Postprint: Malicious Vehicle Node Detection Mechanism Based on Repeated Game in Internet of Vehicles Environment

Authors: Dong Wenyuan, Zhu Yan, Yonghong Wang, Zhang Guanghua

Date: 2019-04-01T00:00:00+00:00

Abstract

To address false information attacks within vehicular networks and the low efficiency of malicious vehicle node detection mechanisms caused by rapid node dynamics and varying densities, a malicious vehicle node detection mechanism based on repeated game theory is proposed. First, a repeated game model is established based on vehicle behaviors in information interaction, and node payoffs are utilized to compute trust values and dynamic thresholds; through comparison of these two, suspicious malicious vehicle nodes are filtered out. Second, malicious vehicle nodes are identified from the suspicious ones through a weighted voting algorithm. Finally, the next-hop vehicle node with the highest trust value is selected from the neighbor list for cooperation. Simulation and analysis demonstrate that, compared with existing relevant mechanisms, the proposed mechanism improves the detection rate of false information attacks and reduces the false detection rate.

Full Text

Preamble

Vol. 37 No. 5
Application Research of Computers

Malicious Vehicle Node Detection Mechanism Based on Repeated Game in VANET

Dong Wenyuan[1]†, Zhu Yan[1], Wang Yonghong[2], Zhang Guanghua[1]
(1. College of Information Science & Engineering, Hebei University of Science & Technology, Shijiazhuang 050018, China;
2. Dept. of Computer & Information Engineering, Chengde Petroleum College, Chengde Hebei 067000, China)

Abstract: To address false information attacks within vehicular networks and the inefficiency of malicious vehicle node detection mechanisms caused by rapid node dynamics and varying node densities, this paper proposes a malicious vehicle node detection mechanism based on repeated game theory. First, a repeated game model is established according to vehicle behaviors during information interaction, and node trust values and dynamic thresholds are calculated from the generated node payoffs. Suspicious malicious vehicle nodes are then screened out through comparison between these values. Second, malicious vehicle nodes are identified from the suspicious ones through a weighted voting algorithm. Finally, the next-hop vehicle node with the highest trust value is selected from the neighbor list for cooperation. Simulation and analysis demonstrate that compared with existing mechanisms, the proposed mechanism improves the detection rate of false information attacks while reducing the false detection rate.

Keywords: repeated game; false information attack; voting algorithm; detection rate; error detection rate

0 Introduction

The Internet of Vehicles (IoV) represents a concrete application of the Internet of Things (IoT) in smart urban transportation. By dynamically collecting, distributing, and processing data through vehicular networks and utilizing wireless communication for information sharing, IoV enables information exchange between vehicles, between vehicles and infrastructure, between vehicles and pedestrians, and between vehicles and other facilities, thereby interconnecting automobiles with urban networks [**?**]. However, the inherent contradiction between wireless communication characteristics and the high reliability and security requirements of IoV applications makes vehicles vulnerable to malicious attacks, posing significant security challenges.

From a data communication perspective, security threats in IoV can be analyzed from three aspects: in-vehicle network security, vehicular ad-hoc network security, and vehicular mobile Internet security [**?**, **?**, **?**, **?**].

False information attacks constitute a typical threat to vehicular ad-hoc network security, representing an active attack that exploits the shared open channel characteristics of VANETs [**?**]. In such attacks, once an attacker captures the frequency band of the shared channel, they can impersonate legitimate vehicle nodes to disseminate false messages or tamper with, delay, or drop messages that need to be forwarded, causing severe impacts on road traffic and endangering personal safety and property. Furthermore, the rapid dynamics of vehicles and varying node densities in IoV create substantial obstacles for introducing efficient malicious vehicle node detection mechanisms [**?**, **?**, **?**], making it difficult to eliminate false information attacks. Previous research on false information attack detection has primarily focused on static networks such as wireless sensor networks, with limited investigation into vehicular networks.

This paper introduces game theory concepts into IoV [?, ?] and proposes a malicious vehicle node detection mechanism based on repeated game theory, termed MDMBRV (Malicious Node Detection Mechanism Based on Repeated Game in VANET). This mechanism utilizes a game model to generate trust values and dynamic thresholds. By comparing these parameters, suspicious malicious vehicle nodes are identified and reported to base stations. Upon receiving information about suspicious nodes, base stations employ a voting algorithm to determine malicious vehicle nodes. Finally, a node optimization algorithm selects the next-hop vehicle node to promote cooperation among nodes. The proposed mechanism is simulated and compared with MIDS (Mixed Intrusion Detection Scheme) [?] and AHP (Analytical Hierarchy Process) mechanism [?] in terms of performance.

1 Related Work

To ensure IoV security while improving the detection efficiency of malicious vehicle node detection mechanisms, existing approaches have incorporated game theory into vehicular networks [?, ?, ?, ?, ?, ?, ?, ?]. Game theory offers the advantage of selecting appropriate security strategies based on attack patterns at each stage, thereby reducing the damage caused by malicious nodes. Current game-theoretic security mechanisms can be broadly categorized into two types: static node detection mechanisms and dynamic node detection mechanisms based on game theory.

In static node detection mechanisms, reference [?] proposed a multi-criteria game-based intrusion detection mechanism for wireless sensor networks, considering the trade-offs among information security, node reputation, and energy consumption. This mechanism not only prevents information leakage regarding minimum energy consumption but also removes malicious nodes with high reputation from the network. However, it is unsuitable for dynamic scenarios with incomplete node information. Reference [?] introduced a game-theoretic attack-defense model where attackers and defenders can periodically change their strategies to maximize their respective payoffs, thereby improving energy consumption and detection rates of ESN in IDS. Nevertheless, this theoretical model is only applicable to static embedded scenarios. Reference [?] proposed a multi-layered intrusion detection framework for wireless sensor networks based on game theory, combining specification-based rules and lightweight neural network-based anomaly detection modules to identify malicious sensor nodes. Additionally, the framework established a game model between IDS and monitored sensor nodes to reduce IDS traffic and network energy consumption. However, its detection efficiency decreases when numerous malicious nodes are present. Reference [?] presented a collaborative security detection method based on game theory for IoT, deriving quantitative relationships between collaborative game models and Nash equilibrium under conditions of infinite (or finite) iterations with complete (or incomplete) information through analysis of attacker-defender games. This detection method improves malicious vehicle

node detection rates and network performance but fails to consider the impact of node dynamics. In summary, while these approaches provide reasonable suggestions for malicious node detection and cooperation in static networks, they are not applicable to networks with dynamic node changes.

In dynamic node detection mechanisms, reference [**?**] proposed a security routing protocol based on evolutionary game theory for delay-tolerant networks, which can thwart threats from wormhole attacks, black hole attacks, greedy attacks, and tampering attacks without requiring infrastructure support. However, this protocol is only suitable for delay-tolerant networks, with applications to other networks still under investigation. Reference [**?**] introduced a game-theoretic network trust model for vehicular networks that utilizes three parameters—majority opinion, betweenness centrality, and node density—to enable nodes to better understand the network and its surroundings, effectively preventing malicious behavior. However, this scheme does not address communication reliability issues. Reference [**?**] proposed a game-theoretic model for multi-packet collaborative intrusion detection in mobile ad-hoc networks, achieving high detection accuracy and low delay but suffering from high computational complexity and energy consumption. Reference [**?**] proposed a cooperative intrusion detection incentive mechanism based on evolutionary game theory due to concerns about privacy leakage and resource costs. This mechanism studies a game algorithm to maximize node utility and promotes cooperation among nodes, but its detection efficiency for malicious vehicle nodes is not high.

The aforementioned game-theoretic detection mechanisms, whether for static or dynamic nodes, have not simultaneously considered the problems caused by node dynamics and density variations in vehicular networks. Therefore, this paper proposes a malicious vehicle node detection mechanism based on repeated game theory that analyzes the game process among nodes, generates node trust values and dynamic thresholds, and processes these parameters according to the proposed rules to identify malicious vehicle nodes in the network, thereby ensuring improved detection rates and reduced false detection rates within acceptable overhead and energy consumption limits.

2 Research on Malicious Vehicle Node Detection Mechanism Based on Repeated Game

To improve the detection efficiency of malicious vehicle node detection mechanisms and prevent false information attacks by malicious vehicle nodes, this scheme can be analyzed from five aspects, as shown in [Figure 1: see original paper]. (a) Based on repeated game theory, vehicle information interactions are regarded as a multi-stage game process, and a stage repeated game model is established to calculate vehicle node payoffs, which are then sent to the base station S in each region (this paper assumes base station S is completely trustworthy). (b) A conversion factor is used to transform vehicle node payoffs into trust values and dynamic thresholds. (c) Base station S compares vehicle node trust values with dynamic thresholds to select suspicious malicious vehicle nodes.

(d) Considering different vehicle densities, either a multi-vehicle weighted voting algorithm or a single-vehicle weighted voting algorithm is employed to determine malicious vehicle nodes, and the node information is broadcasted so that other vehicles can remove the node from their neighbor lists. (f) A node optimization cooperation algorithm selects the next-hop vehicle node.

2.1.1 Network Model Definition

The repeated game model between malicious vehicle nodes and normal vehicle nodes comprises four aspects: participating nodes, action space, payoff situation, and number of repeated games. The definitions are as follows:

Definition 1. Participating nodes refer to the entities involved in actions during a game. The type space of participating nodes in this model is {m, n}, where m represents malicious vehicle nodes conducting false information attacks that can threaten and damage neighbor nodes, and n represents normally operating vehicle nodes that pose no threat to neighbor vehicles.

Definition 2. Action space refers to the strategies selected by participating nodes during the game process. This paper considers two action schemes for malicious vehicle nodes: conducting false information attacks and normal operation, denoted as $M = \{M_1, M_2\}$. Similarly, normal vehicle nodes have two action schemes: activating the malicious vehicle node detection mechanism for defense N_1 and normal operation N_2, denoted as $N = \{N_1, N_2\}$. Combining M and N pairwise yields the complete action combination matrix G for malicious and normal vehicle nodes, as shown in equation (1).

Definition 3. Payoff situation refers to the benefits obtained by participating nodes based on their types and selected actions in the game model. This paper assumes U_m as the payoff obtained by malicious vehicle nodes in each stage of the game, and U_n as the payoff obtained by normal vehicle nodes in each stage.

Definition 4. Number of repeated games. Since the game process in this model cannot determine when the game will terminate or how many times it will be repeated, the game process is regarded as a randomly terminated repeated game.

2.1.2 Game Model Establishment

For calculation convenience, this paper only analyzes the game process between malicious vehicle nodes and normal vehicle nodes in vehicular networks, ignoring the game analysis processes among normal vehicle nodes themselves and among malicious vehicle nodes themselves.

To determine the payoff functions for malicious and normal vehicle nodes, several symbols need to be defined, as shown in .

Table 1 Symbol definitions for repeated game model

Symbol	Definition
$C_i(t)$	Payoff obtained by malicious vehicle node for conducting false information attack at time t
$V_i(t)$	Cost paid by malicious vehicle node for conducting false information attack at time t
$Q_i(t)$	Payoff obtained by normal vehicle node for conducting defense at time t
$P_i(t)$	Cost paid by normal vehicle node for conducting defense at time t
$U(t)$	Payoff obtained by vehicle node for normal operation at time t

By analyzing the game process of the repeated game model, the payoff functions for malicious vehicle nodes and normal vehicle nodes in each stage can be obtained, as shown in equations (2) and (3).

To save network resources, this paper specifies the maximum payoff indicator as μ. When a node' s payoff in the game reaches this maximum indicator μ, the game process terminates. The algorithm for the repeated game model is presented as Algorithm 1.

Algorithm 1: Repeated Game Model Algorithm
Input: Maximum payoff μ
1. Nodes A and B engage in the game.
2. Calculate the payoff for A and B at each stage, and compute their total payoffs $U(A)$ and $U(B)$.
3. If $U(A) \geq \mu$ or $U(B) \geq \mu$, the game process ends.
4. Otherwise, the game continues, executing steps 1 and 2 until step 3 is satisfied.
5. End

2.2 Benefit and Trust Value Conversion

Since malicious and normal vehicle nodes adopt different strategies to obtain more payoffs during the game process, to distinguish between the two types, this mechanism assumes a conversion factor δ to transform node payoffs into node trust values. If the payoff corresponds to malicious behavior, the node trust value is calculated as the difference between δ and the node payoff. If the payoff corresponds to normal behavior, the node trust value is calculated as the sum of δ and the node payoff. When the payoff is negative, the node trust value is represented as 0. Finally, the node trust value T_i is calculated, and the node information is sent to base station S. The conversion method between node payoff and trust value is presented as Algorithm 2.

Algorithm 2: Benefit and Trust Value Conversion Algorithm
Input: Node trust value T_i
Output: Node trust value T_i after game

1. Through analysis, determine whether the node' s action is malicious (represented by 1) or normal (represented by 2), with node denoted as N.
2. If the action is malicious:
- If $U < 0$, then $T_i = 0$;
- Otherwise, $T_i = T_i - U$.
3. If the action is normal:
- If $U < 0$, then $T_i = 0$;
- Otherwise, $T_i = T_i + U$.
4. Continue game detection.
5. End

2.3 Suspicious Malicious Vehicle Node Selection

To accurately select suspicious malicious vehicle nodes that generate false information attacks, appropriate dynamic thresholds must be set. This paper adopts a global threshold solving algorithm to address this issue. The detailed algorithm flow is as follows:

a) Set parameter ε_0 and select an initial estimated threshold ε_1 based on node trust values.

b) The estimated threshold ε_1 divides nodes into two parts, N_1 and N_2, where N_1 represents nodes with trust values greater than ε_1, and N_2 represents nodes with trust values less than ε_1.

c) Calculate the average trust values λ_1 and λ_2 for all nodes in N_1 and N_2, respectively, and compute the new threshold $\varepsilon_2 = (\lambda_1 + \lambda_2)/2$.

d) If $|\varepsilon_1 - \varepsilon_2| < \varepsilon_0$, then ε_2 is the optimal dynamic threshold; otherwise, assign ε_2 to ε_1 and repeat steps b) to d) until the optimal threshold ε is obtained.

From Algorithm 1 and Algorithm 2, nodes have corresponding trust values T_i during the game process, and the optimal dynamic threshold ε is obtained through the global threshold method. Subsequently, the obtained node trust value T_i is compared with the dynamic threshold ε to determine whether node N is a suspicious malicious vehicle node:

- If $T_i > \varepsilon$, node N is a suspicious normal vehicle node.
- If $T_i < \varepsilon$, node N is a suspicious malicious vehicle node.
- If $T_i = \varepsilon$, wait for the next game detection result.

Algorithm 3: Suspicious Malicious Vehicle Node Selection Algorithm
Input: Node trust value T_i and dynamic threshold ε
Output: Selection result indicating whether the node is a suspicious malicious or suspicious normal vehicle node

1. If $T_i > \varepsilon$, the node is a suspicious normal vehicle node.
2. If $T_i < \varepsilon$, the node is a suspicious malicious vehicle node.
3. If $T_i = \varepsilon$, wait for the next vote.
4. End

2.4 Malicious Vehicle Node Judgment and Removal

In vehicular networks, different distances and link quality between vehicles may lead to errors in single vehicle node judgment results. Therefore, a multi-vehicle node voting algorithm is needed to avoid such issues. When the majority of vehicles determine that a certain vehicle node is suspicious, the node can be identified as a malicious vehicle node.

During actual voting, considering that vehicles have different trust levels, the concept of weight is introduced to improve judgment accuracy. The node weight in this paper can be calculated using equation (4), where a larger weight indicates greater influence in voting, and a smaller weight indicates less influence.

Meanwhile, different vehicle densities reduce the stability and reliability of node voting algorithms. To address this, based on the Boyer-Moore voting algorithm [**?**] and incorporating node weights from equation (4), two types of algorithms are proposed: a multi-vehicle weighted voting algorithm suitable for dense node scenarios (Algorithm 4) and a single-vehicle weighted voting algorithm suitable for sparse node scenarios (Algorithm 5).

Algorithm 4: Multi-Vehicle Weighted Voting Algorithm
Input: Initial vote count $a_i = 0$
Output: Total vote count C_{sum}
1. Establish a neighbor list set $\{a_1, a_2, a_3, ..., a_i\}$ that engages in games with node N, where each element a_i represents the judgment of whether node N is a malicious or normal vehicle node (0 for suspicious normal, 1 for suspicious malicious).
2. Calculate the weight W_i of each vehicle node in the neighbor list based on trust values.
3. If $a_i = 1$, then $C_{sum} = C_{sum} + W_i$; otherwise, $C_{sum} = C_{sum} - W_i$.
4. End

Algorithm 5: Single-Vehicle Weighted Voting Algorithm
Repeat steps 1 and 2 from Algorithm 4 to calculate the weight W_i of each node. Compare the weights of all nodes to find the maximum weight node W_{ia}. If W_{ia} is the maximum weight node, then the judgment of node n with weight W_{ia} is considered the correct judgment result.

The judgment of whether N is a malicious vehicle node using the multi-vehicle weighted voting algorithm depends on the total vote count C_{sum} from participating vehicles. When neighbor vehicles judge N as a malicious vehicle node, the vote count decreases; when judged as normal, the vote count increases. A larger total vote count C_{sum} indicates higher accuracy that N is a normal vehicle

node, and vice versa.

- If $C_{sum} > 0$, the majority of votes indicate N is a normal vehicle node, so N is judged as a normal vehicle node.

- If $C_{sum} < 0$, the majority of votes indicate N is a malicious vehicle node, so N is judged as a malicious vehicle node.

- If $C_{sum} = 0$, N cannot be determined as normal or malicious, and we wait for the next vote.

The specific process is presented as Algorithm 6.

Algorithm 6: Malicious Vehicle Node Judgment
Input: Total vote count C_{sum}
1. Determine node density.
2. If node density is high, execute Algorithm 4.
- If $C_{sum} > 0$, n is a normal vehicle node.
- If $C_{sum} < 0$, n is a malicious vehicle node, and the base station broadcasts a warning for surrounding nodes to remove this node from their neighbor lists.
- If $C_{sum} = 0$, wait for the next vote.
3. Otherwise, execute Algorithm 5.
4. End

2.5 Node Optimization Cooperation Algorithm

Based on the above models and algorithms, the trust values and weights of all vehicle nodes have been calculated, and malicious vehicle nodes have been removed from the network. To further improve the reliability and security of transmitted information and ensure efficient cooperation among nodes, a node optimization cooperation algorithm is proposed. This algorithm enables nodes to prioritize selecting the next-hop node with the highest trust value in the neighbor list for information transmission. The specific node selection process is as follows:

a) The requesting node sorts the trust values of next-hop nodes in its neighbor list from high to low, selects the next-hop node with the highest trust value as its cooperation partner, and sends a request message.

b) Upon receiving the request, the next-hop node informs the requesting node of its status information (including location, speed, surrounding vehicle density, etc.) and asks whether to receive and forward the information.

c) Based on steps a) and b), the information is continuously transmitted until it reaches the destination node.

3 Simulation Experiment and Analysis

3.1 Environment Setup

The traffic simulation tool used in this research is NS-2 [**?**], and the vehicle traffic scenario generation tool is SUMO [**?**]. NS-2 is a discrete-event network simulator developed by UC Berkeley, defined in C++ and providing simulation interfaces through Otcl scripting language, supporting VANET routing protocols and 802.11 MAC implementation. SUMO is an open-source microscopic traffic simulation software that generates required road network and route XML files through MOVE configuration. This paper simulates a complex urban street scenario with varying vehicle densities, generating trace files containing realistic vehicle positions, speeds, and density data for a 20km×20km city area, which are then loaded into the NS-2 simulator. Simulation parameters are shown in .

Table 2 Simulation parameter settings

Parameter	Value
Simulation area	20km × 20km
Vehicle speed	30-100 km/h
Communication range	1000m
MAC protocol	802.11p
Data packet transmission rate	1 Kbit/s
Attack type	False information attack

3.2 Experimental Results and Comparative Analysis

To validate the effectiveness of the proposed scheme, two evaluation metrics are defined: detection rate and false detection rate. The detection rate refers to the ratio of successfully detected malicious vehicle nodes to the total number of malicious nodes in the network, while the false detection rate refers to the proportion of normal vehicle nodes mistakenly detected as malicious. To improve accuracy, multiple simulation runs are conducted and averaged. The detection and false detection rates of MDMBRV against false information attacks under different numbers of malicious vehicle nodes are shown in [Figure 2: see original paper] and [Figure 3: see original paper].

[Figure 2: see original paper] compares the detection rates of MDMBRV, MIDS, and AHP mechanisms. As the number of malicious vehicle nodes increases, the detection rates of all three mechanisms show a slight downward trend, with MIDS declining most significantly, followed by AHP, and MDMBRV showing the smallest decline. Compared with MIDS and AHP, MDMBRV maintains a higher detection rate for malicious vehicle nodes, primarily because it employs a multi-vehicle voting algorithm that enables surrounding vehicles to judge suspicious nodes collectively, thereby improving detection accuracy.

[Figure 3: see original paper] compares the false detection rates of the three mechanisms. As the proportion of malicious vehicle nodes increases, the false detection rates of MDMBRV, MIDS, and AHP gradually rise. However, MDMBRV maintains a relatively low false detection rate compared to MIDS and AHP. This is mainly because the global threshold method introduced in this mechanism can dynamically adjust the threshold in real-time according to environmental changes.

When node dynamics change, node density also varies. [Figure 4: see original paper] and [Figure 5: see original paper] show the detection and false detection rates of MDMBRV under different vehicle densities.

[Figure 4: see original paper] demonstrates that as vehicle density increases, the detection rates of all three mechanisms improve. The proposed mechanism consistently outperforms MIDS and AHP when vehicle density is between 1×10^{-3} and 1×10^{-2} vehicles/m², achieving a detection rate as high as 96.5% at a density of 1×10^{-2} vehicles/m². This is primarily because increased vehicle density adds more neighbor vehicles around suspicious nodes, enhancing voting algorithm accuracy.

[Figure 5: see original paper] shows that as vehicle density increases, the false detection rates of MIDS and AHP rise significantly, while MDMBRV' s false detection rate initially increases slightly before showing a downward trend, remaining stable overall and lower than MIDS and AHP. Compared with MIDS and AHP, the proposed mechanism is less susceptible to vehicle density interference and achieves better false detection rates, mainly because it can appropriately select either the multi-vehicle weighted voting algorithm or the single-vehicle weighted voting algorithm based on different vehicle densities.

To analyze the impact of vehicle density on network overhead, scenarios with different vehicle densities were configured at a constant speed of 30 km/h. Two malicious vehicles conducting false information attacks were randomly selected to observe network overhead during attack identification under different scenarios. As shown in [Figure 6: see original paper], network overhead for both mechanisms gradually increases with vehicle density. MDMBRV shows a more pronounced upward trend and higher overhead than MIDS, because increased vehicle density intensifies the game processes among nodes in MDMBRV, generating greater network overhead.

4 Conclusion

This paper proposes a malicious vehicle node detection mechanism based on repeated game theory to improve detection efficiency in vehicular networks and protect vehicles from false information attacks. By combining repeated game theory with voting algorithms, the mechanism identifies malicious vehicle nodes through analysis of inter-node game behaviors and voting algorithms. Finally, to promote cooperation among nodes, the optimal next-hop node is selected for information transmission. The effectiveness of MDMBRV is validated from

three aspects: detection rate, false detection rate, and communication overhead. Future work will focus on reducing network overhead in the current MDMBRV framework and investigating detection methods for malicious vehicle nodes conducting Sybil, DoS, and other types of attacks.

References

[1] Xu Wenchao, Zhou Haibo, Cheng Nan, et al. Internet of Vehicles in Big Data Era [J]. IEEE/CAA Journal of Automatica Sinica, 2018, 5(1): 58-69.

[2] Chen Jiacheng, Zhou Haibo, Zhang Ning, et al. Service-oriented dynamic connection management for software-defined Internet of vehicles [J]. IEEE Transactions on Intelligent Transportation Systems, 2017, 18(10): 2826-2837.

[3] Yadav K, Vijayakumar P. VANET and its security aspects: a review [J]. Indian Journal of Science and Technology, 2016, 9(44): 59-64.

[4] Muhammad A, Elyes B, Wassim Z, et al. Security in intelligent transport systems for smart cities: from theory to practice [J]. Sensors, 2016, 16(6): 879.

[5] Li Fujuan, Wang Qun, Qian Huanyan, et al. Survey on security threats of Internet of vehicles [J]. Application of Electronic Technique, 2017, 43(5): 29-33, 37.

[6] Roshan J, Preetam S. Detection of malicious node and development of routing strategy in VANET [C]//Proc of International Conference on Signal Processing and Integrated Networks. 2016: 472-476.

[7] Subba B, Biswas S, Karmakar S. A game theory based multi layered intrusion detection framework for VANET [J]. Future Generation Computer Systems, 2018, 82(5): 12-28.

[8] Jared O. A Distributed reputation scheme for situation awareness in vehicular Ad hoc networks (VANETs) [C]//Proc of IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support. 2016: 1-5.

[9] Liang Xiannuan, Xiao Yang. Game theory for network security [J]. IEEE Communications Surveys & Tutorials, 2013, 15(1): 472-486.

[10] Abdalzaher M, Seddik K, Elsabrouty M, et al. Game theory meets wireless sensor networks security requirements and threats mitigation: a survey [J]. Sensors, 2016, 16(7): 1003.

[11] Li Chunyan, Liu Yiliang, Wang Liangmin. Intrusion detection scheme based on traffic scenarios in vehicular ad hoc networks [J]. Journal of Shandong University, 2014, 44(1): 29-34.

[12] Saraswat D, Chaurasia B. AHP Based Trust Model in VANETs [C]//Proc of the 5th International Conference on Computational Intelligence and Communication Networks. 2013: 27-29.

[13] Guan Sanghai, Wang Jingjing, Jiang Chunxiao, et al. Intrusion detection for wireless sensor networks: a multi-criteria game approach [C]//Proc of IEEE Wireless Communications and Networking Conference. 2018: 1-6.

[14] Wang Kun, Du Miao, Yang Dejun, et al. Game-theory-based active defense for intrusion detection in cyber-physical embedded systems [J]. ACM Transactions on Embedded Computing Systems, 2016, 16(1): 1-21.

[15] Subba B, Biswas S, Karmakar S. A game theory based multi layered intrusion detection framework for wireless sensor networks [J]. International Journal of Wireless Information Networks, 2018(4): 1-23.

[16] Wu Hao, Wang Wei. A game theory based collaborative security detection method for Internet of things systems [C]//IEEE Transactions on Information Forensics & Security, 2018, 13(6): 1432-1445.

[17] Guo Hang, Wang Xingwei, Cheng Hui, et al. A routing defense mechanism using evolutionary game theory for delay tolerant networks [J]. Applied Soft Computing, 2016, 38(C): 469-476.

[18] Mehdi M, Raza I, Hussain S. A game theory based trust model for vehicular Ad hoc networks [J]. Computer Networks, 2017, 121(7): 1-14.

[19] Purbita C, Koushik M, Anurag D. A game theoretic model to detect cooperative intrusion over multiple packets [C]//Artificial Intelligence and Evolutionary Computations in Engineering Systems. 2016: 895-907.

[20] Guo Yunchuan, Zhang Han, Zhang Lingcui, et al. Incentive mechanism for cooperative intrusion detection: an evolutionary game approach [C]//Proc of International Conference on Computational Science. 2018: 1-10.

[21] Rahim R, Ahmar A, Ardyanti, et al. Visual Approach of Searching Process using Boyer-Moore Algorithm [C]//Proc of International Conference on Information and Communication Technology. 2017: 1-5.

[22] Henderson T. Network simulator 2.31 [EB/OL]. (2007-03-10) [2018-11-08]. http://mailman.isi.edu/pipermail/ns-developers/2007-March/002931.html.

[23] Krajzewicz D, Hertkorn G, Rossel C, et al. SUMO (simulation of urban mobility): an open-source traffic simulation [C]//Proc of the 4th Middle East Symposium on Simulation and Modelling. 2002: 183-187.

Note: Figure translations are in progress. See original paper for figures.