Equilibrium Strategy of Attack and Defense in Computer Networks Based on Markov Signal Game Theory

Xue Bai[1,*] and Yongguo Bai[2]

[1]*Information Center, Jilin Institute of Chemical Technology, Jilin, 132022, China*
[2]*College of Information & Control Engineering, Jilin Institute of Chemical Technology, Jilin, 132022, China*
E-mail: jlbaixue@126.com
[*]*Corresponding Author*

Received 11 May 2024; Accepted 11 January 2025

Abstract

In actual network attack and defense, the information between the two sides is often unbalanced and asymmetric, and the defender cannot fully understand the attacker's true intentions and attack methods. At the same time, the complexity, rapid changes, and limited resources of network attack and defense make it crucial to optimize network defense strategies. The moving target defense strategy is introduced, and the moving target Markov signaling game defense strategy is built to optimize the defense decision. PageRank algorithm is applied to compute the stage weight value in the multi-stage process. The refined Bayesian equilibrium of the model is calculated. From the results, when the security resources were 8, the average defender profit was −0.95, which was 3.11 and 19.15 higher than that of the single-stage Stackelberg and the equitable distribution model, respectively. The average attacker profit was below the other models when the number of security resources was less than 10. Among them, when the number of security resources was 4,

Journal of Cyber Security and Mobility, Vol. 14_1, 127–154.
doi: 10.13052/jcsm2245-1439.1416

the average profit of attackers in the moving target Markov signaling game defense model was only 1.78, which was significantly lower than that of the single-stage Stackelberg model and the equitable distribution model. In addition, the detection/defense success rate proposed by the research is the highest. This proves that the model proposed in the study can effectively enhance the defense ability against network attacks, greatly improve network security defense technology, and provide new reference technologies for network security maintenance.

Keywords: Markov, signal game, network attack and defense, PageRank, refined Bayesian equilibrium.

1 Introduction

While the rapid progress of the Internet has brought convenience, it has also caused many network security problems. Data theft, network spoofing, security vulnerabilities and other network security problems are increasingly serious, which poses a huge threat to the security of computer network system [1]. To better deal with network attacks, researchers in related fields have designed various defense means. However, these strategies have not produced significant effects on network defense. While the network defender updates the defense technology, the attack technology is also improving, showing high concealment and long duration [2]. Among them, Advanced Persistent Threat (APT) has become the mainstream in the field of network attack. In the current network environment, network security accidents occur frequently, and attackers have a great advantage in attack cost, time and other aspects [3]. The general network defense system has some defects such as similarity and static, strong lag and passivity, and high defense costs [4]. The current research gap lies in the frequent occurrence of misjudgment of defender types due to the confusing effect of defense signals, and the limited selection of effective and accurate means for different strategies for different attacks. It is of great significance to explore how to seek more effective defense strategies on the basis of reducing system losses.

In recent years, active defense technology has gradually come into people's vision. Moving Target Defense (MTD), which aims at attacking attackers, is gradually applied to network security. MTD is a method proposed by the National Science and Technology Commission of the United States to transform the defense defects of existing information systems based on dynamic, randomized and diversified ideas. The core of MTD is to

increase the attack difficulty of network attackers by building a dynamic, heterogeneous and uncertain cyberspace target environment. The randomness and unpredictability of the system are used to combat network attacks. However, the difficulty of MTD is the optimal decision problem. Game theory is a mathematical theory and analytical tool that studies the competitive phenomenon of two or more people interacting with each other. It is applied to decision-making problems in various fields, and the basic characteristics of its research content are consistent with the characteristics of the MTD attack defense confrontation process. Applying game theory to network attack and defense adversarial analysis and studying the selection of MTD defense strategies has become trending topics in research in the field of network attack and defense. Currently, several advanced new types of network attack and defense game models include evolutionary game models, time game models, stochastic game models, differential game models, and signal game models. Among them, the evolutionary game model conforms to the characteristics of actual network attack and defense confrontation, but has the disadvantage of replicating dynamic learning mechanisms that are difficult to objectively describe the behavior of players in the game. The time game model has good applicability in describing the control rights of both attack and defense parties over system resources, but its scalability is correspondingly reduced. The stochastic game model can effectively analyze the randomness and dynamics of network attack and defense processes, but the determination of state transition probability is somewhat subjective. The differential game model well describes the characteristics of time continuity and dynamic changes in the process of network attack and defense confrontation, but the disadvantage is that the model construction and equilibrium solution are relatively complex, which increases defense costs. Compared with other models, the signal game model has a good effect in describing the impact of attack and defense information on attack and defense decisions and equilibrium. It affects the game process through the signal sending mechanism. The signal receiver is not fully aware of the type of signal sender, but will have some understanding before making a decision. When receiving the signal from the sender, it makes corrections to existing judgments and selects the optimal strategy.

Network defense exerts a crucial function in maintaining the security of computer network systems, devices, and data. Sun Z et al. found that the number of nodes in intelligent transportation systems continued to increase, posing serious threats to the security of vehicle networks. The study introduced a game theory to analyze the individual or group behavior of communication entities in virtual networks. This method could effectively

improve the security of the network [5]. Zhu M et al. built a defensive deception strategy for network defense. Through this method, defenders could prevent network attacks by luring and misleading attackers. This method also incorporated machine learning algorithms to enhance network defense effectiveness. The results indicated that the proposed defensive deception method could effectively maintain network security [6]. Zhang Z et al. found that APT posed a serious threat to edge devices with limited resources. An interpretable intelligent driven edge defense mechanism was proposed. This mechanism implemented resource allocation based on deep reinforcement learning. The proposed mechanism could improve the defense capability of APTs and the edge protection level [7]. Zhang Z et al. proposed an information physical collaborative defense strategy to address the risk of power outages during network attacks. At the same time, a zero sum multi-level Markov Stackelberg game model was introduced at the network layer. The results indicated that the proposed defense strategy effectively reduced risk, which had better performance [8]. To avoid unplanned load shedding caused by malicious network attacks, Shao C W constructed a two-layer defense resource allocation optimization framework and solved the model framework using a binary algorithm. The model and solution strategy had significant application effects in IEEE 14 and IEEE 118 node system experiments [9]. In response to the impact of selfish behavior on the security and throughput of the blockchain network of newer proof-of-stake (PoS) systems during block propagation (or rumors), Abbasihafshejani M et al designed a role-based approach for selfish node detection, and the results proved the effectiveness of this technique in improving the throughput of the algorithm [10]. Abolfathi M et al. developed a multi-path routing and spoofing method to protect user privacy in response to complex network traffic attacks. The results show that this method can significantly reduce the accuracy of network attacks [11].

Game theory is a mathematical theory that studies decision-making and strategy. In the field of network security, the interaction between network systems and attackers can be seen as a game process. Researchers such as Abdalzaher M S developed a repeated game model for the feasibility management of power and data in the Internet of Things. This model could enhance data credibility against selective forwarding attacks and detect hardware failures of cluster members. Compared with non cooperative defense mechanisms, the proposed mechanism improved the performance of data credibility against selective forwarding attacks [12]. Hu H et al. found that there were certain difficulties in selecting the optimal defense strategy with the highest returns. A stochastic evolutionary game strategy was proposed

to simulate dynamic opponents in attack and defense. Meanwhile, the team adds relevant parameters to the Logit quantum reaction kinetics equation. The results showed that this method was helpful in selecting the optimal defense strategy, which could achieve the maximum return rate [13]. To solve the hidden link flooding attacks, Aydeger A et al. proposed a mobile target defense technology that dynamically changed network settings to deceive attackers. At the same time, signal game was introduced to construct a belief function to select the best response. The results showed that this method effectively improved the protection level of hidden link flooding attacks and reduced network overhead [14]. For power allocation under intelligent interference attack, Liu j et al. analyzed the interaction between intelligent jammer and cluster head node using Stackelberg game framework. Among them, the intelligent jammer used the deep neural network to infer the jamming power and took it as the attack strategy. Numerical simulation results showed that the proposed mechanism was significantly better than other allocation mechanisms [15]. For denial of service attacks in secondary control, Zhang B et al. developed a defense mechanism ground on evolutionary game. This mechanism mainly constructed a small signal model. The evolutionary game was applied to find the optimal defense strategy. The results showed that this method achieved remarkable results in network defense [16]. Falsafain H et al. designed a binary integer linear programming formula to address the combinatorial programming problem and proposed a branch and price framework, which proved to require less computational effort [17]. In order to study the equilibrium mechanism in price competition, Fadavi N regards competition as a one-time pricing game in view of the remaining sales period and the current demand pattern, so as to obtain the optimal response to determine the seller, and the results prove that the subgame perfect Nash equilibrium plays an effective role in mixed strategies [18].

Previous studies have proposed various network defense strategies, including the game theory. However, few scholars use Markov signal game defense model for network defense. At the same time, in order to solve the problem of network security, an effective active defense technology is urgently needed. Moving target defense is a kind of active defense technology which constructs dynamic, heterogeneous and uncertain environment for target information system to defeat the attacker and then prevent the attack. Game theory has a significant advantage in the analysis of network security problems because of its process characteristics and network attack and defense process. This paper applies a new Game Model to the research of network offensive and defensive decision-making in Moving Target Defense,

and proposes a Moving Target Markov Signaling Game Defense Model (MTMSGDM). It is used in defense decision making to improve active defense capability. The innovation of the research lies that the Markov signal game theory is used to build a MTD game model. It fully combines the characteristics of dynamic, random and diversified, helping to better respond to network attacks and improve network security.

2 Methods and Materials

In view of the unequal information between the attack and defense sides, an active defense method, MTD, is proposed. On this basis, the MTMSGDM is constructed. In this model, the PageRank is applied to calculate the stage weight value in the multi-stage process. Then, the game process of MTMSGDM is introduced, and the refined Bayesian equilibrium is solved. Finally, the overall process of MTMSGDM defense decision optimization algorithm is introduced.

2.1 Construction of Moving Target Markov Signaling Game Defense Model

In the actual network attack and defense, the ways for attackers to obtain security defects and vulnerabilities include active attack and passive attack, and the attack objects are resources and systems. It is often difficult for the defender to achieve zero defects and zero vulnerabilities in the design of the system, thus being attacked [19, 20]. In fact, the information between the attack and defense sides is often unbalanced and asymmetric. To change this situation, an active defense method, MTD, is introduced. In this method, the defender publishes real or false network system and resource information on the network, so as to induce the attacker to make wrong judgments and decisions, and improve the attack difficulty of the attacker. When an attacker receives such false information, due to his limited ability, misjudgment often occurs, which leads to the wrong attack method and the loss of attack [21–23]. Signal game is an incomplete dynamic game model involving information transmission. The model includes two participants, the sender and the receiver. First, the signal sender sends a signal about its own type to the receiver, and then the receiver takes action depending on the received signal. The final benefits of both parties depend on the sender type, the signal selected by the sender and the actions of the receiver [24, 25]. To achieve active defense, the research takes the defender as the sender and the

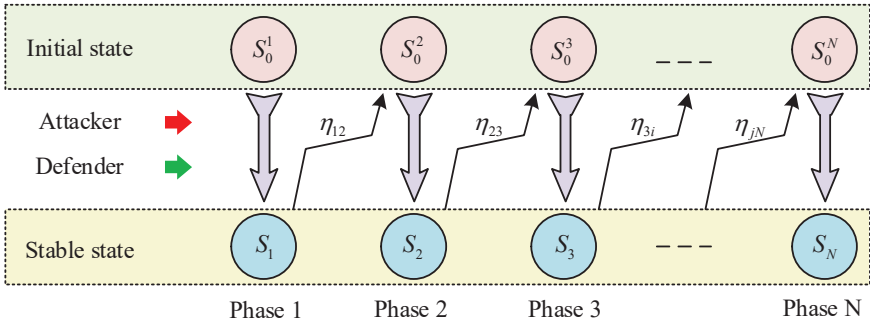


Figure 1 Schematic diagram of multi-stage attack and defense game process.

attacker as the receiver. The minimum risk Bayesian decision of the attacker is applied to quantify the benefits of the attacker. The network attack and defense process has multiple stages. The multi-stage attack and defense game process is displayed in Figure 1.

In Figure 1, S_0 and S_1 respectively represent the initial and stable states of each stage. Under the action of the attacker and defender, the game system enters the stable state of this stage from the initial state. Because the environment is changing all the time, the stable state of one stage is difficult to maintain. It will enter the initial state of the next new stage according to the state transition probability η, thus forming a multi-stage process of network attack and defense. In view of this characteristic, Markov decision process is introduced into the basic signal game model, and the MTMSGDM model is constructed. The assumption of this model is that attackers always pursue the minimum cost and the maximum return. At the same time, the attacker aims to improve its attack authority in the target system. The ultimate goal of attackers is to enhance their attack privileges in the target system, that is, to capture the target system or obtain higher privileges, so that subsequent attacks can be more effective. Defenders mainly induce attackers to react by releasing signals. The defender does not know the exact type of attacker, but can infer the attacker's choice through game strategies. In MTMSGDM, the set of attackers and defenders is represented as Equation (1).

$$N = \{N_a, N_d\} \tag{1}$$

In Equation (1), N_a signifies the attacker. N_d is the defender. The type space representation of both is shown in Equation (2).

$$\Phi = \{\Phi_a, \Phi_d\} \tag{2}$$

The type set of the two sides is shown in Equation (3).

$$\begin{cases} \Phi_d = \{\phi_d^1, \phi_d^2, \ldots, \phi_d^n\} \\ \Phi_a = \{\vartheta\} \end{cases} \tag{3}$$

The attacker cannot obtain the defender type information, but has a priori probability to judge the defense type Φ_d. The attacker does not know the exact strategy of the defender at the beginning of the game, but they will form a probability distribution based on previous experience, observed signals, or existing information in the environment to estimate the likelihood of the defender adopting different defense types. This prior probability setting reflects the incompleteness of the attacker's information and how the attacker makes the optimal decision in an incomplete information environment. The type of signal released by the defender is shown in Equation (4).

$$M = \{m_1, m_2, \ldots, m_n\} \tag{4}$$

The defense strategy and attack strategy are shown in Equation (5).

$$\begin{cases} D = \{d_1, d_2, \ldots, d_g\} \\ A = \{a_1, a_2, \ldots, a_h\} \end{cases} \tag{5}$$

The attacker' prior probability to the defense type is shown in Equation (6).

$$p_k = \{p_1^k, p_2^k, \ldots, p_n^k\} \tag{6}$$

In Equation (6), k represents the stage k, and $k \in [1, T]$. T signifies the total stages of the multi-stage game. p_k^* is a posteriori probability of the attacker to the defense type. The income function of both sides at stage k is shown in Equation (7).

$$U_k = (U_A^k, U_D^k) \tag{7}$$

In the Markov process, the income function of the offensive and defensive sides is mainly calculated through the discount expectation function. For the stage weight value in multi-stage process, PageRank algorithm is used. This algorithm is a classic representative of graph link analysis and a typical unsupervised learning method on graph data. The algorithm ranks the importance of web pages ground on the link value between web pages, which is used to measure the importance of a specific web page relative to other web pages. The algorithm contains two basic assumptions. First, the more links a web page receives, the more important it is. Second, when a high-quality web page points to another web page, it means that the page pointed to is important.

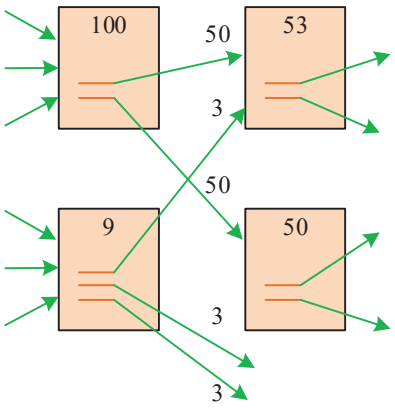


Figure 2 PageRank value allocation diagram.

The nature of the algorithm includes the transitivity of PageRank value and the transitivity of importance [26–28]. The PageRank algorithm is based on the random surfer model, and its basic idea can be summarized as follows: the algorithm evaluates the importance level of each webpage based on the link relationship between webpages. The PageRank value of a webpage not only considers the number of links pointing to it, but also the importance of other webpages pointing to it. The basic principle of calculating stage returns using the PageRank algorithm is based on the importance assessment of network graph models and links. It not only considers the number of links directly pointing to the current stage, but also the importance of these links themselves, in order to comprehensively evaluate the relative importance or potential of each stage in the entire network. When page A directs to B, the PageRank value of A will also be passed to page B. At the same time, the weight of a web page with high importance is greater than that of a web page with low importance. The PageRank value allocation diagram is shown in Figure 2.

There are two links in a page with a PageRank value of 100, so they are assigned to both linked pages. Then it allocates according to the PageRank value of the linked page itself, and finally makes the pages in the whole network have a stable PageRank value. PageRank is calculated, as shown in Equation (8).

$$PR(p_i) = \alpha \sum_{p_i \in M_i} \frac{PR(q_j)}{L(q_j)} + \frac{1-\alpha}{N} \tag{8}$$

In Equation (8), PR is the PageRank value. q_i stands for the i-th page. M_i signifies the set of inbound links to q_i. q_j stands for page j. L represents the number of outgoing links. α indicates the probability that the user will not jump randomly. α stands for the number of all pages. The PR of all web pages is shown in Equation (9).

$$R = \begin{bmatrix} PR(q_0) \\ PR(q_1) \\ \dots \\ PR(q_n) \end{bmatrix} \tag{9}$$

If there are m links pointing to web page q_i, the calculation is shown in Equation (10).

$$il(p_i, p_j) = \frac{m}{sum} \tag{10}$$

In Equation (10), sum represents the sum of the j-th column of matrix R, which is the total number of outer chains q_j. This can prove that the calculation process of PR value is a Markov process. As the model proposed in the study is a multi-stage Markov process, the PageRank algorithm is applied to calculate the stage weight values in the multi-stage process of the model. At the same time, because the PageRank algorithm also introduces random jump operations on the standard Markov chain, this is similar to the multi-stage and multi-state transition process of studying network attack and defense models. So the research introduces the PageRank algorithm to analyze the multi-stage process of network attack and defense, constructs the PageRank link analysis algorithm for the multi-stage state transition diagram of moving target Markov signal game, and obtains the weight values of each stage. In addition, to improve the ability to effectively detect and bind network attacks, research has combined methods of network security situational awareness, including multi-source data correlation analysis and real-time threat assessment, to improve the effectiveness and response speed of network security defense. Among them, multi-source data correlation analysis collects information from multiple data sources (such as network traffic, logs, terminal behavior data, etc.) to achieve network data integration and cleaning, thereby constructing a network security view. Subsequently, statistical analysis techniques were used to identify abnormal activities and potential security threats. At the same time, real-time threat assessment is used to continuously monitor information from various threat intelligence sources, assess the current threat level and potential impact on the organization, and

establish a rapid response mechanism to quickly take action to block attack traffic and achieve real-time updates of protection strategies.

2.2 Game Equilibrium Solution and Defense Decision Algorithm Design

The game process of MTMSGDM has several stages. Attackers will continuously adjust their belief inference and adopt effective attack strategies based on defense signals. On the other hand, the defender will adopt effective defense strategies ground on the observed attack strategies. The specific game sequence is shown in Figure 3.

In Figure 3, at the beginning of the attack and defense, the defender selects a type from different types, and the attacker does not know the specific type but has a prior belief. Then the defender releases a signal to interfere with the attacker's inference, guiding them to make incorrect decisions. Subsequently, the attacker acquires the signal and makes an attack decision, updating the posterior probability inference of the defender type. Next, the defender makes defense decisions based on the signal and conducts defensive attacks. Finally, the attacker adopts the updated posterior probability

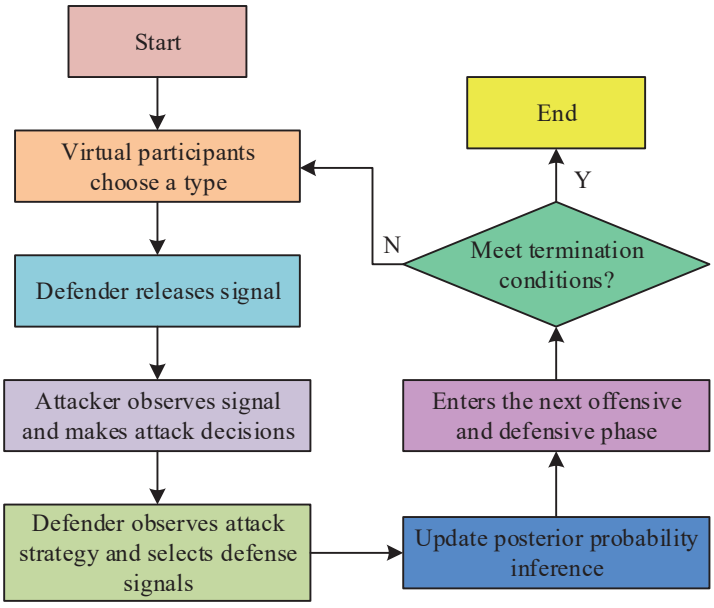


Figure 3 The game order of MTMSGDM.

inference as a prior belief for the defender type in the next stage. Then the operation enters the next attack and defense stage. The above operations are repeated until the attack and defense end. Due to the fact that MTMSGDM is an incomplete information dynamic game, analyzing the game equilibrium of this model is equivalent to analyzing the refined Bayesian equilibrium [29–31]. In the k-th stage, the optimal attack strategy with the highest profit is calculated, as shown in Equation (11).

$$a^{k*} = \arg\max \left(U_A^k(a^{k*}, m^{k*}, d^{k*}) + \sum_{h=k}^{T} \xi^h \eta_{kh}(S_0^h | S_k) R_A^k(S_0^h, S_h) \right) \tag{11}$$

After foreseeing the optimal attack strategy in the k-th stage, the defender selects the optimal defense strategy that maximizes the cumulative benefit of defense, as shown in Equation (12).

$$\begin{aligned} & m*(\phi_d, d*) \\ & \quad = \arg\max \left(U_D^k(a^{k*}, m^{k*}, d^{k*}) + \sum_{h=k}^{T} \xi^h \eta_{kh}(S_0^h | S_k) R_D^k(S_0^h, S_h) \right) \end{aligned} \tag{12}$$

The MTMSGDM single stage process has a refined Bayesian equilibrium, which is calculated in Equation (13).

$$EQ = (m*(\phi_d, d*), a*(m), p*(\phi_d|m)) \tag{13}$$

In Equation (13), $m*(\phi_d, d*)$ represents the signal released by the defender of type ϕ_d. The defense strategy is $d*$. $a*(m)$ represents the optimal attack decision taken by the attacker based on the signal released by the defender. $p*(\phi_d|m)$ represents the posterior inference probability in the game process, which is mainly calculated based on defense signal m, prior probability inference p, and the attacker's optimal strategy $a*(m)$. The refined Bayesian equilibrium solution process of MTMSGDM is shown in Figure 4.

In Figure 4, the refined Bayesian equilibrium solution first requires constructing a posterior inference probability $p*(\phi_d|m)$ during the game process. Next, the optimal attack strategy $a*(m)$ corresponding to the attacker is calculated. In this stage, when the attacker obtains the signal m released by the defender, ground on the posterior probability inference of the defender type,

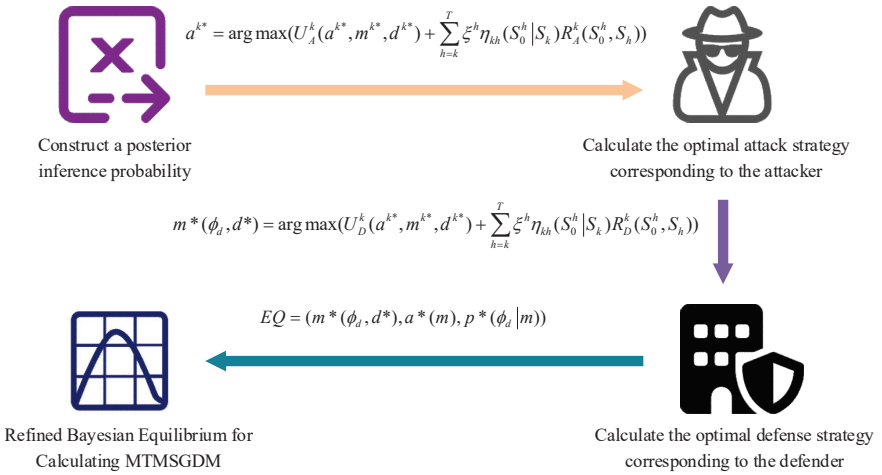


Figure 4 The solution process of refined Bayesian equilibrium of MTMSGDM.

the optimal attack strategy that maximizes the attack benefit U_A is selected, that is, the attacker selects the corresponding optimal attack strategy $a*(m)$ through calculation. On this basis, the optimal defense strategy $m*(\phi_d, d*)$ corresponding to the defender is calculated. In this process, the defender anticipates that the attacker will select the optimal attack strategy $a*(m)$ according to the signals released by the attacker, and therefore selects the defense strategy $m*(\phi_d, d*)$ with the maximum defense benefit U_D, that is, the defender selects the corresponding optimal decision through calculating $\max U_D(\phi_d, a*(m), m)$. Finally, $p*(\phi_d|m)$ is deduced according to the posterior probability calculated by the attacker's optimal strategy $a*(m)$, defender's optimal strategy $m*(\phi_d, d*)$ and Bayes' rule. When $p*(\phi_d|m)$ and $p(\phi_d|m)$ do not conflict, $EQ = (m*(\phi_d, d*), a*(m), p*(\phi_d|m))$ is a refined Bayesian equilibrium. According to this solution process, the refined Bayes equilibrium of each stage in the process of network attack and defense can be obtained successively.

The proposed game process is a finite time step Markov Decision Process (MDP), so there is at least one global optimal solution that can be obtained using dynamic programming methods. Dynamic programming can transform multi-stage processes into single-stage problems. The discount factor is introduced to transform MTMSGDM into a dynamic programming problem that solves the maximum value with the overall profit as the objective criterion function. The defense decision optimization algorithm flow of MTMSGDM is shown in Figure 5.

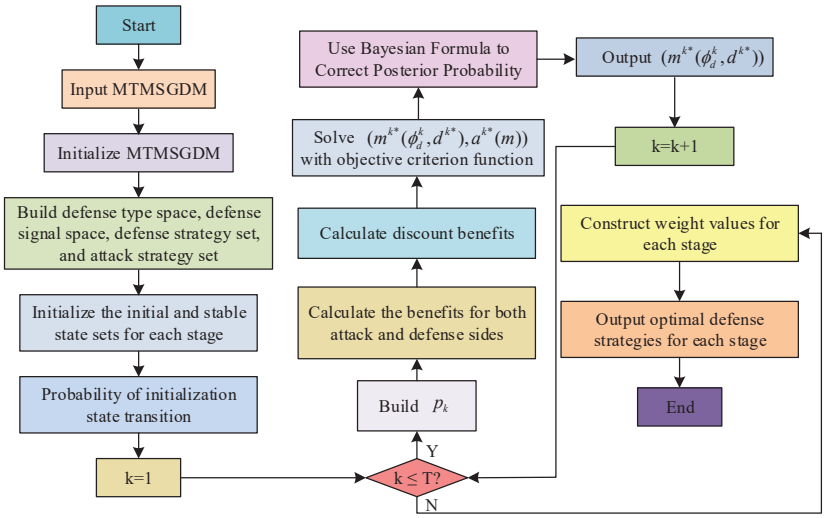


Figure 5 Optimization algorithm process for defense decision of MTMSGDM.

According to the equilibrium analysis of the algorithm, the calculation process of refined Bayesian equilibrium in a single-stage attack and defense game determines the time complexity. If the type space of the defender is n, and $r = \max(g, h)$, then the time complexity is $o(r^3 + n^2 + 2n)$. The storage space mainly stores the intermediate results of the attack and defense benefits and equilibrium calculation process in each stage, with a spatial complexity of $o(nr)$.

3 Results

To prove the effectiveness of the MTMSGDM, simulation analysis is conducted. Firstly, a system topology diagram is constructed and specific vulnerability information is introduced. Next, the MTD offensive and defensive confrontation is divided into 7 stages. The offensive and defensive benefits and PageRank weight values of each stage are analyzed. Subsequently, the attack and defense benefits and detection/defense success rates of different models are verified under different numbers of security resources.

3.1 Analysis of Game Equilibrium Strategies at Different Stages

To demonstrate the MTMSGDM, a simulation system is constructed for experiments. The system includes a client, a Web server, network defense

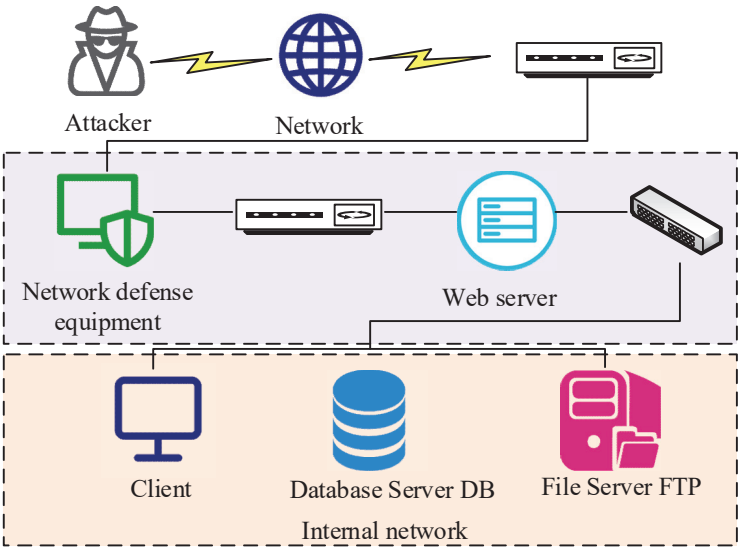


Figure 6 System topology diagram.

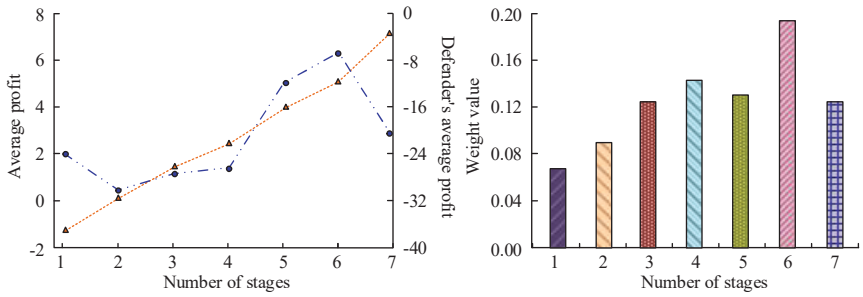
devices, a File Transfer Protocol Server (FTP), and a Database Server (DB). The system topology diagram is shown in Figure 6.

The Nessus tool is used to scan simulation systems and combine data from the National Information Security Vulnerability Database to obtain vulnerability information of devices in the system. The vulnerability information is displayed in Table 1.

MTD offensive and defensive confrontation is divided into 7 stages, each of which includes an initial state and a stable state, with a total of 14 states. The discount factor is 0.4. The Pycharm2020.2.3 tool is used to measure the objective criterion function values for each stage. On this basis, the optimal defense strategy and the optimal attack strategy are calculated. The PageRank link analysis algorithm is used to calculate the weight values of each stage. The attack and defense benefits and weight values of the equilibrium strategies in each stage of the game are shown in Figure 7. From Figure 7(a), the attack profit in the sixth stage exceeded the other stages, at 6.22. In Figure 7(b), the weight value corresponding to the sixth stage was also as high as 0.198. If the weight is high, it indicates that the target system has high value. If the attacker adopts appropriate attack strategies, it is easy to break through the defense line of the target system and enter the next attack and defense stage and state. Therefore, when formulating defense strategies, it is necessary to strengthen the formulation of defense strategies for these

Table 1 The content of vulnerability information

Number	Host	Vulnerability Types	Hazard Level	Initial Permissions	Target Permissions
1	Network defense equipment	/	/	Access	Root
2	File server	Remote code execution	High risk	User	Root
3	Client	Access validation error	Low risk	User	Root
4	Web server	Structured Query Language injection attack	Medium risk	User	User
5	Database server	Stealing backups	High risk	No access	Root
6	Database server	Structured Query Language injection attack	High risk	No access	Root

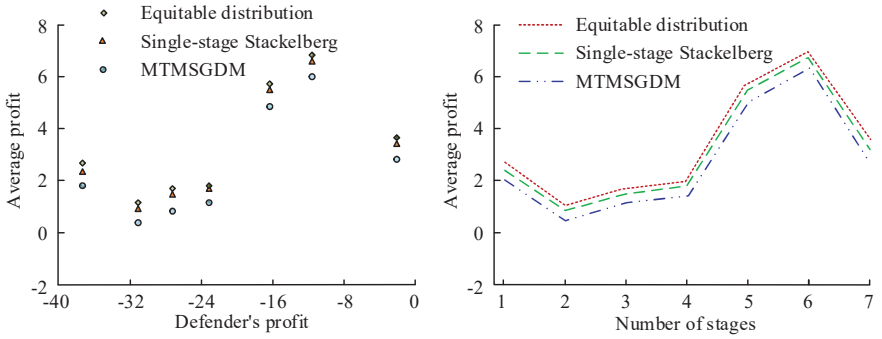


(a) Attack and defense benefits at different stages (b) Weight values at different stages

Figure 7 Attack and defense profits and weight values at each stage.

stages with higher weights, and strive to strike attackers in the early stages of attack and defense.

The equitable distribution model and the single-stage Stackelberg model are further introduced for comparison with MTMSGDM. In the equitable distribution model, the detection load is evenly distributed among virtual machines. The single-stage Stackelberg model takes into account both the attacker's strategy and resource constraints. The attack and defense profits of the three models in each stage are displayed in Figure 8. Figure 8(a) displays the attack and defense profits of various models at different stages. Under the same defense profits, the attack profits of MTMSGDM were significantly lower than those of other models. In the second stage, when the defense profit



(a) Attack and defense profits at different stages (b) Average profit at different stages

Figure 8 Comparison of attack and defense profits of three models at different stages.

was −31, the attack profit of MTMSGDM was only 0.36, which was 0.98 and 0.57 less than the equitable distribution model and single-stage Stackelberg model, respectively. From Figure 8(b), the attack profits of MTMSGDM were lower than the other two models in all stages. In stage 6, the attack profit of MTMSGDM was only 6.38, significantly lower than the other models. It indicates that MTMSGDM can effectively combat attack actions and achieve active defense.

3.2 Analysis of Game Equilibrium Strategy Under Different Security Resource Numbers

To verify the effectiveness of MTMSGDM under different numbers of security resources, the equitable distribution model and the single-stage Stackelberg model are used for comparison. The changes in the number of attacks for the three models under different numbers of security resources are shown in Figure 9. In Figure 9, when $z \leq 10$, the number of attacks on each model increased with the increase of z. When $z = 8$, the attack frequency of the equitable distribution model and the single-stage Stackelberg model was as high as 1000 times, while the attack frequency of MTMSGDM was only 30 times. More disposable security resources can better defend against attack behavior, and the defense effect of MTMSGDM is better.

The study continues to explore the average benefits of defenders and attackers for each model under different numbers of security resources, as shown in Figure 10. In Figure 10(a), the average defender profit of each model increased with the increase of the number of security resources. Among them, the average defender profit of MTMSGDM was superior to other models

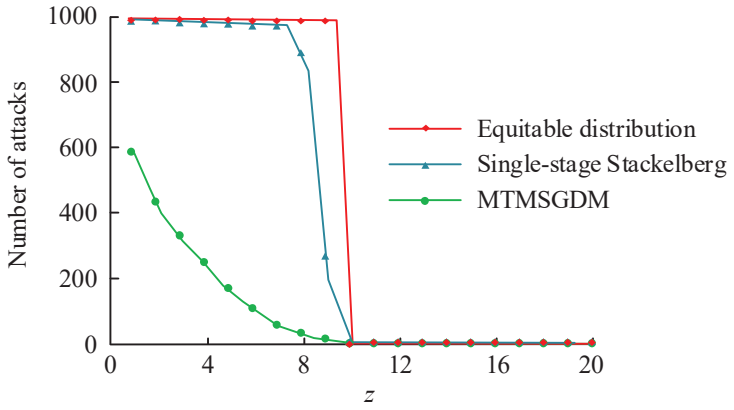
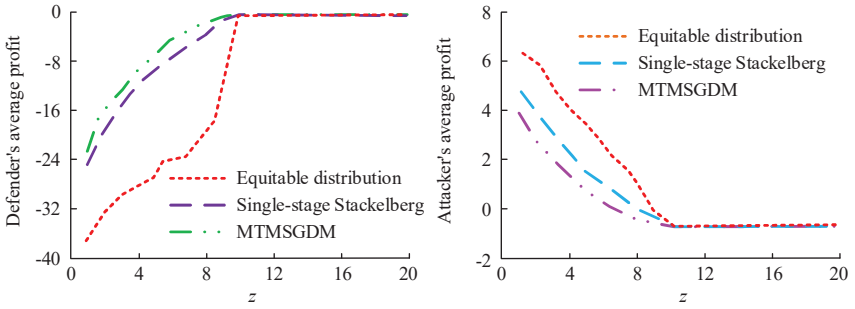


Figure 9 Changes in the number of attacks by attackers under different numbers of security resources.



(a) Defender's average profit for different models (b) Attacker's average profit for different models

Figure 10 The average profit of both attack and defense sides under different numbers of security resources.

when $z \leq 10$. When $z = 8$, the average defender profit of MTMSGDM was -0.95, which was 3.11 and 19.15 higher than the single-stage Stackelberg model and equitable distribution model. In Figure 10(b), the average attacker profit for each model decreased with the increase of security resources. When $z = 10$, the profit values of each model all decreased to 0. At the same time, the average attacker profit in MTMSGDM was lower than other models when $z \leq 10$. Among them, when $z = 4$, the average attacker profit in MTMSGDM was only 1.78, which was significantly lower than the single-stage Stackelberg model and equitable distribution model. In addition, when $z \geq 10$, the average profit of both attack and defense was 0, because there are sufficient security resources for attackers not to carry out attacks.

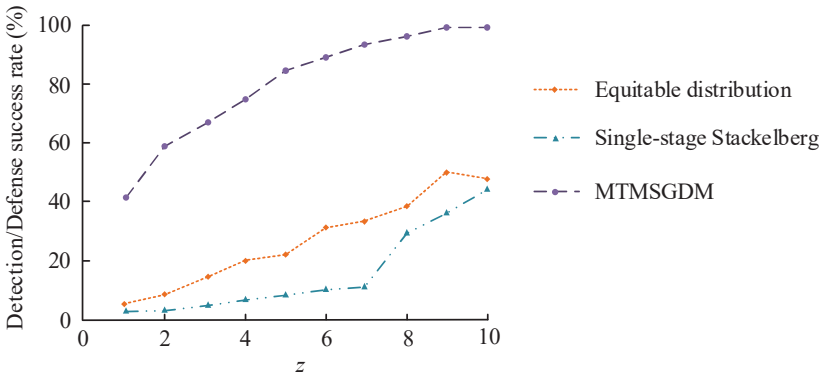


Figure 11 The detection/defense success rates of three models.

In the case of limited security resources ($1 \leq z < 10$), the detection/defense success rates of the three models are further explored. The detection/defense success rate is the ratio of the sum of successfully detected attacks and the attacks not initiated to the total number of experiments. The specific experimental results are displayed in Figure 11. The detection/defense success rates of all models increased with the increase of security resources. Among them, MTMSGDM had the highest detection/defense success rate. When $z = 8$, the detection/defense success rates of the equitable distribution model and the single-stage Stackelberg model were only 39.14% and 30.45%, respectively, while the MTMSGDM was as high as 96.68%. The reason is that MTMSGDM expands the decision space of defenders, greatly increasing the probability of not attacking.

To further verify the application effectiveness of the proposed model, the robustness of the model in the face of various interference factors in the network was studied and analyzed. During this process, advanced persistent threats (APTs) were added to the research, including APT attack methods such as phishing, rootkits, and vulnerability exploitation tools. At the same time, the study introduced complex attack methods such as dynamic fake data injection attacks, and selected 9 attack strategies for network attacks, including Install Trojan, Attack SSH on Web server, Install listener program, and Send abnormal data to buffer. To enhance the persuasiveness of the results, the study compared the model with the benchmark model and other research findings. Among them, the benchmark model includes the game model before improvement, the target immune strategy model, and the optimal attack strategy model. Other research achievements include network defense methods in references [6, 12], and [27], all of which have performed

Table 2 Comparison results between research methods and six selected models

Method Type	Defense Vulnerability Detection Rate	Defense Benefits	Defense Success Rate
The game model before improvement	51.05%	243	49.63%
Target Immune Strategy Model	53.78%	267	69.88%
Optimal attack strategy model	68..92%	255	65.72%
Reference [6]	73.61%	269	80.05%
Reference [12]	82.55%	274	85.24%
Reference [27]	84.64%	271	81.66%
This study	89.11%	288	92.57%

well in network security systems, are comparable, and have strong reference value. In the presentation of comparative results, the study mainly evaluated three indicators: defense vulnerability detection rate, defense benefits, and defense success rate, with each indicator taking the average value. In terms of experimental duration, the APT attack method lasts for 3 days, while other attack types are independently tested for 60 minutes. The comparison results between the research methods and the six selected models are shown in Table 2.

From Table 2, it can be seen that in terms of vulnerability detection rate, the model proposed in the study can reach 89.11%, while the benchmark model has a maximum of only 68.92%, which is significantly better. Meanwhile, in terms of defense benefits and defense success rates, the proposed models are 288 and 92.57%, respectively, which still have significant advantages compared to the latest three research methods. Overall, the proposed method has good robustness in the face of interference factors and can effectively cope with complex attack modes.

To validate the advantages of MTMSGDM proposed by the research institute, it was tested in a larger scale real-world network scenario, which contains thousands of links and has been subjected to attacks including DDoS attacks, malware propagation, and information theft. The research mainly compares the fair allocation model, single-stage Stackelberg model, Adversarial Website Fingerprinting Defense Based on Covariance Matrix Adaptation Evolution Strategy (CMAES-WFD) [32], and Multi-level Stackelberg model [33] with the MTMSGDM model. As shown in Figure 12, in large-scale network scenarios, the average defense effectiveness of MTMSGDM is as high as 273, followed by CMAES-WFD with an average defense effectiveness of 261. The average defense benefits of the fair distribution model, multi-level Stackelberg model, and single-stage Stackelberg model

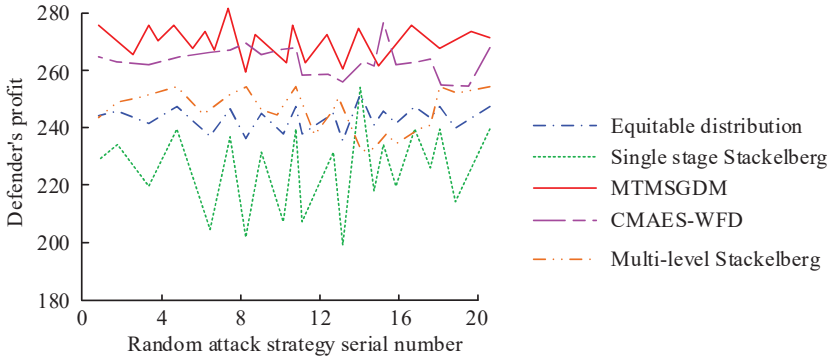


Figure 12 Comparison of defense benefits of different defense strategies in large scale scenarios.

are only 248, 251, and 231, respectively, far lower than MTMSGDM. In addition, it can be seen that the defense return volatility of the single-stage Stackelberg model is high, mainly due to its simplified game structure. This model assumes that the decision-making relationship between defenders and attackers is relatively fixed, lacking the ability to respond to dynamic changes in complex environments, and failing to make timely adjustments based on changes in attackers, resulting in significant fluctuations in defense effectiveness. In contrast, although the multi-level Stackelberg model considers multi-level decision structures to some extent, its complexity is still insufficient to cope with the changing environment and high-frequency attack behavior in large-scale networks. Therefore, although its defense benefits are better than the single-stage Stackelberg model, they are still far lower than MTMSGDM. Overall, the MTMSGDM model proposed in the study has significant defense advantages when facing complex, dynamic, and adversarial attack behaviors.

4 Discussion

In response to the problem of unequal status between the attacking and defending sides in traditional network defense technology, MTMSGDM was studied and constructed to optimize defense decision-making. The results show that compared with the fair allocation model and the single-stage Stackelberg model, MTMSGDM has significantly lower attack benefits when the defense benefits are the same. In the second stage, when the defense benefit is -31, the attack benefit of MTMSGDM is only 0.36, which is

0.98 and 0.57 less than the fair allocation model and single-stage Stackelberg model, respectively. In stage 6, the attack profit of MTMSGDM was only 6.38, significantly lower than the other models. The main reason is that MTMSGDM can dynamically adjust defense strategies based on real-time network status and attack information, which enables it to have strong adaptability in the face of rapidly changing attack scenarios. However, fair allocation models typically assume that resource allocation is static or based on fixed rules, and cannot be dynamically adjusted based on real-time attack situations. Although the single-stage Stackelberg model takes into account the defender's first mover advantage, it lacks flexibility in responding to multi-stage and multi strategy responses, making it vulnerable to attackers optimizing and attacking known strategies. Similarly, Seo S et al. [34] proposed active MTD technology, which models threats based on partially observable Markov decision processes and considers the internal and external operation sequences of the target drone. Meanwhile, the results of this study show that the defense efficiency of the proposed MTMSGDM. model is significantly higher than that of the random Stackelberg and partial signal game models, proving the effectiveness of the model. In the future, we will attempt to use more objective coefficient determination methods and further quantify the parameters of the attack defense game model accurately to better guide network defense.

5 Conclusion

The rapid development of Internet technology has brought a series of security problems. Traditional network defense technologies are often difficult to fundamentally solve the inequality between network attack and defense. To address this challenge, the MTD strategy was introduced and based on it, MTMSGDM was constructed to optimize defense decisions. The results indicate that in the seven stages of offensive and defensive confrontation, the attack profit of MTMSGDM in the sixth stage reached 6.22, and the corresponding weight value in this stage was as high as 0.198. This indicates that MTMSGDM can minimize the profit of attackers and improve the success rate of defense in dynamically changing environments. Meanwhile, under the same defense profit, the attack profit of MTMSGDM is significantly lower than other models. This indicates that MTMSGDM can effectively suppress the profit of attackers, making it difficult for them to obtain expected attack benefits and improving the security of the system. When the number of secure resources is 8, the detection/defense success rate of the MTMSGDM model is

as high as 96.68%, far higher than the fair allocation model's 39.14% and the single-stage Stackelberg model's 30.45%. This indicates that MTMSGDM has a high defense success rate in the face of complex network attacks, effectively protecting user data and system resources from illegal access or destruction. Overall, the proposed MTMSGDM model has important practical value in network security maintenance, as it can effectively reduce the number of attacks, lower the interests of attackers, and thus improve the overall security of the system. However, network attack and defense are easily influenced by various external factors. Subsequent research can consider adding interference factors in experiments to verify the robustness of the game model.

Fundings

The research is supported by: Jilin Province Education Science 13th Five-Year Plan 2020 general topics, "Research on the Influence of Online Presence on the Effectiveness of Online Learning in the Context of Big Data" Subject Approval, (No. GH20286); Research topic of higher education teaching reform of Jilin Institute of Chemical Technology in 2022, "Research on online learning participation and teaching strategies based on data analysis", (NO. 202206).

References

[1] Abdallah M, Naghizadeh P, Hota A R, Cason, T., Bagchi, S., Sundaram, S. Behavioral and game-theoretic security investments in interdependent systems modeled by attack graphs. IEEE Transactions on Control of Network Systems, 2020, 7(4): 1585–1596.

[2] Sengupta S, Chowdhary A, Sabur A, Alshamrani, A., Huang, D., Kambhampati, S. A survey of moving target defenses for network security. IEEE Communications Surveys & Tutorials, 2020, 22(3): 1909–1941.

[3] Tsemogne O, Hayel Y, Kamhoua C, Deugoué, G. Game-theoretic modeling of cyber deception against epidemic botnets in internet of things. IEEE Internet of Things Journal, 2021, 9(4): 2678–2687.

[4] Li, W. Li, J., Zhang, C., Yao, G., and Xu, X. (2023). A Priori Algorithm Based Network Security Situational Awareness Multi-Source Data Correlation Analysis Method. Journal of Cyber Security and Mobility, 12(06), 869–892. https://doi.org/10.13052/jcsm2245-1439.1263.

[5] Sun Z, Liu Y, Wang J, Li, G., Anil, C., Li, K., Cao, Applications of game theory in vehicular networks: A survey. IEEE Communications Surveys & Tutorials, 2021, 23(4): 2660–2710.

[6] Zhu M, Anwar A H, Wan Z, Cho, J. H., Kamhoua, C. A., Singh, M. P. A survey of defensive deception: Approaches using game theory and machine learning. IEEE Communications Surveys & Tutorials, 2021, 23(4): 2460–2493.

[7] Zhang, Z. (2023). Analysis of Network Security Countermeasures from the Perspective of Improved FS Algorithm and ICT Convergence. Journal of Cyber Security and Mobility, 12(01), 1–24. https://doi.org/10.13052/jcsm2245-1439.1211.

[8] Zhang Z, Huang S, Chen Y, Li, B., Mei, S. Cyber-physical coordinated risk mitigation in smart grids based on attack-defense game. IEEE Transactions on Power Systems, 2021, 37(1): 530–542.

[9] Shao C W, Li Y F. Optimal defense resources allocation for power system based on bounded rationality game theory analysis. IEEE Transactions on Power Systems, 2021, 36(5): 4223–4234.

[10] Abbasihafshejani M, Manshaei M H, Jadliwala M. Detecting and Punishing Selfish Behavior During Gossiping in Algorand Blockchain. 2023 IEEE Virtual Conference on Communications (VCC). IEEE, 2023: 49–55.

[11] Abolfathi M, Shomorony I, Vahid A, Jafarian, J. H. A game-theoretically optimal defense paradigm against traffic analysis attacks using multipath routing and deception. Proceedings of the 27th ACM on symposium on access control models and technologies. 2022: 67–78.

[12] Abdalzaher M S, Muta O. A game-theoretic approach for enhancing security and data trustworthiness in IoT applications. IEEE Internet of Things Journal, 2020, 7(11): 11250–11261.

[13] Hu H, Liu Y, Chen C, Zhang, H., Liu, Y. Optimal decision making approach for cyber security defense using evolutionary game. IEEE Transactions on Network and Service Management, 2020, 17(3): 1683–1700.

[14] Aydeger A, Manshaei M H, Rahman M A, Akkaya, K. Strategic defense against stealthy link flooding attacks: A signaling game approach. IEEE Transactions on Network Science and Engineering, 2021, 8(1): 751–764.

[15] Liu J, Wang X, Shen S, Fang, Z., Yu, S., Yue, G., and Li, M. Intelligent jamming defense using DNN Stackelberg game in sensor edge cloud. IEEE Internet of Things Journal, 2021, 9(6): 4356–4370.

[16] Zhang B, Dou C, Yue D, Park, J. H., and Zhang, Z. Attack-defense evolutionary game strategy for uploading channel in consensus-based secondary control of islanded microgrid considering DoS attack. IEEE Transactions on Circuits and Systems I: Regular Papers, 2021, 69(2): 821–834.

[17] Falsafain H, Heidarpour M R, Vahidi S. A branch-and-price approach to a variant of the cognitive radio resource allocation problem. Ad Hoc Networks, 2022, 132: 102871.

[18] Fadavi N. Dynamic Price Dispersion of Seasonal Goods in Bertrandâ "Edgeworth Competition". Applied Economics and Finance, 2024, 11(2): 14–33.

[19] Wang H, Memon F H, Wang X, Li, X., Zhao, N., and Dev, K. Machine learning-enabled MIMO-FBMC communication channel parameter estimation in IIoT: A distributed CS approach. Digital Communications and Networks, 2023, 9(2): 306–312.

[20] Wang H, Xu L, Yan Z, Gulliver, T. A. Low-complexity MIMO-FBMC sparse channel parameter estimation for industrial big data communications. IEEE Transactions on Industrial Informatics, 2020, 17(5): 3422–3430.

[21] He Q, Wang C, Cui G, G., Li, B., Zhou, R., Zhou, Q., Yang, Y. A game-theoretical approach for mitigating edge DDoS attack. IEEE Transactions on Dependable and Secure Computing, 2021, 19(4): 2333–2348.

[22] Yang Y, Wang W, Liu L, Dev, K., Qureshi, N. M. F. AoI optimization in the UAV-aided traffic monitoring network under attack: A stackelberg game viewpoint. IEEE Transactions on Intelligent Transportation Systems, 2022, 24(1): 932–941.

[23] Zheng Y, Li Z, Xu X, Zhao, Q. Dynamic defenses in cyber security: Techniques, methods and challenges. Digital Communications and Networks, 2022, 8(4): 422–435.

[24] Xie Y, Ji L, Li L, S., Guo, Z., Baker, T. An adaptive defense mechanism to prevent advanced persistent threats. Connection Science, 2021, 33(2): 359–379.

[25] Yang L X, Huang K, Yang X, et al. Defense against advanced persistent threat through data backup and recovery. IEEE Transactions on Network Science and Engineering, 2020, 8(3): 2001–2013.

[26] Zhong K, Yang Z, Xiao G, Li, X., Yang, W., Li, K. An efficient parallel reinforcement learning approach to cross-layer defense mechanism

in industrial control systems. IEEE Transactions on Parallel and Distributed Systems, 2021, 33(11): 2979–2990.

[27] Gheisari M, Hamidpour H, Liu Y, Saedi, P., Raza, A., Jalili, A., Amin, R. Data Mining Techniques for Web Mining: A Survey. Artificial Intelligence and Applications. 2023, 1(1): 3–10.

[28] Wang H, Li X, Jhaveri R H, Gadekallu, T. R., Zhu, M., Ahanger, T. A., and Khowaja, S. A. Sparse Bayesian learning based channel estimation in FBMC/OQAM industrial IoT networks. Computer Communications, 2021, 176: 40–45.

[29] Rahiminasab A, Tirandazi P, Ebadi M J, Ahmadian, A., and Salimi, M. An energy-aware method for selecting cluster heads in wireless sensor networks. Applied Sciences, 2020, 10(21): 7886.

[30] Larijani A, Dehghani F. An Efficient Optimization Approach for Designing Machine Models Based on Combined Algorithm. FinTech, 2023, 3(1): 40–54.

[31] Odumuyiwa, V., and Alabi, R. (2021). DDOS Detection on Internet of Things Using Unsupervised Algorithms. Journal of Cyber Security and Mobility, 10(3), 569–592. https://doi.org/10.13052/jcsm2245-1439.1034.

[32] Di Wang, Yuefei Zhu, Jinlong Fei, Maohua Guo. CMAES-WFD: Adversarial Website Fingerprinting Defense Based on Covariance Matrix Adaptation Evolution Strategy. Computers, Materials & Continua, 2024, 79(5): 2253–2276.

[33] Zhang C, Costa-Perez X, Patras P. Adversarial attacks against deep learning-based network intrusion detection systems and defense mechanisms. IEEE/ACM Transactions on Networking, 2022, 30(3): 1294–1311.

[34] Seo S, Moon H, Lee S, Kim, D., Lee, J., Kim, B., Kim, D. D3GF: A study on optimal defense performance evaluation of drone-type moving target defense through game theory. IEEE Access, 2023.

Biographies

Xue Bai received her Bachelor of Science degree from Yanbian University in China in 2012. She received her Master of Science degree from Northeast Normal University in China in 2015. At present, she is working in the Information Construction Office (Information Center) of Jilin Institute of Chemical Technology in China. Her areas of interest are computer education, data analysis, and network security.

Yongguo Bai obtained his Bachelor of Engineering (1986) form Jilin Institute of Chemical Technology, China. Presently, he is working at the College of Information & Control Engineering, Jilin Institute of Chemical Technology, China. He has published articles in domestic and foreign journals. His area of interest include teaching practice in education.