J. Meas. Sci. Instrum., 2022, 13(1): 96-104
DOI: 10.3969/j.issn.1674-8042.2022.01.011
http://xuebao.nuc.edu.cn
jmsi@nuc.edu.cn

# Behavior analysis of malicious sensor nodes based on optimal response dynamics

GONG Junhui, HU Xiaohui, HONG Peng

(*School of Electronics and Information Engineering, Lanzhou Jiaotong University, Lanzhou 730070, China*)

**Abstract**: Wireless sensor networks are extremely vulnerable to various security threats. The intrusion detection method based on game theory can effectively balance the detection rate and energy consumption of the system. The accurate analysis of the attack behavior of malicious sensor nodes can help to configure intrusion detection system, reduce unnecessary system consumption and improve detection efficiency. However, the completely rational assumption of the traditional game model will cause the established model to be inconsistent with the actual attack and defense scenario. In order to formulate a reasonable and effective intrusion detection strategy, we introduce evolutionary game theory to establish an attack evolution game model based on optimal response dynamics, and then analyze the attack behavior of malicious sensor nodes. Theoretical analysis and simulation results show that the evolution trend of attacks is closely related to the number of malicious sensors in the network and the initial state of the strategy, and the attacker can set the initial strategy so that all malicious sensor nodes will eventually launch attacks. Our work is of great significance to guide the development of defense strategies for intrusion detection systems.

**Key words**: wireless sensor network; intrusion detection; malicious node; evolutionary game; optimal response dynamics

## 0 Introduction

Wireless sensor network is a multi-hop self-organized network formed by a large number of sensor nodes through wireless communication[1]. It is widely used in environment, industry, military, home and other fields. People can perceive all kinds of information in the real physical world through WSN, which greatly improves the ability of human beings to understand the objective world.

Due to limited resources, open wireless communication and complex working environment of sensor nodes, wireless sensor networks are vulnerable to various security threats. As an active defense technology, intrusion detection can effectively detect unsafe behaviors in the network. The operation of intrusion detection system needs to consume more resource overhead of sensor nodes, but the energy, computing and storage capacity of nodes are very limited. How to use intrusion detection system effectively in wireless sensor network is a very challenging task[2].

Game theory, a mathematical theory to study the competition phenomenon, has been used by many scholars in the research of wireless sensor network intrusion detection[3-5]. The antagonism of attack and defense in wireless sensor networks is just in line with the competitive and non-cooperative characteristics of game theory. Therefore, game theory can be used to formulate the best intrusion prevention strategy which is suitable for the characteristics of wireless sensor network[6]. A suitable detection strategy can balance the accuracy and energy efficiency of the system, and help wireless sensor networks to more effectively use IDS[7].

The detection method based on game theory has no training process and does not need additional data to build the model, so its complexity is lower than those of misuse detection, anomaly detection and other methods. Shen et al. used signal game to describe and analyze the interaction process between malicious sensor nodes and intrusion detection system in wireless sensor networks, established a repeated multi-stage signal game model, and realized the mechanism and algorithm of optimal intrusion detection strategy[8]. Huang et al. proposed Markov intrusion detection system algorithm based on misuse detection and anomaly detection, and inferred the

**Received date**: 2021-11-14
**Foundation items**: National Natural Science Foundation of China (No. 61163009)
**Corresponding author**: GONG Junhui (526413367@qq.com)

optimal defense strategy by using incomplete information static game[9]. Based on the prior probability of external nodes, Zhou et al. used Bayesian method to infer the posterior probability of malicious nodes in the following time, and made the best strategy on the proposed multi-stage dynamic intrusion detection game model[10]. In view of the diversity of attack methods and the limited resources in wireless sensor networks, Han et al. used the classical game theory to get the mixed strategy, Nash Equilibrium defense strategy, which balances the detection efficiency and resource cost of the system[11].

However, the traditional game models have some shortcomings. They use the assumption of complete rationality to find the optimal strategy through a game, but less consider the stability of the optimal strategy. These hypotheses are unreasonable in the real network confrontation. The irrationality of the hypotheses will lead to the deviation between the established model and the actual situation. The defense strategy based on the model is not suitable for the real scene, which reduces the guiding significance of the research results. Evolutionary game theory no longer uses the assumption that participants are completely rational in classic game theory. It uses the limited rationality of participants as the basis for game analysis, and emphasizes the dynamic changes in the game process[12].

If we know the stable attack behavior of malicious nodes, we can make better intrusion prevention strategies. Therefore, based on the theory of evolutionary game, we analyze the attack behavior of malicious sensors using the optimal response dynamic mechanism, and then obtain the stable attack behavior of malicious sensors.

## 1 Evolutionary game

Evolutionary game theory originated from Darwin's thought of biological evolution. It abandons the assumption of complete rationality in classical game theory and regards participants as individuals with limited rationality in biological groups. It combines game theory with dynamic evolution process[12]. Since it is impossible for participants to get the optimal strategy through one game, they need to correct the strategy through continuous trial, error correction and learning. Only through a rather complex and dynamic repeated long-term game process can they get the optimal strategy.

An important concept in evolutionary games is evolutionary stability strategy (ESS), which is used to analyze whether there is stable equilibrium in games under bounded rationality. The definition of evolutionary stability strategy is as follows.

Definition 1 Evolutionary stability strategy

We first define the strategy space is $S$, any strategy $y \neq x \in S$, and $u(x, x)$ represents the benefits of taking the strategy $x$, which is expressed as

$$\text{If } \exists\ \overline{\varepsilon_y} \in (0,1), \forall \varepsilon_y \in (0, \overline{\varepsilon_y}), \text{ and}$$
$$u[x, \varepsilon y + (1-\varepsilon)x] > u[y, \varepsilon y + (1-\varepsilon)x], \quad (1)$$

the strategy $x$ is a stable evolution strategy.

From the definition of evolutionary stability strategy, it can be seen that if the evolutionary stability strategy $x$ is adopted at the beginning of a group, the strategic income of the participants in the large group is always greater than that of the participants in the small group, that is to say, the group can resist the strategic invasion of the small group. If the strategy adopted by the group at the beginning is strategy $y$, the strategy income of the participants in the large group is always less than that of the participants in the small group, that is, the income of the strategy $y$ is always less than that of the evolutionary stability strategy $x$, therefore, the group will be successfully invaded by the evolutionary stability strategy $x$, and the members of the group will eventually adopt the evolutionary stability strategy.

The optimal response dynamic equation can be used to analyze the evolutionary stability strategy of small group members with fast learning ability[13].

## 2 Network model

Cluster routing protocol is used to divide the wireless sensor network into several interconnected clusters[14]. Each cluster has a cluster head node (CH) and several member nodes. The cluster head node is elected regularly, and it has no essential difference with the member nodes in the cluster.

Assuming that there are $N$ nodes in the wireless sensor network, the cluster routing protocol divides the network into $k$ clusters, which are recorded as $C_1, C_2, \cdots, C_k$, and the number of member nodes in each cluster is $M_i (i = 1, 2, \cdots, r)$. Fig. 1 shows the network model.

The energy consumption of nodes in wireless sensor networks is very limited, and the operation of IDS on each node will inevitably increase the energy

consumption of nodes and reduce the working time of nodes[15]. Therefore, we use distributed centralized hybrid intrusion detection system to balance the energy consumption and detection performance of the network. Distributed and centralized mixed mode refers to that every sensor node in the network has installed an intrusion detection system, but not all nodes run an intrusion detection system. In order to save energy consumption, only the intrusion detection system on the cluster head is opened to identify the attack behavior of malicious sensor nodes in the cluster.

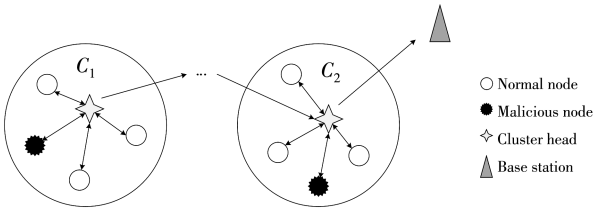


**Fig. 1 Intrusion detection network model of wireless sensor network**

When a sensor node is selected as a cluster head, its intrusion detection system will wake up at the same time, and the intrusion detection system on the member nodes in the cluster will be disabled. Therefore, in this study, cluster head node takes on the function of intrusion detection.

If there are multiple malicious nodes in the network, they can choose to attack the cluster head node, or they can choose not to attack and participate in the normal work of the network[16]. Previous research work usually assumes that malicious sensor nodes are completely rational and attack the network only once, which is not in line with the actual situation. Therefore, assuming that the malicious sensor nodes are limited rational, they attack the network many times, and their attack methods are various.

## 3 Game model

If the behavior of the malicious sensor node is known, the node can easily decide whether to start the intrusion detection system. If the malicious sensor node chooses to attack the network and the cluster head chooses not to turn on the intrusion detection system, it will suffer a heavy loss. If the malicious nodes choose to participate in the normal network operation instead of attacking the network, the cluster head can only waste energy to start the intrusion detection system.

The optimal response dynamics is one of the typical dynamic mechanisms in evolutionary game theory. Under this mechanism, participants lack the ability of accurate prediction in complex situations, but they have the ability of fast learning. After each game, participants will evaluate the results of the game and adjust their strategies accordingly.

According to the evolutionary game theory, the evolutionary game model of malicious sensor node attack based on the optimal response dynamics $RADEGM=(A,AS,P,U)$ is constructed.

1) $A=\{A_1,A_2,\cdots A_n\}$ is the set of all malicious sensor nodes, where $n$ is the number of attackers;

2) $AS=\{A,N\}$ is the attacker's strategy space, which $A$ means "attack", $N$ means "not attack";

3) $P=\{p_1,p_2\}$ is the set of attack probabilities for attackers, where $p_1$ represents the probability of the attacker to select strategy $A$, and $p_2$ represents the probability of the attacker to select strategy $N$;

4) $U=\{U_1,U_2\}$ is the set of profit functions under different strategies, where $U_1$ represents the attacker's benefit under strategy $A$, and $U_2$ represents the benefit of strategy $N$.

The malicious sensor nodes will destroy the network through cooperation, and they can be characterized as problems of cooperation and betrayal. In the context of evolutionary games, punishment can promote cooperation. When the strategies adopted by the two sides are different, malicious nodes will punish the traitors, that is, they would rather pay a certain price for themselves, but also make the traitors pay a heavy price.

Let $b_1$ be the benefit when both attackers choose not to attack, and $b_2$ be the benefit when both attackers choose to attack, and $b_2>b_1$. $\beta$ is the punishment that the attacker receives when betraying, $\gamma$ is the price paid by the attacker to punish the betrayer, and $\gamma>b_2-b_1$, $\beta>\gamma$. Their income matrix is shown in Table 1.

**Table 1 Benefit matrix of attacker**

| Strategy | Attack | Not attack |
|---|---|---|
| Attack | $(b_2,b_2)$ | $(b_2-\gamma,b_1-\beta)$ |
| Not attack | $(b_1-\beta,b_2-\gamma)$ | $(b_1,b_1)$ |

From the above benefit matrix, it can be seen that this game is a coordination game. Through analysis, we know this game model has two pure strategy Nash Equilibrium $(A,A)$ and $(N,N)$, in which strategy combination $(A,A)$ is Pareto optimal strategy, but considering the other party's rationality, the possibility of strategy combination $(N,N)$ is relatively large.

## 4 Analysis of game model

Based on the evolutionary game model of the optimal response dynamic attack, we use the optimal response dynamics to dynamically analyze the strategy changes between attackers to find out the stable attack behavior of attackers with the continuous evolution of time.

The optimal response dynamic equation[13] is

$$N_{t+1}=f(N_t)=\begin{cases}n, & U_1>U_2,\\ N_t, & U_1=U_2,\\ 0, & U_1<U_2,\end{cases} \tag{2}$$

where $N_t$ is the number of selection strategies among $n$ participants at time $t$.

The dynamic equation of optimal response shows that when the benefit of strategy $A$ is greater than that of strategy $N$, all participants can make the optimal response at the next moment, that is, all participants will adopt strategy $A$, otherwise all participants will adopt strategy $N$ at the next moment. When the two benefits are equal, the number of participants adopting strategy $A$ remains unchanged.

Based on the optimal response dynamic equation, it is assumed that all attackers play a circle game, that is, they are all in the same circle and play repeated games with their left and right neighbors. In the process of game, low-income people learn the attack strategy with higher profits than their own strategy.

Among the neighbors of attacker $i$, the number of neighbors who choose strategy $A$ is $q_{i,t}$ at time $t$, which can be 0, 1 and 2. Then the number of neighbors selecting strategy $N$ is $2-q_{i,t}$, which also has three values of 0, 1 and 2. When selecting strategy $A$ at time $t$, the benefit is $U_1=b_2q_{i,t}+(b_2-\gamma)(2-q_{i,t})$. Then the benefit of selecting strategy $N$ is $U_2=(b_1-\beta)q_{i,t}+b_1[2-q_{i,t}]$. Let $U_1=U_2$, then $q=\dfrac{2(\gamma+b_1-b_2)}{\beta+\gamma}$.

The change equation of the strategy obtained from the optimal response dynamic equation is

$$S_{i,t+1}=\begin{cases}A, & q_{i,t}>q,\\ S_{i,t}, & q_{i,t}=q,\\ N, & q_{i,t}<q,\end{cases} \tag{3}$$

where $S_{i,t}$ represents the strategy selected by attacker $i$ at time $t$.

Because $\gamma>b_2-b_1$ and $\beta>\gamma$, so $q<1$. Since $q_{i,t}$ can only take the values of 0, 1 and 2, $q_{i,t}$ can take the values of 1 and 2 when $q_{i,t}>q$, therefore, when an attacker has one or two neighbors who adopt strategy $A$ at time $t$, that is, as long as a neighbor chooses strategy $A$, it will adopt strategy $A$ at time $t+1$. When $q_{i,t}<q$, $q_{i,t}$ is only 0. Thus, when the attacker has not one neighbor who selects strategy $A$ at time $t$, that is to say, its neighbors all adopt strategy $N$, and it will adopt the strategy $N$ in at time $t+1$. To sum up, the attacker's strategy choice at time $t$ has nothing to do with itself, but depends on its neighbor's strategy choice at time $t$.

The number of players in a circle game will affect the result of the game. The following is a classification discussion of the circle game.

First, we discuss the case of odd numbers, assuming that there are five attackers distributed on the circumference. Because the attacker has two strategies to choose, the game has 32 initial states. According to the number of strategy $A$, all the initial states can be divided into 8 cases: $0A$, $1A$, adjacent $2A$, non-adjacent $2A$, adjacent $3A$, non-adjacent $3A$, adjacent $4A$, $5A$.

When all five attackers choose strategy $A$ or strategy $N$ at first, the strategies of all attackers will not change with the evolution of time.

If only one attacker chooses strategy $A$ at the beginning of the game, that is to say, the initial state is $(A,A,A,A,A)$, then after four stages of strategy evolution, all attackers finally reach the stable state of adopting strategy $A$. The change of strategy is shown in Fig. 2. It can be seen that the strategy change process has included three initial adjustment processes: non-adjacent $2A$, non-adjacent $3A$ and $4A$, which need three, two and one adjustment stages to reach stable state, respectively.

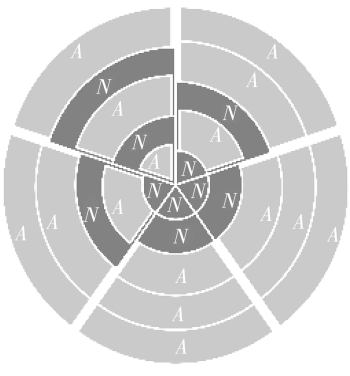

**Fig. 2 Evolution process in initial state $(A,A,A,A,A)$**

It can be seen from Figs. 3 and 4 that the adjustment process of two neighboring attackers adopting strategy $A$ only needs two stages, and three neighboring attackers adopting strategy $A$ only needs one stage.

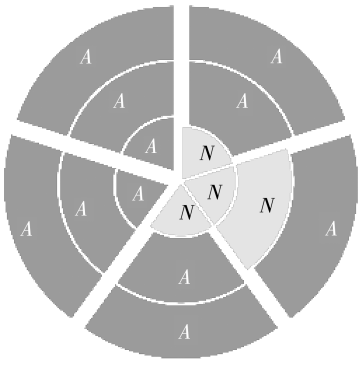

**Fig. 3 Evolution process in initial state (*A*,*A*,*N*,*N*,*N*)**

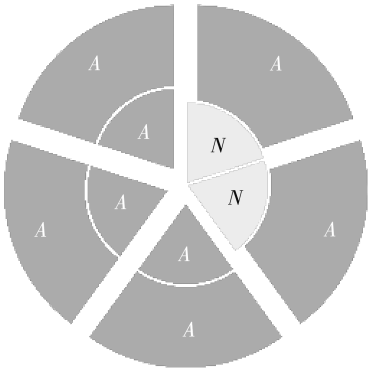

**Fig. 4 Evolution process in initial state (*A*,*A*,*A*,*N*,*N*)**

Next, we analyze the even number situation. Supposing six attackers are in six different positions of the circle, there are 64 initial states in the circle game. We only discuss some of them.

In Fig. 5, at the beginning of the game, if only one attacker uses strategy $A$, while other attackers use strategy $N$. The optimal response dynamic mechanism does not make the attackers' strategies converge to a stable state, but the strategies change back and forth between $(A,N,A,N,A,N)$ and $(N,A,N,A,N,A)$.

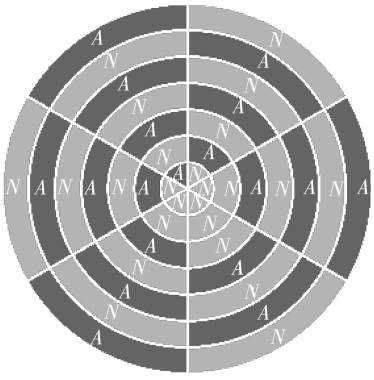

**Fig. 5 Evolution process in initial state (*A*,*N*,*N*,*N*,*N*,*N*)**

In Fig. 6, two non-adjacent attackers initially adopt strategy $A$, while other attackers adopt strategy $N$. After several rounds of evolution, the attacker's strategy does not tend to be stable, but falls into a cycle.

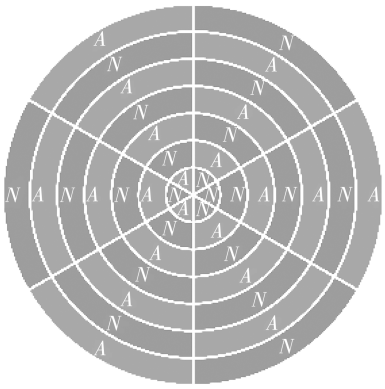

**Fig. 6 Evolution process in initial state (*A*,*N*,*A*,*N*,*N*,*N*)**

In Fig. 7, two attackers who are not adjacent to each other adopt strategy $A$, while other attackers adopt strategy $N$. Through repeated game adjustment, all attackers finally choose strategies, and the game reaches a stable state.

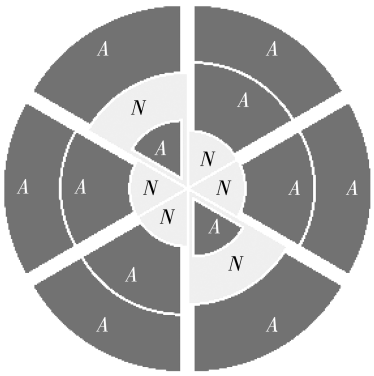

**Fig. 7 Evolution process in initial state (*A*,*N*,*N*,*A*,*N*,*N*)**

Through the above specific analysis, assuming that there are $n$ attackers in $n$ different positions on the circumference, the following general conclusions can be drawn.

**Conclusion 1** When $n$ attackers initially adopt the strategy $A$, the final stable state is that all attackers adopt the strategy.

**Conclusion 2** When $n$ is an odd number, if there is an attacker adopting strategy $A$ at the beginning of the game or in the process of the game, all the attackers finally adopt strategy $A$.

**Conclusion 3** When $n$ is an even number, if there are no two adjacent attackers using strategy $A$ at the same time at the beginning or in the process of the game, all attackers will not converge to a stable state and can only fall into periodic changes.

**Conclusion 4** When $n$ is an even number, if two adjacent attackers adopt strategy $A$ at the beginning of the game or in the process of the game, after a limited number of games, all the attackers will

eventually converge to the stable state of strategy $A$.

**Conclusion 5** By arranging the attacker's strategy, one of the above four conclusions will appear in the game, and they will follow the same evolutionary state in the future.

## 5 Experimental results and analysis

In the simulation experiment, python programming language is used to simulate the attack behavior of malicious sensor nodes in wireless sensor networks. One hundred sensor nodes are randomly deployed in the monitoring area. Once deployed successfully, the sensor nodes cannot be moved and their energy cannot be recovered. The base station is located outside the monitoring area and its energy can be recovered. In wireless sensor network, LEACH clustering protocol is used to divide the network topology. The probability of node being selected as cluster head is set to be 0.1, then there will be about 10 cluster heads in the network. The simulation parameters are shown in Table 2.

**Table 2 Network parameters**

| Parameter | Value | Description |
|---|---|---|
| $X$/m | 200 | Length of monitoring area |
| $Y$/m | 200 | Width of monitoring area |
| $N$ | 100 | Number of nodes |
| $B_X$/m | 100 | Abscissa value of base station |
| $B_Y$/m | 250 | Ordinate value of base station |
| $CP$ | LEACH | Clustering protocol |
| $P_c$ | 0.1 | Probability of being CH |
| $E_o$/J | 2 | Initial energy |
| $E_{elec}$/(nJ·bit) | 50 | Unit energy consumption for sending or receiving data |
| $E_{fs}$/(pJ·bit·m$^{-2}$) | 10 | Free space channel model |
| $E_{mp}$/(pJ·bit·m$^{-2}$) | 0.013 | Multi-path attenuation channel model |

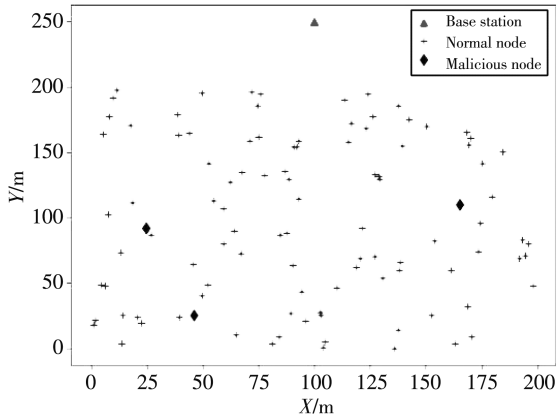


**Fig. 8 Network without clustering**

Firstly, there are three malicious sensor nodes in the network, which attack the cluster head. Fig. 8 shows the network topology when the network is not clustered, and Fig. 9 shows the network structure after adopting LEACH[17] clustering protocol.

The follow-up simulation experiments are carried out according to the parity of the number of malicious sensor nodes in the network.

Firstly, the number of malicious nodes in the network is set to be 5. According to the optimal response dynamic mechanism, the simulation experiment is carried out on the change of initial strategy of malicious nodes with time evolution.

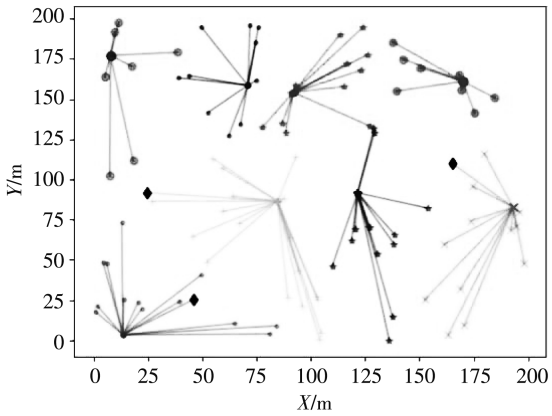


**Fig. 9 Network after clustering**

Figs. 10—12 show the change processes under different initial strategy states when there are five malicious sensor nodes in the network. When one, two or three malicious sensor nodes choose strategy $A$ in the initial stage of the game, the game eventually reaches a stable state with the passage of time, and all attackers choose strategy $A$. It can be seen from the changes of strategies in Figs. 10—12 that they are consistent with the conclusion. If the more malicious sensor nodes are chosen to attack at the beginning of the game, the faster the convergence speed will be.

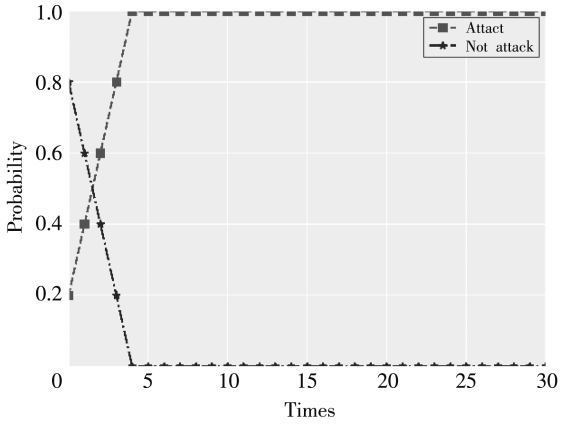


**Fig. 10 Changes of strategies with one strategy *A***

Next, the number of malicious nodes in the network is even.

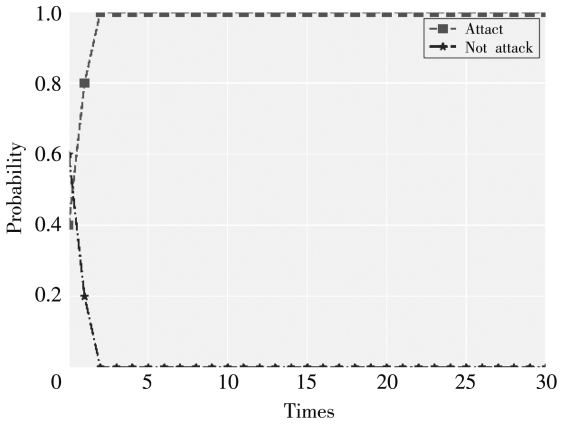


**Fig. 11 Changes of strategies with two strategies *A***

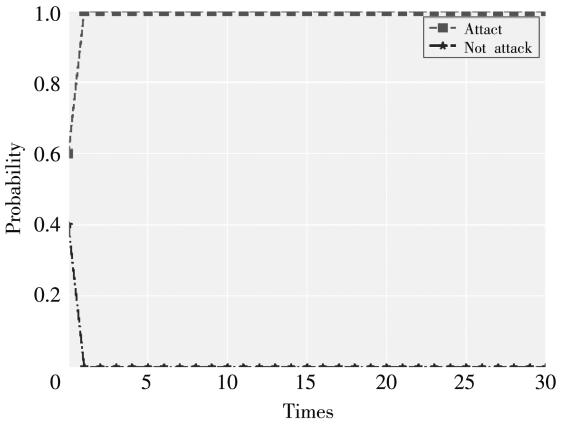


**Fig. 12 Change of strategies with three strategies *A***

The number of malicious nodes is changed to 6, and the simulation experiments are carried out under different strategies, which are $(A,N,A,N,N,N)$, $(A,N,A,N,N,N)$, $(A,A,N,N,N,N)$ and $(A,N,N,A,N,N)$.

Figs. 13 and 14 show that in the case of initial strategies $(A,N,A,N,N,N)$ and $(A,N,A,N,N,N)$, the system does not reach a stable state, and the probability of each malicious node selection attack is 50%.

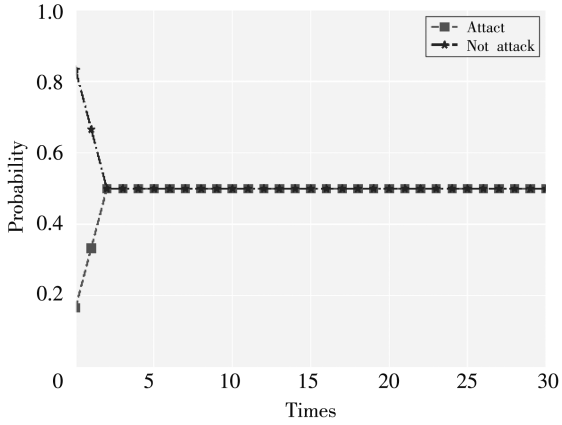


**Fig. 13 Changes of strategies under $(A,N,A,N,N,N)$**

Figs. 15 and 16 show that under the initial strategies $(A,A,N,N,N,N)$ and $(A,N,N,A,N,N)$, the system finally reaches a stable state, and the attacker finally chooses to attack. During the game where the initial strategies is $(A,N,N,A,N,N)$, two neighboring attackers adopt strategy $A$ at the same time. The experimental results are in line with the conclusion.

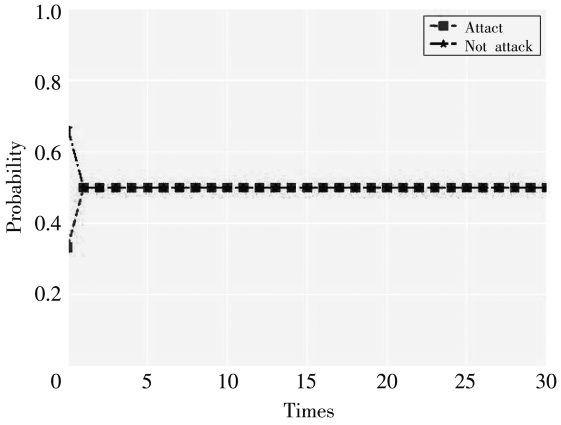


**Fig. 14 Changes of strategies under $(A,N,A,N,N,N)$**

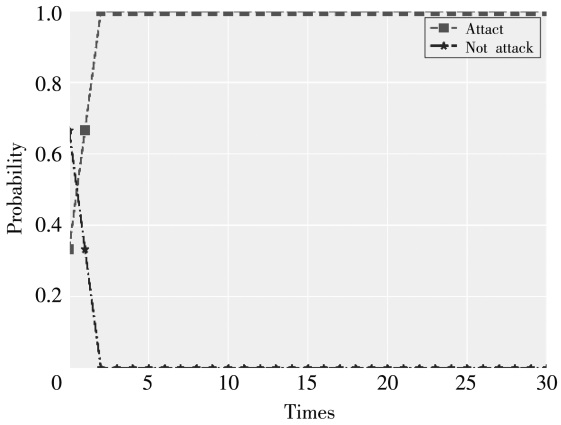


**Fig. 15 Changes of strategies under $(A,A,N,N,N,N)$**

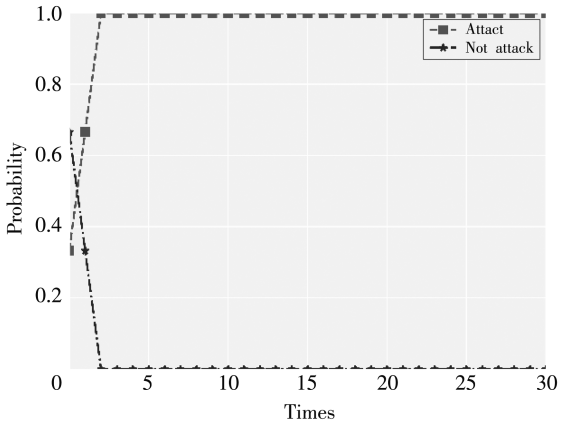


**Fig. 16 Changes of strategies under $(A,N,N,A,N,N)$**

The simulation results are consistent with the conclusion. The evolutionary game results of malicious nodes based on the optimal response dynamics are closely related to the number of attackers in the network and the initial strategies. However, the system will eventually reach a stable

state after continuous evolution by setting the initial strategies, that is, all malicious sensor nodes will launch attacks.

## 6 Conclusions

Starting from the limited rationality of malicious sensor nodes, we introduce the evolutionary game theory, constructs an attack evolutionary game model based on the optimal response dynamics, and analyzes the behavior of nodes based on the node benefit. The trend of attack evolution is closely related to the number of malicious sensor nodes in the network and the initial strategies. Since the attacker can set the initial strategies, all malicious sensor nodes will eventually attack the network. and the malicious sensor node will attack the cluster head, therefore the cluster head should start the intrusion detection system for defense. The simulation results show the rationality and validity of the evolutionary model, and provide substantive guidance for the subsequent development of defense strategy of intrusion detection system in wireless sensor networks.

## References

[1] BUTUN I, MORGERA S D, SANKAR R. A survey of intrusion detection systems in wireless sensor networks. IEEE communications surveys & tutorials, 2013, 16(1): 266-282.

[2] MITCHELL R, CHEN R. A survey of intrusion detection in wireless network applications. Computer Communications, 2014, 42: 1-23.

[3] MACHADO R, TEKINAY S. A survey of game-theoretic approaches in wireless sensor networks. Computer Networks, 2008, 52(16): 3047-3061.

[4] SHEN S, YUE G, CAO Q, et al. A survey of game theory in wireless sensor networks security. Journal of Networks, 2011, 6(3): 521.

[5] SHI H Y, WANG W L, KWOK N M, et al. Game theory for wireless sensor networks: a survey. Sensors, 2012, 12(7): 9055-9097.

[6] ABDALZAHER M S, SEDDIK K, ELSABROUTY M, et al. Game theory meets wireless sensor networks security requirements and threats mitigation: a survey. Sensors, 2016, 16(7): 1003.

[7] AGAH A, DAS S K, BASU K. A game theory based approach for security in wireless sensor networks//IEEE International Conference on Performance, Computing, and Communications, Apr. 17, 2004, Phoenix, AZ, USA. New York: IEEE, 2004: 259-263.

[8] SHEN S, LI Y, XU H, et al. Signaling game based strategy of intrusion detection in wireless sensor networks. Computers & Mathematics with Applications, 2011, 62(6): 2404-2416.

[9] HUANG J Y, LIAO I E, CHUNG Y F, et al. Shielding wireless sensor network using Markovian intrusion detection system with attack pattern mining. Information Sciences, 2013, 231: 32-44.

[10] ZHOU W, YU Bin. Optimal defense strategy in WSNs based on the game of multi-stage intrusion detection. Journal of Electronics & Information Technology. 2018, 40(1): 63-71.

[11] HAN L, ZHOU M, JIA W, et al. Intrusion detection model of wireless sensor networks based on game theory and an autoregressive model. Information Sciences, 2019, 476: 491-504.

[12] LOPEZ DELGADO M. On the effectiveness of intrusion detection strategies for wireless sensor networks: an evolutionary game approach. Ad hoc & Sensor Wireless Networks, 2017, 35(1/2): 25-40.

[13] WANG X, LI Y. Best-response dynamic model for Gencos' bidding strategies in regional electricity. Journal of North China Electric Power University, 2006(6): 51-54.

[14] SUBBA B, BISWAS S, KARMAKAR S. A game theory based multi layered intrusion detection framework for wireless sensor networks. International Journal of Wireless Information Networks, 2018, 25(4): 399-421.

[15] GHOSH D, SHARMA A, SHUKLA K K, et al. Globalized robust Markov perfect equilibrium for discounted stochastic games and its application on intrusion detection in wireless sensor networks: Part I—theory. Japan Journal of Industrial and Applied Mathematics, 2020, 37(1): 283-308.

[16] ZHANG W, HAN D, LI K C, et al. Wireless sensor network intrusion detection system based on MK-ELM. Soft Computing, 2020, 24(2): 1-14.

[17] HEINZELMAN W B, CHANDRAKASAN A P, BALAKRISHNAN H. An application-specific protocol architecture for wireless microsensor networks. IEEE Transactions on Wireless Communications, 2002, 1(4): 660-670.

# 基于最优反应动态的恶意传感器节点行为分析

巩俊辉，胡晓辉，洪　鹏

（兰州交通大学 电子与信息工程学院，甘肃 兰州 730070）

**摘　要：** 无线传感器网络极易遭受各种安全威胁，基于博弈论的入侵检测方法能有效平衡系统的检测率和能耗，对恶意传感器节点攻击行为的准确分析有助于更好地配置入侵检测系统，减少不必要的系统消耗，提升检测效率。但是，传统博弈模型的完全理性假设常常导致建立的模型与实际攻防场景不符，为了能够制定合理且有效地入侵检测策略，引入了演化博弈论，建立了基于最优反应动态的攻击演化博弈模型，对恶意传感器节点的攻击行为进行了分析。理论分析和仿真实验结果表明，攻击演化趋势与网络中恶意传感器数量的奇偶性以及策略的初始状态密切相关，攻击者可以通过设定初始策略使所有恶意传感器节点最终都会发起攻击。该研究对指导制定入侵检测系统的防御策略具有重要意义。

**关键词：** 无线传感器网络；入侵检测；恶意节点；演化博弈；最优反应动态

**引用格式：** GONG Junhui, HU Xiaohui, HONG Peng. Behavior analysis of malicious sensor nodes based on optimal response dynamics. Journal of Measurement Science and Instrumentation, 2022, 13(1): 96-104. DOI: 10.3969/j.issn.1674-8042.2022.01.011