Securing Traffic-Related Messages Exchange Against Inside-and-Outside Collusive Attack in Vehicular Networks

Jingyu Feng, Nan Liu, Jie Cao, Yuqing Zhang, *Member, IEEE*, and Guangyue Lu

***Abstract*—Traffic-related messages exchange (TME) is considered as a powerful approach to improve traffic safety and efficiency in vehicular networks. However, TME assumes all vehicles always are honest, and thus offering opportunities for attackers to fake traffic-related messages. To combat such threat, recent efforts have been made to trust mechanism. In this article, a vulnerability for trust mechanism is found, that is, the ratings from initiator vehicles (IVs) are generally unchecked. Such ratings corresponding to the truth of traffic-related events can be exploited by attackers to disturb trust mechanism. Specially, attackers would form a clique to help with each other in an inside-and-outside collusive (IOC) manner. One of the IOC attackers can disguise as an IV who sends the rating in accordance with the traffic-related messages of his conspirators, result in promoting their trust value quickly. With high trust value, attackers can escape the detection of trust mechanism. We conduct an in-depth investigation on IOC attack and propose a defense scheme called TFAA from the design ideas of trust fluctuation association analysis. In addition, the trust data management of central and distributed trust mechanism may be unsuitable for vehicular networks. To support the trust data management for the TFAA scheme, we also design a semi-distributed trust data storage scheme called TruChain with the combination of consortium blockchain and vehicular regions partition. The simulation results show that the TFAA scheme can enhance the accuracy of trust value evaluation, and thus successfully reducing the power of IOC attack against TME.**

***Index Terms*—Collusive attack, traffic-related messages exchange (TME), trust mechanism, vehicular networks.**

I. Introduction

IT IS estimated that the number of registered vehicles will reach two billion within the next 10 to 20 years [1]. All infrastructures and smart vehicles constitute vehicular networks, which have been suggested as foundation of the intelligent transportation systems to improve transportation efficiency and road safety [2]. In vehicular networks, vehicles are equipped with on-board devices, namely sensors, resource command processor, storage, and communication devices, which are used for data gathering, processing, and sharing. With the help of on-board devices, vehicles can automatically detect traffic-related events and send warning messages to others. Such traffic-related messages exchange (TME) can help vehicles timely be aware of traffic situations, and hence improve the transportation safety and efficiency [3].

Vehicular networks has become an important scenario of Internet of Things (IoT) [4] and 5G mobile networks [5]. However, the unique characteristics of vehicular networks, such as high mobility and volatility make neighboring vehicles usually unrelated and unknown to each other. This offers opportunities for malicious vehicles to broadcast incredible messages on purpose. For example, a malicious vehicle may report a nonexisting collision to make the vehicles behind react by braking abruptly, which could possibly cause a chain collision among these vehicles [6]. These misbehaviors may not only decrease the transportation efficiency but may also cause accidents that can threaten human's life in the worst cases [7]. Fortunately, trust mechanism can enable vehicles to decide whether the received message is trustworthy or not, and also provides network operators the basis of rewards or punishments on specific vehicles [8]. Generally, the trust value of a vehicle can be calculated using ratings on his historical behaviors, which are generated by relevant vehicles.

To avoid the detection of trust mechanism, attackers would change their strategies. In TME, each vehicle actually plays two roles: 1) the role of initiator vehicle (IV) who utilizes traffic-related messages and 2) the role of cooperator vehicle (CV) who submits traffic-related messages. Currently, the ratings from IVs for the truth of traffic-related events after TME are unchecked. In this case, attackers can exploit ratings to disturb trust mechanism, in order to gain high trust value with the help of each other. In this article, we report the inside-and-outside collusive (IOC) attack along this line and propose a defense scheme called TFAA from the design idea of trust fluctuation association analysis to defend against this attack. The main contributions of this article are as follows.

1) Conduct an in-depth investigation on IOC attack. The basic idea of IOC is as follows. IOC attackers conspire with each other to form a collusive clique and help with each other by exploiting the ratings intentionally. Concretely, an IOC attacker is assigned to disguise as an IV (inside attacker) who upload the rating in accordance

Manuscript received April 26, 2019; revised June 21, 2019; accepted August 3, 2019. Date of publication August 7, 2019; date of current version December 11, 2019. This work was supported in part by the National Science Foundation of China under Grant 61701399, in part by the National Science Foundation of Shaanxi Province under Grant 2019JM-442, and in part by the Support Plan for Innovation Ability Project of Shaanxi Province under Grant 2017KCT-30-02. *(Corresponding author: Guangyue Lu.)*

J. Feng, N. Liu, J. Cao, and G. Lu are with the Shaanxi Key Laboratory of Information Communication Network and Security, Xi'an University of Posts and Telecommunications, Xi'an 710121, China (e-mail: tonylugy@163.com).

Y. Zhang is with the National Computer Network Intrusion Protection Center, University of Chinese Academy of Sciences, Beijing 100190, China.

Digital Object Identifier 10.1109/JIOT.2019.2933632

with the traffic-related messages of his conspirators (outside attackers) who play the role of CVs. In this case, his conspirators' trust value will be increased. After several rounds of attack, IOC attackers would become honest. With high trust value, IOC attackers can manipulate the aggregation result of TME more easily by incredible messages.

2) Design a blockchain-based semi-distributed trust data storage scheme called TruChain to manage trust data for the TFAA scheme in vehicular networks. To avoid the defeats of central and distributed trust mechanism, we find that the combination of consortium blockchain [9] and regions partition are suitable for vehicular networks. With the consortium blockchain technology, the region trusted authority (RTA) in a vehicular region can help vehicles to store blocks and maintain blockchain due to high computational power and sufficient storage capacity. When a new block is created, it will be broadcasted to all RTAs who chain the accepted block sequentially to the blockchain by its timestamp. So, our TruChain scheme can facilitate a vehicle to know the trust data of CVs rapidly, even though they have just moved from another region to the current region. In addition, the roadside units (RSUs) can forward trust data from an RTA to vehicles and perform some operations for vehicles, such as trust value search and trust value update in trust mechanism. With the help of RTAs and RSUs, blockchain cannot add overload to vehicles who can make a rapid decision for a certain traffic-related event through blockchain.

3) Analyze the trust fluctuation and association feature of IOC attackers to propose the TFAA scheme. Such feature can not only inspire us to find the trust fluctuation association rule to detect IOC attackers but also speed up the detection by conducting TFAA as a recursive elimination scheme to reduce suspicious CVs. Since IOC attackers are engaged in reporting credible messages or credible messages, they may behave the feature of trust fluctuation. We can compute and use the trust fluctuation index as the first recursive elimination level to delete unlikely IOC attackers in CVs. Meanwhile, IOC attackers cooperate with each other in the IOC manner, so they often appear together. We can continue to the second recursive elimination level to delete unlikely IOC attackers through the association relationship analysis. By narrowing the scope of suspicious CVs, we can reduce the search volume of the database stored historical traffic-related messages and ratings, and thus ensuring the TFAA scheme to detect IOC attack fast.

The organization of this article is as follows. In Section II, preliminaries related on TME, trust mechanism and blockchain-based trust data management are described. We analyze IOC attack in Section III. To support the construction of TFAA, we design a semi-distributed data storage scheme based on blockchain in Section IV. The TFAA scheme is proposed in Section V to detect IOC attack. Simulation analysis of the TFAA scheme is given in Section VI. Finally, we conclude this article in Section VII. In addition, the abbreviations and key variables used in this article are listed in Tables I and II, respectively.

TABLE I
ABBREVIATIONS USED IN THIS ARTICLE

Abbreviations	Explanation
TME	Traffic-related messages exchange
IOC	Inside-and-outside collusive
TFAA	Trust fluctuation association analysis
IV	Initiator vehicle
CV	Cooperator vehicle
RTA	Region trusted authority
RSU	Roadside unit
V2V	Vehicle-to-vehicle
V2I	Vehicles-to-infrastructure
TMAM	Traffic-related message aggregation model
TruChain	Blockchain-based semi-distributed trust data storage scheme

TABLE II
KEY VARIABLES USED IN THIS ARTICLE

Variables	Explanation
V_i	The i-th vehicle
RTA_k	The k-th RTA
msg_i	The message reported by V_i
cre_i	The number of credible messages for V_i
inc_i	The number of incredible messages for V_i
T_i	The trust value of V_i
Υ	The pre-selected set of miners
Θ_i	The set of trust value of V_i's CVs
Ξ_i	The set of (cre, inc) parameters of V_i's CVs
rat_i	The rating sent by V_i
Ω_i	The trust data set of V_i's CVs
Ψ_i	The set of signatures added by V_i to the trust data in Ω_i
μ_i	The the trust fluctuation index of V_i
minsup	The minimum of support count

II. PRELIMINARIES

A. Traffic-Related Messages Exchange

In order to share the critical traffic-related messages, vehicular networks are established with two types of communication, namely, vehicle-to-vehicle (V2V) and vehicles-to-infrastructure (V2I) communication [10]. In V2V communication, vehicles communicate with nearby vehicles to exchange messages. In V2I communication, vehicles communicate directly with RSUs. Dedicated short range communication radio [11] and a couple of IEEE standards can be used for V2V and V2I communications in vehicular networks.

As shown in Fig. 1, vehicular networks consist of three major components: 1) vehicles; 2) RSUs; and 3) trusted authority (TA) [12]. Each vehicle is equipped with on-board devices to exchange traffic-related messages with their neighbors, e.g., road conditions, traffic congestions, etc. RSUs are generally stationary devices deployed along the road or at dedicated locations such as at intersections or parking lots [13]. TA is responsible for the trust and security management of the entire vehicular networks including verifying the authenticity of vehicles and revoking nodes in the case of vehicles broadcasting incredible messages or performing malicious behaviors [14].

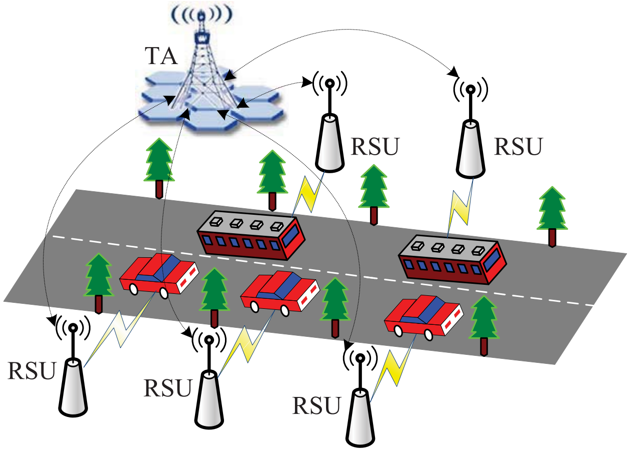


Fig. 1. System model of vehicular networks.

When an IV wants to know the surrounding traffic conditions in advance, the TME action is triggered with three procedures.

1) *Messages Reporting:* Vehicles that are aware of road accidents can report the warnings to other vehicles in the vicinity so that they can take actions in advance and avoid the danger [15].
2) *Messages Aggregation:* Specific models are used for traffic-related messages aggregation to make a quick decision, e.g., the majority rule [4]. The traffic-related message aggregation model (TMAM) can be managed by TA in central vehicular networks or RSUs in distributed vehicular networks.
3) *IV Feedback:* Based on the validation result, the vehicle will generate a rating for each message from the source vehicle [4]. That is, the IV can generate the rating for all traffic-related messages based on the truth of the traffic-related event and upload his rating to update the trust value of relevant CVs.

B. Trust Mechanism

Trust mechanism is increasing influence on many application scenarios, including e-commerce [16], P2P file-sharing [17], cooperative spectrum sensing [18], online social communities [19], etc.

Trust mechanism also plays significant roles in vehicular networks, such as: 1) assist TMAM' rapid decision-making reliably; 2) filter out incredible messages reported by attackers; and 3) prevent attackers from participating into TME. Current trust mechanism systems are mainly classified into two groups, i.e., central and distributed.

In central trust mechanism systems, all trust data are stored and processed in a central authority, which is also utilized to evaluate the trust value of all vehicles. Representative central trust mechanism systems are as follows. In [20], vehicles sense the traffic-related events and publish announcements to neighbors. The receivers need to evaluate the credibilities of messages and generate ratings. All ratings are collected by a central server. Based on these data, the server is able to update the trust value and issue certificates for all vehicles in the network. In [21], a reputation-based global trust establishment scheme is proposed to share the trust information in vehicular networks based on statistical laws. In [22], vehicles periodically come in contact with their certification and traffic control authorities to update their reputation level (trust value), which are determined by the validation of their behavior on the network. However, it is not practical to cope with the requests from large numbers of vehicles using a central authority in a smart city. Too many requests may probably bring about high latency for vehicles. Moreover, the single point of failure is still a big challenge for central vehicular networks.

In distributed trust mechanism systems, trust evaluation and trust data storage tasks are conducted in vehicles themselves or RSUs. Representative distributed trust mechanism systems are as follows. In [23], a decentralized reputation system to analyze the trust of vehicles in order to identify the presence of malicious vehicles and dismiss their warnings. In [24], a comprehensive vehicular network reputation model that aids vehicles in a road network to evaluate the trustworthiness of their peers. To achieve trust among vehicles, each receiving vehicle requests other vehicles within his communication range to give their opinion about the trustworthiness of the sending vehicle. Alternatively, the receiving vehicle gets opinion about the sending vehicle from RSUs. In [25], RSUs are employed for trust mechanism, in which vehicles generate ratings for others and upload these ratings into the nearby RSUs. Vehicles can also send requests to RSUs to query the trust value of neighboring vehicles. However, distributed trust mechanism systems need vehicles and RSUs to store trust data by themselves, which may be incomplete and inconsistent from a global standpoint. It may lead to the incorrect evaluation of trust value for some vehicles. In addition, vehicles cannot store trust data locally in the long term, due to the fast changing traffic environments and limited capacity of on-board devices.

In trust mechanism systems, one of the most popular design is based on beta function. It first counts the number of credible and incredible behaviors a vehicle has conducted, and then evaluates trust value with beta function $\mathrm{Beta}(\alpha, \beta)$ [26]

$$\mathrm{Beta}(\alpha, \beta) = \frac{\Gamma(\alpha + \beta)}{\Gamma(\alpha)\Gamma(\beta)}\theta^{\alpha-1}(1-\theta)^{\beta-1} \tag{1}$$

where θ is the probability of TME behaviors, $0 \leq \theta \leq 1$, $\alpha > 0, \beta > 0$.

A basic trust mechanism system called Baseline can be described to evaluate trust value. When a message (msg_i) is reported by the ith vehicle (V_i), if msg_i is the same as the truth of the traffic-related event rated by the IC, msg_i is considered as a credible message. Otherwise, it is considered as an incredible message. For V_i, the baseline system evaluates the number of credible messages reported by this vehicle, denoted by cre_i, and the number of incredible messages reported by this vehicle, denoted by inc_i. The trust value of V_i can be evaluated with beta function as: $T_i = \mathrm{Beta}(cre_i + 1, inc_i + 1)$. Without any prior observations, $cre_i = inc_i = 0$ and hence, $T_i = \mathrm{Beta}(1, 1)$.

Consider the condition $\Gamma(x) = (x-1)!$ when x is an integer [27]. It can be found that the expectation value of the beta function is given by: $E[\text{Beta}(\alpha, \beta)] = \alpha/(\alpha + \beta)$. Therefore, T_i can be further described as follows:

$$T_i = \frac{1 + cre_i}{2 + cre_i + inc_i} \tag{2}$$

where T_i is a true number ranging from 0 (complete distrust) to 1 (complete trust). For $cre_i = inc_i = 0$, V_i is recognized as a newcomer and T_i is initialized as 0.5. Afterward, the more V_i often reports credible messages, the higher trust value he will get, and vice verse.

C. Blockchain-Based Trust Data Management

To avoid the defeats of central and distributed trust mechanism systems, it is critical to develop a reliable and consistent trust data management method in vehicular networks.

Recently, blockchain, emerged in 2008 for the underlying technology of the Bitcoin protocol [28], is recognized as a new technology to manage trust data for trust mechanism systems. Blockchain is a distributed public ledger encrypted by Merkel trees and hash functions, in which All the broadcasted traffic-related messages and activities of vehicles can be written into the immutable and unforgeable ledger. These significant features of blockchain make it potential for managing trust data in vehicular networks [29].

Representative trust mechanism systems based on blockchain are as follows. In [2], a privacy-preserving [30] trust model named blockchain-based anonymous reputation system to prevent distribution of forged messages while simultaneously preserving the identity privacy of vehicles. In [4], a distributed trust management system based on blockchain is proposed for vehicular networks, which not only enables all RSUs to participate in updating the trust value with a joint proof-of-work and proof-of-Stake consensus mechanism but also provides all RSUs the trust data of all the vehicles in the network. In [31], vehicles rate the received messages based on observations of traffic environments and pack these ratings into a block. Each block is chained to the previous one by storing the hash value of the previous block. Then, a temporary center node is elected from vehicles and it is responsible for broadcasting its rating block to others. Based on ratings stored in the blockchain, vehicles are able to evaluate the trust value of the message senders and then evaluate the credibility of their messages.

The common feature of current trust mechanism systems is that they mainly manage trust data via public blockchain. Thus, the miners selection in the consensus mechanism will waste a lot of time for vehicles or RSUs. With the rapid development of intelligent transportation systems, if all blocks of the whole blockchain are stored in vehicles or RSUs, too many blocks will probably increase the burden on them due to their limited computation and storage capabilities. Moreover, it is necessary to collect the trust data from blockchain fast when finding the trust value for CVs, since a quick decision must be made in TME.

To summarize, there are generally three categories of blockchain-like database applications [32].

1) *Public Blockchain:* A public blockchain is the blockchain that anyone in the world can read, anyone in the world can send transactions to and expect to see them included if they are valid, and anyone in the world can participate in the consensus process—the process for determining what blocks get added to the chain and what the current state is.
2) *Consortium Blockchain:* A consortium blockchain is the blockchain where the consensus process is controlled by a preselected set of miners.
3) *Private Blockchain:* A private blockchain is the blockchain where write permissions are kept central to one organization.

Obviously, the traditional design methods of public blockchain cannot be applied in vehicular networks directly, some novel design ideas combining the characteristics of vehicular networks should be taken into account. With the public blockchain, the selection of miners would cause high energy and computing resources consumption in vehicular networks. With the private blockchain, the single point of failure is a big challenge for the central server. In this article, we find that consortium blockchain is well suitable for vehicular networks since RTAs can be employed as the preselected set of miners.

III. IOC Attack Overview

When trust mechanism system is employed in vehicular networks, the incredible messages threat can be easily suppressed if attackers always report incredible messages. This is because they will obtain a lower trust value when they always report incredible messages. To avoid the detection of trust mechanism, attackers will change their strategies.

Due to the unchecked ratings, a new attack chance may be offered to attackers. We find that IOC attack is applicable under four key factors: 1) each vehicle plays the role of IV and the role of CV in TME, respectively; 2) the ratings are used to identify whether the messages of CVs are credible; 3) no measures have been adopted to check the authenticity of the ratings from IVs since it is difficult to get direct evidence information to design authentication methods; and 4) IOC attackers can form a collusive clique to help with each other, and thus increasing their rate of attack success.

IOC attack can be launched from two aspects of threat: 1) inside and 2) outside. In the aspect of inside threat, one of IOC attackers can play the role of IV (called IOC initiator) who requests the messages for a certain traffic-related event and uploads the rating to help his conspirators with the role of CVs. In the aspect of outside threat, IOC attackers can play the role of CVs (called IOC cooperator) who report messages to prompt their trust value.

IOC attackers are extremely sensitive to their trust value. They begin to launch IOC attack under the constraint

$$T_i \leq \varepsilon + \eta_1.$$

The strategy of IOC attack is shown in Fig. 2. Assuming V_i is one of IOC attackers, T_i is the trust value of V_i. As each $T_i \in [0, 1]$, the threshold of trust value (ε) is usually set to a moderate value, such as 0.5, which is calculated in (1) when $cre = inc$. $T_i > \varepsilon$ means is a high trust value which means

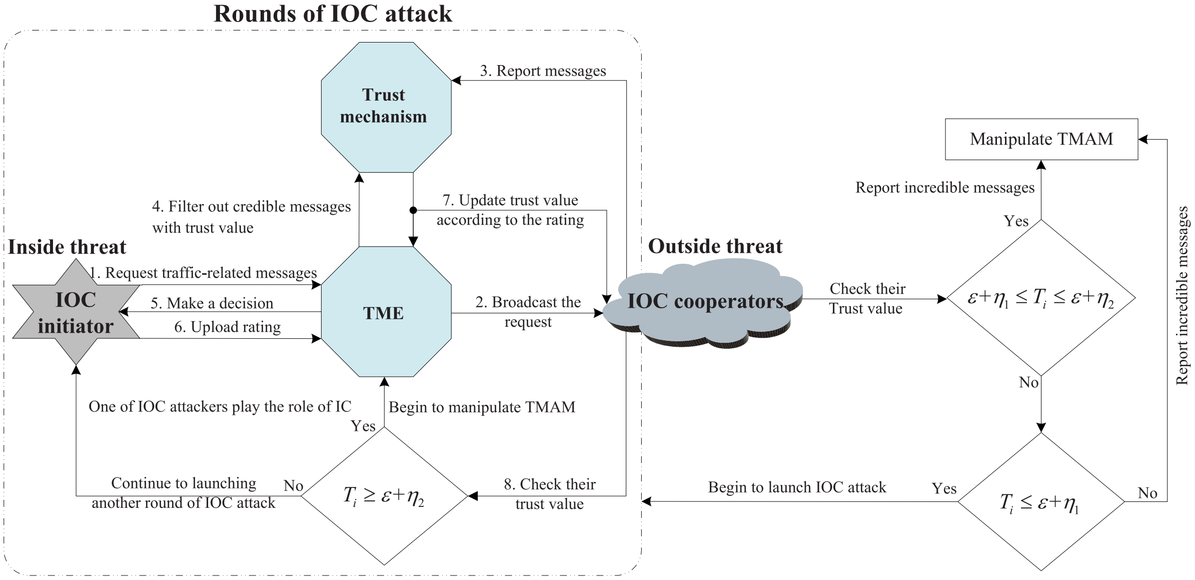

Rounds of IOC attack
Trust mechanism
3. Report messages
4. Filter out credible messages with trust value
7. Update trust value according to the rating
Inside threat
1. Request traffic-related messages
IOC initiator
5. Make a decision
6. Upload rating
TME
2. Broadcast the request
Outside threat
IOC cooperators
Check their Trust value
$\varepsilon+\eta_1 \le T_i \le \varepsilon+\eta_2$
Report incredible messages
Yes
Manipulate TMAM
No
Report incredible messages
One of IOC attackers play the role of IC
Yes
Begin to manipulate TMAM
Continue to launching another round of IOC attack
No
$T_i \ge \varepsilon+\eta_2$
8. Check their trust value
Begin to launch IOC attack
Yes
$T_i \le \varepsilon+\eta_1$
No

Fig. 2. Strategy of IOC attack.

that a vehicle's message can be accepted by TMAM. This inspires IOC attackers to find an attack procedure to prompt their trust value. When $T_i \leq \varepsilon + \eta_1$, V_i would stop to faking traffic-related messages and ask an IOC attack help to prompt trust value from his conspirators. At the moment, the inside threat is launched. One of his conspirators nearby V_i (such as V_p) becomes the IOC initiator who broadcasts the request for a certain traffic-related event. In the next moment, the outside threat is launched. V_i plays the role of a CV. Meanwhile, the other IOC cooperators nearby V_i can hitch-hike. After the TME action, the trust value of IOC cooperators including V_i will be prompted since their messages are the same with the rating of V_p. Here, η_1 $(0 \leq \eta_1 < \varepsilon)$ is the trust warning line. It is too late to prompt trust value when $T_i < \varepsilon$. In this case, such IOC attacker has been marked as suspicious and TMAM will not trust him. This attack pattern continues until $T_i \geq \varepsilon + \eta_2$. $\eta_2(\eta_1 < \eta_2 \leq \varepsilon)$ is the high trust line.

IV. Blockchain-Based Semi-Distributed Trust Data Storage

Due to the features of decentralization, consistence, and tamper-proofing, blockchain is actually a promising technique to support data storage for trust mechanism in vehicular networks. To avoid the defects of central and distributed manner, a semi-distributed data storage scheme based on blockchain called TruChain is designed to offer the data storage service for the construction of TFAA in vehicular networks.

Comparing with central and distributed networks, semi-distributed is the network structure that regions partition can be adopted in vehicular networks, which can help vehicles make a rapid decision and maintain blockchain effectively. In reality, the behaviors of a specific vehicle can hardly affect vehicles far away from it, since each vehicle can only observe the traffic conditions around it for a short distance. In this case, the semi-distributed structure with regions partition is very essential to vehicular networks. Each region can own a TA.

As shown in Fig. 3, a region in vehicular networks mainly includes an RTA, several vehicles on the road and RSUs on the roadside.

1) *RTA:* With high computational power and sufficient storage capacity, RTA is responsible for storing trust data in blocks. To avoid wasting time in the miners selection, all RTAs in the network can be employed as a preselected set of miners (Φ), and thus maintaining a consortium blockchain for trust mechanism in vehicular networks. Specially, the base station of each cellular network can play the role of RTA in 5G environments.

In a region, RTA is also responsible for a round of block creation, which is consisted of block proposal, block validation, and block accept.

1) *Block Proposal:* Only the RTA in a region has the right to propose a block to store the reputation-related data about a traffic-related event queried by a vehicle.
2) *Block Validation:* This RTA sends the proposed block to the RTA leader who verifies the validity of the block. Without loss of generality, the RTA leader rotates among the members in Φ over a period of time. Assuming $\Upsilon = \{\mathrm{RTA}_1, \mathrm{RTA}_2, \ldots, \mathrm{RTA}_k, \ldots, \mathrm{RTA}_l\}$, in which l is the number of members in Υ. When RTA_k approaches the end of his RTA leader tenure, $\mathrm{RTA}_{k+1}(k+1 \leq l)$ will take charge of the new RTA leader. At the end of RTA_l's tenure, RTA_1 will become the new RTA leader again.
3) *Block Accept:* If the proposed block is valid, the RTA leader will accept this block and broadcast it to all RTAs who chain the accepted block sequentially to the blockchain by its timestamp.

As shown in Fig. 4, the block structure of the TruChain scheme contains two parts, namely, block head and block body.

In the block header, our TruChain scheme is different from the traditional blockchain in vehicular networks. Except for

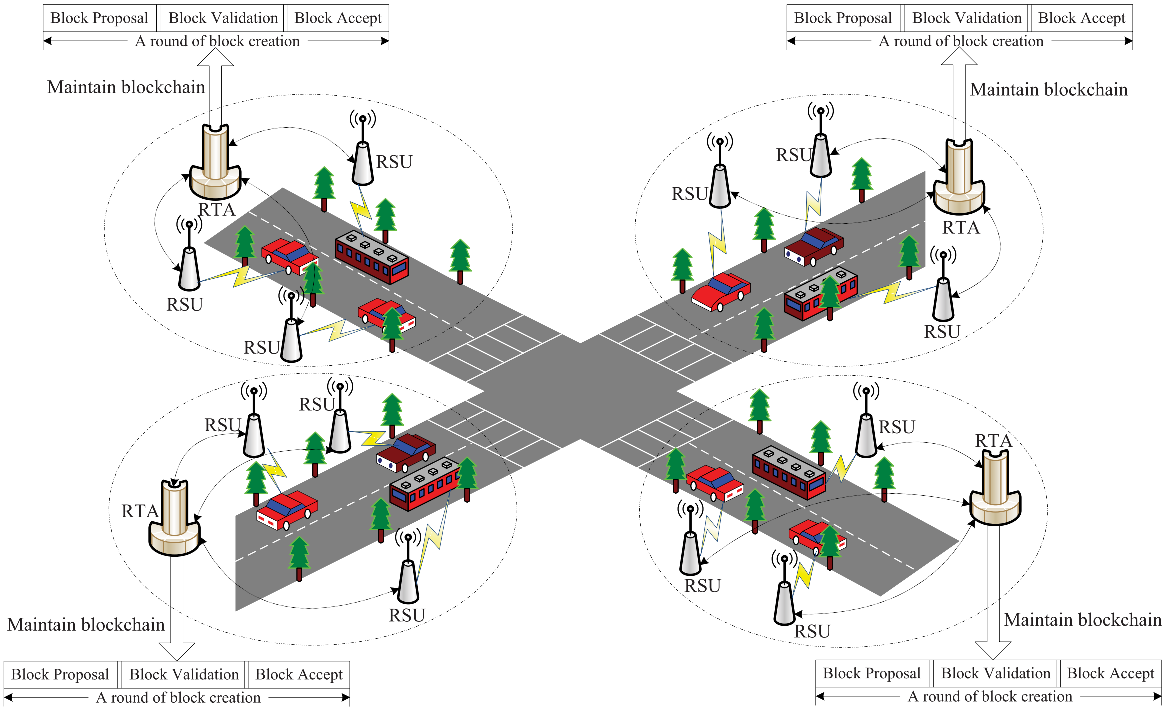


Fig. 3. Architectural view of the TruChain scheme with regions partition.

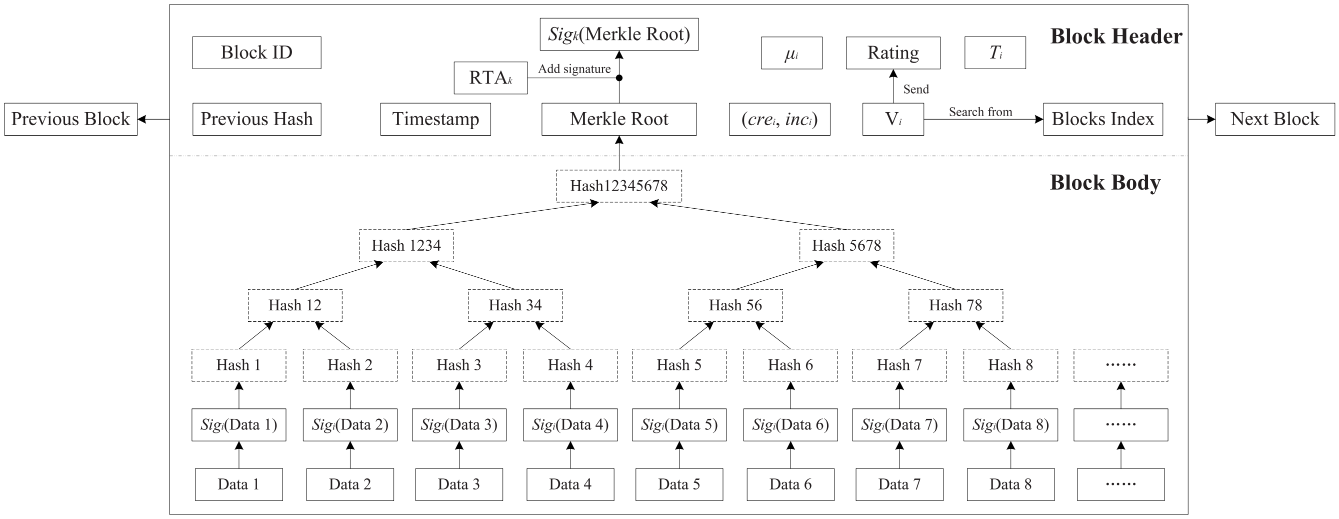


Fig. 4. Block structure of the TruChain scheme.

previous hash, timestamp, Merkle root, and block ID, several new elements are introduced in the block header.

1) *RTA_k:* The ID of RTA who proposes the block. For example, if RTA_k proposes the block, its ID should be recorded in the block header.
2) *Sig_k(Merkle Root):* The signature of Merkle root added by RTA_k. With this signature, the RTA leader can verify the validity of the proposed block rapidly.
3) *V_i:* The ID of a vehicle who queries the traffic-related event from neighboring vehicles (CVs). For example, if V_i queries about CVs, his ID should be recorded in the block header.
4) *T_i:* The trust value of V_i. To assist other vehicles in finding the trust value of V_i quickly in the future, T_i is also recorded in the block header by searching from blockchain.
5) *μ_i:* The trust fluctuation index of V_i, which is used to analyze the trust fluctuation feature of IOC attackers in the TFAA scheme.
6) *(cre_i, inc_i):* The number of credible and incredible messages reported by V_i. The two parameters are useful to update T_i.
7) *Rating:* The rating about the truth of the traffic-related event, which is sent by V_i.

8) *Blocks Index:* The ID index of blocks related to V_i. With the rapid development of trust mechanism in vehicular networks, there may be a lot of blocks related to V_i on the blockchain. If the blocks index is added to the header when creating a new block for V_i, the history trust data of V_i and his history CVs can be found quickly when other vehicles need them urgently.

In the block body, the signatures of V_i adding to the trust data of his CVs are used to build the Merkle tree, instead of hashing these trust data directly.

1) *Data:* The trust data of V_i's CVs. For a CV such as $V_5, Data5 = \{V_5, \text{msg}_5, cre_5, inc_5, T_5\}$.

2) *Block Validation:* The signature of trust data added by V_i. With this signature, RTA$_k$ can verify whether or not the trust data of V_i's CVs are tampered during the transmission from V_i to RTA$_k$.

2) *Vehicle:* To make a rapid decision, each vehicle is responsible for the major tasks, i.e., traffic-related messages collection and traffic-related messages aggregation.

1) *Traffic-Related Messages Collection:* When a vehicle wants to know the traffic-related event around it at one point, the vehicle can query about CVs and then receive some traffic-related messages from them.

2) *Traffic-Related Messages Aggregation:* With the trust value of CVs, the vehicle can filter out the incredible messages reported by attackers. Then, the vehicle can make a rapid decision with TMAM.

3) *RSU:* To help vehicles make a rapid decision, the RSU nearby a vehicle is responsible for the major tasks, i.e., trust value search and trust value update.

1) *Trust Value Search:* Once a vehicle requests the trust value of CVs, the RSU nearby a vehicle can search the trust data of CVs from the RTA.

2) *Trust Value Update:* The RSU updates the trust value of CVs based on the rating sent by the vehicle and submits the updated trust value to the RTA.

As shown in Fig. 5, the TruChain scheme can be executed with five steps.

Step 1: After receiving the traffic-related messages from CVs, a vehicle V_i sends a Query message $Q[i] = (V_i, \Gamma_i, tru_i, st_i)$ to the adjacent RSU. Γ_i is the ID set of V_i's CVs. tru_i indicates that V_i wants to find the trust value of his CVs. st_i is the sending timestamp of $Q[i]$. The adjacent RSU forwards $Q[i]$ to RTA$_k$ in charge of the current region.

Step 2: RTA$_k$ responds a QueryHit message $QH[k] = (\text{RTA}_k, \Theta_i, \Xi_i, st_k)$ to the adjacent RSU by searching blockchain. Θ_i is the set of trust value of V_i's CVs. Ξ_i is the set of (cre, inc) parameters of V_i's CVs. st_k is the sending timestamp of $QH[k]$. The adjacent RSU forwards Θ_i to V_i.

Step 3: V_i sends the rating (rat_i) about the truth of the traffic-related event to the adjacent RSU who updates Θ_i and Ξ_i based on the comparison between the truth of the traffic-related event and the reported messages. To avoid inconsistencies, the reported messages about the traffic-related event can be obtained by the adjacent RSU from V_i and CVs synchronously. Afterward, the adjacent RSU returns the updated Θ_i and Ξ_i to V_i waiting for confirmation.

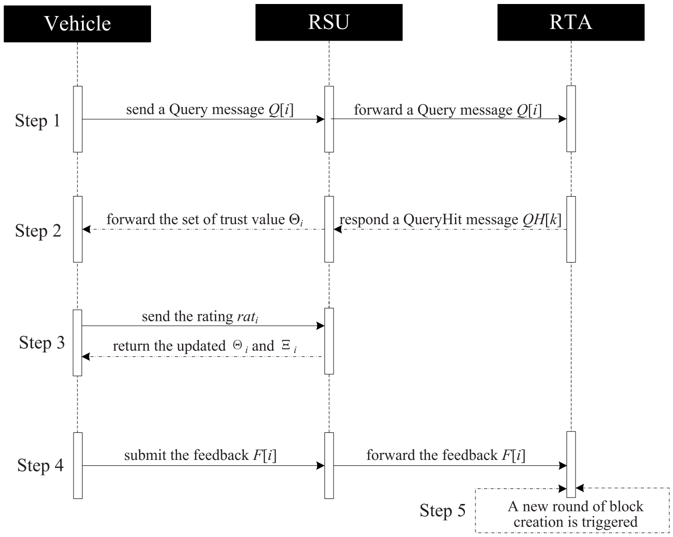

Vehicle
RSU
RTA
Step 1
send a Query message $Q[i]$
forward a Query message $Q[i]$
Step 2
forward the set of trust value Θ_i
respond a QueryHit message $QH[k]$
Step 3
send the rating rat_i
return the updated Θ_i and Ξ_i
Step 4
submit the feedback $F[i]$
forward the feedback $F[i]$
Step 5
A new round of block creation is triggered

Fig. 5. Execution strategies of the TruChain scheme.

Step 4: After the confirmation, V_i submits the feedback $F[i] = (V_i, rat_i, \Omega_i, \Psi_i, st_i')$ to the adjacent RSU who forwards $F[i]$ to RTA$_k$. Ω_i is the trust data set of V_i's CVs and Ψ_i is the set of signatures added by V_i to these trust data. For example, if there are six CVs for $V_i, \Omega_i = \{Data1, Data2, Data3, Data4, Data5, Data6\}$ and $\Psi_i = \{Sig_i(Data1), Sig_i(Data2), Sig_i(Data3), Sig_i(Data4), Sig_i(Data5), Sig_i(Data6)\}$.

Step 5: A new round of block creation is triggered. RTA$_k$ proposes a new block based on $F[i]$ and sends the proposed block to the RTA leader who will verifies the validity of the block. If the proposed block is valid, the RTA leader will broadcast it to all RTAs.

V. Proposed Defense Scheme

Supported by the trust data of TruChain, we develop a defense scheme called TFAA from the design idea of trust fluctuation association analysis to detect IOC attack in TME.

A. Design Idea

We have known that trust mechanism is employed to identify attackers. By discarding their false traffic-related messages in the messages aggregation process, TMAM can make a reliable and rapid decision. However, no guard measures have been adopted to the IV feedback process, result in a vulnerability for trust mechanism. This vulnerability can be utilized by IOC attackers to get high trust value in the IOC manner. Then, IOC attackers can fake traffic-related messages to manipulate the decision of TMAM in the messages aggregation process.

To repair this vulnerability, we find that IOC attackers have the trust fluctuation feature due to the alternative behaviors in reporting credible messages or credible messages, and the association behaviors in reporting messages together. In this

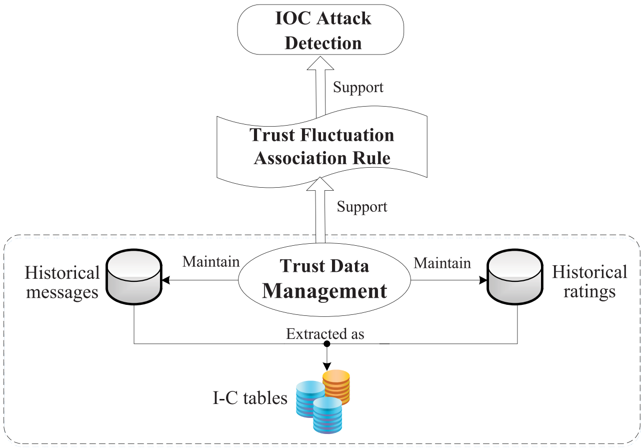


Fig. 6. Architectural view of the TFAA scheme.

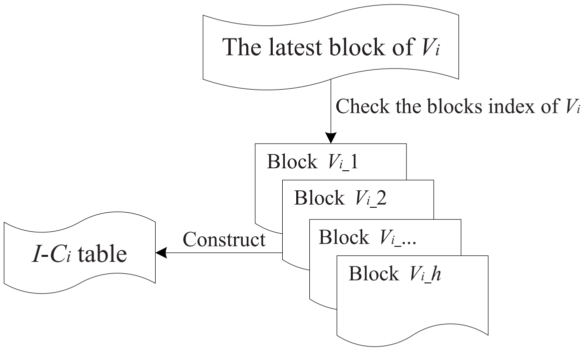


Fig. 7. Construction relationship between $I - C_i$ table and V_i's blocks.

case, the TFAA scheme is proposed to detect IOC attack from the design idea of trust fluctuation association analysis.

As shown in Fig. 6, the TFAA scheme is conducted in three successive stages: 1) trust data management; 2) trust fluctuation association rule; and 3) IOC attack detection.

B. Trust Data Management

With the trust data stored in blockchain by using the TruChain scheme, we can acquire historical messages of CVs and historical ratings of IVs comprehensively.

Considering the demand of detecting IOC attack, the historical messages of CVs should be managed for different IVs individually. Each vehicle can be assigned to an *I–C* table that saves the messages previously provided by all CVs on the vehicle when he plays the role of IV.

Take V_i as an example, the historical messages provided by all CVs and V_i's historical ratings can be managed with the $I - C_i$ table, as shown in Table III.

The construction relationship between $I - C_i$ table and V_i's blocks is shown in Fig. 7. We first seek out the latest block of V_i, in which the blocks index of V_i can be used to look for all the blocks of V_i quickly. Then, $I - C_i$ table can be constructed by the historical messages of CVs and historical ratings of V_i from all the blocks of V_i.

In the current TME action, if V_i is the IV, the $I - C_i$ table is first analyzed, in order to detect IOC attack. The *I–C* tables of all CVs should also be analyzed simultaneously, since IOC attackers often launch the role exchange between IV and CV to help with each other. Therefore, the *I–C* tables of both the IV and all CVs make up the *I–C* database, in which the trust fluctuation association analysis is performed to detect IOC attack in the current TME action.

Algorithm 1 Compute the Trust Fluctuation Index

```
Input: $T_i^g$
Output: $\mu_i$
Initialize each $\mu_i = 0$;
for ($g = 1, g \leq h, g++$) do
    if ($T_i^g \geq \varepsilon + \eta_2$) then
        if ($T_i^g \leq T_{i-1}^g$) then
            if ($T_i^g$ is continuous decreasing) then
                if ($T_i^g \leq \varepsilon + \eta_1$) then
                    $\mu_i++$;
                end if
            end if
        end if
    end if
    if ($T_i^g \leq \varepsilon + \eta_1$) then
        if ($T_i^g \geq T_{i-1}^g$) then
            if ($T_i^g$ is continuous increasing) then
                if ($T_i^g \geq \varepsilon + \eta_2$) then
                    $\mu_i++$;
                end if
            end if
        end if
    end if
end for
```

C. Trust Fluctuation Association Rule

To support the detection of IOC attack, we find the trust fluctuation association rule by analyzing the features of IOC attackers.

Since IOC attackers are engaged in reporting credible messages to maintain high trust value or incredible messages to manipulate TMAM, IOC attackers behave the trust fluctuation feature. We introduce the index μ to quantify this feature. μ can be computed by observing whether a vehicle's trust value is continuous increasing or decreasing. Take V_i is an example again, T_i^g denotes his trust value at time g. Algorithm 1 is performed to compute the trust fluctuation index of V_i (μ_i).

Algorithm 1 can be performed at the end of each TME action to update μ_i, in order to avoid the superfluous computation of μ_i in the detection of IOC attack.

For $\mu_i \geq 2$, it means an attacker has been launched at least one round of IOC attack to prompt his trust value and reported incredible messages. Of course, some attackers who behave honestly sometimes all by themselves can also make $\mu_i \geq 2$. To detect IOC attack effectively, we also need to analyze the association relationship among IOC attackers.

In the TFAA scheme, the association relationship among IOC attackers can be analyzed based on the following three features.

1) *Attacker Together:* IOC attackers often report messages together. They can help with each other in the IOC manner. In the inside threat, the IOC initiator activates a TME action. In the outside threat, the IOC cooperators

TABLE III
DESCRIPTION OF THE *I-C*$_i$ TABLE STYLE

SN	C_ID(messages)						I_ID(ratings)
1	$V_1(msg_1)_1$	$V_2(msg_2)_1$	$\cdots$	$V_j(msg_j)_1$	$\cdots$	$V_n(msg_n)_1$	$V_i(rat_i)_1$
2	$V_1(msg_1)_2$	$V_2(msg_2)_2$	$\cdots$	$V_j(msg_j)_2$	$\cdots$	$V_n(msg_n)_2$	$V_i(rat_i)_2$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
h	$V_1(msg_1)_h$	$V_2(msg_2)_h$	$\cdots$	$V_j(msg_j)_h$	$\cdots$	$V_n(msg_n)_h$	$V_i(rat_i)_h$

- **SN**: The serial number of TME action, in which h is the total number of TME action initiated by V_i.
- **C_ID (messages)**: The ID of CVs and their historical messages. For $V_j(msg_j)_2$, V_j is the ID of j-th CV and $(msg_j)_2$ is his messages at the 2-th TME action.
- **I_ID(ratings)**: The ID of the IV and his historical ratings. For $V_i(rat_j)_2$, V_i is the ID of i-th IV and $(rat_j)_2$ is his rating corresponding to the truth of traffic-related event at the 2-th TME action. Specifically, $V_j(msg_j)_2$ is recorded as $V_j(-)2$ when V_i reported nothing.

report the messages which are the same with the rating of the IOC initiator.

2) *Role Exchange:* An IOC attacker can play the role of IOC initiator to help his conspirators who play the role of IOC cooperators. After a round of IOC attack, one of IOC cooperators will be assigned as a new IOC initiator, while the former IOC initiator can become a new IOC cooperator.
3) *Majority Rule:* The decision made by TMAM should agree with the majority's opinion.

For the first feature, IOC cooperators can be recognized as the frequent cooperators who often appear together. In the association analysis, the index support count $s(\cdot)$ can be used to identified the frequent cooperators. For instance, if V_1, V_2, and V_3 are three frequent cooperators, their support count $s(V_1, V_2, V_3)$ which is the number of simultaneous appearance of V_1, V_2, and V_3 should meet the following rule by searching *I–C* tables:

$$s(V_1, V_2, V_3) \geq \text{minsup} \tag{3}$$

where *minsup* is the minimum of support count.

For the second feature, we can also find that the IOC initiator and IOC cooperators often appear together. For instance, if V_6 is the IOC initiator who launches the inside threat and V_1, V_2, and V_3 are three IOC cooperators who launch the outside threat, the association relationship between them can be described as $V_6 \to V_1, V_2, V_3$.

For the third feature, if the number of IOC cooperators is more than the half of CVs in the current TME action, IOC attackers can manipulate the decision of TMAM successfully. For instance, V_6 is also the IOC initiator and V_1, V_2, V_3 V_4, and V_5 are CVs in the current TME action. V_1, V_2, and V_3 can manipulate TMAM since they are the majority of CVs. According to the association analysis, V_6 and V_1, V_2, and V_3 can be identified as IOC attackers under the rule

$$s(V_6 \to \{V_1, V_2, V_3\}) \geq \text{minsup}. \tag{4}$$

Without loss of generality, assume V_i is an IV and Φ is the set of CVs in the current TME action. We can employ $\Phi_{(1/2)}$ to denote the set of IOC cooperators. According to the majority rule, the number of elements in $\Phi_{(1/2)}$ should be at least the half elements of Φ. The number of elements in $\Phi_{(1/2)}$ can be set as

$$\left|\Phi_{\frac{1}{2}}\right| = \left\lfloor \frac{|\Phi|}{2} \right\rfloor + 1. \tag{5}$$

For each $V_j \in \Phi_{(1/2)}$, the trust fluctuation association rule can be designed as

$$s\left(V_i \to \Phi_{\frac{1}{2}}\right) \geq \text{minsup} \tag{6}$$

under the constraint $\mu_j \geq 2$.

Additionally, we propose a dynamic sampling observation method to ensure the value of *minsup* dynamically. With the increase of rounds of IOC attack, the support of the IOC initiator and IOC cooperators will also augment. So, it is not possible to set *minsup* as a static value, but update *minsup* dynamically with the increase of rounds of IOC attack.

The technological process of the dynamic sampling observation method is shown in Fig. 8. At first, an initial value is set to *minsup*. Each q rounds of the detected IOC attack need to be observed. If the mean value of support count for q rounds of the detected IOC attack is less than the mean value of next q rounds, the minimum of support count of next q rounds of the detected IOC attack is used to update *minsup*.

In the current TME action, if the trust fluctuation association rule is workable, IOC attack can be detected. In this case, the current TME action should be abandoned, and thus depriving the opportunities of IOC attackers to prompt their trust value.

D. IOC Attack Detection

Supported by the trust fluctuation association rule, our goal is to detect IOC attack fast and reduce the search volume of the *I–C* database. Actually, the basic idea of the TFAA scheme to detect IOC attack can be described as a recursive elimination scheme to reduce suspicious CVs, namely unlikely IOC cooperators should be deleted in the current TME action, and thus reducing the detection time of IOC attack. The detection process of IOC attack is shown in Fig. 9.

We can use the trust fluctuation index as the first level to delete unlikely IOC cooperators. Φ_1 denotes the set of the rest CVs who are not deleted from Φ. If $|\Phi_1| < |\Phi_{(1/2)}|$, it means that the current TME action is secure against IOC attack. The detection can exit.

Generally, if a CV rarely appears with V_i, he would also rarely appear with V_i and other CVs together. So, we can continue to the second level to delete unlikely IOC cooperators by analyzing the support count between the IV (V_i) and each CV (such as V_j) in Φ_1. Here, Φ_2 denotes the set of the rest CVs who are not deleted from Φ_1. If $|\Phi_2| < |\Phi_{(1/2)}|$, it means

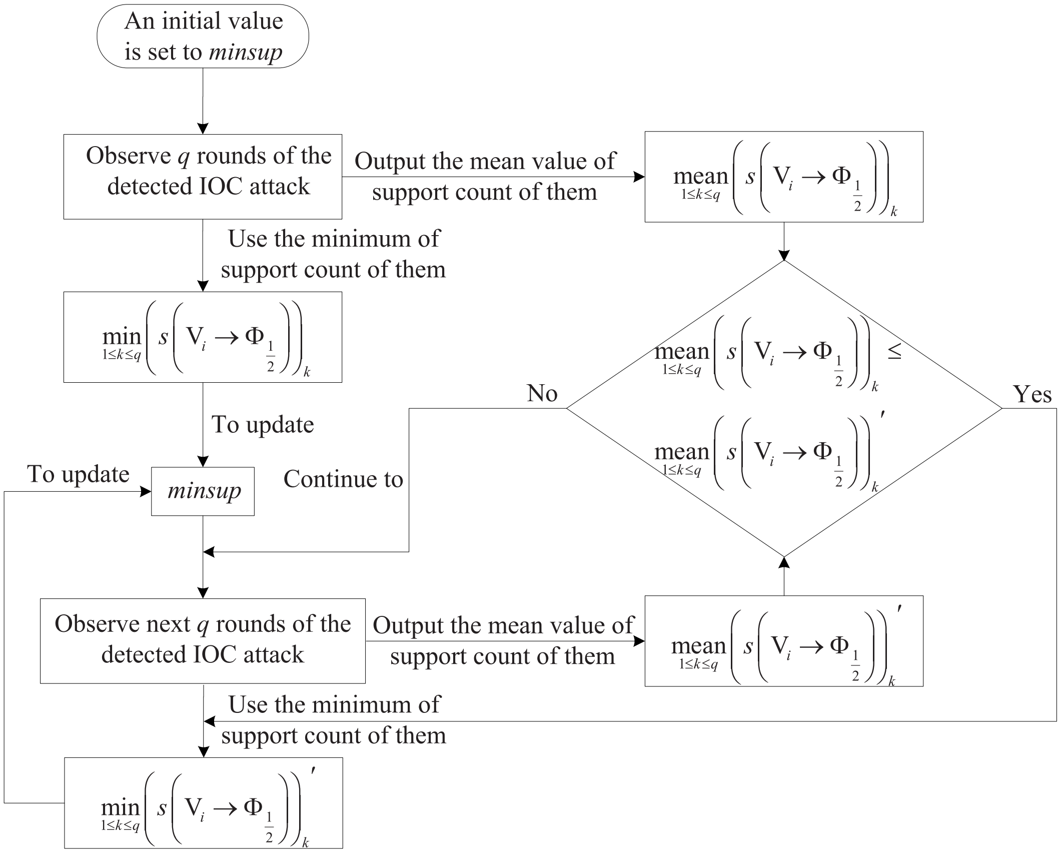

An initial value is set to *minsup*
Observe q rounds of the detected IOC attack
Output the mean value of support count of them
$\underset{1\le k\le q}{\text{mean}}\left(s\left(V_i \to \Phi_{\frac{1}{2}}\right)\right)_k$
Use the minimum of support count of them
$\underset{1\le k\le q}{\min}\left(s\left(V_i \to \Phi_{\frac{1}{2}}\right)\right)_k$
$\underset{1\le k\le q}{\text{mean}}\left(s\left(V_i \to \Phi_{\frac{1}{2}}\right)\right)_k \le \underset{1\le k\le q}{\text{mean}}\left(s\left(V_i \to \Phi_{\frac{1}{2}}\right)\right)'_k$
No
Yes
To update
To update
minsup
Continue to
Observe next q rounds of the detected IOC attack
Output the mean value of support count of them
$\underset{1\le k\le q}{\text{mean}}\left(s\left(V_i \to \Phi_{\frac{1}{2}}\right)\right)'_k$
Use the minimum of support count of them
$\underset{1\le k\le q}{\min}\left(s\left(V_i \to \Phi_{\frac{1}{2}}\right)\right)'_k$

Fig. 8. Technological process of the dynamic sampling observation method.

that the current TME action is secure against IOC attack. The detection can exit.

After the two levels, the search volume of *I–C* database can be reduced obviously. For each $V_j \in \Phi_{(1/2)}$, we can use the trust fluctuation association rule to detect IOC attack by searching his $I - C_j$ table.

In summary, Algorithm 2 can be performed to detect IOC attack.

VI. Simulation Analysis

A. Simulation Setup

Computer simulations are performed to further analyze IOC attack and show the performance of its defense scheme-TFAA. The simulation elements are shown in Table IV.

The simulations are performed by cycle-based fashion. At each cycle, some vehicles are selected randomly to execute TME actions in different vehicular regions. Then, the behavior pattern for honest vehicles is modeled to always report credible messages, while the behavior pattern for attackers is to report credible or incredible messages alternately. With the TruChain scheme, the generated trust data on the relevant vehicles can be shared for the entire network. After a few cycles, a trusted network topology is gradually generated by trust mechanism with the guard of the TFAA scheme. The initial minimum of support count (minsup) is set to 3, which is also updated dynamically for every 20 observing rounds of the detected IOC attack.

TABLE IV
Description of Simulation Elements

Parameters	Description	Default
N_v	Number of vehicles	60
N_r	Number of vehicular regions	10
cycle	Number of cycle simulation	200
round	Rounds of attack	50
p	Percentage of IOC attackers	10∼50%
η_1	Trust warning line	0.1
η_2	High trust line	0.3
ε	Threshold of trust value	0.5

B. Simulation Results

One of main goals of IOC attackers is to prompt their trust value. As we know, a vehicle such as V_i can be identified as malicious by $T_i < \varepsilon$ in trust mechanism. To increase his attack strengthen, V_i need to be disguised as a high-trust attacker, i.e., $T_i \ge \varepsilon$.

To analyze how IOC attack can affect the performance of trust mechanism, we first choose six IOC attackers randomly to observe the variation of their trust value in the Baseline and TFAA scheme. As shown in Fig. 10, their trust value usually outweigh ε in the Baseline scheme. Due to the mobility, their trust value are diverse, but behave the fluctuation feature with the increase of cycles. With the guard of the TFAA scheme, IOC attackers have no chance to prompt their trust value when they are detected in the TME action, so their trust value are decreased with the increase of cycles.

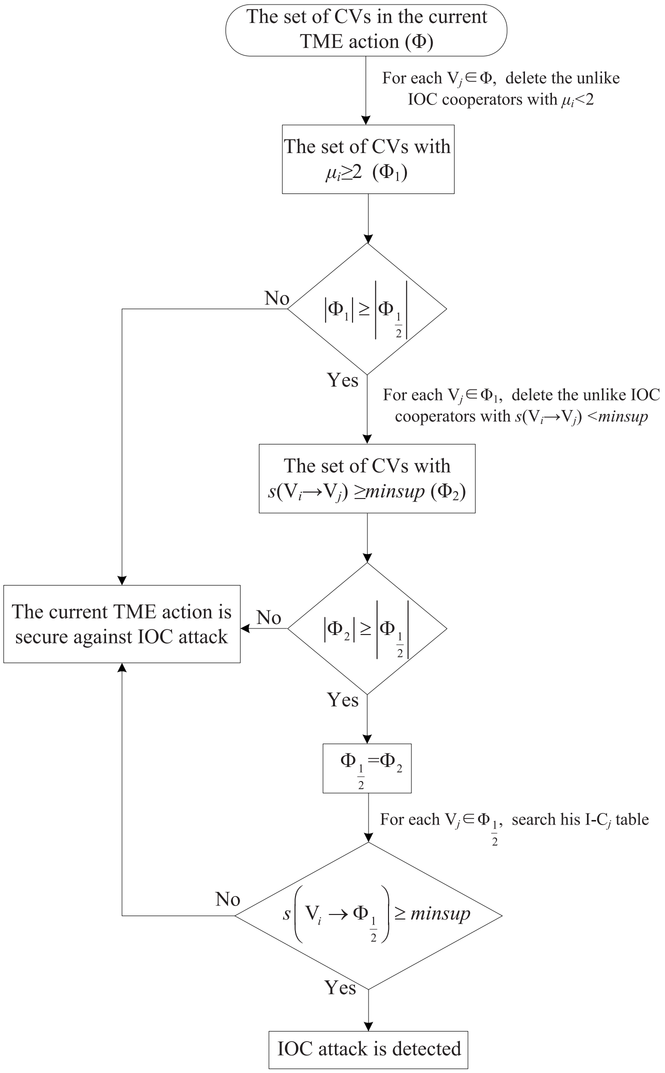

The set of CVs in the current TME action (Φ)
For each V$_j$∈Φ, delete the unlike IOC cooperators with μ_i<2
The set of CVs with μ_i≥2 (Φ$_1$)
$|\Phi_1| \geq |\Phi_{\frac{1}{2}}|$
No
Yes
For each V$_j$∈Φ$_1$, delete the unlike IOC cooperators with s(V$_i$→V$_j$) <*minsup*
The set of CVs with s(V$_i$→V$_j$) ≥*minsup* (Φ$_2$)
$|\Phi_2| \geq |\Phi_{\frac{1}{2}}|$
No
Yes
The current TME action is secure against IOC attack
$\Phi_{\frac{1}{2}} = \Phi_2$
For each V$_j$∈$\Phi_{\frac{1}{2}}$, search his I-C$_j$ table
$s\left(V_i \rightarrow \Phi_{\frac{1}{2}}\right) \geq minsup$
No
Yes
IOC attack is detected

Fig. 9. Detection process of IOC attack.

Algorithm 2 IOC Attack Detection

```
Input: $\Phi$
Output: $dr$ (the detection result)
Initialize $\Phi = \Phi_1 = \Phi_2 = \emptyset$, $dr = 0$, $|\Phi_{\frac{1}{2}}| = \lfloor \frac{|\Phi|}{2} \rfloor + 1$
for each $V_j \in \Phi$ do
    if ($\mu_j \geq 2$) then
        $\Phi_1 \leftarrow V_j$ which is placed to $\Phi_1$
    end if
end for
if ($|\Phi_1| \geq |\Phi_{\frac{1}{2}}|$) then
    for each $V_j \in \Phi_1$ do
        if ($s(V_i \rightarrow V_j) \geq minsup$) then
            $\Phi_2 \leftarrow V_j$ which is placed to $\Phi_2$
        end if
    end for
else
    $dr = 0$
    The current TME action is secure against IOC attack
    Exit
end if
if ($|\Phi_2| \geq |\Phi_{\frac{1}{2}}|$) then
    $\Phi_{\frac{1}{2}} = \Phi_2$
else
    $dr = 0$
    The current TME action is secure against IOC attack
    Exit
end if
for each $V_j \in \Phi_{\frac{1}{2}}$ do
    Search his $I - C_j$ table
end for
if ($s(V_i \rightarrow \Phi_{\frac{1}{2}}) \geq minsup$) then
    $dr = 1$
    IOC attack is detected
else
    $dr = 0$
    The current TME action is secure against IOC attack
end if
```

We note that IOC attackers will deviate the real trust value by forming high-trust attackers, and thus causing some network trust errors (*nte*). A higher errors indicate lower accuracy in the evaluation of trust value. With *nte*, we can analyze how IOC attack affects the performance of trust mechanism from the entire network. *nte* can be specified by

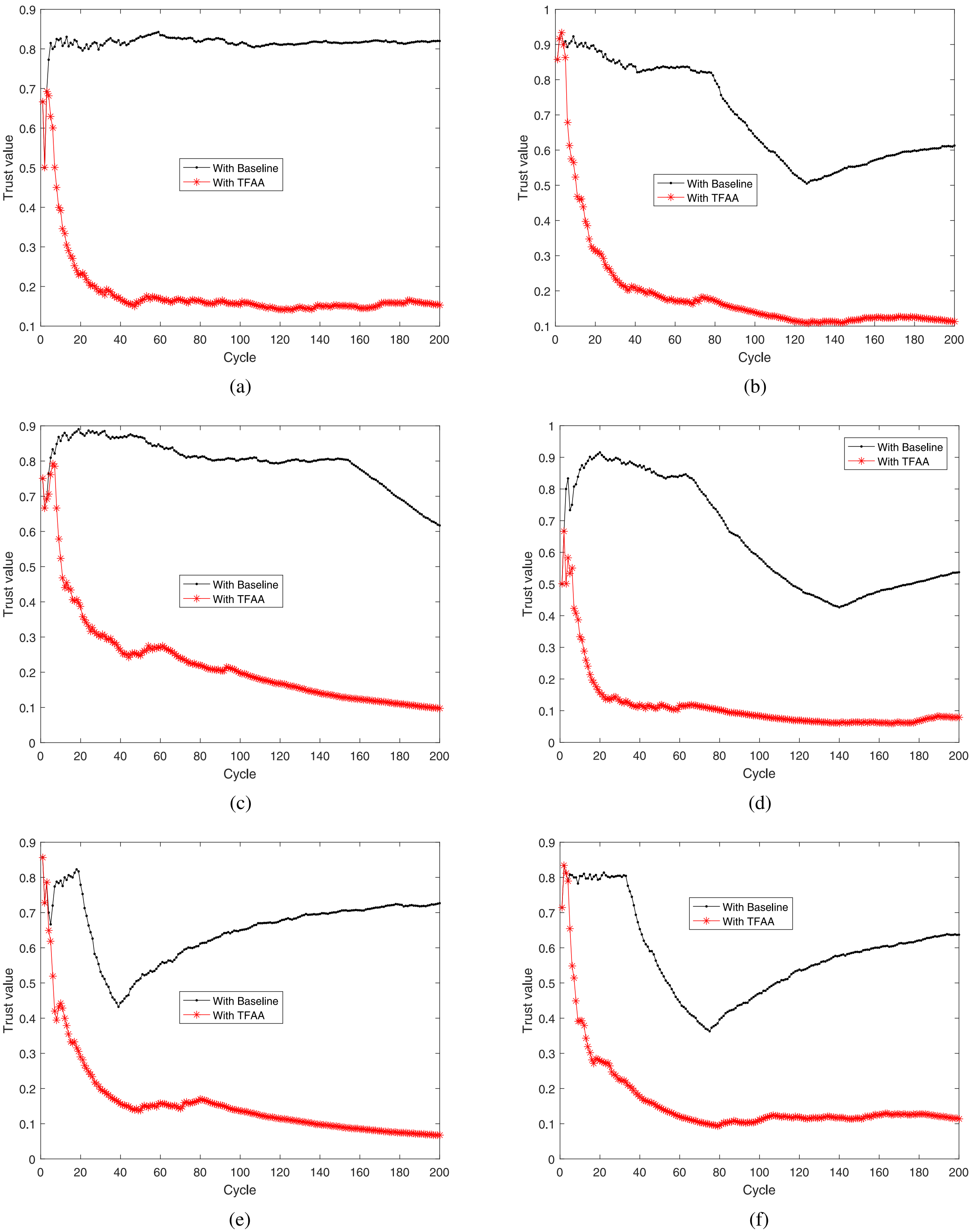
$$nte = \frac{1}{N_v} \sum_{i=1}^{N_v} \sqrt{\frac{1}{T_i'} \left(T_i' - T_i\right)^2} \tag{7}$$

where T_i' and T_i are the actual and measured trust value of T_i, respectively.

In the simulation of *nte*, the actual trust value of an IOC attacker is randomly assigned in the interval (0, 0.5]. Without loss of generality, we employ the averaged *nte* data of 200 cycles as the simulation results. As shown in Fig. 11, the TFAA scheme can reduce *nte* effectively. Even though the percentage of IOC attackers is 50%, the *nte* of the TFAA scheme merely achieves 0.21. Without any guard measures, the *nte* curve with the Baseline scheme increases rapidly.

As we know, attackers launch IOC attack to prompt their trust value, which may generate a large amount of malicious responses at each cycle. The IOC malicious responses may cause the unnecessary waste of network resources. So, the best measure to suppress IOC attack is to reduce these malicious responses. We also validate the effectiveness of the TFAA scheme in terms of reducing malicious responses, as shown in Fig. 12. In this simulation, the percentage of IOC attackers is set to 30%. Without any guard measures in the Baseline scheme, IOC attackers' trust value decreases slowly, they can get more chance to launch IOC attack, resulting in the most malicious responses. In the TFAA scheme, some of IOC attackers are rejected to request the TME action due to their trust fluctuation association feature, and thereby suppress malicious responses effectively.

We also validate the performance of TFAA in terms of attack success ratio when IOC attackers fake traffic-related messages with high trust value. Without loss of generality, we employ the averaged attack success ratio data of 50 rounds of attack as the simulation results. At each round of attack, several CVs are selected randomly to perform a TME action from honest vehicles and IOC attackers. In a TME action, if the IOC attackers with high trust value are more than the majority of CVs, they would attack successfully.



(a)

(b)

(c)

(d)

(e)

(f)

Fig. 10. Variation of IOC attackers' trust value. (a)–(f) IOC attackers 1–6.

As shown in Fig. 13, the attack success ratio against the Baseline scheme amplifies with the percentage of IOC attackers. Because IOC attackers' trust value usually outweigh ε in the Baseline scheme, they can manipulate the decision result of TMAM with incredible messages easily. Fortunately, IOC attackers are difficult to prompt their trust value to outweigh ε

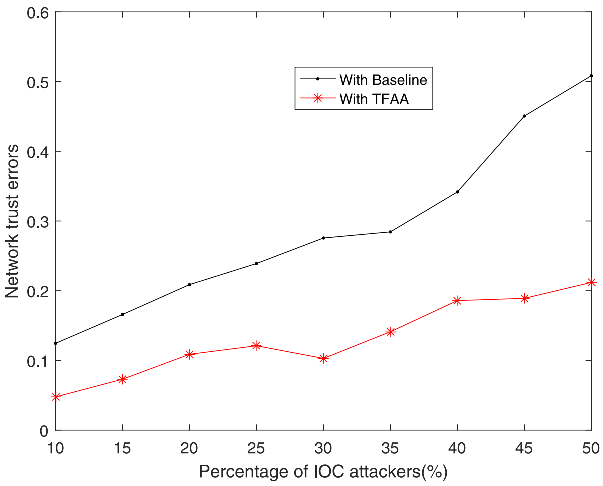


Fig. 11. *nte* with the guard of TFAA.

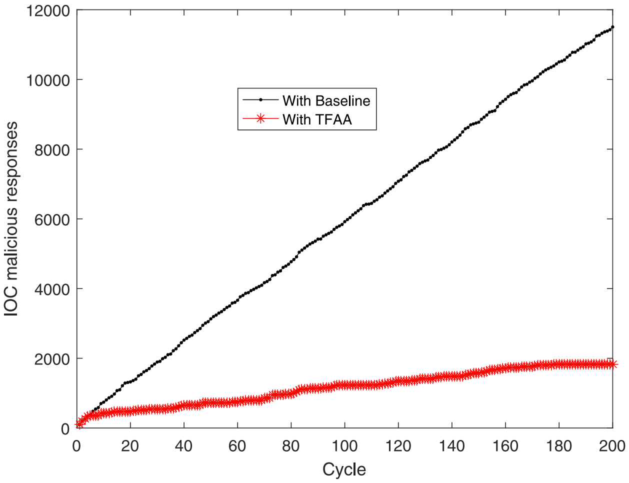


Fig. 12. Suppressing IOC malicious responses.

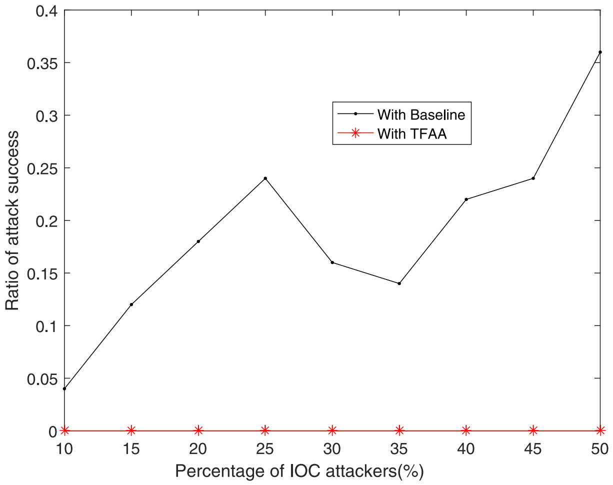


Fig. 13. Suppressing attack success ratio with incredible messages.

in the TFAA scheme. Consequently, IOC attackers are impossible to manipulate the decision result of TMAM, since the IOC attackers with high trust value cannot become the majority of CVs.

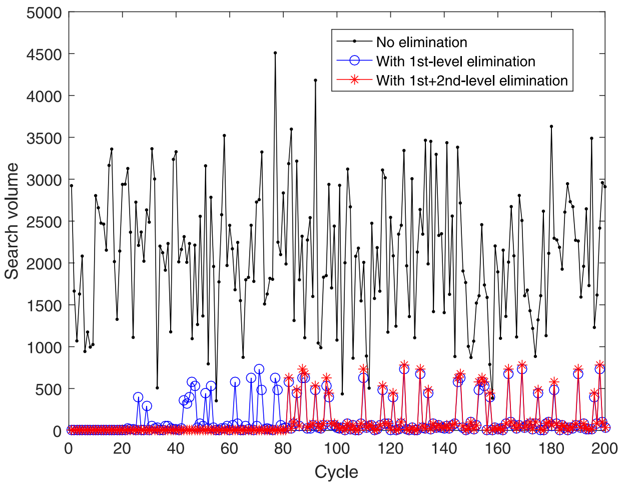


Fig. 14. Variation of search volume under the three cases.

We have known that TFAA is a recursive elimination scheme to detect IOC attack rapidly and effectively. To analyze such recursive elimination characteristic of the TFAA scheme, we observe the search volume to the *I–C* database under the three cases: 1) no elimination; 2) 1st-level elimination; and 3) 1st+2nd-level elimination.

As shown in Fig. 14, the search volume is the largest when no elimination is adopted in TFAA scheme. In the case that using the trust fluctuation index as the 1st-level elimination level to delete unlikely IOC attackers in CVs, the search volume drops significantly. We continue to add the 2nd-elimination level to delete unlikely IOC attackers through the association relationship analysis. In this case, the search volume is less than the 1st-level elimination sometimes. This shows that most of IOC attackers behave the trust fluctuation feature, which can speed up the detection of IOC attack in a TME action.

VII. Conclusion

In this article, we report the description of IOC attack and present the TFAA scheme to defend against this attack in vehicular networks. The TFAA scheme is designed in three successive stages: 1) trust data management; 2) trust fluctuation association rule; and 3) IOC attack detection, in which trust fluctuation association analysis is introduced to propose the TFAA scheme. To avoid the defeats of centralized and distributed trust mechanism, we also design the TruChain scheme based on consortium blockchain to support the management and storage of trust data for the TFAA scheme. The simulation results show that our TFAA scheme can guard trust mechanism effectively and suppress attack success ratio against incredible messages of IOC attackers.

References

[1] D. Jia, K. Lu, J. Wang, X. Zhang, and X. Shen, “A survey on platoon-based vehicular cyber-physical systems,” *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 263–284, 1st Quart., 2016.

[2] Z. Lu, W. Liu, Q. Wang, G. Qu, and Z. Liu, “A privacy-preserving trust model based on blockchain for VANETs,” *IEEE Access*, vol. 6, pp. 45655–45664, 2018.

[3] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and S. Shen, "Security and privacy in smart city applications: Challenges and solutions," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 122–129, Jan. 2017.

[4] B. Kuang, A. Fu, S. Yu, G. Yang, M. Su, and Y. Zhang, "ESDRA: An efficient and secure distributed remote attestation scheme for IoT swarms," *IEEE Internet Things J.*, to be published.

[5] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1495–1505, Apr. 2019.

[6] T. N. D. Pham and C. K. Yeo, "Adaptive trust and privacy management framework for vehicular networks," *Veh. Commun.*, vol. 13, no. 7, pp. 1–12, 2018.

[7] Y.-C. Wei and Y.-M. Chen, "Efficient self-organized trust management in location privacy enhanced VANETs," in *Proc. Int. Workshop Inf. Security Appl.*, 2012, pp. 328–344.

[8] S. Li and X. Wang, "Quickest attack detection in multi-agent reputation systems," *IEEE J. Sel. Topics Signal Process.*, vol. 8, no. 4, pp. 653–666, Aug. 2014.

[9] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proc. IEEE Int. Congr. Big Data (BigData Congr.)*, Jun. 2017, pp. 557–564.

[10] A. Dua, N. Kumar, and S. Bawa, "A systematic review on routing protocols for vehicular ad hoc networks," *Veh. Commun.*, vol. 1, no. 1, pp. 33–52, 2014.

[11] D. Jiang and L. Delgrossi, "IEEE 802.11p: Towards an international standard for wireless access in vehicular environments," in *Proc. IEEE Veh. Technol. Conf. (VTC Spring)*, May 2008, pp. 2036–2040.

[12] Z. J. 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, Feb. 2019.

[13] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, "A comprehensive survey on vehicular ad hoc network," *J. Netw. Comput. Appl.*, vol. 37, no. 1, pp. 380–392, 2014.

[14] M. Azees, P. Vijayakumar, and L. J. Deborah, "Comprehensive survey on security services in vehicular ad-hoc networks," *IET Intell. Transp. Syst.*, vol. 10, no. 6, pp. 379–388, Aug. 2016.

[15] X. Yang, J. Liu, N. H. Vaidya, and F. Zhao, "A vehicle-to-vehicle communication protocol for cooperative collision warning," in *Proc. 1st Annu. Int. Conf. Mobile Ubiquitous Syst. Netw. Services (MOBIQUITOUS)*, 2004, pp. 114–123.

[16] M. A. Morid and M. Shajari, "An enhanced e-commerce trust model for community based centralized systems," *Electron. Commerce Res.*, vol. 12, no. 4, pp. 409–427, Nov. 2012.

[17] X. Y. Li, F. Zhou, and X. D. Yang, "Scalable feedback aggregating (SFA) overlay for large-scale P2P trust management," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 10, pp. 1944–1957, Oct. 2012.

[18] J. Y. Feng, Y. Q. Zhang, G. Y. Lu, and W. Zheng, "Securing cooperative spectrum sensing against ISSDF attack using dynamic trust evaluation in cognitive radio networks," *Security Commun. Netw.*, vol. 8, no. 17, pp. 3157–3166, Nov. 2015.

[19] M. Li, Y. Xiang, B. Zhang, Z. Huang, and J. Zhang, "A trust evaluation scheme for complex links in a social network: A link strength perspective," *Appl. Intell.*, vol. 44, no. 4, pp. 969–987, Jan. 2016.

[20] Q. Li, A. Malip, K. M. Martin, S.-L. Ng, and J. Zhang, "A reputation-based announcement scheme for VANETs," *IEEE Trans. Veh. Technol.*, vol. 61, no. 9, pp. 4095–4108, Nov. 2012.

[21] X. Li, J. Liu, X. Li, and W. Sun, "RGTE: A reputation-based global trust establishment in VANETs," in *Proc. 5th Int. Conf. Intell. Netw. Collaborative Syst.*, Sep. 2013, pp. 210–214.

[22] R. Mühlbauer and J. H. Kleinschmidt, "Bring your own reputation: A feasible trust system for vehicular ad hoc networks," *J. Sensor Actuator Netw.*, vol. 7, no. 3, pp. 1–23, Sep. 2018.

[23] C. P. Fernandes, I. D. Simas, E. R. D. Mello, and M. S. Wangham, "RS4VANETs—A decentralized reputation system for assessing the trustworthiness of nodes in vehicular networks," in *Proc. Int. Wireless Commun. Mobile Comput. Conf.*, Aug. 2015, pp. 268–273.

[24] J. Oluoch, "A distributed reputation scheme for situation awareness in vehicular ad hoc networks (VANETs)," in *Proc. IEEE Int. Multidiscipl. Conf. Cogn. Methods Situation Awareness Decis. Support.*, Mar. 2016, pp. 1–5.

[25] X. Huang, R. Yu, J. Kang, and Y. Zhang, "Distributed reputation management for secure and efficient vehicular edge computing and networks," *IEEE Access*, vol. 5, pp. 25408–25420, 2017.

[26] A. Josang and R. Ismail, "The beta reputation system," in *Proc. 15th Bled Electron. Commence Conf.*, Jun. 2002, pp. 1–14.

[27] Wikipedia. (Aug. 2016). *Gamma Function*. [Online]. Available: http://en.wikipedia.org/wiki/Gamma function

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

[29] M. Atzori, "Blockchain-based architectures for the Internet of Things: A survey," UCL Res., Center Blockchain Technol., London, U.K., Rep. SSRN 2846810, May 2016.

[30] A. Fu, S. Yu, Y. Zhang, H. Wang, and C. Huang, "NPP: A new privacy-aware public auditing scheme for cloud data sharing with group users," *IEEE Trans. Big Data*, to be published.

[31] Z. Yang, K. Zheng, K. Yang, and V. C. M. Leung, "A blockchain-based reputation system for data credibility assessment in vehicular networks," in *Proc. IEEE 28th Annu. Int. Symp. Pers. Indoor Mobile Radio Commun.*, Montreal, QC, Canada, Oct. 2017, pp. 1–5.

[32] V. Buterin. (Aug. 2015). *On Public and Private Plockchains*. [Online]. Available: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains

Jingyu Feng received the B.S. degree in electrical information science and technology from the Lanzhou University of Technology, Lanzhou, China, in 2006, and the Ph.D. degree in information security from Xidian University, Xi'an, China, in 2011.

He is an Associate Professor and a Supervisor of M.S. students with the Xi'an University of Posts and Telecommunications, Xi'an. His current research interests include wireless communication security and trust management.

Nan Liu received the B.S. degree in information security from the Xi'an University of Posts and Telecommunications, Xi'an, China, in 2017, where she is currently pursuing the M.S. degree.

Her current research interest includes wireless communication security.

Jie Cao is currently pursuing the undergraduation degree with the Xi'an University of Posts and Telecommunications, Xi'an, China.

His current research interest includes wireless communication security.

Yuqing Zhang (M'10) received the B.S. and M.S. degrees in computer science and the Ph.D. degree in cryptography from Xidian University, Xi'an, China, in 1987, 1990, and 2000, respectively.

He is a Professor and a Supervisor of Ph.D. students with the University of Chinese Academy of Sciences, Beijing, China. His current research interests include cryptography and network security.

Guangyue Lu received the B.S. and M.S. degrees in physics from Yangtze University, Jingzhou, China, in 1992 and 1995, respectively, and the Ph.D. degree in signal and information processing from Xidian University, Xi'an, China, in 1999.

He is a Professor and a Supervisor of M.S. students with the Xi'an University of Posts and Telecommunications, Xi'an. His current research interests include wireless communication, cognitive radio, and cooperative spectrum sensing.