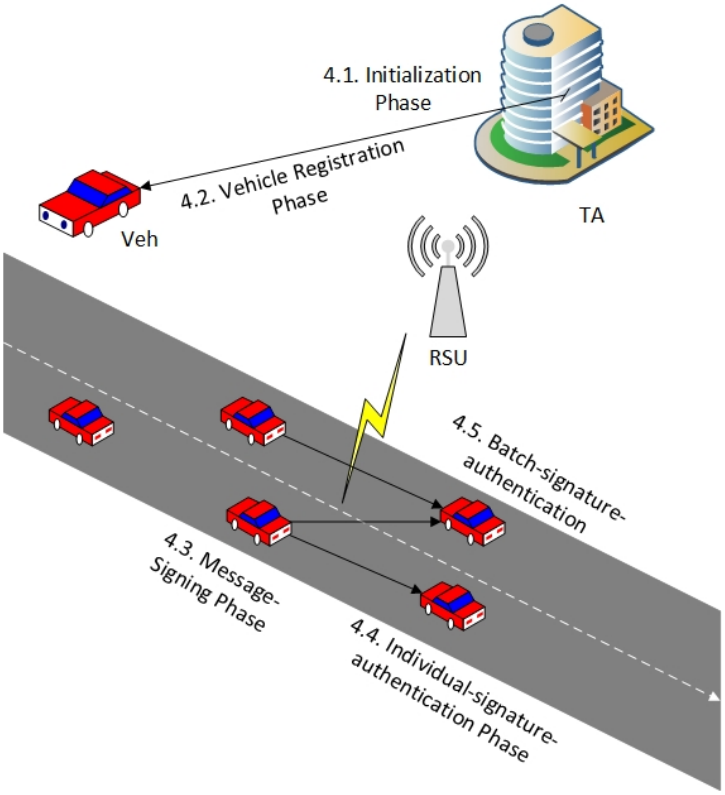

Figure 2. Overall flowchart of the proposed scheme.

Table 1. Notations and their description.

Notations	Descriptions
a, b	Two large prime numbers
p	A large prime number
E	The elliptic curve
G	The additive group based on E
P	The base generator P$\in$ G
h_1, h_2, h_3	The three functions of the one-way hash
ID_{VI}, PW	The identity and password of the vehicle
s, P_{pub}	The private and public key of the system
pid_{il}^1, pid_{il}^2	The pseudo-identity of the vehicle
$\oplus$	The XOR operator
$LPID_i$	The list of pseudo-identities
ζ_l	The random secret value
$\|\|$	The concatenation operation
LSK_i	The list of signature keys

4.1. Initialization

The TA executes the initialization parameter of the public system in the following steps:

- The TA sets the chosen elliptic curve E determined by the non-singular equation ($y^2 = x^3 + ax + b \bmod p$), where $a, b \in F_p$ and p is a large prime number;
- The TA chooses a point P on $E_p(a, b)$ as an adaptive group generator G of prime order q;
- The TA selects the private key $s \in Z_q^*$ of the system and computes the respective public key $P_{pub} = sP$ of the system;
- The TA selects three secure cryptographic hash functions $h_1 : G \rightarrow Z_q^*$ $h_2 : \{0,1\}^* \times \{0,1\}^* \times G \rightarrow Z_q^*$ $h_3 : \{0,1\}^* \rightarrow Z_q^*$;
- The TA publishes the functions and the public parameters of the system to all RSUs via public channels.

4.2. Vehicle Registration

The TA registers the vehicle as follows:

- The owner of the vehicle submits personal information including the identity ID_{vi} and password PW to the TA through a secure communication channel;
- After the personal information is received, the TA first starts the authenticity of ID_{vi};
- After checking the validity of ID_{vi}, the TA chooses n random secret values $\zeta_l \in Z_q^*$, where $l = 1 : n$, and calculates a family of unlinkable pseudo-IDs $LPID_i = < pid_{il}, \ldots, pid_{in} >$ as follows:

$$\begin{aligned} pid_{in} &=< pid_{il}^1, pid_{il}^2 > \\ &=< \zeta_l P, ID_{vi} \oplus h_1(\zeta_l P_{pub}) > \end{aligned} \tag{1}$$

  where l = 1,2, … n;
- For each pseudo-ID $pid_{il} \in LPID_i, l = 1 : n$, the TA calculates the respective signature key SK as follows and organizes $LSK_i =< sk_{il}, \ldots, sk_{in} >$:

$$sk_{il} = s \cdot h_2(pid_{il}^1 || pid_{il}^2); \tag{2}$$

- The TA then transmits the n of ζ_l, $LPID_i$, and LSK_i to the vehicle via a secret technology.

The process of preloading as introduced in [26,36] is to guarantee the requirements of the security and privacy of ζ_l, the pseudo-ID, and the signature keys for the proposed scheme. The TA preloads a new list of ζ_l, the pseudo-ID, and the signature keys that are utilized for a short time for each vehicle moving in a VANET close to the expiration time; they are renewed with a new pseudo-ID and signature key pool.

Our previous study [37] was based on the RSU executing the authentication process by issuing and preloading a pool of pseudonym-IDs and the corresponding signature keys into each registered vehicle. However, the disadvantages of RSU utilization are: (i) once a single RSU is compromised, as a result, the whole system becomes insecure; (ii) RSUs are expensive in terms of installation and maintenance; (iii) adding a TPD to both the OBU and the RSU makes the system even more costly. Besides, our previous study [37] depended on generating several keys to each domain, which makes the key exchange complete.

Therefore, this paper aimed to address these issues by issuing and preloading a pool of pseudonym-IDs and the corresponding signature keys from the TA. This was because the resource of the TA is high in terms of computation and communication costs. Hence, the proposed scheme does not use RSUs during the mutual authentication process. Besides, only the private key and public key of the TA are used to sign and verify the messages.

4.3. Message Signing

The signer (OBU or RSU) signs and broadcasts traffic-related messages m_i to other vehicles in the VANET. A vehicle with pseudo-ID pid_{in} receives a message m_i and signs it

by utilizing its signature keys sk_{il} and the public parameter of the system. This is executed in the phases below:

- OBU_i randomly chooses a pseudo-ID pid_{in} with the respective ζ_l and sk_{il};
- OBU_i computes the message signature $\delta_{m_i} = sk_{il} + \zeta_l \cdot h_3(m_i||T)$, where T is the current timestamp;
- OBU_i computes $Y_i = h_3(m_i||T)pid_{il}^1$;
- OBU_i sets the authentic signature as $\sigma_i = \{\delta_{m_i}, Y_i\}$ for m_i;
- Finally, the message signature tuple $\{pid_{in}, m_i, T, \sigma_i\}$ is sent to the neighboring recipient.

4.4. Individual Signature Authentication

The main aim of this method was to verify only one message signature δ_{m_i} on traffic-related message m_i by the recipient (OBU or RSU). Before accepting the message m_i, once having received a signed message m_i, the recipient would check the node authenticity and validity of the message. This guarantees that no illegitimate recipient is impersonating a legitimate recipient or sending fake messages. The recipient receives an authentic signature $\sigma_i = \{\delta_{m_i}, Y_i\}$ on the traffic-related message m_i from the vehicle with a pseudo-ID pid_{in} in timestamp T, where $i = 1$, and checks its authenticity and validity as below:

- Once the message signature tuple $\{pid_{in}, m_i, T, \sigma_i\}$ is received, the OBU first verifies the validity of timestamp T. If $(T > T_r - T_{\bigtriangledown})$, where T_r is the time of receiving and $T_{\bigtriangledown}$ is the time of the predefined delay, then T is fresh. Otherwise, the message is rejected;
- The OBU utilizes the public parameter and functions of the system and authentic signature $\sigma_i = \{\delta_{m_i}, Y_i\}$ on the message m_i. Therefore, if Equation (3) holds, the OBU accepts it.

$$\delta_{m_i} P = h_2(pid_{il}^1||pid_{il}^2)P_{pub} + Y_i \tag{3}$$

The proof of the correctness is as follows:

$$\begin{aligned} & L.H.S\Big(\delta m_i \cdot P\Big) \\ &= \Big(sk_{il} + \zeta_l \cdot h_3(m||T)\Big).P \\ &= \Big(s \cdot h_2(pid_{il}^1||pid_{il}^2) + \zeta_l \cdot h_3(m||T)\Big) \cdot P \\ &= h_2(pid_{il}^1||pid_{il}^2)s \cdot P + h_3(m||T)\zeta_l \cdot P \\ &= h_2(pid_{il}^1||pid_{il}^2)P_{pub} + h_3(m||T)pid_{il}^1 \\ &= h_2(pid_{il}^1||pid_{il}^2)P_{pub} + Y_i \\ &= R.H.S \end{aligned}$$

Thus, the individual signature authentication correctness is accurate.

4.5. Batch Signature Authentication

The main aim of this method is to authenticate a multiple of messages signature $\delta_{m_i} = \{\delta_{m_1}, \delta_{m_2}, \delta_{m_3}, \ldots, \delta_{m_n}\}$ on n traffic-related messages $m_i = \{m_1, m_2, m_3 \ldots, m_n\}$ from n vehicles with n pseudo-ID $pid_{in} = \{pid_{i1}, pid_{i2}, pid_{i3}, \ldots, pid_{in}\}$. The verifying recipient checks its authenticity and validity as shown in the following steps:

- The OBU checks the validity of timestamp T. If $(T > T_r - T_{\bigtriangledown})$, T is fresh. Otherwise, the message is rejected;
- The OBU utilizes the small exponent technique [23,38] to achieve security in the proposed scheme. The OBU issues a random value γ_i= $\{\gamma_1, \gamma_2, \gamma_3, \ldots, \gamma_n\}$, where $\gamma_i \in [1 : 2^t]$ and t is a small value;
- The OBU utilizes the following Equation (4) to accept them.

$$\left(\sum_{i=1}^{n}(\gamma_i \cdot \delta_{m_i})\right) \cdot P = \left(\sum_{i=1}^{n}(\gamma_i.h_2(pid_{il}^1||pid_{il}^2)P_{pub})\right) + \sum_{i=1}^{n}(\gamma_i Y_i) \quad (4)$$

5. Illustrative Example

In this section, we describe an illustrative example of the five phases of the proposed scheme: initialization, vehicle registration, message signing, individual signature authentication, and batch signature authentication according to our simulation experiment (Section 7.1). The illustrative example of the proposed scheme is as follows.

5.1. Example of Initialization Phase

The first phase includes the initialization of the system's public parameters and the generation of the secure key pairs by the TA component in the VANET system. Figure 3 shows the parameters and their assigned values used in the illustrative examples. These parameters were generated based on the NIST P-192 Curve.

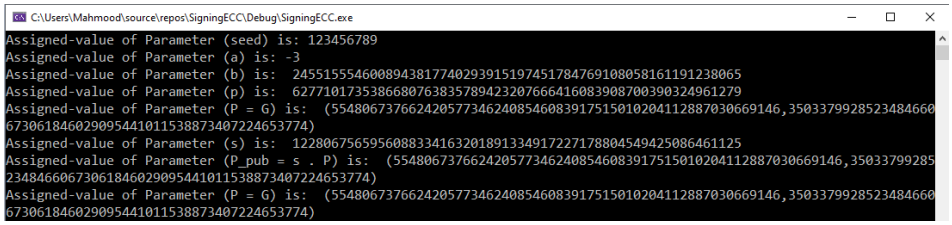

Figure 3. Input parameters and assigned values for the illustrative examples.

5.2. Example of the Vehicle Registration Phase

The second phase includes the vehicle registration by the TA before the vehicle leaves the factory. The TA is responsible for issuing and preloading the list of pseudonym-IDs and the corresponding signature keys to each participating vehicle. Figure 4 shows one example of a list of pseudonym-IDs and the corresponding signature keys.

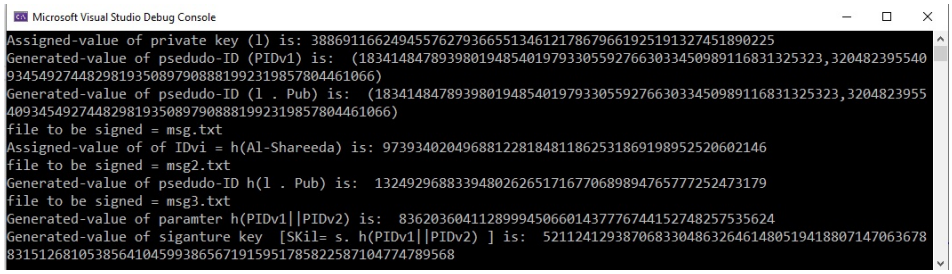

Figure 4. List of pseudonym-IDs and the corresponding signature keys.

As mentioned in Equation (1), $pid_{il}^2 = ID_{vi} \oplus h_1(\zeta_l P_{pub})$, where ID_{vi} = 973934020496 8812281848118625318691989525206021 46 and $h_1(\zeta_l P_{pub})$ = 1324929688339480262651716770689 8947657777252473179. Therefore, the result of pid_{il}^2 is :

$$97393402049688122818481186253186919895252060214 6 \oplus$$
$$1324929688339480262651716770689894765777252473179 =$$
$$3799002363776098056355358412905730353285183926 97$$

where pid_{il}^2 is the pseudonym-ID of the vehicle, ID_{vi} is the real identity of the vehicle, ζ_l is a random private key of pid_{il}^2, and P_{pub} is the published key of the system (TA). All these parameters are based on an elliptic curve.

5.3. Example of the Message Signing Phase

After the vehicle has saved the list of signature keys and the corresponding signature keys, it is considered as an authenticated node and allowed to broadcast messages. Figure 5 shows the broadcasting message signature tuple in the VANET.

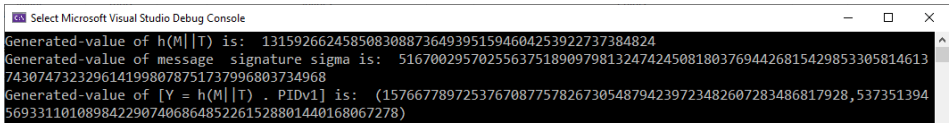

Figure 5. Broadcasting message signature tuple in the VANET.

5.4. Example of the Individual Signature Authentication Phase

Upon receiving the message signature tuple, the verifier uses a scalar multiplication operation to check the freshness of the timestamp and the validity of the message. The verifier executes the following process :

$\sigma_i \cdot P =$ (22703271006009480431127231989852855648084166670641804549 20, 19529674221127474676683725225909509869008660716656608958 60)

5.5. Example of the Batch Signature Authentication Phase

Upon receiving several message signature tuples, the verifier checks all signatures simultaneously as follows :

$\sum_{i=1}^{n}(\sigma_i \cdot \gamma_i) \cdot P =$ (3108195267006925604593061313615253284225390209158609199161, 29442277778847502914236757540708445811667053944962683474 67), where $\sigma_i = 11$.

6. Security Proof and Analysis

This section evaluates the proposed scheme's security proof, analysis, and comparison as follows.

6.1. Security Proof

Several scholars [25,30,31] have proposed the most secure signature algorithms that satisfy the random oracle model based on their scheme. This work was also needed to satisfy the random oracle model based on the renew procedure, pseudo-ID, and signature keys for the proposed scheme. Based on the network model and the ability of the malicious node, we show the security proof in the proposed scheme by identifying a game between attacker A and challenger C. When the game is won by attacker A, a legally forged signature can easily be returned. Consequently, if attacker A has negligible effectiveness, the proposed scheme is secure in the VANET.

Theorem 1. *Under the random oracle model, the proposed scheme can be unforgeable against an adaptively selected message attack.*

Proof. Suppose an attacker A can forge a legitimate message signature tuple $\{pid_{in}, m_i, T, \sigma_i\}$ for the VANET; therefore, a challenger C could be issued to return the ECDL problem by working A as a subroutine with non-negligible probability.

Setup initialization phase: Challenger C first sets value $s \in Z_q^*$ chosen randomly as the system's master key and calculates $P_{pub} = sP$ as the system's public key. Hence, C broadcasts the system's functions and public parameters to A.

h_1-oracle. C initializes h_{list_1} in the form of $(\alpha, \tau h_1)$. Once A receives a message in the form of (α), C tests whether (α) is in h_{list_1}, and if it exists, C sends $(\tau h_1 = h(\alpha))$ to A. Otherwise, C sets the chosen value $\tau h_1 \in Z_q^*$ randomly and adds $(\alpha, \tau h_1)$ into h_{list_1}. Then, A broadcasts $\tau h_1 = h(\alpha)$ to C.

h_2-oracle. C initializes h_{list_2} in the form of $(pid_{il}^1, pid_{il}^2, \tau h_2)$. After A receives the message in the form of (pid_{il}^1, pid_{il}^2), C tests whether (pid_{il}^1, pid_{il}^2) is in h_{list_2}, and if it exists, C broadcasts $(\tau h_2 = h(pid_{il}^1||pid_{il}^2||\tau h_2)$ to A. Otherwise, C sets the chosen value $\tau h_2 \in Z_q^*$ randomly and adds $(pid_{il}^1, pid_{il}^2, \tau h_2)$ into h_{list_2}. Then, A broadcasts $\tau h_2 = h(pid_{il}^1||pid_{il}^2||\tau h_2)$ to C.

h_3-oracle. C initializes h_{list_3} in the form of $(m_i, T, \tau h_3)$. After A receives the message in the form of (m_i, T), C tests whether (m_i, T) is in h_{list_3}, and if it exists, C sends $(\tau h_3 = h(m_i||T||\tau h_3)$ to A. Otherwise, C chooses $\tau h_3 \in Z_q^*$ randomly and puts $(m_i, T, \tau h_3)$ into h_{list_3}. Then, A sends $\tau h_3 = h(m_i||T||\tau h_3)$ to C. □

Sign oracle:

Upon receiving a sign request from A, C calculates three random numbers, $h_{i,2}$; $h_{i,3}$; $\delta_{m,i} \in Z_q^*$ and a random point $pid_{il}^2 \in G$. Then, C computes $pid_{il}^1 \in = (\delta_{m,i}P - h_{i,2}P_{pub}/h_{i,3})$. C puts $(pid_{il}^1, pid_{il}^2, \tau h_2)$ into h_{list_2} and (m_i, T) into h_{list_3}. Finally, C generates a message signature tuple $\{pid_{in}, m_i, T, \sigma_i\}$ and transmits it to A, where $pid_{in} = pid_{il}^1, pid_{il}^2$. The reply is a legal sign oracle due to the message signature tuple $\{pid_{in}, m_i, T, \sigma_i\}$ achieving the following equation:

$$\begin{aligned} \delta m_i \cdot P &= h_{i,2}P_{pub} + Y_i \\ where Y_i &= h_{i,3}pid_{il}^1 \\ \delta m_i \cdot P &= h_{i,2}P_{pub} + h_{i,3}pid_{il}^1 \\ &= h_{i,2}P_{pub} + (\delta m_i P - h_{i,2}P_{pub}) = \delta m_i \cdot P \end{aligned}$$

Output: Lastly, A results in a message signature tuple $\{pid_{in}, m_i, T, \sigma_i\}$. C tests this message using the following equation:

$$\delta_{m_i}P = h_{i,2}P_{pub} + Y_i \tag{5}$$

If Equation (5) does not hold, C ends the game.

According to the cross lemma, A can output another message signature tuple $\{pid_{in}, m_i, T\ \sigma_i^*\}$ that achieves the following equation:

$$\delta_{m_i}^*P = h_{i,2}^*P_{pub} + Y_i \tag{6}$$

According to Equations (5) and (6), we can obtain:

$$\begin{aligned} (\delta_{m_i} - \delta_{m_i}^*)P &= \delta_{m_i}P - \delta_{m_i}^*P \\ &= (h_{i,2}P_{pub} + Y_i) - (h_{i,2}^*P_{pub} + Y_i) \\ &= h_{i,2}P_{pub} - h_{i,2}^*P_{pub} \\ &= (h_{i,2} - h_{i,2}^*)P_{pub} \\ &= (h_{i,2} - h_{i,2}^*)sP \end{aligned}$$

Then, we can obtain $(\delta_{m_i} - \delta_{m_i}^*) = (h_{i,2} - h_{i,2}^*)$ s mod P.

C solves the ECDL problem by computing $(\delta_{m_i} - \delta_{m_i}^*).(h_{i,2} - h_{i,2}^*)^{-1}$. Nevertheless, under the random oracle model, owing to the ECDL problem difficulty with the non-negligible probability, the proposed scheme is resistant against an adaptively selected message attack.

6.2. Security Analysis

This subsection discusses the analyses of the proposed scheme that should achieve the security requirements according to Section 3.2 as follows.

- Authentication and integrity: Consistent with Theorem 1, no malicious node can return the ECDL problem and generate the legitimate signature; it is considered to be forged otherwise. In our scheme, the verifying recipient can test the authenticity and integrity of the message signature tuple $\{pid_{in}, m_i, T, \sigma_i\}$ sent from the vehicle by checking the equation $\delta_{m_i}P = h_2(pid_{il}^1||pid_{il}^2)P_{pub} + Y_i$ before accepting it. If verified and validated, the recipient accepts traffic-related message m_i; otherwise, the message is rejected. Thus, our scheme can satisfy messages' authentication and integrity requirements;
- Identity privacy preservation: After the identity ID_{vi} of a vehicle is received, the TA converts it to pseudo-ID pid_{in} in the proposed scheme. The main purpose of this requirement is to support anonymous communication and preserve the driver's privacy. The pseudo-ID pid_{in} involves two secret values ζ_l and s selected randomly

by the OBU and TA, respectively. It is impossible for an attacker to disclose identity ID_{vi} from pseudo-ID $pid_{in} = pid_{in} =< pid_{il}^1, pid_{il}^2 > =< \zeta_l P, ID_{vi} \oplus h_1(\zeta_l P_{pub}) >$ of any vehicle without knowing ζ_l and s. Therefore, it cannot calculate $spid_{il}^1 = s\zeta_l P$ from $P_{pub} = sP$ and $pid_{il}^2 = \zeta_l P$ to obtain the identity ID_{vi} of the vehicle because it is a difficult CDHP problem. Thus, the proposed scheme can satisfy the identity privacy-preservation requirement in the VANET;

- Traceability: If a malicious node broadcasts a bogus message, i.e., m_i to participating vehicles to disrupt the system managing the road, the TA can revoke the malicious node's identity after tracing him/her during traveling. Suppose a vehicle V_i issues a false message m_i and sends it to a vehicle V_j. The TA receives a report on the forged message m_i from vehicle V_j. The TA verifies the pseudo-ID pid_{in} on message m_i for vehicle V_i in its database registration list. When the pseudo-ID pid_{in} is match stored, the TA uses its private key s to disclose the identity ID_{vi} of vehicle V_i by calculating the following:

$$\begin{aligned} ID_{vi} &= pid_{il}^2 \oplus h_1(s.pid_{il}^1) \\ &= h_1(\zeta_l.P_{pub}) \oplus h_1(s.pid_{il}^1) \\ &= ID_{vi} \end{aligned} \tag{7}$$

After tracing the vehicle's identity, the TA revokes its database registration list, saves it in the Certificate Renovation List (CRL). The vehicle cannot send traffic-related messages in the VANET. Therefore, our scheme can satisfy the traceability requirement in the VANET;

- Unlinkability: Each message signature tuple $\{pid_{in}, m_i, T, \sigma_i\}$ involves a pseudo-ID $pid_{in} =< pid_{il}^1, pid_{il}^2 >$, where $pid_{il}^1 = \zeta_l \cdot P$ and $\zeta_l \in Z_q^*$ is a random secret value; therefore, the particular vehicle generates the different pseudo-ID in our scheme. Furthermore, since vehicles utilize different pseudo-IDs to sign every message m_i, an attacker cannot link multiple messages transmitted by the same source. Thus, the proposed scheme can satisfy the unlinkability requirement in the VANET;
- Security attack resistance: The proposed scheme can resist the common attacks as follows. Figure 6 shows the process of the system resisting replay, modification, and impersonation attacks;

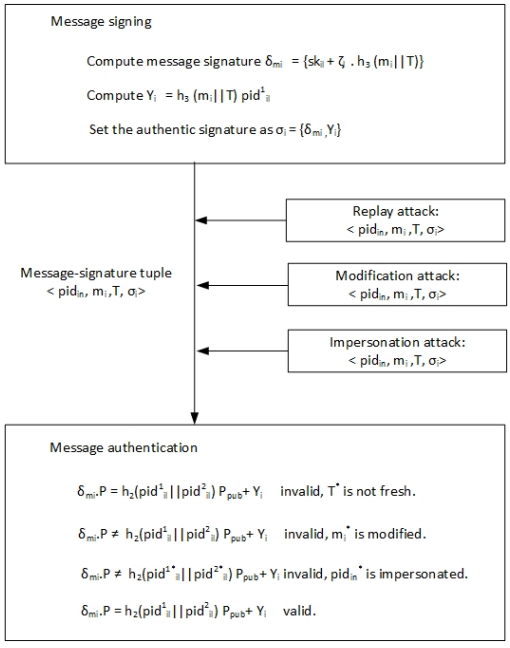

Figure 6. The process of the system resisting attacks.

- Replay attacks. In the proposed scheme, timestamp T in the message signature tuple $\{pid_{in}, m_i, T, \sigma_i\}$ allows the recipient to check the authenticity of the message m_i. Once the vehicle receives the message m_i, it verifies the freshness of the timestamp by verifying whether the inequalities $(T > T_r - T_{\bigtriangledown})$ hold. If it is fresh, the message m_i is accepted; otherwise, the vehicle does not accept message m_i. The proposed scheme can detect the message m_i replay in the VANET. Therefore, our scheme can withstand replay attacks in the VANET;
- Modification attacks. An attacker cannot modify a message signature tuple $\{pid_{in}, m_i, T, \sigma_i\}$ consistent with Theorem 1 since the vehicle can expose any alteration in the tuple by verifying the equation $\delta_{m_i} P = h_2(pid_{il}^1 || pid_{il}^2) P_{pub} + Y_i$. Therefore, the alteration probability of the signature for the message m_i is minimal. Therefore, the proposed scheme can withstand modification attacks in the VANET;
- Impersonation attacks. It is impossible for an attacker to forge a legitimate message signature tuple $\{pid_{in}, m_i, T, \sigma_i\}$ consistent with Theorem 1 because the recipient verifies the authenticity of the tuple $\{pid_{in}, m_i, T, \sigma_i\}$ by checking the equation $\delta_{m_i} P = h_2(pid_{il}^1 || pid_{il}^2) P_{pub} + Y_i$. The forged signature probability for message m_i is trivial. Therefore, the proposed scheme can resist impersonation attacks in the VANET;
- Man-In-The-Middle (MITM) attacks. In the proposed scheme, mutual authentication is executed among the nodes in the VANET. If an attacker tries an MITM attack, forged messages must link with the signer and the receiver. Nevertheless, consistent with Theorem 1, it is impossible for an attacker to launch this attack type. Therefore, the proposed scheme can resist MITM attacks in the VANET.

6.3. Security Comparison

We compared the performance of our scheme with other ID-based schemes. Table 2 presents the comparison results, where SC-1, SC-2, and SC-3 denote bilinear pair used, vulnerable to insider attacks, and RSU authentication, respectively.

As presented in Table 2, we know that none of them completely address all security issues such as bilinear pair used, vulnerability to an insider attack, and RSU authentication in their scheme. However, the proposed scheme addresses all security issues regarding identity-based schemes in VANETs.

Table 2. Comparison of the security issues .

	[17–24]	[25–29]	[30,31]	Proposed
SC-1	✓	✗	✗	✗
SC-2	✓	✓	✗	✗
SC-3	✗	✗	✓	✗

7. Performance Analysis and Comparison

This section presents the experiment and the comparative performance analysis of the proposed scheme and other schemes in terms of computation and communication costs.

7.1. Experimental

The simulation experiment of the proposed scheme includes two parts, namely network generation and road traffic generation. As shown in Figure 7, this paper used OMNeT++ [39], VEINS [40], MIRACL [41,42], OpenStreetMap [43], GatcomSUMO [44], and SUMO [45] to carry out the simulation experiments for VANETs. OMNeT++ is a modular, component-based C++ simulation library for communication networks. VEINS combines road traffic generation and network generation. MIRACL is a cryptographic library used to execute cryptography operations for algorithms. OpenStreetMap is the most prominent crowd-sourced web-based mapping platform. GatcomSUMO is a graphical application that simplifies VANET simulation, specifically the SUMO traffic and the OMNeT++ network

generation. SUMO is a highly portable, multi-model traffic simulation. Table 3 presents the simulation experiment parameters.

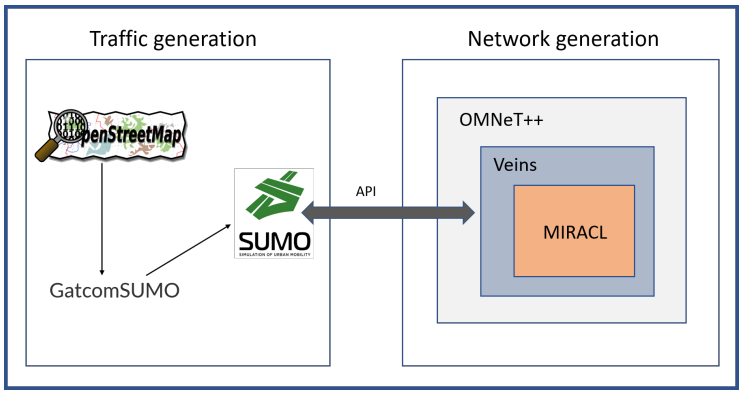

Figure 7. VANET simulation.

Table 3. Simulation experiment parameters.

Parameters	Value
Simulation time	200 s
Playground size	x = 3463 m, y = 4270 m and z = 50 m
Mac layer	IEEE 1609.4
Physical layer	IEEE 802.11p
Maximum transmission	20 mW
Bit rate	6 Mbps
Number of vehicles	500
Minimum speed	30 Km/H
Maximum speed	60 Km/H

For road traffic generation, each vehicle has some functional characteristics such as the minimum and maximum speed, dimension, and direction. These characteristics influence and restrict the mobility model.

In this work, the trip trajectory and mobility model were random, and the number of vehicles was constant. In the simulation experiment of the proposed scheme, the Security Processing Service (SPS) layer was added in each RSU and OBU on network simulators (VEINS/OMNeT++). The main reason behind the SPS layer used was to execute the process of signing and verifying messages that was higher than the MAC and physical layer and lower than the application layer, as shown in Figure 8. In the VANET communications, the data flow for sending and receiving messages during three layers, namely, the App, SPS, and NIC layers, is shown in Figure 9.

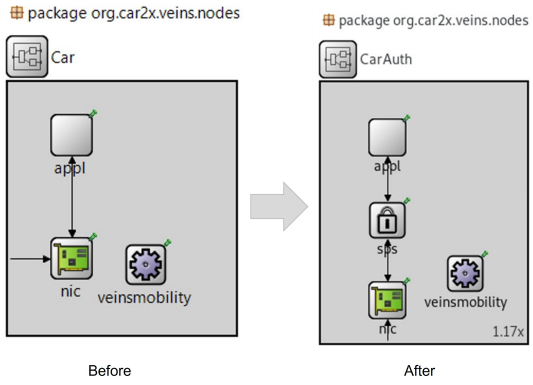

Figure 8. Signing and verifying messages in OMNeT++.

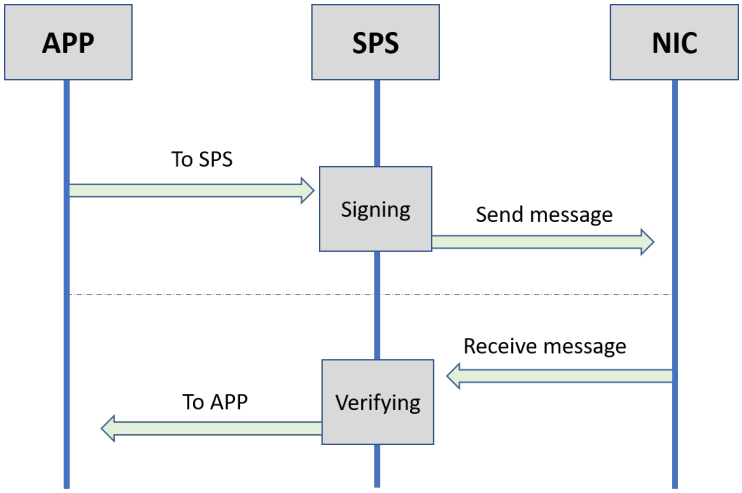

Figure 9. Data flow for sending and receiving messages.

7.2. Computation Cost Analysis and Comparison

This subsection evaluates and compares the computation costs between the proposed scheme and the existing schemes. The notations for the executing time and time cost are as follows:

- T_{bp} indicates the time needed to perform a bilinear pairing operation. Hence, the time cost of T_{bp} is 5.811 ms;
- $T_{b.a}$ indicates the time needed to perform the point addition operation for the bilinear pairing in G_1. Hence, the time cost of T_{b-a} is 0.0106 ms;
- $T_{b.sm}$ indicates the time needed to perform a small scalar multiplication operation for the bilinear pairing in G_1. Hence, the time cost of $T_{b.sm}$ is 0.1829 ms;
- $T_{b.m}$ indicates the time needed to perform a scalar multiplication operation for the bilinear pairing in G_1. Hence, the time cost of $T_{b.m}$ is 1.5654 ms;
- T_{mtp} indicates the time needed to perform a map-to-point function for the bilinear pairing in G_1. Hence, the time cost of T_{mtp} is 4.1724 ms;
- T_{e-m} indicates the time needed to perform a scalar multiplication operation for ECC in an additive group G. Hence, the time cost of T_{e-m} is 0.6718 ms;
- T_{e-a} indicates the time needed to perform a point addition operation for ECC in an additive group G. Hence, the time cost of T_{e-a} is 0.0031 ms;
- $T_{e.sm}$ indicates the time needed to perform a small scalar multiplication for ECC in G. Hence, the time cost of $T_{e.sm}$ is 0.0665 ms;
- T_h indicates the time required to perform a secure hash cryptography function. Hence, the time cost of T_h is 0.001 ms.

For easy measurement, let MSG, ISA, and BSA be the message signing generation, individual signature authentication, and batch signature authentication, respectively.

In He et al.'s scheme [25], three secure hash cryptography functions and three ECC-based scalar multiplication operations are needed during the MSG, resulting in a total cost of $3T_{e-m} + 3T_h \approx 2.0184$ ms. This scheme involved two point-addition operations, two secure hash cryptography functions, and three scalar multiplication operations for ISA, resulting in a total cost of $3T_{e-m} + 2T_{e-a} + 2T_h \approx 2.0236$ ms. During the BSA, $(2n)$ functions regarding secure hash cryptography, $(2n-1)$ operations regarding point addition, $(2n)$ operations regarding small scalar multiplication, and $(n+2)$ operations regarding scalar multiplication are needed in this scheme; thus, the whole cost is $(n+2)T_{e-m} + (2n)T_{e-sm} + (2n-1)T_{e-a} + (2n)T_h \approx 0.6718n + 1.3405$ ms. MSG includes a scalar multiplication and two secure hash cryptography functions in the proposed scheme, resulting in the whole cost being $1T_{e-m} + 2T_h \approx 0.6738$ ms. Meanwhile, ISA includes two scalar multiplication, one secure hash cryptography, and one point addition operation in the proposed scheme, resulting in the whole cost being $2T_{e-m} + 1T_h + 2T_{e-a} \approx 1.3477$ ms.

Finally, BSA includes two operations regarding scalar multiplication, $(2n)$ operations regarding small scalar multiplication, $(n+1)$ operations regarding point addition, and (n) functions regarding secure hash cryptography in the proposed scheme; thus, the whole cost is $2T_{e-m} + (2n)T_{e-sm} + (n+1)T_{e-a} + (n)T_h \approx 0.0737n + 1.3467$ ms. We also measured the computation cost of other schemes' MSG, ISA, and BSA using the same procedure, as tabulated in Table 4.

Table 4. The computation cost of the five authentication schemes.

Scheme	*MSG*	*ISA*	*BSA*
Jianhong et al. [24]	$6T_{b-m} + 2T_{b-a} + 1T_{mtp} + 4T_h \approx 13.59$	$3T_{bp} + 2T_{b-m} + 1T_{b-a} + 3T_h \approx 20.5774$	$3T_{bp} + (n+1)T_{b-m} + (2n)T_{b-sm} + (3n-2)T_{b-a} + (3n)T_h \approx 1.966n + 18.9772$
He et al. [25]	$3T_{e-m} + 3T_h \approx 2.0184$	$3T_{e-m} + 2T_{e-a} + 2T_h \approx 2.0236$	$(n+2)T_{e-m} + (2n)T_{e-sm} + (2n-1)T_{e-a} + (2n)T_h \approx 0.6718n + 1.3405$
Wu et al. [28]	$2T_{e-m} + 2T_h \approx 1.3456$	$4T_{e-m} + 2T_h + 2T_{e-a} \approx 2.6954$	$(2n+2)T_{e-m} + (2n)T_{e-sm} + (2n+2)T_{e-a} + (2n)T_h \approx 1.4786n + 1.3498$
Cui et al. [30]	$2T_{e-m} + 2T_h \approx 1.3456$	$3T_{e-m} + 7T_h + 1T_{e-a} \approx 2.0255$	$(n+2)T_{e-m} + (2n)T_{e-sm} + (n+1)T_{e-a} + (7n)T_h \approx 0.8149n + 1.3467$
Our scheme	$1T_{e-m} + 2T_h \approx 0.6738$	$2T_{e-m} + 1T_h + 1T_{e-a} \approx 1.3477$	$2T_{e-m} + (2n)T_{e-sm} + (n+1)T_{e-a} + (n)T_h \approx 0.0737n + 1.3467$

To satisfy the privacy requirements in terms of identity preserving and unlinkability, the scheme uses the elliptic curve operations. For example, the proposed scheme randomly selects unused pseudonym-IDs for signing a message from a pseudonym-ID list to avoid the adversary linking two or more messages sent from the same source, while the proposed scheme computes a new pseudonym-ID to sign each message. Thereby the computing cost will increase. For He et al.'s scheme [25], we can conclude $(1 - 0.0020184)/0.0020184 \approx 494.44$, $(1 - 0.0020236)/0.0020236 \approx 693.17$ and $(1 - (0.6718 \times 50 + 1.3405)/1000)/0.0349305 \approx 27.63$ that signed messages, individual signature authentication, and batch signature authentication in 1 s, respectively. For the proposed scheme, we can conclude $(1 - 0.0006738)/0.0006738 \approx 1483.12$, $(1 - 0.0013477)/0.0013477 \approx 741$ and $(1 - (0.0737 \times 50 + 1.3467)/1000)/0.0050317) \approx 198.46$ that signed messages, individual signature authentication, and batch signature authentication in 1 s, respectively. A similar method was used for the schemes for comparative purposes, and the result is shown in Figure 10.

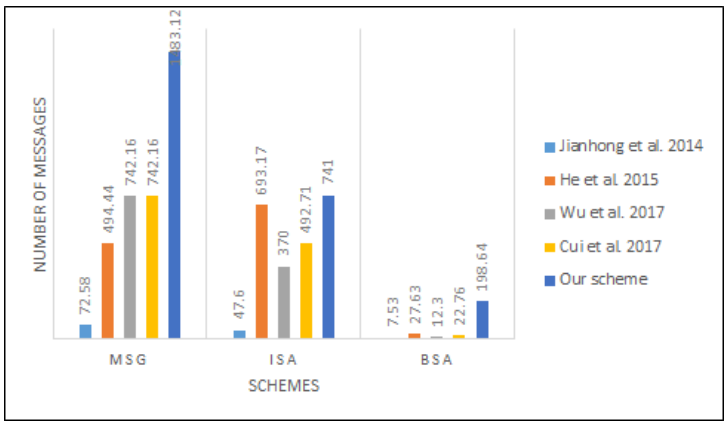

Figure 10. The computation cost's speed.

As presented in Table 4, the computation cost of the proposed scheme decreased by $(2.0184 - 0.6738)/2.0184 \approx 66.7\%$, $(2.0236 - 1.3477)/2.0236 \approx 33.4\%$ and $((0.6718 \times 50 + 1.3405) - (0.0737 \times 50 + 1.3467))/(0.6718 \times 50 + 1.3405) \approx 90.3\%$ for MSG, ISA, and BSA, respectively, compared to the He et al. scheme [25]. Table 5 presents the performance of the proposed scheme against the existing schemes for MSG, ISA, and BSA. The computational result shows that the elliptic curve used in the proposed scheme could handle the very fast pseudonym-changing process in signing and verifying messages in VANETs.

Table 5. Improvement of computation overhead comparison.

Scheme	*MSG*	*ISA*	*BSA* (50 Messages)
Jianhong et al. [24]	96.9%	94.5%	97.8%
He et al. [25]	66.7%	33.4%	90.3%
Wu et al. [28]	49.9%	50%	94.9%
Cui et al. [30]	49%	33.3%	90.2%

Hence, the total time was based on the execution time of each operation. The Elapsed Time (*ET*) between the exit and entrance to the SPS layer is the overhead cost.

$$ET = \frac{1}{M}\sum_{i=1}^{n} M(T_{out}^{i} - T_{in}^{i}) \quad (8)$$

where M is the number of messages and T_{out}^{i} and T_{in}^{i} are the exit and entrance times of message i, respectively. Figures 11 and 12 depict the average time to sign and verify the message between the proposed scheme and that of Cui et al. [30].

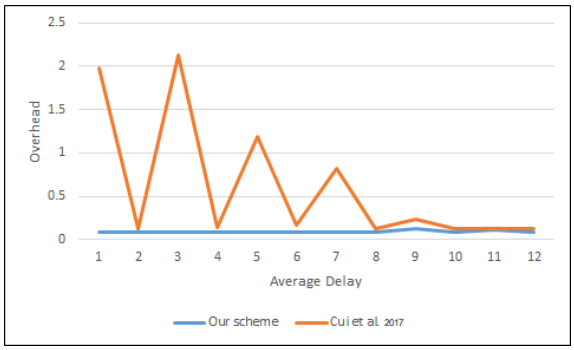

Figure 11. Average delay to a sign message in OMNeT++.

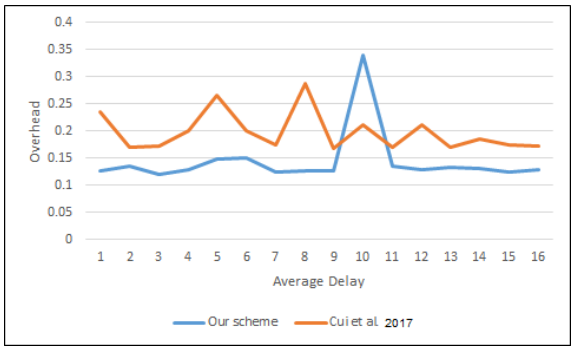

Figure 12. Average delay to verify a message in OMNeT++.

7.3. Communication Cost Analysis and Comparison

This subsection evaluates and compares the communication costs between the proposed scheme and the existing schemes. Based on the experiment by He et al. [25], let the sizes of the elements in G_1 and G be 128 bytes and 40 bytes, respectively. Besides, let the elements in Z_q^*, the size of the timestamp, and the output of a hash function be 20 bytes, 4 bytes, and 20 bytes, respectively.

In the scheme of He et al. [25], the format of the message signature tuple $<pid_{in}, m_i, T_i, R_i, \sigma_i>$, due to the pid_{il}^1, pid_{il}^2 and $\sigma_i \in Z_q^*$, $R_i \in G$ and one timestamp; thus, the full size is $40 \times 3 + 20 + 4 = 144$ bytes. In the proposed scheme, the vehicle sends the message signature tuple $\{pid_{in}, m_i, T, \sigma_i\}$ with size $40 + 20 \times 3 + 8 = 104$ bytes. The metrics for the other schemes were also measured using the same procedure. Table 6 lists the communication cost comparison of our scheme with the other schemes.

Table 6. Comparison of communication costs.

Schemes	Single Message (Bytes)	Batch Messages (Bytes)
Jianhong et al. [24]	388	388 n
He et al. [25]	144	144 n
Wu et al. [28]	148	148 n
Cui et al. [30]	84	84 n
Our scheme	104	104 n

8. Conclusions

This paper proposed a secure pseudonym-based conditional privacy-preservation authentication scheme to secure V2V and V2I communications in VANETs. The proposed scheme eliminates the dependency on RSU-only authentication by using many pseudo-IDs with corresponding signature keys from the TA, therefore allowing each vehicle to authenticate the received messages directly. The proposed scheme is resistant to insider attacks as the TA can revoke rogue vehicles' certificates, preventing them from continuously broadcasting fake messages. The security analysis proved that the proposed scheme under the random oracle model is secure, and it also satisfies the security and privacy requirements. Since the proposed approach uses ECC, its computation cost overhead is lower than other related bilinear pair-based approaches. Future work could include the analysis and performance measurement of the proposed approach in terms of latency, average delay, and throughput using network simulators, such as OMNeT++, and road traffic simulators, such as SUMO. Besides, the future work will also include the design of an authentication scheme based on fog computing that does not use ECC in 5G-enabled vehicular networks.

Author Contributions: Conceptualization, M.A.A.-S., M.A. and S.M.; methodology, M.A.A.-S., M.A. and S.M.; software, M.A.A.-S. and M.A.; validation, M.A.A.-S., M.A. and S.M.; formal analysis, M.A.A.-S., M.A. and S.M.; investigation, M.A.A.-S., M.A. and S.M.; resources, I.H.H.; data curation, M.A.A.-S., M.A. and S.M.; writing—original draft preparation, M.A.A.-S., M.A. and S.M.; writing—review and editing, M.A.A.-S., M.A. and S.M.; visualization, M.A.A.-S., M.A. and S.M.; supervision, M.A. and S.M.; project administration, M.A.A.-S.; funding acquisition, I.H.H. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Universiti Sains Malaysia (USM) External Grant Number 304/PNAV/650958/U154.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data sharing not applicable.

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

References

1. Zhang, J.; Cui, J.; Zhong, H.; Chen, Z.; Liu, L. PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad hoc networks. *IEEE Trans. Dependable Secur. Comput.* **2019**, *18*, 722–735. [CrossRef]
2. Alazzawi, M.A.; Chen, K.; Yassin, A.A.; Lu, H.; Abedi, F. Authentication and revocation scheme for VANETs based on Chinese remainder theorem. In Proceedings of the 2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Zhangjiajie, China, 10–12 August 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1541–1547.
3. Lloyd, D. Reported Road Casualties in Great Britain: Main Results 2015. 2016. Available online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/533293/rrcgb-main-results-2015.pdf (accessed on 19 January 2022).
4. Al-Shareeda, M.A.; Anbar, M.; Manickam, S.; Hasbullah, I.H. SE-CPPA: A Secure and Efficient Conditional Privacy-Preserving Authentication Scheme in Vehicular Ad-Hoc Networks. *Sensors* **2021**, *21*, 8206. [CrossRef]
5. Aung, N.; Zhang, W.; Dhelim, S.; Ai, Y. Accident prediction system based on hidden markov model for vehicular ad hoc network in urban environments. *Information* **2018**, *9*, 311. [CrossRef]

6. Cheng, H.; Liu, Y. An improved RSU-based authentication scheme for VANET. *J. Internet Technol.* **2020**, *21*, 1137–1150.
7. Kerrache, C.A.; Lakas, A.; Lagraa, N. Detection of intelligent malicious and selfish nodes in VANET using threshold adaptive control. In Proceedings of the 2016 5th International Conference on Electronic Devices, Systems and Applications (ICEDSA), Ras Al Khaimah, United Arab Emirates, 6–8 December 2016; pp. 1–4.
8. 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]
9. Muhammad, M.; Safdar, G.A. Survey on existing authentication issues for cellular-assisted V2X communication. *Veh. Commun.* **2018**, *12*, 50–65. [CrossRef]
10. Manvi, S.S.; Tangade, S. A survey on authentication schemes in VANETs for secured communication. *Veh. Commun.* **2017**, *9*, 19–30. [CrossRef]
11. Leaby, A.K.; Yassin, A.; Hasson, M.; Rashid, A. Towards design strong emergency and COVID-19 authentication scheme in VANET. *Indones. J. Electr. Eng. Comput. Sci.* **2021**, *21*, 1808–1819. [CrossRef]
12. Alazzawi, M.A.; Lu, H.; Yassin, A.A.; Chen, K. Robust conditional privacy-preserving authentication based on pseudonym root with cuckoo filter in vehicular ad hoc networks. *KSII Trans. Internet Inf. Syst. (TIIS)* **2019**, *13*, 6121–6144.
13. 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]
14. Raya, M.; Papadimitratos, P.; Hubaux, J.P. Securing vehicular communications. *IEEE Wirel. Commun.* **2006**, *13*, 8–15. [CrossRef]
15. Alazzawi, M.A.; Al-behadili, H.A.; Almalki, M.N.S.; Challoob, A.L.; Al-shareeda, M.A. ID-PPA: Robust Identity-Based Privacy-Preserving Authentication Scheme for a Vehicular Ad-Hoc Network. In Proceedings of the International Conference on Advances in Cyber Security, Penang, Malaysia, 8–9 December 2020; Springer: Berlin/Heidelberg, Germany, 2020; pp. 80–94.
16. 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.
17. 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.
18. Zhang, C.; Ho, P.H.; Tapolcai, J. On batch verification with group testing for vehicular communications. *Wirel. Netw.* **2011**, *17*, 1851. [CrossRef]
19. 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]
20. 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]
21. 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]
22. Lee, C.C.; Lai, Y.M. Toward a Secure Batch Verification with Group Testing for VANET. *Wirel. Netw.* **2013**, *19*, 1441–1449. [CrossRef]
23. 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]
24. 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.
25. 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]
26. Zhong, H.; Wen, J.; Cui, J.; Zhang, S. Efficient Conditional Privacy-preserving and Authentication Scheme for Secure Service Provision in VANET. *Tsinghua Sci. Technol.* **2016**, *21*, 620–629. [CrossRef]
27. 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]
28. Wu, L.; Fan, J.; Xie, Y.; Wang, J.; Liu, Q. Efficient location-based conditional privacy-preserving authentication scheme for vehicle ad hoc networks. *Int. J. Distrib. Sens. Netw.* **2017**, *13*, 1550147717700899. [CrossRef]
29. Xie, Y.; Wu, L.; Shen, J.; Alelaiwi, A. EIAS-CP: New efficient identity-based authentication scheme with conditional privacy-preserving for VANETs. *Telecommun. Syst.* **2017**, *65*, 229–240. [CrossRef]
30. Cui, J.; Zhang, J.; Zhong, H.; Xu, Y. SPACF: A secure privacy-preserving authentication scheme for VANET with cuckoo filter. *IEEE Trans. Veh. Technol.* **2017**, *66*, 10283–10295. [CrossRef]
31. Zhong, H.; Huang, B.; Cui, J.; Xu, Y.; Liu, L. Conditional privacy-preserving authentication using registration list in vehicular ad hoc networks. *IEEE Access* **2017**, *6*, 2241–2250. [CrossRef]
32. Al-Shareeda, M.A.; Anbar, M.; Manickam, S.; Hasbullah, I.H. Password-Guessing Attack-Aware Authentication Scheme Based on Chinese Remainder Theorem for 5G-Enabled Vehicular Networks. *Appl. Sci.* **2022**, *12*, 1383. [CrossRef]
33. Ahmad, F.; Adnane, A.; Franqueira, V.N.; Kurugollu, F.; Liu, L. Man-in-the-middle attacks in vehicular ad hoc networks: evaluating the impact of attackers' strategies. *Sensors* **2018**, *18*, 4040. [CrossRef]
34. 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] [PubMed]

35. Cui, J.; Wu, D.; Zhang, J.; Xu, Y.; Zhong, H. An efficient authentication scheme based on semi-trusted authority in VANETs. *IEEE Trans. Veh. Technol.* **2019**, *68*, 2972–2986. [CrossRef]
36. 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]
37. 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]
38. Li, J.; Choo, K.K.R.; Zhang, W.; Kumari, S.; Rodrigues, J.J.; Khan, M.K.; Hogrefe, D. EPA-CPPA: An efficient, provably-secure and anonymous conditional privacy-preserving authentication scheme for vehicular ad hoc networks. *Veh. Commun.* **2018**, *13*, 104–113. [CrossRef]
39. Varga, A. Discrete event simulation system. In Proceedings of the European Simulation Multiconference (ESM'2001), Prague, Czech Republic, 6–9 June 2001; pp. 1–7.
40. Sommer, C.; German, R.; Dressler, F. Bidirectionally coupled network and road traffic simulation for improved IVC analysis. *IEEE Trans. Mob. Comput.* **2010**, *10*, 3–15. [CrossRef]
41. Scott, M. MIRACL-A Multiprecision Integer and Rational Arithmetic C/C++ Library. 2003. Available online: http://www.shamus.ie (accessed on 19 January 2022).
42. Ltd, S.S. Multi Precision Integer and Rational Arithmetic Cryptographic Library (MIRACL). 2018. Available online: http://www.certivox.com/miracl/ (accessed on 19 January 2022).
43. Haklay, M.; Weber, P. Openstreetmap: User-generated street maps. *IEEE Pervasive Comput.* **2008**, *7*, 12–18. [CrossRef]
44. Abenza, P.P.G.; Malumbres, M.P.; Peral, P.P. 10 GatcomSUMO: A Graphical Tool for VANET Simulations Using SUMO and OMNeT+. In *SUMO 2017–Towards Simulation for Autonomous Mobility*; Deutsches Zentrum für Luft- und Raumfahrt e. V.: Cologne, Germany, 2017; p. 113.
45. Behrisch, M.; Bieker, L.; Erdmann, J.; Krajzewicz, D. SUMO–simulation of urban mobility: An overview. In Proceedings of the SIMUL 2011, The Third International Conference on Advances in System Simulation, ThinkMind, Barcelona, Spain, 23–28 October 2011.