Intrusion Detection Scheme for Autonomous Driving Vehicles

Weidong Zhai and Zhou Su(✉)

School of Cyber Science and Engineering, Xi'an Jiaotong University, Xi'an, China
384914432@qq.com, zhousu@ieee.org

Abstract. With the recent breakthroughs, autonomous driving vehicles (ADVs) are promising to bring transformative changes to our transportation systems. However, recent hacks have demonstrated numerous vulnerabilities in these emerging systems from software to control. Safety is becoming one of the major barriers for the wider adoption of ADVs. ADVs connect to vehicular ad-hoc networks (VANETs) to communicate with each other. However, malicious nodes can falsify information and threaten the safety of passengers and other vehicles with catastrophic consequences. In this work, we present a novel reputation-based intrusion detection scheme to detect malicious ADVs through dynamic credit and reputation evaluation. To further encourage user's participation, an incentive mechanism is also built for ADVs in the intrusion detection system. We demonstrate the feasibility and effectiveness of our proposed system through extensive simulation, compared with current representative approaches. Simulation results show that our proposed scheme can acquire better intrusion detection results, reduced false positive ratio, and improved user participation.

Keywords: Autonomous driving vehicles · Credit · Dynamic threshold · Intrusion detection · Incentive model

1 Introduction

With the rapid development of the automobile industry, many believe that autonomous driving vehicles (ADVs) will bring transformative changes to our society. As a networked cyber-physical system, ADVs will greatly improve the current traffic environment and bring convenience to people's travel. A number of leading carmakers, including Toyota and Volkswagen, have announced their plain to commercialize self-driving cars to the general public in the next five years. As reported in [1], 25% of the vehicles on the road will be ADVs by 2035.

ADVs communicate with each other through vehicular ad-hoc network (VANET), which can be broadly considered as a mobile ad-hoc network on the road tailored for automobiles [2]. For example, ADVs can share information about current road conditions to help others plan their routes. Apart from vehicle-to-vehicle communication, ADVs can also communicate with Roadside

S. Yu et al. (Eds.): SPDE 2020, CCIS 1268, pp. 278–291, 2020.
https://doi.org/10.1007/978-981-15-9129-7_20

Units (RSUs) to obtain desired information. All transmitted data which ADVs rely heavily on for safe driving should be protected by the security mechanisms [3]. Existing security approached mainly focus on cryptographic mechanisms. Although cryptographic mechanisms can protect the confidentiality and integrity of data, they cannot cope with the insider attackers well. When there are malicious nodes inside the VANET, they can manipulate data and connection to sabotage the network. For example, some ADVs will release a lot of false news (such as traffic accidents, road congestion, etc.), and these false news may cause chaotic traffic and accidents [4]. Besides, there are many new attack surfaces in the VANET, such as selfish attack, black hole attack, sybil attack and so on [5].

To cope with these issues, Intrusion Detection System (IDS) has been a primary instrument to detect the presence of attackers for many organizations and governments during the past decade. Existing works on leveraging IDS to augment communication security often attempts to address denial of service (DOS) external network [6] and unauthorized access from remote machine (R2L), while internal attacks are not handled well. In [7], the detection is based on voting among randomly selected clusters. This approach makes a strong assumption that cluster head can be trusted, and this is often not true when under attack.

In this paper, distinguished from the current paradigm, we explore mechanisms to incentivize mutual inspection among the peers in the VANET. ADVs can accumulate credits by contributing community-vetted information to the network, and falsified information can be detected using a jointly computed SVM among all the peers. More specifically, we first let ADVs evaluate neighboring vehicles' behaviors and filter these evaluation value, and then derive the credit value of each vehicle. Next, we established the intrusion detection mechanism by calculating the dynamic threshold and setting rules based on SVM. In order to encourage ADVs to take part in network activities, we develop an incentive model based on bargaining game. We conduct extensive experiments and simulations to demonstrate the feasibility and efficiency of our scheme by comparing with the conventional intrusion detection schemes in VANETs.

The structure of this paper is organized as follows. In the second part, we review the related work. The third part provides the system model for VANET, and the forth part describes the intrusion detection scheme. The fifth part shows our incentive model. In order to demonstrate the effectiveness of our scheme, the sixth part shows our simulation results. In the last part, we conclude the paper.

2 Related Work

In this section, we briefly review the researches on security of VANET, including IDS and the credibility mechanism. IDS is one of the most reliable methods to protect VANET from being attacked [8]. The research on external attacks has been relatively mature, so the recent work mainly focuses on how to deal with attacks launched by internal malicious nodes in VANET. Zhang *et al.* [9] present a cluster-based intrusion detection method. It no longer requires each node to conduct monitoring, but chooses a cluster head among a group of nodes to be an

intrusion detection agent. The agent carries out detection by collecting information in real time. Amiri *et al.* [10] combines neural network and clustering algorithm to propose a multi-agent-based intrusion detection method, which greatly saves energy consumption in the VANET. Bismeyer *et al.* [11] introduces an IDS based on the ideas of existing position and movement verification approaches. Their schemes are effective against the fake congestion attack and the denial of congestion attack. In [12,13], the authors propose IDS based on rule matching to detect malicious vehicles. Although they have high detection rate, they can only detect specified attacks and ignore other unknown attacks. However, this is different from our approach which is extensible in attack scenarios.

There are increasing security schemes of VANET using the credibility mechanism. Initial credibility schemes were deployed based on centralized or decentralized infrastructure, such as [14,15], but this approach proved difficult to adapt to the rapidly changing nature of VANET. Xu *et al.* [16] present a credit evaluation scheme consisting of direct evaluation and indirect evaluation, which is used to evaluate the reliability of edge nodes in mobile social networks. Hu *et al.* [17] propose a recommendation scheme for a group of vehicles, that is, a node with high credibility is voted on each group as the cluster head. The head node evaluates group's credibility based on feedback back from other vehicles in the group. These schemes will undoubtedly result in substantial resource savings. However, some selfish nodes in the network have not been well handled, and these vehicles will not have the enthusiasm to share and forward information to save their own network resources.

3 System Model

3.1 Traffic Model

In our work, the entire traffic model is composed of the Credit Center, RSUs and ADVs. The RSUs are scattered on both sides of the road. ADVs travels on the road, and each car will pass at least one RSU signal coverage. We assume that the width of each road in the entire traffic is the same.

According to Little's Law, which states that the long-term average number of customers is equal to the long-term effective arrival rate multiplied by the average waiting time of customers in this stable system, the traffic flow μ of each RSU (the number of ADVs arriving per unit time) can be calculated as

$$\mu = \frac{\bar{C}}{\bar{t}}, \tag{1}$$

where $\bar{C}$ is the average number of ADVs covered by a RSU, and $\bar{t}$ is the average time that takes a car to travel this distance. We have

$$\bar{t} = \frac{l}{\bar{v}}, \tag{2}$$

where l is the length of the road covered by the RSU and $\bar{v}$ is the average speed of the ADV. Therefore, the traffic flow can be expressed as:

$$\mu = \frac{\bar{C}}{l} \times \bar{v}. \tag{3}$$

$\bar{v}$ is affected by the degree of traffic congestion, which can be expressed as

$$\bar{v} = \max\left\{v_{\max} \times \left(1 - \frac{\bar{C}}{C_{\max}}\right), v_{\min}\right\}. \tag{4}$$

According to [18], in free and steady-state traffic flow, the speed of vehicles follows a normal distribution, that is

$$f(v) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\left(\frac{v-\bar{v}}{\sigma\sqrt{2}}\right)^2}, \tag{5}$$

where $\sigma = \alpha\bar{v}$, and $v_{\min} = \bar{v} - \beta\sigma$. (α, β) is determined according to the constantly changing traffic conditions on the road section. In order to guarantee $v_{\min} \leq v \leq v_{\max}$, we need to find a truncated normal distribution of v. It can be formulated as

$$f(v, \bar{v}, \sigma, v_{\min}, v_{\max}) = \frac{2f(v)}{erf\left(\frac{v_{\max}-\bar{v}}{\sigma\sqrt{2}}\right) - erf\left(\frac{v_{\min}-\bar{v}}{\sigma\sqrt{2}}\right)}, \tag{6}$$

and

$$erf(x) = \sqrt{\frac{2}{\pi}} \int_0^x e^{-\eta^2} d\eta. \tag{7}$$

3.2 Attack Model

Selfish Attack. Selfish attack refers to that some ADVs in VANET don't respond to the communication request of other nodes in order to save its network resources and storage space, or intentionally discards the packets that other nodes wish to forward, so that some important information in the network cannot be conveyed. It is conceivable that if there is an accident on a road, and the message cannot be transmitted because of the selfish attack, it will lead to traffic congestion and even more serious accidents. The packet loss rate of these nodes is usually much higher than that of nearby nodes.

On-Off Attack. Malicious ADVs in the network behave normally from time to time and carry out some attacks. Such nodes usually use a certain period of normal performance to accumulate the credit of other nodes, and then launch malicious attacks to consume this value. But they always keep themselves in the trusted range to ensure that they will not be excluded the network.

Hostile Attack. It mainly includes data packet replication and resource exhaustion attacks. Their common feature is that malicious nodes will send a large number of unwanted data packets to overload the network and waste bandwidth. Therefore, when a malicious vehicle performs such an attack, its message replication rate or packet transmission rate will be higher, respectively.

4 Intrusion Detection Scheme

4.1 Global Credit Model

Firstly, we need to calculate the direct trust value between the ADVs. After each ADV interacts with another ADV, it needs to evaluate the satisfaction of the other. We define the satisfaction of ADV i to ADV j at the k-th interaction as

$$S_{i,j}^{k} = \begin{cases} 0, dissatisfaction \\ 1, satisfaction \\ t \in (0,1), \ otherwise \end{cases}. \tag{8}$$

ADV i will calculate the direct trust to ADV j in combination with the satisfaction obtained from previous interactions, and as the time goes by, the proportion of satisfaction in past periods should be reduced. The time decay function is defined as follows

$$h_k = e^{\xi(k-K)}, \xi > 0, h_k \in (0,1], \tag{9}$$

where K is the total number of evaluations, and ξ is the adjustment parameter. The evaluation value of ADV i to ADV j can be expressed as

$$DT_{i,j} = \frac{\sum_{k=1}^{K} S_{i,j}^{k} h_k}{\sum_{k=1}^{K} h_k}. \tag{10}$$

According to [19], ADVs that continuously provided low-quality information should be penalized. The penalty function can be shown as

$$P_{i,j} = \delta \left(\sum_{k=1}^{k} h_k - DT_{i,j} \right). \tag{11}$$

Therefore, the direct trust value that ADV i evaluates ADV j can be obtained by

$$ET_{i,j} = \frac{DT_{i,j}}{DT_{i,j} + P_{i,j}}. \tag{12}$$

Then, we will calculate the global credit of ADVs. ADVs should periodically send RSU its own collection of direct trust values about other ADVs. The RSU will send credit center these data to calculate the global credit. The direct trust values of all ADVs for ADV i can be regarded as a set of variables with independent and identical distribution, so this set of values satisfies the central limit theorem, and we denote it as $ET_i = \{ET_{1,i}, ET_{2,i}, ..., ET_{k,i}, ..., ET_{n,i}\}$. We have

$$\mu_i = E\left(ET_{i,j}\right) = \frac{1}{n-1} \sum_{k=1, k \neq i}^{n} ET_{k,i}, \tag{13}$$

$$\sigma_i = \sqrt{D\left(ET_{i,j}\right)} = \sqrt{\frac{1}{n-1}\sum_{k=1,k\neq i}^{n}\left(ET_{k,i}-\mu_i\right)^2}, \tag{14}$$

where μ_i is the mathematical expectation of the set of values, and σ_i is the standard deviation. We use these two parameters to filter this set of values so that it satisfies $ET_{k,i} \in [\mu_i - \varepsilon\sigma_i, \mu_i + \varepsilon\sigma_i]$, where ε is the regulator, and its size is positively correlated with σ_i.

The behavior of node i in the most recent period can be quantified as

$$\bar{\mu}_i = \frac{1}{m}\sum_{k\in S} ET_{k,i}, \tag{15}$$

where S is the set of direct trust values satisfying the condition and m is the number of elements in the set. Combined with past credit values, the global credit value of the i-th period can be calculated by

$$T_{i,n} = T_{i,n-1} + \frac{\bar{\mu}_i - T_{i,n-1}}{\left|\bar{\mu}_i - T_{i,n-1}\right|}\theta. \tag{16}$$

4.2 Dynamic Credit Threshold

When a vehicle's credit value falls below a threshold, it is marked as a malicious node. The traditional credit scheme gives a fixed threshold to determine, which results in on-off attack. In order to accurately identify malicious nodes in the process of frequent credit changes, we propose to set a dynamic global credibility threshold.

We use $\mathcal{T} = \{T_1, T_2, ..., T_k, ..., T_n\}$ to represent the current credit of all ADVs. Assuming that $T_1 < T_2 < ... < T_k < ... < T_n$, we have

$$\widehat{T} = (1-p)\left(T_1 + T_2 + ... + T_k + ... + T_n\right), \tag{17}$$

where p is the proportion of normal nodes in the VANET. According to [20], it is easy to prove that there must be a value T_k in the set $\mathcal{T}$ that satisfies

$$\begin{cases} T_1 + T_2 + ... + T_{k-1} < \widehat{T} \\ T_1 + T_2 + ... + T_{k-1} + T_k \geq \widehat{T} \end{cases}. \tag{18}$$

Then, the critical value to judge the credit state of ADVs in the n-th cycle can be expressed as $S_n = T_n$. Finally, considering the critical value calculated in the previous period and combining with the time attenuation function, we calculated the threshold value of credit detection in the current vehicle network as

$$S = \frac{\sum_{k=0}^{n} S_k \times h_k}{\sum_{k=0}^{n} h_k}. \tag{19}$$

Only the ADV with credit value above S are considered to be trustworthy and thus able to participate in network activities normally.

4.3 Intrusion Detection

Combined with the credibility model designed above, this section proposes an scheme to identify malicious nodes in VANET. ADVs on the road are required to monitor the network attributes of their neighbors and calculate related monitoring indicators, including packet loss rate (PLR), packet transmission rate (PTR), and message repetition rate (MRR) during this period [7]. Each node needs to determine whether its neighbors are malicious according to the following rules:

- If $PLR > TH_1$, it is marked as the malicious node that launched the Selfish Attack.
- If $PTR > TH_2$, and the value is significantly higher than others, We tagged it as the malicious node that launched the Resource Depletion Attack.
- If $MRR > TH_3$, this ADV should be marked as the malicious node which launched the Packet Replication Attack.

Here, TH_1, TH_2, TH_3 are thresholds set in advance.

In addition to the rule-based judgment method mentioned above, the ADVs also need to incorporate a detection method based on machine learning. We use the Support Vector Machine (SVM) algorithm. Compared with other traditional machine learning methods, such as neural networks, SVM's training time is shorter, and it occupies less memory. We only need to save the support vector. The algorithm includes training and classification processes.

During the training process, the ADVs will continuously collect the network features (PLR, PTR, MRR) of its nearby nodes, and then use these features as the input vector of the training algorithm. The purpose of training is to calculate a set of feature values called support vectors. This set of vectors allows the data to be separated into two sides, namely normal and abnormal (binary classification). The detailed content of the algorithm is not repeated in this solution.

In the classification process, each vehicle node will make abnormal judgments on the newly collected data according to the training model. If a vehicle is judged as a malicious node, it will be recorded. Subsequently, the monitoring node will make the final decision according to the following rules:

- If both the SVM and the rule-based judgment method determine that the ADV is a malicious node, the monitoring node should send an intrusion report to the nearby RSU, including its network characteristics and ID, and update the experience trust for the malicious node according to the penalty function in the experience trust.
- If the SVM determines that the ADV is a malicious node, and the rule determines that the node is a normal node, then the rule needs to be updated, and its threshold (PLR, PTR, MRR) is replaced by the current features (such as support vectors) provided by the SVM.

The ADVs must perform anomaly detection on their current neighbor nodes and send monitoring reports to nearby RSUs. When a ADV is suspected of being a malicious node, the RSU needs to make a decision based on the credit values

of the judgment nodes. Suppose RSU receives an intrusion report about node i, let $\mathcal{M} = \{1, 2, ..., m, ..., M\}$ denote the set of vehicles in neighboring nodes that consider i to be a malicious node, and $\mathcal{N} = \{1, 2, ..., n, ..., N\}$ denote the set of vehicles that consider i to be a normal node. Then, We calculate the judgement value as:

$$C_i = \frac{\sum_{m \in \mathcal{M}} (\max T_m \times T_m) - \sum_{n \in \mathcal{N}} (\max T_n \times T_n)}{\sum_{m \in \mathcal{M}} T_m + \sum_{n \in \mathcal{N}} T_n}. \tag{20}$$

We compare C_i to the predefined threshold A. If $C_i > A$, we consider node i as a malicious node and reduce its credibility to an untrusted state.

5 Incentive Model

The Credit Center needs to increase ADVs' credit value based on their activity level. Let the activity level of ADV i in k-th cycle be a_i^k and $a_i^k \in$[0,I]. I is the highest activity level. The formula for calculating the credit rewards is

$$R_i\left(a_i^k\right) = \frac{a_i^k \left(1 - \widehat{T}_i^{k-1}\right)\theta}{I+1}, \tag{21}$$

where θ is the weight parameter. $\widehat{T}_i^{k-1}$ is the new credit value in the $(k-1)$-th cycle, and it can be updated by

$$\widehat{T}_i^k = \begin{cases} T_i \quad k = 0, \\ T_i^{k-1} + R_i \quad \widehat{T}_i^k < 1, \\ 1 \quad other, \end{cases}. \tag{22}$$

We regard the credit center as the buyer A, and R_i is the highest price the buyer is willing to pay.

According to the activity level, we quantified the resource consumption of ADV i. It can be expressed by

$$E_i\left(a_i^k\right) = \psi \log_2 \left(1 + e^{1 - \frac{I+1}{a_i^k}}\right), \tag{23}$$

where ψ is the weight parameter. We regard ADV i as the seller B, and E_i is the lowest price that seller can accept.

Depending on the reward value and the amount of resource consumption, we consider the following three cases:

- $R_i < E_i$: This situation means that the highest price offered by the buyer is lower than the lowest price acceptable to the seller, so the transaction fails, and the vehicle will be unwilling to remain active and participate in activities on the network.
- $R_i = E_i$: In this case, we default to normal transaction.

– $R_i > E_i$: This means that the highest price offered by the buyer is higher than the lowest price accepted by the seller, that is, the two parties have not reached a consensus on the transaction price. Due to the selfishness of the two parties in the game, the seller will pursue the maximization of benefits, while the buyer wants to reduce the payment.

Let's just consider the case of $R_i > E_i$. We use the bargaining game to solve the optimal transaction price. The cake C can be denoted by

$$C = R_i\left(a_i^k\right) - E_i\left(a_i^k\right). \tag{24}$$

Let χ_A and χ_B be the return functions of A and B, respectively, we have

$$\chi_A\left(\gamma_A\right) = \gamma_A C, \chi_B\left(\gamma_B\right) = \gamma_B C, \tag{25}$$

$$\gamma_A + \gamma_B = 1, \gamma_A \geq 0, \gamma_B \geq 0. \tag{26}$$

The bargaining model is a process in which two parties take turns to make offers until one party's allocation is accepted by the other. Each round of bidding will have a certain cost for both parties, that is, both parties have their own patience value, which we will call the discounted value here. Considering the relationship between the discounted values of A and B and the activity of the other, according to [21], we can define the discounter value of A is

$$\delta_A = 1 - \frac{e^{v\theta} - e^{-v\theta}}{e^{v\theta} + e^{-v\theta}}, \theta = \frac{I-1}{a_i}, \tag{27}$$

and the discounter value of B is

$$\delta_B = \frac{e^{v\theta'} - e^{-v\theta'}}{e^{v\theta'} + e^{-v\theta'}}, \theta' = \frac{I}{a_i}. \tag{28}$$

So, we can get the sub-game Nash equilibrium of the game

$$\gamma_A^* = \frac{1-\delta_B}{1-\delta_A\delta_B}, \gamma_B^* = \frac{\delta_B - \delta_A\delta_B}{1-\delta_A\delta_B}. \tag{29}$$

At this point, we can get the transaction price of both parties in the case which can be formulized by

$$R_i^* = E_i + \frac{1-\delta_B}{1-\delta_A\delta_B} C \tag{30}$$

6 Simulation Experiment

In this section, we present relevant simulation setup and results of the proposed scheme.

6.1 Setup

We use Network Simulator version 2 (NS2) combined with Simulation of Urban Mobility (SUMO) to carry out the simulation experiment of the proposed scheme. NS2 is an object-oriented network simulator, which provides various protocols and programming interfaces for researchers to use. SUMO is a traffic system simulation software that can realize microscopic control of traffic flow, including specifying the number, speed, behavior of vehicles and setting the type and conditions of roads. In the experiment, SUMO generates tracking files for the movement of ADVs, and NS2 loads these files and runs the intrusion detection scheme we propose.

Table 1. The main parameters of the traffic model.

Parameter name	Value
Number of ADVs	100
Simulation area	5 km^2
Maximum speed	80 km/h
Wireless communication protocol	802.11p
Transmission range	500 m
Simulation time	2 min
Detection period	10 s
μ	50
C_i	0.8
TH_1, TH_2, TH_3	0.85

Table 1 summarizes the main parameters of the simulation. To facilitate the experiment, we initialize the global credit value of each ADV according to normal distribution, and the value is between 80 and 100. We consider two metrics to verify the practicability of our intrusion detection scheme, including detection ratio (DR) and false positive ratio (FPR). The DR means the percentage of the number of correctly identified malicious nodes in the experiment, and the FPR refers to the percentage of the number of malicious nodes misreported in the experiment to the number of normal nodes. We set the DR of both schemes to be 100 when the malicious nodes in the network do not exist, and FPR to be 0 when the normal nodes do not exist.

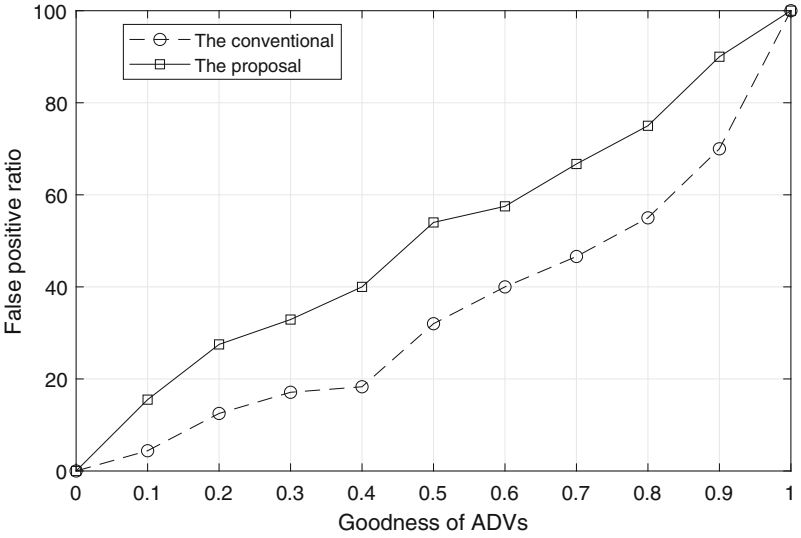

Fig. 1. Comparison of success rate of intrusion detection under different ratio of trusted ADV.

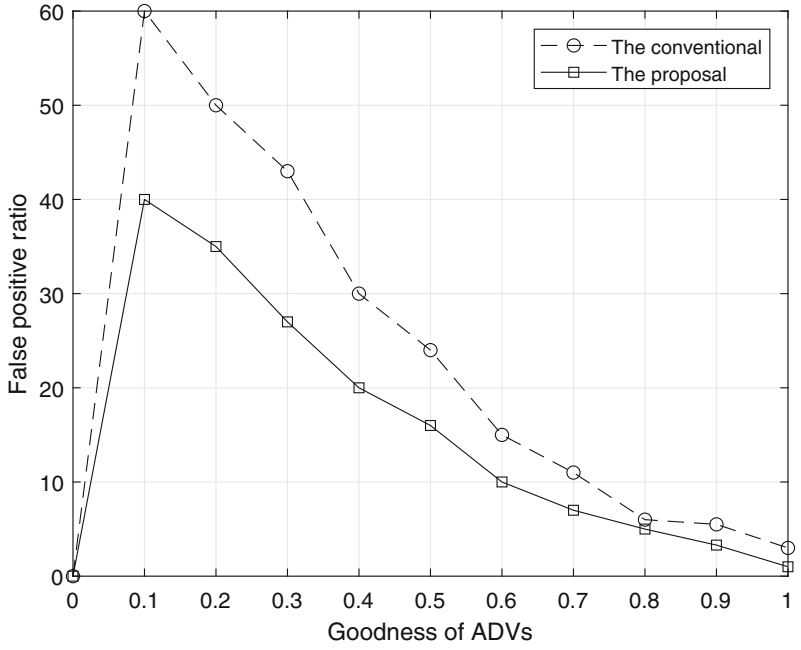

Fig. 2. Comparison of false positive ratio of intrusion detection under different ratio of trusted ADV.

6.2 Results

We compare the proposed detection scheme with the conventional neural network. Figure 1 shows the comparison of the success rates of intrusion detection of the two schemes under different trusted ADV ratios. It can be seen that the effect of the proposed scheme in this paper is significantly better than that of neural network. This is because the rule setting in the scheme of this paper adds a comparison with the network attributes of surrounding nodes. The topological structure of the vehicle-mounted network changes frequently. When the ADVs' density of some road sections is large, the relevant indicators generated by it will increase or decrease significantly. The neural network cannot adapt well to this scenario. Figure 2 shows that the FPR of our scheme is lower than that of the traditional scheme. When the number of trusted ADVs in the network is lower, the FPR is obviously higher. This is because the collusion attack launched by a large number of malicious nodes will greatly affect the evaluation of normal ADVs' credit values. Although such a situation is rarely encountered in future reality, it cannot be ignored.

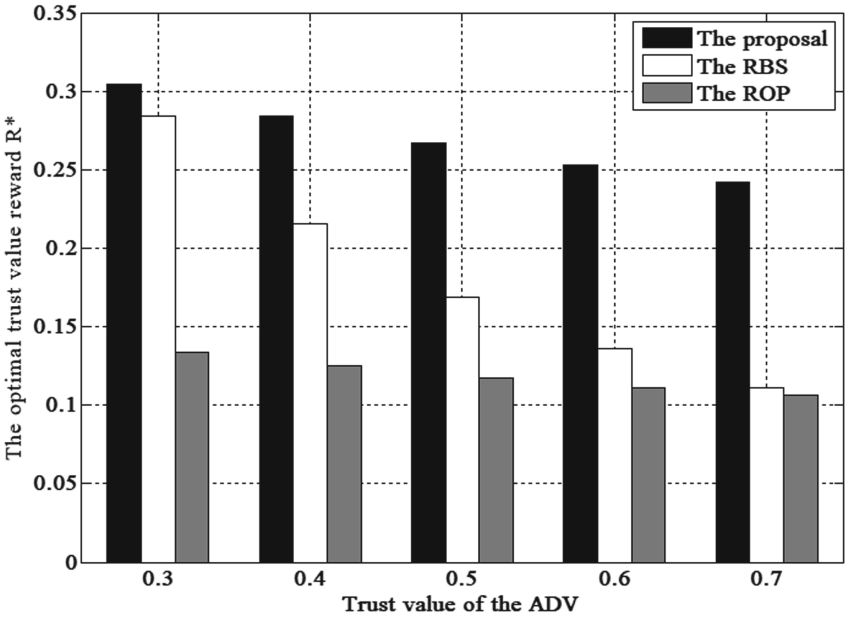

Fig. 3. The optimal credibility reward obtained by ADV with different trust value in the two-round game

In addition, we also simulate the incentive model in the scheme. Figure 3 shows the optimal trust value rewards given by our scheme under different trust value. As it is shown that ADVs with less trust value can get the better rewards, which can motivate it to behave more positively. We considered two

traditional schemes for comparison, i.e., Reputation-Based Scheme (RBS) and Random Offer Price (ROP). In the RBS, the quotes of buyer and seller are only related to their credibility, and the reward value decreases too much with the increase of trust value, which will cause the ADVs with high credit degree lose the motivation to keep active. In the ROP, the buyer and seller quote at random, and the reward value is too low to encourage ADVs to participate in the VANET activities. In contrast, our scheme can give different ADVs appropriate incentive values to ensure the stability of the VANET.

7 Conclusion

In this paper, we have proposed an intrusion detection scheme based on the credit of ADVs and SVM. The credit value of each ADV is calculated by their assessment and center limit theorem. Based on the credit values, we have presented a method to calculate the dynamic credibility threshold which forms the basis for an intrusion detection scheme by combining the SVM algorithm. Furthermore, we have proposed an incentive model to encourage users to actively participate in network activities. The simulation results have shown that the proposed scheme have a higher detection rate than the conventional scheme.

References

1. Bierstedt, J., Gooze, A., Gray, C., Raykin, L., Walters, J.: Effects of next-generation vehicles on travel demand and highway capacity. FP Think Working Group **2**, 11 (2014)
2. Guo, J., Zhang, Y., Chen, X., Yousefi, S., Guo, C., Wang, Y.: Spatial stochastic vehicle traffic modeling for VANETs. IEEE Trans. Intell. Transp. Syst. **19**(2), 416–425 (2018)
3. Tangade, S., Manvi, S.S., Lorenz, P.: Trust management scheme based on hybrid cryptography for secure communications in VANETs. IEEE Trans. Veh. Technol. **69**(5), 5232–5243 (2020)
4. Singh, P.K., Singh, R., Nandi, S.K., Ghafoor, K.Z., Rawat, D.B., Nandi, S.: Blockchain-based adaptive trust management in internet of vehicles using smart contract. IEEE Trans. Intell. Transp. Syst. (2020)
5. Kumar, M., Jain, V., Jain, A., Bisht, U.S., Gupta, N.: Evaluation of black hole attack with avoidance scheme using aodv protocol in vanet. J. Discrete Math. Sci. Cryptogr. **22**(2), 277–291 (2019)
6. Anand, S. J. V., Pranav, I., Neetish, M., Narayanan, J.: Network intrusion detection using improved genetic k-means algorithm. In: 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 2441–2446, Bangalore (2018). https://doi.org/10.1109/ICACCI.2018.8554710
7. Sedjelmaci, H., Senouci, S. M.: A new intrusion detection framework for vehicular networks. In: IEEE International Conference on Communications (ICC), Sydney, NSW, pp. 538–543 (2014). https://doi.org/10.1109/ICC.2014.6883374
8. Sedjelmaci, H., Senouci, S.M., Feham, M.: An efficient intrusion detection framework in cluster-based wireless sensor networks. Secur. Commun. Netw. **6**(10), 1211–1224 (2013)

9. Zhang, Y., Lee, W., Huang, Y.A.: Intrusion detection techniques for mobile wireless networks. Wireless Netw. **9**(5), 545–556 (2003)
10. Amiri, E., Keshavarz, H., Heidari, H., Mohamadi, E., Moradzadeh, H.: Intrusion detection systems in MANET: a review. In: International Conference on Innovation (2014)
11. Bismeyer, N., Stresing, C., Bayarou, K. M.: Intrusion detection in VANETs through verification of vehicle movement data (2010)
12. Sedjelmaci, H., Bouali, T., Senouci, S.M.: Detection and prevention from misbehaving intruders in vehicular networks. In: IEEE Global Communications Conference, vol. 2, pp. 39–44 (2015)
13. Nguyen, A., Mokdad, L., Othman, J.: DJAVAN: detecting jamming attacks in vehicle ad hoc networks. Perform. Eval. **87**, 405–410 (2013)
14. Patwardhan, A., Joshi, A., Finin, T., Yesha, Y.: A data intensive reputation management scheme for vehicular ad hoc networks. In: 2006 Third Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services, San Jose, CA, pp. 1–8 (2006). https://doi.org/10.1109/MOBIQ.2006.340422
15. Minhas, U.F., Zhang, J., Tran, T., Cohen, R.: Towards expanded trust management for agents in vehicular ad-hoc networks. Int. J. Comput. Intell.: Theory Pract. (IJCITP) **5**(1), 1–8 (2006)
16. Xu, Q.Y., Su, Z., Wang, Y.T., Dai, M.H.: A trustworthy content caching and bandwidth allocation scheme with edge computing for smart campus. IEEE Access **6**, 63868–63879 (2018)
17. Hu, H., Lu, R., Zhang, Z., Shao, J.: Replace: a reliable trust-based platoon service recommendation scheme in vanet. IEEE Trans. Veh. Technol. **66**(2), 1–1 (2016)
18. Khabbaz, M.J., Fawaz, W.F., Assi, C.M.: A simple free-flow traffific model for vehicular intermittently connected networks. IEEE Trans. Intell. Transp. Syst. **13**(3), 1312–1326 (2012)
19. Xing, R., Su, Z., Zhang, N.: Trust-evaluation-based intrusion detection and reinforcement learning in autonomous driving. IEEE Netw. **33**(5), 54–60 (2019)
20. Gingold, H., Xue, F.: On asymptotic summation of potentially oscillatory difference systems. J. Math. Anal. Appl. **330**(2), 1068–1092 (2007)
21. Le, V., Lin, Y.W., Wang, X.M., Feng, Z.Y., Zhang, P.: A cell based dynamic spectrum management scheme with interference mitigation for cognitive networks. In: VTC Spring 2008 - IEEE Vehicular Technology Conference, pp. 1594–1598 (2008)