Malicious vehicle node detection mechanism based on repeated game and trust evaluation in VANET

Yatao Zhu¹, Yongli Wang¹∗

¹School of Computer Science and Engineering, Nanjing University of Science and Technology, Nanjing, Jiangsu, 210094, China
∗yongliwang@njust.edu.cn

Abstract. In order to solve the problem of malicious vehicle nodes attack in VANET system and improve the security of VANET communication, the paper proposes a method of malicious vehicle nodes detection based on repeated games and trust evaluation. First of all, according to vehicle nodes communicating, a repeated game model is established to generate vehicle nodes revenue by punishing attack behavior nodes and rewarding normal behavior nodes. Secondly, a trust evaluation mechanism is introduced to convert vehicle nodes revenue into nodes trust value. Finally, the optimal dynamic threshold is calculated through multiple iterations, comparing and analyzing nodes trust value and dynamic threshold to screen out the malicious vehicle nodes. Simulation experiments show that this mechanism improves the detection rate of malicious nodes and reduces the error detection rate, effectively isolates malicious vehicle nodes according to the change of node trust value, and improves the security of VANET communication.

1. Introduction

The Intelligent Transportation System (ITS) is a comprehensive application of information technology, communication technology and artificial intelligence[1]. Vehicle Ad-hoc network (VANET)[2] is a mobile wireless self-organizing network composed of vehicle-mounted units, roadside infrastructure and servers [3]. It can avoid potential accidents and improving road safety. Compared with the traditional basic network facilities, VANET has the characteristics of low cost, fast movement speed and strong computing power. However, vehicles running on the road are vulnerable to false information attacks by malicious vehicle nodes, which obviously brings great challenges to the safety of VANET[4]. Malicious vehicle nodes attack is a very representative security issue in VANET security[5]. Malicious nodes can use the mutual communication between nodes to attack and maliciously spoof other vehicle nodes, resulting in vehicle location failure, causing a particularly serious threat to the safety of life and property on vehicle drivers and pedestrians[6].

Currently, researchers have been aware of the impact of malicious node behaviour in VANET, and have proposed many solutions to improve security. Guan[7] proposes a multi-standard game intrusion detection mechanism based on dual parameters.; Guo[8] propose an incentive mechanism for cooperative intrusion detection based on evolutionary games; Mehdi[9] proposed a network trust model based on game theory in the Internet of Vehicles; Yang[10] proposed a RV selection algorithm based on game theory; Yu et al.[11] proposed an incentive model for VANET. Ostermaier et al.[12] used the voting mechanism between nodes to design an algorithm to judge the correct message based on the voter's point of view; The Hermes model[13] calculates the credibility based on the statistics of the success rate of datagram forwarding as the trust criterion. The method described above does not
consider the relationship between game revenue and vehicle node trust, and the impact of node
dynamic changes on malicious vehicle detection in VANET is ignored.

Considering the above points, we study malicious vehicle Nodes detection mechanism using
repeated games\cite{14} and trust evaluation in VANET. We have established a repeated game model to
courage vehicle node cooperation and calculate node revenue. Through multiple games, the
maximum revenue of the vehicle nodes is calculated. We introduce a trust evaluation to convert
the vehicle node's revenue value into the node's trust value. The optimal dynamic threshold is calculated
through multiple iterations, and then the trust value of the vehicle node is compared with the threshold
to select the malicious vehicle node.

2. Model of repeated game and trust evaluation
In order to improve the efficiency of the malicious vehicle node detection mechanism and prevent
malicious nodes from attacking other normal nodes, the structural process is proposed shown in figure
1. Firstly, the communication interaction between vehicle nodes is regarded as a process of multiple
games, establish a stage repeat model, find the vehicle node's revenue in each stage, and send the
revenue to each regional base station S; Secondly, the trust value function is used to calculate the trust
value and dynamic threshold of the vehicle node revenue; Finally, the regional base station S
compares the trust value of nodes with the dynamic threshold, and selects the malicious vehicle node.

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{figure1.png}
\caption{Malicious vehicle node detection process}
\end{figure}

2.1. Building a repeated game model
In order to calculate the profit function for malicious vehicle nodes and normal vehicle nodes, some
symbols need to be defined. $B_i$ is the revenue from the malicious vehicle node's attack; $C_i$ is the price
from the malicious vehicle node's attack; $D_i$ is the revenue from the normal vehicle node's defense; $Q_i$
is the price from the normal vehicle node's defense; $S_i$ is the revenue from the normal behavior of the
vehicle nodes; $P_m$ is the probability of malicious vehicle nodes to attack; $P_n$ is the probability of
normal vehicle nodes to defend.

By analyzing the repeated game process, the revenue matrix as shown in equations (1)(2). $R(m)$
and $R(n)$ Represent the revenue of normal nodes and malicious nodes respectively.

\begin{align*}
R(m) &= \begin{bmatrix}
-C_i P_m \\ S_i(1 - P_m)
\end{bmatrix} - \begin{bmatrix}
B_i - C_i P_m \\ S_i(1 - P_m)
\end{bmatrix} P_m \\
R(n) &= \begin{bmatrix}
-(D_i + Q_i) P_n \\ S_i(1 - P_n)
\end{bmatrix} - \begin{bmatrix}
Q_i P_n \\ S_i(1 - P_n)
\end{bmatrix} P_n
\end{align*}

(1)

(2)
In order to save network resources, this paper stipulates that the maximum return index of a node is $u$. When the return of a node in the game reaches the maximum return $u$, the game process ends, otherwise the game process is repeated. The algorithm of the repeated game model is shown in table 1.

Table 1. Repeated game model algorithm.

| Repeated game model algorithm |
|-------------------------------|
| Input: highest revenue $u$. |
| Output: node revenue $R$. |
| 1) Node A and Node B play a game. |
| 2) Calculate the returns of games A and B at each stage, and find the overall returns $R(A)$ and $R(B)$. |
| 3) If $R(A)>u$ or $R(B)>u$, the game process ends. |
| 4) else goto 1) until the above conditions are met. |

2.2. Conversion of revenue and trust value

Because the malicious vehicle node and the normal vehicle node adopt different strategies to play the game in order to obtain more revenue, in order to distinguish the two types, this mechanism sets a parameter $a$ to convert the node's revenue $U$ into the node's trust value $r_i$, as shown in table 2.

Table 2. Revenue and trust value conversion algorithm.

| Revenue and trust value conversion algorithm |
|-----------------------------------------------|
| Input: Node trust value $r_i$. |
| Output: Node trust value $r_i$ after game. |
| 1) If it is a normal behavior node, $U<0$, then $r_i=U+0$; otherwise, $r_i=U(1-a)$. |
| 2) If it is an attack behavior node, $U<0$, then $r_i=U+0$; otherwise, $r_i=U(1-a)+a$. |

3. Malicious nodes detection

3.1. Dynamic threshold calculation

In order to accurately select malicious vehicle nodes that generate false information attacks, it is necessary to set an appropriate dynamic threshold. The algorithm of calculation of the optimal dynamic threshold of the trust value of the vehicle nodes is shown in table 3.

Table 3. Calculation of the optimal dynamic threshold of trust value of the vehicle nodes algorithm.

| Calculation of the optimal dynamic threshold of trust value of the vehicle nodes algorithm |
|------------------------------------------------------------------------------------------|
| Input: the number of vehicle nodes $N$, each node trust value $r_i$. |
| Output: the optimal dynamic threshold $t$. |
| 1) Set the parameter $c_0$ and select an initial estimated threshold $c_1$ according to the trust value of the node. |
| 2) The estimated threshold $c_1$ divides the node into two parts $n_1$ and $n_2$, $n_1$ is the number of nodes with a trust value greater than $c_1$, and $n_2$ is the number of nodes with a trust value less than $c_1$. |
| 3) Calculate the average trust values $t_1$ and $t_2$ of the two partial nodes in $n_1$ and $n_2$, respectively. |

$$t_1 = \frac{\sum_{i=1}^{n_1} r_i}{n_1} \quad (3)$$

$$t_2 = \frac{\sum_{i=1}^{n_2} r_i}{n_2} \quad (4)$$

then, calculate the average trust value of all nodes:
\[ t = t_1 \frac{n_1}{n_1 + n_2} + t_2 \frac{n_2}{n_1 + n_2} \]  

(5)

4) Find the variance of the trust value of all nodes:

\[ g = \frac{n_1}{n_1 + n_2} (t_1 - t)^2 + \frac{n_2}{n_1 + n_2} (t_2 - t)^2 \]  

(6)

take equations (3), (4) and (5) into (6), and find \( t \) that maximizes \( g \) as:

\[ t = \frac{n_1 n_2}{n_1 + n_2} (t_1 - t_2)^2 \]  

(7)

5) If \(|c_1 - t| < c_0\), then calculate \( t \) as the optimal dynamic threshold; otherwise, assign \( t \) to \( c_1 \) and repeat 2)-4) until the optimal threshold is calculated.

3.2. Detecting malicious nodes

Compare the obtained node trust value \( r_i \) with the dynamic threshold \( t \) obtained above to determine whether the node is a malicious node. Algorithm for detecting malicious nodes is shown in table 4.

| Table 4. Algorithm for detecting malicious nodes |
|--------------------------------------------------|
| **Algorithm for detecting malicious nodes**      |
| **Input:** node trust value \( r_i \) and dynamic threshold \( t \). |
| **Output:** Vehicle node judgment |
| 1) When \( r_i > t \), node i is a malicious node. |
| 2) When \( r_i < t \), node i is a normal node. |
| 3) When \( r_i = t \), enter the next game. |

4. Experiment and analysis

4.1. Experimental environment

The paper will verify the accuracy and reliability of this model through simulation experiments. The hardware environment used for the simulation is: Intel Core i5-10210U CPU, 8G memory, Windows 10 platform, traffic simulation tool NS-3, the vehicle traffic operation scene generation tool is SUMO[15]. We propose two evaluation indicators, detection rate and error detection rate to verify the effectiveness of this mechanism. The detection rate refers to the rate between the number of malicious vehicle nodes detected and the number of malicious vehicle nodes in system. The error detection rate is refers to the proportion of normal vehicle nodes that are mistakenly detected as malicious vehicle nodes. We simulates a city street scene with complicated traffic roads and different vehicle density. In a city of 10km*10km, data files such as vehicle position, speed, density, etc. that are close to real vehicles are generated. The simulation is performed by a simulation simulator. For our analysis, we need to define some parameters as listed in the Table 5.

| TABLE 5. Initial parameter settings of the simulation environment |
|---------------------------------------------------------------|
| Parameter | Parameter value |
| Total number of nodes | 150 |
| Simulation range | 10km*10km |
| Vehicle node speed | 20-100km/h |
| Communication radius | 1000m |
| MAC protocol | IEEE 802.11 |
4.2. Experimental results and analysis

In order to improve the accuracy of experiment, the mechanism is compared with the MIDS[16]. As the number of malicious vehicle nodes changes in the total number of nodes, the detection rate and error detection rate are shown in Figures 2 and 3, and the changes in the trust degree of the malicious vehicle nodes and the normal vehicle nodes are given, as shown in Figure 4.

Figure 2 shows that as the number of malicious nodes increases, the detection rate of both mechanisms is declining. But the decline rate of the mechanism is significantly lower than the MIDS and can maintain a high detection rate. The main reason is that the mechanism uses repeated game and trust evaluation improves the detection rate.

Figure 3 shows that in terms of error detection rate, as the number of malicious nodes increases, MIDS rises significantly faster than this mechanism, and this mechanism maintains a relatively low error detection rate. The main reason is that the mechanism uses repeated games and trust value evaluation, which makes error detection rate lower.

Figure 4 reflects the trust degree of malicious vehicle nodes change greatly, becomes zero gradually. But the trust of the normal vehicle node remains basically unchanged. It can be seen that this mechanism can establish higher trust between normal nodes and effectively isolate malicious nodes.
5. Conclusion
In order to improve the detection efficiency of malicious vehicle nodes in VANET and avoid normal vehicle nodes from being attacked by malicious vehicle nodes, the paper proposes a malicious node detection mechanism based on repeated games and trust evaluation, which rewards the normal behavior and punishes the attack behavior; through repeated game behavior between the nodes, nodes revenue are calculated and converted into nodes trust value; malicious vehicle nodes are detected using the method of trust value and dynamic threshold comparison. Simulation experiments show that this mechanism can effectively improve the detection rate, reduce the error detection rate, isolate malicious vehicle nodes, and significantly improve the security of VANET communication.

Acknowledgments
This article has been awarded by the National Natural Science Foundation of China (61941113), the Fundamental Research Fund for the Central Universities (30918015103, 30918012204), Nanjing Science and Technology Development Plan Project (201805036), and "13th Five-Year" equipment field fund (61403120501), China Academy of Engineering Consulting Research Project(2019-ZD-1-02-02), National Social Science Foundation (18BTQ073), State Grid Technology Project (5211XT190033).

References
[1] Engelbrecht J, Booyse M J, Bruwer F J, et al. Survey of smartphone-based sensing in vehicles for intelligent transportation system applications[J]. Iet Intelligent Transport Systems, 2015, 9(10):924-935.
[2] Singh S, Kumari P, Agrawal S. Comparative Analysis of Various Routing Protocols in VANET[C]// 2015 Fifth International Conference on Advanced Computing & Communication Technologies (ACCT). IEEE, 2015.
[3] Weng J S, Weng J, Zhang Y, et al. BENBI: Scalable and Dynamic Access Control on the Northbound Interface of SDN-Based VANET[J]. IEEE Transactions on Vehicular Technology, 2019, 68(1):822-831.
[4] Zhang C, Xue X, Feng L, et al. Group-Signature and Group Session Key Combined Safety Message Authentication Protocol for VANETs[J]. IEEE Access, 2019, 7:178310-178320.
[5] Zhong X, Chen F, Guan Q, et al. On The Distribution of Nodal Distances in Random Wireless Ad Hoc Network with Mobile Node[J]. Ad Hoc Networks, 2019, 97:102026.
[6] Jamshidi M, Poor S S A, Qader N N, et al. A Lightweight Algorithm against Replica Node Attack in Mobile Wireless Sensor Networks using Learning Agents[J]. Ieie Transactions on Smart Processing & Computing, 2019, 8.
[7] Guan S, Wang J, Jiang C, et al. 2018 IEEE Wireless Communications and Networking Conference (WCNC) - Intrusion detection for wireless sensor networks: A multi-criteria game approach[C]// 2018:1-6.
[8] Guo Y, Zhang H, Zhang L, et al. Incentive Mechanism for Cooperative Intrusion Detection: An Evolutionary Game Approach[C]// International Conference on Computational Science. Springer, Cham, 2018:83-97.
[9] Muhammad Mohsin Mehdi, Imran Raza, Syed Asad Hussain. A Game Theory Based Trust Model for Vehicular Ad hoc Networks (VANETs)[M]. Elsevier North-Holland, Inc. 2017.
[10] Yang B, Sun X, Chai R, et al. Game theory based relay vehicle selection for VANET[C]// IEEE. International Symposium on Personal Indoor & Mobile Radio Communications. IEEE, 2013.
[11] Yuxin, Mao, Ping, etc. A game-based incentive model for service cooperation in VANETs[J]. Concurrency and Computation: Practice and Experience, 2016.
[12] Ostermaier B, Dotzer F, Strassberger M. Enhancing the security of local danger warnings in VANETs - A simulative analysis of voting schemes[C]// The Second International Conference on Availability, Reliability and Security (ARES'07). IEEE, 2007.
[13] Zouridaki C, Mark B L, Hejmo M, et al. Robust cooperative trust establishment for MANETs
[A]. Proceedings of SASN’06 [C].2006.
[14] Michihiro K. Repeated Games Played by Overlapping Generations of Players[J]. Review of
Economic Studies(1):81-92.
[15] Kaur S, Kait R. Comparative Analysis of Routing Algorithms in SUMO for VANET[J]. Ssrn
Electronic Journal, 2019.
[16] Chun-Yan L I, Yi-Liang L, Liang-Min W. Intrusion detection scheme based on traffic scenarios
in vehicular ad-hoc networks[J]. Journal of Shandong University(Engineering Science), 2014.