Hindawi
Security and Communication Networks
Volume 2022, Article ID 3949292, 17 pages
https://doi.org/10.1155/2022/3949292

Research Article

A Cyber Deception Defense Method Based on Signal Game to Deal with Network Intrusion

Chungang Gao,[1,2] Yongjie Wang,[1,2] and Xinli Xiong[1,2]

[1]*National University of Defense Technology, Hefei 230037, China*
[2]*Anhui Key Laboratory of Cyberspace Security Situation Awareness and Evaluation, Hefei 230037, China*

Correspondence should be addressed to Yongjie Wang; wangyongjie17@nudt.edu.cn and Xinli Xiong; xxlyx25@hotmail.com

Received 29 August 2021; Revised 7 October 2021; Accepted 4 January 2022; Published 18 March 2022

Academic Editor: Konstantinos Fysarakis

Increasingly, cyber security personnel are using cyber deception defense techniques to deal with network intrusions. However, traditional cyber deception techniques (such as honeypots and honeynets) are easily detected by attackers, thus leading to failure. Therefore, we propose a cyber deception defense method based on the signal game to improve the effectiveness of the defense. More specifically, first, we propose a moving target defense (MTD) enhanced cyber deception defense mechanism. Then, on the basis of the in-depth analysis of network attack and defense scenarios, a signal game model is constructed to describe the network attack and defense process, and a multistage attack and defense game equilibrium solution method is designed to guide the selection of the optimal deception defense strategy. Meanwhile, considering the actual network attack and defense, we quantify the game revenue based on a probabilistic model. The experimental results show that the defense method proposed in this paper could guide the defender to implement the optimal defense strategy and achieve a better defense effect.

1. Introduction

With the rapid development of Internet technology, networks and information systems have become important infrastructures to ensure the normal operation of various critical areas of the country. However, the endless network attack methods and network security incidents have made network security face severe challenges in recent years. Traditional network security technologies, such as identity verification, firewalls, and intrusion detection, are based on prior knowledge and experience to perform one-sided, static passive security defenses. They will respond only after an attack is detected, but at this time, the network system may have suffered serious losses. Therefore, the existing passive network security defense technology lacks initiative and deterrence ability to attack, and it is difficult to effectively ensure the security of the network.

To prevent or mitigate network intrusion, academics and network security personnel began to focus on active defense methods, and cyber deception defense [1] was proposed as one of them. Cyber deception defense is a defense mechanism evolved from the idea of honeypots. By deploying scams in network information systems, it interferes with the aggressor's perception and judgment of the target network information system, thereby affecting the choice of attack strategy. In the process of network attack and defense, defenders can use cyber deception technology to gain advantages. On the one hand, it can break the certainty and isomorphism of the network, affect the judgment of the aggressor on the network system, and protect essential resources; On the other hand, the aggressor can be introduced into a fake network environment so that the defender can analyze the aggressor's attack behavior to obtain cyber threat intelligence (CTI) [2], help form a defense plan, and mitigate the attack in time [3].

Traditional cyber deception defense techniques such as honeypots and honeynets focus on detecting attacks and collecting attack information by laying down fake resources to lure attackers to attack them. In recent years, the honeypot function has gradually evolved from a single decoy target and has been applied to more areas of network security protection, such as network event monitoring [4], malware

analysis [5], cipher mode research [6], and attack analysis [7]. Saud et al. [8] used NIDS and KFSensor honeypots to detect advanced persistent threat (APT) attacks. Once the honeypot's services are requested, it will immediately send an alert message to the console. Olagunju and Samu [9] created a new type of honeynet system to detect network intrusions in real time. The system provides SSH services to lure aggressors into attacking it, to collect relevant intrusion information such as the aggressor's IP address, attribution, and timestamp.

However, traditional cyber deception defense techniques have the disadvantage of static configuration and fixed location. With the development of antihoneypot technology, attackers begin to use antihoneypot technology to identify honeypots in the target network [10, 11]. Once the attacker recognizes the honeypot and pulls it into the blocklist, it will immediately lose its deception effect. Moreover, current network penetration, especially APT [12], is usually targeted at specific targets, with long duration and strong concealment. However, existing cyber deception defense strategies lack initiative in the interaction process, making it difficult to interest attackers and often failing to achieve the desired deception effect.

In addition, many scholars researched network defense strategy based on game theory in recent years, which provides theoretical guidance for deploying and implementing network defense technology. However, the quantification of the benefits is based on an ideal environment. Both the offensive and defensive parties have known all the vulnerabilities in the target network, and the effect of the strategy implementation of both sides is determined. To our knowledge, if the revenue quantification does not conform to the actual network attack and defense, the effect of network deception defense can only be reflected at the theoretical level, and the practical application value is lacking.

To solve the above problems, we developed an MTD-enhanced cyber deception defense mechanism. Based on this, we established a signal game to guide the selection of the optimal deception defense strategy. Meanwhile, we quantified the offensive and defensive benefits based on a probability model to meet the actual network offense and defense. The main contributions of this paper can be summarized as follows:

(1) MTD-enhanced cyber deception defense mechanism: we combined virtual network topology and IP address randomization to solve the current static problem of cyber deception defense. And we solved the problem of mutual interference when the two technologies are used concurrently, thereby further improving the defense effectiveness.

(2) Multistage attack and defense signal game: we established a signal game model to improve the defender's initiative in the process of attack and defense game. Meanwhile, the attenuation of network spoofing signal was fully considered to realize the dynamic analysis and deduction of multistage network attack and defense confrontation.

(3) Revenue quantification based on probability model: we analyzed the actual network attack and defense scenario and established a probabilistic model based on the Urn model to quantify revenue, making the selection of attack and defense strategies consistent with the reality of network attack and defense.

The rest of this paper is organized as follows. Section 2 presents the related work. Section 3 proposes the MTD-enhanced cyber deception defense mechanism and analyzes the network deception attack and defense scenarios. In Section 4, the offensive and defensive signal game model is defined, and the profit quantification method based on the probability model is proposed. Section 5 proposes the equilibrium solution process of the offensive and defensive game and gives the optimal strategy selection algorithm for cyber deception defense. Finally, simulation experiments are used to verify the effectiveness of this model and method. Table 1 lists the frequently used acronyms.

2. Related Work

Like cyber deception defense, moving target defense is also proposed as one of the active defense technologies. Its idea is to make the system dynamic and improve the system's security by increasing the diversity, dynamics, and randomness of the system [13]. At present, a large number of research results related to MTD have emerged, and many network elements such as IP addresses [14], ports [15], and operating platforms [16] have been used to implement specific MTD technologies. In order to break the static nature of traditional cyber deception defense and prevent them from being recognized by attackers, some scholars have proposed cyber deception defense technologies that integrate moving target defense. Clark et al. [17] proposed a method of periodically changing the IP address of the honeypot to invalidate the honeypot IP address that the aggressor has identified. This method effectively improved the survival rate of honeypots. Sun et al. [18, 19] realized the integration of IP address randomization and network deception technologies. The system dynamically changes the IP addresses of real nodes and decoy nodes in the network through IP address randomization, which interferes with the attacker's identification of decoy nodes. Wang et al. [20] proposed a hybrid defense mechanism combining MTD and cyber deception defense and proposed a dynamic defense strategy generation algorithm to improve the effectiveness of the hybrid defense mechanism. The methods mentioned above solve traditional honeypots' static nature, but there are still two problems. One is that the above techniques lack the interaction of aggressors and do not take the initiative of the network deception technology. The other is that the defense cost is not considered, which leads to lower practicality.

The essence of network security is offensive and defensive confrontation, so it has important practical significance to conduct network offensive and defensive analysis and defense strategy selection from the perspective of offensive and defensive confrontation. Game theory is very consistent with the characteristics of network offense and

Table 1: Frequently used acronyms.

Notation	Description
APT	Advanced persistent threat
CDSGM	Cyber deception signal game model
CTI	Cyber threat intelligence
CVSS	Common vulnerability scoring system
DMZ	Demilitarized zone
MTD	Moving target defense
MTDCD	MTD-enhanced cyber deception defense
SDN	Software-defined network

defense, such as relationship noncooperation, target opposition, and strategy dependence. In recent years, many scholars researched network defense strategy based on game theory, which provides theoretical guidance for deploying and implementing network defense technology. Jiang et al. [21] modeled the network attack and defense process as a two-role zero-sum game process, analyzed the network attack and defense behavior based on the complete information static game theory, and studied the optimal active defense strategy selection. Hengwei et al. [22] introduced static game theory with incomplete information and analyzed the effectiveness of defense strategies by solving static Bayesian equilibrium. Wangqun et al. [23] introduced a complete information dynamic game to study the influence of previous behavior on the subsequent game process. However, the above studies are based on the assumption that both offensive and defensive parties act simultaneously, and the restriction conditions are challenging to meet in actual network offense and defense.

The signal game has received special attention from researchers because it can accurately describe the key role of intelligence information in the choice of network offensive and defensive strategies. It describes the interaction in the game process through the signal transmission mechanism. Hengwei et al. [24] built a signal game model to guide optimal defense strategies for different types of defenders. Still, it is only a single-stage offensive and defensive game research, which does not match the dynamic evolution of network offense and defense. Hu et al. [25] improved the previous work and proposed that the signal attenuation factor represents the change of defense signal function in different stages, guiding the selection of optimal strategy for multistage active defense. However, existing research still lacks a comprehensive analysis of the quantification of the benefits of offensive and defensive strategies.

Motivated by the aforementioned goals and challenges, we go one step beyond and show that cyber deception defense can be further improved. In this paper, we develop an MTD-enhanced cyber deception defense mechanism and strategy selection methods based on signal games. By simulation experiment, our defense method can achieve a better defense effect.

3. Offensive and Defensive Scenario Analysis

3.1. Threat Model. The threat model is shown in Figure 1. The network is divided into three areas: the external network, the DMZ, and the internal network. Both the external and internal networks can access the Web server in the DMZ, but the external network cannot directly access the internal network. The purpose of an attacker's network intrusion is usually to steal or destroy important assets of the target network, but it is difficult for an attacker to directly attack a host that stores important assets in the target network from an external network. We assume that the attacker has used the vulnerability on the website to obtain administrator authority of the Web server in the DMZ and uses this as a springboard for further invasion.

In the process of network attack and defense, attackers usually use network scanning or sniffing to obtain basic network information, to select the most appropriate attack strategy to achieve penetration of the target system and optimize the benefits of network attacks. Lockheed Martin proposed a cyber kill chain model to describe a multistage attack, as illustrated in Figure 2.

This paper divides the aggressor's network intrusion into three stages: network reconnaissance, attack preparation, and attack implementation, which correspond to reconnaissance, weaponization and payload delivery, and exploitation in the cyber kill chain, respectively. In the network reconnaissance stage, the aggressor scans and sniffs the target network to obtain information such as active hosts, open ports, operating system fingerprints, and vulnerabilities. The aggressor analyzes the acquired target network information in the attack preparation stage and constructs the corresponding network attack weapon. After the aggressor prepares for the attack, it will attack the vulnerable hosts in the network. Compared with the previous two stages, the attack implementation stage is very short and negligible, so the attacker's network intrusion time includes the scan detection time and the attack preparation time.

To fight against the network intrusion of aggressors, network defenders usually deploy some honeypots in the network to attract the aggressors to carry out attacks to protect essential assets. However, APT attackers usually have apparent targets, and it is difficult for traditional honeypots and honeynets to attract them. At the same time, APT attackers usually conduct rigorous network reconnaissance and analysis before formally launching an attack. Therefore, traditional honeypots and honeynets often fail to achieve the purpose of deception.

3.2. MTD-Enhanced Cyber Deception Defense Mechanism. Based on the analysis of the threat model in Section 3.1, to further improve cyber deception effectiveness, we propose

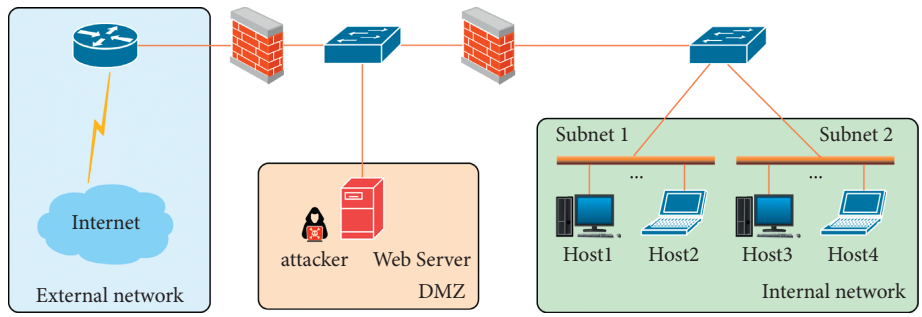

Figure 1: Threat model.

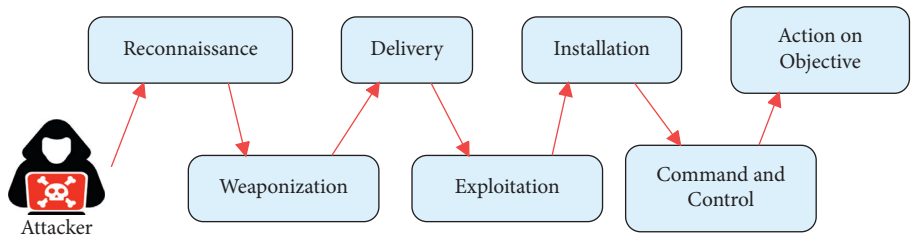

Figure 2: Cyber kill chain.

an MTD-enhanced cyber deception defense method (MTDCD). We implemented a preliminary version of the system based on SDN in [26]. In this paper, we implemented further improvements to the system.

In order to resist the attacker's network intrusion into the target network, the system first converts the real IP address of the host in the network into a virtual IP address and generates a large number of decoy nodes to build the virtual network topology. Through the above operations, the network view detected by the attacker is entirely different from the actual situation of the network system.

Figure 3 is a schematic diagram of a virtual network topology generated from a real network topology, where h_0 is a host occupied by an attacker, $h_1, h_2 \cdots h_6$ are real hosts in the intranet, and b is a honeypot. The virtual network topology is much larger than the real network, and the purpose is to extend the attacker network reconnaissance time. The bait nodes in the virtual network topology are mapped from the honeypot. Compared with traditional honeypots or honeynets, not only are a large number of bait nodes deployed in the virtual network topology but also the connection relationship between real hosts has changed.

The attacker can identify the bait node by analyzing the fingerprint and activity of the node in the network and pull it into the blacklist. In [18–20, 26], the IP address of the bait node is changed dynamically to improve the survival rate of the decoy node. However, when IP address randomization is implemented on bait nodes, the connection between the attacker and bait nodes may be disconnected, which reduces the spoofing effect of bait nodes. To solve the above problems, the MTDCD defense mechanism randomly divides IP addresses into IP address shuffling, IP address shifting, and IP address retention policies. The following describes their definitions.

Definition 1. IP address conversion: the system randomly selects an IP address from the unused IP address pool to replace the current IP address of the node and puts the current IP address back into the unused IP address pool.

Definition 2. IP address transfer: the system randomly selects an IP from the unused IP address pool to replace the host's current IP address and transfers the host's current IP address to a bait node similar to its fingerprint.

Compared with IP address conversion, IP address transfer increases the probability of bait nodes being attacked. Since the fingerprints of the bait node and the real host are similar, when an IP address transfer occurs, the real host's IP address does not change from the attacker's point of view. In order to ensure that attackers cannot distinguish real hosts from bait nodes according to the rule of IP address change, the IP addresses of some bait nodes need to remain unchanged when IP address randomization occurs. So we define an IP address retention policy.

Definition 3. IP address retention: when IP address randomization occurs, the IP addresses of some decoy nodes remain unchanged. In the virtual network topology, there are several decoy nodes with similar fingerprints to a real host in the intranet. In order to capture more different attack information, it is necessary to select decoy nodes with different fingerprints for IP address retention.

Figure 4 shows the state of the network system in the two cycles before and after the randomization of the IP address in the MTDCD. Each grid represents an IP address, where h_1, h_2, and h_3 are real hosts, b_1, b_2, and b_3 are decoy nodes with fingerprints similar to h_1, h_2, and h_3, respectively, and the rest are unused IP addresses. The system periodically performs IP address randomization, and the alteration of the

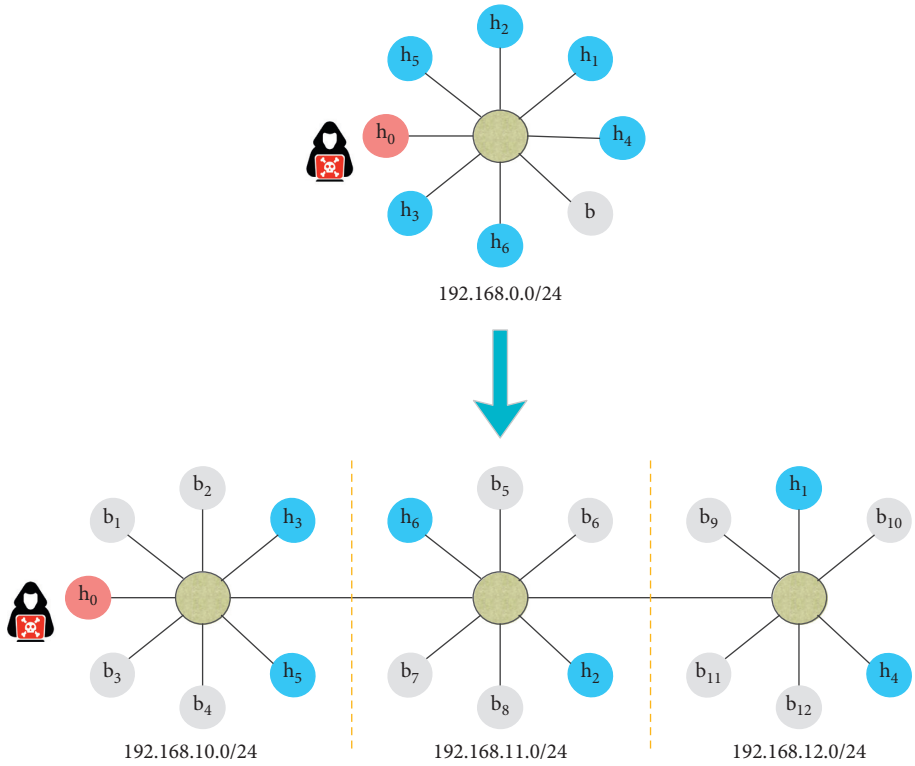

Figure 3: Schematic diagram of virtual network topology generation.

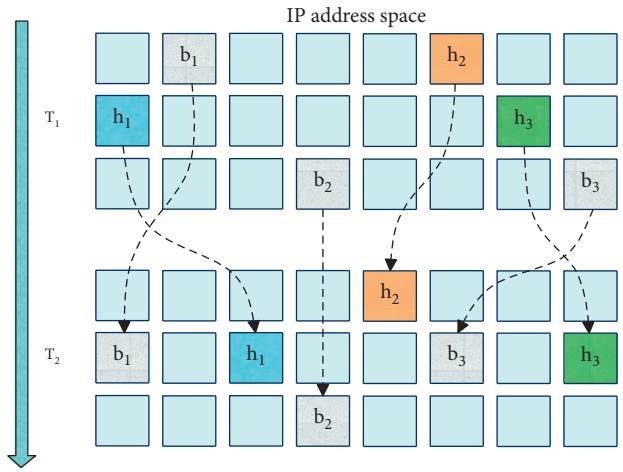

Figure 4: Schematic diagram of MTDCD defense model.

node's position in the graph represents the change of the node's IP address. In the T_2 period, the IP addresses of hosts h_1, h_2, and h_3 are converted to unused IP addresses in the T_1 period, and the IP address of host h_1 is transferred to the bait node b_1. The IP address of the bait node b_2 is not changed, and the IP address of the bait node b_3 is changed to an unused IP address in T_1 period.

The MTDCD defense mechanism can ensure that normal services in the network will not be affected. After deploying the MTDCD defense mechanism, the interaction between nodes in the network is shown in Figure 5. The MTDCD defense mechanism strictly separates the virtual network topology from the real network; that is, the real IP address is still used for the interaction between the intranet hosts, as shown in Figure 5(a). Intranet hosts still use real IP addresses to access the Web server with the MTDCD defense mechanism deployed. When the data packet passes through the OF switch, the real IP address is converted to the virtual IP address through dynamic address translation, as shown in Figure 5(b). Therefore, the deployment of the MTDCD mechanism will not affect the normal interaction in the network.

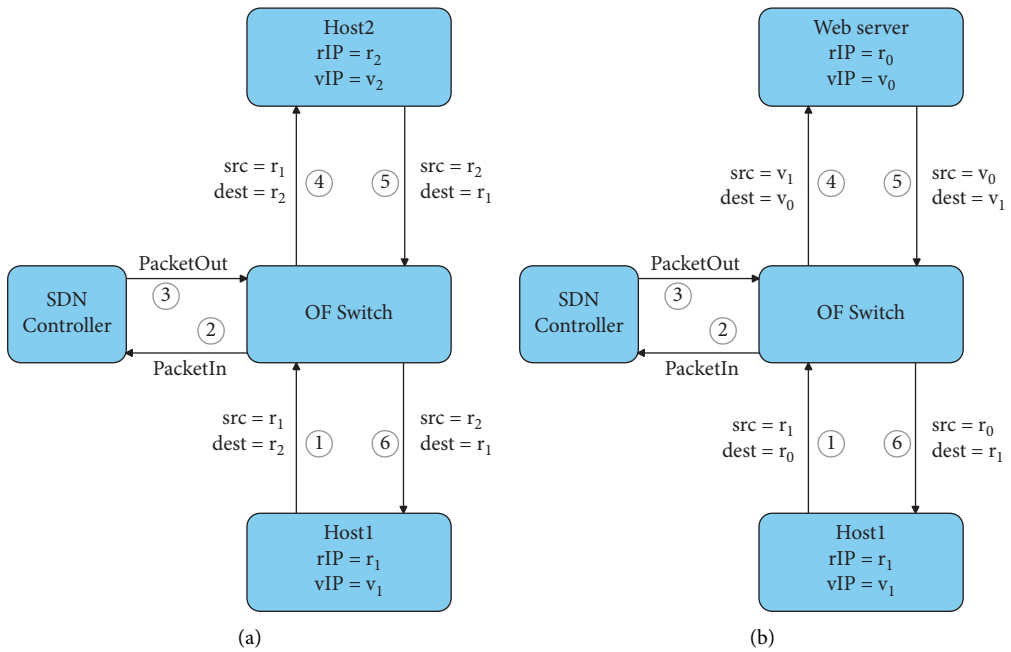

Figure 5: Interaction between nodes in the network after MTDCD is deployed. (a) Interaction between hosts on the intranet. (b) The intranet host accesses the Web server.

3.3. Network Attack and Defense Scenario Analysis. From the previous analysis, it can be seen that deploying the MTDCD defense mechanism makes it more difficult for an aggressor to attack a real host in the network. Even if the aggressor identifies the decoy node and pulls it into the blacklist, after the randomization of the IP address occurs, the aggressor has to restart detection and analysis. Under normal circumstances, the real host is running normal network business activities, and the system is more active, while the decoy node lacks normal business activities, so once a host visits the decoy node, it can be identified as an aggressor. Nevertheless, the aggressor can also judge the network defense level based on the activity of the network system and then determine whether to attack. If the aggressor detects that the network system activity is relatively high, it will determine that there are more real hosts in the network. That is, the network defense level is low, and the attack is biased. Conversely, if the aggressor detects that the activity of the network system is insufficient, it will assume that there are more decoy nodes in the network. That is, the network defense level is high, and it prefers not to attack.

In view of this, the defender may mislead the aggressor to judge the level of network defense by releasing deception signals. The defender can increase the activity of some decoy nodes to make the attacker mistakenly believe that there are more real hosts in the network, thereby attacking false targets. Alternatively, the defender can reduce the activity of some real hosts to make the attacker mistakenly believe that there are more decoy nodes in the network and thus give up the attack.

Drawing on signaling game theory, define the defender as the signal sender and the attacker as the signal receiver. The cyber deception attack and defense game process based on the signal game is as follows:

(1) The defender selectively releases the defense signal according to its defense type, including information that genuinely describes the network system (real signal) or information that is inconsistent with the real situation of the network system (spoofing signal), thereby misleading the attacker's judgment on the target network system.

(2) In the initial stage of the game, the attacker forms a priori belief about the type of defender through network reconnaissance. After receiving the defensive signal, the attacker forms a posteriori belief about the type of defender according to Bayes' rule and chooses the optimal attack strategy accordingly.

(3) The defender chooses the optimal defense strategy.

Compared with pure active defense technology, the cyber deception defense based on signal games improves the defender's initiative in the offensive and defensive game. As the signal sender, the defender confuses or induces the attacker by actively releasing the defense signal, thus influencing the choice of the attacker's strategy.

4. Cyber Deception Signal Game Model

4.1. Cyber Deception Signal Game Model Definition. Definition 4. The cyber deception signal game model $CDSGM = \{\Omega, \Theta, S, \omega, \delta, P, U\}$ is a seven-tuple, and each variable is specifically defined as follows.

(1) $\Omega = \{\Omega_d, \Omega_a\}$ is the set of game participants, where Ω_d is the defender, and Ω_a is the attacker.

(2) $\Theta = (\Theta_a, \Theta_d)$ is the set of player types in the game; $\Theta_d = \theta_h$ is the set of defender types. The defender types are divided into different levels according to

the number of bait nodes in the virtual network topology. $\Theta_a = \{\theta_a\}$, which means there is only one type of attacker.

(3) $S = \{S_d, S_a\}$ is the set of offensive and defensive strategies, where $S_d = \{d_i \mathrm{i} = 1, 2, \cdots, n\}$ is the set of defense strategies. The defense strategy is the probability of IP address transfer; $S_a = \{A_j j = 1, 2, \cdots, m\}$ is the attack strategies set, which is a combination of a series of atomic attacks.

(4) $\omega = \{\omega_k \mathrm{k} = 1, 2, \cdots, K\}$ is the set of defensive signals. The defensive signals include real signals and deception signals.

(5) δ is the signal attenuation factor, representing the attenuation degree of signal deception as the game progresses.

(6) $P = \{P_a, \widetilde{P}_a\}$ is the attacker's game belief set, $P_a = \{P_a(\theta_h)h = 1, 2, \cdots, H\}$ is the attacker's prior belief set, and $\widetilde{P}_a = P_a(\theta_h \omega_k)$ represents the posterior belief obtained by the attacker using Bayes' rule after receiving the spoofing signal.

(7) $U = \{U_d, U_a\}$ is the set of utility functions for both offense and defense, where U_d represents the utility function of the defender, and U_a is the utility function of the attacker.

4.2. Revenue Quantification. The application of game theory to network offense and defense analysis has natural advantages, and the quantification of game revenue determines the accuracy of the final game result. Accurately quantifying the benefits of both sides in the game model becomes the key to selecting the optimal strategy. The quantification of the gains of the offensive and defensive games in existing studies is more subjective and idealized, which is inconvenient to be applied in actual network offense and defense. We build a probability evaluation model based on the Urn model to improve the quantification of the benefits of offensive and defensive games.

The Urn model [27] has been widely used in physics, communications, and computer science to determine the statistical distribution of a given set of events. In [28, 29], researchers established a defense effectiveness evaluation model based on the Urn model to analyze the defense effectiveness of honeypots and moving target defense. This section calculates the probability of an attacker attacking a host or decoy node in a single offensive and defensive game stage based on the Urn model.

The various parameters in the network attack and defense scenario are listed in Table 2.

Based on the Urn model, we model the probability of an attacker successfully attacking the host in a single game stage as an Urn containing n_v marbles, including m green marbles, εe red marbles, and $n_v - m - \varepsilon e$ blue marbles. The green, blue, and red marbles represent the real host, the decoy node that successfully deceives the attacker, and the remaining IP addresses in the address space, respectively. The attacker took out one marble at a time and did not put it back. But because the randomization of the IP address will invalidate the information obtained by the attacker, it is equivalent to periodically returning all the marbles that have been taken out. The condition for the attacker's success is to get at least one green marble and none of the red marbles.

When IP address randomization is not implemented, the probability of an attacker successfully attacking the real host is

$$P_h = \sum_{x=1}^{m} \frac{C_m^x C_{n_v - m - \varepsilon e}^{L-x}}{C_{n_v}^L}. \tag{1}$$

where m is the number of real hosts in the network, εe represents the number of bait nodes that successfully deceived the attacker, n_v is the size of the virtual network topology, and L is the number of addresses detected by the attacker per cycle.

$$L = \frac{T_\tau}{T_s}. \tag{2}$$

where T_τ represents IP address randomization cycle and T_s represents the time for the attacker to probe a single node.

After implementing IP address randomization, there is a case where the attacker successfully detects the host but fails to hit the host during the attack implementation phase. The probability is

$$P_h^{no} = \sum_{x=1}^{m} \frac{C_m^x C_{n_v - m - \varepsilon e}^{L-x}}{C_{n_v}^L} \cdot \frac{1}{\lambda}. \tag{3}$$

where λ represents the ratio of IP address randomization period to attack preparation time.

Therefore, it is easy to know that after implementing IP address randomization, the probability of the attacker successfully attacking the host is

$$P_h^* = \sum_{x=1}^{m} \frac{C_m^x C_{n_v - m - \varepsilon e}^{L-x}}{C_{n_v}^L} \cdot \left(1 - \frac{1}{\lambda}\right). \tag{4}$$

Similarly, the probability of an attacker attacking a bait node without IP address transfer is

$$P_b = \left(1 - \frac{C_{n_v - \varepsilon e}^L}{C_{n_v}^L}\right) \cdot \left(1 - \frac{1}{\lambda}\right). \tag{5}$$

Considering that the IP address transfer assigns the real host IP address of the previous cycle to the decoy node, the probability of the attacker attacking the bait node is

$$\begin{aligned} P_b^* &= P_b + P_h^{no} \cdot \alpha \\ &= \left(1 - \frac{C_{n_v - \varepsilon e}^L}{C_{n_v}^L}\right) \cdot \left(1 - \frac{1 - \alpha}{\lambda}\right) \\ &\quad + \sum_{x=1}^{m} \frac{C_m^x C_{n_v - m - \varepsilon e}^{L-x}}{C_{n_v}^L} \cdot \frac{\alpha}{\lambda}. \end{aligned} \tag{6}$$

where α is the probability of IP address transfer.

Table 2: Parameters in network attack and defense scenarios.

Notation	Description
n_v	The size of the virtual network topology
m	The number of real hosts in the network
e	The number of bait nodes in the network
ε	Deception probability of bait node
T_τ	IP address randomization cycle
T_s	Time to probe a single node
T_a	Attack preparation time
α	Probability of IP address transfer
λ	The ratio of IP address randomization period to attack preparation time

With reference to [30], we combine the probability evaluation model to quantify the benefits of offensive and defensive games.

The notations involved in the quantification of revenue are shown in Table 3.

Definition 5. System damage cost refers to the loss of the system caused by the attacker launching an attack. It is related to the loss of the host being attacked L_h, the probability of the attacker successfully attacking the host P_h^*, attack lethality of the vulnerability L_{V_i}, and probability of the existence of the vulnerability P_{V_i}, which can be expressed as

$$SDC = L_h \cdot P_h^* \cdot \sum_{i=1}^{v} L_{V_i} \cdot P_{V_i}. \tag{7}$$

Definition 6. System protection benefit refers to the benefit that the defender induces the attacker to attack the decoy node, mainly the attack information obtained. It is related to the reward of the bait node being attacked R_b and the probability of the attacker attacking the bait node P_b^*, which can be written as

$$SPB = R_b \cdot P_b^*. \tag{8}$$

Definition 7. Attack reward refers to the profit gained by the attacker successfully attacking the host. It is related to reward of the attack to the host R_h, the probability of the attacker successfully attacking the host P_h^*, attack lethality of the vulnerability L_{V_i}, and probability of the existence of the vulnerability P_{V_i}, which can be expressed as

$$AR = R_h \cdot P_h^* \cdot \sum_{i=1}^{v} L_{V_i} \cdot P_{V_i}. \tag{9}$$

Definition 8. Attack loss refers to the loss caused by attacking the decoy node, mainly attacking information leakage. It is related to the loss caused by the attack to the bait node L_b and the probability of the attacker attacking the bait node P_b^*, which can be written as

$$AL = L_b \cdot P_b^*. \tag{10}$$

Definition 9. Attack cost refers to the cost of attack, including reconnaissance cost and vulnerability exploitation cost, which can be expressed as

$$C_a = C_{rec} + C_{vul}. \tag{11}$$

where C_{rec} represents the cost of network reconnaissance and C_{vul} represents the cost of exploiting vulnerabilities.

Definition 10. Defense cost refers to the cost of performing defense actions, including the deployment cost of bait nodes and the cost of IP address randomization. And the cost of IP address randomization includes IP address conversion cost and IP address transfer cost. Defense cost can be written as

$$C_d = C_{bait} \cdot e + C_{conv} \cdot m \cdot (1 - \alpha) + C_{tran} \cdot m \cdot \alpha.\pi. \tag{12}$$

where C_{bait} represents the cost of deploying a bait node, and C_{conv} represents the cost of IP address conversion per node and C_{tran} represents the cost of IP address transfer per node.

Definition 11. The deception cost refers to the cost of reducing the activity of the real host or increasing the activity of the decoy node, which can be expressed as

$$CD = C_{im} + C_{re}. \tag{13}$$

where C_{im} represents the cost of increasing per bait node activity and C_{re} represents the cost of reducing per real host activity.

Based on the above definition, we can get the expected utilities of both attack and defense, which are

$$U_a\left(\theta_h, \omega_k, A_j, d_i\right) = AR - C_a - AL, \tag{14}$$

$$U_d\left(\theta_h, \omega_k, A_j, d_i\right) = SPB - C_d - CD - SDC. \tag{15}$$

5. Game Equilibrium Solution and Optimal Deception Defense Strategy Selection

5.1. Refined Bayesian Equilibrium Solution. The game model *CDSGM* has equilibrium $EQ = (\omega^*(\theta_h), a^*(\omega_k), \widetilde{P}_a(\theta_h \omega_k))$.

Among them, $\omega^*(\theta_h)$ is the signal dependency strategy of the defender, which means that when the defender type is θ_h, the signal dependence strategy adopted is $\omega^*(\theta_h)$; $a^*(\omega_k)$ is the signal dependence strategy of the attacker,

Table 3: Notations description in profit quantification.

Notation	Description
L_h	The loss of the host being attacked
R_b	The reward of the bait node being attacked
R_h	The reward of the attack to the host
L_b	The loss caused by the attack to the bait node
L_{V_i}	Attack lethality of the vulnerability
P_{V_i}	Probability of existence of a vulnerability
C_{rec}	The cost of a network reconnaissance
C_{vul}	The cost of exploiting vulnerabilities
C_{bait}	The cost of deploying a bait node
C_{conv}	The cost of IP address conversion per node
C_{tran}	The cost of IP address transfer per node
C_{im}	The cost of increasing per bait node activity
C_{re}	The cost of reducing per real host activity

which means that when the attacker receives the defensive signal ω_k, the executed attack strategy is $a^*(\omega_k)$; $\widetilde{P}_a(\theta_h\omega_k)$ is the a posteriori inference of the defender's type after the attacker receives the defense signal ω_k. The equilibrium satisfies the following conditions.

(i) $a^*(\omega_k) \in \arg\max_{A_j \in S_a} \sum P_a(\theta_h\omega_k) U_a(\theta_h, \omega_k, A_j)$

(ii) $\omega^*(\theta_h) \in \arg\max_{\omega_k \in \omega} \sum U_d(\theta_h, \omega_k, a^*(\omega_k))$

(iii) $\widetilde{P}_a(\theta_h\omega_k)$ is given by the attacker based on prior probability P_a, received defensive signal ω_k , and the attacker's optimal attack strategy $a^*(\omega_k)$

The steps to solve the refined Bayesian equilibrium are as follows.

(1) Calculate the posterior inference of different information sets on the offensive and defensive game tree $P_a(\theta_h\omega_k)$.

(2) Choose the optimal attack strategy $a^*(\omega_k)$.

After the attacker receives the defensive signal ω_k, the posterior probability $P_a(\theta_h\omega_k)$ is calculated by combining the prior probability $P_a(\theta_h)$ and then choosing the optimal attack strategy $a^*(\omega_k)$ that maximizes the expected return.

(3) Calculate the optimal defense strategy $d^*(\theta_h)$.

According to the defensive signals, the defender can foresee that the attacker will choose the optimal attack strategy for inferring dependence $a^*(\omega_k)$. The defender can choose the optimal defense strategy $\omega^*(\theta_h)$ that can obtain the maximum defense benefit.

(4) Refined Bayesian equilibrium solution.

According to the optimal inferred dependency strategy and the prior probability of the participants obtained in (2) and (3), the posterior belief $\widetilde{P}_a(\theta_h\omega_k)$ is calculated by the Bayes rule.

5.2. Multistage Offensive and Defensive Game Equilibrium Solution. The set of defender types is $\Theta_d = \{\theta_H, \theta_L\}$. Among them, θ_H is the high-level defense, and θ_L is the low-level defense. The deception signal space of the defender is $\omega = \{\omega_H, \omega_L\}$, and the strategy space of the attacker is $S_a = \{A_1, A_2\}$. The defender strategy space is $S_d = \{d_1, d_2, d_3\}$; the attacker's prior probability of the defender type is $P_a = \{P_a(\theta_H), P_a(\theta_L)\}$.

For the sake of simplification, consider that there is no benefit discount phenomenon in the multistage network attack and defense process.

(1) The solution to the Equilibrium of Offensive and Defensive Game in the Initial Stage.

Construct the initial stage network deception attack and defense game tree, as shown in Figure 6.

Nature chooses the defender type with the probability of $P_a(\theta_H)$ and $P_a(\theta_L)$. The defender releases a defensive signal. After observing the signal, the attacker revises its judgment on the type of defender. When the signal ω_H is received, the probability that the attacker thinks the defender type is $\{\theta_H, \theta_L\}$ is $\{P_a(\theta_H\omega_H), P_a(\theta_L\omega_H)\}$; when the signal ω_L is received, the probability that the attacke thinks the defender type is $\{\theta_H, \theta_L\}$ is $\{P_a(\theta_H\omega_L), P_a(\theta_L\omega_L)\}$.

Because it is in the initial stage of the game, the attacker cannot obtain information from the offensive and defensive confrontation to analyze the type of defender, so there is no signal attenuation, that is, $\delta = 1$.

Solve the refined Bayesian equilibrium of the offensive and defensive game based on the method in Section 5.1, denoted as $EQ_1 = (\omega^*(\theta_h), a^*(\omega_k), \widetilde{P}_a(\theta_h\omega_k))$. $\omega^*(\theta_h)$ is the optimal defense strategy at this stage.

(2) The solution to the Equilibrium of Offensive and Defensive Game in the second stage.

After the first stage of the offensive and defensive game, the attacker corrects judgment on the type of defender through the posterior probability solved in the previous stage, and the natural effect is replaced.

In addition, the attacker improves the ability to discriminate the type of defender by analyzing the

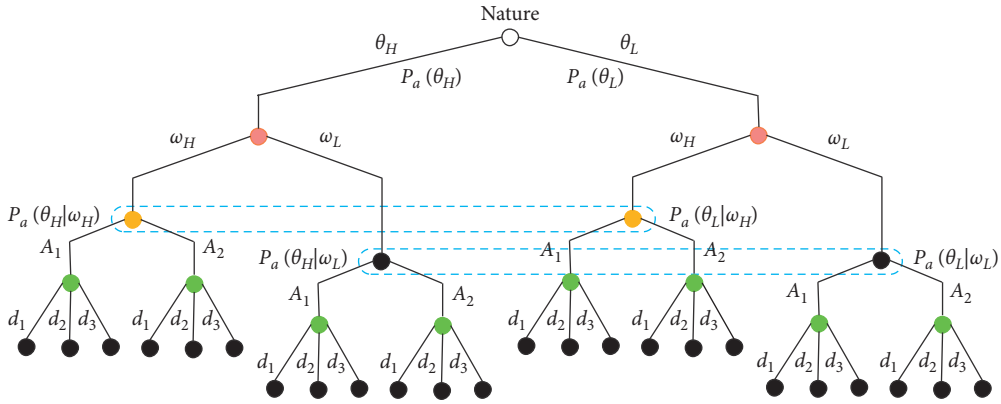

Figure 6: Single-stage network deception attack and defense game tree.

game result, so the deceptive effect of the signal begins to attenuate from the second stage.

For the game path where false signals are released, the deceptive effect of the signal will be attenuated, namely, $0 < \delta < 1$, whereas for the game path where real signals are released, the deceptive effect of the signal will not be attenuated, namely, $\delta = 1$.

Solve the refined Bayesian equilibrium of the offensive and defensive game based on the method in Section 5.1, denoted as $EQ_2 = (\omega^*(\theta_h), a^*(\omega_k), \widetilde{P}_a(\theta_h \omega_k))$.

After the second stage of the offensive and the defensive game is over, the attacker again revises the judgment of the defender's type and uses it as a priori judgment of the third stage, and the role of the defensive signal is further attenuated.

(3) The solution to the Equilibrium of Offensive and Defensive Game in the n-th stage.

As the game progresses, the deceptive effect of signals gradually weakens. Suppose that in the n-th stage, the signal attenuation factor is zero. Attackers can completely screen out false signals. At this time, the offensive and defensive game degenerates into a static game of incomplete information.

5.3. Deception Defense Strategy Selection Algorithm. Based on the above analysis, we give the specific expression of the optimal network deception strategy selection algorithm based on the signal game, as presented in Algorithm 1.

6. Simulation Experiment and Analysis

6.1. Simulation Experiment Environment Description. In order to verify the effectiveness of the method in this paper, we constructed an experimental environment, as illustrated in Figure 7. The real network is divided into three areas: the external network, the DMZ, and the internal network. There is a Web server in the DMZ, and there are two subnets in the intranet. The attacker has used the vulnerability on the website to obtain administrator authority of the Web server in the DMZ. To prevent attackers from invading the internal network, we deploy a network deception system in the network. Therefore, the network detected by the attacker is a dynamically changing virtual network topology. The virtual network topology consists of four subnets with decoy nodes that are similar to the host fingerprint deployed in each subnet. The topology used in the experiment is a tree topology.

6.2. Revenue Calculation. For the calculation of game revenue, existing research usually first analyzes the vulnerabilities in the network through vulnerability scanning tools and then formulates corresponding attack and defense strategies. However, the defender will promptly repair the loopholes in actual network attacks and defenses. Attackers can only use vulnerabilities unknown to the defender, usually zero-day vulnerabilities. Therefore, we count the vulnerabilities in the form of probability to calculate the game revenue.

Rapid7's 2020 vulnerability intelligence report analyzes 50 typical vulnerabilities revealed in 2020 [31]. It divides them into four categories and counts the number of vulnerabilities in each category. Assume that the hosts in the network have zero-day vulnerabilities. We calculated the probability of each vulnerability based on the reported statistical data and referenced CVSS to obtain the attack lethality of each vulnerability, as listed in Table 4.

Based on the vulnerability information in the network system and the attack and defense behavior database of MIT Lincoln Laboratory, we get the attacker's atomic attack information, as shown in Table 5.

The attacker must first conduct network reconnaissance, including network scanning and network sniffing, and then determine the type of defender and the host that can be attacked based on the network reconnaissance results. Attack behaviors a_3, a_4, a_5, and a_6, respectively, indicate exploiting vulnerabilities v_1, v_2, v_3, and v_4 to attack. Therefore, the network attack strategy set $S_a = \{A_1, A_2\}$, where $A_1 = \{a_1, a_2, a_i i = 3, 4, 5, 6\}$ and $A_2 = \{a_1, a_2, a_7\}$. A_1 indicates the exploitation of vulnerabilities after network reconnaissance; A_2 indicates that no attack action is taken after network reconnaissance. The experiment divides the types of defenders into high-level defenders and low-level defenders, using $\Theta_d = \{\theta_H, \theta_L\}$ means. Defensive signal space $\omega = \{\omega_H, \omega_L\}$, which means pretending to be a high-level

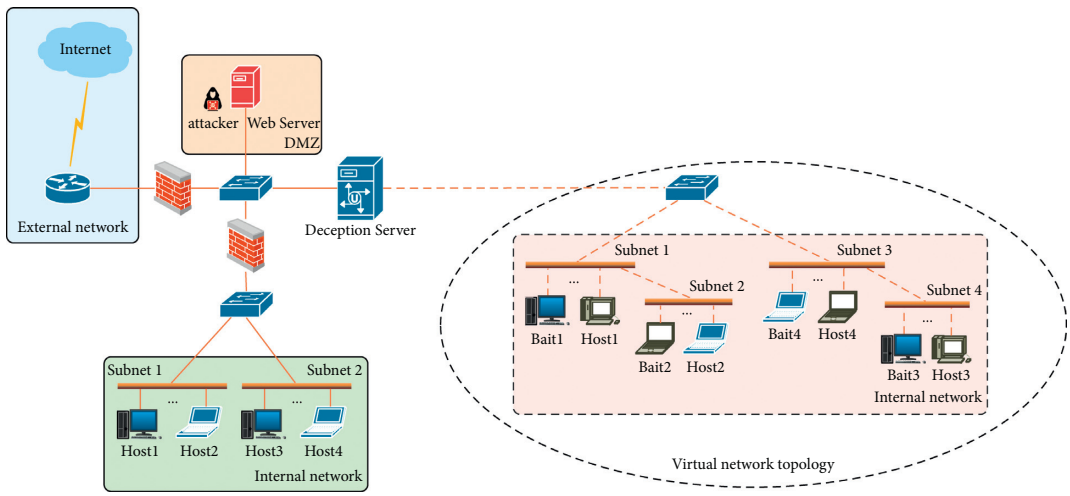

Figure 7: Topography of the experimental network.

defender or a low-level defender. When the defensive signal is the same as the defender type, there is no deception cost. Hence, when the defender type is θ_H, the cost of releasing the signal $\{\omega_H, \omega_L\}$ is $\{0, 20\}$. When the defender type is θ_L, the cost of releasing the signal $\{\omega_H, \omega_L\}$ is $\{10, 0\}$. Defense strategy $S_d = \{d_1, d_2, d_3\}$, respectively, indicates that the IP address transfer probability is 40%, 60%, and 80%. The values of the remaining parameters in the revenue quantification are listed in Table 6.

In the game's initial stage, Nature chooses the defense type with probability (0.5, 0.5). The prior probability of the attacker to the defender type is (0.5, 0.5).

After the attacker receives the defense signal ω_H, the attacker's a posteriori inference about the defender's type is $(\alpha_1, 1-\alpha_1)$. After the attacker receives the defense signal ω_L, the attacker's a posteriori inference about the defender's type is $(\beta_1, 1-\beta_1)$.

Calculate the offensive and defensive game benefits of the attacker and the defender separately according to (14) and (15). When the defender type is θ_L, the spoofing signal is ω_H, attacker adopts strategy A_1, and defender adopts strategy d_1. The utility of both offense and defense is

$$\begin{aligned} U_a(\theta_L, \omega_H, A_1, d_1) &= AR - C_a - AL \\ &= 118.25 - 107.4 - 54.96, \\ &= -44.11 \end{aligned} \tag{16}$$

$$\begin{aligned} U_d(\theta_H, \omega_H, A_1, d_1) &= SPB - C_d - C\ D - S\ DC \\ &= 96.77 - 34.0 - 10.0 - 163.44. \\ &= -110.67 \end{aligned} \tag{17}$$

Similarly, when defenders adopt strategies d_2 and d_3,

$$U_a(\theta_H, \omega_H, A_1, d_2) = -55.21, \tag{18}$$

$$U_d(\theta_H, \omega_H, A_1, d_2) = -87.04, \tag{19}$$

$$U_a(\theta_H, \omega_H, A_1, d_3) = -66.33, \tag{20}$$

$$U_d(\theta_H, \omega_H, A_1, d_3) = -63.40. \tag{21}$$

Because the attacker does not know which strategy the defender adopts, the attacker takes the average benefit of the three defense strategies. The defender can infer the attacker strategy based on the defensive signal released by itself, so the defender adopts the optimal benefits under the three defense strategies. Therefore,

$$U_a(\theta_H, \omega_H, A_1) = -55.21, \tag{22}$$

$$U_d(\theta_H, \omega_H, A_1) = -63.40. \tag{23}$$

In the same way, calculate the benefits under other offensive and defensive strategies.

The offensive and defensive game tree of the initial stage is presented in Figure 8.

6.3. Game Equilibrium Solution and Optimal Defense Strategy Selection. According to the calculation steps given in Section 5.1 and the revenue quantification in Section 6.2, we solve the refined Bayesian equilibrium and select the optimal deception defense strategy.

(1) Offensive and defensive game equilibrium in the initial stage

Calculate the optimal attack strategy inferred by the attacker.

When $\omega_k = \omega_H$, there is

$$\begin{aligned} a^*(\omega_k) \in & \arg\max_{A_j \in S_a} \sum P_a(\theta_h \omega_k) U_a(\theta_h, \omega_k, A_j) \\ = & \arg\max_{A_j \in S_a} \{P_a(\theta_H \omega_H) U_a(\theta_H, \omega_H, A_1) \\ & + P_a(\theta_L \omega_H) U_a(\theta_L, \omega_H, A_1), \\ & P_a(\theta_H \omega_H) U_a(\theta_H, \omega_H, A_2) \\ & + P_a(\theta_L \omega_H) U_a(\theta_L, \omega_H, A_2)\}. \end{aligned} \tag{24}$$

Input: cyber deception signal game model $C\ DS\ GM$, Network environment parameters
Output: optimal defense strategy at each stage
(1) Initialize $(\Theta_d = \{\theta_1, \theta_2, \cdots, \theta_H\})$. //initialize the defender type space.
(2) Initialize $(\omega = \{\omega_1, \omega_2, \cdots \omega_K\})$. //initialize the deception signal space.
(3) Initialize $(S = \{S_d, S_a\}, S_d = \{d_1, d_2, \cdots, d_n\}, S_a = \{A_1, A_2, \cdots, A_n\})$ //initialize the offensive and defensive strategy set.
(4) Initialize $(P_a = \{P_a(\theta_1), P_a(\theta_2), \cdots, P_a(\theta_H)\})$. //initialize a priori belief
(5) while $\theta_h \in \Theta_d, \omega_k \in \omega, d_i \in S_d, A_j \in S_a$ do
(6) $P^*_{T_h} = Urn(n_v, m, e, \varepsilon, T_\tau, T_s, T_a)$
(7) $P^*_{T_b} = Urn(n_v, m, e, \varepsilon, T_\tau, T_s, T_a)$
(8) $U_a(\theta_h, \omega_k, A_j, d_i) = AR - C_a - AL$
(9) $U_d(\theta_h, \omega_k, A_j, d_i) = SPB - C_d - C\ D - S\ DC$
(10) end
(11) for $t = 1; t \le T; t++$ do
(12) Bayesian $(P_a(\theta_h \omega_k))$ //calculate the posterior probability of different information sets.
(13) $a^*(\omega_k) \in \arg\max_{A_j \in S_a} \sum P_a(\theta_h \omega_k) U_a(\theta_h, \omega_k, A_j)$ //calculate the optimal attack strategy.
(14) $\omega^*(\theta_h) \in \arg\max_{\omega_k \in \omega} \sum U_d(\theta_h, \omega_k, a^*(\omega_k))$ //calculate the optimal defense strategy.
(15) Build $(d^*(\theta_h), a^*(d), \widetilde{P}_a(\theta_h \omega_k))$
(16) Output $(d^*(\theta_h))$
(17) end

Algorithm 1: Optimal cyber deception strategy selection algorithm based on the signal game.

Table 4: Vulnerability information in the network.

Symbol	Vulnerability	Attack lethality	Probability of existence (%)
v_1	Improper access control	2	4%
v_2	Memory corruption	6	6%
v_3	Injection	3	8%
v_4	Deserialization	4	12%

Table 5: Atomic attack strategy.

Symbol	Name	Cost	Attack strategy	
			A_1	A_2
a_1	Network scanning	20	√	√
a_2	Network sniffer	30	√	√
a_3	Unauthorized access	50	⊙	
a_4	Remote buffer overflow	100	⊙	
a_5	Code injection	60	⊙	
a_6	Execution	80	⊙	
a_7	No action	0		√

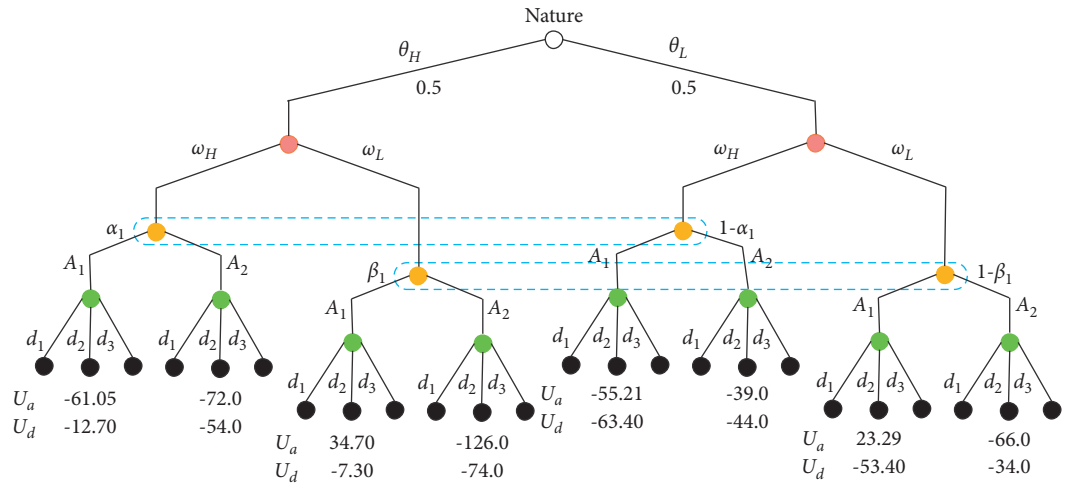

FIGURE 8: Initial stage offensive and defensive game tree.

From this, when $\alpha \in [0,1]$, $a^*(\omega_H) = A_2$.

If $\omega_k = \omega_L$, it can be deduced; when $\beta \in [0,1]$, $a^*(\omega_H) = A_1$.

Calculate the optimal defense strategy inferred by the defender.

When $\theta_h = \theta_H$, there is

$$\begin{aligned}\omega^*(\theta_h) &\in \arg\max_{\omega_k \in \omega} \sum U_d(\theta_h, \omega_k, a^*(\omega_k)) \\ &= \arg\max_{\omega_k \in \omega} \{U_d(\theta_H, \omega_H, a^*(\omega_k)), \\ &\quad U_d(\theta_H, \omega_L, a^*(\omega_k))\} \\ &= \arg\max_{\omega_k \in \omega} \{U_d(\theta_H, \omega_H, A_2), \\ &\quad U_d(\theta_H, \omega_L, A_1)\}.\end{aligned} \tag{25}$$

It can be obtained that $\omega^*(\theta_H) = \omega_L$.

When $\theta_h = \theta_L$, in the same way, $\omega^*(\theta_L) = \omega_H$.

From the above steps, the game equilibrium of the first stage can be obtained as $(\theta_H, \omega_L, A_1)$ and $(\theta_L, \omega_H, A_2)$.

Combined with Bayes' rule, the posterior probability is

$$\begin{aligned}\alpha_1 &= \tilde{P}_a(\theta_H \omega_H) \\ &= P_a(\omega_H \theta_H) P_a(\theta_H) P_a(\omega_H \theta_H) P_a(\theta_H) + P_a(\omega_H \theta_L) P_a(\theta_L) = 0,\end{aligned} \tag{26}$$

$$\begin{aligned}\beta_1 &= \tilde{P}_a(\theta_H \omega_L) \\ &= P_a(\omega_L \theta_H) P_a(\theta_H) P_a(\omega_L \theta_H) P_a(\theta_H) + P_a(\omega_L \theta_L) P_a(\theta_L) = 1.\end{aligned} \tag{27}$$

The obtained posterior inference is used as a priori inference for the attacker in the next stage.

From the definition of refined Bayesian equilibrium, $(\theta_H, \omega_L, A_1)$ and $(\theta_L, \omega_H, A_2)$ are separating equilibrium and can be expressed uniformly as $[(\theta_H, \theta_L) \longrightarrow (\omega_L, \omega_H) \longrightarrow (A_1, A_2), \alpha_1 = 0, \beta_1 = 1]$. In this balance, when the defender chooses a high-level defense type θ_H, we release the defense signal ω_L. After receiving the signal ω_L, the attacker adopts the strategy A_1; at this time, the defender's gain is -7.30. When the defender chooses a high-level defense type θ_L, we release the defense signal ω_H. After receiving the signal ω_H, the attacker adopts the strategy A_2; at this time, the defender's gain is −44.0.

In the later stages, the deceptive effect of the signal begins to decay, expressed as $\delta_t = \delta_{t-1} - 0.1$.

(2) Offensive and defensive game equilibrium in the k-th stage

The attenuation factor at this stage is $\delta_k = 1 - 0.1 \cdot (k-1)$. When $k = 5$, a priori inference can be obtained as $(0.6, 0.4)$. This phase of the offensive and defensive game tree is presented in Figure 9. Using the method in Section 5.1 to solve

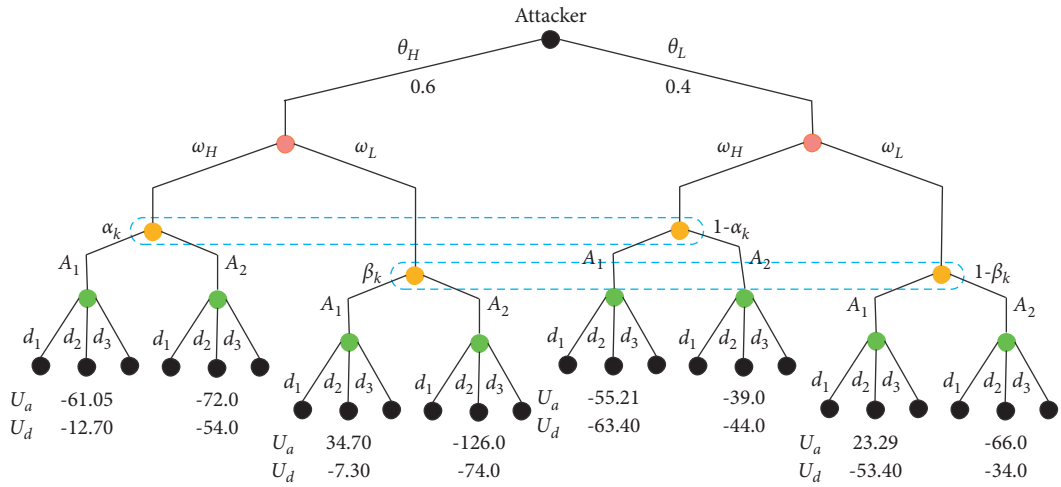

Figure 9: offensive and defensive game trees in the k-th stage.

the refined Bayesian equilibrium, the pooling equilibrium can be obtained as $[(\theta_H, \theta_L) \longrightarrow (\omega_L, \omega_L) \longrightarrow (A_1, A_1), \alpha_k = 0.6, \beta_k = 1]$. In this balance, when the defender chooses the defense type θ_H, its gain is -7.30. And when the defender chooses the defense type θ_L, its gain is -53.40.

(3) Offensive and defensive game equilibrium in the n-th stage

As the game progresses, the deceptive effect of the defense signal gradually disappears and eventually degenerates into an incomplete information static game. This phase of the offensive and defensive game tree is shown in Figure 10.

The defender's optimal strategy can be obtained by solving the offensive and defensive games in this phase. When the defender chooses the high-level defense θ_H, the attacker takes the strategy A_1, and the defender's gain is -12.70. And when the defender chooses the low-level defense θ_L, the attacker takes the strategy A_1, and the defender gains -53.40.

In the experimental environment built in Section 6.1, comparing the CDSGM model of this paper with the incomplete information static game model, the results obtained are presented in Figure 11.

As shown from Figure 11, the defense utilities remain unvaried in the early stage of the network offensive and defensive game, indicating that the offensive and defensive strategy has not changed. The defense utilities decrease when the deceptive effect of the signal decays to a certain extent, indicating that the attacker's strategy has changed, and the defender's strategy has also been adjusted accordingly. Ultimately, the deceptive effect of the signal decays to zero and the defense gain is the same as that of the incomplete information static game.

The game simulated in the paper is compared with other approaches in Table 7. We conducted a multistage offensive and defensive game in a dynamic game with incomplete information. At the same time, we carried out detailed profit quantification and equilibrium solution, which is more in line with the actual attack and defense scenario, and the results can guide the defense decision much more precisely.

6.4. Experiment Analysis. The following conclusions can be drawn through the analysis of the above offensive and defensive game process and game equilibrium.

(1) The defender can use the signaling mechanism to influence the offensive and defensive game process directly and the selection of the attacker's strategy, thus increasing the defender's initiative in the offensive and defensive process. The attacker obtains a posteriori inferences based on the prior probabilities and the defense signals released by the defender and corrects the inference about the defender type. During the preliminary offensive and defensive game, a high-level defender, by releasing low-level defense signals, can lure the attacker into attacking it. Likewise, a low-level defender can achieve the goal of deterring attackers by releasing a high-level defense signal. Hence, using the signaling mechanism, the defender is able to influence the attacker's strategy choice and obtain a defense effect that exceeds the capability. Furthermore, the defender can choose different strategies depending on the purpose.

(2) The deceptive effect of defense signals is somewhat attenuated in the multistage network attack and defense game. During the early attack and defense game, the defender disables the attacker from accurately implementing the optimal attack strategy by releasing signals that are opposite to the type of defense. Thus, the defense gain is improved. However, as the game proceeds, the deceptive effect of the defense signal gradually decays. Until the n-th stage, the deception effect disappears and the network attack and defense game degenerates into a static game with incomplete information. For this reason, the limited deceptive role of defense signals in the game process should be recognized, and the

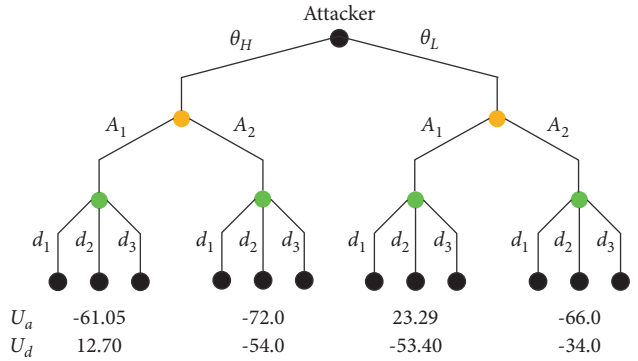

Figure 10: Offensive and defensive game trees in the n-th stage.

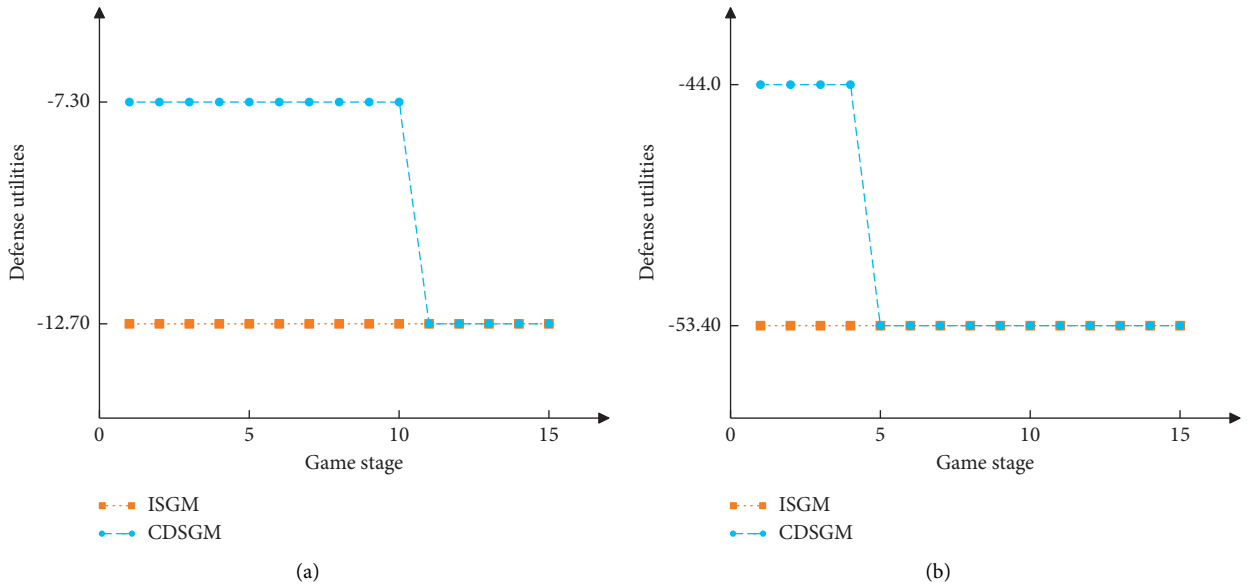

Figure 11: Defensive utility in each stage of the offensive and defensive game. (a) Defense type is θ_H. (b) Defense type is θ_L.

Table 6: Parameters in the revenue quantification.

Notation	Description	Values
n_v	The size of the virtual network topology	1024
m	The number of real hosts in the network	20
e_H	The number of decoy nodes when the defense level is θ_H	40
e_L	The number of decoy nodes when the defense level is θ_L	20
L_h	The loss of the host being attacked	190
R_b	The reward of the bait node being attacked	280
R_h	The reward of the attack to the host	270
L_b	The loss caused by the attack to the bait node	180
C_{bait}	The cost of deploying a bait node	1
C_{conv}	The cost of IP address conversion per node	0.5
C_{tran}	The cost of IP address transfer per node	1

Table 7: Comparison of research methods.

Reference	Type of game	Process of game	Equilibrium solution	Game deduction	Revenue quantification	Algorithm complexity
Ref. [21]	Complete information static	Single stage	Simple	Idealized	Simple	$O(mn)$
Ref. [22]	Incomplete information static	Single stage	Simple	Idealized	Simple	$O(mn)$
Ref. [23]	Complete information dynamic	Multistage	Simple	Idealized	Simple	$O(n+m)^2$
Ref. [24]	Incomplete information dynamic	Single stage	Detailed	Idealized	Simple	$O(n^2+m^2)$
Ref. [25]	Incomplete information dynamic	Multistage	Detailed	Realistic	Simple	$O(2(n^2+m^2))$
Our work	Incomplete information dynamic	Multistage	Detailed	Realistic	Detailed	$O(n^2+m^2)$

preemptive network deception utility should be fully utilized. Consideration should also be given to delay the decay of the signal spoofing effect, e.g., releasing the real signal occasionally.

(3) Realizing the combination of cyber deception defense and CTI will be more helpful to deal with network intrusion. The cyber deception defense method proposed in this paper is able to attract aggressors to attack decoy nodes through a signaling mechanism. The evidence captured on the decoy node is treated as attacks infection with low false-positive and this evidence can also be used as the context of the attacks. This information contributes to the generation of CTI. On the flip side, cyber threat intelligence analysis can help understand aggressors' tactics, techniques, and procedures (TTPs), which can help form targeted defense plans to protect actual systems in the network.

7. Conclusion

To address the problems of insufficient proactivity and easy invalidation of existing cyber deception techniques, this paper proposed a cyber deception defense method based on the signal game. In this paper, we combined MTD and cyber deception defense to enhance the effectiveness of cyber deception defense. On this basis, an offensive and defensive game model based on the signal game was constructed, and the signaling mechanism was used to influence the choice of the attacker's strategy, which improved the initiative of cyber deception defense and maximized the defender's revenue. Meanwhile, we quantified the offensive and defensive gains based on probabilistic models to make the strategy selection consistent with the network offensive and defensive reality. Finally, we verified the effectiveness of the proposed method through simulation experiments and summarized the characteristic regularity of cyber deception defense based on the signal game. In terms of defense effectiveness, the defense method proposed in this paper can increase aggressors' difficulty in attacking real systems. And it increases the probability of aggressors attacking decoy nodes, so as to collect aggressor information and obtain CTI.

In the future, we will consider adjusting the defense strategy to solve the signal attenuation problem existing in the gaming process, so as to make the deception signal achieve a better deception effect. In addition, we can integrate threat analysis tools and use the attack information captured by decoy nodes to formulate defense plans.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This research is partially supported by the National Natural Science Foundation of China under Grant nos. 62002377, 62072424, 61772546, 61625205, 61632010, 61751211, 61772488, and 61520106007; Key Research Program of Frontier Sciences, CAS, no. QYZDY-SSW-JSC002; NSFC with nos. NSF ECCS-1247944 and NSF CNS 1526638; and in part by the National Key Research and Development plan, no. 2017YFB0801702, 2018YFB1004704.

References

[1] C. Wang and Z. Lu, "Cyber deception: Overview and the road ahead," *IEEE Security & Privacy*, vol. 16, no. 2, pp. 80–85, 2018.

[2] T. D. Wagner, K. Mahbub, E. Palomar, and A. E. Abdallah, "Cyber threat intelligence sharing: Survey and research directions," *Computers & Security*, vol. 87, p. 101589, 2019.

[3] H. Almohannadi, I. Awan, J. Al Hamar, A. Cullen, J. P. Disso, and L. Armitage, "Cyber threat intelligence from honeypot data using elasticsearch," in *Proceedings of 2018 IEEE 32nd International Conference on Advanced Information Networking and Applications*, AINA, Krakow, Poland, pp. 900–906, 2018.

[4] E. Vasilomanolakis, S. Karuppayah, P. Kikiras, and M. Mühlhäuser in *Proceedings of the 8th International Conference on Security of Information and Networks*, SIN '15, Association for Computing Machinery, New York, NY, USA, pp. 158–164, 2015.

[5] M. Skrzewski, "About the efficiency of malware monitoring via server-side honeypots. Computer Networks," Edited by

P. Gaj, A. Kwiecień, and P. Stera, Eds., Springer International Publishing, Cham, pp. 132–140, 2016.

[6] H. Mun and K. Han, "Blackhole attack: user identity and password seize attack using honeypot," *Journal of Computer Virology and Hacking Techniques*, vol. 12, no. 3, pp. 185–190, 2016.

[7] T. Sochor, M. Zuzcak, and P. Bujok, "Analysis of attackers against windows emulating honeypots in various types of networks and regions," in *Proceedings of 2016 Eighth International Conference on Ubiquitous and Future Networks (ICUFN)*, IEEE, Vienna, Austria, pp. 863–868, 2016.

[8] Z. Saud and M. H. Islam, "Towards proactive detection of advanced persistent threat (apt) attacks using honeypots," in *Proceedings of*, SIN '15, Association for Computing Machinery, New York, NY, USA, pp. 154–157, 2015.

[9] A. O. Olagunju and F. Samu, "In search of effective honeypot and honeynet systems for real-time intrusion detection and prevention," in *Proceedings of*, Association for Computing Machinery, New York, NY, USA, pp. 41–46, 2016.

[10] J. Uitto, S. Rauti, S. Laurén, and V. Leppänen, "A survey on anti-honeypot and anti-introspection methods," in *Recent Advances in Information Systems and Technologies*, Á. Rocha, A. M. Correia, H. Adeli, L. P. Reis, and S. Costanzo, Eds., Springer International Publishing, Cham, 2017.

[11] B. Li, Y. Xiao, Y. Shi, Q. Kong, Y. Wu, and H. Bao, "Anti-honeypot enabled optimal attack strategy for industrial cyber-physical systems," *IEEE Open Journal of the Computer Society*, vol. 1, pp. 250–261, 2020.

[12] P. Chen, L. Desmet, and C. Huygens, *A Study on Advanced Persistent Threats. Communications and Multimedia Security*, B. De Decker and A. Zúquete, Eds., Springer Berlin Heidelberg, Berlin, Heidelberg, 2014.

[13] R. Zhuang, S. A. DeLoach, and X. Ou, "Towards a theory of moving target defense," in *Proceedings of*, MTD '14, Association for Computing Machinery, New York, NY, USA, pp. 31–40, 2014.

[14] S. Chang, Y. Park, and B. B. Ashok Babu, "Fast ip hopping randomization to secure hop-by-hop access in sdn," *IEEE Transactions on Network and Service Management*, vol. 16, no. 1, pp. 308–320, 2019.

[15] V. A. Cunha, D. Corujo, J. P. Barraca, and R. L. Aguiar, "Totp moving target defense for sensitive network services," *Pervasive and Mobile Computing*, vol. 74, p. 101412, 2021.

[16] M. Torquato, P. Maciel, and M. Vieira, "Security and availability modeling of vm migration as moving target defense," in *Proceedings of 2020 IEEE 25th Pacific Rim International Symposium on Dependable Computing (PRDC)*, pp. 50–59, PRDC, 2020.

[17] A. Clark, K. Sun, and R. Poovendran, "Effectiveness of ip address randomization in decoy-based moving target defense," *52nd IEEE Conference on Decision and Control*, pp. 678–685, 2013.

[18] J. Sun and K. Desir, "DESIR: Decoy-enhanced seamless IP randomization," in *Proceedings of IEEE INFOCOM 2016The 35th Annual IEEE International Conference on Computer Communications*, pp. 1–9, 2016.

[19] J. Sun, K. Sun, and Q. Li, "CyberMoat: Camouflaging critical server infrastructures with large scale decoy farms," in *Proceedings of 2017 IEEE Conference on Communications and Network Security (CNS)*, pp. 1–9, IEEE Conference on Communications and Network Security (CNS), 2017.

[20] S. Wang, Q. Pei, Y. Zhang, X. Liu, and G. Tang, "A hybrid cyber defense mechanism to mitigate the persistent scan and foothold attack," *Security and Communication Networks*, pp. 1–15, 2020.

[21] W. Jiang, B. X. Fang, and Z. TIAN, "Defense strategies selection based on attack-defense game model," *Journal of Computer Research and Development*, vol. 47, no. 12, pp. 818–827, 2014.

[22] Z.H. Hengwei, Y.J. Dingkun, L.D. Tao, and W.T. Jindong, "Active defense strategy selection based on static bayesian game," in *Proceedings of Technology (CCT 2015) Third International Conference on Cyberspace Technology*, pp. 1–7, CCT 2015, 2015.

[23] L. Wangqun, W. Hui, L. Jiahong et al., "Research on active defense technology in network security based on non-cooperative dynamic game theory," *Journal of Computer Research and Development*, vol. 48, no. 2, p. 306, 2011.

[24] Z. Hengwei, Y. Dingkun, H. Jihong, W. Jindong, and L. Tao, "Defense policies selection method based on attack-defense signaling game model," *Journal on Communications*, vol. 37, no. 5, p. 51, 2016, http://www.infocomm-journal.com/txxb/EN/abstract/article157318.shtml.

[25] Y. Hu, H. Zhang, Y. Guo, T. Li, and J Ma, "A novel attack-and-defense signaling game for optimal deceptive defense strategy choice," *Wireless Communications and Mobile Computing*, vol. 2020, 2020.

[26] C. Gao, Y. Wang, X. Xiong, and W. Zhao, "Mtdcd: an mtd enhanced cyber deception defense system," in *Proceedings of IEEE 4th Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC)*, vol. 4, pp. 1412–1417, IEEE, 2021.

[27] H. Mahmoud, *Pólya Urn Models*, CRC Press, 2008.

[28] T. E. Carroll, M. Crouse, E. W. Fulp, and K. S. Berenhaut, "Analysis of network address shuffling as a moving target defense," in *Proceedings of IEEE international conference on communications (ICC)*, pp. 701–706, IEEE, 2014.

[29] M. Crouse, B. Prosser, and E. W. Fulp, "Probabilistic performance analysis of moving target and deception reconnaissance defenses," *Proceedings of the Second ACM Workshop on Moving Target Defense*, pp. 21–29, 2015.

[30] Z. Pang, G. Liu, D. Zhou, and D. Sun, "Secure networked Control under Deception attacks," *Networked Predictive Control of Systems with Communication Constraints and Cyber Attacks*, pp. 147–163, 2019.

[31] Rapid7, *Vulnerability Intelligence Report*, https://www.rapid7.com/research/report/vulnerability-intelligence-report/2020, 2020.