Security of the Internet of Things Based on Game Algorithm

https://doi.org/10.3991/ijoe.v14i08.9178

Yue-e Yi
Changsha Social Work College, Changsha, China
yiyuee1981@21cn.com

Abstract—To explore the security mechanism of the Internet of Things (IoT) perception environment, we perform a security research on the IoT on the basis of game algorithm. The dynamic game method of node cooperation is used in the experiments. Firstly, multiple report nodes are merged into a game party, and the dynamic game for two parties is established with the detection node. In the environment where the malicious nodes are dominant, the detection nodes collaborate, and the state of the unknown nodes is conjectured by the reputation value of the reporting nodes. The high trust reference report is used for the modification and reduction the weight of malicious nodes in the overall report, for node merging, and finally for bias equilibrium. The results show that cooperative game can significantly improve the success rate of incident monitoring and reduce the number of forged reports.

Keywords—Internet of Things; perception environment; game; malicious node; detection node

1 Introduction

In recent years, the Internet of Things (IoT) has elicited wide attention from academia and industry. With the development of the Internet and wireless communications, IoT is expected to bring an essential technological revolution that will lead us into a new era of wide interconnectivity, computing, and communication. The application of IoT is wide, such as climate monitoring, traffic safety, family automation, healthcare, supply chain, agricultural production, rural development, border security, and military applications. In IoT, objects (Objects, Obs, including people and things) are considered to have the ability to perceive physical objects, communicate with each other, and be able to operate intelligently without manual intervention. Among the main technologies that lead to the application of the IoT, the wireless sensor network (WSN) technology and mobile communication technology have a more important position and function. Although wired connections can provide rapid communication, distance and location constraints restrict the development of the IoT. With the rapid development of mobile Internet and wireless communication, information exchange by wireless communication can overcome the limitations of wired communication, thereby greatly promoting the development of the IoT.

The basic function of the IoT is to acquire and transfer information and realize the interconnection of all things. Therefore, expanding information source and realizing rapid and convenient information interaction has been the focus of IoT research. Cooperation is an important feature of the IoT. The IoT is recognized as a global network, enabling communication and cooperation between people and objects, things and objects. Wireless communication can support extensive cooperation in the IoT through wireless networks, which can significantly promote the development of the IoT. Therefore, more attention should be paid to research on cooperative-based wireless communication in the IoT.

The starting point of game theory in mathematics was the publication of *Theory of Games and Economic Behavior* in 1944. The work summarizes the typical behavior characteristics of an economic subject, introduces the expansion and the strategic and matrix representation of game theory, defines the minimal and maximal solution, illustrates that the solution exists for all people's zero-sum games, proposes the concept and analysis method of a stable set solution. On the basis of summarizing the previous research results of game theory, the book *Theory of Games and Economic Behavior* provides the general framework and concept terms and expression methods of game theory and establishes a more systematic game theory. One of the main concerns of game theory is the problem of behavioral equilibrium among interacting strategies, and rational players in the system are important theoretical foundations of game theory. The rationality here refers to the driving effect of players' behavioral decisions. This process is one of the main concerns of game theory, namely, the system decision-making operation mechanism and system optimization based on this guidance.

Based on the above background, this paper mainly combines game theory with the IoT, mainly aiming at the security of IoT based on game theory.

2 State of the art

In the last two years, privacy protection has elicited widespread interest along with the rise of the IoT, prompting several research institutions have started corresponding research plans.

Chettri et al. (2015) pointed out research on the key management and authentication technology of the IoT is relatively mature compared with other security mechanisms. The IoT may consist of many heterogeneous networks from the perception layer to the network layer and then to the application layer. The current key management and authentication methods mainly adopt two centralized management methods based on the Internet and a distributed management mode centered on their respective heterogeneous networks [1]. Zeng et al. (2016) believed that the centralized Internet management mode was responsible for the management of the generation, distribution, and update of keys and for message authentication and identity authentication by an Internet-trusted security center. For example, the sensor network of the perception layer is connected to the Internet, and the key authentication center can interact with the sensor network to realize sensing in the network security management and authenticate device nodes [2]. Li (2017) proposed that the distributed management model, which considers the heterogeneous network as the center, was easier to implement in the Internet and mobile communication network. The sensing layer of the perception layer is the key to solving the problem of key management and authentication because of its limited resources [3].

In IoT mobile communication, Liu et al. (2014) analyzed the privacy of a location and the identity privacy of a 2G/3G system and proposed a solution for location privacy in the cellular network through secure multiparty computing. The privacy protection protocol is described as third party identity authentication, and the encryption-based identity standard is used in the new diffuse area [4]. Xie et al. (2017) used the location privacy protection mechanism based on density distribution function to protect the privacy information, such as vehicle location in a vehicle network. This mechanism needs the help of the trusted third party, and some difficulty arises in the practical application [5].

Meanwhile, Shamshirband et al. (2014) pointed out that the game model can be divided into two categories: non-cooperative and cooperative. The former can be divided into a complete rational game model and a limited rational game model according to the players' rational and irrational assumptions [6]. Tang et al. (2014) in the study pointed out that the game model can be divided into static, dynamic, and repeated action game models [7] in accordance with the sequential order of the players making decision actions in the game. Lee et al. (2015) stated that the information elements that players need to make decisions in the game can be divided into complete information and incomplete information game models, and each of these models can be divided into complete information static, complete information dynamic, incomplete information static, and incomplete information dynamic [8]. Many other criteria and corresponding different division methods are available for game division.

In summary, research on the integration of the IoT and game theory remains lacking. The studies above focuses on either one or the other. Therefore, based on the above research status, this paper mainly studies the security of the IoT based on game theory. First, the game algorithm and the IoT are introduced, and then the game algorithm is applied to the security of the IoT, thereby enhancing the security of the IoT.

3 Method

3.1 Basic concepts of game theory

The basic concepts of game theory include player, action, information, strategy, utility, income, and equilibrium. Among them, the player is the decision maker who selects actions to maximize their utility. Action is the decision variable of the player, and strategy is the rule for players to select actions and provides the time and type of actions players select. Information refers to the knowledge of players in the game, including other players' strategies, actions, or utility functions.

A basic game definition is as follows:

$$G=\left\{S_1,S_2,\mathrm{L}\ \ S_M;u_1,u_2,\mathrm{L}\ \ u_M\right\}. \tag{1}$$

In (1), Si suggests the strategic collection of player I, $S=S_1\times\ldots\times S_M$ is the strategic combination space of all players, x refers to Cartesian product, and u_i indicates the utility function of the player i.

3.2 Related concepts and hierarchical models of the IoT

On the premise of the continuous development of information science and technology, researchers in the related subjects of the IoT and related fields have started to investigate the IoT in depth, thereby producing a concrete image of the concept of the IoT. However, they have not yet formed a complete, accurate, and recognized concept. Generally, two common concepts of the IoT are used.

First, the IoT is a global network. It is based on the computer Internet and is formed by specific wireless data communication technologies (such as sensing technology, radio frequency identification (RFID) technology and so on). Using specific information technology (sensor technology, RFID technology, etc.), the automatic recognition of global goods can be realized so as to share the relevant information of the computer Internet in real time, which is the essence of the IoT.

Second, the IoT is based on certain information sensing devices (such as RFID, infrared sensors, laser scanners, and global positioning systems) and exchanges and processes information according to a single or multiple predetermined transmission protocols. The wired or wireless networks connect products and the Internet for the identification, location, tracking, monitoring, and management of objects, which is an intelligent network. The essence of intelligent network is to realize the interconnection between all goods and the Internet and to achieve the purpose of quick identification and intelligent management. At present, this definition is widely accepted and recognized. Therefore, managing object information perception, transmission, and monitoring processes is the core function of the IoT.

In the well-known architecture of the IoT, the IoT architecture of electric product code (EPC) global is the most representative. Its components are mainly composed of EPC coding technology, EPC label, EPC reader, server, and EPC middleware. Given these different functions, the architecture of the IoT can be roughly divided into three layers, namely, the perception layer, or the bottom, which is used for collecting information; the network layer, or the middle layer, which is used for transmitting data; and the application/middleware layer, which is also known as the top layer.

In the architecture of the IoT, the functions of each layer are described in detail as follows:

The perception layer (low layer): it collects some data and information related to it by information-sensing technologies, such as RFID mobile terminal technology, M2M terminal technology, perceptive node, and sink node. For instance, the perception nodes mentioned earlier can perceive, measure, capture, and transfer information anytime and anywhere. The sink nodes can converge, analyze, process, and transmit data. The main technologies related to the perception layer are RFID technology, sensor control technology, and short-distance wireless transmission and communication technology.

The network layer (middle layer): the network is usually based on the existing Internet or mobile communication network, and the sensing data management and processing technology on this layer is the core technology for realizing the function of the IoT. The technology of perception data management and processing mainly includes the theory of perception data storage, analysis, understanding, mining, and perception of database decision and behavior. As a major boost to the development of the IoT, the cloud computing platform has undergone rapid development. The cloud computing platform has a large storage capacity and capable of rapid analysis of mass sensing data. It is an important part of the network layer of the IoT and is the basis of application development.

The application layer (top layer): the problem of information processing and human–computer intersection is solved in the application layer. Perception data are analyzed and processed and then used in the application layer, which provides all types of applications for users and combines the information demand of individual industry with the technology of IoT. Thus, this layer is extensively used. The intelligent application of the IoT can be divided into various types, namely, logistics monitoring and environmental monitoring, inquiry of intelligent retrieval, intelligent transportation, smart grid control, mobile wallet, high-speed non-parking fee, and scanning type.

In 2005, the following key technologies in the IoT are described: device technology (used to perceive things), RFID technology (used for marking things), nanotechnology, and key technology. Thus, a model of the IoT technology system can be obtained.

3.3 Attack suppression game method in a normal network

Given that malicious nodes in the IoT environment is capable of perceiving an environment and intelligent processing, if the malicious nodes realize that unrestricted attacks will lead to their identification and isolation, a more flexible attack method will be taken, and such an attacker is conditional.

The attack logic of malicious nodes is discussed from the perspective of game theory. If the reputation is expected to be maintained in the inferior scene by the intelligent malicious node, the best strategy is not to take the attack behavior and not to forge the report, thereby reaching the bias equilibrium with the normal report node. This type of game is called the simple game.

As a party of the game, the malicious node r_m first infers an optimal strategy a_2* that the detection node r_n will take and then adopts an optimal strategic a_1* of its own. As the other party of the game, the detection node r_n then takes the corresponding optimal strategic a_2* according to the r_m behavior that has occurred. If the two sides derive the best strategy of the other side, the equilibrium can be considered. Considering that the report of malicious nodes is produced simultaneously and what the detection node investigates is the report itself, we modify it in the construction of a specific simple game. A plurality of reporting nodes are formulated as a game party, and multiple reports on the same incident are combined in a manner that a game between several report nodes and an observation node is formed. Each report node has its own optimal strategic inference, and the final detection node makes its own optimal strategic inference according to the behaviors of all reporting nodes.

The specific deduction process is shown in Figure 1. The node first calculates the prior nature of the other party, the probability of taking a strategy, and the return value of the other side after the other party takes the strategy. After determining the three values, the optimal strategy that maximizes the benefit can be calculated, and the conditional probability of the party is finally updated. This process can be conducted iteratively, and the strategic convergence of both sides is balanced.

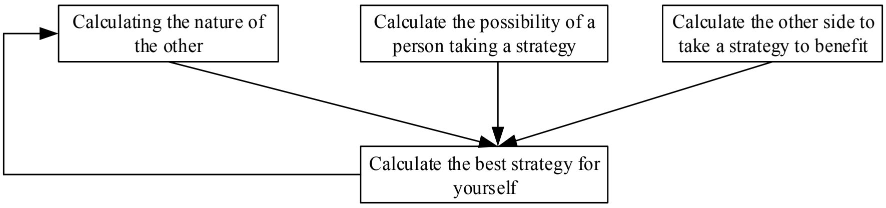
Calculating the nature of the other
Calculate the possibility of a person taking a strategy
Calculate the other side to take a strategy to benefit
Calculate the best strategy for yourself

Fig. 1. Derivation process of simple game

4 Results

4.1 Experimental setup

A network simulator can simulate different scenarios of the perception network. We reuse the module of node detection to evaluate the performance of the intrusion detection mechanism. The default parameters of the simulation are shown in Table 1.

Table 1. Experimental parameter setting

Area volume	**1000×800 m^2**	**Number of nodes**	**80**	**Node communication distance**	**200 m**
Mobile node ratio	30%	Mobile node speed	10 m/s	Simulation time	200 s

We set up two scenarios to compare the detection efficiency of malicious incidents in different environments. The first is the normal scene, in which the nodes normally interact data and no malicious incident occurs and the nodes of the malicious organization falsely reports “some nodes indicate malicious incidents.” The second is an abnormal scene, in which some malicious nodes have malicious behaviors, such as discarding data packets, but other malicious nodes of the same organization forge the evidence in the report that the malicious incident does not exist. The real incidents in these two scenarios are “no malicious incidents” and “malicious incidents,” respectively.

4.2 Effect of simple game

In this section, we design two groups of experiments. In the first group of experiments, malicious nodes unconditionally generate malicious incidents. In the second group of experiments, malicious nodes dynamically detect malicious incidents by a simple game by observing the surrounding environment. Figures 2–5 show the incidence of malicious incidents and the successful detection rate of the both experiments in normal and abnormal scenarios.

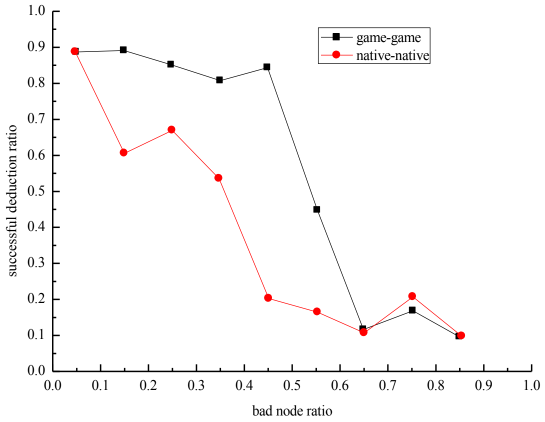

Fig. 2. Success rate of incident detection in normal scene

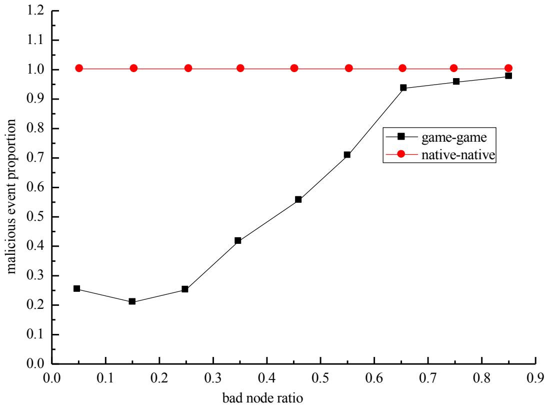

Fig. 3. Incidence rate of false report in normal scene

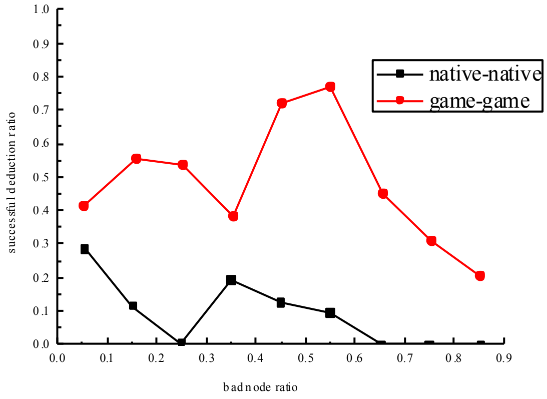

Fig. 4. Success rate of incident detection in abnormal scene

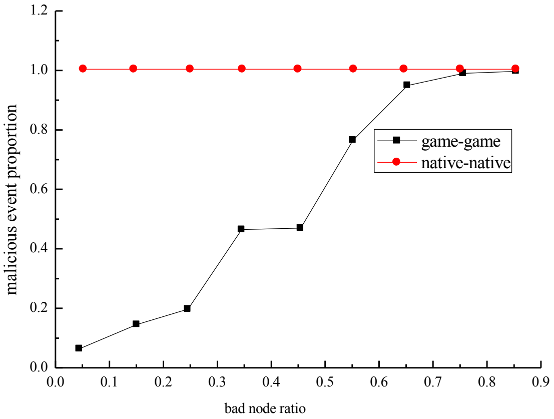

Fig. 5. Incidence rate of false report in abnormal scene

As unconditional malicious nodes forge reports anytime, the incidence of malicious incidents in the two scenes are all 100%, and malicious nodes in a simple game forge report only when the nearby nodes are dominant. Therefore, the numbers of forged reports in Figs. 3 and 5 are approximately linear with the number of malicious nodes.

Even if the nodes side is not dominant, an unconditional malicious node produces malicious reports, so the smaller the proportion of malicious nodes is, the higher the success rate of the event detection is. In this simple game, malicious nodes are normal. Moreover, the detection node has a high rate of inference for the occurrence of incidents, the success rate of the normal scene is above 80%, and the success rate of abnormal scenes is more than 40%. However, when the number of malicious nodes is dominant, unconditional malicious nodes or malicious nodes in the simple game generate malicious incidents. Then, the detection node infers the incidents only by the arithmetic average value reported by all parties. This situation easily causes misjudgment. The greater the proportion of malicious nodes is, the lower the detection success rate is. As a result, when 90% of the malicious nodes are present, the detection success rates of methods are both less than 20%.

When the game mechanism is not used and malicious nodes are small, malicious attacks are easily detected but cannot be suppressed. The use of a simple game mechanism not only enables the detection but also the suppression of malicious attacks. However, when the number of the malicious node is slightly less than that of the normal node, malicious incidents cannot be suppressed. When the number of malicious nodes is equal to the number of normal nodes or larger than the normal node, the success rate of malicious incident detection drops sharply. Thus, the simple game is unsuitable for a scenario with prevalent malicious nodes.

4.3 Effect of cooperative game

The previous experiment indicates that the simple game method cannot reduce the number of false reports of malicious nodes and cannot effectively detect malicious events in environments with prevalent malicious nodes. In this section, we verify the performance of the cooperative game method.

First, we perform four sets of experiments. In the first experiment, malicious report nodes and detection nodes do not use a game (native–native). In the second group, malicious report nodes and detection nodes both use the simple game (game–game). In the third group, malicious report nodes still use the simple game, but detection nodes use the cooperative game (game–cogame) to verify the success rate of the detection of malicious incidents by the cooperative game. In the fourth group, both use the organization cooperative game (cogame–cogame) to verify the restriction effect of the cooperative game on a malicious attack. Then, the forgery report incidence and incident detection success rates of the experiments in normal and abnormal scenarios are compared. The results are shown in Fig. 6–9.

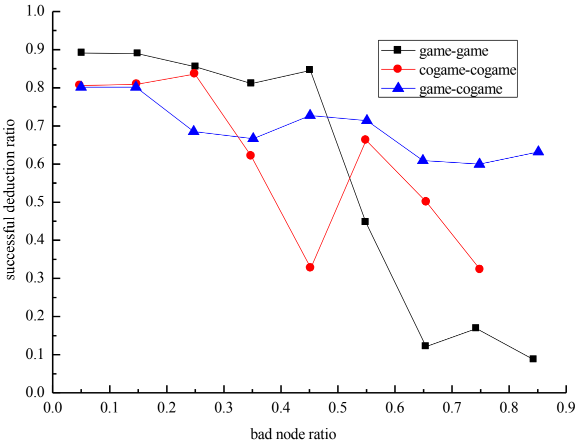

Fig. 6. Success rate of incident detection in normal scene

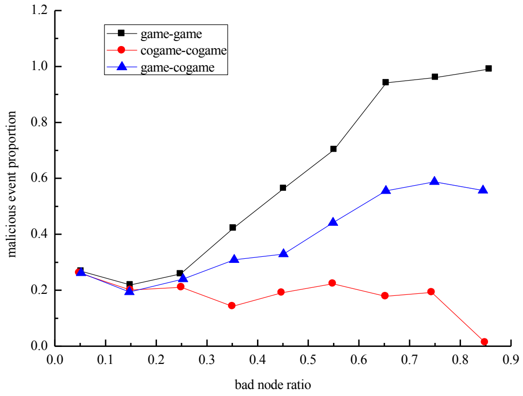

Fig. 7. Incidence rate of false report in normal scene

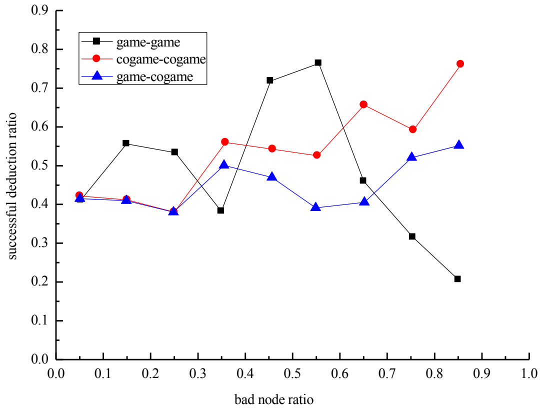

Fig. 8. Success rate of incident detection in abnormal scene

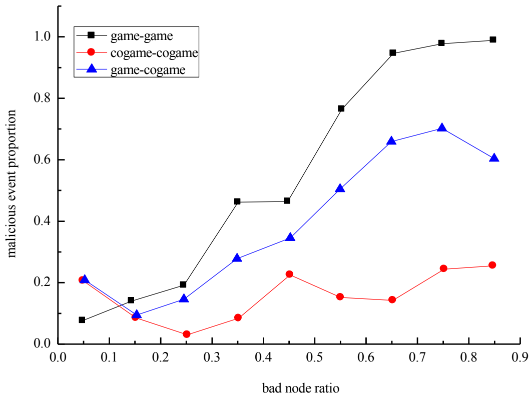

Fig. 9. Incidence rate of false report in abnormal scene

The previous experiment indicates that the success rate of incident detection is low when the detection report node uses a simple game, especially when the malicious nodes are above 80%. The detection success rates under the two scenarios do not exceed 20% and 30%, respectively. When the detection node uses the cooperative game and the normal node is dominant, the number of malicious reports is low, and the report tends to be normal. Thus, the success rate of incident detection is higher. When the malicious node is dominant, the malicious report in game–cogame increases, but at this time, the detection node reduces the weight of the suspicious node according to the observation of its own node, thereby reducing the proportion of the malicious report in the entire report. As a result, the success rate of the game-cogame incident detection is stable. When the historical records of observation nodes and malicious organization nodes are inconsistent with current observations, the larger the number of the inconsistent nodes is, the more effective the weight reduction process of a malicious organization is. When the number of malicious nodes increase from 70% to 90%, the success rate in abnormal scenes increases from 40% to 55%. When malicious organizations are dominant (malicious nodes account for 70%–90%), game–cogame relies on collaboration mechanisms to increase the detection success rate to a value that is higher than that of game-game (48.7% and 17.1% in two scenarios). By contrast, when malicious nodes are dominant, malicious nodes in cogame–cogame infer the strategy of detecting nodes. When the "detection node thinks that the best strategy is the refusal of forged report," the report is not forged. Thus, the occurrence rate of cogame-cogame malicious events in Figs. 7 and 9 is less than 30%, which is far lower than that of the other two methods, and the success rate of incident detection is high.

In a dynamic network, the report node cannot obtain all the data of the detection nodes, and the detection node cannot obtain the state of the uninteractive report node. Thus, an error occurs in the game. Therefore, the incident detection success rates of game–cogame and cogame–cogame contain errors, but the difference average is not higher than 15%. Similarly, few forgery reports are found in cogame-cogame, but they cannot be avoided completely. The two sides attain approximate bias equilibrium.

In the actual detection success rate, although the mechanism cooperation game method can effectively improve the success rate of incident detection, a delay occurs in the interaction between the nodes in an organization. A certain time is required for the updating of the weight of an organization in a dynamic network. If the node is unstable, a certain influence occurs on the detection results. Therefore, the detection success rate of cogame–cogame in both scenarios is not higher than 80%.

4.4 Deduction of the effect of feedback interaction on game

As mentioned above, the cooperative game (cogame–cogame) method can greatly reduce the generation of forged reports, but the data of the nodes in the dynamic reader network is partial. The detection node cannot completely obtain the inference result of the report node, but it will make an error generate. A malicious report node cannot obtain the inference result of the detection node completely. This situation results in the error in the next round of speculation node strategy, and malicious incidents occur. To reduce the number of malicious incidents, a detection node sends the information on weight reduction to the node after the malicious node is derived, so the malicious node may select not to forge a malicious report in the next interaction. Figures 10–13 show the effect of mechanism with and without feedback on a game. In the two scenarios, the number of forged reports produced by the method of inference feedback is 20% and 13% less than that in the absence of feedback. The reason is that when a malicious node forges a report, in the absence of feedback, the detection node detects malicious behavior and reduces its credibility. However, a malicious node does not know the malicious behavior and may continue to take a forged report next time.

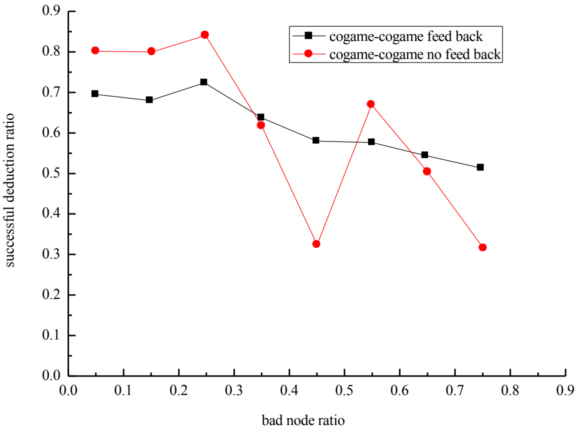

Fig. 10. Success rate of incident detection in normal scene

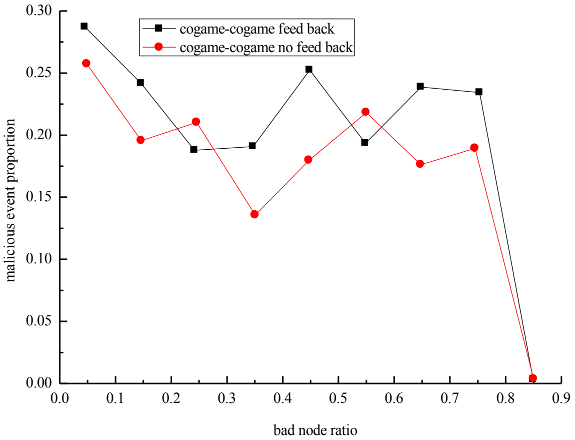

Fig. 11. Incidence rate of forged report in normal scene

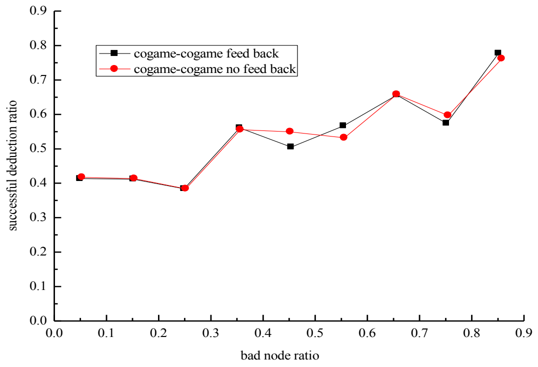

Fig. 12. Success rate of incident detection in abnormal scene

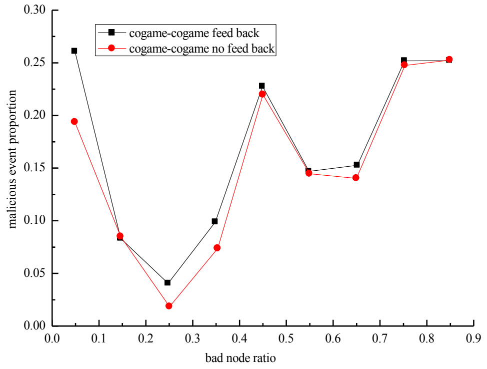

Fig. 13. Incidence rate of forged report in abnormal scene

5 Conclusion

In the IoT environment, the dynamic perception network is prone to have a malicious node dominant scenario, and most intrusion detection works cannot be directly applied. In this study, we define a malicious incident detection model. Although this model can effectively detect malicious incidents in the normal network, it cannot reduce the frequency of malicious attacks. Then, basing on the assumption that an attacker is intelligent, we propose a simple game method and construct a dynamic bias equilibrium by reasonably allocating a reward and punishment mechanism to a report node. However, in the network dominated by malicious organizations, this simple game cannot reach the bias equilibrium. Therefore, we further propose a cooperative game method. It is analyzed that the nodes and their organizations that are inconsistent with their own observations can effectively reduce the weight of the malicious report in the entire incident report. The new bias equilibrium is achieved and the malicious attack is further suppressed by node feedback. The results of our experiments indicate that simple and cooperative games effectively suppress malicious attacks in normal networks and networks dominated by malicious nodes.

6 References

[1] Chettri, R., Pradhan, S., Chettri, L. Internet of things: comparative study on classification algorithms (k-nn, naive bayes and case based reasoning). International Journal of Computer Applications, 2015, vol. 130(4), pp. 1009-1014. https://doi.org/10.5120/ijca2015907120

[2] Zeng, M., Wang, S. Fuzzy comprehensive evaluation algorithm for power information system security level based on the internet of things. International Journal of Online Engineering, 2016, vol. 12(5), pp. 17.

[3] Li, Z. A data classification algorithm of internet of things based on neural network. International Journal of Online Engineering, 2017, vol. 13(9), pp. 28. https://doi.org/10.3991/ijoe.v13i09.7587

[4] Li, C., Liu, Q., Wang, G. Integrity verification algorithm for remote data in internet of things based on bilinear pairings. Zhongnan Daxue Xuebao, 2014, vol. 45(11), pp. 3824-3831.

[5] Xie, M., Huang, M., Bai, Y., & Hu, Z. The anonymization protection algorithm based on fuzzy clustering for the ego of data in the internet of things. Journal of Electrical and Computer Engineering, 2017, vol. 17, pp. 1-10. https://doi.org/10.1155/2017/2970673

[6] Shamshirband, S., Amini, A., Anuar, N. B., Kiah, M. L. M., Ying, W. T., Furnell, S. D-ficca: a density-based fuzzy imperialist competitive clustering algorithm for intrusion detection in wireless sensor networks. Measurement, 2014, vol. 55(9), pp. 212-226. https://doi.org/10.1016/j.measurement.2014.04.034

[7] Tang, X. F., Niu, X. Z., Ali, S. Research on energy-aware topology strategy based on wireless sensor in internet of things. International Journal of Computational Intelligence Systems, 2014, vol. 7(6), pp. 1137-1147. https://doi.org/10.1080/18756891.2014.889858

[8] Lee, J. H., Jang, K. S., Kim, B. G., Jeong, S., Jin, S. C. Fast video encoding algorithm for the internet of things environment based on high efficiency video coding. International Journal of Distributed Sensor Networks, 2015, vol. 6, pp. 4. https://doi.org/10.1155/2015/146067

7 Author

Yue-e Yi is associate professor at the School of Changsha Social Work College, Changsha, China (yiyuee1981@21cn.com), His research interests include soft.

Article submitted 23 May 2018. Resubmitted 17 June 2018. Final acceptance 25 July 2018. Final version published as submitted by the authors.