RESEARCH ARTICLE

MSR-DoS: Modular Square Root-Based Scheme to Resist Denial of Service (DoS) Attacks in 5G-Enabled Vehicular Networks

MAHMOOD A. AL-SHAREEDA AND SELVAKUMAR MANICKAM
National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia, George Town, Penang 11800, Malaysia
Corresponding author: Selvakumar Manickam (selva@usm.my)

This work was supported by Vice Chancellor Initiative Allocation, Universiti Sains Malaysia, grant number 311/PNA/4119101.

ABSTRACT Traffic safety and efficiency are extremely significant in both private and public transportation. The fifth-generation (5G)-enabled vehicular networks works wirelessly to share information among vehicles for helping drivers and passengers. Since the vehicle broadcasts the traffic status messages, privacy and security are considered as a challenging issue in 5G-enabled vehicular networks. In order to satisfy these privacy and security requirements, many privacy-preserving and security attacks schemes have been proposed. Nevertheless, since these schemes use a complex elliptic curve and bilinear pair cryptography operations, the performance efficiency of in terms of communication and computational costs is not satisfactory, which denial of service (DoS) attacks occurs. To address this, this paper proposes modular square root-based to resist denial of service (DoS) attacks (MSR-DoS) scheme in 5G-enabled vehicular networks. Our MSR-DoS scheme satisfies authenticity of source, integrity of message, pseudonym privacy-preserving, unlinkable, traceable and revocable in vehicular networks. The security of our work is proved under burrows abadi needham (BAN) logic. The performance analysis and comparison shows that MSR-DoS scheme has less communication and computational costs as compared to the most recent existing works. Meanwhile, the proposed MSR-DoS scheme reduces the computation overhead of signing the message and verifying the message by 99.80% and 98.55%, respectively.

INDEX TERMS Modular square root (MSR), security, vehicular network, 5G technology, denial of service (DoS), privacy.

I. INTRODUCTION

In the coming fifth-generation (5G) mobile era, the message transmission speed of network services has been greatly increased. As the intended replacement to the 4G networks that connect the majority of modern smartphones, 5G is the 5G technology standard for broadband cellular networks, which cellular phone providers started rolling out globally in 2019. Meanwhile, there have been various scholars [1], [2], [3], [4] that have focused on the adoption of vehicle-to-everything (V2X) technology with 5G communication. The main aim of 5G-enabled vehicular networks is to provide vehicles, users, networks and things with operable, manageable, reliable connectivity, high-quality and controllable [5], [6], [7].

Wide coverage and fast bandwidth are features of the 5G mobile network. It presents vehicular networks with both opportunities and difficulties [8]. The data shows that under 5G wireless networks, the average data transmission rate is over 100Mb/s and the peak data transfer rate can reach 20Gb/s [9]. As opposed to current networks, the supported network has 1000 times the capacity and can offer a more reliable connection [10]. Security and privacy in the vehicular network based on 5G technology are two critical vulnerabilities at sharing data. There are two main of data shared by users namely, traffic-related and entertainment-related in vehicular networks. For traffic-related data, any injection or alteration may damage the safety of road traffic, and the road condition...
is more critical in case of self-driving as the alteration of the sensor or camera data can modify the driving plan [11], [12]. For entertainment-related data, the requests downloaded are often based on privacies of identity. Consequently, it is required to consider the privacy and security objectives in the 5G-enabled vehicular networks.

Several sophisticated schemes have been proposed to tackle the privacy and security vulnerabilities at sharing data in the vehicular network. These schemes based on either elliptic curve (EC) or bilinear pair (BP) cryptographies. Nevertheless, the cryptographic operations included by EC and BP are more complicated and time-consuming, which vulnerability can lead denial of service (DoS) attacks [13]. None of scholars appropriately resist DoS attacks and reduce the efficient performance for signature-verification method. Consequently, our scheme is based on modular square root (MSR) instead of EC or BP operations to resist DoS attack. Our proposed called MSR-DoS scheme for signing and verifying traffic-related and entertainment-related data.

The main aim of our scheme is to resist DoS attacks in 5G-enabled vehicular network. The main important contributions of this research are as follows.

- The classification of related work is retrospected and analyzed. Besides, computational DoS attacks of these schemes are pointed out. Then, it describes the 5G-enabled vehicular network architecture in terms of system model and security goals.
- We propose a modular square root-based to resist denial of service (DoS) attacks (MSR-DoS) scheme for secure communication in 5G-enabled vehicular networks.
- We have proven that the MSR-DoS scheme preserves authenticity of source, integrity of message, pseudonym privacy-preserving, unlinkable, traceable, and revocable in vehicular networks. Additionally, the security of the MSR-DoS scheme is proven in burrows abadi needham (BAN) logic.
- We have evaluated the performance analysis and shown that our work has less communication and computational costs as compared to most recent existing works.

The rest of this paper is organised as follows: In Section II, we review the related work. In Section III, the Background of our work is demonstrated. The main five phases of our work is proposed in Section IV. We analysis the security and performance of this paper in Section V and VI. Lastly, the conclusion of this paper is provided in Section VII.

II. RELATED WORK

Roughly speaking, according to Figure 1, there are three taxonomies of privacy-preserving and security attacks schemes for vehicular networks as follows. This taxonomy is based on Public Key Infrastructure-based; Group Signature-based; and Pseudonym-based (in terms of Bilinear Pair Cryptography and Elliptic Curve Cryptography). These classes are described as follows.

- **A. PUBLIC KEY INFRASTRUCTURE-BASED**
  Public key infrastructure-based schemes were proposed in [14], [15], [16], [17], [18], [19], [20], [21], and [22]. Those scholars aim to provide privacy-preserving and mutual authentication in vehicular networks by issuing and preloading massive numbers of certificates (roughly 44,000) and their corresponding pair-keys (private and public) to the participating vehicle. The TA is responsible to assign these number of certificates according to security level of the anonymity. Nevertheless, the main limitation of this approach is huge computational overheads due to the participating vehicle is also needed to verify certification in the verification algorithm (MsgVerify).

- **B. GROUP SIGNATURE-BASED**
  Group signature-based schemes were proposed [23], [24], [25], [26], [27]. Those scholars aim to address the huge computational overheads caused by the certification in the public key infrastructure-based schemes. Group signature-based schemes provides the privacy-preserving and mutual authentication in vehicular networks by allowing the group members to sign message anonymously on behalf of others. However, the main limitation of this approach is massive computational overhead due to the two pairing-based operations are needed during the certification revocation list (CRL) process. Therefore, the traditional signature-based schemes are most better compared with group signature in term of performance efficiency.

- **C. PSEUDONYM-BASED**
  To address extra computational overheads arising on the public-key infrastructure-based schemes and group signature-based schemes in vehicular networks. The main aims of this approach is that the public key is extracted from the vehicle’s identification and the secret key is generated by the TA. Generally, this approach can be classified into two categories: Bilinear Pair Cryptography and Elliptic Curve Cryptography.

  1) **BILINEAR PAIR CRYPTOGRAPHY**
  Pseudonym-based schemes were proposed [13], [28], [29], [30], [31], [32], [33], [34] by using cryptographic operations associated with bilinear pair cryptography to sign and verify the traffic-related messages. Zhang et al. [28] were the first to propose the use of the bilinear pair cryptography in 2008.

![FIGURE 1. Taxonomies of privacy-preserving and security attacks schemes.](image-url)
However, the cryptographic operations associated with pairing in this approach are time-consuming and complex, which caused huge computational overheads in signing and verifying messages.

2) ELLIPTIC CURVE CRYPTOGRAPHY

Pseudonym-based schemes were proposed [35], [36], [37], [38], [39], [40], [41] by using cryptographic operations associated with elliptic curve cryptography to sign and verify the traffic-related messages. He et al. [35] were the first to propose the use of the elliptic curve cryptography rather than bilinear pair cryptography to achieve security and privacy requirements in 2015. However, the cryptographic operations associated with elliptic curve in this approach are not efficient in terms of signing and verifying messages [26]. Furthermore, to address the use of expensive road-side unit (RSU) during mutual authentication process, several scholars [42], [43], [44] proposed pseudonym-based schemes for 5G-enabled vehicular networks without RSU. However, these schemes use scalar multiplication associated with elliptic curve cryptography.

According to the massive computational overheads, the existing schemes vulnerable to the DoS attacks. Therefore, their schemes cannot resist DoS attacks since timing-consuming and complex operations used. In contrast, this paper will propose modular square root-based DoS attacks Scheme (MSR-DoS) in 5G-enabled Vehicular Networks. The proposed MSR-DoS scheme will use lightweight cryptographic operations associated with MSR to reduce computational overheads and to handle the DoS attacks.

III. BACKGROUND

In this section, the background of our work with regard to system design and security objectives are demonstrated as follows.

A. SYSTEM DESIGN

As presented in Figure 2, the system design of 5G-enabled vehicular network utilized in our paper mainly contains three types of components: trusted authority (TA), 5G-based station (5G-BS), and onboard unit (OBU) installed in the vehicle.

- Trusted Authority (TA): TA acts as the enrollment aspect of vehicles. TA is trusted by all components in vehicular network based on 5G technology. The main responsibility of TA is to generate MSR parameters and preload them to vehicles.
- 5G-base Station (5G-BS): 5G-BS is installed on the road-side, acts as the bridge between vehicles and TA. The main aim of 5G-BS is to provide network access service to vehicles that located in its communication range. In our work, 5G-BS don’t do any computation process or storage data.
- Onboard Unit (OBU): Each vehicle is fitted with OBU that has a tamper-proof device (TPD) to improve driving safety and traffic efficiency.

B. SECURITY OBJECTIVES

Both privacy and security are extremely significant to secure the communication in 5G-enabled vehicular networks. Our work should archive the following requirements.

- Authentication and Integrity: The recipient authenticates the message to ensure it is valid and has not been modified with, i.e., the message recipient must identify the validity of the message.
- Pseudonym Privacy-preserving: to preserve identity privacy, the user utilizes the pseudonym to broadcast all data. No attacker except for TA has the ability to compute the true identity of the vehicle via message sent.
- Unlinkable: To protect privacy, no third party are able to link two messages sent by the same source with same pseudonym.
- Traceable and Revocable: TA has the capability to trace and block the vehicle’s true identity by capturing the message sent but attacker does not have the capability.
- Resist to Security Attacks: Our work should be resisted against common security attacks such as forgery, modify, replay, Man-In-The-model, and DoS Attacks.

C. MATHEMATICAL TOOL

In this subsection, the mathematical used of this paper is provided in terms of the preliminaries, standard of Euler and MSR algorithms as follow.

1) PRELIMINARIES

In 1979, Rabin [45] firstly introduced a new class of public-key functions, namely, modular square root (MSR). Then, Williams [46] further improved MSR by building on the residues of quadratic and its property [47].

Let $a$ indicates any integer and $n \in N$, where $N$ is a number of natural. Assume that the greatest common divisor of $a$ and $n$ is 1 as follows.

$$gcd(a, n) = 1$$ (1)
Then, let \( a \) as a quadratic residue modulo \( n \) when the congruence \( x^2 = a \pmod{n} \) is resolvable. Consequently, the solutions are called quadratic residues modulo \( n \) based MSR.

2) STANDARD OF EULER
Let \( p \) be a prime of odd and \( \gcd(a, p) = 1 \). Then \( a \) be a quadratic residue modulo \( p \) when and only when \( a^{\frac{p-1}{2}} \equiv 1 \pmod{p} \). If \( p = 3 \pmod{4} \) and \( a \) be a quadratic residue modulo \( p \), there is a formula of simple to calculate square roots of quadratic residue a modulo \( p \) as below:

\[
r_{1,2} = \pm a^{\frac{p+1}{4}} \pmod{p}
\]

Then there are two main properties according to standard of Euler [48] as follows.

**Property 1:** Let \( \gcd(a, n) = 1 \) and \( n = p \times q \), where \( p = 3 \pmod{4} \) and, \( p \) and \( q \) are two distinct primes of odd. Then \( a \) is a quadratic residue modulo \( n \) when and only when \( a^{\frac{n-1}{2}} = 1 \pmod{p} \) and \( a^{\frac{n-1}{2}} = 1 \pmod{q} \).

Based on the **Property 1** supposition, and the Chinese remainder theorem, under Equation 2, four modular square roots \( r_{1,2,3,4} \) of a quadratic residue \( a \) modulo \( n \) can be calculated as below.

\[
r_{1,2,3,4} = \pm \alpha \times q \times q^* \pm \beta \times p \times p^* \pmod{n}
\]

where \( \alpha = a^{\frac{p-1}{4}} \pmod{p} \), \( \beta = a^{\frac{q-1}{4}} \pmod{q} \), \( p^* = p^{-1} \pmod{q} \), and \( q^* = q^{-1} \pmod{p} \). Since \( \gcd(p, q) = 1 \), it is possible to identify both \( p^* \) and \( q^* \) according to the extended Euclidean algorithm [49].

**Property 2:** Let \( n = p \times q \), where \( p \) and \( q \) are two distinct primes of odd. Then the value of quadratic residues modulo \( n \) is \( \frac{(p-1)(q-1)}{4} \).

Note that the probability that any integer \( a \) is a quadratic residue modulo \( n \) is about one-quarter based on the supposition of **Property 2**.

3) MODULAR SQUARE ROOT (MSR) ALGORITHMS
Based on the above subsection, the MSR algorithms can be presented below.

- **Key Generation Algorithm:** One component \( X \) selects two distinct large primes \( p \) and \( q \) (such that \( p = q = 3 \pmod{4} \)) and computes \( n = p \times q \). Then component broadcasts \( n \) but saves \( p \) and \( q \) secret.

- **Encryption Algorithm:** When another component \( Y \) wants to broadcast a message \( M \) (where \( M \times 2^l < n \) and \( l \) is an integer more than 30) to component \( X \), \( X \) computes \( C = (M \times 2^l)^2 \pmod{n} \) and broadcasts \( C \) to component \( X \).

- **Decryption Algorithm:** Upon receiving \( C \) from component \( Y \), component \( X \) can identify all four distinct modular square roots of \( x^2 = C \pmod{n} \) with knowledge of \( p \) and \( q \) on the basis of Equation 3. Then the original message \( M \) can be revealed from the modular square root with \( l \).

**Problems of Intractable:** The security of the MSR algorithm is depend on the hardness of disclosing modular square roots of a quadratic residue modulo \( n(n = p \times q) \) when \( p \) and \( q \) are unknown. Furthermore, when \( p \) and \( q \) are large enough, it is computationally infeasible to factorize \( n \).

**IV. THE MSR-DoS SCHEME**
Security and privacy in the vehicular network based on 5G technology are two critical vulnerabilities that needed to be tackled quickly. Recently, there have various researchers focusing on proposing a security attack schemes to tackle the problem existing in the vehicular network based on 5G technology. But, their schemes are suffer from massive overhead with regard to communication and computation, which vulnerability can lead DoS attacks.

In this paper, we propose a modular square root-based to resist DoS attacks (MSR-DoS) scheme for vehicular networks based on 5G technology. Without utilising ECC or BP operations, our work aims to tackle the secure vulnerabilities and reduce the cost of the communication. This paper is depend on the scheme proposed by [50]. Our work has five algorithms, namely: TASetup, PIDGen and CerGen, MsgSign, MsgVerify, and ParUpdate. Nevertheless, unlike the scheme proposed by [50], our work employs a 5G-BS to provide vehicles with high-efficiency sharing data. Also, our work is not required using an expensive component (RSU) during mutual authenticate the messages. The following algorithms should be included in the proposed MSR-DoS scheme.

**A. TA SETUP**
In the TASetup algorithm, the initial system parameters \( \Upsilon \) are generated by the TA, as the following steps.

- TA chooses two large odd numbers of distinct prime \( p_{sys} \) and \( q_{sys} \) such that \( p_{sys} = q_{sys} = 3 \pmod{4} \) and then calculates \( n_{sys} = p_{sys} \times q_{sys} \).
- TA chooses two large odd numbers of distinct prime \( p_{veh} \) and \( q_{veh} \) for each vehicle in 5G-enabled vehicular networks, and then calculates \( n_{veh} = p_{veh} \times q_{veh} \).
- TA selects a secure message authentication code (MAC) function \( MAC(\cdot) \) and a secure hash function \( H(\cdot) \).
- TA sets the initial system parameters as \( \Upsilon = \{n_{sys}, n_{veh}, MAC(\cdot), H(\cdot)\} \). Note that \( p_{sys} \) and \( q_{sys} \) are only known to TA.

**B. PID GEN AND CER GEN**
In the PIDGen and KeyGen algorithms, the TA generates the long-term certificate \( (PID^1_i, r_i, s_i) \) for all participating vehicles in 5G-enabled vehicular networks. To satisfy a mutual authentication and a privacy-preserving in the proposed MSR-DoS scheme, it should be employed the pseudonym-ID \( (PID^1_i) \) that is particularly associated with the corresponding true identity \( TID_{veh_i} \) as the following steps:

- Prior vehicle \( veh_i \) leaving the factory, the true identity \( TID_{veh_i} \) and the password \( PWD \) are submitted to TA for registration purpose.
- Once checking the validity of \( TID_{veh_i} \), TA computes a group of \( PIDs \) for vehicle \( veh_i \) as
\[ \text{PID}^t_\text{veh} = \{\text{PID}^t_1, \text{PID}^t_2, \ldots, \text{PID}^t_n\}, \] where \( \text{PID}^t_i = \text{TID}_{\text{veh}} \oplus H(p_{\text{sys}}, q_{\text{sys}}) \) and \( i \in \{1, 2, \ldots, n\} \).

- TA calculates \( \alpha = H(\text{PID}^t_i, r_i) \) and verify if \( \alpha = p_{\text{sys}}^{-1} \) and \( \alpha^{-1} = 1 \mod d_{\text{sys}} \), where \( r_i = 0 \). Note that if not, TA recomputes \( r_i = r + 1 \) and redoes the computation and confirmation in this step.

- TA calculates four square-roots \( x_{1,2,3,4} \) of \( x^2 = \alpha \mod n_{\text{sys}} \) with the knowledge of \( p_{\text{sys}} \) and \( q_{\text{sys}} \), based on Equation (3), and then selects the smallest square-root as \( s_j \).

- TA outputs the long-term certificate (\( \text{PID}^t_1, r_i, s_i \)) after four loops on the average of above steps according to Property (2).

- TA securely preloads \( H(\text{TID}_{\text{veh}}, \text{PWD}), p_{\text{veh}}, q_{\text{veh}}, \{\text{PID}^t_i, r_i, s_i\} \) into the TPD of participating vehicle.

- Finally, TA saves pseudonym-ID (\( \text{PID}^t_1 \)) and the corresponding true identity \( \text{TID}_{\text{veh}} \) into vehicles registration list (VRL) for tracing malicious vehicles.

### C. MSGSIGN

In the MsgSign algorithm, when vehicle \( \text{veh}_i \) wants to broadcast traffic-related message \( Tmsg_i \) to others for achieving safety road environment in 5G-enabled vehicular networks, it should be signed as the following steps.

- Once user inputting \( \text{TID}_{\text{veh}} \) and \( \text{PWD} \), the TPD of vehicle should first check the valid \( \text{TID}_{\text{veh}} \) and \( \text{PWD} \) by computing \( H(\text{TID}_{\text{veh}}, \text{PWD}) \) to pass login process. If it not so, the TPD will reject to further services. Otherwise, the MsgSign algorithm is continued to next steps.

- Vehicle \( \text{veh}_i \) selects one the long-term certificate (\( \text{PID}^t_i, r_i, s_i \)) and sets the randomly selected number \( \omega \) such that \( \sqrt{n_{\text{veh}}} < \omega < n_{\text{veh}} \).

- Vehicle \( \text{veh}_i \) calculates \( R_i = \omega^{2 \cdot \theta^{-1}} (\mod n_{\text{veh}}) \) to avoid the use of division in the next modular operation [51], where \( \theta = 2^l \) and \( 2^l-1 < n_{\text{veh}} < n^l \).

- Vehicle \( \text{veh}_i \) selects share key \( k = H(\omega) \) and calculates the MAC operation \( U_i = MAC_k(\text{PID}^t_i) \).

- Vehicle \( \text{veh}_i \) encrypts the message \( Tmsg_i \) as \( \sigma_i = Enc_k(Tmsg_i, \text{PID}^t_i, r_i, s_i, T_i) \), where \( T_i \) is the freshness timestamp.

- Finally, Vehicle \( \text{veh}_i \) broadcasts final message-tuples \( (Tmsg_i, \text{PID}^t_i, R_i, U_i, T_i, \sigma_i) \) to others in 5G-enabled vehicular networks.

Note that after broadcasting final message-tuples \( (Tmsg_i, \text{PID}^t_i, R_i, U_i, T_i, \sigma_i) \), Vehicle \( \text{veh}_i \) puts revoked pseudonym \( \text{PID}^t_i \) and the relevant revoked time \( T \) into the pseudonym revocation list (PRL).

### D. MSGVERIFY

In the MsgVerify algorithm, once final message-tuples \( (Tmsg_i, \text{PID}^t_i, R_i, U_i, T_i, \sigma_i) \) from vehicle \( \text{veh}_i \), receiver should be verified the validity of the message to ensure that vehicle \( \text{veh}_i \) is legitimate and registered by the TA, as the following steps.

- Verifying receiver checks the freshness of timestamp \( T_i \) to resist the replay attacks.

- Verifying receiver calculates four square-roots \( x_{1,2,3,4} \) of \( x^2 = R_i \cdot \theta (\mod n_{\text{veh}}) \) with the knowledge of \( p_{\text{veh}} \) and \( q_{\text{veh}} \) according to Equation (3).

- Verifying receiver calculates four hash values as share key \( k_{1,2,3,4} = H(x_{1,2,3,4}) \).

- Verifying receiver distinguishes the share key \( k \) by checking received \( U_i \) with the MAC operation \( U_i = MAC_{k_{1,2,3,4}}(\text{PID}^t_i) \). Note that the probability that more than one share key \( k \) matches is negligible.

- Once distinguishing the share key \( k \), verifying receiver decrypts \( \sigma_i \) with the \( k \) to get \( Dec_k(\sigma_i) = (Tmsg_i, \text{PID}^t_i, r_i, s_i, T_i) \).

- Verifying receiver checks whether \( s_i^2 = H(\text{PID}^t_i, r_i)(\mod n_{\text{veh}}) \) holds or not. If it so, which means vehicle \( \text{veh}_i \) is legitimate and registered by the TA. Otherwise, the message will be rejected.

- At last, vehicle displays the traffic-related message \( Tmsg_i \) to the user for helping judge the road conditions in 5G-enabled vehicular networks.

### E. PARUPDATE

In the ParUpdate algorithm, the long-term certificate (\( \text{PID}^t_i, r_i, s_i \)), the two distinct primes \( p_{\text{veh}} \) and \( q_{\text{veh}} \) for participating vehicle, VRL and PRL are frequently updated. The main aims to update them are to reduce storage capability, enhance management efficiency and provide the system security for 5G-enabled vehicle networks. Based on assumption in this paper, TA could be regularly updated all sensitive information on the system. Therefore, the lists of VRL and PRL could be updated correspondingly. By assisting 5G-BS, the vehicle can request updates to TA for updating them when long-term certificate is used up.

### V. SECURITY ANALYSIS

This section analysis the security of our MSR-DoS scheme as follows.

### A. MUTUAL AUTHENTICATION PROOF

In this subsection, we analysis that the proposed MSR-DoS scheme provides the mutual authentication validity among vehicles using the widely-accepted Burrows Abadi Needham (BAN) logic [52]. The result shows that the proposed MSR-DoS scheme can achieve the authentication goals thorough utilizing BAN logic. The corresponding notations used in the BAN logic are tabulated in Table 1.

Main rules used for BAN logic analysis can be introduced as the following steps.

- **Rule 1**: Message-meaning: \[
\rho[\exists \rho \neq X, \rho < X > X].
\]

- **Rule 2**: Nonce-verification: \[
\rho[\exists \rho \neq X, \rho < X \neq X].
\]

- **Rule 3**: Jurisdiction: \[
\rho[\exists \rho \neq X, \rho = \rho] < X \neq X].
\]

- **Rule 4**: Freshness: \[
\rho[\exists \rho = \rho] < X = X].
\]

- **Rule 5**: Session-key: \[
\rho[\exists \rho = \rho] < X = X].
\]

The proposed MSR-DoS scheme achieves the following goals:
Goal: \( \text{veh}_i \equiv (R_i, U_i, \sigma_i) \) 
Goal 2: \( \text{veh}_j \equiv \leftarrow \text{veh}_i \).

The transformation of the message sent in the proposed MSR-DoS scheme can be given as follows:

\[
\text{veh}_i \rightarrow \text{veh}_j : \text{message-tuples} (T_{msgi}, PID^1_i, R_i, U_i, T_i, \sigma_i), \text{where } PID^1_i = TID_{veh_i} \oplus H(p_{sys}, q_{sys}). R_i = \omega^2 \cdot \theta^{-1} (mod \ n_{veh}), U_i = \text{MAC}_k(PID^1_i) \text{ and } \sigma_i = \text{Enc}_k(T_{msgi}, PID^1_i, r_i, s_i, T_i).
\]

In order to evaluate the proposed MSR-DoS scheme, some assumptions are presented as the following steps.

Assumption 1: \( \text{veh}_i \rightarrow \sigma \text{veh}_j \).
Assumption 2: \( \text{veh}_i \equiv \leftarrow T. \)
Assumption 3: \( \text{veh}_i \equiv \text{veh}_j \rightarrow (PID^1_i, r, s). \)

According to the above logical postulates and assumptions and for BAN logic analysis, the idealized form of the proposed MSR-DoS scheme can be proved as follows.

\[
A_{S1} : \text{veh}_j \leftarrow (R_i, U_i, \sigma_i) : \{< \omega > \theta, (PID^1_i)_{\omega}, \{T_{msgi}, PID^1_i, r_i, s_i, T_i \}_{\omega}\}. \text{Based on } A_{S1}, \text{Assumption 1 and Rule 1}, \text{we obtain:}
\]

\[
A_{S2} : \text{veh}_j \equiv \text{veh}_j \leftarrow \{< \omega > \theta, (PID^1_i)_{\omega}, \{T_{msgi}, PID^1_i, r_i, s_i, T_i \}_{\omega}\}. \text{Based on } A_{S2}, \text{Assumption 2 and Rule 4}, \text{we obtain:}
\]

\[
A_{S3} : \text{veh}_j \equiv \text{veh}_j \equiv \{\omega, PID^1_i, r_i, s_i, T_i \}_{\omega}. \text{Based on } A_{S3}, \text{Assumption 3 and Rule 3}, \text{we obtain:}
\]

\[
A_{S4} : \text{veh}_j \equiv \{\omega, PID^1_i, r_i, s_i \}_{\omega} \rightarrow \text{veh}_j, T_{msgi}, T_i\}. \text{Based on } A_{S4}, \text{Assumption 2 and Rule 5}, \text{we obtain:}
\]

\[
\text{veh}_j \equiv \text{veh}_j \omega \rightarrow \text{veh}_j.
\]

Therefore, Steps \( A_{S4} \) and \( A_{S3} \) are achieved. By these above process formally BAN logic analysis, it proves that the mutual authentication among vehicles can be successfully achieved on the proposed MSR-DoS scheme.

**B. SECURITY REQUIREMENTS**

In this subsection, the security objectives of the proposed MSR-DoS scheme are provided as the following steps.

- Authentication and Integrity: In our work, the vehicle broadcasts final message-tuples \( T_{msgi}, PID^1_i, R_i, U_i, T_i, \sigma_i \) to others in 5G-enabled vehicular networks, where \( \sigma_i = \text{Enc}_k(T_{msgi}, PID^1_i, r_i, s_i, T_i) \), \( U_i = \text{MAC}_k(PID^1_i) \), \( R_i = \omega^2 \cdot \theta^{-1} (mod \ n_{veh}) \) and \( T_i \) is the freshness timestamp. Once receiving the final message-tuples, the verifier can decrypt \( U_i \) to get messages \( T_{msgi} \) since has the knowledge of \( p_{veh} \) and \( q_{veh} \). The verifier can easily utilize its master secrets \( p_{veh} \) and \( q_{veh} \) to calculate the share key \( k_{1, 2, 3, 4} = H(x_i, 1, 2, 3, 4) \) according to Equation 2. Consequently, based on the problem of intractable, for the third party who does not know \( p_{veh} \) and \( q_{veh} \), it is hard to obtain the share key \( K \). Thus, the proposed MSR-DoS scheme ensures authentication and integrity in 5G-enabled vehicular networks.

- Pseudonym Privacy-preserving: In phase of PIDGen and CerGen, each enrolled vehicle obtains a group of pseudonym-IDs \( PIDs \) as \( PIDs^\omega = \{PID^1_i, PID^2_i, \ldots, PID^l_i\} \) and the relevant long-term certificate \( (r_i, s_i) \) from the TA, where \( PID^l_i = TID_{veh_i} \oplus H(p_{sys}, q_{sys}) \) and \( l \in \{1, 2, \ldots, n\} \). Once enrolled vehicle wishes to broadcast a message, it selects one unused pseudonym-ID for purpose of concealment its true identity. Consequently, for any third party, the true identity of the vehicle is hard to reveal by capturing the messages sent. Thus, the proposed MSR-DoS scheme ensures pseudonym privacy-preserving in 5G-enabled vehicular networks.

- Unlinkable: The vehicle in the proposed MSR-DoS scheme publishes message-tuples \( (T_{msgi}, PID^1_i, R_i, U_i, T_i, \sigma_i) \) in 5G-enabled vehicular networks, where \( R_i = \omega^2 \cdot \theta^{-1} (mod \ n_{veh}) \), \( k = H(\omega), U_i = \text{MAC}_k(PID^1_i) \), \( \sigma_i = \text{Enc}_k(T_{msgi}, PID^1_i, r_i, s_i, T_i) \) and \( T_i \) is the freshness timestamp. Since the \( \omega \) is randomness, the malicious vehicle cannot link two or more messages sent by the same source. Thus, the proposed MSR-DoS scheme ensures unlinkability in 5G-enabled vehicular networks.

- Traceable: Once a report about malicious vehicles is received, the TA has the ability to trace her/his who issues the forge messages in 5G-enabled vehicular networks. For instance, suppose that one vehicle receives a forge message-tuples \( (T_{msgi}, PID^1_i, R_i, U_i, T_i, \sigma_i) \). Then the vehicle reports it to the TA through 5G-BS for tracing true identity of the vehicle. Once the TA receiving a forge message-tuples \( (T_{msgi}, PID^1_i, R_i, U_i, T_i, \sigma_i) \), it runs \( \text{MsgVerify} \) algorithm according to MSR operation to get \( (T_{msgi}, PID^1_i, r_i, s_i, T_i) \) from the forged message. If traffic-related message \( T_{msgi} \) is illegal, the TA has the ability to trace the sender of this message by computing the following equation.

\[
TID_{veh} = PID^1_i \oplus H(p_{sys}, q_{sys}) \tag{4}
\]

Therefore, its easy to distinguish the sender of the long-term certificate \( (PID^1_i, r_i, s_i) \). Hence, the proposed MSR-DoS scheme can ensure tracing of true identity \( TID_{veh} \) in 5G-enabled vehicular networks.

- Revocable: After vehicle is judged as malicious in the traceability process, the TA has the ability to revoke malicious vehicle from disrupt traffic condition in

| Table 1. Notations for BAN logic. |
|----------------------------------|
| Notations | Meaning |
| \( \rho \) and \( \varphi \) | Main participates |
| \( X_m \) | Messages |
| \( k \) | Share key |
| \( \rho \vdash X \) | \( \rho \) sees X |
| \( \rho \models X \) | \( \rho \) believes X |
| \( \rho \Rightarrow X \) | \( \rho \) controls X |
| \( \rho \l Morocco's BAN logic analysis proved that the mutual authentication among vehicles can be achieved. However, the proposed scheme requires additional steps for practical implementation. Could you provide a more detailed explanation of these steps and their implications? Respond in a way that emphasizes technical accuracy, while ensuring the explanation is accessible to a broad audience.
5G-enabled vehicular networks. The PRL of all revoked pseudonym-IDs is published by the TA. After revealing true identity of vehicle, the TA puts all pseudonym-IDs \( PID^*_l = \{ PID^l_1, PID^l_2, \ldots, PID^l_n \} \) into PRL, where \( PID^l_i = TID^{veh}_i \oplus H(p_{sys}, q_{sys}) \) and \( l \in \{1, 2, \ldots\} \). Therefore, the long-term certificate is not used by the vehicle. Hence, the proposed MSR-DoS scheme can ensure revoking of pseudonym-IDs \( PID^*_l \) in 5G-enabled vehicular networks.

- **Resist to Forgery Attacks:** In order to forge enrolled vehicles, a legal final message-tuples \( (Tmsg_i, PID^l_i, R_i, U_i, T_i, \sigma_i) \) must be initially created by the third party. That is, the third party should have an valid the long-term certificate (\( PID^*_l \), \( r_i \), \( s_i \)). As previously stated, no third party has the capability to issue such long-term certificate without the knowledge of \( p_{sys} \) and \( q_{sys} \) or \( p_{veh} \) and \( q_{veh} \). Consequently, the forgery attack could be easily detected by enrolled vehicle through testing the long-term certificate. Hence, the forgery attacks could be withstood by the proposed MSR-DoS scheme.

- **Resist to Modify Attacks:** Since \( U_i \) is the main encrypted verification amount in the created final message tuple, it is hardness for the third party to decrypt it to get the plain-text of \( U_i \). Any alteration of the final message-tuples \( (Tmsg_i, PID^l_i, R_i, U_i, T_i, \sigma_i) \) can be discovered even the third party could measure new amounts \( R_i, U_i \). Hence, the modify attacks could be withstood by the proposed MSR-DoS scheme.

- **Resist to Replay Attacks:** In the proposed MSR-DoS scheme, a freshness timestamp \( T_i \) is included in the issued final message-tuples \( (Tmsg_i, PID^l_i, R_i, U_i, T_i, \sigma_i) \). Upon the third party replays a final message-tuples, the verifying vehicle could detect the replayed message by testing the timestamp \( T_i \) that is longer than the service’s expiration time. Hence, the replay attacks could be withstood by the proposed MSR-DoS scheme.

- **Resist to Man-In-The-model (MITM) Attacks:** According to above analyzed, no third party has the ability to intercept the communication among enrolled vehicles. Hence, the MITM attacks could be withstood by the proposed MSR-DoS scheme.

- **Resist to DoS Attacks:** There have various scholars that uses cryptographic operations with regard to EC and BP for signatures-verification method. However, these operations are considered as time-consuming operation in high density traffic conditions. The third party can launches DoS attacks to send a lot of useless messages for causing the network congestion or interference. None of the existing schemes based on EC or BP has the ability to verify all. Our MSR-DoS scheme uses only several lightweight operations, including hash operation, MAC operation, symmetric cryptographic operation, MSR operation and Montgomery operation [51], which satisfies a significant reduction with regard to cost of computation compared to other related schemes (the cost of simulation results can be provided in Section VI). Hence, the DoS attacks could be withstand by the proposed MSR-DoS scheme.

### VI. PERFORMANCE ANALYSIS AND COMPARISON

In this section, we analysis a performance evaluation in terms of computation and communication overheads and give a comparison with most recent existing schemes [41], [42], [43] for 5G-enabled vehicular networks. The scheme in this paper uses the experiment in [50] to run on a macOS High Sierra operation system consists of an Intel Core i5 processor with, 4 GB RAM and 1.6 GHz clock frequency. Before analyzing computation overhead, the underlying operation notation are defined in Table 2. This paper only considered the significant operations of the cryptography, and did not include negligible operations such as XOR.

#### A. OVERHEAD OF COMPUTATIONAL

In this subsection, we analysis and compare the computational overhead of pseudonym-based schemes of Alshudukhi et al. [41], Cui et al. [42], Zhang et al. [43] and Bansal et al. [40] with the proposed MSR-DoS scheme for 5G-enabled vehicular networks. Table 3 summarizes computational overhead comparison and also presented in Figure 3.

The signer of scheme of Alshudukhi et al. [41] needs to add two operations of scalar multiplication \( 2T_{ecc-sm} \) associated with ECC and two hash function operations \( 2T_h \) to the MsgSign phase for singing message. Accordingly, the entire overhead of computational in the MsgSign phase of scheme of Alshudukhi et al. [41] is \( 2T_{ecc-sm} + 2T_h \approx 12.258 \) ms. While, the verifier in the MsgVerify phase of scheme of Alshudukhi et al. [41] requires to run three operations of scalar multiplication \( 3T_{ecc-sm} \) associated with ECC, one operation of addition point \( T_{ecc-ad} \) and two hash function operations \( 2T_h \) to verify message. Accordingly, the entire overhead of computational in the MsgVerify phase of scheme of Alshudukhi et al. [41] is \( 3T_{ecc-sm} + T_{ecc-ad} + 2T_h \approx 18.398 \) ms.

The signer of scheme of Cui et al. [42] needs to add three operations of scalar multiplication \( 3T_{ecc-sm} \) associated with ECC, one operation of addition point \( T_{ecc-ad} \) and

### TABLE 2. Runtime of different cryptographic operations [50].

| Operations       | Description                                      | Time (ms) |
|------------------|--------------------------------------------------|-----------|
| \( T_{ecc-sm} \) | The runtime of scale multiplication operation    | 6.128     |
| \( T_{ecc-ad} \) | The runtime of point addition operation according to ECC. | 0.012     |
| \( T_{rsr} \)   | The runtime of a MSR operation according to Equation (3). | 0.076     |
| \( T_{mac} \)   | The runtime of MAC operation.                    | 0.002     |
| \( T_{mont} \)  | The running time of Montgomery [51] operation, for instance \( R_i = c^{q-2} \text{ (mod } n_{veh}) \). | 0.033     |
| \( T_{enc-a} \) | The runtime of an encryption operation according to AES algorithm. | 0.006     |
| \( T_{dec-a} \) | The runtime of a decryption operation according to AES algorithm. | 0.003     |
| \( T_h \)       | The runtime of general hash function.            | 0.001     |
three hash function operations $3T_h$ to the MsgSign phase for singing message. Accordingly, the entire overhead of computational in the MsgSign phase of scheme of Cui et al. [42] is $3T_{ecc-sm} + T_{ecc-ad} + 3T_h \approx 18.399$ ms. While, the verifier in the MsgVerify phase of scheme of Cui et al. [42] requires to run three operations of scalar multiplication $3T_{ecc-sm}$ associated with ECC, one operation of addition point $T_{ecc-ad}$ and two hash function operations $2T_h$ to verify message. Accordingly, the entire overhead of computational in the MsgVerify phase of scheme of Cui et al. [42] is $3T_{ecc-sm} + T_{ecc-ad} + 2T_h \approx 18.398$ ms.

The signer of scheme of Zhang et al. [43] needs to add two operations of scalar multiplication $2T_{ecc-sm}$ associated with ECC, two operations of addition point $2T_{ecc-ad}$ and one hash function operation $1T_h$ to verify message. Accordingly, the entire overhead of computational in the MsgVerify phase of scheme of Zhang et al. [43] is $2T_{ecc-sm} + 2T_{ecc-ad} + 1T_h \approx 12.281$ ms. While, the verifier in the MsgVerify phase of scheme of Zhang et al. [43] requires to run two operations of scalar multiplication $2T_{ecc-sm}$ associated with ECC, two operations of addition point $2T_{ecc-ad}$ and one hash function operation $1T_h$ to verify message. Accordingly, the entire overhead of computational in the MsgVerify phase of scheme of Zhang et al. [43] is $2T_{ecc-sm} + 2T_{ecc-ad} + 1T_h \approx 12.281$ ms.

The signer of scheme of Bansal et al. [40] needs to add one operation of scalar multiplication $1T_{ecc-sm}$ associated with ECC, one operation of addition point $1T_{ecc-ad}$ and one hash function operation $1T_h$ to verify message. Accordingly, the entire overhead of computational in the MsgVerify phase of scheme of Bansal et al. [40] is $1T_{ecc-sm} + 1T_{ecc-ad} + 1T_h \approx 6.141$ ms. While, the verifier in the MsgVerify phase of scheme of Bansal et al. [40] requires to run one operation of scalar multiplication $1T_{ecc-sm}$ associated with ECC and one operation of addition point $1T_{ecc-ad}$ to verify message. Accordingly, the entire overhead of computational in the MsgVerify phase of scheme of Bansal et al. [40] is $1T_{ecc-sm} + 1T_{ecc-ad} \approx 6.14$ ms.

To sign message in the MsgSign phase of the proposed MSR-DoS scheme, the vehicle requires to run one MAC operation $T_{mac}$, one Montgomery operation $T_{mont}$, one decryption operation $T_{dec-a}$ and five general hash functions $T_h$. Thereby, the entire computational overhead in the MsgVerify phase of the proposed MSR-DoS scheme is $T_{mac} + T_{mont} + T_{dec-a} + 5T_h \approx 0.002 + 0.003 + 0.006 + 0.001 \approx 0.012$ ms. To verify message in the MsgVerify phase of the proposed MSR-DoS scheme, the vehicle requires to run one MAC operation $T_{mac}$, one Montgomery operation $T_{mont}$, one MSR operation $T_{msr}$, one decryption operation $T_{dec-a}$ and five general hash functions $T_h$.

### B. OVERHEAD OF COMMUNICATION

In this subsection, we analysis and compare the communication overhead of pseudonym-based schemes of Alshudukhi et al. [41], Cui et al. [42], Zhang et al. [43], and Bansal et al. [40] with the proposed MSR-DoS scheme for 5G-enabled vehicular networks. We assume that the final sizes of a timestamp and a general hash function be 4 bytes, and 20 bytes, respectively. Besides, the final size of MSR operation and ECC operation are 20 bytes and 64 bytes, respectively.

The vehicle in scheme of Alshudukhi et al. [41] broadcasts $(PsID_i^1, PsID_i^2, m_i, T_{Si}, \sigma_m)$ to other vehicles, where $PsID_i^j \in G$, $PsID_i^2$ and $\sigma_m \in Z_q^*$ and $T_{Si}$ is one freshness timestamp. The whole overhead of communication in scheme of Alshudukhi et al. [41] is $64 + 20 + 20 + 4 = 108$ bytes. While vehicle in our
TABLE 5. Communication overhead comparison.

| Schemes                      | Message Tuples                                                                 | Single Size | Batch Sizes |
|------------------------------|--------------------------------------------------------------------------------|-------------|-------------|
| Alkadad et al. (2021) [41]   | \( (\text{PID}^1, \text{PID}^2, R^1, U^1, T^1) \)                             | 108 bytes   | 108 bytes   |
| Cui et al. (2020) [42]       | \( (\text{PID}^1, \text{PID}^2, D^1, T^1) \)                                 | 172 bytes   | 172 bytes   |
| Zhang et al. (2020) [43]     | \( (\text{PID}^1, \text{PID}^2, F^1, G^1, \sigma_1) \)                       | 220 bytes   | 220 bytes   |
| Bansal et al. (2022) [40]    | \( (\text{PID}^1, R^1, U^1, T^1) \)                                          | 140 bytes   | 140 bytes   |
| Our MSR-DoS                  | \( (\text{Msg}^1, \text{PID}^1, R^1, U^1, T^1, \sigma_1) \)                  | 84 bytes    | 84 bytes    |

FIGURE 4. Comparison of communication overhead.

work broadcasts \( (\text{Msg}^1, \text{PID}^1, R^1, U^1, T^1, \sigma_1) \) to other, where \( \text{PID}^1, R^1, U^1, \sigma_1 \) \( \in \mathbb{Z}_q^* \) and \( T^1 \) is one timestamp. The whole overhead of communication in our work is \( 20 + 20 + 20 + 4 = 84 \) bytes.

Similarity, the overhead of communication of our work is lower than those in [42], [43], and [40], respectively. Table 5 tabulated a summary of the overhead of communication and also presented in Figure 4.

VII. CONCLUSION

This paper has proposed an MSR-DoS scheme that achieves communication security among vehicles in terms of privacy-preserving and security attacks. Our work is based on modular square root (MSR) and could be utilised to establish a communication security for 5G-enabled vehicular networks. The mutual authentication of this work has proven the security by using BAN logic. Furthermore, this work has shown that the scheme satisfies the security requirements in terms of authenticity of source, integrity of message, pseudonym privacy-preserving, unlinkable, traceable, and revocable. The traffic status message shared by vehicles works with low communication and computational costs.

In future work, we extend this work by adding a new component called fog computing instead of cloud computing to update parameters between vehicles and TA. Additionally, we extend this work by supporting batch verification process to check several messages simultaneously. Finally, the simulation experiments will be carried out by using network simulator (OMNeT++) and traffic simulator (SUMO).

ACKNOWLEDGMENT

We would like to acknowledge the Universiti Sains Malaysia for funding this research.

REFERENCES

[1] M. A. Al-Shareeda, S. Manickam, B. A. Mohammed, Z. G. Al-Mekhlafi, A. Qais, A. J. Alzahrani, G. Alshammar, A. N. Salam, and K. Almekhlafi, “Provably secure with efficient data sharing scheme for fifth-generation (5G)-enabled vehicular networks without road-side unit (RSU),” Sustainability, vol. 14, no. 16, p. 9961, Aug. 2022.
[2] C. Lin, D. He, X. Huang, N. Kumar, and K. K. R. Choo, “BCPPA: A blockchain-based conditional privacy-preserving authentication protocol for vehicular ad hoc networks,” IEEE Trans. Intell. Transp. Syst., vol. 20, no. 12, pp. 7408–7420, Dec. 2020.
[3] M. A. Al-Shareeda, S. Manickam, B. A. Mohammed, Z. G. Al-Mekhlafi, A. Qais, A. J. Alzahrani, G. Alshammar, A. N. Salam, and K. Almekhlafi, “CM-CPA: Chaotic map-based conditional privacy-preserving authentication scheme in 5G-enabled vehicular networks,” Sensors, vol. 22, no. 13, p. 5026, Jul. 2022.
[4] J. Ma, T. Li, J. Cui, Z. Ying, and J. Cheng, “Attribute-based secure announcement sharing among vehicles using blockchain,” IEEE Internet Things J., vol. 8, no. 12, pp. 10873–10883, Jul. 2021.
[5] M. A. Al-Shareeda and S. Manickam, “Man-in-the-middle attacks in mobile ad hoc networks (MANETs): Analysis and evaluation,” Symmetry, vol. 14, no. 8, p. 1543, Jul. 2022.
[6] H. Zhong, L. Chen, J. Cui, J. Zhang, I. Bolodurina, and L. Liu, “Secure and lightweight conditional privacy-preserving authentication for fog-based vehicular ad-hoc networks,” IEEE Internet Things J., vol. 9, no. 11, pp. 8485–8497, Sep. 2022.
[7] M. A. Al-Shareeda, M. Anbar, I. H. Hashbullah, and S. Manickam, “Survey of authentication and privacy schemes in vehicular ad hoc networks,” IEEE Sensors J., vol. 21, no. 2, pp. 2422–2433, Jan. 2021.
[8] X. Cheng, R. Zhang, S. Chen, J. Li, L. Yang, and H. Zhang, “5G enabled vehicular communications and networking,” China Commun., vol. 15, no. 3, pp. 3–6, Jul. 2018.
[9] K. N. R. S. V. Prasad, E. Hossain, and V. K. Bhargava, “Energy efficiency in massive MIMO-based 5G networks: Opportunities and challenges,” IEEE Wireless Commun., vol. 24, no. 3, pp. 86–94, Jun. 2017.
[10] H. Wyneers, G. Secco-Granados, G. Destino, D. Dardari, and F. Tufvesson, “5G mmWave positioning for vehicular networks,” IEEE Wireless Commun., vol. 24, no. 6, pp. 80–86, Dec. 2017.
[11] J. Cui, F. Ouyang, Z. Ying, L. Wei, and H. Zhong, “Secure and efficient data sharing among vehicles based on consortium blockchain,” IEEE Trans. Intell. Transp. Syst., vol. 23, no. 7, pp. 8857–8867, Jul. 2022.
[12] J. Zhang, H. Zhong, J. Cui, Y. Xu, and L. Liu, “SMAMC: Secure many-to-many authentication and key agreement scheme for vehicular networks,” IEEE Trans. Inf. Forensics Security, vol. 16, pp. 1810–1824, 2020.
[13] M. A. Al-Shareeda, M. Anbar, S. Manickam, and I. H. Hashbullah, “SECPPA: A secure and efficient conditional privacy-preserving authentication scheme in vehicular ad-hoc networks,” Sensors, vol. 21, no. 24, pp. 8206, Dec. 2021.
[14] P. Cincilla, O. Hicham, and B. Charles, “Vehicular PKI scalability-consistency trade-offs in large scale distributed scenarios,” in Proc. IEEE Veh. Netw. Conf. (VNC), Dec. 2016, pp. 1–8.
[15] D. Huang, S. Misra, M. Verma, and G. Xue, “PACP: An efficient pseudonymous authentication-based conditional privacy protocol for VANETs,” IEEE Trans. Intell. Transp. Syst., vol. 16, no. 3, pp. 736–746, Sep. 2015.
[16] A. Joshi, P. Gaonkar, and J. Bapat, “A reliable and secure approach for efficient car-to-car communication in intelligent transportation systems,” in Proc. Int. Conf. Wireless Commun., Signal Process. Netw. (WiSPNET), Mar. 2017, pp. 1617–1620.
[17] R. Lu, X. Liu, T. Luan, X. Liang, and X. Shen, “Pseudonym changing at social spots: An effective strategy for location privacy in VANETs,” IEEE Trans. Veh. Technol., vol. 61, no. 1, pp. 86–96, Jan. 2011.
[18] T. Thenmozhi and R. M. Somasundaram, “Pseudonyms based blind signature approach for an improved secured communication at social spots in VANETs,” Wireless Pers. Commun., vol. 82, no. 1, pp. 643–658, May 2015.
