A blockchain-based trust management with conditional privacy-preserving announcement scheme for VANETs

Xingchen Liu, Haiping Huang, *Member, IEEE*, Fu Xiao, *Member, IEEE*, Ziyang Ma

***Abstract*—As the infrastructure of intelligent transportation system, vehicular ad hoc networks (VANETs) have greatly improved traffic efficiency. However, due to the openness characteristics of VANETs, trust and privacy are still two challenging issues in building a more secure network environment: it is difficult to protect the privacy of vehicles and meanwhile to determine whether the message sent by the vehicle is credible. In this paper, a blockchain-based trust management model, combined with conditional privacy-preserving announcement scheme (BTCPS), is proposed for VANETs. Firstly, an anonymous aggregate vehicular announcement protocol is designed to allow vehicles to send messages anonymously in the non-fully trusted environment to guarantee the privacy of the vehicle. Secondly, a blockchain-based trust management model is present to realize the message synchronization and credibility. Roadside Units (RSUs) are able to calculate message reliability based on vehicles' reputation values which are safely stored in the blockchain. In addition, BTCPS also achieves conditional privacy since Trusted Authority can trace malicious vehicles' identities in anonymous announcements with the related public addresses. Finally, a mixed consensus algorithm based on Proof-of-work and Practical Byzantine Fault Tolerates algorithm is suggested for better efficiency. Security analysis and performance evaluation demonstrate that the proposed scheme is secure and effective in VANETs.**

***Index Terms*—VANETs, conditional privacy, trust management, blockchain, anonymous group signature**

I. INTRODUCTION

IN RECENT years, vehicular ad hoc networks (VANETs) have attracted the attention of academia and industry as the infrastructure of the intelligent transportation system. VANETs will play an important role in the IoT (Internet of Things) applications based on the emerging fifth generation (5G) technology [1]. VANETs can improve traffic efficiency and reduce the risk of traffic jams and accidents, because it allows important traffic driving information to be shared among vehicles [2-3].

However, the characteristics of mobility, limited resources and data disclosure of VANETs may cause various problems in practical applications. Wherein, the problem of trust and privacy raises concerns especially when malicious vehicles exist in VANETs. A malicious vehicle can not only monitor all the messages in the network to track other vehicles, but also forge some important data to deceive others. In the extreme case, these forged traffic messages may lead to injuries and even deaths. Thus, unresolved trust and privacy issues probably bring great potential risks to traffic safety.

Trust management is considered as an effective measure to solve the trust and privacy problems in VANETs. A well-designed trust management model can guarantee the reliability of the broadcasting message in VANETs by rewarding honest vehicles or publishing malicious ones based on reputation evaluation and identity authentication. The existing trust management models can be divided into two categories [4]: the centralized model and the distributed one. In the centralized model [5-7], the trust management mechanism is deployed on a centralized server. However, the cost of maintaining the centralized server is very high, and meanwhile such centralized model is easy to be the target of attackers, which will cause catastrophic consequences once single points of failure occurs. In order to overcome the defect brought by the centralized model, some researchers [8-10] adopt a distributed architecture as the VANETs' trust management model, where trust evaluation is usually performed by the Roadside Units (RSUs for short). The distributed model has greatly improved efficiency and addressed the problem of single points of failure. Wherein, each RSU is mainly responsible for trust management within its communication range. However, some problems in complex VANETs environment such as untimely trust data synchronization between RSUs will cause a serious adverse effect on the implementation of reputation evaluation. For example, after a vehicle has been punished and marked with "malicious one" in one certain RSU management area, another RSU may not synchronize the real-time trust evaluation message and consider it to be honest when the malicious vehicle moves to this area. In addition, in practical application, RSUs distributed along the road are usually semi-trusted and vulnerable to being compromised by attackers, in the case strong privacy protection strategy is necessary [11].

This work is supported by the National Key Research and Development Program (No. 2018YFB0803403), the National Natural Science Foundation of China (Nos. 61672297 and 61872194), the Key Research and Development Program of Jiangsu Province (Social Development Program, No. BE2017742), and the Jiangsu Natural Science Foundation for Excellent Young Scholars (Nos. BK20160089 and BK20170039).

X. C. Liu, H. P. Huang, F. Xiao and Z. Y. Ma, are with the School of Computer Science, Software and Cyberspace Security and Jiangsu High Technology Research Key Laboratory for Wireless Sensor Networks, Nanjing University of Posts and Telecommunications, Nanjing, Jiangsu, China, 210023 (e-mail: hhp@njupt.edu.cn)

To resolve the problems above, blockchain will be employed in this paper as a distributed ledger technology, which was first proposed by Nakamoto and applied to Bitcoin [12]. Blockchain can be used in many fields of Internet of things such as smart city [13-14], energy trading [15-17], edge computing [18], vehicular social networks [19] and medical IoT systems [20], due to its features of decentralization, tamper-proofing, trustworthiness and anonymity, which can reasonably solve trust and security problems in VANETs. Moreover, benefiting from the distributed consensus algorithm, blockchain enables RSUs to work together and maintain a consistent database in order to ensure the synchronization of reputation evaluation messages. Blockchain can still maintain reliable operation even if some nodes are invaded or fail, which can effectively resist the RSUs being compromised attacks.

Furthermore, we also notice that most of the studies of trust management in VANETs haven't focused on protecting the privacy of the vehicles, where the real identity information of the vehicles will be easily leaked when they interact with each other. Therefore, VANETs should allow vehicles broadcast messages anonymously. However, this way may give malicious vehicles opportunities to commit a crime. For example, some malicious vehicles deliberately send messages that do not conform to the traffic conditions, which will result in serious accidents, such as traffic jams and even threats to life. Therefore, an effective solution such as anonymous aggregate vehicular announcement protocol combined with blockchain is expected to be adopted in order to achieve conditional privacy, which will be of concern in VANETs since it can not only protect honest vehicles' identities but also traces malicious vehicles' identities. In this case, trust evaluation and reputation calculation is also important in order to quickly identify malicious vehicles.

In addition, the cost of establishing a traditional public blockchain is huge due to the characteristics of resource-constrained of VANETs. So we designed a mixed consensus algorithm based on proof-of-work and Practical Byzantine Fault Tolerates (PBFT) algorithm [21] in order to achieve better efficiency. All the RSUs compete to be a miner and some authorized RSUs undertake the consensus work in blockchain. When the number of authorized RSUs remains as a constant, the total time to reach consensus for a new block is stable regardless of the size of VANETs [22].

Aiming at the challenging problems mentioned above, we propose a blockchain-based trust management with conditional privacy-preserving scheme (a.b. BTCPS) for VANETs. The main contributions of this paper can be summarized as follows.

- An anonymous aggregate vehicular announcement protocol is designed in BTCPS. It exploits identity-based group signature technique to achieve conditional privacy: if a malicious vehicle sends a fake message, Trusted Authority can trace its identity in anonymous announcements with the public address in blockchain.
- A trust management model based on blockchain is proposed for VANETs to improve the security and reliability. Wherein, trust calculation based on logistic regression is designed to enhance the sensitivity of reputation value for malicious vehicle. In addition, a mixed consensus algorithm is designed to effectively reduce the cost caused by the traditional public blockchain.
- Theoretical analysis and simulation experiments are conducted to demonstrate that our scheme can achieve reliability, efficiency and conditional privacy-preserving for VANETs.

The rest of this paper is organized as follows. Related works are over-viewed in section 2. Section 3 describes the system model and design goals of BTCPS. An anonymous aggregate vehicular announcement protocol is present in section 4. In section 5, we propose a blockchain-based trust management model for VANETs. Performance evaluation is given in section 6 followed by our conclusion in section 7.

II. Related Work

A. Trust Management in VANETs

The establishment of trust is a fundamental issue in vehicular ad hoc networks [23]. It is an important method in determining the genuine traffic data and identifying malicious vehicles.

Li et al. [6] proposed a reputation-based announcement scheme for VANETs. Wherein, vehicles broadcast messages to their neighbors and the receivers report feedback to the reputation server. And then the reputation server aggregates feedback to produce and propagate reputation. Furthermore, pseudonyms are used to provide a certain level of privacy. However, in this scheme, trust management is established in a centralized manner, which is not practical for the realistic scenario since the number of vehicles are rising rapidly.

Raya M. et al [8] designed a distributed data-centric trust method for VANETs. Once a vehicle receives reports from others, it will calculate the trust level of each report as evidence. And then, these reports related to the same event along with corresponding trust levels will be combined. Finally, the event reliability will be judged by a decision scheme based on Bayesian inference and weighted voting. However, this method is only aiming at a single piece of data rather than at a vehicle. Li W. et al [24] put forward an attack-resistant trust management scheme which introduces two metrics: data trust and node trust, to evaluate the trustworthiness of traffic data and mobile vehicles, respectively. In their scheme, vehicles collect and analyze traffic data which would be regarded as evidence for trust evaluation by Dempster-Shafer theorem (DST). Unfortunately, this scheme is not applicable to the multi-vehicle application scenarios due to suffering from data sparsity problem. Monir et al. [9] designed a categorized trust-based message reporting scheme, where trust evaluation is performed by RSUs instead of vehicles. However, RSUs are not always completely trusted and attackers can invade and tamper the reputation values of vehicles. In [10], a distributed trust management architecture was also adopted, where a local authority (LA) uses a novel multi-weighted subjective logic (MWSL) method for calculating the reputation values of the vehicles. In their scheme, LA collects all the valid reputation

segments generated by the 1-hop neighbors of targeted vehicle. The aggregate reputation value will serve as credibility credentials for the target vehicle, which will be uploaded to a global reputation database to prevent attackers from invading and tampering the reputation information of vehicles. A fuzzy logic-based approach and a Q-learning approach [25] were proposed to calculate the one-hop neighborhood trust value and the indirect trust value, respectively, which can achieve better precision and recall in detecting malicious vehicles. Mahmood A. et al. [26] assumed that each VANET supporting a vehicular cluster and proposed a hybrid trust management model based on cluster formation, which not only can classify messages exchanged between nodes (i.e. vehicles) in the cluster, but also identify and eliminate multiple malicious nodes from the cluster in real time. Analogy of human society to establish trust relationship, Xia et al. [27] selected two attributes called subjective trust (ST) and recommended trust (RT) to quantify the vehicle trust level. However, the privacy problem of the vehicle has not been discussed in these schemes.

A privacy-aware reputation-based announcement scheme for VANETs is proposed by Chen L. [28]. This scheme allows vehicles exchange traffic information anonymously by using group signatures. A centralized reputation system and an off-line trusted authority are contained in this scheme and the reputation values of all vehicles are managed by the centralized server. In the most recent related work, Chen L. et al. used the Boneh-Boyen-shacham (BBS) short group signature scheme to overcome the defect of having to establish a secure channel for reputation value retrieval [29]. However, both of them still adopt the centralized trust management method.

B. Blockchain-Based Trust Management

Blockchain has been paid an increasing attention for trust management. Alexopoulos et al. [30] used blockchain for authentication to enhance the security of Trust Management (TM) systems. They introduced an abstract graph-theoretic model of TM systems for authentication, and meanwhile a matching blockchain model was regarded as a distributed, probabilistic state machine. In this scheme, the ability of traditional authentication system is improved by encoding trust information in blockchain to resist the stale information attack and the censorship attack. Bendiab K. et al [31] designed a novel blockchain-based trust model for identity management. In their proposed framework, blockchain is considered as a decentralized trust model that allows cloud service providers to manage their trust relationships without relying on a trusted third-party. Moreover, Goka S. et al [32] proposed a distributed management system based on blockchain for trust and reward in mobile ad hoc networks. This system can mitigate the negative influence of uncooperative nodes in the network. Therefore, based on the decentralized, safe and data consistent features of blockchain, it is expected to solve the existing problems of trust management system in VANETs.

III. System Model

In this section, we introduce the system model and design goals of our proposed scheme.

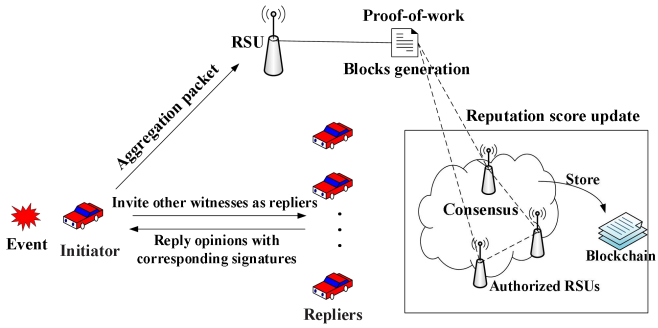


Fig. 1. The system model of BTCPS.

A. Overview of BTCPS

There are three entities in our proposed scheme: 1) a trusted authority; 2) RSUs; 3) vehicles. The system model of BTCPS is illustrated in Fig. 1.

Trusted Authority: TA plays a vital role in our scheme, which is responsible for maintaining the whole VANETs system. Therefore, TA is assumed to be fully trusted and cannot compromise with any opponent. RSUs and vehicles first complete the registration to TA when they want to participate in the network. And then, system public parameters generated by TA are assigned to these vehicles and RSUs when achieving successful registration. Furthermore, TA generates identity-based keys and public addresses (pseudonyms) for each vehicle, and records the relationship between vehicles and their corresponding public addresses.

RSUs: As the infrastructure in VANETs, RSU has a better storage and computation capacity in the trust management system [33]. RSU needs to collect aggregation packages from vehicles in its communication range to evaluate the credibility of messages and update the reputation values of the vehicles. In addition, all RSUs jointly maintain a consistent ledger and some authorized RSUs undertake the consensus work when constructing the blockchain. These RSUs are semi-trusted and may be invaded by attackers. However, due to the constrained capability of the attacker, we assume that only a small percentage of RSUs will be successfully invaded.

Vehicles: Each vehicle in the VANETs is installed with an on-board unit (OBU) which has wireless communication capability to permit the vehicle to communicate with other vehicles and RSUs to share messages [34]. Furthermore, we assume that each OBU has a tamper-proof device (TPD) to store the sensitive information, such as secret keys. The sensitive information stored in TPD is physically isolated. In order to prevent tampering, the cryptographic computations and system parameters should be maintained in the TPD.

BTCPS aims to build a privacy-preserving trust management announcement scheme, consisting of two components. The first component is an anonymous aggregate vehicular announcement protocol based on identity-based group signatures. This protocol maintains the reliability of announcements without revealing vehicles' privacy in the non-fully-trusted environment of VANETs. The specific process is described as follows: an initiator (vehicle) generates a message regarding a traffic incident and invites other

witnesses (vehicles) as repliers to agree with his/her message. Repliers response with corresponding signatures if they accept the signature of the initiator. The initiator generates an aggregation packet containing responses signed by repliers, which would be verified by its nearest RSU.

The second component is blockchain-based trust management model that works together with anonymous aggregate vehicular announcement protocol. When an event occurs, there will be multiple initiators sending the messages associated with this event to the nearest RSU. The RSU will first calculate the reputation values (including direct trust and indirect trust) of the initiators based on the logistic regression method [35]. The reputation value is used to determine whether reported messages are true or not. And then the RSU will pack the updated reputation data into a block and try to be elected as the miner to add this block into the blockchain. The miner based on proof-of-work will work together with the authorized RSUs to verify the correctness of the block and the correct block will be finally stored into the blockchain.

B. Design Goals

BTCPS is to design a secure reputation-based aggregate privacy-preserving announcement protocol for VANETs. Our proposed scheme has the following properties:

Conditional Privacy: In the phases of initiation and reply, any identity of vehicle cannot be revealed in BTCPS (anonymity). An adversary cannot link messages to the same sources under different pseudonyms by changing the address parameters in a period time (unlikability). Furthermore, only TA can trace the identity of malicious user (traceability).

Reliability: In BTCPS, the message announcement is reliable unless it is confirmed by the threshold number vehicles in VANETs (truthfulness). It is unlikely for an adversary to tamper the message content in announcement and the reputation data stored in the RSUs (tamper-resistance).

Timeliness: In BTCPS, a malicious vehicle may travel to different regions, so it is necessary to ensure that the RSUs in all regions have the latest reputation value of this malicious vehicle. Depending on the consensus algorithm of blockchain, the latest vehicle reputation information will be broadcast to all the RSUs in time.

IV. Anonymous for Aggregate Vehicular Announcement Protocol

In this section, we propose anonymous aggregate vehicular announcement protocol, where messages aggregation in VANETs is an effective way to realize threshold authentication and reduce the network overhead. The reliability of message announcement is improved in this way confirmed by the threshold number vehicles. The flow chart of our aggregate vehicular announcement protocol can be seen in Fig. 2.

A. Basic Application Scenario

We design our anonymous aggregate vehicular announcement protocol to apply to the following scenario:

Example: VANETs allow vehicles to generate and broadcast road-related messages (i.e. sending an announcement) such as

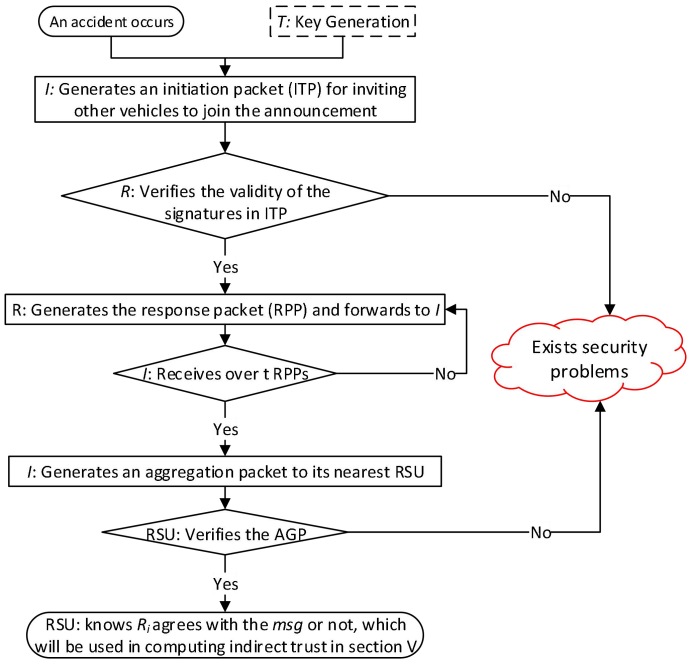


Fig. 2. The flow chart of anonymous aggregate vehicular announcement protocol.

traffic congestion and accidents to timely inform nearby vehicles. Bob (the owner of a vehicle) witnesses a traffic accident and would like to send a message announcement. However, messages generated by vehicles may be unreliable. To confirm the reliability of such an announcement message, Bob needs to cooperate with other witnesses. Bob firstly initiates a request to other witnesses for confirming his announcement message. After receiving the request, the witness verifies the message and returns his/her opinion, if he/she accepts the signature produced by Bob. When getting t replies, Bob makes an aggregate announcement with t confirmations to its nearest RSU. After that, the RSU checks the validity of this announcement.

B. Settings

1) Roles setting

The trusted authority is denoted as T, the *initiator* is denoted as I, and the replier is denoted as R. All symbols and their corresponding explanations are shown in Appendix A.

2) Packets setting

Three types of packets are generated by the vehicles in our secure aggregation announcement protocol.

a) Initiation packet (ITP) is a type of packet sent from an initiator to a group of witnesses. ITP contains the message reports, whose purpose is to inquire the witnesses whether agree with the announcement and sign it.

b) Response packet (RPP) is a type of packet from the replier to the initiator. RPP will be sent back to the initiator, if the witness receives the signature produced by I. Particularly, RPP involves two parts: the message reports and the decision about the message.

c) Aggregation packet (AGP) is a type of packet that is sent from an initiator to the RSU. An aggregate announcement and an identity-based group signature of this

announcement are contained in the AGP.

C. Protocol Details

We construct our anonymous aggregate vehicular announcement protocol by five phases:

- *Setup:* Firstly, public parameters and the corresponding master secret are generated by *T*. Public parameters are sent to all vehicles and the master secret is only stored in *T*. Furthermore, *T* generates identity-based keys for users in our anonymous aggregate vehicular announcement protocol.
- *Initiation:* A vehicle *I* finds an accident and would like to inform other vehicles. *I* will initiate a request for inviting them to join the announcement, in a way of forwarding ITP to other witnesses.
- *Reply:* A witness *R* is willing to confirm the message after accepting the signature of *I*. *R* will forward a RPP back to *I*, which contains information on whether or not to agree with the message.
- *Aggregation: I* generates an AGP by combining RPPs, and forwards the AGP to its nearest RSU.
- *Verification:* The RSU verifies the validity of AGP and knows R_i agrees with the msg or not.

Fig. 2 explains the process of anonymous aggregate vehicular announcement protocol. The keys are generated by T and updated periodically as needed. When an accident occurs, one vehicle I first generates an initiation packet (ITP) for inviting other vehicles to join the announcement. If the other vehicle R wants to join the announcement and verify the validity of ITP, it will generate the response packet (RPP) and forward to *I*. When I receives over t RPPs, an aggregation packet (AGP) is generated and sent to its nearest RSU. The RSU will verify the validity of AGP. And then, by verifying Eq. (5), the RSU knows R_i agrees with the msg or not, which will be used in computing indirect trust in section V.

In order to make the announcement protocol easier to understand, we make the following instructions: a) Let $x \leftarrow X$ denote selecting an element *x* from the set *X* at random. b) Let G be an addition group of points on an elliptic curve. Let $q \in G$ be an order of G and g is the generator of *G*. c) Let $E_k(x)$ be a symmetric encryption algorithm using k to encrypt *x*, and the length of k is *n*. d) Let H be an anti-collision hash function. These parameters are illustrated in Appendix A. The construction of aggregate announcement protocol is as follows:

Step 1: *Setup: T* conducts the following steps:

a) Generate H_0:$\{0.1\}^* \rightarrow \{0.1\}^n$, H_1:$G \rightarrow \mathbb{Z}_q$.

b) Select $(x_1,x_2,\cdots,x_n) \leftarrow \mathbb{Z}_q^*$, and define $\vec{x} = (x_1,x_2,\cdots,x_n)$ as the master private key vector.

c) Calculate $y_i = x_i \cdot g$, where $x_i \in (x_1,x_2,\cdots,x_n)$. Define $\vec{y} = (y_1,y_2,\cdots,y_n)$ as the master public key vector.

d) Publish the system public parameters $(G,q,\vec{y},H,E_k)$ to all and $\vec{x}$ is the corresponding master secret, which is only stored in *T*.

Furthermore, *T* generates identity-based keys for users. VIN (Vehicle identification Number) denotes the *ID* of a user. The identity-based key is generated for every user with its *ID* as follows:

d-1) *T* generates the following identity-based keys

$$sk_{ID} = \sum_{i=1}^{n} h_i x_i \ mod\ q. \quad (1)$$

and

$$pk_{ID} = \sum_{i=1}^{n} h_i y_i . \quad (2)$$

where h_i is the *i*th bit of $H_0(ID)$, i = 1, 2, ⋯, n.

d-2) *T* randomly selects an address parameter $ap \leftarrow \mathbb{Z}_q$ and calculates $g' = s \cdot g$.

d-3) *T* computes $z_i = x_i \cdot g'$, and $addr = \sum_{j=1}^{n} h_j z_j$, where h_j is the *j*th bit of $H_0(ID)$, i, j = 1, 2, ⋯, n. The public address of a user is $addr$, which is the pseudonym of a user with its *ID*.

d-4) sk_{ID} and $addr$ are confidentially delivered to the corresponding user via the secure channel.

Step 2: *Initiation: I* conducts the following steps:

a) An accident explanation message msg is produced in accordance with the specific context.

b) Generate the list set $(ID_1, ID_2, \cdots, ID_l) \leftarrow ID$ (including his/her own *ID*) where the value of l is the length of the ring signature.

c) For each $ID_i \in (ID_1, ID_2, \cdots, ID_l)$, it calculates $PK_i = \sum_{j=1}^{n} h_j y_j$ where h_j is the *j*th bit of $H_0(ID)$ and y_j is the *j*th value in $\vec{y}$, j = 1, 2, ⋯, n.

d) For each $ID_i \in (ID_1, ID_2, \cdots, ID_l)$, it generates identity-based signature (α_i,β_i) which is a valid EC-Elgamal signature of m_i. Selects $a_i,b_i \leftarrow \mathbb{Z}_q^*$ arbitrarily ($gcd(b_i,q-1) = 1$), and computes the following parameters:

$$\alpha_i = a_i g + b_i \cdot PK_i$$
$$\beta_i = - b_i^{-1} H_1(\alpha_i)$$
$$m_i = a_i \beta_i$$

e) Choose threshold value t and define ITP = ($< ID_1,\alpha_1,\beta_1,m_1 >, \cdots, < ID_l,\alpha_l,\beta_l,m_l >, msg,t)$, and then broadcast the ITP to invite other witnesses.

Step 3: *Reply: R* conducts the following steps:

a) *R* obtains ITP and calculates $PK_i = \sum_{j=1}^{n} h_j y_j$ for each ID_i.

b) For each ID_i, *R* confirms the following equation

$$m_i \cdot g = H_1(\alpha_i) \cdot PK_i + \beta_i \alpha_i. \quad (3)$$

R will not accept the validity of the ITP generated by *I*, provided that any one of the tuples $< \alpha_i,\beta_i,m_i >$ does not satisfy Eq.(3). Otherwise, *R* receives the ITP since all signatures in it are verified to be valid.

c) *R* computes $k = H_0(msg)$, where k is a symmetric key.

d) *R* generates the judgment parameter *J*, where $J = g'$ represents that *R* subscribes to the msg, while $J = 0$ represents that *R* objects to the msg. Furthermore, *R* computes $m' = E_k(J)$.

e) *R* selects $r \leftarrow \mathbb{Z}_q^*$ ($gcd(r,q-1) = 1$), and computes the EC-Elgamal signature (α',β'') of m'.

$$\alpha' = r \cdot g'$$
$$\beta' = (m' - sk_{ID} H_1(\alpha'))r^{-1}.$$

f) *R* defines $(m', (\alpha', \beta'), addr)$ as the RPP. And then, *R* forwards the RPP to *I*.

Step 4: *Aggregation:* After forwarding an ITP, *I* is waiting for RPPs. When *I* receives over *t* RPPs, *I* conducts the

following steps:

a) I combines RPPs to generate an AGP.

$\text{AGP} = (< addr_1, \alpha_1', \beta_1', m_1' >, \cdots, < addr_t, \alpha_t', \beta_t', m_t' >, msg)$

b) I forwards the AGP to its nearest RSU.

Step 5: *Verification:* When the nearest RSU receives an AGP, it confirms the AGP as following:

a) It gets and analyzes the AGP($< addr_1, \alpha_1', \beta_1', m_1' >, \cdots, < addr_t, \alpha_t', \beta_t', m_t' >, msg$).

b) It calculates $k = H_0(msg)$, where k is a symmetric key and it can prevent msg from being tampered.

c) For each $addr_i$, it calculates

$$J_i = E_k^{-1}(m'), i = 1, 2, \cdots, t. \quad (4)$$

If any $J_i \notin (g', 0)$, the RSU will not accept the validity of the ITP generated by I.

d) For each $addr_i$ (i = 1, 2, ⋯, t), it confirms the following equation

$$m_i' \cdot J_i = H_1(\alpha_i') \cdot addr_i + \alpha_i' \beta_i'. \quad (5)$$

If the tuple $< addr_i, \alpha_i', \beta_i', m_i' >$ satisfies Eq. (5), R_i agrees with this msg; Otherwise, R_i rejects it.

D. Security Analysis

1) Identity Privacy Preserving

During the message communication and authentication in VANETs, the anonymity of the vehicles is preserved.

When I and R communicate with each other, the identity of R can easily be anonymized by using a pseudonym. However, attackers may achieve the identities of vehicles by analyzing the related statistical information in the process of mutual communication. Therefore, the pseudonym of a vehicle should be transformed through changing the address parameter *ap* periodically. In this way, it is difficult for an adversary to link messages with different pseudonyms in VANETs.

Furthermore, we also should ensure the anonymity of I in the process of mutual communication by the use of ring signature. Since the identities of l vehicles will be covered in the ITP, R cannot acquire the real identity of I.

2) Message Integrity

Our proposed scheme can withstand against message modification attack.

During transmission in VANETs, an adversary has a high probability of attacking the transmitted packets, such as changing the content of the message. Once this attack occurs, messages in announcement will be changed, which will lead to the symmetric key k to be changed since $k = H_0(msg)$. Since $m' = E_k(J)$, m' will vary with the change of k, which will result in Eq. (5) is invalid in the verification phase.

3) Anti-forgery Attack

Forgery attack is a common attack in VANETs. In order to protect the transmitted packets, digital signature technology is adopted in BTCPS. However, it is difficult for an adversary to forge valid digital signatures due to the secret key is generated directly by TA and kept in TPD in VANETs. According to the assumption (seen in section 3.1), TA is fully trusted and TPD is physically isolated. Thus, the probability of forging a valid ElGamal signature by attacker is considered to be negligible.

4) Prevention of Replay Attack

For performing a reply attack, attackers just need to replay an existing legitimate message received before. In our vehicular announcement protocol, the event time is contained in the msg. When a vehicle or an RSU receives a packet, he/she will check the current time and the event time. An adversary will fail to perform a reply attack unless the adversary can tamper the content of the message and forges a valid signature. According to the analysis above, the probability of launching replay attack is considered to be negligible.

V. Blockchain-Based Trust Management Model

In this section, the blockchian-based trust management model together with anonymous aggregate vehicular announcement protocol allows the RSU to determine whether the reported msg is true or not.

A. Basic Idea

In order to apply the blockchain to the trust management model, each vehicle is given a blockchain address, which is actually the vehicle pseudonym in section IV. Our blockchain-based trust management model contains a reputation value update mechanism and a distributed consensus algorithm.

In the reputation value update mechanism, the reputation data is stored in the blocks. The reputation value will be evaluated by two metrics: direct trust value and indirect trust one. The former is depicted based on the vehicle historical behavior, and the latter is the recommendation degree, that is, the proportion of witnesses who agree with the msg in all witnesses. We can know whether witnesses agree with the msg or not by verifying Eq. (5) in section IV.

A distributed consensus algorithm will be carried out in order to synchronize all the data in the blockchain, which is shared by all RSUs in VANETs. Furthermore, a mixed consensus algorithm based on PoW and PBFT will be employed to ensure the data reliability and consensus efficiency.

B. Model Description

***Step* 1:** *calculation for the reputation of initiator:* The reputation value (involved direct trust and indirect trust) of the initiator I is calculated by the RSU using the logistic regression method. Direct trust consists of two parameters: abnormal rate and flag, respectively. Indirect trust is referred as recommendation degree.

The abnormal rate implies the probability that a vehicle has malicious behavior at the time s, which is the time parameter in reputation data. Let the vehicle I send $p_s(I)$ incorrect messages out of total $q_s(I)$ messages. The current abnormal rate $Ar_s(I)$ is given by

$$Ar_s(I) = \frac{p_s(I)}{q_s(I)}. \quad (6)$$

The abnormal rate will be compared against with a threshold value λ. If the abnormal rate exceeds the threshold λ, the value of flag denoted as $f_s(I)$ at the time s will be raised. The flag indicates the possible malicious behavior of the initiator. And the flag can be lowered if the vehicle maintains honest

activities.

Recommendation degree totally reflects the attitudes of witnesses towards msg. At the time s, $a_s(I)$ indicates the number of witnesses who agree to this msg; however, $d_s(I)$ denotes the number of witnesses who disagree with this msg. And then, the recommendation degree $Re_s(I)$ is given by

$$Re_s(I) = \frac{a_s(I)}{a_s(I)+d_s(I)}. \quad (7)$$

The reputation value of vehicle I using logistic regression can be calculated as

$$r_s(I) = \frac{1}{1+e^{-(\vec{X}\cdot\vec{A}+A_0)}}. \quad (8)$$

where,

$$\vec{X} = \{Ar_s(I), Re_s(I), f_s(I), r_{s-1}(I)\}. \quad (9)$$

$\vec{A}$ is the weighted vector and can be evaluated using the linear least square method and A_0 denotes the deviation value to provide adjustment for the initial reputation value $r_s(0)$. $r_{s-1}(I)$ is the reputation value calculated in the last time. If the newest calculated reputation value $r_s(I)$ is below the threshold φ, the vehicle will be declared as a malicious one and the flag will also be raised. This malicious vehicle mark can only be eliminated unless this vehicle has an honest performance continuously for a long time. And then, the flag will be lowered. At the time s, the reputation data in blockchain consists of $Ar_s(I)$, $f_s(I)$, $r_{s-1}(I)$ and the corresponding pseudonym (the public address $addr_I$) of the vehicle I. Therefore, the RSU can query the data of vehicle I easily.

***Step* 2 :** *calculation for the credibility of* msg*:* this step allows the RSU to confirm whether the event-related msg is true or not. The RSU receives the event-related messages from different initiators. In order to evaluate the correctness of the msg, a weighted voting method is utilized. The RSU creates two sets, namely set-1 and set-0, respectively. Set-1 indicates that the event reported by the msg has occurred and set-0 indicates that the event has not occurred. We assume that there are M initiators belonging to set-1 and N initiators belonging to set-0. And then the average reputation values of the two sets are respectively given by

$$R_1 = \sum_{i\in M} r_s(i)\ ;\ R_0 = \sum_{j\in N} r_s(j). \quad (10)$$

where $r_t(i)$ and $r_t(j)$ represent the reputation values of the ith and the jth initiator in set-1 and set-0, respectively. The weight w_i and w_j are calculated as follows:

$$w_i = \frac{r_s(i)}{R_1}\ ;\ w_j = \frac{r_s(j)}{R_0}. \quad (11)$$

Therefore, the weighted average of reputation values of the witnesses in set-1 and set-0 are respectively as follows:

$$Ravg_1 = \frac{w_i * r_s(i)}{M}\ ;\ Ravg_0 = \frac{w_j * r_s(j)}{N}. \quad (12)$$

The msg is considered to be trusted if the following condition is met

$$Ravg_1 - Ravg_0 > 0. \quad (13)$$

where $0 \le Ravg_{0\,or\,1} \le 1$. If the msg is trusted, the RSU will broadcast it with its signature to the vehicles in its communication range. Finally, the RSU tries to put the latest data about the initiators into the blockchain.

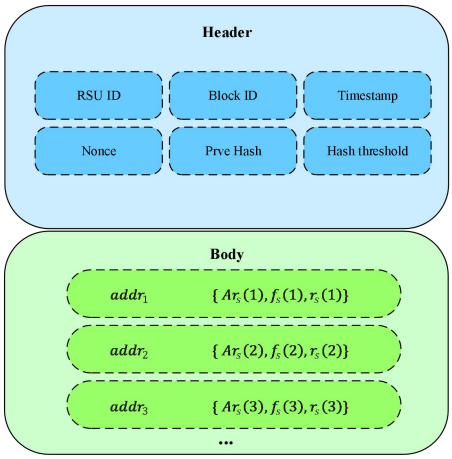


Fig. 3. The format of the block.

***Step* 3:** *miner election and block generation:* The RSU tries to add the new block into the blockchain. A miner should be elected from all the RSUs in order to generate new blocks. Each RSU calculates the hash value of its block based on a random nonce value δ, the previous timestamp, RSU ID and so on (denoted as $previous_{rep}$). So, the recommended miner election principle is:

$$Hash(\delta + previous_{rep}) < Difficult. \quad (14)$$

where $Difficulty$ is the hash value of the current block. Here, $Difficulty$ can be adjusted by the system to control the block generation speed. The RSU who calculates the nonce δ at the fastest and meanwhile satisfies the above condition will be elected as the miner and it can generate the new block. The format of the reputation data update block is shown in Fig. 3. It contains a block header and a block body. The header is composed of block ID, RSU ID, a timestamp of block generation, the hash of the previous block, the hash threshold and the nonce for proving the validity of this block. The body mainly contains the vehicles' reputation data.

***Step* 4:** *Distributed consensus algorithm:* The consensus process is carried out by authorized RSUs and a leader who is the RSU with the fastest-computing speed and valid proof-of-work. Here, the authorized RSUs act as the consensus nodes (denoted as ASUs). The leader broadcasts the block data (denoted as $Block_{new}$) with the timestamp, its signature (denoted as Sig_{leader}) and its proof-of-work to the ASUs for verification. After ASUs confirmed that the message from the leader is valid, these ASUs will broadcast their audit results with their signatures (denoted as Sig_{ASU}) with each other. The ASU collects the audit results from other nodes and compares its result with others. If the number of the matching audit results is more than $2f$ (f is the number of Byzantine nodes), it will send a confirmation message to all ASUs. If an ASU collects more than $2f+1$ confirmation messages, then the $Block_{new}$ can be stored into the blockchain. More details are shown in **Algorithm 1**. Moreover, if the consensus is not reached, the leader will analyze the audit results and launch another round of consensus if necessary.

Algorithm 1: Distributed Consensus Algorithm

1. The leader broadcasts block data to all ASUs for verification.

leader → *All*: Request = $(Block_{new}||Block\_hash||Sig_{leader}||timestamp,$ where $Block\_hash = Hash(Block_{new}||timestamp))$

2. The ASUs will broadcast their audit results with their signatures with each other.

$ASU_l \rightarrow ASU_j$: Audit = $(aduit\_result_l||Sig_{ASU_l})$

3. If an ASU receives more than $2f$ matching audited messages, it will send a confirmation message to all the ASUs

$ASU_l \rightarrow ASU_j$: Confirmation= $(confirmation_l||Sig_{ASU_l})$

4. If an ASU receives more than $2f$+1 confirmation messages, the block data will be stored into the blockchain.

***Step* 5:** *Vehicle tracing and revocation:* When a vehicle's reputation value is below the threshold φ and it still broadcast wrong messages, the vehicle will eventually be marked as a malicious one by TA. Due to the vehicle's address is retrieved from the blockchain, TA can find it easily according to the list recording the relations between the public address and the vehicle identity. These malicious vehicles will be added into the revocation list. Once revoked, the vehicle is unable to receive any service from the vehicular network.

C. Security Analysis

1) Conditional Privacy Preservation

BTCPS provides conditional privacy preservation due to the identity of the malicious vehicle can be revealed by TA. In BTCPS, each vehicle uses a public address as a pseudonym which can be retrieved from the blockchain. TA who owns the higher authority can find malicious vehicles easily according to the storage list which records the relations between public addresses and vehicles' identities.

2) Data Integrity

In BTCPS, the reputation data of vehicles recorded in the blockchain has already reached consensus by all the authorized RSUs. The sequence and the data of blocks are protected by the use of a hash chain. The hash value for each block is unique and the hash values of the other blocks would be changed once any content of any block was modified [36]. Thus, an adversary needs not only modify the contents of the current block but also recalculate the hash values of all blocks, if he/she would like to perform a message modification attack.

3) Defense Against Compromised RSU

If a compromised RSU wants to broadcast a forged block into the blockchain, at the consensus phase, each authorized RSU will check the validity of the block and prevent illegal blocks from being written to the blockchain. In addition, the attacker may have successfully captured several authorized RSUs. However, due to PBFT has an approximate 33% fault tolerance rate for failure or malicious nodes [21], even if an adversary successfully invaded several authorized RSUs, it cannot store the wrong block into the blockchain yet.

4) Prevention of Replay Attack

An adversary can replay a legitimate reputation data calculated before to implement the replay attack in VANETs, which will cause an interference on determining whether the msg is reliable or not. Each vehicle reputation data has a unique time parameter s, which is associated with the content of reputation data. Therefore, we can effectively prevent replay attacks by comparing parameter s and the corresponding content of reputation data.

D. Extremely Cases Discussion

In some extremely cases, such as at night or in remote areas, no enough vehicles serve as the replier to verify the message. We will reduce the value of threshold t so that the initiator can receive enough event-related messages from the repliers in time. In the worst case, we can accept the messages sent by the initiator for granted since only one initiator on the road witnessed the accident. However, if the message is proved to be false later, the initiator will encounter serious penalties, including but not limited to zero of its reputation value.

VI. Performance Analysis

We implement BTCPS in the Python and Golang environment using a desktop computer with 3.6 GHz Intel Core i7 and 16 GB 2400 MHz DDR4. In this section, we analyze the performance of BTCPS through extensive simulation experiments to validate its reliability and effectiveness.

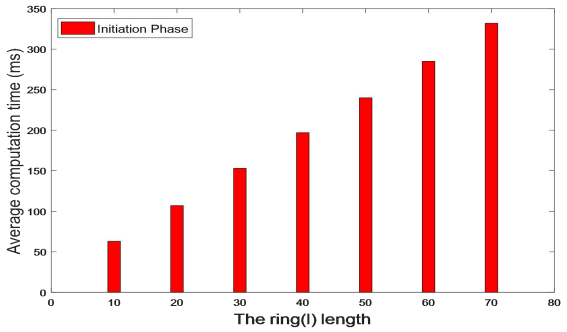


Fig. 4. The average computation time of initiation phase.

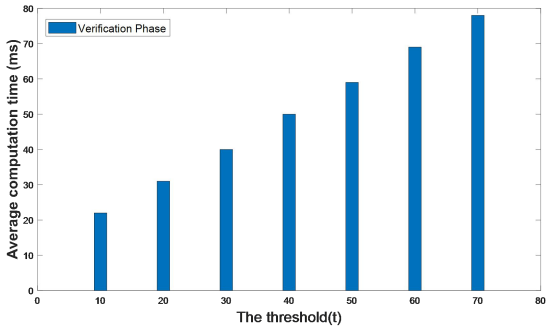


Fig. 5. The average computation time of different threshold values.

A. Evaluation of Announcement Protocol

In our anonymous aggregate vehicular announcement protocol, we achieve the evaluation results with the math library PBC [37].

Fig. 4 shows the average of 500 times calculation results of initiation phase proposed in Section IV, in which $l \in \{10, 20, 30, 40, 50, 60, 70\}$. In our scheme, the security increases with the length of the ring which occupies most of the computation time.

Therefore, the exhausting time of initiation phase is mainly related to the length of the ring. Specifically, the computation time is usually under 350ms up to the ring length of 70 in total, which can satisfy the safety requirements of our scheme.

The average computation time of different threshold values is depicted in Fig. 5. By the use of group signatures in verification phase, the time of verification has been greatly reduced. Especially, the cost of verification is mainly related to the size of the threshold value as confirming that the discriminant equation occupies most of the computation time, which is proportional to the threshold value.

According to the principles in [38] and [39], the computation time in our simulation experiments meets the practical requirements of VANETs while the privacy is preserved adequately in our scheme.

B. Validity of Trust Calculation Based on Logistic Regression

In order to verify the validity of the reputation calculation based on logistic regression, we assume that the scenarios including 100 vehicles in a 2 square kilo meter area. The impact of the initial distribution of vehicles in VANETs lies in the difference in the number of vehicles within the communication range of each RSU, which hardly has effect on the execution of our solution unless the number of vehicles under the jurisdiction of one RSU exceeds its communication load, and this extreme case may result in message delay. Without loss of generality, we assume the vehicles are evenly distributed in network area. Furthermore, the speed of these vehicles is between 20 to 24 meters per second, which is equivalent to a highway speed of 72 to 86 km per hour. Too fast speed would result in less reaction time for the vehicles and they would miss some accidents and participate in the verification of message with less probability than those vehicles with moderate speed. A road event, such as a serious traffic accident, can occur at random in this area while the vehicles are moving. Vehicles near the event will first observe it and start sending a message. And then, they will also work with other vehicles that are also witnesses to verify the message. The communication radius that the vehicle can cooperate with other witnesses is 250m, which is a reasonable assumption for the practical OBU equipment. Therefore, the distance between nearby vehicles should be kept within 250 meters when these vehicles pass through the scene of accident, they will start decelerating at a rate of 5m per second, which is a normal reaction to the incident on the road. However, a malicious vehicle may mislead other vehicles to keep a normal forward speed, even if it has started to slow down. We set 50% of malicious vehicles in our experiments. The initial reputation value of the vehicle is 0.3, and the reason for selecting this value can be explained below. As shown in Fig. 6, when the reputation value is set to as low as 0.1, it takes a long time to distinguish the malicious nodes from honest ones. And when the reputation value is large for example 0.8, it will spend more time to lower the reputation value of a malicious vehicle. This means it takes longer to identify a malicious vehicle. Through observations, both 0.3 and 0.5 are appropriate to differentiate honest vehicles from malicious vehicles and we choose 0.3 finally.

We compare the performance of our solution with the multi-weighted subject logic (MWSL) method [10] and the traditional subject logic (TSL) method [40]. First, we consider the impact of the probability p of a malicious vehicle sending a false message. We observe the change of the reputation value of one malicious vehicle within an hour when p=20%, p=50% and p=80%, respectively. As shown in Fig. 7, when p=80%, all of these methods can quickly reduce the reputation values of malicious vehicles. However, we observed that when p=20% and p =50%, MWSL and TSL lack sufficient evidence to identify malicious vehicles, which is why when p is small, the convergence rates of MWSL and TSL are sharply lower than that of logistic regression-based method.

And then, we compare the recognition rate of malicious vehicles with the increase of p. As shown in Fig. 8, when p is low, the logistic regression-based method has a better recognition rate for malicious vehicles because it makes decision by combining recommendation degree with direct trust. When p becomes larger and larger, the three methods have increasingly similar performance since incremental malicious activities can help MWSL and TSL identify the malicious vehicles. Therefore, the reliability of our proposed scheme can be validated, since malicious vehicles can be effectively identified even when the probability of sending malicious messages is low.

Furthermore, we also observe the false recognition rate in the case of a high percentage of malicious vehicles (60%, 70% and 80%, respectively). It is very difficult to distinguish honest vehicles from malicious ones in a dense network. Even so, as shown in Fig. 9, since the logistic regression-based method considers both direct trust and indirect trust, it keeps the false recognition rate below 0.08.

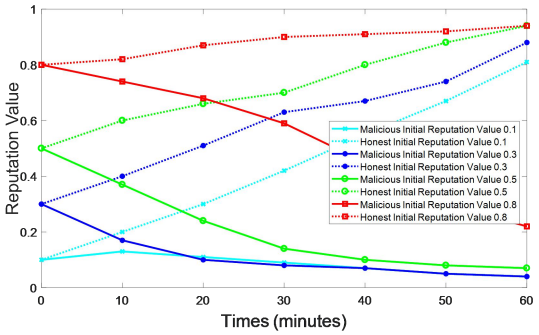
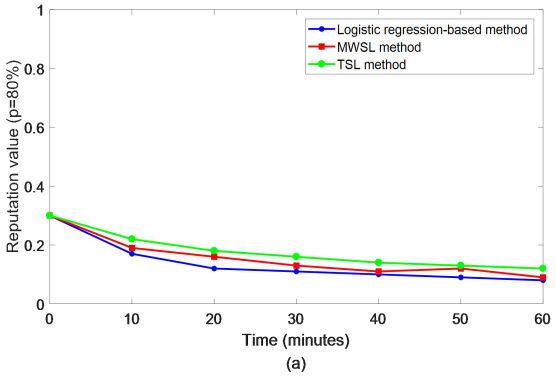


Fig. 6. Reputation value that evolves over time.



This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2019.2957421, IEEE Internet of Things Journal

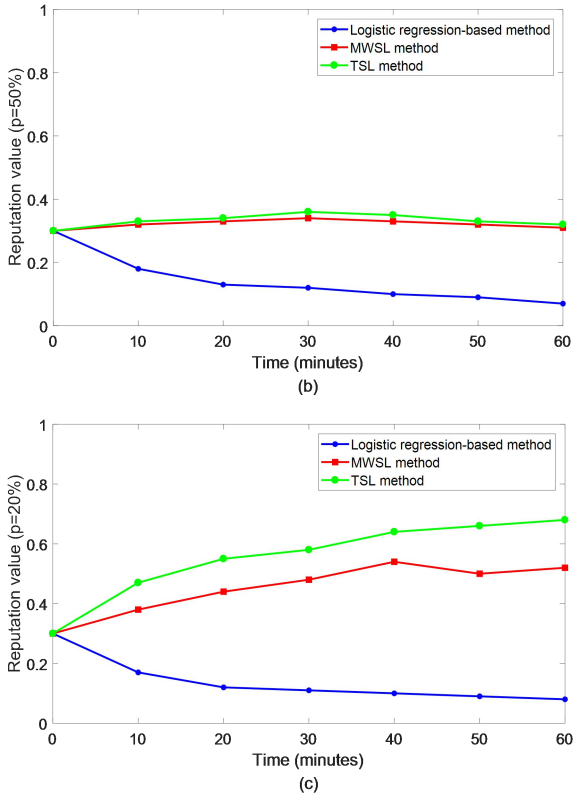


Fig. 7. The change of reputation value of one malicious vehicle over time. (a) The probability of sending a false message is 80%. (b) The probability of sending a false message is 50%. (c) The probability of sending a false message is 20%.

C. Average Latency of Proposed Consensus Algorithm

We compare the reaction time of each reputation value update message between our consensus algorithm, the traditional blockchain consensus algorithm PoW of Ethereum [41] and the joint proof-of-work and proof-of-stake consensus algorithm proposed in [42]. In [42], PoS method was adopted to facilitate the high stake RSUs to calculate nonce to improve the mining speed. In our experiments, the number of update messages requests are set to 1, 10, 100, 1000, 10000 and each experimental result is averaged in ten independent runs. The total number of the pre-selected ASUs is 50 in our blockchain. Fig. 10 shows that, both for the traditional blockchain consensus algorithm and the joint PoW and PoS consensus algorithm, the latency time is much longer than that of our consensus algorithm when the number of reputation data update messages increases. When the total number of messages reaches 10,000, the average latency of traditional blockchain consensus algorithm reaches 1311.11s, which is far more than the delay of our consensus algorithm. This is because our algorithm only carries out the consensus process on the pre-selected ASUs instead of all connected nodes. The results indicate that our proposed consensus algorithm has a more satisfactory efficiency.

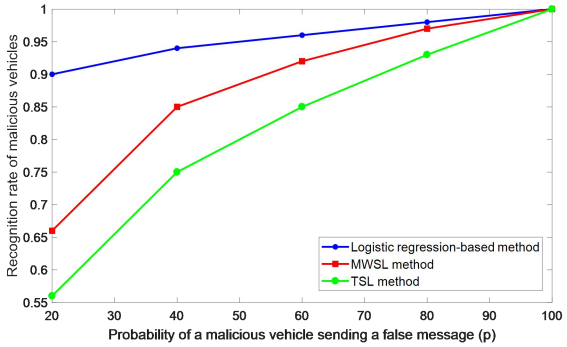


Fig. 8. The recognition rate of malicious vehicles with respect to *p*.

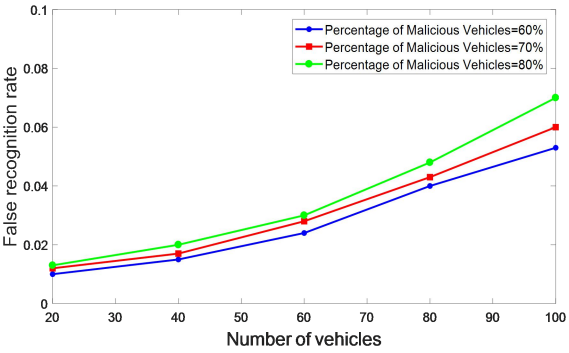


Fig. 9. The false recognition rate with different number of vehicles in the case of a high percentage of malicious vehicles.

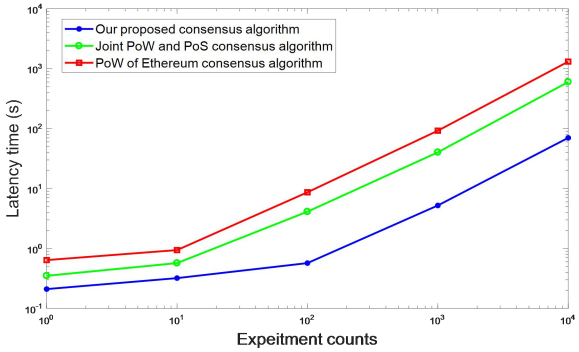


Fig. 10. Average Latency of Pow of Ethereum, joint PoW and PoS algorithm and our proposed consensus algorithm.

VII. Conclusion

In this paper, we have proposed a blockchain-based trust management scheme together with a conditional privacy-preserving announcement protocol (named as BTCPS) for secure vehicular communication in VANETs. By the use of group signatures in our proposed anonymous aggregate vehicular announcement protocol, the reliability of announcements can be maintained without revealing users' privacy in the non-fully-trusted environment. In addition, BTCPS also achieved conditional privacy since TA can trace anonymous malicious vehicles' identities with the public addresses in blockchain. Furthermore, a blockchain-based trust management model was employed to realize reputation message synchronization and prevent malicious vehicles from broadcasting forged messages. The trust calculation based on logistic regression can further facilitate the identification of

malicious vehicles. And meanwhile, a mixed consensus algorithm based on Proof-of-work and Practical Byzantine Fault Tolerates algorithm was put forward to achieve better efficiency compared with the traditional public blockchain consensus algorithms.

We have obtained the satisfactory experimental results. However, the sensitivity analysis and discussion regarding simulation parameters is not comprehensive and it will be the focus of our future work. Besides, we will plan to further enhance the privacy protection level of the proposed scheme in the completely untrusted VANETs environment.

APPENDIX

A. Notation Setting

Notation	Description
T	Trusted authority
I	Initiator
R	Replier
ITP	Initiation Packet
RPP	Response Packet
AGP	Aggregation Packet
G/q	An addition group/ the order of the group
H	Anti-collision hash function
E_k	A symmetric encryption algorithm with key k
k,sk,pk	Symmetric/ private/ public keys
$\vec{x},\vec{y}$	Master private/ public key vectors
msg	Message description of an event
$addr$	Pseudonym of a user
l	The length of the ring
t	Threshold of an announcement
Ar_s	Abnormal rate
λ	Threshold of abnormal rate
f_s	Value of flag
Re_s	Recommendation degree
r_s	Reputation value
φ	Reputation value threshold to declare malicious vehicles
$Ravg$	Weighted average of the reputation values
δ	Random nonce
f	Number of Byzantine nodes

REFERENCES

[1] K. Zheng, Q. Zheng, P. Chatzimisios, W. Xiang, and Y. Zhou, "Heterogeneous vehicular networking: A survey on architecture, challenges, and solutions," *IEEE Commun. Surveys Tuts.,* vol. 17, no. 4, pp. 2377–2396, 4th Quart., 2015.

[2] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET security challenges and possible cryptographic solutions," *Veh. Commun.,* vol. 1, no. 2, pp. 53–66, Apr. 2014.

[3] E. C. Eze, S.-J. Zhang, E.-J. Liu, and J. C. Eze, ''Advances in vehicular ad-hoc networks (VANETs): Challenges and road-map for future development,'' *Int. J. Auto. Comput.,* vol. 13, no. 1, pp. 1–18, 2016.

[4] Z. Lu, G. Qu, and Z. Liu, "A survey on recent advances in vehicular network security, trust, and privacy," *IEEE Trans. Intell. Transp. Syst.,* vol. 20, no. 2, pp. 760-776, 2018.

[5] X. Li, J. Liu, X. Li and W. Sun, "RGTE: A Reputation-Based Global Trust Establishment in VANETs," *Proc. 5th Int. Conf. IEEE Intell. Netw. Collaborative Syst. (INCoS)* Xi'an, 2013, pp. 210-214.

[6] Q. Li, A. Malip, K. M. Martin *et al.*, "A reputation-based announcement scheme for VANETs," *IEEE Trans. Veh. Technol.,* vol. 61, no. 9, pp. 4095-4108, 2012.

[7] N. Bißmeyer, J. Njeukam, J. Petit, and K. M. Bayarou, "Central misbehavior evaluation for VANETs based on mobility data plausibility," in *Proc. 9th ACM Int. Workshop Veh. Inter-Netw., Syst., Appl. ACM*, 2012, pp. 73–82.

[8] M. Raya, P. Papadimitratos, V. D. Gligor, and J.-P. Hubaux, "On data centric trust establishment in ephemeral ad hoc networks," in *Proc. IEEE INFOCOM,* Phoenix, AZ, USA, Apr. 2008, pp. 1–9.

[9] M. Monir, A. Abdel-Hamid, and M. A. El Aziz, "A categorized trust based message reporting scheme for VANETs," in *Advances in Security of Information and Communication Networks*. Berlin, Germany: Springer, 2013, pp. 65–83.

[10] X. Huang, R. Yu, J. Kang *et al.*, "Distributed reputation management for secure and efficient vehicular edge computing and networks," *IEEE Access,* vol. 5, pp. 25408-25420, 2017.

[11] J. Ni, A. Zhang, X. Lin *et al.*, "Security, privacy, and fairness in fog-based vehicular crowdsensing," *IEEE Commun. Mag.,* vol. 55, no. 6, pp. 146-152, 2017.

[12] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[13] P. K. Sharma, N. Kumar and J. H. Park, "Blockchain-Based Distributed Framework for Automotive Industry in a Smart City," in *IEEE Trans. Ind. Inform.* vol. 15, no. 7, pp. 4197-4205, July 2019.

[14] M. Shen, X. Tang, L. Zhu, X. Du and M. Guizani, "Privacy-Preserving Support Vector Machine Training Over Blockchain-Based Encrypted IoT Data in Smart Cities," in *IEEE Internet Things J.,* vol. 6, no. 5, pp. 7702-7712, Oct. 2019.

[15] Z. Li, J. Kang, R. Yu *et al.*, "Consortium blockchain for secure energy trading in industrial internet of things," *IEEE Trans. Ind. Inform.,* vol. 14, no. 8, pp. 3690-3700, 2017.

[16] J. Kang, R. Yu, X. Huang *et al.*, "Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains," *IEEE Trans. Ind. Inform.,* vol. 13, no. 6, pp. 3154-3164, 2017.

[17] J. Xiong *et al*., "Enhancing Privacy and Availability for Data Clustering in Intelligent Electrical Service of IoT," in *IEEE Internet Things J.,* vol. 6, no. 2, pp. 1530-1540, April 2019.

[18] P. K. Sharma, S. Rathore, Y.-S. Jeong *et al.*, "SoftEdgeNet: SDN Based Energy-Efficient Distributed Network Architecture for Edge Computing," *IEEE Commun. Mag.,* vol. 56, no. 12, pp. 104-111, 2018.

[19] M. Shen, J. Zhang, L.H. Zhu *et al.*, "Security SVM Training over Vertically-Partitioned Datasets using Consortium Blockchain for Vehicular Social Networks." *IEEE Trans. Veh. Technol.,* to appear, 2019.

[20] M. Shen, Y. Deng, L. Zhu, X. Du and N. Guizani, "Privacy-Preserving Image Retrieval for Medical IoT Systems: A Blockchain-Based Approach," in *IEEE Network*, vol. 33, no. 5, pp. 27-33, Sept.-Oct. 2019.

[21] M. Castro, and B. Liskov, "Practical Byzantine fault tolerance and proactive recovery," *ACM Trans. Comput. Syst.,* vol. 20, no. 4, pp. 398-461, 2002.

[22] L. Luu *et al.*, "A secure sharding protocol for open blockchains," *Proc. ACM SIGSAC Conf. Comput. Commun. Security,* 2016, pp. 17–30.

[23] T. Gazdar, A. Belghith, and H. Abutair, "An enhanced distributed trust computing protocol for VANETs," *IEEE Access,* vol. 6, pp. 380-392, 2017.

[24] W. Li and H. Song, "ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks," in *IEEE Trans. Intell. Transp. Syst.,* vol. 17, no. 4, pp. 960-969, April 2016.

[25] S. Guleng, C. Wu, X. Chen, X. Wang, T. Yoshinaga and Y. Ji, "Decentralized Trust Evaluation in Vehicular Internet of Things," in *IEEE Access,* vol. 7, pp. 15980-15988, 2019.

[26] A. Mahmood, B. Butler, W. E. Zhang, Q. Z. Sheng and S. A. Siddiqui, "A Hybrid Trust Management Heuristic for VANETs," in *Proc. IEEE Intl. Conf. PerCom Workshops*, Kyoto, Japan, 2019, pp. 748-752.

[27] H. Xia, S. Zhang, Y. Li, Z. Pan, X. Peng and X. Cheng, "An Attack-Resistant Trust Inference Model for Securing Routing in Vehicular Ad Hoc Networks," in *IEEE Trans. Veh. Technol.,* vol. 68, no. 7, pp. 7108-7120, July 2019.

[28] L. Chen, Q. Lit, K. M. Martin and S. Ng, "A privacy-aware reputation-based announcement scheme for VANETs," *Proc. IEEE WiVeC*, Dresden, 2013, pp. 1-5.

[29] L. Chen, Q. Li, K. M. Martin *et al.*, "Private reputation retrieval in public–a privacy-aware announcement scheme for VANETs," *IET Inf. Secur.,* vol. 11, no. 4, pp. 204-210, 2016.

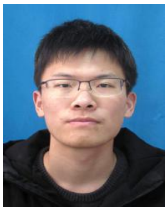
[30] N. Alexopoulos, J. Daubert, M. Mühlhäuser and S. M. Habib, "Beyond the Hype: On Using Blockchains in Trust Management for

Authentication," *2017 IEEE Trustcom/BigDataSE/ICESS*, Sydney, NSW, 2017, pp. 546-553.
[31] K. Bendiab, N. Kolokotronis, S. Shiaeles, and S. Boucherkha, "WiP: A novel blockchain-based trust model for cloud identity management, " in *Proc. IEEE 16th Intl. Conf. Dependable, Autonomic Secure Comput.,* Aug. 2018, pp. 724–729.
[32] S. Goka and H. Shigeno, "Distributed management system for trust and reward in mobile ad hoc networks," *Proc. 15th IEEE CCNC*, Las Vegas, NV, 2018, pp. 1-6.
[33] L. Zhang, Q. Wu, A. Solanas and J. Domingo-Ferrer, "A Scalable Robust Authentication Protocol for Secure Vehicular Communications," in *IEEE Trans. Veh. Technol.,* vol. 59, no. 4, pp. 1606-1617, May 2010.
[34] H. Xu, J. Ding, Y. Zhang and J. Hu, "Queue length estimation at isolated intersections based on intelligent vehicle infrastructure cooperation systems," *Proc. IEEE Intelligent Vehicles Symposium (IV)*, Los Angeles, CA, 2017, pp. 655-660.
[35] Y. Wang, Y.-C. Lu, I.-R. Chen, J.-H. Cho, A. Swami, and C.-T. Lu, "Logittrust: A logit regression-based trust model for mobile ad hoc networks," in *Proc. 6th ASE Int. Conf. Privacy, Security, Risk Trust*, 2014, pp. 1–10.
[36] J. Al-Jaroodi and N. Mohamed, "Blockchain in Industries: A Survey," in *IEEE Access*, vol. 7, pp. 36500-36515, 2019.
[37] PBC Library. Accessed: Jan. 10, 2018. [Online]. Available: http://crypto.stanford.edu/pbc/
[38] L. Li *et al*., "CreditCoin: A Privacy-Preserving Blockchain-Based Incentive Announcement Network for Communications of Smart Vehicles," in *IEEE Trans. Intell. Transp. Syst.,* vol. 19, no. 7, pp. 2204-2220, July 2018.
[39] M. Azees, P. Vijayakumar and L. J. Deboarh, "EAAP: Efficient Anonymous Authentication With Conditional Privacy-Preserving Scheme for Vehicular Ad Hoc Networks," in *IEEE Trans. Intell. Transp. Syst.,* vol. 18, no. 9, pp. 2467-2476, Sept. 2017.
[40] S. Zhong, J. Chen, and Y. R. Yang, "Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks," in *Proc. 22nd Annu. Joint Conf. IEEE Comput. Commun. Soc.*, 2003, pp. 1987–1997.
[41] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum project yellow paper,* vol. 151, no. 2014, pp. 1-32, 2014.
[42] Z. Yang, K. Yang, L. Lei, K. Zheng and V. C. M. Leung, "Blockchain-Based Decentralized Trust Management in Vehicular Networks," in *IEEE Internet Things J.,* vol. 6, no. 2, pp. 1495-1505, April 2019.

Xingchen Liu received his B.S. degree in computer science and technology from Nanjing University of Posts and Telecommunications in 2017. He is now a Ph. D candidate with the School of Computer Science, Software and Cyberspace Security, Nanjing University of Posts and Telecommunications. His research interests include information security and privacy protection of Internet of Things.

Haiping Huang (M'07) received the B.Eng. And M.Eng. degrees in computer science and technology from the Nanjing University of Posts and Telecommunications, Nanjing, China, in 2002 and 2005, respectively, and the Ph.D. degree in computer application technology from Soochow University, Suzhou, China, in 2009. From May 2013 to November 2013, he was a Visiting Scholar with the School of Electronics and Computer Science, University of Southampton, Southampton, U.K. He is currently a Professor with the School of Computer Science and Technology, Nanjing University of Posts and Telecommunications. His research interests include information security and privacy protection of Internet of Things.

Fu Xiao (M'12) received the Ph.D. degree in computer science and technology from the Nanjing University of Science and Technology, Nanjing, China, in 2007. He is currently a Professor and a Ph.D. supervisor with the School of Computer Science and Technology, Nanjing University of Posts and Telecommunications, Nanjing, China. His research interests include wireless sensor networks. Dr. Xiao is a member of the IEEE Computer Society and the Association for Computing Machinery.



Ziyang Ma received his B.S. degree in computer science and technology from Taihu University of Wuxi in 2017. He is now a postgraduate student with the School of Computer Science, Software and Cyberspace Security, Nanjing University of Posts and Telecommunications. His research interests include blockchain and smart transportation.