sensors

MDPI

*Article*

# On a Blockchain-Based Security Scheme for Defense against Malicious Nodes in Vehicular Ad-Hoc Networks

**Guandong Liu [1], Na Fan [2], Chase Q. Wu [3,*] and Xiaomin Zou [2]**

[1] School of Economics and Management, Chang'an University, Xi'an 710064, China; liuguandong@chd.edu.cn
[2] School of Information Engineering, Chang'an University, Xi'an 710064, China; fnsea@chd.edu.cn (N.F.); 2020124138@chd.edu.cn (X.Z.)
[3] Department of Data Science, New Jersey Institute of Technology, Newark, NJ 07102, USA
* Correspondence: chase.wu@njit.edu

**Abstract:** Vehicular ad-hoc networks (VANETs) aim to provide a comfortable driving experience. Sharing messages in VANETs can help with traffic management, congestion mitigation, and driving safety. However, forged or false messages may undermine the efficiency of VANETs. In this paper, we propose a security scheme based on blockchain technology, where two types of blockchain are constructed based on roadside units (RSUs) and Certificate Authorities (CAs), respectively. The proposed security scheme has multifold goals to identify malicious nodes and detect forged messages based on multiple factors, such as reputation of sender nodes, and time and distance effectiveness of messages. In addition, an incentive mechanism is introduced on the RSU blockchain to encourage RSUs to adopt active behaviors. Extensive simulations show that the proposed scheme exhibits superior performances to existing methods in detecting forged messages and identifying malicious nodes. Meanwhile, it provides privacy protection and improves the efficiency of vehicular networks.

**Keywords:** vehicular networks; detection of messages; blockchain; consensus mechanism; privacy protection

check for updates

**Citation:** Liu, G.; Fan, N.; Wu, C.Q.; Zou, X. On a Blockchain-Based Security Scheme for Defense against Malicious Nodes in Vehicular Ad-Hoc Networks. *Sensors* **2022**, *22*, 5361. https://doi.org/10.3390/s22145361

Academic Editor: Peter Han Joo Chong

Received: 17 June 2022
Accepted: 14 July 2022
Published: 18 July 2022

## 1. Introduction

It is estimated that the total number of registered vehicles will reach two billion within the next 10 to 20 years [1]. Vehicular ad-hoc networks (VANETs) has been considered as the foundation of an intelligent transportation system (ITS) to improve transportation efficiency and ensure the safety of both vehicles and drivers. There are two types of communications in VANETs, namely, vehicle-to-vehicle (V2V) communication and vehicle-to-infrastructure (V2I) communication, which are carried out to facilitate cooperation and sharing among vehicles and RSUs.

Compared with the traditional networks, VANETs has its own unique characteristics, such as dynamic topology, high mobility and volatility, which render it vulnerable to various types of attacks from malicious vehicular nodes. Malicious nodes behave in different ways. For example, they may broadcast false information, which causes traffic jams or threatens drivers' lives; they may intentionally drop a received message or refuse to help other vehicular nodes' forward messages. Therefore, it has become an important yet practical problem to identify malicious nodes and detect forged messages in VANETs.

There exist many solutions in the literature, which can be divided into three categories. (i) Entity-oriented trust models, which evaluate the trustworthiness levels of vehicle nodes to identify selfish or malicious nodes [2,3]. (ii) Data-oriented trust models, which detect malicious nodes by evaluating the trustworthiness of messages [4]. (iii) Hybrid trust models, which combine both entity-oriented and data-oriented methods [5]. In addition, some security certification schemes have been proposed to determine the legitimacy of a vehicle node, such as the methods based on frequency identification [6], anonymous certificates [7,8] and group signature [9,10].

Blockchain is the underlying technology for the Bitcoin protocol that emerged in 2008 [5]. Blockchain provides a secure shared database as a ledger or log of transactions, without requiring a central trusted party for management. The consistency of blockchain is guaranteed through a distributed consensus protocol, where a set of participants (validators), in a trust-less, peer-to-peer network, collaborate in a completely transparent way to accept only valid transactions. These significant features of blockchain make it an excellent candidate for establishing a desirable trust model in VANETs. However, the original design goal of Bitcoin did not consider the privacy of nodes. By reviewing the ledger, the transactions made with any public key are traceable to a real identity.

Considering the characteristics of blockchain, we propose a security scheme to identify malicious nodes and detect forged messages based on the technology of blockchain while simultaneously preserving the identity privacy of vehicles.

In particular, compared with the existing methods, our work makes the following main contributions:

(1) We developed a blockchain-based security scheme for VANETs, where the blockchain on RSUs is able to identify malicious nodes and detect forged messages, and the blockchain on CAs is able to issue and revoke certificates for vehicles.

(2) We designed an incentive consensus mechanism on RSUs to encourage cooperative behaviors using award and punishment measures.

(3) Combined with the storage characteristics of blockchain, we designed a public–private key pseudonym strategy to protect the privacy of vehicles.

The rest of this paper is organized as follows. In Section 2, we summarize the related work. In Section 3, we formulate the problem under study. Section 4 details the proposed scheme. Section 5 presents and analyzes the simulation results. We conclude our work in Section 6.

## 2. Related Work

Differently from mobile ad hoc networks (MANETs), VANETs have several unique characteristics which make it challenging to design an effective scheme to identify malicious nodes and detect forged messages. First of all, its characteristic of high mobility makes it unpractical to maintain long-term interactions between vehicular nodes. Secondly, the topology of VANETs is subject to constant, rapid changes. Thirdly, application scenarios of VANETs are complicated and varying over time. A desirable scheme should function efficiently at any level of traffic density and preserve the privacy of vehicular nodes simultaneously.

In this section, we present a survey of the existing methods for identifying malicious nodes in VANETs and discuss the applications of blockchain in VANETs.

### *2.1. Detection Models in VANETs*

The detection methods in VANETs fall into three categories. The first category is based on entity-oriented trust models to identify malicious nodes and permanently or temporarily prevent them from transmitting or forwarding any information.

Gong et al. [11] proposed a social-contribution-based routing protocol for vehicular networks with selfish nodes. The protocol considers two factors when making a forwarding decision, namely, the probability of delivery to the destination and the social contribution of the relay node. A node with a low social contribution and a high probability of delivery is preferred as the next hop node. Sedjelmaci et al. [12] proposed an efficient and lightweight intrusion detection mechanism in vehicular networks. This mechanism can not only detect internal and external attacks, but also defend against denial of service (DoS) attacks, integrity targets, and false alarm attacks. Compared with the contemporary detection schemes, it only uses cryptography algorithms to protect vehicular networks from external attacks.

Further efforts have been made over years in this direction. Khan et al. [13] proposed a new scheme named DMN for detecting malicious nodes in VANETs. The proposed scheme is node-centric and uses a monitoring approach to identify and isolate malicious nodes. DMN is an optimized DMV algorithm and considers multiple parameters to select a certain node as the verifier node. Haddadou et al. [14] proposed a distributed VANETs trust model named DTM2 and used a Markov chain for modeling. In this model, malicious nodes can be detected and evicted by a self-selection algorithm among network nodes. Moreover, the cooperative level of selfish nodes is improved by giving rewards to those nodes that enact active and cooperative behaviors. Bali et al. [15] proposed a novel secure clustering scheme for efficient data dissemination in VANETs. In order to calculate the trust between different devices, a trust metric is proposed based on the dynamic transmission characteristics of vehicles. On the basis of this trust metric, the proposed scheme designs secure clustering and trust establishment.

In entity-oriented trust methods, excluding malicious nodes from any operation may lead to disconnection and other issues. Many researchers believe that constructing trust in data is practically more useful than reporting on their nodes. Data are the foundation of applications in VANETs. Sharing trustworthy, safe and efficient data are critical to the performance of transportation. Therefore, the second category of methods focus on identifying the trustworthiness of data.

Shaikh et al. [16] proposed a decentralized trust management scheme for vehicular ad-hoc networks based on identity and anonymity, which can detect false location and false timestamp information. Gurung et al. [17] proposed a new trust model that can directly evaluate the credibility of message contents received from other vehicles. Various factors, such as content similarity, content conflict and route similarity, are considered to construct the trust model. Mohamed et al. [18] proposed a new voting-based enhancement algorithm (EVA) to improve the security of DSRC applications. The proposed algorithm reduces the time for decision making and increases the reliability of applications, but increases the delay and computational overhead of OBU. Alturkostan et al. [19] used a threshold-based method to check the security of messages and analyzed the impact of jamming attacks on the security scheme. On this basis, they proposed a new adaptive threshold algorithm that can effectively resist jamming.

The third category, defined as hybrid trust models, aim to ensure reliable communication between nodes and prevent malicious nodes from interfering with them. Therefore, the main goals of these models are to maintain communications, revoke suspicious nodes and stop malicious messages.

Saneeha et al. [20] proposed a trust model to evaluate the reliability of recommendations in VANETs. The trust model can effectively alleviate recommendation attacks and help nodes to identify malicious senders and incorrect recommendations. Yao et al. [21] proposed an entity-centered dynamic trust model to adapt to the dynamic environment in VANETs. In order to balance direct trust and recommendation, a dynamic adjustment factor $\alpha$ is introduced. The proposed trust model can evaluate the reliability of data. Li et al. [22] proposed an anti-attack trust management scheme (ART) for VANETs, which can detect and mitigate malicious attacks. It also considers the reliability of data and vehicle nodes in VANETs. Moreover, this trust scheme is not only suitable for a wide range of VANETs applications, but also can improve traffic efficiency. Ahmed et al. [23] proposed the notion of logistic trust to detect misbehavior in VANETs. In this scheme, the receiver uses the suggestions received from other nodes as its observation results, and then identifies the correctness of the information according to its own observation results and the trustworthiness of the sender. Sedjelmac et al. [24] proposed an accurate, lightweight framework for intrusion detection named AECFA, which is an improved algorithm based on security clustering and can detect dangerous attacks in VANETs. Sanjay et al. [25] proposed VSRP for communication between vehicles based on reputation evaluation systems. It is a stable and efficient method to detect malicious nodes in VANETs.

### *2.2. Applications of Blockchain in Vehicle Networking*

Blockchain technology is an emerging distributed storage technology. The decentralized consensus mechanism used in blockchain effectively improves the security and privacy of the system, and brings considerable convenience to data exchange between connected smart devices. It has found many applications in various fields, especially in vehicular networks, for various purposes, such as data storage, identity authentication, privacy protection, and security trust. We summarize some of the typical security models based on blockchain technology in vehicular networks as follows.

Arora et al. [26] proposed an authentication and secure data transmission algorithm for Internet of Vehicles (IoV) using blockchain technology. This method can manage and calculate the trust of nodes in IoV and ensure secure communications between nodes. Lu et al. [27] proposed a blockchain-based anonymous reputation system (BARS) and established a privacy protection trust model in VANETs. To improve vehicle safety, it also integrates a reputation evaluation algorithm that relies on direct historical interactions and indirect opinions about vehicles. Yang et al. [28] proposed a decentralized trust management system for vehicular networks using blockchain technology. This method calculates the trust value based on Bayesian inference model to perform message verification, and all RSUs maintain and update the trust blockchain. Yang et al. [29] proposed a blockchain-based traffic event verification framework (BTEV) to complete event verification and alarm vehicle nodes near RSUs, and introduced a proof-of-event consensus mechanism (PoE), which can identify malicious behaviors and prevent the spread of false warning information. Wagner et al. [30] proposed a blockchain-based VANET framework which changes the transaction verification mechanism and management process of blockchain, and adds a trusted CA. This framework can realize the verification of traffic events without the assistance of RSUs and other infrastructures.

Malikl et al. [31] proposed a blockchain-based authentication and fast revocation framework for VANETs, which preserves vehicle nodes' anonymity without revealing their real identities, and reduces the dependence on authentication and the computing, and the communication overhead. In addition, it also realizes the rapid updating of the status of revoked vehicles in the blockchain shared ledger. Lu et al. [32] proposed a blockchain-based anonymous reputation system (BARS), which uses two blockchains (CerBC and RevBC) to achieve authentication and revocation transparency, and designed a reputation management algorithm based on historical interaction and indirect opinion to prevent the spread of false messages. In addition, public keys are used as communication pseudonyms to protect the privacy of vehicle nodes. Khan et al. [33] proposed a blockchain-based security architecture that can prevent attacks in VANETs, such as denial of service (DoS) attacks, Sybil attacks, impersonation attacks, and replay attacks. This work designed a message rating and trust method based on blockchain to ensure the security and privacy of vehicle nodes. Li et al. [34] proposed a distributed architecture-based blockchain for VANETs, which has advantages in identity and privacy protection. The proposed architecture includes blockchain setup, registration of vehicles, SBMs upload, and blockchain record. It can effectively solve the problem of trust between entities and centralized deployment. Javaid et al. [35] proposed a distributed trust management scheme based on blockchain to achieve secure message sharing and privacy protection between vehicles in VANETs. It assigns a unique encrypted fingerprint to each vehicle, and a CA is used to eliminate the linkage between public key and real identity to protect the identities of vehicle nodes from attacks. Dai et al. [36] proposed a security framework based on reinforcement learning and blockchain, which firstly uses the blockchain to protect messages from tampering and records the trust of vehicle nodes on the blockchain, and then selects reliable intermediate nodes by using reinforcement learning.

In summary, the existing methods have been proven to be effective and successful in their targeted applications, but still face some technical challenges, including improving the accuracy of detection and enhancing protection of privacy. Therefore, we propose a security scheme based on blockchain technology to identify malicious nodes and detect forged messages. Meanwhile, we address the issue of privacy protection for vehicles and designed an incentive mechanism to encourage cooperative behaviors of RSUs. Additionally, the proposed security scheme enables decentralized management in vehicle networks and effectively reduces network overheads.

## 3. Problem Statement

In this section, we present application scenarios in VANETs, construct a model of VANETs based on blockchain, and define the objectives of our design.

### *3.1. Application Scenarios in VANETs*

Generally, there are two types of communications in VANETs: vehicle to vehicle (V2V) and vehicle to infrastructures (V2I). Vehicle nodes equipped with sensors communicate with each other. They are able to send, transmit, and share various types of data, such as traffic condition, service information, and entertainment information. Vehicle nodes are also able to communicate with RSUs. Sharing information, especially traffic safety-related messages, is fundamental for vehicles in VANETs.

However, malicious vehicle nodes in VANETs may send forged messages for their own interests. In Figure 1, a malicious vehicle node sends a forged message that reports a crash accident ahead to its neighbor nodes. When a normal node receives the forged message, it will modify its original driving route accordingly. Such false information may affect the drivers' judgment and endanger the safety of driving. Therefore, identifying forged messages and malicious vehicle nodes is the basis of secure communication in VANETs.

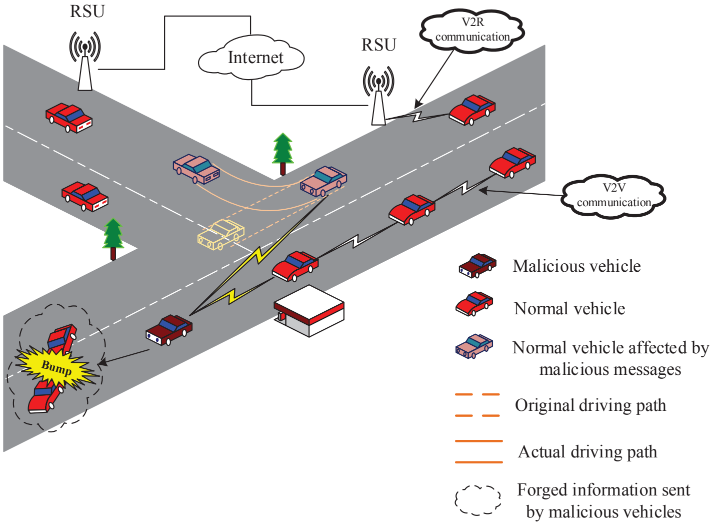

**Figure 1.** A scenario with malicious nodes in vehicular networks.

In this paper, we propose a security scheme based on blockchain to identify forged safety information (such as inclement weather broadcast, icy road, traffic jam, and traffic accident) and malicious vehicle nodes.

### *3.2. Blockchain-Based VANETs Model*

We propose to adopt the technology of blockchain in VANETs, as illustrated in Figure 2, where there are four types of entities: vehicle nodes, RSUs, Certificate Authority, and Law Enforcement Authority, as described below.

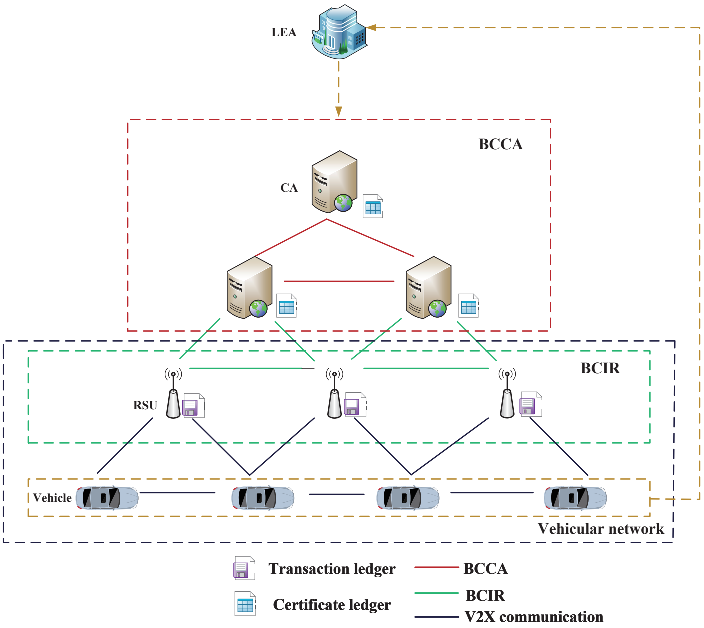

**Figure 2.** Blockchain-based vehicle networks.

- Law Enforcement Authority (LEA): The functions of LEA include registration of vehicles, authorization of a CA to issue certificates, etc.
- Certificate Authority (CA): A CA issues a certificate for a vehicle when it obtains a warrant from the LEA. All actions of a CA will be recorded transparently in the blockchain of CAs and can be verified by every CA in the VANETs.
- RSU: All broadcasted messages and transactions are verified by RSUs and then recorded in the RSU blockchain. The main functions of RSU include monitoring behaviors of vehicles and evaluating the reputation scores of each vehicle.
- Vehicles: Vehicles equipped with OBU devices are moving entities and communicate with each other to share various types of messages.

There are two blockchains in the proposed scheme:

(1) Blockchain for Certification on CA (BCCA)

BCCA acts as the public ledger for all issued certifications. All actions of a CA are recorded transparently in the BCCA. A transaction in the BCCA refers to a message broadcasted by a CA to issue or revoke a certificate. Each transaction contains the timestamp and the digital signature of the CA. In order to preserve the privacy of vehicles, no information linkable to the real identity is included in the transaction.

(2) Blockchain for Identification on RSU (BCIR)

BCIR acts as the public ledger for all transactions, which include identifying forged messages or malicious vehicle nodes among RSUs. All actions of a RSU are recorded transparently in the BCIR blockchain. A transaction in BCIR refers to a message broadcasted by a RSU, which is able to identify the trustworthiness of message sharing in VANETs, and also evaluate the behaviors of vehicles. The results of identification or evaluation are broadcasted and regarded as transactions.

BCCA and BCIR bring considerable convenience to data exchange between connected smart device, such as CAs or RSUs. In BCCA, the blockchain technology is able to secure assigning and revoking certifications for vehicles. In BCIR, the blockchain technology is able to secure management of vehicles' reputations and ensure secure communications between RUSs. Simultaneously, it also can help identify malicious nodes and detect forged messages.

Each vehicle registers with the LEA using its own real identity to ensure the traceability of malicious nodes. The CA assigns a certification to a vehicle if it achieves a warrant from the LEA. Certifications help vehicles construct trusted relationships when a vehicle communicates with other vehicles or RSUs.

In the framework illustrated in Figure 3, node $V_j$ receives a message sent by $V_i$. To assess the trustworthiness of the message, $V_j$ sends this message to the nearest RSU. To determine the legitimacy of $V_j$, the RSU sends $V_j$'s pseudonym to the nearest CA when it receives the message from $V_j$. As the blockchain of CA contains the linkages between the vehicles' pseudonyms and their real identities, the CA is able to identify whether or not $V_j$ is a legitimate node and sends the result of identification to the RSU. If $V_j$ is not a legitimate node, the RSU drops this message; otherwise, the blockchain of RSU evaluates the trustworthiness of the message and sends the result of evaluation to $V_j$.

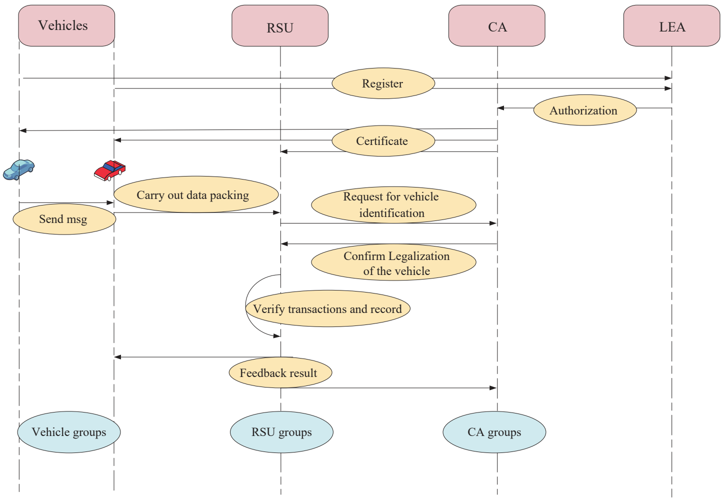

**Figure 3.** The flow chart of detection.

### 3.3. Design Objectives

Due to the unique characteristics of high mobility and limited connectivity, VANETs are prone to various types of cyber attacks from malicious vehicle nodes, which affect the efficiency of VANETs and threaten the safety of drivers. Towards this end, we propose a detection scheme based on a blockchain consensus mechanism following several design goals:

- The first goal was to address the problem of centralization in vehicular networks. Our work adopted blockchain technology to construct a novel decentralized architecture for vehicular networks.
- The second goal was to design a malicious node identification scheme based on an incentive consensus mechanism which is able to identify the legitimacy of a received message and detect malicious nodes by evaluating the trustworthiness of the source nodes. Meanwhile, the consensus is able to stimulate RSUs to enact active behaviors.

## 4. A Security Scheme Based on a Blockchain Consensus Mechanism

In this section we propose a blockchain-based security method, referred to as *BCSM*, and present its design details.

### 4.1. Assumption

Firstly, we give some necessary assumptions as the foundation of the proposed scheme.

(1) The adversary is not able to compromise more than a half of the vehicles in the network. This is a reasonable assumption in practice.
(2) Certification Authorities (CAs) and RSUs are equipped with customized hardware with high computing power.
(3) Cryptography technology provides a secure communication channel between entities as long as the secret key is not compromised.

### 4.2. Initialization of VANETs Based on Blockchain

Initially, each entity on BCCA and BCIR generates a pair of private and public keys. When a vehicle $V_i$ enters VANETs, it sends a message that contains its private information to prove its legitimate identification. If the message is valid, LEA sends a signed warrant to the CA, which then issues an initial certificate to vehicle $V_i$. LEA stores the received message in the database with high-level security, which will be used for tracking the vehicle's real identity in cases of disputes.

(1) Blockchain establishment: There are two blockchains set up during this stage. All CAs form a blockchain for certification, and all RSUs form a blockchain for identification. Each member of a blockchain is equal and has the same rights and obligations.
(2) Certification: $V_i$ registers with a CA for the first time by submitting its vehicle ID obtained from the LEA. The CA verifies the vehicle ID and issues a certification to $V_i$, which contains the expiration date, a pseudo-ID $PID_{V_i}$, the public–private keys, the signatures of authorities, and the initial reputation value assigned for $V_i$.

The blockchain of CA maintains a database, which stores the hash map of a mapping of pseudo-IDs of vehicles with the certificates. This blockchain ensures the traceability of issuing or revoking certificates.

### 4.3. Detection Scheme

Messages transmitted in VANETs are described in Table 1 and fall into three categories: beacon messages, alert messages, and entertainment messages. Alert messages are broadcast in an emergency and are critical to safe driving. Therefore, in this paper, we focus on how to detect forged alert messages based on the blockchain technology in VANETs. Alert messages normally report emergency situations described in Table 2, where $TTL_{event}$ and $Ran_{msg}$ denote life cycle and the longest transmission range of the event reported in an alert message, respectively. As shown in Table 2, alert messages are divided into four categories and have different life cycles.

As illustrated in Figure 4, the security scheme is comprised of four components: identification of the legitimacy of a vehicle; an incentive consensus mechanism; identification of forged messages and malicious vehicle nodes; and the public–private key mechanism and RSA encryption algorithm are adopted in the scheme to protect the security and privacy of vehicles. The ledgers of BCIR and BCCA in this scheme are illustrated in Figure 5.

**Table 1.** Message packet format.

| Abbreviation | Values |
|---|---|
| SouID | ID of source node |
| RecID | ID of destination node |
| RecTime | Received Time |
| EventTime | The exact time of occured event |
| Event Type | I/II/III/IV |
| $Loc_{event}$ | Location of event |
| $Loc_{vehicle}$ | Location of source node |
| $TTL_{event}$ | The life cycle of event |
| $Ran_{msg}$ | Transmission range of the message |

**Table 2.** Alert message classification.

| Event ID | Event Type | $TTL_{event}$ | $Ran_{msg}$ |
|---|---|---|---|
| I | Road jam | $Th_{t-I}$ | $Th_{d-I}$ |
| II | Road accident | $Th_{t-II}$ | $Th_{d-II}$ |
| III | Icy road | $Th_{t-III}$ | $Th_{d-III}$ |
| IV | Road construction | $Th_{t-IV}$ | $Th_{d-IV}$ |

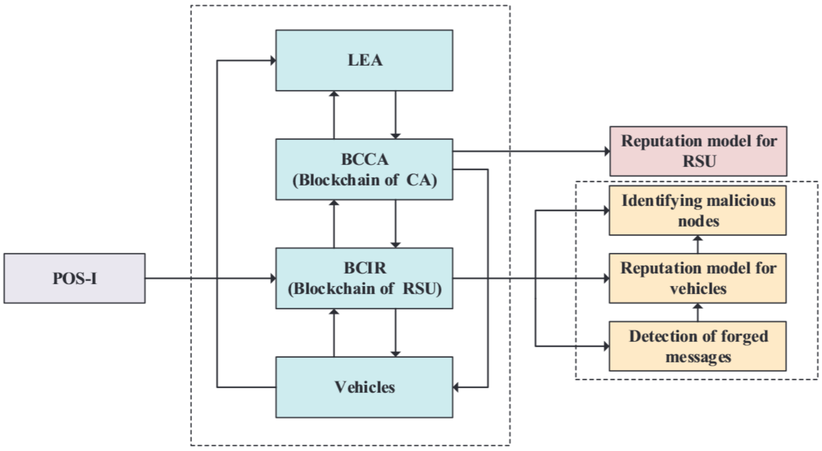

**Figure 4.** The scheme structure.

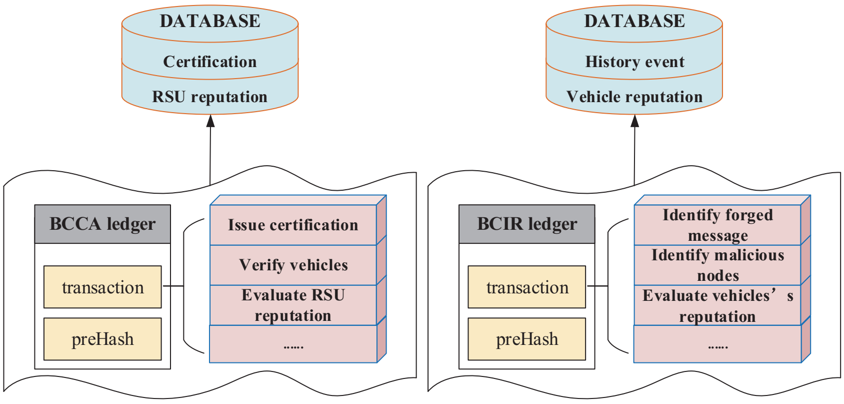

**Figure 5.** The ledgers of BCIR and BCCA.

(1) **Verify a vehicle's legal identification**

When $V_i$ receives an alert message from $V_j$, it sends the received message to a nearby RSU and requests it to identify the legitimacy of the message. The RSU checks if $V_i$ has a legal identification before evaluating the trustworthiness of the message. Algorithm 1 illustrates the steps to verify the identification of $V_i$. For secure communication, the RSA method is adopted in Algorithm 1.

Step 1: Vehicle $V_i$ sends a request to a RSU within its communication range to verify the message received from vehicle $V_j$. The request includes the received message, the pseudo-ID $PID_{V_i}$, and $PK_{V_i}$, which is the public key of $V_i$.

Step 2: After receiving the request, the RSU sends a message, which includes $PID_{V_i}$ and a random value $L$ to the closest CA. Note that $L$ is produced by the method of linear congruence generator (LCG), calculated as:

$$\begin{cases} L_0 = d \\ L_{r+1} = (A * L_r + Z) \mod (M)' \end{cases} \tag{1}$$

where $d$ is a seed value, and its initial value is set to be the current system time; $A$ is a multiplier; $Z$ is an increment value; and $M$ is a modulus. Note that $M$ and $Z$ are prime numbers to each other.

Step 3: When the CA receives the message from the RSU, it checks the ledger of BCCA. If $PID_{V_i}$ is stored in the ledger, then $V_i$ is a legitimate vehicle; otherwise, it is an illegitimate one. Then, a session key $k_s$ is created by the random value $L$ encrypted with the private key of the CA. $E_{PB_{RUS}}[k_s]$ is created by encrypting $k_s$ with the public key of the RSU $PB_{RSU}$ and $E_{k_s}[report]$ is created by encrypting the checking report with $k_s$. Finally, $E_{k_s}[report]$ and $E_{PB_{RUS}}[k_s]$ are encrypted with $PB_{RSU}$ and sent to the RSU. The encryption is performed as

$$E : C = E_{PB_{RSU}}\left[E_{PB_{RSU}}[K_s]||E_{K_s}[report]\right], \tag{2}$$

where $E$ is a function of encryption and $C$ represents the plaintext.

Step 4: When the RSU receives the encrypted result from the CA, it decrypts the result with its own $PK_{RSU}$ to obtain $E_{k_s}[report]$ and $E_{PB_{RUS}}[k_s]$. Then, the RSU decrypts $E_{PB_{RUS}}[k_s]$ with its $PK_{RSU}$ to obtain $k_s$. Finally, the report is created by decrypting $E_{k_s}[report]$ with $k_s$. This decryption process is described as

$$D : \left[E_{PB_{RSU}}[K_s]||E_{K_s}[report]\right] = D_{PB_{RSU}}[C], \tag{3}$$

where $D$ is a function of decryption.

**Algorithm 1** Verify a vehicle's legal identification

```
Input: $V_i$, $PIDV_i$, $PB_{RSU}$ and $PK_{CA}$ ;
Output verification result;
$V_i$ sends a request to BCIR;
LCG is used to produce $L$;
$L$ and $PIDV_i$ are sent to BCCA;
CA checks the ledger on BCCA;
if $PIDV_i$ is stored in the ledger then
    $V_i$ is a legal vehicle;
else
    $V_i$ is an illegal vehicle;
end if
Encrypt $L$ with $PK_{CA}$ as $K_s$;
Encrypt the verification result with $K_s$ as $E_{K_s}[report]$;
Encrypt $E_{K_s}[report]$ and $E_{PB_{RSU}}[K_s]$ with $PB_{RSU}$;
Send $E_{PB_{RSU}}[K_s]||E_{K_s}[report]$ to the RSU;
The RSU decrypts $E_{PB_{RSU}}[K_s]||E_{K_s}[report]$;
Output the verification result.
```

(2) **POS consensus with an incentive mechanism**

If $V_i$ is verified as a legitimate vehicle by the BCCA blockchain, the BCIR blockchain then identifies whether or not the message sent by $V_i$ was forged.

To stimulate the RSUs to take active behaviors, a consensus appropriate for VANETs should be constructed. Consensus in a blockchain is a process where all peers of the network reach a common agreement on the present state of the distributed ledger. At present, the most common consensus algorithms include POW, POS, and PBFT. From the advent of Bitcoin to today, there over 30 consensus algorithms have emerged [37], most of which are based on the above three consensus algorithms.

Unlike other traditional consensus, nodes in BCIR are designed to utilize computing power for forged message validation rather than merely solving the difficult hash problem. Therefore, we designed a novel consensus POS based on an incentive mechanism (POS-I) for BCIR in VANETs. According to the POS consensus with an incentive mechanism, when an RSU enacts active behavior, it receives energy benefit. POS-I is described in Algorithm 2.

**Algorithm 2** Consensus mechanism POS-I

```
Input: $Egy_o$, $k$, $Th_{Egy}$, $\Delta\mathrm{T}_{\mathrm{pos}}$, $a$, $J$, $Pr$;
Output committer peer;
RSU sends a request to CA;
BCCA initializes an election for selecting committer peer;
for all RSU participating in the election do
    $R_l$ submits $\Delta Egy_{consume\_l} = \frac{k}{2(k+1)} Egy_{o\_l}$ as deposit;
    Calculate $Egy_{e\_l} = Egy_{o\_l} - \Delta Egy_{consume\_l}$;
    if $Egy_{e\_l} < Th_{Egy}$ then
        $R_l$ cannot participate in the election;
    else
        $R_l$ is regarded as a candidate;
    end if
    Calculate $Stake_{R-l} = \sum_{x=1}^{J} Egy_x * (1 + a\%)^J$;
end for
Selecting the node whose has $Max_{stake}$ as the committer peer ;
Calculate $\Delta Egy_{reword} = \frac{1 - Egy_{J-1}}{2}$;
Calculate $Egy_J = Egy_{J-1} \times e^{\frac{1}{\Delta T_{J-1\_J}}} + \Delta Egy_{consume} \times Pr + \Delta Egy_{reword}$;
Output committer peer.
```

Step 1: BCCA initializes an election to select a committer peer. The RSUs, which would like to participate in the election, submit deposits in order to become candidates. The energy value of every candidate *RSU* is reduced as a deposit. The process of calculating deposit is described as:

$$\Delta Egy_{consume\_l} = \frac{k}{2(k+1)} Egy_{o\_l}, \tag{4}$$

where $\Delta Egy_{consume\_l}$ denotes the submitted deposit, $Egy_{o\_l}$ denotes the current energy value of $RSU_l$, $k$ denotes the total number of participation elections of $RSU_l$, and the initial value $k$ is set to zero.

RSUs have various types of behaviors in VANETs, such as broadcasting messages, participating election of selecting a committer peer, and identifying the trustworthiness of a message. Normally, the energy of a RSU changes with different behaviors. For example, when it broadcasts messages in VNAETs, its energy is consumed. Meanwhile, in order to encourage its active behaviors, it is also rewarded a certain energy. The reward is larger than the consumed energy.

After submitting the deposit, the energy of $R_l$ is updated as:

$$Egy_{e\_l} = Egy_{o\_l} - \Delta Egy_{consume\_l}. \tag{5}$$

Step 2: If the energy of $R_l$ is lower than $Th_{Egy}$, which is a threshold, $R_l$ is deleted from the candidate group; otherwise, it remains in the candidates group.

Step 3: The total number of elections initialized by BCCA is counted as $J$. After every election for a committer, the energy of every RSU on BCIR is updated. Stakes refer to the assets (or energy) owned by a node. The idea is that the more active behaviors an RSU has, the more stakes it owns. The stake of each RSU candidate is calculated as

$$Stake_{R-l} = \sum_{x=1}^{J} Egy_x * (1 + a\%)^J, \tag{6}$$

where $Stake_{R-l}$ denotes the stake of $R_l$, and $Egy_x$ denotes the energy value of $R_l$ after the $x$-th election. The RSU, which has the highest stake value among the candidate group, is selected as the committer peer.

Step 4: When the committer peer is selected according to the above process, BCCA refunds a certain percent of deposit to each candidate RSU. Now, BCCA updates all RSUs. The updating process is described as

$$Egy_J = Egy_{J-1} \times e^{\frac{1}{\Delta T_{J-1\_J}}} + \Delta Egy_{consume} \times Pr + \Delta Egy_{reword}, \tag{7}$$

where $Egy_J$ denotes the energy of a RSU after the $Jth$ election initialized by BCCA, $Egy_{J-1}$ denotes the energy of a RSU after the $(J-1)th$ election, and $P_r$ denotes a certain percent of deposit refunded. Especially, we set $e^{\frac{1}{\Delta T_{J-1\_J}}}$ to be an attenuation coefficient. Meanwhile, BCCA offers a reward $\Delta Egy_{reword}$ to the committer peer, calculated as

$$\Delta Egy_{reword} = \frac{1 - Egy_{J-1}}{2}. \tag{8}$$

As mentioned above, if $RSU_l$ is selected as a committer peer on BCIR, it gains the reward energy and be refunded at a certain percentage.

(3) **Verify the integrity of messages**

The RSU, which is elected as a committer peer, verifies the message integrity sent from $V_i$. Algorithm 3 describes the verification process for message integrity.

**Algorithm 3** Verify message integrity

```
Input: $PK_{committer}$, $PB_{committer}$ , $PK_{CA}$, $PB_{CA}$;
Output  Message integrity result;
Calculate the hash code $h(m)$ of $m$;
Encrypt $h(m)$ with the $PK_{committer}$ as the committer $RSU's$ digital signature;
Add the digital signature in the message $m$ to get $m'$;
Use LCG to get a random number $G$;
Encrypt G with the $PB_{committer}$ as $Committer_{K_s}$;
Encrypt $m'$ with $Committer_{K_s}$ as $E_{Committer_{K_s}}[m']$;
Encrypt $Committer_{K_s}$ with $PB_{CA}$ as $E_{PB_{CA}}[Committer_{K_s}]$;
Send $E_{Committer_{K_s}}[m']$ and $E_{PB_{CA}}[Committer_{K_s}]$ to BCCA;
CA decrypts $E_{PB_{CA}}[Committer_{K_s}]$ with $PK_{CA}$ to get $Committer_{K_s}$;
Decrypt $E_{Committer_{K_s}}[m']$ with $Committer_{K_s}$ to get digital signature;
Decrypt digital signature with $PB_{committer}$ to get $h(m)$;
CA on the message $m$ hashes to get $H(m)$;
if $h(m) = H(m)$ then
    the $m$ is verified as integrity;
else
    the $m$ is tampered;
end if
Output the message integrity result.
```

Step 1: The committer RSU on a message $m$ hashes to get the synopsis of $m$, which is denoted as $h(m)$. Then, $h(m)$ is encrypted with the committer RSU's private key $PK_{committer}$.

The result of encryption is considered as the committer RSU's digital signature and is added in the message $m$ to get $m'$.

Step 2: The committer RSU employs the LCG method to obtain a random number $G$, and a session key $Committer_{K_s}$ is created by encrypting $G$ with the committer RSU's public key $PB_{committer}$.

Step 3: $E_{Committer_{K_s}}[m']$, which is created by encrypting $m'$ with $Committer_{K_s}$, and $E_{PB_{CA}}[Committer_{K_s}]$ are sent to the CA, which is the closest to the RSU.

Step 4: The CA decrypts $E_{PB_{CA}}[Committer_{K_s}]$ with its private key $PK_{CA}$ to get $Committer_{K_s}$, and $E_{Committer_{K_s}}[m']$ is decrypted with $Committer_{K_s}$ to get $m$ and the committer RSU's digital signature.

Step 5: The committer RSU's digital signature is decrypted with $PB_{Committer}$ to get $h(m)$. The CA that is the closest to the RSU on the message $m$ hashes to get $H(m)$. If $h(m)$ is equal to $H(m)$, $m$ is verified as integrity.

(4) **Verify the legitimacy of messages.**

In our scheme, BCIR acts as a distributed public ledger, which stores the reputation values of every vehicle in the blockchain. BCIR first checks the sender vehicle $V_j$'s reputation and then verifies the trustworthiness of the message. If the reputation of $V_j$ is smaller than the reputation threshold $R_{threshold}$, the message from this node is labeled as forged information. Otherwise, BCIR checks the message based on the evidence with respect to $EventType$, $Loc_{event}$, $EventTime$, time effectiveness, and distance effectiveness.

As mentioned above, the committer RSU follows the message verification policies to determine the message's trustworthiness as follows:

- Check the sender's reputation from the vehicle reputation table on BCIR.
- Check $EventType$, $Loc_{event}$, and $EventTime$.
- Check time effectiveness and distance effectiveness.

If the sender's reputation is larger than $R_{threshold}$, $EventType$, $Loc_{event}$, and $EventTime$ of the received message are checked in the historical event table on BCIR in order to evaluate if an event reported in the message has been stored in the historical event table.

If $EventType$ of a message in the historical event table is the same as $m_{EventType}$, the message is placed in $S_m$, defined as $S_m = \{e_1, e_2, ..., e_z\}$, where $z$ denotes the total number of messages in $S_m$. For $e_q \in S_m$, the distance between $e_q$ and $m$ is calculated as:

$$Dis = \sqrt{(m_{xLoc_{event}} - e_{qx_{Loc_{event}}})^2 + (m_{y_{Loc_{event}}} - e_{qy_{Loc_{event}}})^2 + (m_{EventType} - e_{q_{EventType}})^2}, \tag{9}$$

where $m_{Loc_{event}} =< m_{xLoc_{event}}, m_{yLoc_{event}} >$, where $m_{xLoc_{event}}$ and $m_{yLoc_{event}}$ denote the longitude and latitude of $m$, respectively; and $e_{q_{Loc_{event}}}$ is defined as $< e_{qx_{Loc_{event}}}, e_{qy_{Loc_{event}}} >$, which denote the longitude and latitude of $e_q$, respectively. The similarity of $e_q$ and $m$ is calculated as

$$Sim_{e_q\_m} = \frac{1}{1 + Dis}. \tag{10}$$

If $Sim_{e_q\_m}$ is larger than $Th_{Sim}$, $m$ is considered to be the same as $e_q$, and it checks time effectiveness and distance effectiveness. Otherwise, $m$ is treated as a new one.

If $\Delta t$ is over $Th_t$, the distance effectiveness is checked; otherwise, it is dropped because it expires:

$$\begin{cases} \Delta t < Th_t, \\ \Delta t = RecTime - EventTime. \end{cases} \tag{11}$$

If $\Delta t$ is over $Th_d$, the message is dropped; otherwise, it is considered to be a reliable message:

$$\begin{cases} \Delta d < Th_d, \\ \Delta d = Loc_{vehicle} - Loc_{event}. \end{cases} \tag{12}$$

The process for identifying the trustworthiness of a message is illustrated in Algorithm 4.

**Algorithm 4** Verify the legitimacy of messages

```
Input: $R_{threshold}$, $Th_{Sim}$, $Th_t$, $Th_d$;
Output the legitimacy of messages;
For a message $m$;
if $R_{source} < R_{threshold}$ then
    $m$ is verified as a forged message;
end if
for all events recorded in historical event table on BCIR do
    Compare $EventType$ of the event with $m_{EventType}$;
    if $EventType$ of the event is the same as $m_{EventType}$ then
        Place the event in $S_m$;
        for all events in $S_m$ do
            Calculate $Sim = \frac{1}{1+Dis}, e_q \in S_m$;
            if $Sim > Th_{Sim}$ then
                The event in $m$ is the same as $e_q$ ;
            end if
        end for
    else
        Calculate $\Delta t = RecTime - EventTime$;
        if $\Delta t > Th_t$ then
            $m$ is outdated and discarded;
        else
            Calculate $\Delta d = Loc_{vehicle} - Loc_{event}$;
            if $\Delta d < Th_d$ then
                $m$ is a legitimate message;
            end if
        end if
    end if
end for
```

If the received message is valid and trustworthy based on the aforementioned policy, it is stored in the historical event table on BCIR and the sender vehicle's reputation is increased. Otherwise, the sender vehicle's reputation is decreased. When a vehicle's reputation value is below the threshold $R_V$, it is considered to be a malicious node. The reputation of $V_i$ is calculated as

$$R_{V_{j\_T}} = R_{V_{j\_T-1}} \times \frac{True_{msg\_T}}{Sum_{msg\_T}}, \quad (13)$$

where $R_{V_{j\_T}}$ represents the reputation value of $V_j$ in the time period $T$, $R_{V_{j\_T-1}}$ denotes $V_j$'s reputation in the time period $T-1$, and $Sum_{msg\_T}$ and $True_{msg\_T}$ represent the total numbers of messages and forged messages sent from $R_{V_j}$ in the time period $T$, respectively.

## 5. Simulation-Based Experiments and Performance Analysis

We present the performance evaluation of our proposed blockchain-based VANETs architecture in this section.

### *5.1. Simulation Environment*

Simulation System Setup

To test and optimize the performance of the security scheme, we used ONE to simulate the network. Meanwhile, the SUMO (Simulation of Urban Mobility) framework was used as the mobility generator to prototype inter-modal traffic systems.

The vehicles in the SUMO simulator are shown as the dynamic nodes in the ONE framework. We programmed their functionality and behavior while the movement utilized the built-in libraries and procedures. In the simulation-based experiments, we used the shortest path map-based movement model in ONE to simulate vehicle behaviors on the road. The model initially places the nodes at random locations, but selects specific destinations for all nodes in the map and uses Dijkstra's shortest path algorithm to find the shortest path to the destination.

There were two scenarios in the simulation experiments: low traffic density and high traffic density. As shown in Figure 6, the vehicle node performed simulated motion based on the Helsinki City map (Finland). The settings of the nodes are not arbitrary and include various types: emergency vehicles, such as police cars and ambulances; vehicles with fixed lines, such as buses and trams; and randomly distributed vehicles, such as private cars and taxis.

The specific simulation parameters are shown in Table 3. Each simulation is repeated twenty times to calculate the average. In our experiments, the number of malicious vehicles that sent forged or bogus messages in VANETs varied from 10% to 45%. When the malicious vehicles were over 45%, VANETs had drastically decreasing efficiency and could not provide any reliable services. Hence, we did not consider this extreme situation.

**Table 3.** Simulation parameter settings.

| **Parameter Description** | **Value** |
|---|---|
| Simulation area | 4500 m × 3400 m |
| Simulation time | 43,200 s |
| Mobility model | Shortest Path Map Based Movement |
| No. of groups | 11 |
| Number of nodes | 100; 400 |
| Transmission rage | 10 m |
| Node speed | 2 m/s |
| Warm-up period | 1000 s |
| Time to live | 300 |
| Buffer size | $5M$ |
| RSU quantity | 10 |
| Routing scheme | $ProphetRouter$ |
| $Egy_o$ | 0.5 |
| $Th_{Egy}$ | 0.3 |
| a | 5 |
| $Pr$ | 80% |

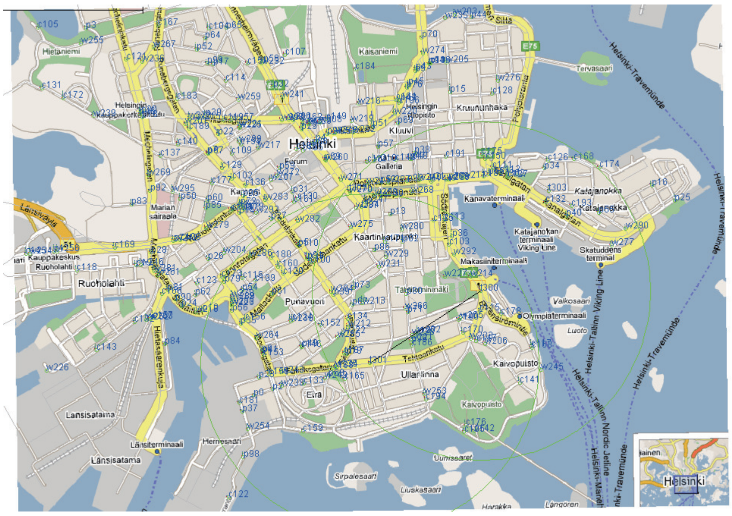

**Figure 6.** Helsinki City map (Finland).

Additionally, several fixed nodes are manually added to the map to function as RSU infrastructure. The locations of all nodes are shown in Figure 7, where we also identify the specific locations of the deployed RSUs.

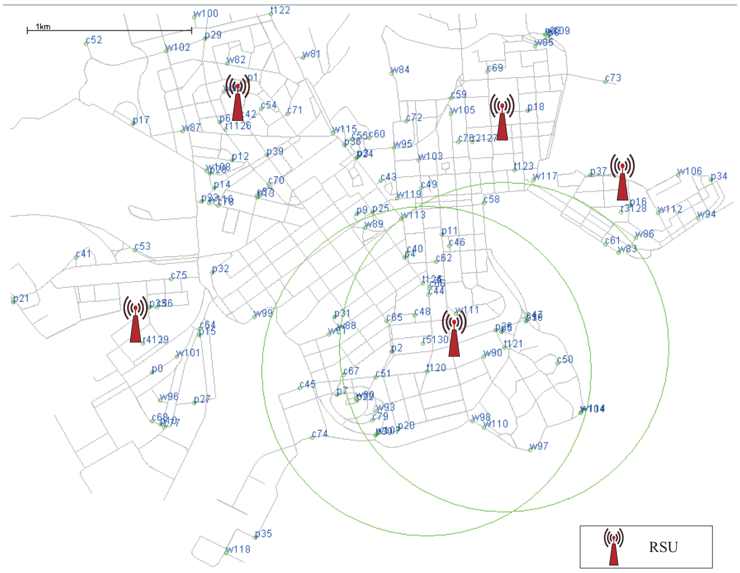

**Figure 7.** Locations of all nodes before the simulation started.

We conducted detailed analysis of the experiments under these parameters and simulation settings in the following section.

### 5.2. Simulation Results and Analysis

In order to evaluate the proposed scheme, we ran two sets of experiments: the first evaluated the detection of malicious forged messages; the second set evaluated the performance of the protocol combined with the security scheme.

#### 5.2.1. Evaluate the Detection of Forged Messages

To evaluate the detection performance of the proposed scheme, we considered false alarm rate ($FAR$) and missed detection rate ($MDR$) as the performance metrics:

$$FAR = \frac{N_f}{N_i}, \tag{14}$$

$$MDR = \frac{N_{miss}}{N}, \tag{15}$$

where $N_f$ denotes the total number of true messages that are identified as false messages by the method, $N_i$ denotes the total number of true messages, $N_{miss}$ denotes the total number of false messages that are identified as true messages by the method, and $N$ denotes the total number of false messages.

We chose $HCPDS$ [38] and $GBPM$ [39] as baseline methods for comparison. $BCSM$ is the security mechanism proposed in this paper. Note that there are two blockchains in $BCSM$: $BCCA$ and $BCIR$. In our experiments, POS consensus with an incentive mechanism was used to encourage RSUs to take active behaviors. We compared $BCSM$ with the baseline methods mentioned above.

Figures 8 and 9 plot the $FAR$ in high and low traffic density scenarios, respectively. Compared with $HCPDS$ and $GBPM$, $BCSM$ had lower $FAR$ because it adopts two types of blockchain $BCIR$ and $BCCA$ to validate the legitimacy of sender nodes and identify the trustworthiness of messages transmitted in VANETs.

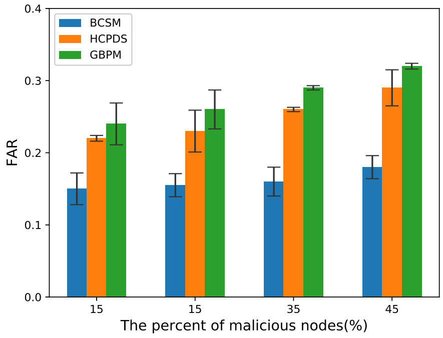

**Figure 8.** $FAR$ for low traffic density.

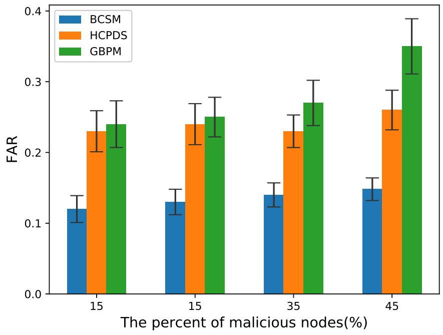

**Figure 9.** $FAR$ for high traffic density.

Figures 10 and 11 plot the $MDR$ in high and low traffic density scenarios, respectively. As the percentage of malicious nodes increases from 15% to 45%, the $MDR$ of $HCPDS$ and $GBPM$ increases. Compared with these two methods, $BCSM$ is able to effectively mitigate the negative effect from the increase of malicious vehicle nodes and maintain a relatively stable level in terms of $MDR$.

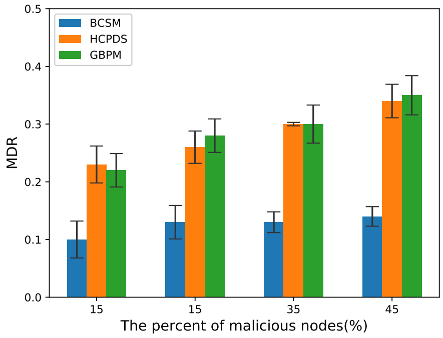

**Figure 10.** $MDR$ for low traffic density.

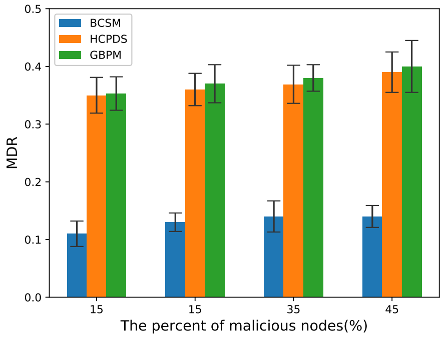

**Figure 11.** $MDR$ for high traffic density.

### 5.2.2. Evaluate the Performance of Transmission

For the evaluation of message transmission, we considered three performance metrics: delivery rate, delay and overhead rate.

(1) Delivery rate: It refers to the percentage of successful transmissions among all messages sent by nodes in the network. The higher the delivery rate, the higher the communication quality between nodes, and the better the overall network performance.

(2) Delay: It refers to the average time from creating a message to successfully delivering the message to the target node. The shorter the delay, the better the overall simulation performance.

(3) Overhead rate: It refers to the difference between the number of forwarded and the number of delivered messages.

We compare the proposed scheme with $AODV$, $TBM$ [40], and $BSIA$ [31], and summarize the simulation results as follows.

Figures 12 and 13 plot the delivery rate in high and low traffic density scenarios, respectively. In either case, as the number of malicious nodes increases, the delivery rate decreases. $AODV$ has a less packet delivery fraction because malicious nodes drop packets. Compared with other baseline methods, our proposed algorithm shows better performance in terms of delivery rate.

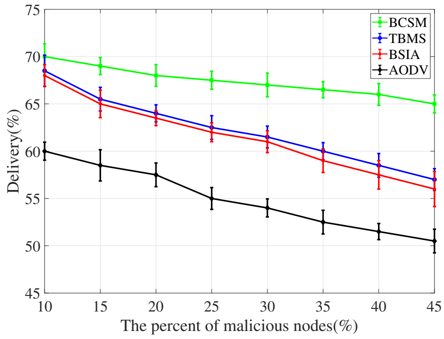

**Figure 12.** Delivery for low traffic density.

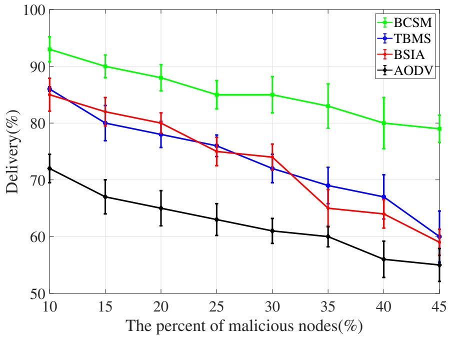

**Figure 13.** Delivery for high traffic density.

Delay rate is the most important metric for assessing the network performance, as it depicts how an additional overhead of the security measure increases the delay in the process of routing. As shown in Figures 14 and 15, *AODV* has the lowest delay rate because it does not consider any security measures. Compared with *TBMS* and *BSIA*, *BCSM* has a lower delay rate.

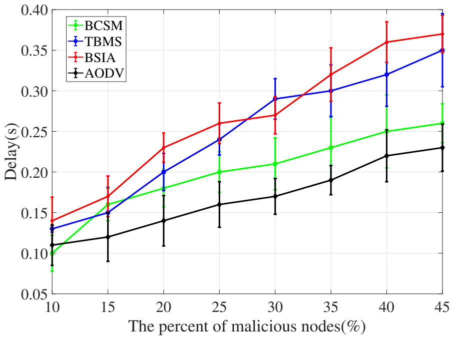

**Figure 14.** Delay for low traffic density.

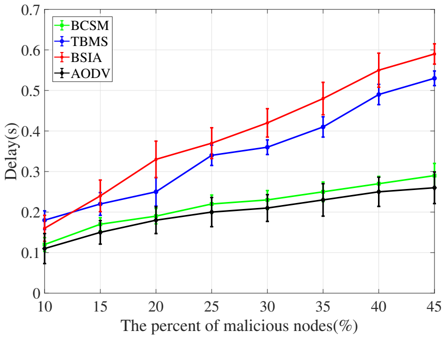

**Figure 15.** Delay for high traffic density.

Figures 16 and 17 show the comparison results of overhead rate. $AODV$ has the lowest delay rate because it does not consider any security measures. In low traffic density, the overhead of our proposed algorithm is higher than that of other methods. In high traffic density, compared with other baseline methods, the overhead of our proposed algorithm is slightly higher than those of $TBMS$ and $BSIA$. Obviously, $BCSM$ is more suitable for urban traffic environments where high traffic density is almost the norm.

$BCSM$ based on blockchain technology provides secure communications for CAs and RSUs. The experimental results show that $BCSM$ effectively improves the efficacy of VANETs. Meanwhile, it achieves better performance in detecting forged messages and identifying malicious nodes.

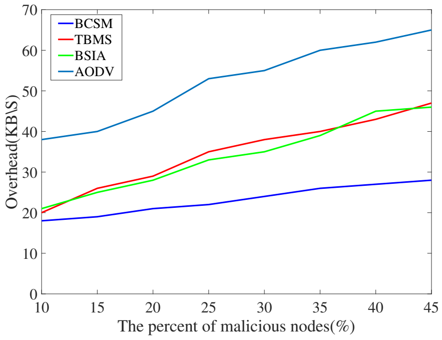

**Figure 16.** Overhead with low traffic density.

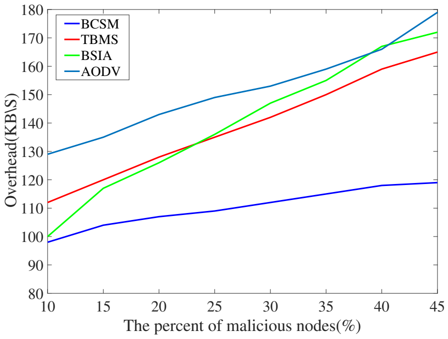

**Figure 17.** Overhead with high traffic density.

## 6. Conclusions and Discussion

Detecting and identifying forged messages and malicious nodes in highly dynamic and complicated mobile networks is a challenging problem. In this paper, we proposed a security scheme based on blockchain technology for communication security in VANETs. The proposed scheme constructs two types of blockchains in VANETs: BCIR on RSUs and BCCA on CAs. An incentive consensus mechanism, which encourages RSUs to take active behaviors in VANETs, was designed for BCIR. BCCA is able to identify if a vehicle has a legitimate identity. The legitimacy of a message is evaluated, taking into account various factors, such as integrity of messages, reputation of the sender node, time effectiveness, and distance effectiveness. Meanwhile, the reputation of a node is decided by its communication behaviors. By analyzing a node's communication behaviors, the scheme is able to identify whether or not the node is malicious. Moreover, the proposed scheme can protect the privacy of vehicles. Simulation-based experiments show that our scheme is feasible and effective for detecting malicious nodes and identifying forged messages in practical vehicle networks.

In the future, we plan to deepen our research to improve the accuracy of the scheme. We are currently in the process of building a traffic service platform to evaluate the performance of our scheme in real-life transportation networks. We will also consider additional security metrics for performance and robustness evaluation.

**Author Contributions:** Conceptualization, G.L., N.F. and C.Q.W.; Methodology, G.L. and C.Q.W.; Project administration, N.F.; Software, X.Z.; Writing—original draft preparation, N.F.; writing—review and editing, C.Q.W. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research was funded by the Key Research and Development Plan Project of Shaanxi Province, China. Grant number: 2022GY-039, 2022GY-030.

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** Not applicable.

**Acknowledgments:** This study is supported by Funds for the Key Research and Development Plan Project of Shaanxi Province, China (2022GY-039, 2022GY-030).

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

## References

1. Jia, D.; Lu, K.; Wang, J.; Shen, X. A survey on platoon-based vehicular cyber-physical systems. *IEEE Commun. Surv. Tutorials* **2015**, *18*, 263–284. [CrossRef]
2. Kerrache, C.A.; Lakas, A.; Lagraa, N. Detection of Intelligent Malicious and Selfish Nodes in VANET using Threshold Adaptive Control. In Proceedings of the International Conference on Electronic Devices IEEE, Coimbatore, India, 20–22 April 2017.
3. Kerrache, C.A.; Calafate, C.T.; Lagraa, N.; Cano, J.-C.; Manzoni, P. Rita: Risk-aware trust-based architecture for collaborative multi-hop vehicular communications. *Secur. Commun. Netw.* **2016**, *9*, 4428–4442. [CrossRef]
4. Kothari, A.; Shukla, P.; Pandey, R.. Trusit centric approach based on similarity in VANET. In Proceedings of the International Conference on Signal Processing IEEE, Xiamen, China, 21–23 September 2017.
5. Rostamzadeh, K.; Nicanfar, H.; Torabi, N.; Gopalakrishnan, S.; Leung, V. A contex- t-aware trust-based information dissemination framework for vehicular networks. *IEEE Internet Things J.* **2015**, *2*, 121–132. [CrossRef]
6. Qun, W.; Huanyan, Q.; Gang, Z. An Identity and Location for Vehicle Networking Methods. *Comput. Sci.* **2012**, *39*, 131–134.
7. Li, L. *Research on Pseudo-Name Based Privacy Protection in the Internet of Vehicles*; Springer: Berlin/Heidelberg, Germany, 2017.
8. Xu, H.;Zhengguo, S.;Daxin, T.;Yunpeng, W.;Xuting, D.;Victor C.M., L. Optimized anonymity updating in VANET based on information and privacy joint metrics. In Proceedings of the 8th ACM International Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications, Montreal, QC, Canada, 25 October 2018; pp. 63–69.
9. Minghui, Z.; Yangyang, D.; Hanxiao, L.Y.U. Research on Group Signature Based Identity Authentication Protocol in Internet of Vehicles. *Eng. Sci. Technol.* **2018**, *50*, 134–138.
10. Hong, Z.;Jingyu, W.;Jie, C.;Shun, Z. Efficient conditional privacy-preserving and authentication scheme for secure service provision in VANET. *Tsinghua Sci. Technol.* **2017**, *21*, 620–629.
11. Gong, H.; Yu, L.; Zhang, X. Social contribution-based routing protocol for vehicular network with selfish nodes. *Int. J. Distrib. Sens. Netw.* **2014**, *2014*, 700–705. [CrossRef]
12. Sedjelmaci, H.; Senouci, S.M.; Abu-Rgheff, M.A. An efficient and lightweight intrusion detection mechanism for service-oriented vehicular networks. *IEEE Internet Things J.* **2014**, *1*, 570–577. [CrossRef]
13. Khan, U.; Agrawal, S.; Silakari, S. Detection of malicious nodes (DMN) in vehicular ad hoc networks. *Proc. Comput. Sci.* **2015**, *46*, 965–972. [CrossRef]
14. Haddadou, N.; Rachedi, A.; Ghamri-Doudane, Y. A job market signaling scheme for incentive and trust management in vehicular ad hoc networks. *Veh. Technol. IEEE Trans.* **2015**, *64*, 3657–3674. [CrossRef]
15. Bali, R.S.; Kumar, N. *Secure Clustering for Efficient Data Dissemination in Vehicular Cyber Physical Systems*; Elsevier: Amsterdam, The Netherlands, 2016.
16. Shaikh, R.A.; Alzahrani, A.S. Intrusion-aware trust model for vehicular ad hoc networks. *Secur. Commun. Netw.* **2016**, *7*, 1652–1669. [CrossRef]
17. Gurung, S.; Lin, D.; Squicciarini, A.C.; Bertino, E. *Information-Oriented Trust-Worthiness Evaluation in Vehicular Ad-Hoc Networks*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 94–108.
18. Mohamed, M.S.; Hussein, S.; Krings, A. An Enhanced Voting Algorithm for Hybrid Jamming attacks in VANET. In Proceedings of the IEEE 7th Annual Computing and Communication Workshop and Conference(CCWC), Las Vegas, NV, USA, 9–11 January 2017; pp. 1–7.
19. Alturkostani, H.; Krings, A. The impact of jamming on threshold-based agreement in VANET. In Proceedings of the International Conference on Connected Vehicles and Expo (ICCVE), Vienna, Austria, 3–7 November 2014; pp. 882–887.
20. Ahmed, S.; Tepe, K. Recommendation trust for improved malicious node detection in ad hoc networks. In Proceedings of the IEEE 86th VTC-Fall, Toronto, ON, Canada, 24–27 September 2017; pp. 1–5.
21. Yao, X.; Zhang, X.; Ning, H. Using trust model to ensure reliable data acquisition in VANETs. *Ad Hoc Netw.* **2016**, *55*, 107–118. [CrossRef]

22. Li, W.; Song, H. ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks. *IEEE Trans. Intell. Transp. Syst.* **2016**, *17*, 960–969. [CrossRef]
23. Ahmed, S.; Tepe, K. Misbehaviour detection in vehicular networks using logistictrust. In Proceedings of the Wireless Communications and Networking Conference (WCNC), Doha, Qatar, 3–6 April 2016; pp. 1–6.
24. Sedjelmaci, H.; Senouci, S.M. An accurate and efficient collaborative intrusion detection framework to secure vehicular networks. *Comput. Electr. Eng.* **2015**, *43*, 33–47. [CrossRef]
25. Dhurandher, S.K.; Obaidat, M.S.; Jaiswal, A. Vehicular Security Through Reputation and Plausibility Checks. *IEEE Syst. J.* **2014**, *8*, 384–394. [CrossRef]
26. Arora, A.; Yadav, S.K. Block Chain Based Security Mechanism for Internet of Vehicles (IoV). In Proceedings of the 3rd International Conference on Internet of Things and Connected Technologies, (ICIoTCT) 2018, Jaipur, India, 26–27 March 2018; pp. 267–272.
27. Lu, Z.; Liu, W.; Wang, Q.; Qu, G.; Liu, Z. A privacy-preserving trust model based on blockchain for VANETs. *IEEE Access* **2018**, *6*, 45655–45664. [CrossRef]
28. Yang, Z.; Yang, K.; Lei, L.; Zheng, K.; Leung, V.C.M. Blockchain-based decentralized trust management in vehicular networks. *IEEE Internet Things J.* **2018**, *6*, 1495–1505 . [CrossRef]
29. Tsung, Y.Y.; Der, C.L.; Wei, T.C.; Hsun, T.F.; Chang, L.C. Blockchain-Based Traffic Event Validation and Trust Verification for VANETs. *IEEE Access* **2019**, *7*, 30868–30877.
30. Wagner, M.; McMillin, B. Cyber-Physical Transactions: A Method for Securing VANETs with Blockchains. In Proceedings of the IEEE Pacific Rim International Symposium on Dependable Computing, PRDC, Taipei, China, 4–7 December 2018; pp. 64–73.
31. Nisha, M.; Priyadarsi, N.; Arushi, A.; Xiangjian, H.; Deepak, P. Blockchain Based Secured Identity Authentication and Expeditious Revocation Framework for Vehicular Networks. In Proceedings of the 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering, New York, NY, USA, 1–3 August 2018; pp. 674–679.
32. Zhaojun, L.; Qian, W.; Gang, Q.; Zhenglin, L. BARS: A Blockchain-Based Anonymous Reputation System for Trust Management in VANETs. In Proceedings of the 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, New York, NY, USA, 1–3 August 2018; pp. 98–103.
33. Khan, A.S.; Balan, K.; Javed, Y.; Tarmizi, S.; Abdullah, J. Secure Trust-Based Blockchain Architecture to Prevent Attacks in VANET. *Sensors* **2019**, *19*, 4954. [CrossRef]
34. Li, H.; Pei, L.; Liao, D.; Sun, G.; Xu, A.D. Blockchain Meets VANET: An Architecture for Identity and Location Privacy Protection in VANET. *Peer-to-Peer Netw. Appl.* **2019**, *12* , 1178–1193. [CrossRef]
35. Javaid, U.; Aman, M.N.; Sikdar, A.B. DrivMan: Driving Trust Management and Data Sharing in VANETs with Blockchain and Smart Contracts. In Proceedings of the IEEE Vehicular Technology Conference, Kuala Lumpur, Malaysia, 28 April–1 May 2019.
36. Dai, C.; Xiao, X.; Ding, Y.; Xiao, L.; Tang, Y.; Zhou, S. Learning Based Security for VANET with Blockchain. In Proceedings of the IEEE International Confrence onCommunication System(ICCS), Chengdu, China, 19–21 December 2018; pp. 210–215.
37. Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An overview of blockchain technology: Architecture, consensus, and future trends. In Proceedings of the IEEE 6th International Congress on Big Data, BigData Congress 2017, Honolulu, HI, USA, 25–30 June 2017; pp. 557–564.
38. Prabakeran, S.; Sethukarasi, T. Optimal solution for malicious node detection and prevention using hybrid chaotic particle dragonfly swarm algorithm in VANETs. *Wirel. Netw.* **2020**, *26*, 5897–5917. [CrossRef]
39. Malhi, A.K.; Batra, S. Genetic-based framework for preventionof masquerade and DDoS attacks invehicularad-hocnetworks. *Secur. Commun. Netw.* **2016**, *9*, 1–15.
40. Tripathi, K.N.; Sharma, S.C. A trust based model (TBM) to detect rogue nodes in vehicular ad-hoc networks (VANETS). *Int. J. Syst. Assur. Eng. Manag.* **2019**, *11*, 1–15. [CrossRef]