Blockchain-Assisted Trust Management Scheme for Securing VANETs

Waheeb Ahmed[1*], Di Wu[1], and Daniel Mukathie[1]
[1] School of Computer Science and Technology, Dalian University of Technology
Dalian 116024, China
[e-mail: waheeb@mail.dlut.edu.cn,wudi@dlut.edu.cn,mukathej@mail.dlut.edu.cn]
[*]Corresponding author: Waheeb Ahmed

Received July 7, 2021; revised September 11, 2021; accepted February 10, 2022; published February 28, 2022

Abstract

The main goal of VANETs is to improve the safety of all road users. Therefore, the accuracy and trustworthiness of messages transmitted in VANETs are essential, given that life may rely on them. VANETs are provided with basic security services through the use of public key infrastructure-based authentication. However, the trust of users is still an open issue in VANETs. It is important to prevent bogus message attacks from internal vehicles as well as protect vehicle privacy. In this paper, we propose a trust management scheme that ensures trust in VANETs while maintaining vehicle privacy. The trust scheme establishes trust between vehicles where a trust value is assigned to every vehicle based on its behavior and messages are accepted only from vehicles whose trust value is greater than a threshold, therefore, protecting VANETs from malicious vehicles and eliminating bogus messages. If a traffic event happens, vehicles upload event messages to the reachable roadside unit (RSU). Once the RSU has confirmed that the event happened, it announces the event to vehicles in its vicinity and records it into the blockchain. Using this mechanism, RSUs are prevented from sending fake or unverified event notifications. Simulations are carried out in the context of bogus message attacks to evaluate the trust scheme's reliability and efficiency. The results of the simulation indicate that the proposed scheme outperforms the compared schemes and is highly resistant to bogus message attacks.

Keywords: VANET, Trust management, Blockchain, Bogus message attack, Privacy.

1. Introduction

Vehicular Ad hoc Networks (VANETs) allow vehicles to communicate with their neighbors and share road-related messages about traffic conditions, such as congestion, and traffic accidents. The messages enable vehicles to become more aware of traffic situations in real-time, thus improving transportation safety and efficiency [1]. In VANETs, there are two modes of communication: vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I). The V2V and V2I protocols make it possible for vehicles to communicate with each other and exchange useful driving data over a dedicated short-range communication channel (DSRC) [2]. For example, if a traffic accident or crash occurs, it is necessary to send a warning alert to all vehicles on the road to prevent traffic jams and ensure safety.

Therefore, whether the relevant information is trustworthy is a very essential requirement for overall traffic safety. However, VANETs are often characterized by high mobility, so neighboring vehicles are often unfamiliar to one another and can't be fully trusted. When malicious vehicles are present in the network, the problem becomes even worse. These malicious vehicles can purposefully broadcast bogus messages. For example, a message claiming that the road is clear may be broadcasted by a malicious vehicle when there is actually an accident or traffic jam. This misbehavior will endanger the transportation system's safety and efficiency. Due to this, how the trustworthiness of messages and vehicles are evaluated is a critical issue in VANETs [3].

To ensure that only authenticated vehicles transmit messages, a variety of authentication methods are used. Although the authentication based on public key infrastructure (PKI) can protect against external attacks and ensure anonymity, it can't prevent legitimate vehicles from distributing maliciously bogus or tampered messages which may reduce transportation efficiency and they may also cause accidents that, in the worst scenario, endanger human life [4]. Since it is typically necessary to cope with inside attackers with valid certificates and to address the limitations of traditional cryptography solutions, trust management has been introduced as a complementary security layer [5]. While there are methods to isolate external attackers by providing secure communication channels, privacy protection and trust management for vehicles in VANETs are still open issues [6-8].

To establish a secure communication environment, trust management is used to determine the credibility of messages using both direct experiences and indirect feedback about the senders [5]. Blockchain is seen as a useful tool for creating a desirable trust model [9]. It's a decentralized and distributed public ledger with a proof of work (PoW) mechanism for consensus. Because of these important characteristics, blockchains help develop an appropriate data-sharing platform for VANETs.

To fill the security gaps in VANET, in this paper, a blockchain-assisted trust management solution for VANETs is proposed. First, vehicle authentication is established in the VANET. The public key infrastructure (PKI) is used for generating a pair of public and private keys to each vehicle for purposes of communication. Privacy preservation is accomplished by eliminating the links between the vehicle’s public key and its real identity and protecting it from attackers. A certificate provided by a trusted authority is used to break the connection between the vehicle's real identity and its public key. In addition, the trust model on a vehicle measures the sender vehicle's trust value before making a decision to accept or reject any message from that vehicle. Furthermore, RSU evaluates the event messages received from vehicles. If the result is verified to be an incident, the RSU will broadcast an event alert to the

vehicles in its communication range, and the event details will be permanently stored on the blockchain. The following is a summary of our major research contributions.

1) We propose a blockchain-assisted trust management scheme that protects vehicle identity privacy and ensures that transmitted messages are sent by authorized vehicles.
2) The proposed trust management model ensures a trust communication environment where only trustworthy messages are accepted in VANETs where a blockchain is used to store the trust values of vehicles and event blockchain is used to record verified event messages.
3) Finally, we conduct a security analysis to demonstrate that the proposed schemes can withstand a variety of security attacks while still meeting the privacy requirements of VANETs. The obtained performance results show that the proposed trust management scheme is efficient and reliable.

The rest of this paper is organized as follows. In Section 2, we review current work on privacy-preserving authentication and trust management models in VANET. An overview of blockchain is presented in section 3. The system model and components are presented in Section 4. Sections 5 and 6 introduce the system authentication and the detailed trust scheme. The security analysis is presented in section 7. The performance evaluation is presented in Section 8. Finally, in Section 9, we conclude the proposal.

2. Related Work

With the increasing concerns about vehicle privacy and authentication [10], two requirements are necessary for establishing effective vehicular communications. As messages usually contain users' private information, such as their geographic location, they must be transmitted anonymously. However, broadcasting messages anonymously cannot guarantee their authenticity. In particular, preventing the spread of bogus messages from internal vehicles is difficult. These bogus messages have the potential to cause accidents and decrease transportation efficiency. Therefore, a trusted authority should be able to track the real identities of vehicles that display malicious behavior.

The existing works on conditional privacy and authentication [11,12], lack efficient authentication and sufficient scalability. Many researchers have recently centered on VANET privacy, trust, and security issues [13-27].

Wasef et al.[13] proposed EMAP, expedite message authentication protocol, which uses a hash-based authentication code to speed up the integrity check and a PKI for vehicle authentication.

Feng et al. [14] presented a novel authentication scheme that preserves privacy and provides authentication automatically in VANETs. It enables conditional tracking and dynamic revocation of misbehaving vehicles. In [15], a temporary anonymous certificate is used for each session to improve the unlinkability property.

Lin et. al.[16] proposed a PKI-based solution for secure communication in VANETs that is based on Ethereum. To achieve effective certificate management, the authors combined a key derivation algorithm with blockchain technology. That eliminates the need to keep large numbers of private keys by participating vehicles.

Zheng et al.[9] designed an ID-based BCP-PA protocol with traceable anonymity using pseudonym technology, but it cannot withstand a compromised certificate authority and it requires ideal hardware.

To secure V2V communications, Rowan et al. [17] presented an inter-vehicle session key establishment protocol based on blockchain. Dorri et al. [18] proposed blockchain and changeable public keys privacy-preserving authentication, but it has scalability and membership management issues.

Chuang et al.[19] presented a privacy protection authentication scheme (PPAS) for V2I communication in VANETs, which enables RSU and vehicles to authenticate each other while meeting most security requirements. However, this method does not operate in a distributed manner.

The authors in [20] presented a solution that uses RSUs to validate beacon messages, then use the notification messages to classify and publish lists of legal and illegal vehicles. In this scenario, before verifying the sender's authenticity, the vehicle would have to wait for a notification message, which may consume some time.

Luo et. al. [21] introduced a blockchain and trust-based location privacy protection scheme. The authors proposed an approach that uses Dirichlet distribution, in which the requester and cooperator vehicles would only work with vehicles they trust. Vehicles' trustworthiness is stored on publicly accessible blocks, allowing any vehicle to access the historical trust information of other vehicles when they need to communicate with these vehicles.

In [22,23] to evaluate reported events, the authors proposed a Bayesian decision module. However, due to the dynamic topology of the VANET, estimating the prior probability is difficult. Furthermore, the credibility of the message is not guaranteed by the authentication of the vehicular nodes, since authenticated vehicles can send false messages for malicious purposes.

Li and Song [28] designed a hybrid trust management system in which the trustworthiness of data is determined by evaluating messages obtained from multiple vehicles, while functional and recommendation trusts are used to determine the trustworthiness of the vehicle. Their methods, on the other hand, ignore the VANET's data sparsity.

Kchaou et al. [29] designed privacy-aware reputation and trust management models using blockchain. The transaction is assumed by both schemes to record the events in VANET securely. Such recorded events may be permanent proof for evaluating a vehicle’s reputation. Although their systems promote strict transparency, they are unable to prevent malicious activity from occurring in the first place.

Chen et. al. [30] introduced a trust management system based on beacon messages (named BTM) to prevent internal vehicles in VANETs from sending fake messages. The authors use the Dempster-Shafer Theory to consider the event message's trustworthiness as well as the vehicle's trustworthiness when deciding whether to accept or reject an event message.

Arshad et. al. [31] developed a beacon-based trust management system and fake data detection (called BTMS-FDD) that discards false safety events in VANETs. To create a relationship with nearby vehicles, the proposed system utilizes information about speed and density.

The existing literature on trust management schemes lacks a proper trust scheme that can not only evaluate the trustworthiness of event messages efficiently but can also ensure vehicle identity privacy protection and resist various attacks. Therefore, in order to improve existing trust management schemes, the proposed solution provides a newer, efficient, and robust scheme that combines privacy-preserving authentication with vehicles- and RSU-based trust computation.

3. Blockchain

Blockchain technology was first adopted by Bitcoin to solve the problem of double-spending, without needing third parties to verify transactions [32]. Basically, blockchain is a decentralized distributed database that stores data in blocks that are chained together [33]. The block is made of two parts: a block header and a block body as shown in **Fig. 1**.

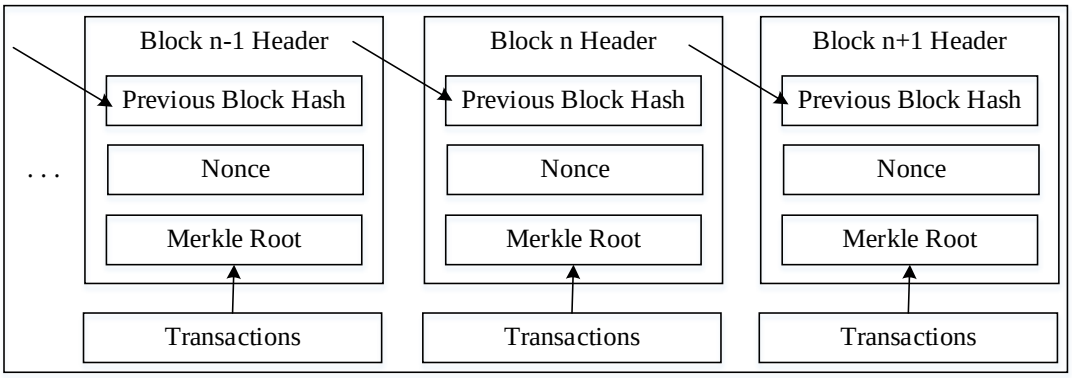

Fig. 1. Blockchain architecture

The block header consists of a hash of the previous block, a nonce, a timestamp, Merkle's root, and the current block's hash, while the block body is made of transactions represented by a Merkle tree. Chaining occurs by having the hash of the previous block in the header of the current block, this ensures once data is stored is immutable. To add a block to the blockchain, mining nodes compete to achieve a difficulty target. The first node to achieve the target becomes the successful miner and proceeds to publish the block. The other participants verify whether the target has been met and if it has, they add the block to their blockchains. Otherwise, they reject the block [34]. As a result, all nodes in the network maintain the same version of blockchain which ensures consistency of data.

Blockchain has a number of features that have made it a promising tool for establishing trust in vehicular networks,

1. Decentralization: Blockchain is a decentralized and distributed system that ensures nodes in the whole network maintain the same copy of the database. Unlike centralized networks, its database is secure from a single point of failure, thus it’s reliable.
2. Immutability: Immutability is one of the key features of the blockchain. Unlike traditional databases, blockchain records cannot be altered, removed, or added arbitrarily.
3. Consistency: Through blockchain, RSUs are able to read, write and update the trust values of vehicles in a consistent manner. As a result, the same query on vehicle trust produces the same results, hence consistency is guaranteed.
4. Faster transactions: Setting up a blockchain system is easy. Besides, Blockchain transactions take a few seconds or minutes to process.
5. Reliable and accurate data: Blockchains are decentralized in nature, which makes their data reliable, accurate, consistent, timely, and accessible to everyone. Therefore, blockchain technology is highly secure, and it is immune to many network attacks.

Therefore, due to these important features of blockchain, it has the potential to create a robust trust model in VANETs [9,35]. All revoked public keys, issued certificates, the mapping of a vehicle's pseudonyms and their trust values will be recorded into immutable, tamper-resistance, and decentralized ledgers.

4. System Model and Components

This section outlines the proposed scheme's system model and design objectives.

4.1. Overview of the proposed approach

The system model is illustrated in **Fig. 2**. The proposed scheme is composed of several entities.

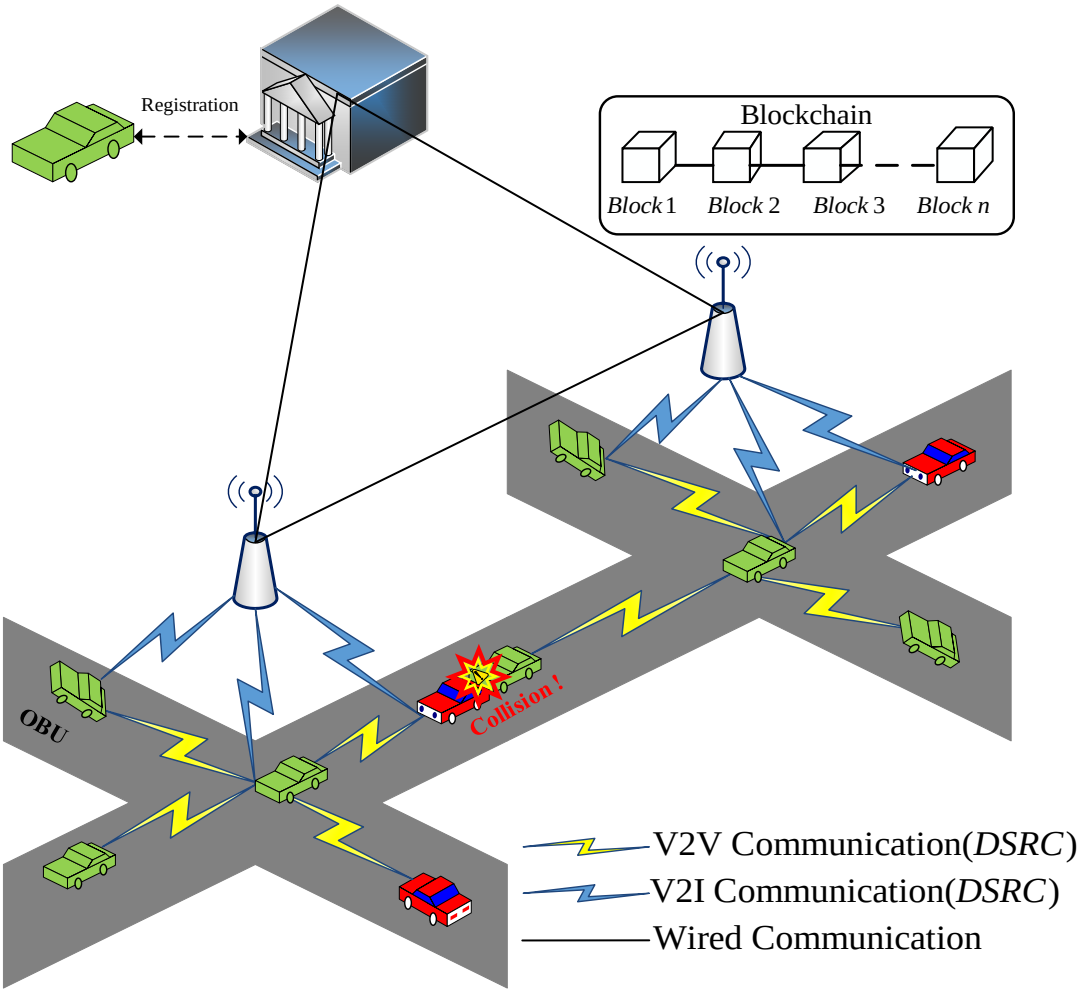

Fig. 2. System Model

Trusted Authority(TA): TA is in charge of issuing certificates to vehicles and revoking malicious vehicles' public keys. As a result, TA is considered to be completely trusted. TA

issues certificates to vehicles during registration and revokes public keys only if it gets a warrant from RSU. TA has a database of public key-real identity pairs. If RSUs and vehicles want to participate in the network, they must first register with TA. When an RSU informs the TA about a malicious vehicle, the TA revokes the vehicle's public key and informs all other vehicles about it.

RSUs: RSU is equipped with higher storage and computing capabilities in VANETs [36]. It stores all of the blockchains' transaction records. In addition, RSU is responsible for collecting event messages from vehicles within its communication range, evaluating the vehicles' trustworthiness, updating the vehicles' trust values, and broadcasting event notifications to vehicles in its vicinity. Furthermore, all RSUs work together to create a stable ledger, and RSUs do the consensus work while constructing the blockchain.

Vehicle: Using an onboard unit (OBU), a vehicle can communicate and exchange messages with other vehicles and RSUs. A tamper-proof device (TPD) is attached to the OBU to store sensitive data including public/private keys. TPD stores confidential data in a physically secure environment.

Digital Signature: Each vehicle has its public-private key pair, and messages are digitally signed using the sender's private key, with the receiver verifying the message's validity using the public key. TA signs these public keys in order to authenticate them as belonging to a legitimate vehicle (generating certificates). The certificate has an expiration date and a public key, but no real identity. Before a vehicle sends a message to another vehicle, it must first sign the message with its private key. In addition, the certificate issued by the TA should also be sent so that the sender's public key can be verified by the receiver before authenticating the message.

Certificates Blockchain (CertificateBC): CertificateBC stores all issued certificates. During the authentication process, a vehicle checks the CertificateBC for the presence of another vehicle's certificate.

Revoked public keys Blockchain (RevocationBC): RevocationBC stores all revoked public keys. During the authentication process, a vehicle checks the RevocationBC for the absence of the sender's public key.

Event Blockchain (EventBC): To maintain permanent evidence in case of disputes, all verified event messages will be recorded into EventBC.

Trust Blockchain (TrustBC): TrustBC acts as a public ledger for vehicle trust values. RSUs access it to retrieve and update the trust value of vehicles during the event validation phase.

4.2 Design Goals

Our scheme aims to satisfy the following requirements: authentication and trust, identity privacy-preserving, conditional traceability, and resistance to attacks.

(i) Authentication and trust: The vehicles or RSUs should be able to authenticate received messages to ensure their authenticity. Entity authentication means that two communicating entities are able to identify each other. Message authentication confirms that the received messages are generated by authenticated vehicles and unmodified during transmission. In addition, the trustworthiness of the messages and sender vehicles should be checked by receiver vehicles and RSUs.

(iii) Privacy-preserving: Vehicles in VANETs periodically broadcast messages about their speed, position, and direction. Preserving the privacy of a vehicle's identity means that no entity could find out the binding between messages and real identities of vehicles. The real identity of the vehicle should not be revealed to other vehicles and RSUs, and no adversary

should deduce the real identity by analyzing the message contents.

(iv) Conditional traceability: The real identities of vehicles should be retrievable in some cases (e.g., malicious behaviors). Conditional traceability allows only TA to access the vehicles' real identities. Traceability is required when fake messages are sent by malicious vehicles to mislead others.

(v) Resistance to Attacks: The blockchain-based VANETs should be resilient against popular attacks (for example, modification, bogus message, distributed denial of service, and replay attacks).

4.3 Adversary Model

The performance of the proposed scheme is evaluated under the influence of malicious vehicles. We used bogus message attacks as an adversary model for our scheme. Since a bogus message attack poses a serious risk in VANET. The designed adversary model is equipped with the capability to send bogus messages.

5. System Authentication

Since VANET communication relies on an open wireless connection, it is subject to various types of security attacks. Therefore, the first important requirement for any security system is a module that assesses sender authenticity.

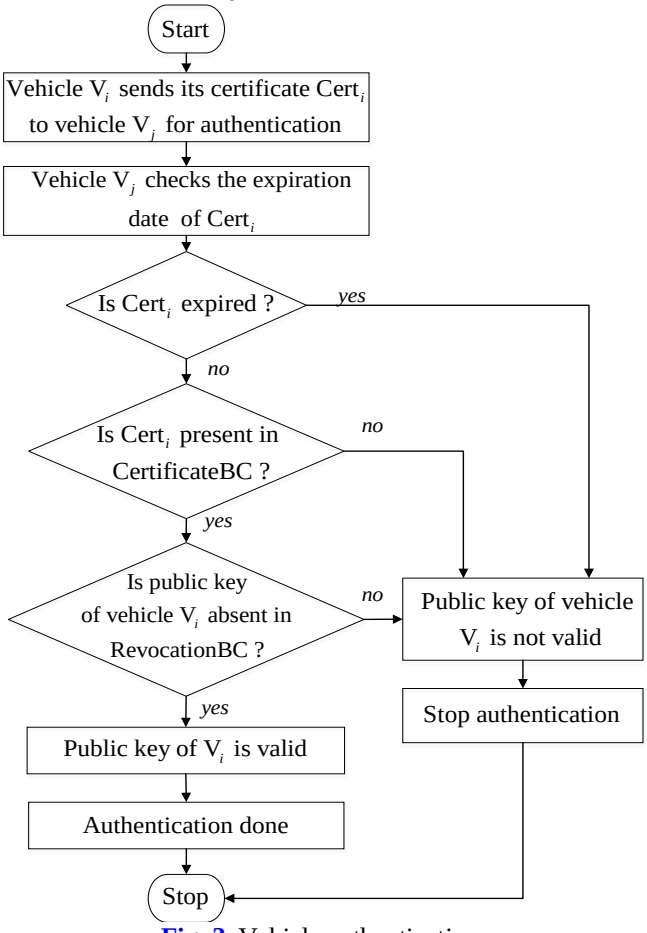

Fig. 3. Vehicle authentication

As shown in **Fig. 3**, the authentication process is based on two blockchains. It starts when a vehicle V_i wants to communicate with a vehicle V_j. Vehicle V_i sends its certificate Cert_i to vehicle V_j. When vehicle V_j receives the certificate from the vehicle V_i, it checks whether the Cert_i of vehicle V_i is valid. The certificate would contain the public key as well as the expiration of Cert_i. Vehicle V_j will check the expiration of Cert_i. If Cert_i has not expired, then, vehicle V_j checks CertificateBC for the presence of Cert_i. If Cert_i is present in the CertificateBC blockchain, vehicle V_j proceeds to check RevocationBC to see if the public key of the vehicle V_i is not available in the RevocationBC blockchain. Once the above three criteria are satisfied, then the vehicle V_i and vehicle V_j can communicate with each other. In case, any of the three conditions mentioned are not met, the authentication process will be halted immediately.

6. Proposed Trust Management Model

The related trust values of participating vehicles are estimated using the proposed trust management model. It estimates vehicles' trustworthiness.

6.1 Trust calculation on Vehicle

During network interaction, the receiver vehicle's OBU keeps track of the sender vehicles' trust values and stores them in its historic table. The trust value varies from (0.0) to (1.0) and is subject to change based on the sender vehicle's behavior. Trust is based on direct and indirect computation. The direct trust measures how reliable the information is from vehicle V_j and is denoted as $DirectT_s(V_i, V_j)$. The indirect trust metric calculates the average level of trust that neighbors R have about the vehicle V_j. Total trust represents the total trust vehicle V_i has about the vehicle V_j and it incorporates the direct trust, indirect trust, and RSU recommendation. Assume that in time slot s, the vehicle V_i receives B messages from the vehicle V_j. The trust is calculated in a decentralized manner by vehicles and RSUs. In the first phase, when the vehicle V_i needs to evaluate the trust of the vehicle V_j, it follows a two-step procedure: Step 1) In its communication history table, the vehicle V_i gathers information about direct communications with the vehicle V_j. Step 2) Vehicle V_i requests its nearby vehicles for trust information about the vehicle V_j based on their interactions with the vehicle V_j. The direct trust is calculated using the information obtained in the first step, while the indirect trust is calculated using the information obtained in the second step. In the second phase, the trust value of the vehicle V_j is determined using the direct and indirect trust values computed in the first phase. The final trust value of the vehicle V_j is updated by including the RSU trust about V_j and it is retrieved from the TrustBC. Finally, if the total trust of vehicle $V_j \geq a\ threshold$, vehicle V_i accepts the message from the vehicle V_j, otherwise it drops the message as it is considered a bogus message.

The model allows receiver vehicles to validate messages sent by sender vehicles using three criteria: event time, sender location, and the recommendation degree. Therefore, the receiver will check the validity of messages received from sender vehicles using the event validation policy below:

An event message is considered to be fake if any of the following conditions are matched:

1. When the sender's location is detected to be false.
2. When the event time is detected to be false.
3. When the recommendation degree about the message is less than a threshold.

When an event occurs happens in the network, such as a vehicle accident or traffic congestion, vehicles broadcast event messages including their location to other vehicles. The estimated distance DISTANCE(S, R) between the receiver vehicle and the sender vehicle is calculated using

$$DISTANCE(S,R) = \sqrt{(S.X - R.X)^2 + (S.Y - R.Y)^2} \le TR \tag{1}$$

where $(S.X, S.Y)$ is the current coordinates of the sender vehicle, and $(R.X, R.Y)$ represents the current coordinates of the receiver vehicle. The Global Positioning System (GPS) is assumed to be installed on all vehicles to provide location information. The communication range of a vehicle TR is 250m. The sender's location is considered to be correct if it is satisfying the condition $DISTANCE(S,R) \le TR$.

The expected arrival time of the event message is calculated using,

$$t_{EXP} = t_E + \frac{DISTANCE(S,R)}{c} \tag{2}$$

where t_{EXP} represents the expected time when the receiver vehicle received the message, t_E is the time when the event message is generated at the sender vehicle, and c is the speed of light. $If\ |t_{EXP} - t_{RCV}| < \varepsilon$, then the time is considered true, otherwise, it is false. Here, T_{RCV} is the time when the event message is received by the receiver vehicle and ε represents tolerable estimation error.

When a vehicle receives event messages from other vehicles, it splits the senders into two sets: W(a) and W(d) where W(a) is the number of vehicles agreeing to this message, and W(d) is the number of vehicles disagreeing with this message. The recommendation degree (RD) is calculated as

$$RD = \frac{W(a)}{W(a) + W(d)} > 1 - \varepsilon \tag{3}$$

Messages are accepted only if (3) holds, where ε is a tolerable error rate.

Algorithm 1: Message Validation

Input: Location of sender (S.X,S.Y), Location of receiver (R.X,R.Y), Transmission range(TR), Time of event (t_E), Speed of light (C), Time of receiving message (t_{RCV}) , Tolerable error rate(ε).
Output: Distance between sender and receiver DISTANCE(S,R), Expected arrival time(t_{EXP}), Recommendation degree(RD);

```
Compute DISTANCE(S,R) using (1);
Compute t_EXP using (2);
Compute RD using (3);
if (DISTANCE(S,R)≤TR and | t_EXP -t_RCV | <ε and RD<(1-ε)) then
    The event message is valid;
else
    The event message is not valid;
    Discard event message;
end
```

After verifying the validity of event messages, the direct trust, indirect trust, and total trust will be calculated by vehicle V_i .

Direct Trust (DirectT)

Direct trust $DirectT_s\left(V_i,V_j\right)$ is computed by,

$$DirectT_s\left(V_i,V_j\right)=\begin{cases}? \text{ all event messages are false}\\ A_s\left(V_j\right)\\ \overline{B_s\left(V_j\right)} \quad Otherwise\end{cases} \tag{4}$$

where $A_s(V_j)$ is the number of true messages received from the vehicle V_j in time period s, and $B_s\left(V_j\right)$ is the total number of messages received from the vehicle V_j in time period s. The updated direct trust is the weighted sum of current direct trust and previous direct trust and is calculated as

$$DirectT_s\left(V_i,V_j\right)=\alpha * DirectT_s\left(V_i,V_j\right)+\left(1-\alpha\right) * DirectT_{s-1}\left(V_i,V_j\right)? \tag{5}$$

where $0.5 < \alpha < 1$.

Indirect Trust (IndirectT)

The indirect trust is computed using the feedback provided by the neighbors $V_x \in R$ about V_j . The vehicle V_i collects the trust from neighbor vehicles $V_x \in R$ and computes indirect trust as

$$IndirectT_s(V_i,V_j)=\begin{cases}\dfrac{\sum_{V_x \in R} T_s(V_x,V_j)}{R}, \; if \;\; R>0\\ 0 \qquad\qquad Otherwise\end{cases} \tag{6}$$

where $T_s(V_x,V_j)$ is the trust that neighboring vehicle V_x has for the vehicle V_j at time s.

Total Trust

The indirect trust $IndirectT_s\left(V_i,V_j\right)$ calculated in (6) and the direct trust $DirectT_s(V_i,V_j)$ from (5) is used to compute total trust $T_s(V_i,V_j)$ based on the true reports sent by the vehicle V_j in time period s as :

$$T_s(V_i,V_j)=\begin{cases}\beta \times DirectT_s(V_i,V_j)+(1-\beta)\times IndirectT_s(V_i,V_j), \; if \;\; B_s(V_j)>0\\ 0.3 \quad Otherwise\end{cases} \tag{7}$$

Where $0.5 < \beta < 1$.

Vehicle V_i requests the trust of V_j from the reachable RSU. The total trust is updated as follows,

$$T(V_i,V_j) = \gamma \times T_s(V_i,V_j) + (1-\gamma) \times T_{RSU(V_j)} \tag{8}$$

$T_{RSU(V_j)}$ is the trust value provided by the RSU about the vehicle V_j. It is retrieved by the RSU from TrustBC. $T_s(V_i,V_j)$ is the trust value that vehicle V_i has about vehicle V_j. After determining the trust value of a sender, the receiver accepts the message from the sender which has a trust $T \geq T_{thr}$, if this condition is not satisfied the receiver rejects the event message.

$$Decision = \begin{cases} Accept & if\ T(V_i,V_j) \geq T_{thr} \\ Reject & Otherwise \end{cases} \tag{9}$$

The threshold value T_{thr} for trusting a message is set to 0.5. Hence, if the trust value $T(V_i,V_j)$ sender V_j is equal to or greater than the threshold T_{thr} the message will be accepted and considered to be credible/trustworthy and the honest vehicles are rewarded by the award factor (ω) for their honesty. Otherwise, the receiver vehicle V_i will discard the message and the message is classified as bogus and the sender's trust is reduced by the penalty factor (φ). The trust $T(V_i,V_j)$ can be updated as

$$T(V_i,V_j) = \begin{cases} T(V_i,V_j) + \omega & if\ T(V_i,V_j) \geq T_{thr} \\ T(V_i,V_j) - \varphi & if\ T(V_i,V_j) < T_{thr} \end{cases} \tag{10}$$

Algorithm 2: Trust Calculation on Vehicle

Input: Number of true messages A, Total number of messages B, Trust threshold(T_{thr}), Factor of reward(ω), Factor of punishment (φ).

Output: Direct trust(DirectT), Indirect trust(IndirectT), Total trust(T);

Calculate DirectT using (4);
Update DirectT using (5);
Calculate IndirectT using (6);
Calculate T using (7);
Update T using (8);
if ($T \geq T_{thr}$) **then**
    Accept message;
    Classify vehicle as honest;
    $T = T + \omega$;
    Store T in vehicle historic table;
else
    Discard message;
    Classify vehicle as malicious;
    $T = T - \varphi$;
    Store T in vehicle historic table;
end

6.2 Trust calculation on RSU

The details of the RSU level trust management are described below:

Step 1: Trust Calculation

Vehicles send event messages with each message containing an event description, a signature, and a public-key certificate to the RSU. The message verification policy is adopted by the RSU to identify the message trustworthiness as bellow:

- Verify the sender location
- Verify the time-stamp
- Verify the signature

After the received event message is verified according to the verification policy mentioned above, the sender vehicle's trust value is measured. The RSU will compute and store the new trust value of the sender vehicle into the TrustBC blockchain. If the number of true messages increases, the trust value of a vehicle increases. Trust is computed as follows

$$T(V_i) = \frac{C_1}{C_1 + C_2} \begin{cases} if\ event\ message\ is\ correct, then\ C_1 = C_1 + 1 \\ if\ event\ message\ is\ incorrect, then\ C_2 = C_2 + 1 \end{cases} \tag{11}$$

where C_1 is correct and C_2 is incorrect event message counter. From TrustBC, the RSU retrieves the sender vehicle's previous trust value. The trust value is updated as,

$$T_{New}(V_i) = \psi \times T(V_i) + (1-\psi) \times T_{RSU(V_i)} \tag{12}$$

where $0.5 < \psi < 1$, and $T_{RSU(V_i)}$ is the old trust value of the vehicle V_i which is retrieved from the TrustBC. If the trust value $T_{New} \geq T_{thr}$, the message is accepted, otherwise it will be discarded. The new trust value of a vehicle will be stored in the TrustBC blockchain. Vehicles with trust value $< T_{thr}$ are put in the malicious list. The RSU sends list of malicious vehicles to the TA. TA revokes their public keys and these vehicles will no longer receive any services from the vehicular network.

Step 2: Event Validation

If the number of true event messages is greater than a threshold (a new event is confirmed to have happened if 10 event messages are received (E_{thr})), then the event is valid. The RSU will enter the transaction phase after validating the event. In this phase, a transaction that includes the event description, along with the event proof, all signatures, and certificates belonging to the participating vehicles will be created by the RSU.

Step 3: Miner election and block generation

There is no constant central point to run the blockchain due to the decentralized nature of the network. Hence, new blocks are generated periodically by electing a miner from all RSUs. Proof-of-work (PoW) is the most common method of electing miners in blockchain-based systems, like Bitcoin. Each RSU continuously changes the nonce and calculates the block's hash values including the nonce. Anyone with a hash value lower than a threshold becomes a miner and can publish his blocks. The same threshold is used by all RSUs, which makes it easier for RSUs with more processing power to obtain the correct nonce and win the election. It ensures that data stored in the blockchain is updated in a timely manner.

Step 4: Distributed consensus

In order to add a block to its blockchain, the RSU must check whether the nonce provided by the miner is valid. It is possible for the RSU to receive more than one block simultaneously. As a result, the blockchain begins to fork. The solution to this problem is to implement a distributed consensus mechanism. In each RSU, a fork is chosen and blocks are added to that fork after it. As more RSUs begin to acknowledge a fork, it grows faster than other forks. To ensure a distributed consensus, the longest fork is selected, while others are discarded. Furthermore, each RSU should attempt to add the blocks it created in the discarded forks to the blockchain. Consequently, all RSUs are storing the same version of the blockchain, ensuring consistency.

Algorithm 3: Trust Calculation on RSU

Input: Number of true messages C_1, Number of false messages C_2, Old trust $T_{RSU(V_j)}$ of a vehicle from TrustBC, Trust threshold(T_{thr}), Event threshold(E_{thr});
Output: Trust value (T_{New});

Check the new message according to validation policy;
Calculate the trust value T using (11);
Update the trust value T_{New} using (12);
if ($T_{New} \geq T_{thr}$) **then**
    Accept message;
    Store T in TrustBC blockchain;
    Counter++;
else
    Add a vehicle to the malicious list;
    Goto step 1;
end
if (Counter= E_{thr}), **then**
    RSU announces event notification;
    RSU creates a transaction containing event details;
else
    Goto step 1;
end
Miner election and block generation;
if (Nonce is VALID) **then**
    RSUs add the block to their versions of blockchains;
else
    Discard the block;
end

7. Security Analysis

Message Authentication and Integrity

This property emphasizes that neither a malicious vehicle nor an adversary can forge a legitimate signature. The authentication of the public key's certificate of a vehicle is ensured by the CertificateBC and RevocationBC. The signature on each event message is generated

using the sender vehicle's private key, and receivers can check the sender's public keys to verify the signatures. The adversary is unable to produce a valid signature since it lacks access to this private key.

Anti-Bogus message attack

Malicious event messages can be generated and sent to other vehicles and RSUs by malicious vehicles. The trust model allows vehicles to accept only trustworthy messages from other vehicles and enables RSUs to broadcast event notifications about only verified events to vehicles in its communication range.

Replay Attack Prevention

To carry out a reply attack, attackers simply need to replay a previously received valid message. The event time is stored in the message in our scheme. When a vehicle or RSU receives a message, it compares the current with the event time. An adversary won't be able to execute a reply attack only if it can tamper with the message's content and fake a legitimate signature. Therefore, the chances of being able to successfully launch a replay attack are low.

DDoS (Distributed Denial of Service) Attack Resistance

Our scheme inherits the blockchain's resistance to DDoS attacks, assuring that no unauthorized transactions are recorded in the blockchain and no changes are made to transactions.

Privacy Preservation and Traceability

To eliminate the connection between the public key and the real identity, vehicles use the public key as a pseudonym. The public key-real identity pairs' database is stored in TA to maintain a balance between security and privacy. Since only the TA has access to the real identity of any public key, TA can trace a malicious vehicle as it broadcasts bogus messages or engages in misbehaviors.

8. Performance Evaluation

Our trust management model's performance is tested through simulations in the presence of malicious vehicles in the network. We used the open-source framework, Veins [37], the traffic simulator, SUMO [38], and the discrete event simulator, OMNET++ [39], to carry out our simulations.

The proposed scheme utilizes the location and time information in event messages to verify the sender's location, the event time, and the recommendation degree. Once the sender location and event time are verified to be true as well as the recommendation degree is less than a threshold, the event message is considered true. Next, the receiver vehicle calculates the total trust of the sender vehicle by integrating the computed direct trust, indirect trust, and the trust value sent by the RSU. Moreover, RSU performs additional verification for the event messages received from vehicles using sender location, time-stamp, and signature to identify their credibility. Then it calculates the vehicles' trust values. In the end, the trust threshold value is used to decide whether the event message is trustworthy or bogus.

BTM scheme calculates vehicle trust from beacon messages and calculates data trust from checking the credibility of beacon messages and event messages. The vehicle trust is calculated using cosine similarity between the claimed velocity, direction, and position of the vehicle and the estimated values. The data trust is obtained by computing the similarity

between received event messages and beacon messages using the Tanimoto coefficient. In the next step, the combined trustworthiness of the received event message will then be determined using vehicle trust, data trust, and reputation value. Trust is combined by Dempster-Shafer's theory (DST). Finally, the trust degree threshold is used to make a decision.

BTMS-FDD uses the density and speed information from received beacon messages for establishing trust with neighboring vehicles. All vehicles are initially assigned a trust value of 0. Then, positive or negative trusts are assigned based on the correctness of the data. In order to validate an event message, speed and location information are used. The receiver vehicle utilizes the beacon and relative data from the event message. Beacon and relative data consist of the speed and position of the vehicle. The receiver vehicle uses speed and position to estimate the distance covered by the event message. In the case of a relation between two messages of a vehicle, the event is considered true and vice versa.

Table 1. Simulation Details

Parameter		Value
Simulation Details	Simulation Area (km x km)	2 x 2
	Simulation Time	500 Sec
	Number of RSUs	5
	Communication range	250 m
Scenario	Legitimate Vehicles	200
	Malicious Vehicles (%)	10, 20, 30, 40, 50
Protocols	Network Protocol	IEEE 1609.4
	MAC Protocol	IEEE 802.11p
Trust Model	Initial Trust	0.3
	Trust threshold(T_{thr})	0.5
	Event threshold(E_{thr})	10
	The factor of honesty (ω)	0.01
	The factor of punishment (φ)	0.1
	Weight Factors $\alpha, \beta, \gamma, \psi$	0.6
Adversary Model	Actions	Create Bogus Messages

8.1 End-To-End Delay

End-to-End delay refers to the time it takes a packet to travel from a source vehicle to a destination vehicle. It is calculated as below,

$$End\ to\ End\ Delay = \sum T_A - T_G \tag{13}$$

Where packet arrival time is denoted by T_A and packet generation time is denoted by T_G . In the proposed model, the legitimacy of a message must be checked, which causes a delay. We compare the delay of our model with two other models: BTM and BTMS-FDD under different percentages of malicious vehicles. As depicted in **Fig. 4** increasing the percentage of malicious vehicles increases end-to-end delay for all the schemes. Despite this, the proposed scheme incurred less delay than other schemes. For instance, when the network has 50% malicious vehicles, our scheme experiences a 1100ms delay which is 8.3% and 12% efficient compared to BTM and BTMS-FDD respectively.

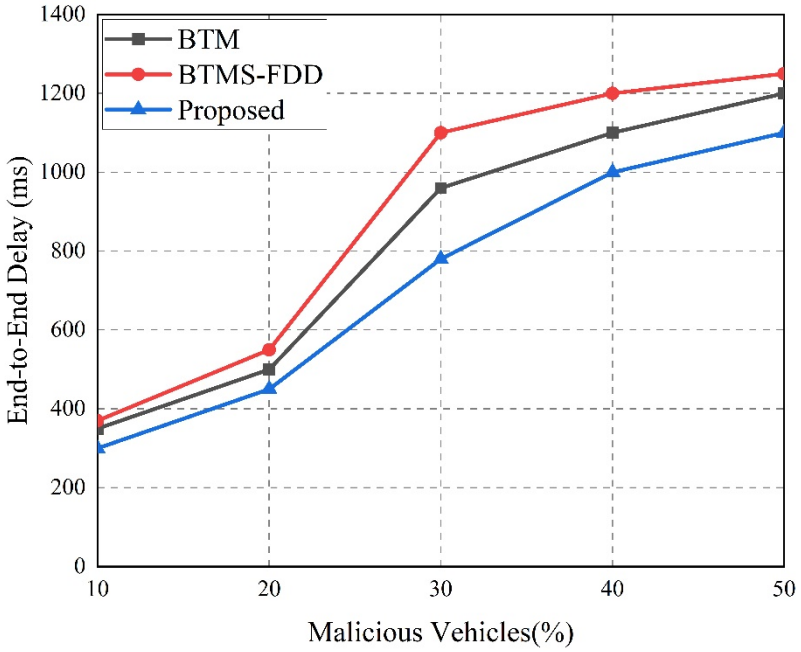

Fig. 4. Delay

8.2 Trust

In **Fig. 5**, the trust metric of the proposed trust model is compared with those of BTM and BTMS-FDD when the network contains malicious vehicles.

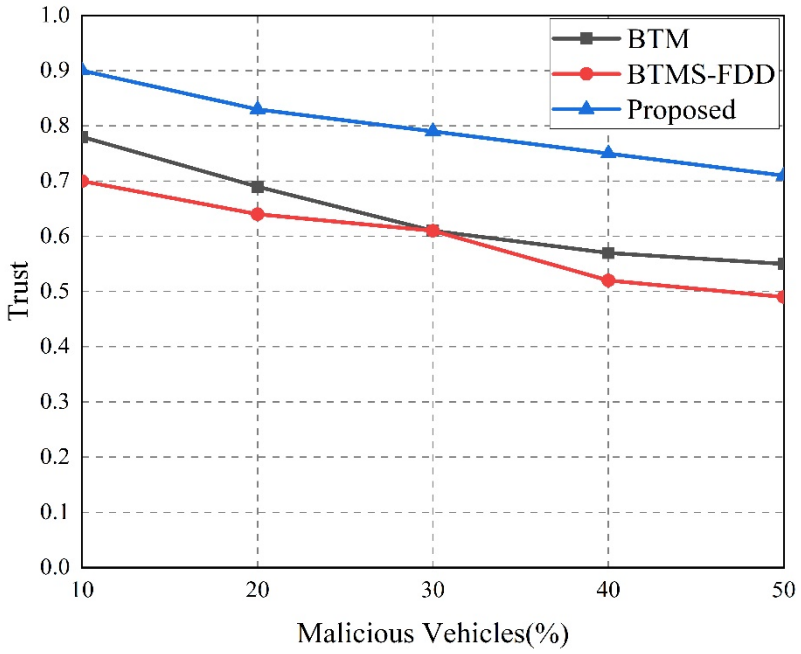

Fig. 5. Trust

From **Fig. 5**, trust in the network reduces as the percentage of malicious vehicles increases. In other words, the trust model's ability to propagate trusted packets reduces due to the existence

of malicious vehicles. When the network has 50% malicious vehicles, the trust value in the proposed model is 0.71 which is, 29% and 44.9% higher than BTM and BTMS-FDD respectively. That is because the proposed trust model relies on several factors (direct, previous direct, and indirect trust) and threshold when calculating the trust value.

8.3 False Event Success Rate

The relationship between the percentage of malicious vehicles and the false event success rate is evaluated. As shown in **Fig. 6**, the false event success rate rises with an increase in the number of malicious vehicles. When the percentage of malicious vehicles is less than 50%, the false event success rate is almost below 10%. When the malicious vehicle count reaches 50%, the false event success rate increases significantly, and the three trust models begin to report incorrect events more frequently. Our proposed model outperforms the BTM and BTMS-FDD due to the two-level check for the trustworthiness of event messages (vehicle level check and RSU level check) which reduces the false event success rate.

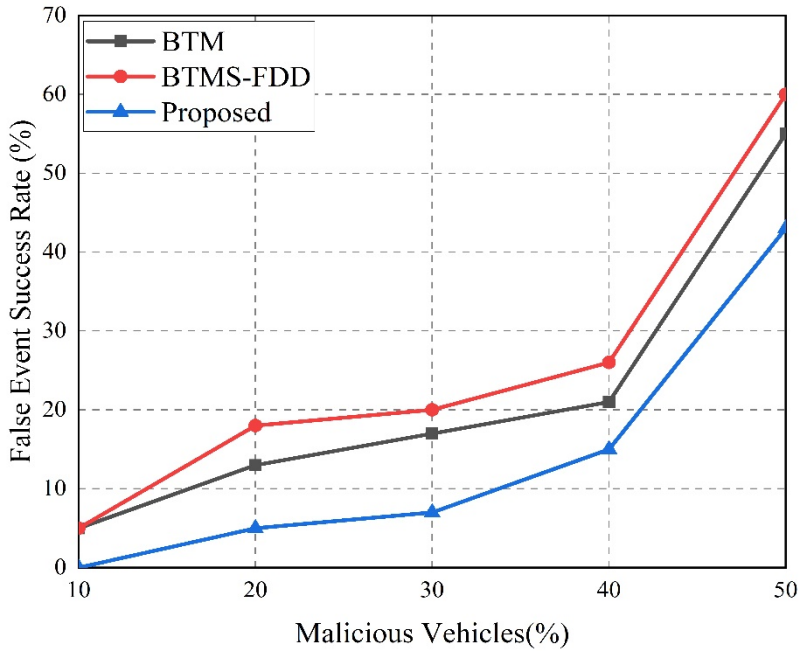

Fig. 6. False Event Success Rate

8.4 Bogus Message Detection Rate

Whenever the trust value of a malicious vehicle goes below the set threshold, its messages are detected as bogus messages. In all the models, the detection rate of bogus messages tends to decrease when the number of malicious vehicles increases, this is because teams of malicious vehicles collaborate to spread bogus messages. Therefore, fewer bogus messages can be detected. When 50% of malicious vehicles are present in the network, our model can detect 63% of total bogus messages sent whereas BTM and BTMS-FDD can detect 51% and 55% respectively. This is because every vehicle in our scheme uses the direct trust, previous trust as well as indirect trust value to compute the trust value of the message initiator. **Fig. 7** shows the bogus message detection rate.

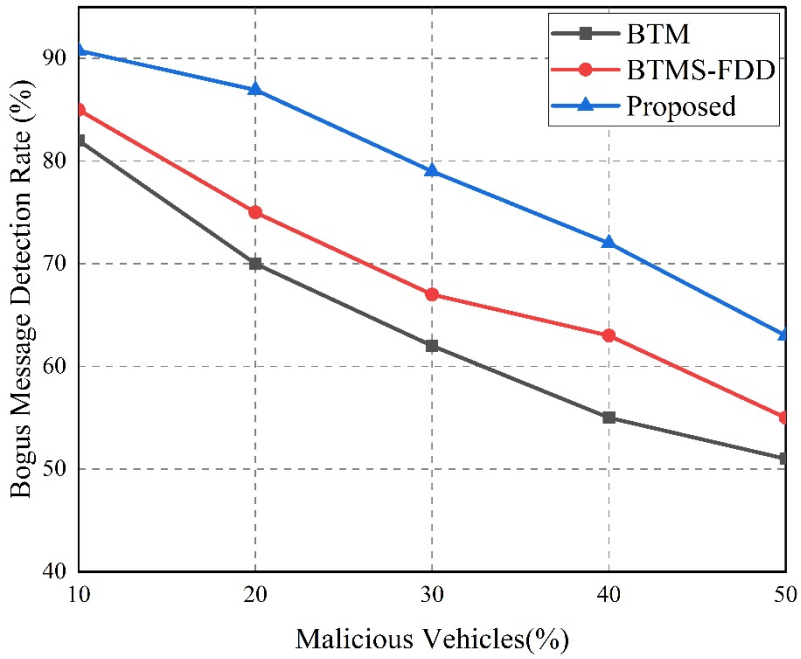

Fig. 7. Bogus Message Detection Rate

8.5 Number of Dropped Bogus Messages

Since legitimate vehicles are able to receive and verify bogus messages, the number of dropped bogus messages increases when the network contains a larger number of legitimate vehicles.

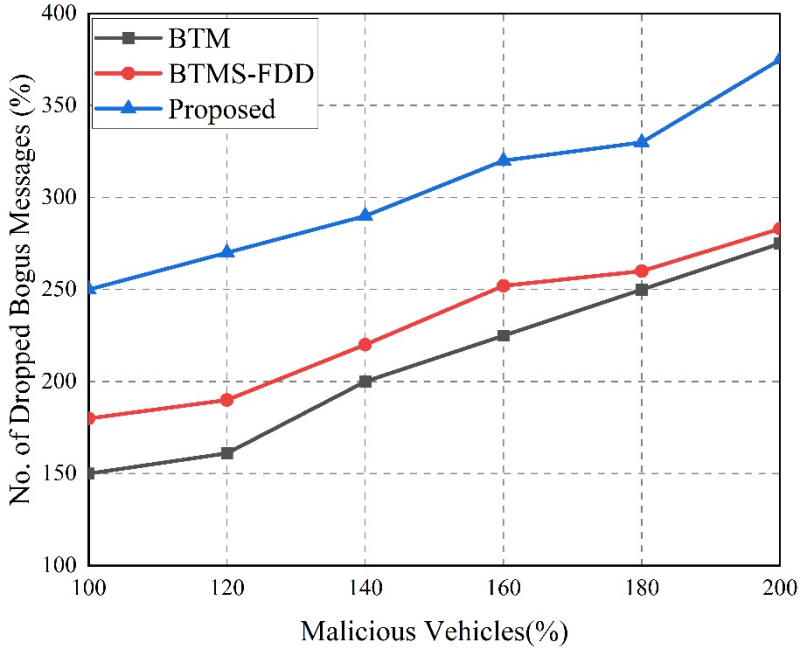

Fig. 8. No. of Dropped Bogus Messages (With 20% malicious vehicles)

As depicted in **Fig. 8**, at 200 vehicles with 20% being malicious, the number of dropped bogus messages for the proposed model is 375 which is 36% and 32.5% more than BTM and BTM-FDD respectively. We attribute the good performance of our model to multi-factors considered in total trust computation before a message is accepted or dropped i.e., direct trust, indirect trust, and previous trust of vehicles.

9. Conclusion

In this paper, we designed four blockchains namely: CertificateBC and RevocationBC for authentication, TrustBC for storing trust values of vehicles, and EventBC in order to save verified event messages. PoW mechanism is used to achieve consensus and to synchronize the TrustBC and EventBC blockchains versions on RSUs. In V2V and V2I communications, public keys are used as pseudonyms in order to protect vehicle identity privacy as well as offer anonymous authentication. The proposed trust management scheme calculates the total trust value of a vehicle by using direct experiences, indirect information about senders. The calculated trust value assists vehicles and RSUs in identifying malicious vehicles and the bogus messages they generate. Honest vehicles sending trustworthy messages are rewarded and malicious vehicles sending bogus messages are punished. RSUs send lists of malicious vehicles to the TA which revokes their public keys. Revoked public keys are stored in RevocationBC. Finally, we analyze and evaluate the various aspects regarding the security and performance of the proposed scheme. The results show that the proposed scheme not only provides an efficient trust management solution for VANETs but also outperforms BTM and BTMS-FDD schemes.

References

[1] S. Zeadally, R. Hunt, Y. S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETS): Status, results, and challenges," *Telecommun. Syst.*, vol. 50, no. 4, pp. 217–241, Aug. 2012. Article (CrossRef Link)

[2] Y. Li, "An Overview of the DSRC/WAVE Technology," in *Proc. of Quality, Reliability, Security, and Robustness in Heterogeneous Networks*, vol. 74, X. Zhang and D. Qiao, Ed. Berlin, Germany: Springer, pp. 544–558, 2010. Article (CrossRef Link)

[3] A. K. Malhi, S. Batra, and H. S. Pannu, "Security of vehicular ad-hoc networks: A comprehensive survey," *Comput. Secur.*, vol. 89, p. 101664, Feb. 2020. Article (CrossRef Link)

[4] R. W. Van Der Heijden, S. Dietzel, T. Leinmüller, and F. Kargl, "Survey on misbehavior detection in cooperative intelligent transportation systems," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 1, pp. 779–811, 2019. Article (CrossRef Link)

[5] C. A. Kerrache, C. T. Calafate, J. C. Cano, N. Lagraa, and P. Manzoni, "Trust Management for Vehicular Networks: An Adversary-Oriented Overview," *IEEE Access*, vol. 4, pp. 9293–9307, Dec. 2016. Article (CrossRef Link)

[6] R. Hussain, J. Lee, and S. Zeadally, "Trust in VANET: A Survey of Current Solutions and Future Research Opportunities," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 5, pp, 2553-2571, 2021. Article (CrossRef Link)

[7] M. S. Sheikh, J. Liang, and W. Wang, "A Survey of Security Services, Attacks, and Applications for Vehicular Ad Hoc Networks (VANETs)," *Sensors*, vol. 19, no. 16, p. 3589, Aug. 2019. Article (CrossRef Link)

[8] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANet security challenges and solutions: A survey," *Veh. Commun.*, vol. 7, pp. 7–20, Jan. 2017. Article (CrossRef Link)

[9] D. Zheng, C. Jing, R. Guo, S. Gao, and L. Wang, "A Traceable Blockchain-Based Access Authentication System With Privacy Preservation in VANETs," *IEEE Access*, vol. 7, pp. 117716–117726, Aug. 2019. Article (CrossRef Link)
[10] T. Zhang and Q. Zhu, "Distributed Privacy-Preserving Collaborative Intrusion Detection Systems for VANETs," *IEEE Trans. Signal Inf. Process. over Networks*, vol. 4, no. 1, pp. 148–161, Feb. 2018. Article (CrossRef Link)
[11] J. Ren and L. Harn, "An efficient threshold anonymous authentication scheme for privacy-preserving communications," *IEEE Trans. Wirel. Commun.*, vol. 12, no. 3, pp. 1018–1025, Jan. 2013. Article (CrossRef Link)
[12] D. He, S. Chan, and M. Guizani, "An Accountable, Privacy-Preserving, and Efficient Authentication Framework for Wireless Access Networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 3, pp. 1605–1614, March 2016. Article (CrossRef Link)
[13] A. Wasef and X. S. Shen, "EMAP: Expedite message authentication protocol for vehicular ad hoc networks," *IEEE Trans. Mob. Comput.*, vol. 12, no. 1, pp. 78–89, Jan. 2013. Article (CrossRef Link)
[14] Q. Feng, D. He, S. Zeadally, and K. Liang, "BPAS: Blockchain-Assisted Privacy-Preserving Authentication System for Vehicular Ad Hoc Networks," *IEEE Trans. Ind. Informatics*, vol. 16, no. 6, pp. 4146–4155, June 2020. Article (CrossRef Link)
[15] R. Lu, X. Lin, H. Zhu, P. H. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in *Proc. of IEEE INFOCOM*, Phoenix, AZ, USA, pp. 1229-1237, 2008. Article (CrossRef Link)
[16] 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. 22, no. 12, pp. 7408-7420, 2021. Article (CrossRef Link)
[17] S. Rowan, M. Clear, M. Gerla, M. Huggard, and C. Mc Goldrick, "Securing vehicle to vehicle communications using blockchain through visible light and acoustic side-channels," *arXiv*, April 2017.
[18] A. Dorri, M. Steger, S. S. Kanhere and R. Jurdak, "BlockChain: A Distributed Solution to Automotive Security and Privacy," *IEEE Communications Magazine*, vol. 55, no. 12, pp. 119-125, Dec. 2017. Article (CrossRef Link)
[19] M. C. Chuang and J. F. Lee, "PPAS: A privacy preservation authentication scheme for vehicle-to-infrastructure communication networks," in *Proc. of 2011 Int. Conf. Consum. Electron. Commun. Networks, in Proc. of CECNet 2011*, Xianning, China, pp. 1509–1512, 2011. Article (CrossRef Link)
[20] J. Cui, J. Zhang, H. Zhong, and Y. Xu, "SPACF: A secure privacy-preserving authentication scheme for VANET with cuckoo filter," *IEEE Trans. Veh. Technol.*, vol. 66, no. 11, pp. 10283–10295, Nov. 2017. Article (CrossRef Link)
[21] B. Luo, X. Li, J. Weng, J. Guo, and J. Ma, "Blockchain Enabled Trust-Based Location Privacy Protection Scheme in VANET," *IEEE Trans. Veh. Technol.*, vol. 69, no. 2, pp. 2034–2048, Feb. 2020. Article (CrossRef Link)
[22] M. Raya, P. Papadimitratos, V. D. Gligor, and J. P. Hubaux, "On data-centric trust establishment in ephemeral ad hoc networks," in *Proc. of IEEE INFOCOM*, Phoenix, AZ, USA, pp. 1238-1246, 2008. Article (CrossRef Link)
[23] R. El Sibaï, T. Atéchian, J. B. Abdo, J. Demerjian, and R. Tawil, "A new software-based service provision approach for vehicular cloud," in *Proc. of GSCIT 2015*, Sousse, Tunisia, pp. 1-6, 2015. Article (CrossRef Link)
[24] S. F. Tzeng, S. J. Horng, T. Li, X. Wang, P. H. Huang, and M. K. Khan, "Enhancing Security and Privacy for Identity-Based Batch Verification Scheme in VANETs," *IEEE Trans. Veh. Technol.*, vol. 66, no. 4, pp. 3235–3248, April 2017. Article (CrossRef Link)
[25] Y. Xiao and Y. Liu, "BayesTrust and VehicleRank: Constructing an Implicit Web of Trust in VANET," *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2850–2864, March 2019. Article (CrossRef Link)

[26] M. Azees, P. Vijayakumar, and L. J. Deboarh, "EAAP: Efficient Anonymous Authentication with Conditional Privacy-Preserving Scheme for Vehicular Ad Hoc Networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 9, pp. 2467–2476, Sept. 2017. Article (CrossRef Link)
[27] R. Lu, X. Lin, T. H. 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. 2012, Article (CrossRef Link)
[28] W. Li and H. Song, "ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 4, pp. 960–969, April 2016, Article (CrossRef Link)
[29] A. Kchaou, R. Abassi, and S. Guemara, "Toward a distributed trust management scheme for VANET," in *Proc. of the 13th International Conference on Availability, Reliability and Security*, pp. 1-6, Aug. 2018, Article No. 53. Article (CrossRef Link)
[30] Y. M. Chen and Y. C. Wei, "A beacon-based trust management system for enhancing user centric location privacy in VANETs," *J. Commun. Networks*, vol. 15, no. 2, pp. 153–163, April 2013. Article (CrossRef Link)
[31] M. Arshad et al., "Beacon trust management system and fake data detection in vehicular ad-hoc networks," *IET Intell. Transp. Syst.*, vol. 13, no. 5, pp. 780–788, May 2019. Article (CrossRef Link)
[32] I. Ali, M. Gervais, E. Ahene, and F. Li, "A blockchain-based certificateless public key signature scheme for vehicle-to-infrastructure communication in VANETs," *J. Syst. Archit.*, vol. 99, p. 101636, Oct. 2019. Article (CrossRef Link)
[33] X. Zhang and X. Chen, "Data Security Sharing and Storage Based on a Consortium Blockchain in a Vehicular Ad-hoc Network," *IEEE Access*, vol. 7, pp. 58241–58254, Jan. 3, 2019. Article (CrossRef Link)
[34] H. Li, L. Pei, D. Liao, G. Sun, and D. Xu, "Blockchain Meets VANET: An Architecture for Identity and Location Privacy Protection in VANET," *Peer-to-Peer Netw. Appl.*, vol. 12, no. 5, pp. 1178–1193, Jul. 2019. Article (CrossRef Link)
[35] M. Atzori, "Blockchain-Based Architectures for the Internet of Things: A Survey," *SSRN Electron. J.*, Apr. 2017. Article (CrossRef Link)
[36] L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer, "A scalable robust authentication protocol for secure vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 59, no. 4, pp. 1606–1617, 2010. Article (CrossRef Link)
[37] C.Sommer, J. Härri, F. Hrizi, B. Schünemann, and F. Dressler, "Simulation tools and techniques for vehicular communications and applications," *Vehicular Ad Hoc Networks*, Cham, Switzerland: Springer, pp. 365–392, 2015. Article (CrossRef Link)
[38] M. Behrisch, L. Bieker, J. Erdmann, and D. Krajzewicz, "SUMO— Simulation of urban mobility: An overview," in *Proc. of 3rd Int. Conf. Adv. Syst. Simul.*, Barcelona, Spain, pp. 55–60, 2011.
[39] X. Xian, W. Shi, and H. Huang, "Comparison of OMNET++ and other simulator for WSN simulation," in *Proc. of 3rd IEEE Conf. Ind. Electron. Appl.*, Singapore, pp. 1439–1443, Jun. 3-5, 2008. Article (CrossRef Link)

Waheeb Ahmed received his B.E. degree in Computer Science and Engineering from Aden University, Yemen, in 2008, the master degree in Computer Applications from Osmania University, India, in 2013 and currently pursuing a Ph.D. degree in Computer Science and Technology, Dalian University of Technology, China. His research interests include Vehicular Ad hoc Networks, Blockchain, and Security.

Di. Wu was born in April 1972, Liaoning, associate professor and master tutor of School of Computer Science and Technology /Dalian University of Technology, Dalian, China. The main research directions are the VANETs, Internet, wireless ADHOC networks, computer network and the computer simulation application in engineering, etc. Since 2001, he is the associate professor of Dalian University of technology, college of computer, and the Internet of things institute. 2009-2010, he was a visiting scholar at the Canadian Simon Fraser University, college of compute.1999-2001, he is a postdoctoral at Northeastern university, institute of computer application and the network and communication center. He has published more than 50 papers and 2 patents in domestic and international academic conferences and journals. He is a senior member of the computer society.

Daniel Mukathe received his Bachelor in Computer Science from Masinde Muliro University of Science and Technology, Kenya. Currently, he is a student at the School of Computer Science and Technology, Dalian University of Technology, China. His research interest includes VANET, Internet of Things and Blockchain.