IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received November 13, 2019, accepted December 20, 2019, date of publication January 15, 2020, date of current version February 4, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2966747

AATMS: An Anti-Attack Trust Management Scheme in VANET

JINSONG ZHANG[1], KANGFENG ZHENG[1], DONGMEI ZHANG[2], AND BO YAN[2]
[1]School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing 100876, China
[2]School of Computer Science, Beijing University of Posts and Telecommunications, Beijing 100876, China

Corresponding author: Dongmei Zhang (zhangdm@bupt.edu.cn)

This work was supported in part by the National Key Research and Development Program of China under Grant 2017YFB0802703, and in part by the National Nature Science Foundation of China under Grant 61602052.

ABSTRACT Vehicular Ad-hoc Network (VANET) is a significant component of intelligent transportation system, which facilitates vehicles to share sensitive information and corporate with others. However, due to its unique characteristics, such as openness, dynamic topology and high mobility, VANET suffers from various attacks. This paper proposes an anti-attack trust management scheme in VANET called AATMS to evaluate the trustworthiness of vehicles. With the help of AATMS, vehicles in VANET can avoid malicious vehicles and cooperate with trusted vehicles. The idea of AATMS is mainly inspired by TrustRank algorithm, which is used to combat web spams. In this paper, we calculate local trust and global trust, which indicate the local and global trust relationships among vehicles. First, Bayesian inference is adopted to calculate local trust of vehicles based on historical interactions. Then we select a small set of seed vehicles according to local trust and some social factors. Once we identify the reputable seed vehicles, we use the local trust link structure of vehicles to evaluate the global trust of all vehicles. The simulation results show that AATMS can efficiently identify trustworthy and untrustworthy vehicles in VANET even under malicious attacks.

INDEX TERMS VANET, trust management, local trust, global trust, social factors.

I. INTRODUCTION

Vehicular Ad-hoc Network (VANET) is a self-organized network, which is the key component contributing to Intelligent Transport System (ITS) [1]. VANET contains two types of communication, i.e., vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication [2], through which vehicles can communicate directly with neighboring vehicles and Road Side Units(RSUs) [3]. It brings benefits to road safety, traffic efficiency and local services. However, the unique characteristics of VANET, such as high mobility and dynamic connections, make it vulnerable to various kinds of external and internal attacks [4]. Traditional security solutions, such as certificates [5], signatures [6] and Public Key Infrastructures (PKIs) [7], are for defensing the external attackers, while for authorized and authenticated attackers from internal, these solutions are useless. Hence, to against internal attacks, trust management is proposed [8]. Trust management assesses the trustworthiness of vehicles in VANET according to their historical interactions, then vehicles can choose trustworthy vehicles to corporate with and avoid malicious vehicles.

Over the last few years, many trust models are proposed [9]–[13]. They use different algorithms, such as fuzzy logic, graph theory, D-S evidence theory and collaborative filtering. And multiple factors are considered, such as direct trust and recommendation trust. However, these models are determined by expert knowledge to some extent and many models are only suitable for special scenarios, such as highway vehicular platooning. In [14], social relationships, i.e. direct neighborhood, indirect neighborhood and friendship, are introduced to VANET. The weights assignation of these three parts is very important, however, it is difficult to determine the weights. Hao *et al.* [15] propose the concepts of local trust and global trust, which indicate the local and global trust relationships among vehicles. They adopt PageRank algorithm [16] used for web pages' rank to calculate the global trust of vehicles. Nevertheless, this scheme is vulnerable to some threat models.

To deal with these problems, we propose an anti-attack trust management scheme called AATMS. This scheme calculate local trust and global trust of vehicles respectively. First, we adopt Bayesian inference to calculate local trust

The associate editor coordinating the review of this manuscript and approving it for publication was Luca Cassano.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see http://creativecommons.org/licenses/by/4.0/

values based on historical interactions. Bayesian inference gets empirical knowledge by using historical statistical data, therefore it is not dependent on expert knowledge. Second, we design a novel TrustRank based algorithm to calculate global trust values. TrustRank algorithm [17] is an improvement of PageRank algorithm and has the ability of combating spam pages, which makes our proposed scheme attack-resistance. Besides, we introduce some social factors, i.e. diver factors, vehicle factors and behavior factors, to help filter untrustworthy vehicles. These social factors reflect the degree of the public trust on vehicles. The main contributions of this paper are summarized as follow.

- We propose an anti-attack trust management scheme called AATMS, which can not only effectively evaluate trustworthiness of vehicles in multiple application scenarios, but also be capable of resisting various attacks and keep robust.
- A Bayesian inference based method is proposed to calculate local trust values of vehicles. The local trust values are used to build the trust link graph. Since this graph is independent from the fast-changing topology of VANET, it is relatively stable and can be used to do link analysis.
- We design a novel TrustRank based algorithm to calculate global trust value of vehicles. Specifically, we introduce some social factors to help select reputable seed vehicles. The trust values transfer from seed vehicles to other vehicles along the trust link graph, which can be treated as a Markov process. Meanwhile, in order to prevent a vehicle's trust value from rising rapidly and allow it to drop quickly, we introduce an adaptive forgetting factor and an adoptive decay factor to update local trust values and global trust values respectively.
- Experiments are conducted by using Veins [18] simulation platform. The experimental results show that the proposed AATMS scheme can effectively evaluate the trustworthiness of vehicles in VANET even under three malicious attacks, i.e. newcomer attack, on-off attack and collusion attack.

The rest of paper is organized as follow. Section II gives an overview of related works. Section III presents the network architecture and attack model of AATMS. Section IV describes the proposed scheme AATMS in details. The simulation results and analysis of AATMS are presented in section V. Finally, the conclusion is drawn in Section VI.

II. RELATED WORKS

We first present relevant studies on web pages' ranking algorithm, because the hyperlink structure of web pages is similar with the trust link graph of vehicles. Then we introduce some relevant studies of trust model in VANET.

A. RANKING ALGORITHM FOR WEB PAGES

Many algorithms are used to get the relative importance of web pages. PageRank algorithm [16] objectively and mechanically assigns global importance scores to all web pages according to web pages' hyperlink structure. In specific, a page is important when several other important web pages point to it. However, pages can cheat to improve their rank. For example, attackers can place many hyperlinks pointing to the target page in portal sites, such as Sina and NetEase. Since these portal sites are highly ranked, the target page's rank will become high. In order to deal with this problem, TrustRank algorithm [17] is proposed. This algorithm introduces expert knowledge to identify the reputable seed pages, then uses the link structure of the web to discover other pages that are likely to be good. The techniques of link analysis used in TrustRank algorithm are introduced to develop AATMS.

B. TRUST MODELS FOR VANET

Trust establishment is a significant issue in VANET because it can assist vehicles to avoid malicious vehicles and make a wise decision to collaborate with trustworthy vehicles. With the development of Vehicular ad-hoc network, many trust models are proposed.

Most trust managements are based on the direct trust factors to establish evaluation model. Tan *et al.* [9] presented a trust management system for securing data plane of adhoc networks, which mainly collected two direct trust factors, i.e., the data packet delivery ratio and the average delay. They employed fuzzy logic to evaluate the path trust by using these two trust factors. Then graph theory was adopted to assess the node trust value. Finally, the proposed trust management system was integrated into the optimized link state routing (OLSR) protocol to choose the best route. Soley *et al.* [10] proposed a trust model based on fuzzy logic. Many factors related to the correctness of the received messages were considered, such as the lifetime of the message, the experience of direct interactions and the plausibility of sender. Besides, fog node was applied as a facility to assess the level of accuracy of event's location. It can be regarded as an authoritative node, which can help detect malicious attackers in VANET.

In trust management, except the direct trust factors, recommendation and feedback are commonly considered. Besides, more and more trust models are focusing on the security threats in VANET. Li and Song [11] proposed an attack-resistant trust management scheme for VANET, which can cope with simple attack, bad mouth attack and on-off attack. And node trust was assessed in two dimensions, i.e., functional trust and recommendation trust. Xia *et al.* [12] combined subjective trust and recommendation trust to construct an attack-resistant trust inference model in VANET. This model can establish secure and reliable communication paths by selecting trusted relay vehicles. Meanwhile, trust managements were proposed in some special scenarios, such as highway vehicular platoon. Hu *et al.* [13] presented a reliable trust-based platoon service recommendation scheme (REPLACE), which can help the user vehicles to avoid choosing badly behaved platoon head vehicles. It calculated the

TABLE 1. Main existing trust models.

	Architecture		Trust factors			Attack immunity				Revocation target	
	centralized	distributed	direct trust	indirect trust	social factors	newcomer	on-off	badmouth & ballot	others	dishonest entities	malicious messages
[9]		✓	✓						✓	✓	
[10]		✓	✓						✓	✓	✓
[11]		✓	✓	✓			✓	✓		✓	✓
[12]		✓	✓	✓			✓	✓	✓	✓	
[13]	✓			✓		✓	✓	✓		✓	
[14]	✓		✓	✓	✓					✓	
[19]		✓	✓	✓	✓				✓	✓	✓
[20]		✓	✓	✓	✓					✓	
[15]	✓		✓							✓	
[21]		✓	✓						✓	✓	✓

trust values of platoon head vehicles by using their user vehicle's feedback. Besides, an iterative filtering algorithm was proposed to resist against badmouth and ballot stuffing attacks.

In recent years, some new trust factors and trust evaluation algorithms are introduced into trust models of VANET. Lin *et al.* [14] introduced social behaviors into vehicular network and proposed a new concept, namely Vehicular Social Networks (VSNs). This paper considered three social relationships, i.e., the direct neighborhood, indirect neighborhood and friendship. Chaker *et al.* [19] introduced the role of vehicles to help assign the initial trust value. Vehicles were classified into two types, i.e. official vehicles (e.g. police cars, ambulances, etc.) and normal vehicles, and the initial trust value of official vehicles is twice as much as that of normal vehicles. In [20], considering that most driving decisions are made by drivers, drivers honesty was used as a weighting factor to enhance the inter-vehicle trust establishment. The experimental results showed that the human factor consideration had clearly enhanced the detection ratio of dishonest vehicles. Social factors used in AATMS are manly inspired by these papers illustrated above. Xiao *et al.* [15] proposed a trust model called IWOT-V to evaluate the trustworthiness of vehicles, which presented two algorithms, i.e., BayesTrust and VehicleRank. These two algorithms were based on Bayesian inference and PageRank algorithm. They were responsible for deriving the local and global trust relationships respectively. The local and global trust relationships used in [15] are borrowed to develop AATMS. Ezedin *et al.* [21] presented a novel blockchain-based solution to evaluate the trust values of unmanned aerial vehicles and ensure the security of critical infrastructure. Although they combined proof-of-work and proof-of-stack miner selection to reduce the energy consumption and network latency, this model is still not suitable for some delay sensitive scenarios of VANET. Table 1 summarizes the characteristics of existing trust models and evaluates them qualitatively regarding some key characteristics and evaluation metrics.

III. NETWORK ARCHITECTURE AND ATTACK MODEL

In this section, we describe the network architecture and attack model of our proposed scheme AATMS.

A. NETWORK ARCHITECTURE

As shown in Fig. 1, VANET consists of three major components: vehicles equipped with On Board Unit (OBU), Road Side Units (RSUs) and Trusted Authority (TA) [22].

- Vehicles: Vehicles can be regarded as a group of highly mobile nodes equipped with OBUs, which allow them to communicate with other vehicles and RSUs. In our scheme, vehicles are responsible for evaluating local trust values and transferring new generated local trust values to RSUs. Unlike TA and RSUs, there are no authorities managing vehicles, therefore some vehicles may be untrustworthy. That's why we need AATMS to evaluate trustworthiness of vehicles.
- RSUs: RSUs take charge of collecting local trust values from vehicles via wireless connections and providing collected local trust values to TA through backbone network. In order to collect enough trust information, RSUs are commonly deployed at important transportation hubs, such as street intersection and high speed exit [23].
- TA: TA plays a significant role in VANET, which verifies the authenticity of vehicles. In our scheme, TA is also responsible for calculating global trust values of vehicles by using local trust values from RSUs, social factors and old global trust values. To ensure the implement of these functions, TA should have sufficient storage and computing resources.

B. ATTACK MODEL

Similar to most security schemes, there are multiple attacks against the trust management scheme itself, such as newcomer attack, betrayal attack, on-off attack, badmouthing/ballot stuffing attack and collusion attack. In this

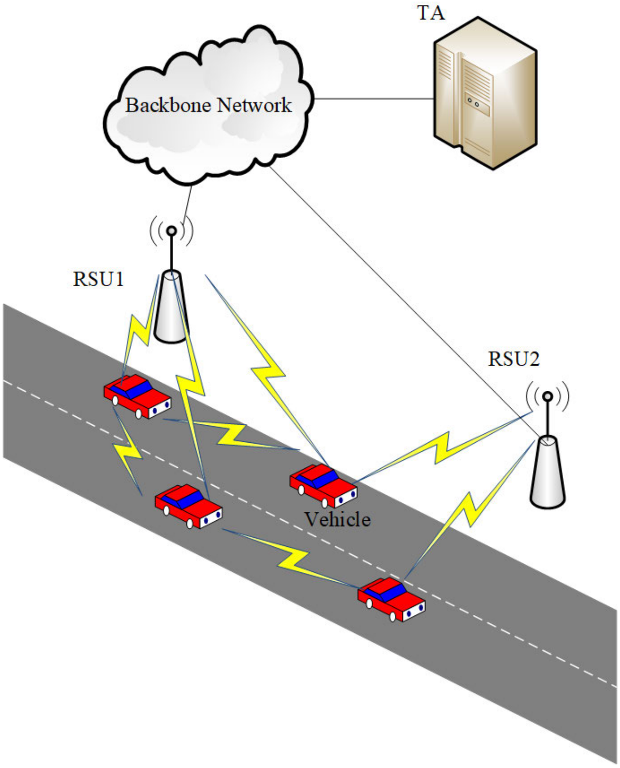


FIGURE 1. Network architecture.

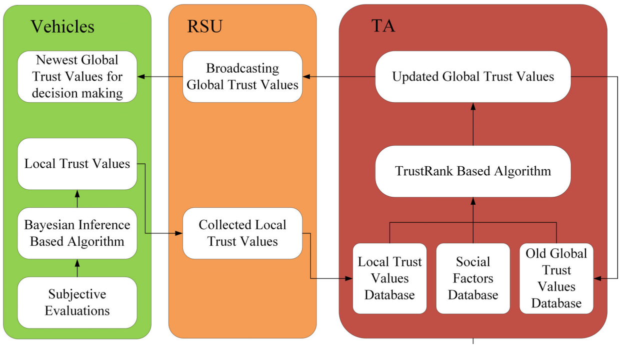

Vehicles
Newest Global Trust Values for decision making
Local Trust Values
Bayesian Inference Based Algorithm
Subjective Evaluations
RSU
Broadcasting Global Trust Values
Collected Local Trust Values
TA
Updated Global Trust Values
TrustRank Based Algorithm
Local Trust Values Database
Social Factors Database
Old Global Trust Values Database

FIGURE 2. The scheme overview of AATMS.

paper, we focus on three malicious attacks illustrated as below.

- Newcomer attack: The newcomer attack occurs when malicious vehicles erase their bad historical interactions by registering new IDs to re-launch [24]. In our proposed scheme, newcomers are assigned low initial trust values and an adoptive decay factor is introduced to prevent trust value from rising rapidly, therefore newcomers have to behave well during a long period to accumulate trust. Meanwhile, we can also connect the vehicle IDs in VANET with driving license in real world, which makes it hard for malicious vehicles to register new vehicle IDs [13].
- On-off attack: The on-off attack refers that malicious vehicles behave well and poorly alternatively to avoid being detected [25]. For example, attackers keep trustworthy for a period to accumulate high trust value and launch attacks suddenly, then go back to good behavior state. Since most trust management systems forget vehicles' past behaviors gradually, on-off attackers' trust values can recover again and repeat the above steps. To handle this problem, our proposed AATMS adopts an adaptive forgetting factor to strengthen memories of bad behaviors.
- Collusion attack: The collusion attack means that multiple vehicles form an alliance to launch attacks together in VANET [12]. For instance, malicious vehicles always give good feedback to their allies even their performance are poorly in order to improve allies' trust level. This kind of attack is also called ballot-stuffing attack. In contrast, allies give bad feedback to a well-performed vehicle to decline its trust level, which is called badmouth attack. These attacks can destroy the accuracy and truthfulness of the trust management system. To defense collusion attack, social factors are introduced in our proposed scheme to help filter untrusted vehicles.

IV. AN ANTI-ATTACK TRUST MANAGEMENT SCHEME OF VANET

In this section, we first describe the overview of our proposed scheme. Then we present how to calculate local trust value and global trust value. The details are described as follow.

A. SCHEME OVERVIEW

In our scheme, we make the assumption that TA and RUSs are fully trusted, and we only uncertain about the trustworthiness of vehicles. Although the network topology of VANET is dynamically changing, the trust relationship between vehicles is relatively stabled. And we can calculate the accumulated global trust of vehicles through the relatively stabled trust link graph of VANET.

The scheme overview of AATMS is depicted in Fig. 2. First, when interactions between vehicles happen, the served vehicles would give the serving vehicles subjective evaluations. Second, when conditions meet, such as enough sample size or specified time interval, local trust values are calculated based on Bayesian inference by using stored evaluation data. Third, vehicles periodically send newest local trust values to RSUs. We assume there are always enough RSUs along the road. Fourth, collected local trust values are stored and periodically sent to TA through RSUs. Fifth, by using the collected local trust values, TA can build the trust link graph like Fig. 3. In Fig. 3 the directed edge from node 3 to node 5 means vehicle 3 give some local trust values to vehicle 5 according to the interaction experience between them. While, node 7 has no links with any nodes, maybe vehicle 7 is a newcomer and has not enough interaction information. Sixth, based on the trust link relationship, social factors of vehicles and old global trust values, TA updates the global trust values of all vehicles by using TrustRank based algorithm. Finally, the global trust

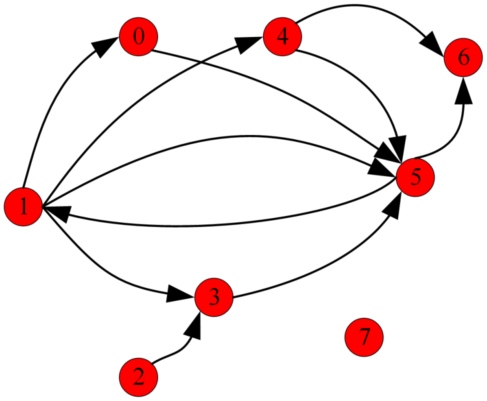


FIGURE 3. Trust link graph among vehicles.

values are broadcasted through RSUs, then one vehicle in VANET will cooperate with other vehicles who has high trust values.

B. CALCULATE LOCAL TRUST VALUE

We assume that the evaluation results among vehicles are only two levels {trustworthy, untrustworthy} and each time is taken as an independent process, so the evaluation results obey binomial distribution. Supposing that vehicle v_i received n messages from vehicle v_j, and among them, k items are true. The likelihood function is described as follow:

$$f(k|p_{ij}) = C_n^k p_{ij}^k (1-p_{ij})^{n-k} \tag{1}$$

where p_{ij} represents the probability that vehicle v_j sends true messages to v_i. The local trust value is related to p_{ij}. Since the conjugate prior distribution of binomial distribution is beta distribution, we suppose the probability distribution of p_{ij} is $beta(\alpha, \beta)$, and the prior distribution is given by:

$$f(p_{ij}; \alpha, \beta) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)} p_{ij}^{\alpha-1}(1-p_{ij})^{\beta-1} \tag{2}$$

where Γ is the gamma function, parameters $\alpha, \beta > 0$ and $0 \leq p_{ij} \leq 1$. At first, there are no interactions between vehicle v_i and vehicle v_j, and we do not have any prior knowledge, so we assume p_{ij} obeys uniform distribution, which is a special beta distribution with $\alpha = 1$ and $\beta = 1$.

According to Bayesian Inference, the posterior distribution is given by:

$$f(p_{ij}|k) \propto f(k|p_{ij}) f(p_{ij}) \tag{3}$$

By combining Eq.(1)-(3), we can describe the posterior distribution as below:

$$f(p_{ij}|k) = \frac{\Gamma(n+\alpha+\beta)}{\Gamma(k+\alpha)\Gamma(n-k+\beta)} p_{ij}^{k+\alpha-1}(1-p_{ij})^{n-k+\beta-1} \tag{4}$$

which is also a beta distribution, namely $beta(\alpha + k, \beta + n - k)$. Now we get the distribution of probability p_{ij}, and the expected value of p_{ij} can be regarded as local trust value m_{ij} of vehicle v_j from vehicle v_i.

Considering that in different application scenarios, the sample weights of false messages and true messages are different, therefore $w_{relative}$ is introduced to indicate the relative weight of false messages. Besides, in order to put more focus on recent interactions and prevent v_i from easily forgetting bad behaviors of v_j, we introduce a forgetting factor γ to update α and β:

$$\alpha = \gamma \cdot \alpha + k \tag{5}$$

$$\beta = \gamma \cdot \beta + (n-k) \cdot w_{relative} \tag{6}$$

The forgetting factor γ is an adoptive value, which is related to last updated local trust value m_{ij}^{old}. The equation is described as below [13]:

$$\gamma = c \cdot (1 - m_{ij}^{old}) \tag{7}$$

where c is a parameter to control the forgetting factor. We set the $c = 2$. From Eq. (7), we can see that, when $m_{ij}^{old} > 0.5$, γ is less than 1, which means that previous good behaviors of v_j will be gradually forgotten. On the contrary, when $m_{ij}^{old} > 0.5$, γ is greater than 1, and all of previous bad behaviors of v_j will be strongly memorized, then it will take longer time for v_j to build up a high trust value again. So adopting this adaptive decay factor into our scheme can effectively defense on-off attack, which is confirmed by the simulating results in Section V.

finally, we get the current local trust values m_{ij} as below:

$$m_{ij} = \frac{\alpha}{\alpha + \beta} \tag{8}$$

Since the Bayesian inference is effective only when the prior is trustworthy, which means vehicles should interact enough times before we first update m_{ij}. In this paper, in order to keep the minimum sample size n_{min} for the first update is greater than the sample size of above uniform distribution, we set the $n_{min} = 3$. For different application scenarios, we can adjust the value of n_{min}.

Algorithm 1 gives a detailed description about the calculation of local trust value. And we initialize all $m_{ij} = 0.5$. The output of Algorithm 1 is used to calculate global trust value in section IV-C.

C. CALCULATE GLOBAL TRUST VALUE

After local trust values are calculated and collected to TA, we can model the trust network among vehicles as a graph $g = (V, E, W)$ like Fig. 3, where vertex $v_i \in V$ denotes a vehicle, edge $e_{ij} \in E$ represents the trust link from vehicle v_i to v_j, and weight $w_{ij} \in W$ of the edge e_{ij} indicates the degrees of how v_i trusts v_j. This section will specifically describe how to calculate global trust value based on link analysis of this graph and social factors of vehicles.

1) TRANSITION MATRIX

The transition matrix is a $N \times N$ matrix W representing the trust transition among vehicles. The matrix value w_{ij} can be

Algorithm 1 The Calculation of Local Trust Value

```
Input:
    $k \geq 0$    // number of true messages
    $n \geq 0$    // total number of messages
    $n_{min} > 0$    // the minimum sample size of first update
    $w_{relative} > 0$    // the relative importance weight
    $c > 0$    // the parameter to control the forgetting factor
Output:
    $m_{ij}$    // local trust value of vehicle $v_j$ from vehicle $v_i$
if it is the first time to calculate $m_{ij}$ then
    if $n < n_{min}$ then
        return $null$
    else
        set $\alpha = 1$ and $\beta = 1$
    end if
else
    read $\alpha$, $\beta$ from local dataset
end if
read $m_{ij}^{old}$ from local dataset
calculate $\gamma$ with Eq.(7)
$\alpha = \gamma \cdot \alpha + k$
$\beta = \gamma \cdot \beta + (n - k) \cdot w_{relative}$
$m_{ij} = \frac{\alpha}{\alpha+\beta}$
save $\alpha$, $\beta$, $m_{ij}$ to local dataset
return $m_{ij}$
```

obtained by:

$$w_{ij} = \begin{cases} m_{ij}, & \text{if } m_{ij} > 0.5 \\ 0, & \text{otherwise} \end{cases} \tag{9}$$

where m_{ij} is the local trust value of vehicle v_j from vehicle v_i. Only when local trust value is greater than 0.5, we consider there is a trust relationship between vehicle v_i and vehicle v_j, then a certain degree of trust value is transferred from vehicle v_i to vehicle v_j. Otherwise, vehicle v_i would not allocate trust value to vehicle v_j, i.e. $w_{ij} = 0$. Then we normalize w_{ij} as below:

$$w_{ij} = \frac{w_{ij}}{\sum_{j \in s_{v_i}} w_{ij}} \tag{10}$$

where s_{v_i} is the set of vehicles serving vehicle v_i. However, vehicles that never provide trust evaluation but get allocation of trust value from other vehicles, just like node 6 in Fig. 3, can cause trust loss problem, because they do not distribute their trust value at all. This generates 0 rows in transition matrix. To address this problem, we replace 0 rows with t^{old}, which represents the old global trust value in the last update. It means that when a vehicle does not participate in the subjective evaluation process, its trust value will be allocated to all vehicles by default. And the amount of trust values that a vehicle gets is determined by its old global trust value.

2) SELECTING SEED VEHICLES

The goal of selecting seed vehicles is to find vehicles that will be most trustworthy and useful in identifying other vehicles' trust value. To achieve this purpose, we refer to the PageRank algorithm [16] and introduce social factors of vehicles.

Step 1: We adopt PageRank algorithm to order vehicles, which means vehicles with higher PageRank values (PR values) are more likely to be chose as seed vehicles. At first, all vehicles have the same PR values, namely $1/N$, where N is the total number of vehicles in VANET. Then we assume PR value consists of two parts, one is the trust value gained through providing trustworthy service, the other is obtained from the whole system, and the amount of second part is determined by vehicle's last updated global trust value. By adding these two parts together, we can get the final matrix equation form as below:

$$r = \alpha_1 \cdot W^T \cdot r + (1 - \alpha_1) \cdot t^{old} \tag{11}$$

where t^{old} is the last updated global trust vector and at first $t^{old} = 1/N \cdot 1_N$, W is the transition matrix introduced above, and α_1 is dampening factor indicating the weight of the first part, where $0 < \alpha_1 < 1$. The usage of dampening factor is to ensure convergence of Eq.(11), keeping the transition of PR value stable and continuous. When reaching up the maximum iteration number C_{max1}, iteration process is stopped and we get the final PR vector r.

Step 2: We sort vehicles in decreasing order according to PR vector and select the top L composing candidate set. Then we introduce some social factors of vehicles to select seed vehicles from candidate set. Social factors of vehicles reflect the degree of the public trust on vehicles. For example, compared to private cars, the public has more faith in public vehicles, such as bus and taxi. These public vehicles are usually drove by experienced drivers and are managed by trustworthy and authoritative institutions, therefore it is difficult for them to be controlled by attackers. As show in Fig. 4, social factors mainly come from three aspects: diver factors, vehicle factors and behavior factors. Diver factors reflect the characteristics of the diver, such as age, driving age and driving license score. Vehicle factors reflect the characteristics of the vehicle, such as vehicle type, vehicle age, handling stability, braking performance and other vehicle performance. Behavior factors reflect the characteristics of vehicles' behavior. For different application scenarios, specific behavior factors should be taken into account. For example, when we assess the performance of driving behavior, we can consider these factors: number of speeding, number of running red lights, number of traffic accidents and number of other traffic violation. We can use these social factors as filtering conditions to get the most reputable seed vehicles from candidate set. Since social factors reflects the driving skill of drivers and the quality of vehicles, they are useful for identifying untrustworthy vehicles. The filter function G is

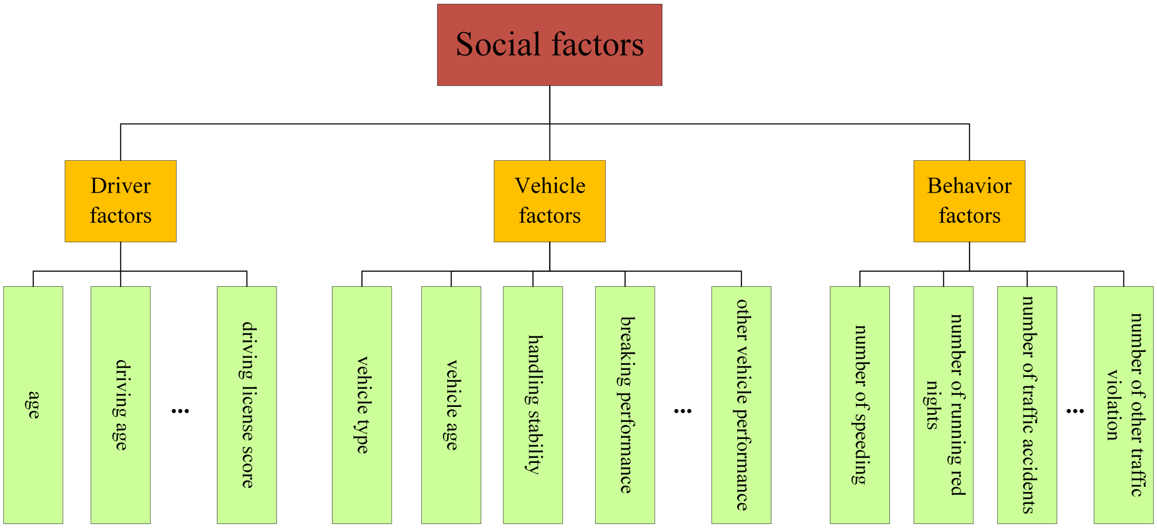


FIGURE 4. Social factors of vehicles.

shown as below:

$$G(i) = \begin{cases} 1, & \text{if } v_i \in \phi \\ 0, & \text{otherwise} \end{cases} \tag{12}$$

where ϕ denotes the set of vehicles passing through filtering. After we get seed vehicles by using social factors, we keep the PR values of seed vehicles unchanged and set others to zero. And we get the seed vector s. Then we normalize s so that its elements sum up to one.

3) GLOBAL TRUST VECTOR

This section shows the iteration process of global trust value. The iterative formula is based on the belief that trust flows out from reputable seed vehicles, and trust is reduced as a vehicle moves further and further away from seed vehicles in trust link graph. The formula is show as below:

$$t = \alpha_2 \cdot W^T \cdot t + (1 - \alpha_2) \cdot s \tag{13}$$

where t is the global trust vector and at first it is assigned as vector s. α_2 is dampening factor, where $0 < \alpha_2 < 1$. α_2 indicates the degree of trust loss when a vehicles is one link away from seed vehicles. When reaching up the maximum iteration number C_{max2}, we stop the iteration process and get the final global trust vector t.

In section IV-B, we introduce an adoptive forgetting factor γ to update local trust value. It can make the vehicle's trust value to drop quickly when the vehicle launch attacks, but it can not prevent trust value from rising rapidly. In order to deal with this problem, we design an adaptive decay factor to update global trust value. The decay method is shown as below:

$$z = \frac{t^{cur} - t^{old}}{t^{cur} + \epsilon} \tag{14}$$

$$\lambda = \frac{1}{1 + e^{-\theta \cdot z}} \tag{15}$$

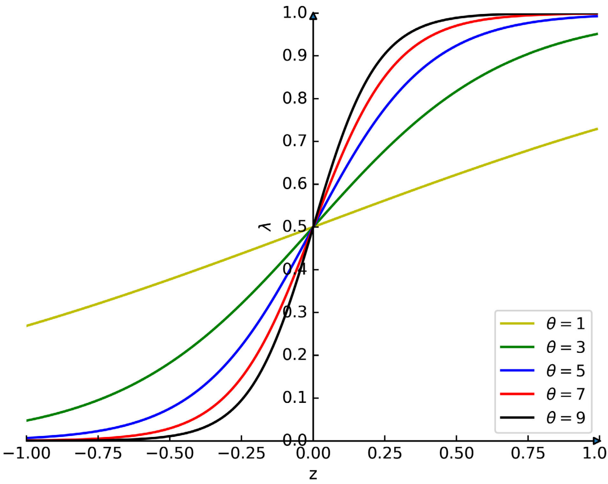


FIGURE 5. Curve of λ with different adjustment parameter θ.

$$t^{new} = \lambda \cdot t^{old} + (1 - \lambda) \cdot t^{cur} \tag{16}$$

where t^{cur} is the current global trust vector; t^{old} is the last updated global trust vector; t^{new} is the final updated global trust vector; parameter λ is the decay factor, which is determined by parameters z and θ. z indicates the change rate between t^{cur} and t^{old}, while θ is the adjustment parameter, and $\theta \geq 0$. ϵ is a very small value to avoid the denominator of Eq. (14) becoming zero. Several curves of the decay factor with different adjustment parameter θ are show in Fig. 5. We can see that θ determines the change rate of λ. As show in Eq. (14)-(16), when a vehicle's trust value rises rapidly, λ is a big value, and t^{new} will remain in a low level. Therefore, adopting this adaptive decay factor into our scheme can effectively defense newcomer attack. Besides, when a vehicle's trust value drops a lot, λ is a small value, and t^{new}

will decrease quickly. Hence, it would not affect the function of the adoptive forgetting factor γ.

Algorithm 2 gives a detailed description about the calculation of Global Trust Value. We initialize $t^{old} = 1/N \cdot 1_N$.

Algorithm 2 The Calculation of Global Trust Value

```
Input:
    $m_{ij}$ for all vehicles    // local trust value
    $N > 0$    // total number of vehicles in VANET
    $\alpha_1, \alpha_2$    // dampening factor
    $C_{max1}, C_{max2}$    // maximum number of iterations
    $\theta$    // adjustment parameter
    $L$    // the size of candidate set
Output:
    $t^{new}$    // global trust vector
for all $w_{ij} \in W$ do
    calculate $w_{ij}$ with Eq. (9)-(10)
end for
read $t^{old}$ from dataset
replace 0 rows in $W$ with $t^{old}$
$r = t^{old}$
for $i = 1$ to $C_{max1}$ do
    $r = \alpha_1 \cdot W^T \cdot r + (1 - \alpha_1) \cdot t^{old}$
end for
$\sigma = Rank(\{1, 2, \ldots, N\}, r)$//rank vehicles based on $r$
$s = 0_N$
for $i = 1$ to $L$ do
    if $G(\sigma(i)) == 1$ then
        $s(\sigma(i)) = r(\sigma(i))$
    end if
end for
$s = s/|s|$    // normalization
$t = s$
for $i = 1$ to $C_{max2}$ do
    $t = \alpha_2 \cdot W^T \cdot t + (1 - \alpha_2) \cdot s$
end for
$t^{cur} = t$
update $t^{new}$ with Eq.(14)-(16)
save $t^{new}$ to dataset
return $t^{new}$
```

V. EXPERIMENTS

This section illustrates the settings of evaluation experiments in simulation platform and presents the evaluation results of our proposed model. We compare our proposed scheme AATMS with the relevant model (i.e. IWOT-V [15]) under three malicious attacks to verify the attack resistance of AATMS.

A. SIMULATION DSIGN

1) SIMULATION PLATFORM

We use Veins [18] as the simulation platform, which is a hybrid framework for running vehicular network simulations. It is composed of the network simulator OMNeT++ [26] and the road traffic simulator SUMO [27]. OMNeT++ is an event-based network simulator, which is used to simulate network environment of VANET. SUMO can import road maps and generate the mobility model of vehicles. Both simulators are bi-directionally coupled and simulations are performed online.

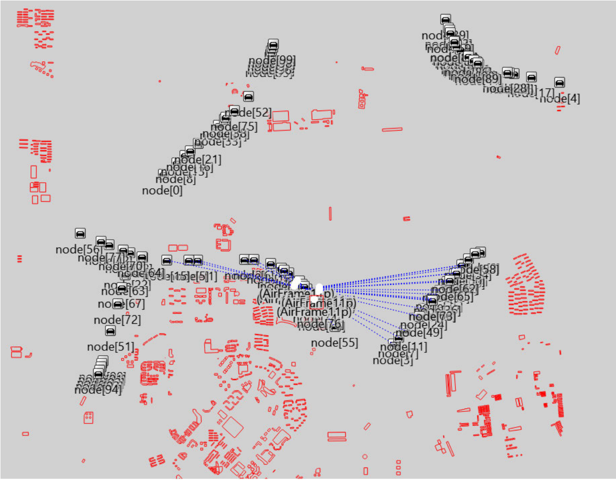


FIGURE 6. Traffic network in simulation.

2) SIMULATION SCENARIO CONSTRUCTION

Our proposed scheme is suitable for multiple trust evaluation scenarios, such as the trust evaluation of road condition messages and driving behaviors. In this paper, we apply it to assess the driving behaviors in motorway. Specifically, a vehicle driving over the road speed limit v_{road} is considered as an untrusted vehicle, otherwise, it is trustworthy. We can use the speed factor f_i in SUMO to preset the behavior of a vehicle, because the maximum speed v_{max} of a vehicle is determined by $f_i * v_{road}$. For example, a vehicle with speed factor 1.2 drives up to 20% above the speed limit whereas a vehicle with speed factor 0.8 would always stay below the speed limit by 20%. Therefore, a vehicle can be labeled as good or bad according to its speed factor. In the simulation, we set good vehicles' speed factors $f_{good} = 0.8$ and bad vehicles' speed factors $f_{bad} = 1.2$.

In this scenario, all vehicles are randomly spread over the traffic network. During trips of vehicles, they observe their neighbors' speed and give outcome of every observation according to the formula given below:

$$o_i = \begin{cases} 0, & \text{if } v_{vehicle} > v_{road} \\ 1, & \text{otherwise} \end{cases} \tag{17}$$

where $v_{vehicle}$ is current speed of a vehicle and o_i is the outcome of i^{th} observation. After a vehicle finished its trip, it would calculate local trust values about vehicles who had interactions with it, then sends the local trust values to RSUs. In order to accumulate enough interactions, we simulate 30 rounds with different random seeds and the global trust values of vehicles are updated 30 times.

TABLE 2. Simulation parameters.

Parameter	Value	Description
n_{min}	3	the minimum size of first updated
$w_{relative}$	3	the relative importance weight
c	2	the parameter to control forgetting factor
N	100	total number of vehicles
α_1, α_2	$0.85, 0.95$	dampening factor
C_{max1}, C_{max2}	$20, 20$	num. of iterations
θ	3	adjustment parameter
L	80	size of candidate set

3) PARAMETERS SETUP

We select the map of an area of Beijing, China and filter OSM data [28] to get motorways and buildings by using Overpass turbo [29]. The traffic network is shown in Fig. 6. The study area is 10km long and 12km wide. The red polygons in the figure are buildings, which are obstacles in wireless communication. The blue dotted lines represent the communications among vehicles. And the white dots are messages about speed information. We adopt Krauss' car-following model (Krauβ) [30], default path loss model (SimplePathlossModel) and default obstacle shadowing model (SimpleObstacleShadowing). In order to prevent front vehicles from blocking the vehicles behind, we set the parameter lcSpeedGain = 1, then vehicles can change lane to gain speed. It makes sure that most of vehicles can reach their maximum speed. In the simulation, there are 100 vehicles and the road speed limit is 44m/s. Parameters used in Algorithm 1 and Algorithm 2 are listed in Table 2.

4) EVALUATION METRIC

This section introduces three metrics that help us to evaluate the efficiency of AATMS.

The first metric is the pairwise orderedness [17], which is based on the assumption that good vehicles should be ranked higher than bad vehicles by an ideal algorithm. Supposing that we have already got the global trust value of all vehicles $T = t_1, t_2, t_3, \ldots, t_N$ and the corresponding labels $Y = y_1, y_2, y_3, \ldots, y_N$. $y_i = 1$ means v_i is a good vehicle, while $y_i = 0$ means v_i is a bad vehicle. P is the set of all ordered pairs of vehicles $(i, j), i \neq j$. The pairwise orderedness is defined as below:

$$I(T, Y, i, j) = \begin{cases} 1, & \text{if } t_i \geq t_j \text{ and } y_i < y_j \\ 1, & \text{if } t_i \leq t_j \text{ and } y_i > y_j \\ 0, & \text{otherwise} \end{cases} \tag{18}$$

$$pairord(T, Y, P) = \frac{|P| - \sum_{(i,j)\in p} I(T, Y, i, j)}{|P|} \tag{19}$$

We can see that if pairord equals one, there are no cases when a bad vehicle is ranked higher than a good vehicle. Conversely, if pairord equals zero, then all pairs are error ranked.

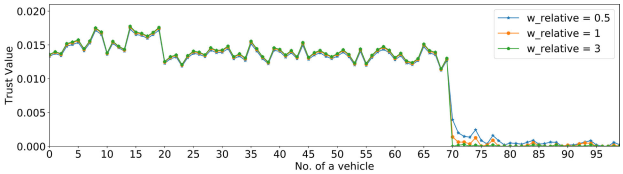


FIGURE 7. Global trust values of 100 vehicles in AATMS with different $w_{relative}$.

The next two metrics are related to the threshold of trust value. In order to classify vehicles into trustworthy or untrustworthy, we need to set the threshold of trust value. Since the total trust values are allocated by selected seed vehicles, seed vehicles will have higher trust values than other ordinary vehicles no matter these ordinary vehicles are bad or good. Therefore, the threshold should be set as the average trust value of vehicles excluding seed vehicles. Supposing that at current iterator, the number of selected seed vehicles is D and the sum of seed vehicles' trust values is T_{seed}, since the total trust value of all vehicles is 1, the threshold is described as below:

$$\bar{t} = \frac{1 - T_{seed}}{N - D} \tag{20}$$

Since average trust value indicates the average trust level of vehicles, vehicle v_i is trustworthy when $t_i \geq \bar{t}$ and untrustworthy when $t_i < \bar{t}$. Based on global trust value and preset speed factor, we can assess the performance of AATMS. Two metrics are used: True Positive Rate(TPR) and True Negative Rate (TNR). And they are defined as follow:

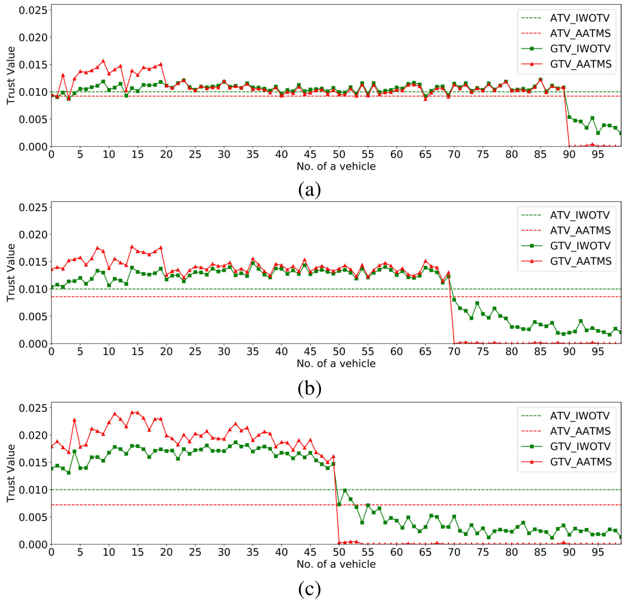
- TPR: the proportion of good vehicles that are classified as trustworthy.
- TNR: the proportion of bad vehicles that are classified as untrustworthy.

B. TRUST MODEL PERFORMANCE COMPARISON

In order to verify the effectiveness and the attack resistance of our scheme, we compare it with the relevant model (i.e. IWOT-V) under three malicious attacks. Three evaluation metrics: Pairord, TPR and TNR, are used to measure these two models.

1) PERFORMANCE COMPARISON WITHOUT ATTACKS

At first, we simulate the scenario without malicious attacks. We set No. 70 to No. 99 as bad vehicles. Since some social factors, such as diver factors, are concerned with privacy and it is very difficult to get real data, we suppose there are 20 vehicles in VANET passing filtering, that is No. 0 to No. 19 vehicles. These 20 vehicles compose of authority set. The rest of vehicles are ordinary good vehicles. Fig. 7 shows the global trust values of 100 vehicles in AATMS with different $w_{relative}$. From this figure, we can see that the greater $w_{relative}$ the lower global trust values of bad vehicles. Therefore, $w_{relative}$ represents the punishment intensity of bad



(a)

(b)

(c)

FIGURE 8. **Performance comparison under different percentage of bad vehicles without malicious attacks. (a) 10% of bad vehicles. (b) 30% of bad vehicles. (c) 50% of bad vehicles.**

behaviors and we can control the punishment intensity of bad behaviors in different scenarios of VANET by setting $w_{relative}$.

In the next simulation, we set $w_{relative} = 3$ and compare our proposed model with IWOT-V. Fig. 8 shows the global trust values of 100 vehicles in AATMS and IWOT-V under different percentage of bad vehicles. The red and green dotted lines represent the average trust value in AATMS and IWOT-V respectively. The red and green solid lines indicate the global trust value of each vehicle in AATMS and IWOT-V respectively. It can be seen that the good vehicles with speed factors less than 1 in AATMS are allocated much higher trust values than bad vehicles, especially the seed vehicles, trust values of which are mostly above 0.015. The reason why some seed vehicles' trust values are even lower than that of some ordinary good vehicles is because these seed vehicles give positive feedback to ordinary good vehicles frequently. Hence, they allocate most of their trust values. In the future, we would consider designing an incentive mechanism to reward nodes, which give feedback positively. In IWOT-V, the gap of trust value between good vehicles and bad vehicles is smaller than that of AATMS, especially when there are 50% of bad vehicles in VANET. It is because that with the increase of the proportion of bad vehicles, good vehicles' trust values increase both in IWOT-V and AATMS, while bad vehicles' trust values increase in IWOT-V and remain unchanged in AATMS. Since our proposed scheme can control the punishment intensity of bad behaviors by setting the value of $w_{relative}$, it effectively avoids the influence of the bad vehicles' proportion. The simulation result shows that when the percentage of bad vehicles increases, AATMS has a greater threshold space to accurately distinguish bad vehicles from good vehicles.

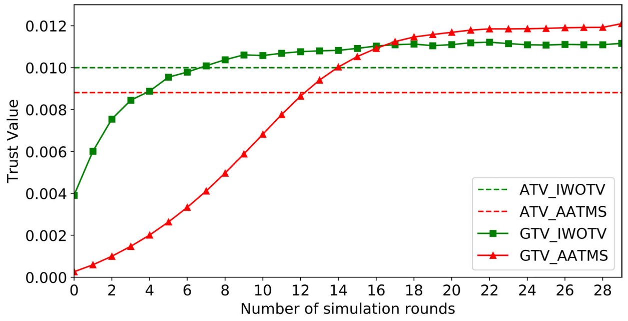


FIGURE 9. **The average global trust value of the newcomer attackers in AATMS and IWOT-V.**

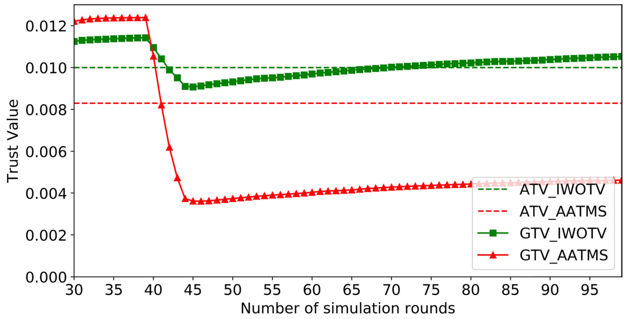
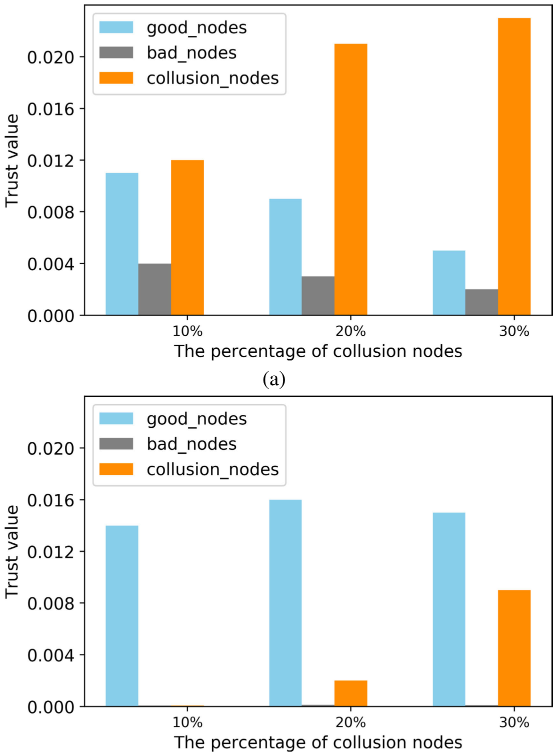


FIGURE 10. **The average global trust value of the onoff attackers in AATMS and IWOT-V.**

2) PERFORMANCE COMPARISON UNDER THREE MALICIOUS ATTACKS

In the experiments, we compare the robustness of our proposed scheme and IWOT-V against three different types of attacks. One threat is the newcomer attack. The newcomer attackers abound old low-trusted IDs and register new IDs to relaunch attacks. In the simulation, there are 20 bad vehicles, 60 good vehicles and 20 newcomer attackers. Newcomer attackers are new added vehicles in VANET and behave well during simulation process. Fig. 9 shows the average global trust value of newcomer attackers in IWOT-V and AATMS after they are added in VANET. We can see that in IWOT-V, the newcomers are allocated much higher initial trust values than that in AATMS. Besides, they gain trust values very fast and are over the average trust value of IWOT-V on round 8. While in AATMS, since we adopt the decay factor, it takes longer time for the newcomers to accumulate a converged trust value. Therefore, our proposed scheme is more robust than IWOT-V against the newcomer attack.

We also evaluate the performance of AATMS and IWOT-V under on-off attack. In the simulation, 20 vehicles are on-off attackers and we simulate a total of 100 rounds, during top 40 rounds on-off attackers behave well to accumulate trust values and suddenly become speeding vehicles during round 40 to 44 (number of simulation rounds starts from 0), then they back to good vehicles again. By setting speed factors greater than 1 and less than 1, we can get bad vehicles and good vehicles. Fig. 10 presents the average global trust

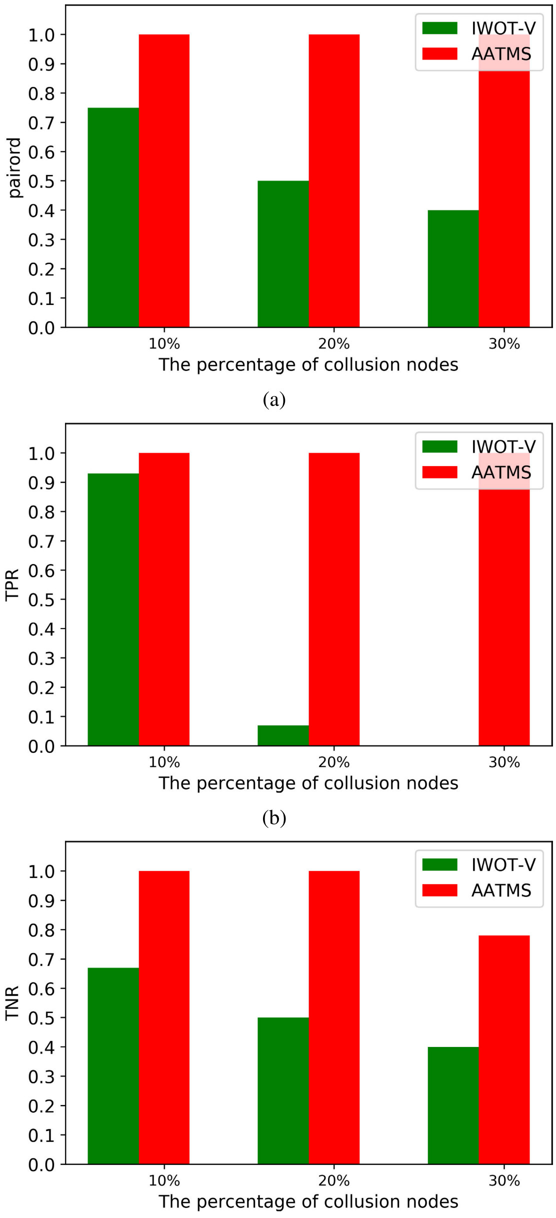


(a)

(b)

FIGURE 11. The average global trust values of good nodes, bad nodes and collusion nodes in IWOT-V and AATMS under different percentage of collusion nodes. (a) IWOT-V. (b) AATMS.

value of the on-off attackers when they accumulate enough trust values after 30 rounds. From the figure, we can find that IWOT-V is more vulnerable to on-off attackers. Since the attackers' trust values just decrease about 0.002 when they launch attack. On the contrary, in AATMS, when on-off attackers build up high trust values and start launching attacks, their forgetting factors are small, resulting in a steep decrease of their trust values. When the attackers stop attack, our proposed scheme still remembers more of the previous performance, therefore it takes longer for them to recover. Even after 55 rounds, on-off attacker's trust values still remain in a low level. It shows that our proposed scheme is very effective in protecting the trust model against on-off attackers.



(a)

(b)

(c)

FIGURE 12. Three metrics of IWOT-V and AATMS under different percentage of collusion attacks. (a) Pairord of IWOT-V and AATMS. (b) TPR of IWOT-V and AATMS. (c) TNR of IWOT-V and AATMS.

Finally, we compare the performance of AATMS and IWOT-V under collusion attack. Collusion attack happens when a group of malicious vehicles corporate together by providing false feedback to other vehicles. In the simulation, collusion attackers always provide good feedback $y = 1$ to their allies regardless of whether their allies' speed exceeding the road speed limit or not, and always provide bad feedback $y = 0$ to other vehicles. We set the percentage of collusion nodes as 10%, 20% and 30% respectively to test the influence on IWOT-V and AATMS. Collusion nodes are also speeding vehicles with speed factors greater than 1. Besides, we fix the number of bad nodes as 20. Fig. 11 shows the average global trust value of good nodes, bad nodes and collusion nodes in IWOT-V and AATMS when the percentage of collusion nodes varies. From Fig. 11(a), we can find that the average global trust value of collusion nodes is higher than that of other nodes in IWOT-V, especially when the percentage of collusion nodes is more than 10%. It means that collusion nodes can accumulate high trust values in IWOT-V even they behave badly. While in AATMS, the average global trust value of collusion nodes is lower than that of good vehicles. Although with the increase of collusion nodes' proportion, the trust value of collusion nodes increases a lot, it is still less than the trust value of good nodes. The trust value of bad

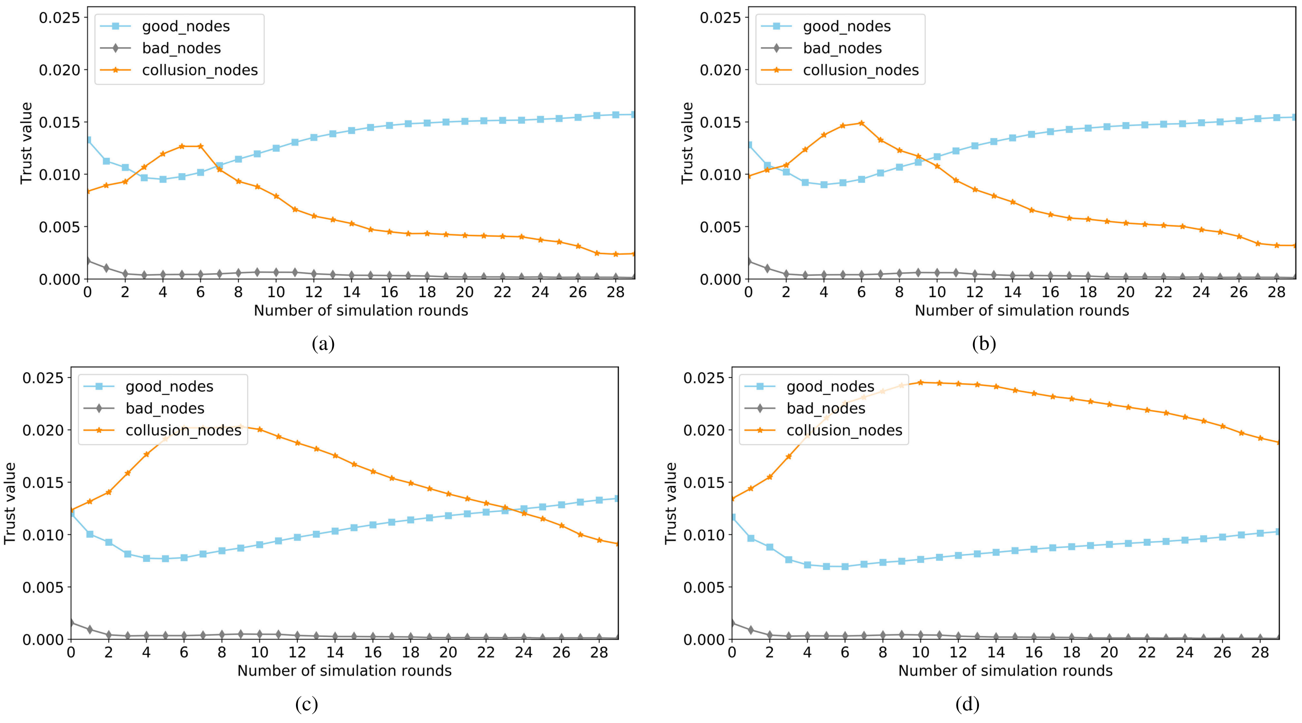


FIGURE 13. Performance of AATMS under different percentage of collusion nodes in seed vehicles. (a) 5% of collusion nodes in seed vehicles. (b) 10% of collusion nodes in seed vehicles. (c) 15% of collusion nodes in seed vehicles.(d) 20% of collusion nodes in seed vehicles.

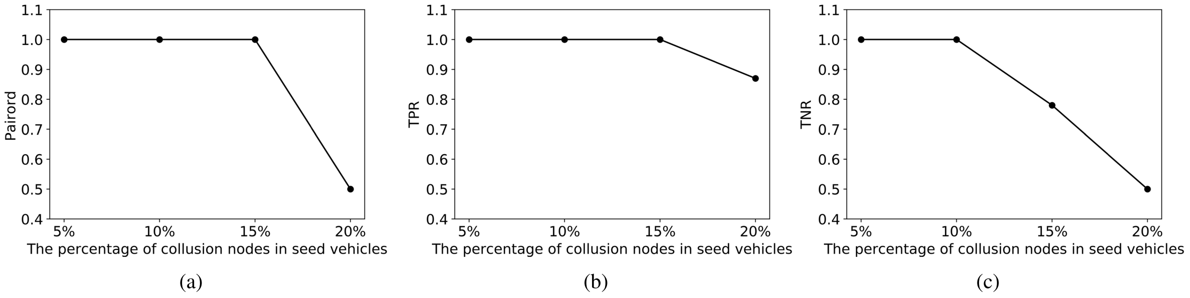


FIGURE 14. Three metrics of AATMS under different percentage of collusion nodes in seed vehicles. (a) Pairord of AATMS. (b) TPR of AATMS. (c) TNR of AATMS.

nodes is close to zero under different percentage of collusion nodes, which means that the percentage of collusion nodes has no influence on bad nodes.

Fig. 12 presents three metrics of IWOT-V and AATMS under different percentage of collusion attacks. Since there is no mechanism in IWOT-V to defense collusion attack, the three metrics of IWOT-V are more and more poor with the increase of collusion nodes' proportion. When there are 30 % of collusion nodes, the pairord of IWOT-V is only 0.4, which means only some bad nodes' trust values are lower than good nodes' trust values. The TPR and TNR of IWOT-V are 0 and 0.4 respectively, which demonstrates that all good nodes are classified as untrustworthy nodes and all collusion nodes are considered as trustworthy nodes. On the contrary, when the percentage of collusion nodes is less than 30%, AATMS can effectively identify collusion nodes, since three metric of AATMS are all equal to 1. When the percentage is 30%, only TPR metric decrease to 0.4. It means that part of collusion nodes are incorrectly classified as trustworthy nodes. The simulation results verify that the AATMS is far more resistant than the IWOT-V when there are collusion attackers in VANET.

The reason why AATMS can effectively defense collusion attack is that we select a set of trustworthy seed vehicles to distribute trust values to other vehicles. Considering the situation that some collusion nodes may passing through the filtering of social factors and become seed vehicles, we set the percentage of collusion nodes in seed vehicles as 5%, 10%, 15% and 20 % respectively to test the influence on our proposed scheme. In the simulation, we set the number of collusion nodes as 20. Fig.13 shows the simulation results. As we can see, when the percentage is less than 10%, our proposed scheme can also effectively identify collusion nodes and assign lower trust values to them. When the percentage becomes 15%, although the trust values of collusion nodes are much higher than that of good vehicles in earlier rounds, they drop quickly from 10^{th} round and are lower than that of good nodes after 30 rounds. However, when the percentage is 20%, the collusion nodes accumulate the most trust values and even good vehicles' trust values are lower than them, which means the collusion nodes damage our proposed trust management scheme totally. The three metrics of AATMS under different percentage of collusion nodes in seed vehicles is shown in Fig. 14. We can find that AATMS can effectively defense collusion attack when the percentage of collusion nodes in the set of seed vehicles is below 10%.

VI. CONCLUSION

In this paper, we present an anti-attack trust management scheme called AATMS to evaluate trustworthiness of vehicles in VANET. Our proposed scheme adopts Bayesian inference to calculate local trust values of vehicles. Then we design a TrustRank based algorithm to calculate global trust values. Social trust of vehicles from real life is introduced to select seed vehicles, which is helpful for defensing collusion attack. We also adopt a decay factor and a forgetting factor to resist newcomer attack and on-off attack. The effective and robustness of our trust management scheme are demonstrated through simulations. The results show that our proposed scheme can effectively recognize trustworthy and untrustworthy vehicles even under malicious attacks.

In the future, other link analysis algorithms will be considered to evaluate the global trust of vehicles in VANET.

REFERENCES

[1] C. A. Kerrache, C. T. Calafate, J.-C. Cano, N. Lagraa, and P. Manzoni, "Trust management for vehicular networks: An adversary-oriented overview," *IEEE Access*, vol. 4, pp. 9293–9307, 2016.

[2] 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, Jan. 2014.

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

[4] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "VANET security surveys," *Comput. Commun.*, vol. 44, pp. 1–13, May 2014.

[5] K. P. Laberteaux, J. J. Haas, and Y.-C. Hu, "Security certificate revocation list distribution for VANET," in *Proc. 5th ACM Int. Workshop Veh. Inter-NETworking (VANET)*, 2008, pp. 88–89.

[6] J. Guo, J. P. Baugh, and S. Wang, "A group signature based secure and privacy-preserving vehicular communication framework," in *Proc. Mobile Netw. Veh. Environ.*, May 2007, pp. 103–108.

[7] A. Wasef, R. Lu, X. Lin, and X. Shen, "Complementing public key infrastructure to secure vehicular ad hoc networks [security and privacy in emerging wireless networks]," *IEEE Wireless Commun.*, vol. 17, no. 5, pp. 22–28, Oct. 2010.

[8] M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized trust management," in *Proc. IEEE Symp. Secur. Privacy*, Dec. 2002, pp. 164–173.

[9] S. Tan, X. Li, and Q. Dong, "A trust management system for securing data plane of ad-hoc networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 9, pp. 7579–7592, Sep. 2016.

[10] S. A. Soleymani, A. H. Abdullah, M. Zareei, M. H. Anisi, C. Vargas-Rosales, M. Khurram Khan, and S. Goudarzi, "A secure trust model based on fuzzy logic in vehicular ad hoc networks with fog computing," *IEEE Access*, vol. 5, pp. 15619–15629, 2017.

[11] W. Li and H. Song, "ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 4, pp. 960–969, Apr. 2016.

[12] H. Xia, S.-S. Zhang, Y. Li, Z.-K. Pan, X. Peng, and X.-Z. Cheng, "An attack-resistant trust inference model for securing routing in vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 68, no. 7, pp. 7108–7120, Jul. 2019.

[13] H. Hu, R. Lu, Z. Zhang, and J. Shao, "REPLACE: A reliable trust-based platoon service recommendation scheme in VANET," *IEEE Trans. Veh. Technol.*, vol. 66, no. 2, pp. 1786–1797, Feb. 2017.

[14] B. Lin, X. Chen, and L. Wang, "A cloud-based trust evaluation scheme using a vehicular social network environment," in *Proc. 24th Asia–Pacific Softw. Eng. Conf. (APSEC)*, Dec. 2017, pp. 120–129.

[15] Y. Xiao and Y. Liu, "BayesTrust and VehicleRank: Constructing an implicit Web of trust in VANET," *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2850–2864, Mar. 2019.

[16] L. Page, S. Brin, R. Motwani, and T. Winograd, "The PageRank citation ranking: Bringing order to the Web," Stanford Univ., Stanford, CA, USA, Tech. Rep., 1998.

[17] Z. Gyöngyi, H. Garcia-Molina, and J. Pedersen, "Combating Web spam with trustrank," in *Proc. 30th Int. Conf. Very Large Data Bases*, vol. 30, 2004, pp. 576–587.

[18] C. Sommer, R. German, and F. Dressler, "Bidirectionally coupled network and road traffic simulation for improved IVC analysis," *IEEE Trans. Mobile Comput.*, vol. 10, no. 1, pp. 3–15, Jan. 2011.

[19] C. A. Kerrache, N. Lagraa, C. T. Calafate, and A. Lakas, "TFDD: A trust-based framework for reliable data delivery and DoS defense in VANETs," *Veh. Commun.*, vol. 9, pp. 254–267, Jul. 2017.

[20] C. A. Kerrache, N. Lagraa, A. Benslimane, C. T. Calafate, and J.-C. Cano, "On the human factor consideration for VANETs security based on social networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2018, pp. 1–6.

[21] E. Barka, C. A. Kerrache, H. Benkraouda, K. Shuaib, F. Ahmad, and F. Kurugollu, "Towards a trusted unmanned aerial system using blockchain for the protection of critical infrastructure," *Trans. Emerg. Telecommun. Technol.*, 2019, Art. no. e3706, doi: 10.1002/ett.3706.

[22] 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, Feb. 2019.

[23] 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, pp. 380–392, Jan. 2014.

[24] C. J. Fung, J. Zhang, I. Aib, and R. Boutaba, "Dirichlet-based trust management for effective collaborative intrusion detection networks," *IEEE Trans. Netw. Service Manag.*, vol. 8, no. 2, pp. 79–91, Jun. 2011.

[25] J. Zhang, "A Survey on Trust Management for VANETs," in *Proc. IEEE Int. Conf. Adv. Inf. Netw. Appl.*, Mar. 2011, pp. 105–112.

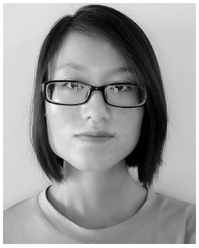
[26] A. Varga, "Discrete event simulation system," in *Proc. Eur. Simulation Multiconf. (ESM)*, 2001, pp. 1–7.

[27] D. Krajzewicz, J. Erdmann, M. Behrisch, and L. Bieker, "Recent development and applications of SUMO-Simulation of Urban MObility," *Int. J. Adv. Syst. Meas.*, vol. 5, no. 3, pp. 128–138, 2012.

[28] M. Haklay and P. Weber, "OpenStreetMap: User-generated street maps," *IEEE Pervas. Comput.*, vol. 7, no. 4, pp. 12–18, Oct. 2008.

[29] M. Raifer, *Overpass Turbo*, vol. 3. Overpass API, 2018. [Online]. Available: http://overpass-turbo.eu/

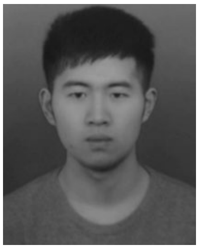
[30] S. Krauss, P. Wagner, and C. Gawron, "Metastable states in a microscopic model of traffic flow," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 55, no. 5, pp. 5597–5602, Jul. 2002.



JINSONG ZHANG received the B.S. degree from the School of Information Engineering, Communication University of China. She is currently pursuing the master's degree with the Department of Computer Science and Technology, Beijing University of Posts and Telecommunications. Her research interests include trust management for vehicular networks.

KANGFENG ZHENG received the Ph.D. degree from the Beijing University of Posts and Telecommunications, in 2006. He is currently a Professor with the Information Security Center, School of Cyberspace Security, Beijing University of Posts and Telecommunications. He has published over 50 technical articles in international conferences and journals. His research interests include networking and system security, network information processing, and network coding. He has presided over a number of national scientific research projects and received a number of national and provincial awards.

DONGMEI ZHANG received the Ph.D. degree from the Beijing University of Posts and Telecommunications, in 2007. She is currently an Associate Professor with the Network Technology Center, School of Computer Science, Beijing University of Posts and Telecommunications. Her research interests include the Internet Technology, Internet of Things Technology, and Internet of Things Security. She has published over 30 technical articles in international conferences and journals. She has presided over and participated in a number of national scientific research projects.



BO YAN received the B.S. degree from the Department of Computer Science and Technology, Hanzhou Dianzi University, China. He is currently pursuing the master's degree with the Department of Computer Science and Technology, Beijing University of Posts and Telecommunications, China. His research interests are information extraction, knowledge graph, and transfer learning.