










Article

Provably Secure with Efficient Data Sharing Scheme for Fifth-Generation (5G)-Enabled Vehicular Networks without Road-Side Unit (RSU)

Mahmood A. Al-Shareeda ¹, Selvakumar Manickam ^{1,*}, Badiea Abdulkarem Mohammed ², Zeyad Ghaleb Al-Mekhlafi ², Amjad Qtaish ², Abdullah J. Alzahrani ², Gharbi Alshammari ², Amer A. Sallam ³ and Khalil Almekhlafi ⁴

- ¹ National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia, Penang 11800, Malaysia
² College of Computer Science and Engineering, University of Ha'il, Ha'il 81481, Saudi Arabia
³ Engineering and Information Technology College, Taiz University, Taiz 6803, Yemen
⁴ CBA-Yanbu, Taibah University, Al Madinah 42353, Saudi Arabia
* Correspondence: selva@usm.my; Tel.: +604-653-3004

Abstract: The vehicles in the fifth-generation (5G)-enabled vehicular networks exchange the data about road conditions, since the message transmission rate and the downloading service rate have been considerably brighter. The data shared by vehicles are vulnerable to privacy and security issues. Notably, the existing schemes require expensive components, namely a road-side unit (RSU), to authenticate the messages for the joining process. To cope with these issues, this paper proposes a provably secure efficient data-sharing scheme without RSU for 5G-enabled vehicular networks. Our work included six phases, namely: TA initialization (TASetup) phase, pseudonym-identity generation (PIDGen) phase, key generation (KeyGen) phase, message signing (MsgSign) phase, single verification (SigVerify) phase, and batch signatures verification (BSigVerify) phase. The vehicle in our work has the ability to verify multiple signatures simultaneously. Our work not only achieves privacy and security requirements but also withstands various security attacks on the vehicular network. Ultimately, our work also evaluates favourable performance compared to other existing schemes with regards to costs of communication and computation.

Keywords: security and privacy; 5G-enabled vehicular networks; without RSU; data sharing scheme



Citation: Al-Shareeda, M.A.; Manickam, S.; Mohammed, B.A.; Al-Mekhlafi, Z.G.; Qtaish, A.; Alzahrani, A.J.; Alshammari, G.; Sallam, A.A.; Almekhlafi, K. Provably Secure with Efficient Data Sharing Scheme for Fifth-Generation (5G)-Enabled Vehicular Networks without Road-Side Unit (RSU). *Sustainability* **2022**, *14*, 9961. <https://doi.org/10.3390/su14169961>

Academic Editors: G G Md Nawaz Ali, Md. Noor-A-Rahim, Mohammad Omar Khyam, Xuejun Li, Lei Zhang and Manuel Fernandez-Veiga

Received: 21 May 2022

Accepted: 8 August 2022

Published: 11 August 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

With the continuous increasing demand for fifth-generation (5G) technology, research on the management of vehicle-to-everything (V2X) communication has emerged. Unlike the conventional vehicular networks, the V2X communication provides networks, things, users, and vehicles with reliable connectivity, manageable, operable, controllable, and high-quality [1–4].

The characteristics of 5G-enabled vehicular networks have a wide high bandwidth and coverage area. Based on data shared by 5G wireless, during peak periods, the data transmission rate can approach 20 Gb/s, while the average data transfer rate is over 100 Mb/s [5–8]. The capacity of the supported network is 1000 times that of conventional networks, and it can give a more steady connection [9–11].

Each vehicle in V2X communication is usually fitted with several expensive sensors, such as cameras of high-resolution, radars of microwave, and lidars of multi-beam, to get comprehensive and reliable data within urban or highway areas [12–17]. Moreover, each vehicle has installed wireless devices, namely onboard units (OBUs), to share large amounts of traffic-related information with others and connect technologies of heterogeneous wireless access during the outside world [18–20].

There are mainly two categories of data shared by vehicles in V2X communication [21,22]. One is calamities noticed by users, such as nearby hotel ratings

and parking lot occupancy. The other is that information is collected by sensors when the vehicle crosses the road environment, such as conditions of the poor road, congestion of traffic, and extreme weather. With these data shared, vehicles offer the driver and passenger a comfortable driving experience, satisfactory transport access, and a safe driving environment.

Given the fact the 5G-enabled vehicular network exploits wireless channels, the data shared by vehicles have security and privacy vulnerabilities [23]. The third-party has the ability to change, delete, and alter the data shared by the vehicle to cause damage to the road environment. Meanwhile, when an attacker exposes any personal data of the user (e.g., location or identity), it will cause criminal charges. Therefore, several scholars have focused on achieving security and privacy requirements for vehicular networks by proposing sophisticated data-sharing schemes.

Nevertheless, these schemes require expensive components called road-side units (RSUs) to cooperate in the mutual authentication phase, which raises the latency of the vehicular networks. Besides, studies [11,24] have proven that a compromised RSU causes leakage of secret information preserved in the RSU.

Hence, the main motivation of this paper is to reduce the massive overhead of performance system in terms of communication and computation costs by proposing a lightweight operations instead of bilinear pair and map-to-point function operations. Our proposed solution does not use RSU to authenticate the vehicle during mutual authentication process. Our proposed solution applies the 5G technology to the fast exchange of messages among vehicles. This work is carried out in our simulation experiments with regards to network simulator (OMNeT++) and traffic simulator (SUMO) to analyze the results. The major contributions of our work can be listed as follows:

- We retrospectively analyze the taxonomy of existing schemes for vehicular networks. Furthermore, some security vulnerabilities of these schemes are highlighted. Then, we present the vehicular network architecture with regard to the system model and security goals.
- We propose a provably secure with an efficient data-sharing scheme for 5G-enabled vehicular networks. To improve efficiency further, our work does not use an expansive component called RSU for the authentication process.
- We implement simulation experiments over a simulation platform (traffic generation simulator and network generation simulator), displaying that the performance efficiency of our work in terms of computation and communication costs has been enhanced compared with the existing works.

The remainder of our work is organized as follows: Section 2 reviews the taxonomy of the existing schemes. Section 3 introduces vehicular network architecture. The six algorithms of the proposed scheme are provided in Section 4. The security analysis and performance comparison of our work are presented in Sections 5 and 6, respectively. Section 7 shows the conclusions of our work.

2. Related Work

In this section, we retrospectively analyze some related work focusing on data-sharing among vehicles for vehicular networks. The taxonomy of existing schemes is as below. Additionally, we provide a critical analysis of the related work as well.

2.1. Massive Certificate-Based (MCB) Schemes

The fundamental concept of Massive Certificate-Based (MCB) schemes is that TA is responsible for issuing and preloading massive numbers of certificates (roughly 44,000) and their relevant pair-keys (private and public) to participating vehicles. These certificates are assigned based on level of the anonymity to archive security and privacy for vehicular networks.

Several scholars [25–33] have proposed MCB schemes for vehicular networks. However, there are three main drawbacks of the MCB schemes: (i) massive certificate

arrangement burden for TA owing to the huge pool of anonymous certificates and the relevant pair-keys are needed; (ii) storage arrangement burden owing to limit vehicle storage, and (iii) massive computation and communication overheads owing to the need to verify certification in the investigation methods.

2.2. Group Signature-Based (GSB) Schemes

Chaum and van Heyst [34] first proposed the fundamental concept of group signatures in 1991. The group members are permitted to sign information anonymously on behalf of all members.

Several scholars [35–39] have proposed GSB schemes to overcome the drawbacks arising MCB schemes in a vehicular network. However, there are two main drawbacks of the GSB schemes: (i) the massive size of the Certification revocation list (CRL) owing to the number of blocked vehicle's number is growing; and (ii) massive overheads of communication and computation owing to the two pairing-based operations that are needed.

2.3. Pseudonym Identity-Based (PIB) Schemes

To overcome the limitations concerning the two above (MCB and GSB) schemes, several scholars proposed Pseudonym Identity-Based (PIB) schemes to provide high-level security in vehicular networks.

In 2015, He et al. [40] first used elliptic curve cryptography rather than pairing-based cryptography to provide efficient performance and secure communications. In the scheme presented by He et al. [40], the private key of the system is saved on each vehicle. Nevertheless, if the vehicle is compromised by an adversary, the whole system is insecure. In 2017, Zhang et al. [41] designed a mutual authentication and preservation scheme to achieve distributed aggregate for the vehicular network. In the scheme designed by Zhang et al. [41], RSU is accountable for producing secret shares for vehicles within its communication area. In the same year, Azees et al. [42] designed an anonymous authentication by helping RSU to secure communication in vehicular networks. In 2018, Pournaghi et al. [43] combined the TPD of RSU and TPD of vehicles to achieve high-level security. In their scheme, the TA is saved with two private keys on the TPD of RSU. Therefore, RSU is responsible for temporarily computing the specific timestamp and generating the signature key of the vehicle. In 2019, Alazzawi et al. [44] designed a pseudonym-based system to achieve a robust integrity scheme. The scheme proposed by Alazzawi et al. [44] has not achieved likability requirements, since only one pseudonym identity is used within all travelling. Furthermore, the system's secret key is saved on the RSU without using the TPD, which makes it an easy task for the attacker to disclose the key. In the same year, Bayat et al. [45] designed a pseudonym-based to design a RSU-based authentication scheme. RSU is responsible for preloading a pool of signature keys and pseudonym-IDs to each vehicle.

Ali and Li [46] proposed an authentication data-sharing scheme by using RSU to authenticate a large number of messages for vehicle-to-infrastructure (V2I) communication. This scheme replaced map-to-point hash functions by general one-way hash functions to sign message and verify signature. Nevertheless, this scheme uses bilinear pair operations, which are considered time-consuming and complicated.

Al-Shareeda et al. [47] designed a data-sharing scheme by using bilinear pair cryptography and cryptographic hash function. This scheme applies RSU to generate a signature key for the corresponding pseudonym-ID for authentic vehicles. This scheme is vulnerable to a massive overhead of performance costs as it uses complicated operations and is time-consuming.

Alshudukhi et al. [48] applied elliptic curve cryptography to propose an authentication data-sharing scheme for vehicular network. The TA in this scheme saves the system's private key to each RSU. Once a vehicle wants to join the system, RSU computes and preloads security parameters to vehicles. However, since this scheme uses a large number of multiplication point operations based on ECC, the performance costs is challenged.

Ali et al. [49] constructed a hybrid signcryption based on and public key infrastructure and certificateless cryptosystem to provide security criteria in a single logical phase. This scheme uses bilinear pair operations to sign messages and verify signatures, which causes a massive overhead of performance system.

2.4. Critical Analysis

The summation of related work is as follows. The majority of existing schemes are based on three classes of approaches: (i) Massive certificate-based (MCB) schemes, (ii) Group signature-based (GSB) schemes, and (iii) Pseudonym identity-based (PIB) schemes. The first two approaches required high overhead costs to sign messages and verify signatures, which is not suitable for deployment in vehicular networks. In contrast, the third approach is called pseudonym identity-based (PIB) schemes, proposed by the researcher to address the overhead costs of the system. Our work is based on the third approach to address the existing scheme based on PIB schemes by applying 5G technology and avoiding using RSU.

Since the existing PIB schemes apply RSU to participate authentication process, if they make assumptions that no other things can discover the secrets in a TPD of a vehicle, if a vehicle is corrupted in one RSU, the third party can calculate the RSU's master key.

3. Vehicular Network Architecture

This section presents the vehicular network architecture with regard to the system model and security goals in our work for 5G-enabled vehicular networks.

3.1. System Model

As presented in Figure 1, the three main entities are called: trusted authority (TA), 5G-base station (5G-BS), and onboard unit (OBU) for 5G-enabled vehicular networks. The main work of these entities is explained in the following steps.

- **Trusted Authority (TA):** TA is trustworthy by all entities in the 5G-enabled vehicular networks and has sufficient resources with regards to storage, communication, and computation. The TA is also in charge of generating the initial parameters of the network and registering the vehicles.
- **5G-base Station (5G-BS):** is a radio receiver and has sufficient fast-moving and broad-spectrum in 5g-enabled vehicular networks. The main task of 5G-BS is to connect vehicles and TA. The 5G-BS does not save or compute the data regarding vehicular networks.
- **Onboard Unit (OBU):** Each enrolled vehicle has one onboard unit (OBU) for sending and receiving information about the surrounding environment. Each OBU has TPD to preserve sensitive data and do computation processes for cryptographic operations. OBU is considered as a terminal node in networks which enjoys all types of services for 5G technology. Therefore, this work adds a security algorithm in a secure processing service (SPS) layer in each node for the simulation, as shown in Figure 2. The main reason behind using the SPS layer is to implement an authentication process that is higher than the MAC and physical layer.

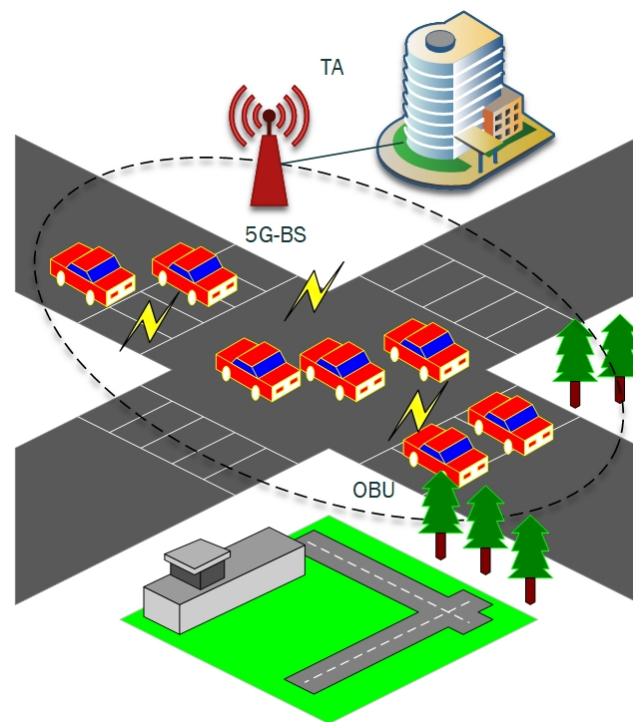


Figure 1. The System Model of 5G-enabled Vehicular Networks.

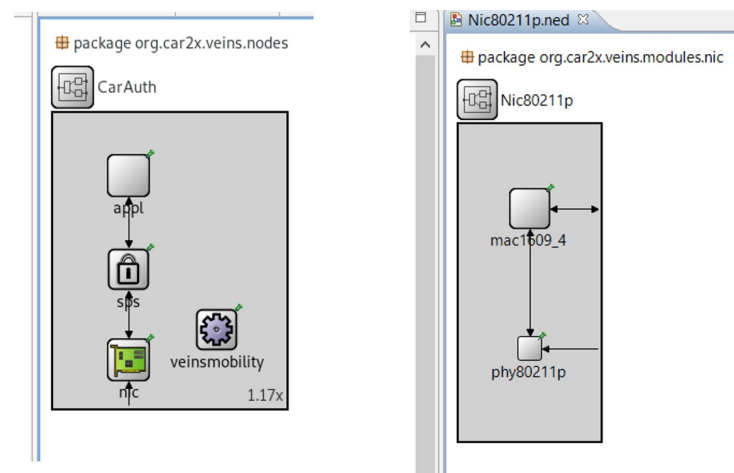


Figure 2. Authentication Node Layers in OMNeT++.

Device-to-Device (D2D) Communication

The D2D wireless network in 5G technology is determined as direct communication among vehicles (terminal nodes) without passing via infrastructure node. In a traditional network, all data must go through the infrastructure node called the base station, even if it is inside the range of D2D communication. As a result, D2D communication can considerably increase the network's spectral efficiency in this instance.

3.2. Security Goals

In this section, the security requirements should be achieved in our work.

- **Authentication and Integrity:** To make sure that the message transmitted has been carried out by a registered vehicle. Besides, the message has not been tampered with.
- **Privacy Preserving:** The original identity of the message broadcasting vehicle must be protected and the message should not disclose the identity to other units so that an attacker cannot utilize their identity for themselves.

- Traceability: When issuing a forged message, the vehicle has the traceable to its signer and that power must lie with the TA.
- Replaying Resistance: Our work should be capable of resisting replay attackers to avoid repeating the message sent by the registered vehicle.

4. Proposed Scheme

To address limitations in the existing schemes, this paper proposes a provably secure efficient data-sharing scheme for 5G-enabled vehicular networks. Our work has six phases, namely: TA initialization (TAS_{Setup}) phase, pseudonym-ID generation (PID_{Gen}) phase and key generation (Key_{Gen}) phase, message signing (Msg_{Sign}) phase, single verification (Sig_{Verify}) phase, and batch signatures verification (BSig_{Verify}) phase.

Our work is based on the scheme proposed by [50]. However, unlike the scheme proposed by [50], the proposed scheme uses 5G-BS to provide high-efficiency data-sharing among vehicles. This paper carried out the simulation experiments with regard to network simulators and traffic simulators (SUMO) to analyze the results of these phases. Furthermore, the proposed scheme does not need an expensive component (RSU) to authenticate the messages. Vehicles in our work can renew the security groups by sending a request to TA through 5G-BS wirelessly, which avoids repeat parameters used. The proposed scheme should be divided into the following phases:

- **TAS_{Setup}:** The TA executes TAS_{Setup} phase to obtain security parameter η . The network parameters Y and the private (secret) keys α and β are returned on this algorithm. The system parameters Y are considered as an implicit input to all methods explained below.
- **PID_{Gen} and Key_{Gen}:** The TA executes the PID_{Gen} and Key_{Gen} algorithms to return the pseudonym-ID PID_i and the signature key SK_i , respectively.
- **Msg_{Sign}:** The registered vehicle V_i executes Msg_{Sign} algorithm. The safety-related message M_i for a pseudonym-ID PID_i is taken as input for returning the signature δ_i .
- **Sig_{Verify}:** The verifying vehicle V_j executes Sig_{Verify} algorithm. Once receiving a signature δ_i on a safety-related message M_i for a pseudonym-ID PID_i from a vehicle V_i , if the signature δ_i is legitimate, it results true; otherwise, it outputs false.
- **BSig_{Verify}:** The verifying vehicle V_j executes Sig_{Verify} algorithm. Once receiving a batch of n signature $(\delta_1, \delta_2, \dots, \delta_n)$ on n safety-related messages (M_1, M_2, \dots, M_n) for n pseudonym-IDs $(PID_1, PID_2, \dots, PID_n)$ from n vehicles (V_1, V_2, \dots, V_n) simultaneously, if the signatures $(\delta_1, \delta_2, \dots, \delta_n)$ are legitimate, it results true; otherwise, it results false.

4.1. TAS_{Setup}

The TA executes the TAS_{Setup} algorithm to return the network parameters Y and the private (secret) keys α and β as the following steps.

- Given a network parameter $\eta \in Z^+$, TA selects a generator g based on a group G of the order prime q .
- Four cryptographic general hash functions, H_1, H_2, H_3 and H_4 , are chosen by TA and set as $H_1 : G \times G \rightarrow Z_q^*$, $H_2 : [0, 1]^* \rightarrow Z_q^*$, $H_3 : [0, 1]^* \times [0, 1]^* \times G \times G \times [0, 1]^* \rightarrow Z_q^*$ and $H_4 : G \rightarrow Z_q^*$.
- TA sets the randomly picked number $\alpha \in Z_q^*$ as a private (secret) key, then measures its corresponding public key $\zeta_{Pub-\alpha} = g^\alpha$ for private key extraction.
- TA sets the randomly picked number $\beta \in Z_q^*$ as a private (secret) key, then measures its corresponding public key $\zeta_{Pub-\beta} = g^\beta$ for traceability.
- The network public parameters are set as $Y = \{g, G, q, H_1, H_2, H_3, H_4, \zeta_{Pub-\alpha}, \zeta_{Pub-\beta}\}$. Note that private (secret) keys α and β are only known to TA.

Since our work is based on 5G technology, it is an easy task to renew the groups to avoid repeating them during the next steps. The renew process executes between vehicle and TA through 5G-BS.

4.2. PIDGen and KeyGen

To achieve mutual authentication and privacy-preservation in our work, the pseudonym-IDs (PIDs) that are particularly concerned with the relevant original identities OIDs should be used by following these steps:

- User submits the original identity OID of his/her vehicle to TA via secure communication. TA is responsible for testing the validity of OID .
- Once confirmed the authenticity of OID , TA sets a group of the randomly selected values $\{\omega_{i,1}, \omega_{i,2}, \dots, \omega_{i,n}\} \in Z_q^*$ as a private key and then measures the relevant public keys $PK_i^* = \{PK_{i,1}, PK_{i,2}, \dots, PK_{i,n}\}$, where $PK_{i,l} = g^{\omega_{i,l}}$ and $l \in \{1, 2, \dots, n\}$.
- TA then computes a group of PIDs for vehicle V_i as $PID_i^* = \{PID_{i,1}, PID_{i,2}, \dots, PID_{i,n}\}$, where $PID_{i,l} = OID_i \oplus H_1(PK_{i,l}^\beta, \zeta_{Pub-\beta})$ and $l \in \{1, 2, \dots, n\}$.
- Once calculating the PID_i^* , TA sets randomly selected values $SK_i^* = \{SK_{i,1}, SK_{i,2}, \dots, SK_{i,n}\}$ as a signature keys, where $SK_{i,l} = \alpha \cdot H_2(PID_{i,l})$ and $l \in \{1, 2, \dots, n\}$.
- Ultimately, TA preloads the network parameters Y and groups $\{PK_i^*, PID_i^*, SK_i^*\}$ to TPD of vehicle V_i through a secure channel.

4.3. MsgSign

Prior to sending the safety-related messages to public channel in 5G-enabled vehicular network, vehicle V_i signs them to achieve integrity and authentication. The message-signature tuples on one message $M_i \in [0, 1]^*$ by participating vehicle V_i is demonstrated as the following steps.

- Vehicle V_i sets the randomly selected a signature key $SK_{i,l}$, a relevant $PK_{i,l}$ and pseudonym-ID $PID_{i,l}$ from the groups PK_i^* , PID_i^* , and SK_i^* , respectively.
- Vehicle V_i sets the randomly picked value $d_i \in Z_q^*$ and calculates $D_i = g^{d_i}$.
- Vehicle V_i signs message $M_i \in [0, 1]^*$ as $\Theta_i = H_3(M_i, D_i, T_i, PID_{i,l}, PK_{i,l})$, where T_i is a freshness timestamp.
- Vehicle V_i computes signature $\delta_i = (H_4(D_i) - SK_{i,l} \cdot \Theta_i) \cdot d_i^{-1}$.
- Finally, vehicle V_i broadcasts the message-signature tuples $\{M_i, PK_{i,l}, PID_{i,l}, D_i, T_i, \delta_i\}$ to others in 5G-enabled vehicular networks.

4.4. SigVerify

Once the verifying vehicle V_j has acquired a single tuple signed by V_i , the following steps should be executed.

- Upon receiving the message-signature tuples $\{M_i, PK_{i,l}, PID_{i,l}, D_i, T_i, \delta_i\}$, the verifying vehicle V_j tests the brightness of timestamp T_i . Verifying vehicle V_j rejects the message if it is not valid.
- If T_i is fresh, verifying vehicle V_j then calculates $H_2(PID_{i,l})$ and $\Theta_i = H_3(M_i, D_i, T_i, PID_{i,l}, PK_{i,l})$.
- Finally, verifying vehicle V_j checks whether Equation (1) holds or not.

$$D_i^{\delta_i} \cdot \zeta_{Pub-\alpha}^{H_2(PID_{i,l}) \cdot \Theta_i} \stackrel{?}{=} g^{H_4(D_i)} \quad (1)$$

If Equation (1) is achieved, then the verifying vehicle V_j accepts the message M_i ; otherwise, the V_j rejects it. The correctness of the SigVerify's Equation is explained as follows:

$$\begin{aligned}
& D_i^{\delta_i} \cdot \zeta_{Pub-\alpha}^{H_2(PID_{i,l}) \cdot \Theta_i} \\
&= (g^{d_i})^{(H_4(D_i) - SK_{i,l} \cdot \Theta_i) \cdot d_i^{-1}} \cdot (g^\alpha)^{H_2(PID_{i,l}) \cdot \Theta_i} \\
&= g^{d_i \cdot (H_4(D_i) - \alpha \cdot H_2(PID_{i,l}) \cdot \Theta_i) \cdot d_i^{-1}} \cdot g^{\alpha \cdot H_2(PID_{i,l}) \cdot \Theta_i} \\
&= g^{d_i \cdot d_i^{-1} \cdot H_4(D_i) - \alpha \cdot H_2(PID_{i,l}) \cdot \Theta_i} \cdot g^{\alpha \cdot H_2(PID_{i,l}) \cdot \Theta_i} \\
&= g^{H_4(D_i) - \alpha \cdot H_2(PID_{i,l}) \cdot \Theta_i} \cdot g^{\alpha \cdot H_2(PID_{i,l}) \cdot \Theta_i} \\
&= g^{H_4(D_i) - \alpha \cdot H_2(PID_{i,l}) \cdot \Theta_i + \alpha \cdot H_2(PID_{i,l}) \cdot \Theta_i} \\
&= g^{H_4(D_i)}
\end{aligned}$$

4.5. BSigVerify

Upon receiving n message-signature tuples $\{M_i^1, PID_{i,l}^1, PK_{i,l}^1, D_i^1, T_i^1, \delta_i^1\}$, $\{M_i^2, PID_{i,l}^2, PK_{i,l}^2, D_i^2, T_i^2, \delta_i^2\}, \dots, \{M_i^n, PID_{i,l}^n, PK_{i,l}^n, D_i^n, T_i^n, \delta_i^n\}$ simultaneously. Verifying vehicle V_j uses the system public parameters $Y = \{g, G, q, H_1, H_2, H_3, H_4, \zeta_{Pub-\alpha}, \zeta_{Pub-\beta}\}$ to verify batch messages as the following steps.

- Verifying vehicle V_j tests the validity of $\{T_1, T_2 \dots T_n\}$, and drops the messages if some of them are not valid.
- Verifying vehicle V_j sets the randomly selected n values $\{\gamma_1, \gamma_2 \dots \gamma_n\}$, where $\gamma_i \in R[1, 2^m]$ for $m = 80$ and $i = 1, 2 \dots, n$ is typically acceptable [51].
- Verifying vehicle V_j then calculates $H_2(PID_{i,l})$ and $\Theta_i = H_3(M_i, D_i, T_i, PID_{i,l}, PK_{i,l})$, where $i = 1, 2 \dots, n$.
- Finally, verifying vehicle V_j checks whether Equation (2) holds or not.

$$g^{\sum_{i=1}^n (\gamma_i \cdot H_4(D_i))} \stackrel{?}{=} \sum_{i=1}^n D_i^{\gamma_i \cdot \delta_i} \cdot \zeta_{Pub-\alpha}^{\gamma_i \cdot H_2(PID_{i,l}) \cdot \Theta_i} \quad (2)$$

If Equation (2) is achieved, then the verifying vehicle V_j accepts the messages; otherwise, the V_j discards them. The correctness of the BSigVerify's Equation is explained as follows:

$$\begin{aligned}
& \sum_{i=1}^n D_i^{\gamma_i \cdot \delta_i} \cdot \zeta_{Pub-\alpha}^{\gamma_i \cdot H_2(PID_{i,l}) \cdot \Theta_i} \\
&= \sum_{i=1}^n (g^{\gamma_i \cdot d_i})^{(H_4(D_i) - SK_{i,l} \cdot \Theta_i) \cdot d_i^{-1}} \cdot (g^{\gamma_i \cdot \alpha})^{H_2(PID_{i,l}) \cdot \Theta_i} \\
&= \sum_{i=1}^n g^{\gamma_i \cdot d_i \cdot (H_4(D_i) - \alpha \cdot H_2(PID_{i,l}) \cdot \Theta_i) \cdot d_i^{-1}} \cdot g^{\gamma_i \cdot \alpha \cdot H_2(PID_{i,l}) \cdot \Theta_i} \\
&= \sum_{i=1}^n g^{\gamma_i \cdot d_i \cdot d_i^{-1} \cdot H_4(D_i) - \alpha \cdot H_2(PID_{i,l}) \cdot \Theta_i} \cdot g^{\gamma_i \cdot \alpha \cdot H_2(PID_{i,l}) \cdot \Theta_i} \\
&= \sum_{i=1}^n g^{\gamma_i \cdot H_4(D_i) - \alpha \cdot H_2(PID_{i,l}) \cdot \Theta_i} \cdot g^{\gamma_i \cdot \alpha \cdot H_2(PID_{i,l}) \cdot \Theta_i} \\
&= \sum_{i=1}^n g^{\gamma_i \cdot H_4(D_i) - \alpha \cdot H_2(PID_{i,l}) \cdot \Theta_i + \gamma_i \cdot \alpha \cdot H_2(PID_{i,l}) \cdot \Theta_i} \\
&= g^{\sum_{i=1}^n \gamma_i \cdot H_4(D_i)}
\end{aligned}$$

5. Security Analysis

In this section, the security definition, provable security, and security level of our work are analyzed in the following subsections.

5.1. Security Definition

The security model for the proposed scheme is provided by a game activated between a polynomial-time adversary \mathcal{A} and a challenger \mathcal{I} . In the model, adversary \mathcal{A} can access polynomially bounded queries oracle adaptively to challenger \mathcal{I} as the following steps.

Setup: In this process, a TSetup algorithm of the 5G-enabled vehicular networks is simulated. \mathcal{I} runs the TSetup algorithm to compute the network parameters Y and the private (secret) keys α and β . Once receiving this query, \mathcal{I} sends Y to \mathcal{A} .

$H_{i=1,2,3,4}$: When sending the information query IQ , \mathcal{I} sets the randomly selected number $\theta_i \in Z_q^*$ and saves (IQ, θ_i) in the list \mathcal{L}_i . Then, \mathcal{I} returns θ_i to \mathcal{A} .

GenerateVeh: When receiving the original identity OID_i of vehicle V_i , \mathcal{I} computes pseudonym-IDs PID_i^* and signature keys SK_i^* of vehicle V_i . Then \mathcal{I} saves $\{OID_i, PID_i^*, SK_i^*\}$ in the list \mathcal{L}_{veh} .

CorruptVeh: When receiving the original identity OID_i of vehicle V_i , \mathcal{I} sends pseudonym-IDs PID_i^* and signature keys SK_i^* of vehicle V_i to \mathcal{A} .

SignatureGen: When submitting pseudonym-ID PID_i and message M by \mathcal{A} , \mathcal{I} produces and returns the relevant the message-signature tuples to \mathcal{A} .

Upon performing the above queries, \mathcal{A} forges the signature δ_i^* of safety-related message M_i^* related with original identity OID_i^* of vehicle V_i^* .

Forgery: When the below steps are achieved, \mathcal{A} wins the game.

- δ_i^* is a legal signature of the message M^- .
- \mathcal{A} signature of M^- has not been queried in the **CorruptVeh** and **SignatureGen**.

Let the function $Adv_{\Omega, \mathcal{A}}^{Scheme}$ indicate the advantage of \mathcal{A} in breaking the proposed scheme Ω .

Definition 1. The proposed scheme Ω for 5G-enabled vehicular networks is chosen-message and chosen-identity secure, when the function $Adv_{\Omega, \mathcal{A}}^{Scheme}$ is negligible for \mathcal{A} .

5.2. Provable Security

According to Definition 1, the selected message and chosen identity of our work utilizing the random oracle model (ROM) are analyzed. Figure 3 shows a game between a challenger \mathcal{I} and an attacker \mathcal{A} .

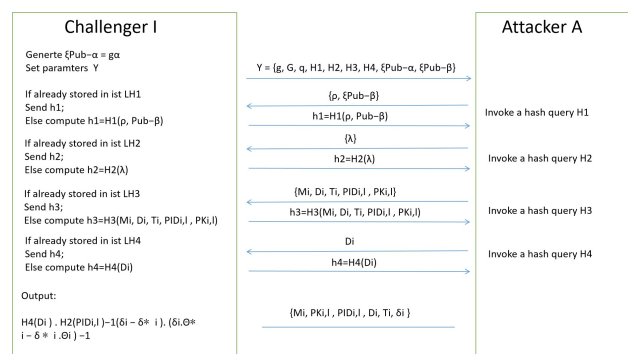


Figure 3. A game between a challenger \mathcal{I} and an attacker \mathcal{A} .

Theorem 1. Supposing that the underlying DLP is unsolvable, the proposed scheme for 5G-enabled vehicular networks is secure in the ROM.

Proof. Suppose that an attacker of polynomial-time \mathcal{A} can forge a legal the message-signature tuples $\{M_i, PK_{i,l}, PID_{i,l}, D_i, T_i, \delta_i\}$ by an advantage of non-negligible $Adv_{\Omega, \mathcal{A}}^{Scheme}$,

then challenger \mathcal{I} could resolve DLP with advantage of non-negligible via working the \mathcal{A} as a subroutine. Consider $\xi_{Pub-\alpha} = g^\alpha$ be an example of the DLP, and main work of the \mathcal{A} is to calculate α . Initially, \mathcal{I} produces $Y = \{g, G, q, H_1, H_2, H_3, H_4, \xi_{Pub-\alpha}, \xi_{Pub-\beta}\}$ to \mathcal{A} . Then \mathcal{A} runs oracle-queries adaptively modeled by \mathcal{I} as the following steps. \square

Oracle(H_1) : \mathcal{I} initializes the form of $\{q, \xi_{Pub-\beta}, \mu_1\}$ in the list \mathcal{L}_{H_1} firstly. Once a query $\{q, \xi_{Pub-\beta}\}$ is issued by \mathcal{A} , \mathcal{I} tests whether the form of $\{q, \xi_{Pub-\beta}, \mu_1\}$ existing in the list \mathcal{L}_{H_1} . If exists, \mathcal{I} produces $\mu_1 = H_1(q, \xi_{Pub-\beta})$ to \mathcal{A} , otherwise, \mathcal{I} sets the randomly selected nonce $\mu_1 \in Z_q^*$, produces to $\mu_1 = H_1(q, \xi_{Pub-\beta})$ to \mathcal{A} and puts $\{q, \xi_{Pub-\beta}, \mu_1\}$ to the list \mathcal{L}_{H_1} .

Oracle(H_2) : \mathcal{I} initializes the form of $\{\lambda, \mu_2\}$ in the list \mathcal{L}_{H_2} firstly. Once a query $\{\lambda\}$ is issued by \mathcal{A} , \mathcal{I} tests whether the form of $\{\lambda, \mu_2\}$ existing in the list \mathcal{L}_{H_2} . If exists, \mathcal{I} produces $\mu_2 = H_2(\lambda)$ to \mathcal{A} , otherwise, \mathcal{I} sets the randomly selected nonce $\mu_2 \in Z_q^*$, produces to $\mu_2 = H_2(\lambda)$ to \mathcal{A} and puts $\{\lambda, \mu_2\}$ to the list \mathcal{L}_{H_2} .

Oracle(H_3) : \mathcal{I} initializes the form of $\{M_i, D_i, T_i, PID_{i,l}, PK_{i,l}, \mu_3\}$ in the list \mathcal{L}_{H_3} firstly. Once a query $\{M_i, D_i, T_i, PID_{i,l}, PK_{i,l}\}$ is issued by \mathcal{A} , \mathcal{I} tests whether the form of $\{M_i, D_i, T_i, PID_{i,l}, PK_{i,l}, \mu_3\}$ existing in the pool \mathcal{L}_{H_2} . If exists, \mathcal{I} produces $\mu_3 = H_3(M_i, D_i, T_i, PID_{i,l}, PK_{i,l})$ to \mathcal{A} , otherwise, \mathcal{I} sets the randomly selected nonce $\mu_3 \in Z_q^*$, produces to $\mu_3 = H_3(M_i, D_i, T_i, PID_{i,l}, PK_{i,l})$ to \mathcal{A} and puts $\{M_i, D_i, T_i, PID_{i,l}, PK_{i,l}, \mu_3\}$ to the list \mathcal{L}_{H_3} .

Oracle(H_4) : \mathcal{I} initializes the form of $\{D_i, \mu_4\}$ in the list \mathcal{L}_{H_4} firstly. Once a query $\{D_i\}$ is issued by \mathcal{A} , \mathcal{I} tests whether the form of $\{D_i, \mu_4\}$ existing in the list \mathcal{L}_{H_4} . If exists, \mathcal{I} produces $\mu_4 = H_4(D_i)$ to \mathcal{A} , otherwise, \mathcal{I} sets the randomly selected nonce $\mu_4 \in Z_q^*$, produces to $\mu_4 = H_4(D_i)$ to \mathcal{A} and puts $\{D_i, \mu_4\}$ to the list \mathcal{L}_{H_4} .

Oracle(GenerateVeh): \mathcal{I} initializes the form of $\{OID_i, \eta, SK_i, PID_i, PK_i\}$ in the list \mathcal{L}_{veh} firstly. Once sending a query $\{OID_i, \eta, SK_i, PID_i, PK_i\}$ to by \mathcal{I} , \mathcal{A} tests whether the form of $\{OID_i, \eta, SK_i, PID_i, PK_i\}$ existing in the pool \mathcal{L}_{veh} . If exists, \mathcal{I} results PK_i to \mathcal{A} , otherwise, \mathcal{I} runs the following two points.

- If $OID_i = OID_i^*$, \mathcal{I} sets the randomly selected three values η_i, μ_1 and μ_2 , calculates $PK_i = g^{\eta_i}$ and holds $\{SK_i, PID_i\}$. \mathcal{I} saves $\{OID_i, \eta, SK_i, PID_i, PK_i\}$, $\{q, \xi_{Pub-\beta}, \mu_1\}$ and $\{\lambda, \mu_2\}$ in the list \mathcal{L}_{veh} , \mathcal{L}_{H_1} and \mathcal{L}_{H_2} respectively. Finally, \mathcal{I} returns PK_i to \mathcal{A} .
- If $OID_i \neq OID_i^*$, \mathcal{I} sets the randomly selected three values η_i, μ_1 and μ_2 , calculates $PK_i = g^{\eta_i}$, $PID_i = OID_i \oplus \mu_1$ and $SK_i = \alpha \cdot \mu_2$. \mathcal{I} saves $\{OID_i, \eta, SK_i, PID_i, PK_i\}$, $\{q, \xi_{Pub-\beta}, \mu_1\}$ and $\{\lambda, \mu_2\}$ in the list \mathcal{L}_{veh} , \mathcal{L}_{H_1} and \mathcal{L}_{H_2} respectively. Ultimately, \mathcal{I} results PK_i to \mathcal{A} .

Oracle(CorruptVeh): \mathcal{I} invokes $\{OID_i, \eta, SK_i, PID_i, PK_i\}$ from \mathcal{L}_{veh} and produces $\{SK_i, PID_i\}$ to \mathcal{A} .

Oracle(SignatureGen): When receiving a query with pseudonym-ID PID_i and message M_i from \mathcal{A} , \mathcal{I} sets the randomly selected three values d_i, μ_3 and μ_4 and calculates $D_i = g^{d_i}$, $\delta_i = (H_4(D_i) - SK_{i,l} \cdot \Theta_i) \cdot d_i^{-1}$. \mathcal{I} saves $\{M_i, D_i, T_i, PID_{i,l}, PK_{i,l}, \mu_3\}$ and $\{D_i, \mu_4\}$ in the list \mathcal{L}_{H_3} and \mathcal{L}_{H_4} , respectively. Finally, \mathcal{I} returns the message-signature tuples $\{M_i, PK_{i,l}, PID_{i,l}, D_i, T_i, \delta_i\}$ to \mathcal{A} .

At last, \mathcal{A} outputs the message-signature tuples $\{M_i, PK_{i,l}, PID_{i,l}, D_i, T_i, \delta_i\}$ to \mathcal{I} . If $PID_i \neq PID_i^*$, then \mathcal{I} ends the game. \mathcal{I} verifies whether Equation (3) holds.

$$D_i^{\delta_i} \cdot \xi_{Pub-\alpha}^{H_2(PID_{i,l}) \cdot \Theta_i} \stackrel{?}{=} g^{H_4(D_i)} \quad (3)$$

When it is wrong, then \mathcal{I} breaks the game by using forking lemma in [52]. When the \mathcal{I} attempts the process with a various chosen H_2 , then \mathcal{A} can result in another valid message-signature tuple $\{M_i, PID_{i,l}, PK_{i,l}, D_i, T_i, \delta_i^*\}$ with the advantage $Adv_{\Omega, \mathcal{A}}^{Scheme} \geq \frac{1}{9}$. Therefore, it obtains the following equation.

$$D_i^{\delta_i^*} \cdot \xi_{Pub-\alpha}^{H_2(PID_{i,l}) \cdot \Theta_i^*} \stackrel{?}{=} g^{H_4(D_i)} \quad (4)$$

Based on Equations (3) and (4), it can be concluded as follows.

$$D_i^{\delta_i - \delta_i^*} \stackrel{?}{=} \zeta_{Pub-\alpha}^{H_2(PID_{i,l}) \cdot (\Theta_i - \Theta_i^*)} \quad (5)$$

$$D_i^{\delta_i \cdot \Theta_i^* - \delta_i^* \cdot \Theta_i} \stackrel{?}{=} g^{H_4(D_i) \cdot (\Theta_i^* - \Theta_i)} \quad (6)$$

Thus, according to the above two equations, it can be respectively concluded as follows.

$$\bullet \quad D_i^{\delta_i - \delta_i^*} \stackrel{?}{=} g^{H_4(D_i) \cdot (\Theta_i^* - \Theta_i)}, \quad (g)^{d_i \cdot (\delta_i - \delta_i^*)} \stackrel{?}{=} (g)^{x \cdot H_2(PID_{i,l}) \cdot (\Theta_i^* - \Theta_i)}$$

$$d_i \cdot \delta_i - \delta_i^* \stackrel{?}{=} \alpha \cdot H_2(PID_{i,l}) \cdot (\Theta_i^* - \Theta_i) \quad (7)$$

$$\bullet \quad D_i^{\delta_i \cdot \Theta_i^* - \delta_i^* \cdot \Theta_i} \stackrel{?}{=} g^{H_4(D_i) \cdot (\Theta_i^* - \Theta_i)}, \quad g^{d_i \cdot (\delta_i \cdot \Theta_i^* - \delta_i^* \cdot \Theta_i)} \stackrel{?}{=} g^{H_4(D_i) \cdot (\Theta_i^* - \Theta_i)}$$

$$d_i \cdot (\delta_i \cdot \Theta_i^* - \delta_i^* \cdot \Theta_i) \stackrel{?}{=} H_4(D_i) \cdot (\Theta_i^* - \Theta_i) \quad (8)$$

Based on the above two equations, \mathcal{I} results $H_4(D_i) \cdot H_2(PID_{i,l})^{-1} (\delta_i - \delta_i^*) \cdot (\delta_i \cdot \Theta_i^* - \delta_i^* \cdot \Theta_i)^{-1}$ as the output of the DLP. The following events to resolve the DLP by \mathcal{I} are analyzed.

- EV_{pid} indicates the event that $PID_i^* = PID_i$.
- $EV_{fabricate}$ indicates the event that \mathcal{I} can fabricate two legal signatures.

Let N_{H_2} indicates the value of H_2 oracle queries. Therefore, it outputs $Prob[EV_{pid}] = \frac{1}{N_{H_2}}$, $Prob[EV_{fabricate}|EV_{pid}] \geq \frac{1}{9}$. The advantage and $Adv_{\Omega, \mathcal{A}}^{Scheme}$ that \mathcal{A} could resolve the DLP is as follows.

$$Prob[EV_{fabricate} \wedge EV_{pid}] = Prob[EV_{fabricate}|EV_{pid}] \cdot Prob[EV_{pid}] \geq \frac{1}{9} \cdot Adv_{\Omega, \mathcal{A}}^{Scheme} \cdot \frac{1}{N_{H_2}} = \frac{Adv_{\Omega, \mathcal{A}}^{Scheme}}{9N_{H_2}}.$$

Thus, \mathcal{I} resolves the DLP with an advantage of non-negligible $\frac{Adv_{\Omega, \mathcal{A}}^{Scheme}}{9N_{H_2}}$ owing to the bounded N_{H_2} and non-negligible $Adv_{\Omega, \mathcal{A}}^{Scheme}$. Hence, this completes the security proof for the proposed scheme.

5.3. Security Requirements

Our work should be achieved the security goals (Section 3.2) concerning security requirements as follows.

- **Authentication and Integrity:** Once the vehicle sending the message-signature tuples $\{M_i, PK_{i,l}, PID_{i,l}, D_i, T_i, \delta_i\}$ to others, the checker in our work checks the correctness $D_i^{\delta_i} \cdot \zeta_{Pub-\alpha}^{H_2(PID_{i,l}) \cdot \Theta_i} \stackrel{?}{=} g^{H_4(D_i)}$ for testing the tuple's integrity and authenticity. According to Theorem 1 in Section 5.2, there is no attacker \mathcal{A} of polynomial-time that could impersonate/generate a legitimate message if the DLP is hardness.
- **Privacy Preserving:** In the PIDGen and KeyGen phase, the vehicle's true identity is hidden in the $PID_i^* = \{PID_{i,1}, PID_{i,2}, \dots, PID_{i,n}\}$ by TA, where $PID_{i,l} = OID_i \oplus H_1(PK_{i,l}^\beta, \zeta_{Pub-\beta})$ and $l \in \{1, 2, \dots, n\}$. To disclose the vehicle's true identity OID_i from $PID_{i,l} = OID_i \oplus H_1(PK_{i,l}^\beta, \zeta_{Pub-\beta})$, \mathcal{A} requires to calculate $\zeta_{Pub-\beta} = g^\beta$ based on $\beta \in Z_q^*$. Nevertheless, this process contradicts the hardness of CDHP. Thus, our work satisfies privacy preserving.
- **Traceability:** By tracing the origin of messages sent, the TA is able to revoke and block the enrollment of any attacker that attempts to broadcast forge messages or disturb the system in 5G-enable vehicular networks. Once receiving the forge message, the vehicle reports it to the TA to verify its aid and, if available in the list, calculates the OID_i as $OID_i = PID_{i,l} \oplus H_1(\beta, PK_{i,l}^\beta, \zeta_{Pub-\beta})$ utilizing master key β . Thus, the function of traceability is provided by our work.

- **Replaying Resistance:** Our work can resist replay attacks by utilizing timestamp T_i in the message-signature tuples $\{M_i, PK_{i,l}, PID_{i,l}, D_i, T_i, \delta_i\}$. It denotes the signing time of tuples. Let T_{ri} is the arrival time of the message. It requires to verify if $T_{ri} - T_i \geq \Delta T$. When this condition holds, then there is no replay attacks.

5.4. Security Level

In this section, we show the security level of our work compared to the existing schemes in terms of privacy and security requirements. Therefore, we summarize and compare the security and piracy requirements of our work with the existing works He et al. [40], Azees et al. [42], Pournaghi et al. [43], and Bayat et al. [45] in Table 1. Thereby, all related works require RSU aid. Schemes of Azees et al. [42] and Bayat et al. [45] are vulnerable to replay attacks. Azees et al.'s scheme [42] is not satisfied by mutual authentication. As a result of Table 1, it can be concluded that our work achieves better security properties as compared to other works tabulated in that table.

Table 1. Comparison of Security Properties.

Schemes	Authentication and Integrity	Privacy Preserving	Replaying Resistance	Traceability	No RSU Aided
He et al. [40]	✓	✓	✓	✓	✗
Azees et al. [42]	✗	✓	✗	✓	✗
Pournaghi et al. [43]	✓	✓	✓	✓	✗
Bayat et al. [45]	✓	✓	✗	✓	✗
Our work	✓	✓	✓	✓	✓

6. Performance Comparison

In this section, the performance comparison of our work is evaluated with regard to costs of communication and computation. Meanwhile, the performance of our work is compared with schemes He et al. [40], Azees et al. [42], Pournaghi et al. [43], and Bayat et al. [45] via an experiment of simulation.

As presented in Figure 4, this work utilizes traffic generation simulator and network generation simulator such as OpenStreetMap [53], GatcomSUMO [54], SUMO [55] OMNeT++ [56], VEINS [57], Simu5G [58], and MIRACL [59,60] to execute experiments of simulation for 5G-enabled vehicular networks. OpenStreetMap is a very real trusted map website. GatcomSUMO is a java-based program utilized to facilitate the connection between the generation of traffic (SUMO) and the generation of the network (OMNeT++). SUMO is a road traffic simulation with a highly portable. OMNeT++ is a open-architecture for networks. Veins are joined with the generation of road traffic and the generation of networks. INET is a framework OMNeT++ suited for wired, wireless, and mobile networks. Simu5G is suited for a 5G-enabled vehicular network. MIRACL is a cryptographic library utilized to run operations based on cryptography algorithms. Table 2 lists the parameters of the simulation experiment.

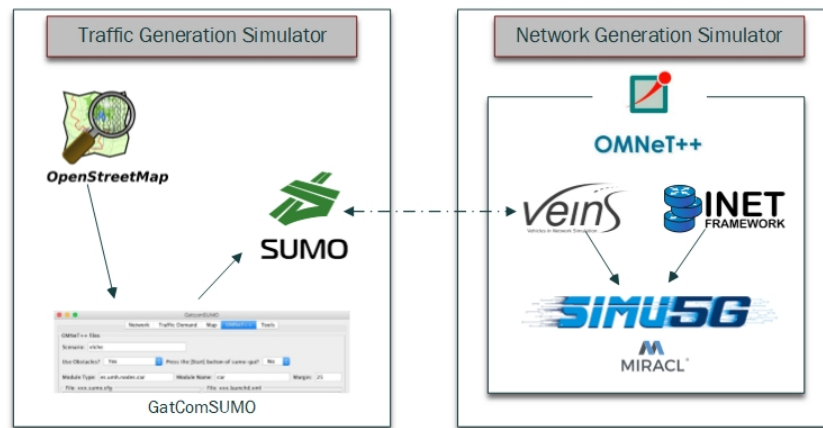


Figure 4. Simulation Experiments for 5G-enabled Vehicular Networks.

Table 2. Parameters of Simulation Experiment.

Parameters	Value
Play ground size	x = 3463 m, y = 4270 m and z = 50 m
Simulation time	200 s
Physical Layer	IEEE 802.11p
Mac Layer	IEEE 1609.4
Bit rate	6 Mbps
Maximum transmission	20 mW

6.1. Computation Costs

For a fair evaluation, the notations with the costs of the execution time of some cryptographic operations are tabulated in Table 3. This paper considers the computation overheads of generating pseudonym-IDs, signed message, and verification process, and compares them with existing schemes in Table 4.

Table 3. Notation with its Costs of Execution Time.

Notation	Descriptions	Execution Time
T_{bp}	a bilinear pairing $\bar{e}(P, Q)$	5.811 ms
T_{mul}	a BP scalar multiplication $s \cdot \bar{P}$	1.5654 ms
T_{add}	a BP point addition $\bar{P} + \bar{Q}$	0.0106 ms
T_{MTP}	a MapToPoint hash function	4.1724 ms
t_{mul}	a ECC scalar multiplication operation $s \cdot P$	0.6718 ms
t_{add}	a ECC point addition operation $P + Q$	0.0031 ms
t_h	a secure cryptographic hash function	0.0001 ms

Table 4. The Cost of Computation of Five Authentication Schemes.

Scheme	MsgSign Phase	SigVerify Phase	BSigVerify Phase
He et al.'s scheme [40]	$3t_{mul} + 3t_h \approx 2.0156$ ms	$5t_{mul} + t_{add} + 2t_h \approx 3.3622$ ms	$(2 + 3n)t_{mul} + (2n - 1)t_{add} + (2n)t_h \approx 1.3405 + 2.0236n$ ms
Azees et al.'s scheme [42]	$1T_{mul} + 1t_h \approx 1.5655$ ms	$2T_{bp} + 5T_{mul} + 2T_{add} \approx 19.661$ ms	$(1 + n)T_{bp} + (5n)T_{mul} + (2n)T_{add} \approx 5.811 + 13.6592n$ ms
Pournaghi et al.'s scheme [43]	$3T_{mul} + 1T_{add} + 2t_h + 1T_{MTP} \approx 8.8794$ ms	$3T_{bp} + (n)T_{mul} + (n)T_{MTP} \approx 21.6054$ ms	$3T_{bp} + (n)T_{mul} + (n)T_{MTP} \approx 17.433 + 5.7378n$ ms
Bayat et al.'s scheme [45]	$1T_{MTP} \approx 4.1724$ ms	$3T_{bp} + (n)T_{mul} + (n)T_{MTP} \approx 21.6054$ ms	$3T_{bp} + (n)T_{mul} + (n)T_{MTP} \approx 17.433 + 5.7378n$ ms
The proposed scheme	$1t_{mul} + 2t_h \approx 0.6719$ ms	$4t_{mul} + t_{add} + 2t_h \approx 2.6904$ ms	$(2 + 2n)t_{mul} + (n)t_{add} + (2n)t_h \approx 1.3436 + 1.3469n$ ms

In the MsgSign phase of the scheme of He et al. [40], the user needs to run three operations with regard to ECC scalar multiplication and three operations with regard to general hash function. Hence, the cost of computation of the MsgSign phase is $3t_{mul} + 3t_h \approx 2.0156$ ms. In the SigVerify phase of He et al.'s scheme [40], the user needs to run five operations with regard to scalar multiplication, one operation with regard to addition point and two operations with regard to hash function. Hence, the cost of computation of the SigVerify phase is $5t_{mul} + t_{add} + 2t_h \approx 3.3622$ ms. In the BSigVerify phase of He et al.'s scheme [40], the vehicle needs to run $(2 + 3n)$ operations with regard to scalar multiplication, $(2n - 1)$ operations with regard to addition point and $(2n)$ operations with regard to hash function. Hence, the cost of computation of the BSigVerify phase is $(2 + 3n)t_{mul} + (2n - 1)t_{add} + (2n)t_h \approx 1.3405 + 2.0236n$ ms.

In the MsgSign phase of Azees et al.'s scheme [42], the user needs to run one operation with regard to BP scalar multiplication and one operation with regard to general hash function. Hence, the cost of computation of the MsgSign phase is $1T_{mul} + 1t_h \approx 1.5655$ ms. In the SigVerify phase of Azees et al.'s scheme [42], the user needs to run two operations with regard to bilinear pair, five operations with regard to scalar multiplication, and two operations with regard to addition point. Hence, the cost of computation of the SigVerify phase is $2T_{bp} + 5T_{mul} + 2T_{add} \approx 19.661$ ms. In the BSigVerify phase of Azees et al.'s scheme [42], the user needs to run $(1 + n)$ operations with regard to bilinear pair, $(5n)$ operations with regard to scalar multiplication, and $(2n)$ operations with regard to addition point. Hence, the cost of computation of the BSigVerify phase is $(1 + n)T_{bp} + (5n)T_{mul} + (2n)T_{add} \approx 5.811 + 13.6592n$ ms.

In the MsgSign phase of Pournaghi et al.'s scheme [43], the user needs to run three operations with regard to scalar BP multiplication, one operation with regard to addition point, two operations with regard to general hash function, and one operation with regard to MapToPoint hash function. Hence, the cost of computation of the MsgSign phase is $3T_{mul} + 1T_{add} + 2t_h + 1T_{MTP} \approx 8.8794$ ms. In the SigVerify phase of the Pournaghi et al.'s scheme [43], the user needs to run three operations with regard to bilinear pair, one operation with regard to scalar multiplication, and one operation with regard to MapToPoint hash function. Hence, the cost of computation of the SigVerify phase is $3T_{bp} + (n)T_{mul} + (n)T_{MTP} \approx 21.6054$ ms. In the BSigVerify phase of Pournaghi et al.'s scheme [43], the user needs to run three operations with regard to bilinear pair, (n) operations with regard to scalar multiplication, and (n) operations with regard to MapToPoint hash function. Hence, the cost of computation of the BSigVerify phase is $3T_{bp} + (n)T_{mul} + (n)T_{MTP} \approx 17.433 + 5.7378n$ ms.

In the MsgSign phase of Bayat et al.'s scheme [45], the user needs to run only one operation with regard to MapToPoint hash function. Hence, the cost of computation of the MsgSign phase is $1T_{MTP} \approx 4.1724$ ms. In the SigVerify phase of the Bayat et al.'s scheme [45], the user needs to run three operations with regard to bilinear pair, one operation with regard to scalar multiplication, and one operation with regard to

MapToPoint hash function. Hence, the cost of computation of the SigVerify phase is $3T_{bp} + (n)T_{mul} + (n)T_{MTP} \approx 21.6054$ ms. In the BSigVerify phase of Bayat et al.'s scheme [45], the user needs to run three operations with regard to bilinear pair, (n) operations with regard to scalar multiplication, and (n) operations with regard to MapToPoint hash function. Hence, the cost of computation of the BSigVerify phase is $3T_{bp} + (n)T_{mul} + (n)T_{MTP} \approx 17.433 + 5.7378n$ ms.

In the MsgSign phase of our work, the user needs to run one operation with regard to ECC scalar multiplication and two operations with regard to general hash function. Hence, the cost of computation of the MsgSign phase is $1t_{mul} + 2t_h \approx 0.6719$ ms. In the SigVerify phase of our work, the vehicle needs to run four operations with regard to scalar multiplication, one operation with regard to addition point and two operations with regard to hash function. Hence, the cost of computation of the SigVerify phase is $4t_{mul} + t_{add} + 2t_h \approx 2.6904$ ms. In the BSigVerify phase of our work, the user needs to run $(2 + 2n)$ operations with regard to scalar multiplication, (n) operations with regard to addition point, and $(2n)$ operations with regard to hash function. Hence, the cost of computation of the BSigVerify phase is $(2 + 2n)t_{mul} + (n)t_{add} + (2n)t_h \approx 1.3436 + 1.3469n$ ms.

Furthermore, the entire time is based on the runtime of each cryptographic operation. The elapsed time (ET) between the exit and entrance is the overhead cost.

$$ET = \frac{1}{M} \sum_{i=1}^n M(T_{out}^i - T_{in}^i) \quad (9)$$

where, M is the message number, T_{in}^i is the entrance time of message i , and T_{out}^i is the exit time of message i . Figures 5 and 6 depict the average time to sign and verify a message between the proposed and scheme of He et al. [40]. The main reason for comparing our work against only He et al. [40] is to the same cryptography operations (e.g., ECC) used to sign message and verify signature. Additionally, the cost of He et al.'s scheme [40] is most efficient compared with other schemes according to Table 4. The results of the experimental methods show that our work is much more efficient than existing methods.

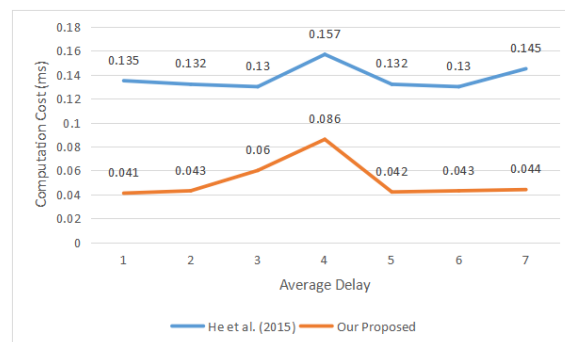


Figure 5. Average Time to Sign Message.

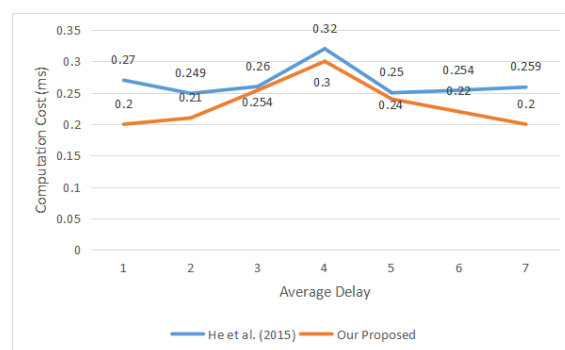


Figure 6. Average Delay to Verify Message.

6.2. Communication Costs

In this section, the primary concentrate is the cost of communication included in the timestamps, signatures, and pseudonym-IDs for the message-signature tuples. Table 5 shows the sizes of cryptographic elements used for communication costs.

Table 5. The Sizes of Elements Used.

Element	Size
Z_q^*	160 bits
G	320 bits
G_1	1024 bits
Timestamp	32 bits
Hash function	160 bits

In the scheme of He et al. [40], the signer broadcasts the message-signature tuple $\{M_i, R_i, AID_{i,1}, T_i, AID_{i,2}, \sigma_i\}$ to the recipient, where $\sigma_i \in Z_q$, $\{R_i, AID_{i,2}, AID_{i,1}\} \in G$ and T_i is a timestamp. Consequently, the cost of communication is $3 \times 320 + 160 + 32 = 1152$ bits. In the scheme of Azees et al. [42], the signer broadcasts the message-signature tuple $\{Cert_k || Y_k || Sig\}$ to the recipient, where $Cert_k = \{E_i || \sigma_1 || |y_v| || \lambda || \sigma_2 || Y_k || y_u || DID_{ui}\}$, $\{E_i, y_u, Y_k, DID_{ui}, sig\} \in G_1$, $\{\sigma_2, \sigma_1, \lambda\} \in Z_q^*$, c is a hash operation. Consequently, the cost of communication is $6 \times 1024 + 3 \times 160 + 32 = 6656$ bits. In Pournaghi et al.'s scheme [43], the signer sends the message-signature tuple $\{M_i, ID_{RSU_i}, pID_i^1, pID_i^2, \sigma_i\}$ to the recipient, where $\{pID_i^1, pID_i^2\} \in G_1$ and $\{\sigma_i, ID_{RSU_i}\} \in Z_q^*$. Consequently, the cost of communication is $2 \times 1024 + 2 \times 160 = 2368$ bits. In Bayat et al.'s scheme [45] the signer broadcasts the message-signature tuple $\{M_i, pID_i^1, pID_i^2, \sigma_i\}$ to the recipient, where $\{pID_i^1, pID_i^2\} \in G_1$ and $\sigma_i \in Z_q^*$. Consequently, the cost of communication is $2 \times 1024 + 1 \times 160 = 2208$ bits. In our work, the signer sends the message-signature tuple $\{M_i, PK_{i,l}, PID_{i,l}, D_i, T_i, \delta_i\}$ to others in 5G-enabled vehicular networks, where $\{PK_{i,l}, D_i\} \in G$, T_i is the timestamp and $\{\delta_i, PID_{i,l}\}$ is a hash operations. Consequently, the cost of communication is $2 \times 320 + 2 \times 160 + 32 = 992$ bits.

Communication cost comparisons for all works are presented in Table 6. Similar to the cost of computation, our work is significantly better than other existing works, as presented in Figure 7.

Table 6. The Costs of Communication Comparison.

Scheme	Message-Signature Tuple	Size (bits)	n Size (bits)
He et al. [40]	$\{AID_{i,1}, AID_{i,2}, M_i, R_i, T_i, \sigma_i\}$	$3 \times 320 + 160 + 32 = 1152$	1152 n
Azees et al. [42]	$\{Sig Y_k Cert_k\}$	$6 \times 1024 + 3 \times 160 + 32 = 6656$	6656 n
Pournaghi et al. [43]	$\{M_i, ID_{RSU_i}, pID_i^1, pID_i^2, \sigma_i\}$	$2 \times 1024 + 2 \times 160 = 2368$	2368 n
Bayat et al. [45]	$\{M_i, pID_i^1, pID_i^2, \sigma_i\}$	$2 \times 1024 + 1 \times 160 = 2208$	2208 n
Our Proposed	$\{M_i, PK_{i,l}, PID_{i,l}, D_i, T_i, \delta_i\}$	$2 \times 320 + 2 \times 160 + 32 = 992$	992 n

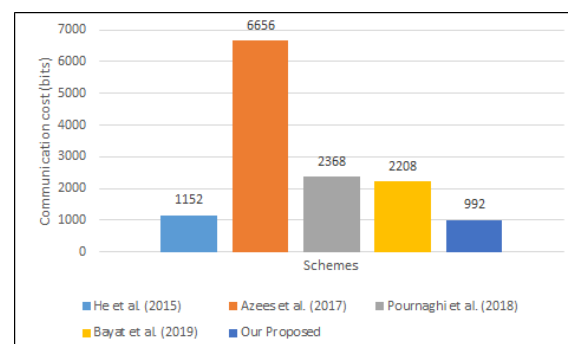


Figure 7. The Costs of Communication Comparison.

7. Conclusions

This paper proposed a provably secure with efficient data-sharing scheme without using RSU for 5G-enabled vehicular networks. Our work does not use an expansive component called RSU for the authentication process to improve efficiency further. Furthermore, the provable security displayed that our work is secure against adaptive selected-message attacks based on the random oracle model. Furthermore, our work not only achieves the requirements of security (message authentication and integrity, identity privacy preservation, and traceability) but also resists the security attacks such as replay attacks. This work carried out our simulation experiments with regard to network simulator (OMNeT++) and traffic simulator (SUMO) to analyze the results. Lastly, this paper reduces the computation cost to sign the message, verify signature, and batch signature verification by 66.67%, 19.98%, and 20.01%, respectively. This paper reduces the communication overhead the message-signature-tuple size by 13.89%.

The major limitation the proposed approach is uses large numbers (e.g., four operations) of ECC-based multiplication point to verify messages sent among vehicles. A fast-moving vehicle requires fast verification by using lightweight operations to verify messages. Therefore, in future work, it will contain the design of a fog computing-based authentication scheme that uses an operation based on ECC cryptographic algorithm in 5G-enabled vehicular networks.

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

Funding: This research has been funded by the Scientific Research Deanship at the University of Ha'il, Saudi Arabia, through project number RG-21098.

Institutional Review Board Statement: Not Applicable.

Informed Consent Statement: Not Applicable.

Data Availability Statement: Not Applicable.

Acknowledgments: We would like to acknowledge the Scientific Research Deanship at the University of Ha'il, Saudi Arabia, for funding this research.

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

References

1. Al-Shareeda, M.A.; Manickam, S.; Mohammed, B.A.; Al-Mekhlafi, Z.G.; Qtaish, A.; Alzahrani, A.J.; Alshammari, G.; Sallam, A.A.; Almekhlafi, K. CM-CPPA: Chaotic Map-Based Conditional Privacy-Preserving Authentication Scheme in 5G-Enabled Vehicular Networks. *Sensors* **2022**, *22*, 5026. [[CrossRef](#)]
2. Al-Shareeda, M.A.; Manickam, S. Man-In-The-Middle Attacks in Mobile Ad Hoc Networks (MANETs): Analysis and Evaluation. *Symmetry* **2022**, *14*, 1543. [[CrossRef](#)]
3. Cheng, X.; Chen, C.; Zhang, W.; Yang, Y. 5G-enabled cooperative intelligent vehicular (5GenCIV) framework: When Benz meets Marconi. *IEEE Intell. Syst.* **2017**, *32*, 53–59. [[CrossRef](#)]
4. Al-Shareeda, M.A.; Anbar, M.; Manickam, S.; Khalil, A.; Hasbullah, I.H. Security and Privacy Schemes in Vehicular Ad-Hoc Network With Identity-Based Cryptography Approach: A Survey. *IEEE Access* **2021**, *9*, 121522–121531. [[CrossRef](#)]
5. Al-Shareeda, M.A.; Anbar, M.; Manickam, S.; Hasbullah, I.H. Towards identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. *IEEE Access* **2021**, *9*, 113226–113238. [[CrossRef](#)]
6. Prasad, K.S.V.; Hossain, E.; Bhargava, V.K. Energy efficiency in massive MIMO-based 5G networks: Opportunities and challenges. *IEEE Wirel. Commun.* **2017**, *24*, 86–94. [[CrossRef](#)]
7. Al-Shareeda, M.A.; Manickam, S.; Mohammed, B.A.; Al-Mekhlafi, Z.G.; Qtaish, A.; Alzahrani, A.J.; Alshammari, G.; Sallam, A.A.; Almekhlafi, K. Chebyshev Polynomial-Based Scheme for Resisting Side-Channel Attacks in 5G-Enabled Vehicular Networks. *Appl. Sci.* **2022**, *12*, 5939. [[CrossRef](#)]

8. Fascista, A.; Coluccia, A.; Wymeersch, H.; Seco-Granados, G. Downlink single-snapshot localization and mapping with a single-antenna receiver. *IEEE Trans. Wirel. Commun.* **2021**, *20*, 4672–4684. [[CrossRef](#)]
9. 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. [[CrossRef](#)] [[PubMed](#)]
10. Dong, P.; Zheng, T.; Yu, S.; Zhang, H.; Yan, X. Enhancing vehicular communication using 5G-enabled smart collaborative networking. *IEEE Wirel. Commun.* **2017**, *24*, 72–79. [[CrossRef](#)]
11. 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](#)]
12. Alazzawi, M.A.; Al-behadili, H.A.; Srayyih Almalki, M.N.; Challoor, 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: Singapore, 2020; pp. 80–94.
13. Al Shareeda, M.; Khalil, A.; Fahs, W. Realistic heterogeneous genetic-based RSU placement solution for V2I networks. *Int. Arab J. Inf. Technol.* **2019**, *16*, 540–547.
14. Hamdi, M.M.; Mustafa, A.S.; Mahd, H.F.; Abood, M.S.; Kumar, C.; Al-shareeda, M.A. Performance Analysis of QoS in MANET based on IEEE 802.11 b. In *Proceedings of the 2020 IEEE International Conference for Innovation in Technology (INOCON)*, Bangalore, India, 6–8 November 2020; pp. 1–5.
15. Hamdi, M.M.; Audah, L.; Rashid, S.A.; Al Shareeda, M. Techniques of Early Incident Detection and Traffic Monitoring Centre in VANETs: A Review. *J. Commun.* **2020**, *15*, 896–904. [[CrossRef](#)]
16. Al-shareeda, M.A.; Anbar, M.; Manickam, S.; Hasbullah, I.H.; Khalil, A.; Alazzawi, M.A.; Al-Hiti, A.S. Proposed efficient conditional privacy-preserving authentication scheme for v2v and v2i communications based on elliptic curve cryptography in vehicular ad hoc networks. In *Proceedings of the International Conference on Advances in Cyber Security, Penang, Malaysia, 8–9 December 2020*; Springer: Singapore, 2020; pp. 588–603.
17. Al-shareeda, M.A.; Alazzawi, M.A.; Anbar, M.; Manickam, S.; Al-Ani, A.K. A Comprehensive Survey on Vehicular Ad Hoc Networks (VANETs). In *Proceedings of the 2021 International Conference on Advanced Computer Applications (ACA)*, Maysan, Iraq, 25–26 July 2021; pp. 156–160.
18. Xu, W.; Zhou, H.; Cheng, N.; Lyu, F.; Shi, W.; Chen, J.; Shen, X. Internet of vehicles in big data era. *IEEE/CAA J. Autom. Sin.* **2017**, *5*, 19–35. [[CrossRef](#)]
19. Cheng, J.; Cheng, J.; Zhou, M.; Liu, F.; Gao, S.; Liu, C. Routing in internet of vehicles: A review. *IEEE Trans. Intell. Transp. Syst.* **2015**, *16*, 2339–2352. [[CrossRef](#)]
20. Bai, F.; Krishnan, H. Reliability analysis of DSRC wireless communication for vehicle safety applications. In *Proceedings of the 2006 IEEE intelligent transportation systems conference*, Toronto, ON, Canada, 17–20 September 2006; pp. 355–362.
21. Yang, Q.; Zhu, B.; Wu, S. An architecture of cloud-assisted information dissemination in vehicular networks. *IEEE Access* **2016**, *4*, 2764–2770. [[CrossRef](#)]
22. Cui, J.; Ouyang, F.; Ying, Z.; Wei, L.; Zhong, H. Secure and efficient data sharing among vehicles based on consortium blockchain. *IEEE Trans. Intell. Transp. Syst.* **2021**, *23*, 8857–8867. [[CrossRef](#)]
23. Lai, C.; Lu, R.; Zheng, D.; Shen, X. Security and privacy challenges in 5G-enabled vehicular networks. *IEEE Netw.* **2020**, *34*, 37–45. [[CrossRef](#)]
24. Vijayakumar, P.; Azees, M.; Chang, V.; Deborah, J.; Balusamy, B. Computationally efficient privacy preserving authentication and key distribution techniques for vehicular ad hoc networks. *Clust. Comput.* **2017**, *20*, 2439–2450. [[CrossRef](#)]
25. Cincilla, P.; Hicham, O.; Charles, B. Vehicular PKI Scalability-consistency Trade-offs in Large Scale Distributed Scenarios. In *Proceedings of the 2016 IEEE Vehicular Networking Conference (VNC)*, Columbus, OH, USA, 8–10 December 2016; pp. 1–8.
26. 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](#)]
27. Joshi, A.; Gaonkar, P.; Bapat, J. A Reliable and Secure Approach for Efficient Car-to-Car Communication in Intelligent Transportation Systems. In *Proceedings of the 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, Chennai, India, 22–24 March 2017; pp. 1617–1620.
28. 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](#)]
29. 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](#)]
30. Rajput, U.; Abbas, F.; Oh, H. A hierarchical privacy preserving pseudonymous authentication protocol for VANET. *IEEE Access* **2016**, *4*, 7770–7784. [[CrossRef](#)]
31. Asghar, M.; Doss, R.R.M.; Pan, L. A Scalable and Efficient PKI based Authentication Protocol for VANETs. In *Proceedings of the 2018 28th International Telecommunication Networks and Applications Conference (ITNAC)*, Sydney, Australia, 21–23 November 2018; pp. 1–3.
32. 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; pp. 25–32.

33. Sun, Y.; Zhang, B.; Zhao, B.; Su, X.; Su, J. Mix-zones optimal deployment for protecting location privacy in VANET. *Peer Peer Netw. Appl.* **2015**, *8*, 1108–1121. [[CrossRef](#)]
34. Chaum, D.; Van Heyst, E. Group signatures. In *Workshop on the Theory and Application of Cryptographic Techniques*; Springer: Berlin/Heidelberg, Germany, 1991; pp. 257–265.
35. Shao, J.; Lin, X.; Lu, R.; Zuo, C. A Threshold Anonymous Authentication Protocol for VANETs. *IEEE Trans. Veh. Technol.* **2015**, *65*, 1711–1720. [[CrossRef](#)]
36. Alimohammadi, M.; Pouyan, A.A. Sybil attack detection using a low cost short group signature in VANET. In Proceedings of the 2015 12th International Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC), Rasht, Iran, 8–10 September 2015; pp. 23–28.
37. Zhang, L.; Wu, Q.; Qin, B.; Domingo-Ferrer, J.; Liu, B. Practical secure and privacy-preserving scheme for value-added applications in VANETs. *Comput. Commun.* **2015**, *71*, 50–60. [[CrossRef](#)]
38. Cui, J.; Wang, Y.; Zhang, J.; Xu, Y.; Zhong, H. Full Session Key Agreement Scheme Based on Chaotic Map in Vehicular Ad hoc Networks. *IEEE Trans. Veh. Technol.* **2020**, *69*, 8914–8924. [[CrossRef](#)]
39. Lim, K.; Tuladhar, K.M.; Wang, X.; Liu, W. A scalable and secure key distribution scheme for group signature based authentication in VANET. In Proceedings of the 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), New York City, NY, USA, 19–21 October 2017; pp. 478–483.
40. 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](#)]
41. 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](#)]
42. Azees, M.; Vijayakumar, P.; Deboarh, L.J. EAAP: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks. *IEEE Trans. Intell. Transp. Syst.* **2017**, *18*, 2467–2476. [[CrossRef](#)]
43. Pournaghi, S.M.; Zahednejad, B.; Bayat, M.; Farjami, Y. NECPA: A novel and efficient conditional privacy-preserving authentication scheme for VANET. *Comput. Networks* **2018**, *134*, 78–92. [[CrossRef](#)]
44. 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](#)]
45. Bayat, M.; Pournaghi, M.; Rahimi, M.; Barmshoory, M. NERA: A New and Efficient RSU based Authentication Scheme for VANETs. *Wirel. Networks* **2019**, *26*, 1–16. [[CrossRef](#)]
46. Ali, I.; Li, F. An efficient conditional privacy-preserving authentication scheme for Vehicle-To-Infrastructure communication in VANETs. *Veh. Commun.* **2020**, *22*, 100228. [[CrossRef](#)]
47. 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](#)] [[PubMed](#)]
48. Alshudukhi, J.S.; Al-Mekhlafi, Z.G.; Mohammed, B.A. A Lightweight Authentication With Privacy-Preserving Scheme for Vehicular Ad Hoc Networks Based on Elliptic Curve Cryptography. *IEEE Access* **2021**, *9*, 15633–15642. [[CrossRef](#)]
49. Ali, I.; Chen, Y.; Ullah, N.; Afzal, M.; Wen, H. Bilinear pairing-based hybrid signcryption for secure heterogeneous vehicular communications. *IEEE Trans. Veh. Technol.* **2021**, *70*, 5974–5989. [[CrossRef](#)]
50. 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](#)]
51. Liu, J.K.; Yuen, T.H.; Au, M.H.; Susilo, W. Improvements on an authentication scheme for vehicular sensor networks. *Expert Syst. Appl.* **2014**, *41*, 2559–2564. [[CrossRef](#)]
52. Pointcheval, D.; Stern, J. Security arguments for digital signatures and blind signatures. *J. Cryptol.* **2000**, *13*, 361–396. [[CrossRef](#)]
53. Haklay, M.; Weber, P. Openstreetmap: User-generated street maps. *IEEE Pervasive Comput.* **2008**, *7*, 12–18. [[CrossRef](#)]
54. Abenza, P.P.G.; Malumbres, M.P.; Peral, P.P. 10 GatcomSUMO: A Graphical Tool for VANET Simulations Using SUMO and OMNeT+. In Proceedings of the SUMO 2017—Towards Simulation for Autonomous Mobility, Berlin, Germany, 8–10 May 2017; p. 113.
55. 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, 23–29 October 2011.
56. Varga, A. Discrete event simulation system. In Proceedings of the European Simulation Multiconference (ESM’2001), Prague, Czech Republic, 7–9 June 2001; pp. 1–7.
57. 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](#)]
58. Nardini, G.; Sabella, D.; Stea, G.; Thakkar, P.; Virdis, A. Simu5G—An OMNeT++ library for end-to-end performance evaluation of 5G networks. *IEEE Access* **2020**, *8*, 181176–181191. [[CrossRef](#)]
59. Scott, M. MIRACL—A Multiprecision Integer and Rational Arithmetic C/C++ Library. Available online: <http://www.shamus.ie> (accessed on 2003).
60. Ltd, S.S. Multi Precision Integer and Rational Arithmetic Cryptographic Library (MIRACL). Available online: <http://www.certivox.com/miracl/> (accessed on 2018).