Research Article

Exploring the Optimum Proactive Defense Strategy for the Power Systems from an Attack Perspective

Jinxiong Zhao , Xun Zhang, Fuqiang Di, Sensen Guo, Xiaoyu Li, Xiao Jing, Panfei Huang, and Dejun Mu

School of Cybersecurity, Northwestern Polytechnical University, Xi'an, Shaanxi 710072, China

Correspondence should be addressed to Jinxiong Zhao; jxzhao1229@163.com

Received 30 December 2020; Revised 19 January 2021; Accepted 4 February 2021; Published 12 February 2021

Academic Editor: James Ying

Copyright © 2021 Jinxiong Zhao et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Proactive defense is one of the most promising approaches to enhance cyber-security in the power systems, while how to balance its costs and benefits has not been fully studied. This paper proposes a novel method to model cyber adversarial behaviors as attackers contending for the defenders' benefit based on the game theory. We firstly calculate the final benefit of the hackers and defenders in different states on the basis of the constructed models and then predict the possible attack behavior and evaluate the best defense strategy for the power systems. Based on a real power system subnet, we analyze 27 attack models with our method, and the result shows that the optimal strategy of the attacker is to launch a small-scale attack. Correspondingly, the optimal strategy of the defender is to conduct partial-defense.

1. Introduction

Energy is one of the most important forces to promote the development of industry in the entire society. The energy systems, the only channels for energy transmission, are responsible for the stable transmission of energy. As the primary branch of the energy systems, the power systems have been the focus to be assaulted in recent years [1]; in 2010, a power plant in Iran was attacked by the Stuxnet virus, which made the Iranian nuclear power plant lose its power generation capacity for a short time [2]; in 2014, the malicious software Black Energy invaded into USA power turbines during which USA power systems suffered a total of no less than 79 hacker attacks; in 2015, Ukrainian power systems were attacked by a malicious code, which caused a large-scale blackout; in 2016, a great many computers of the power systems, attacked in Israel by hackers, were in a suspended state; in 2019, many major hydropower stations in Venezuela were under cyber-attack, which occurred in more than half of the regions with a large-scale power outage for more than 6 days.

The fundamental reason that energy systems such as the power systems can be frequently attacked successfully is that the protection strategy of each system is passive and static and it does not have an autoimmune function [3]. For such prominent problems, a lot of researches on proactive defense have been conducted in the industry areas and the related works include moving target defense, mimic defense, and end-to-end hopping [3, 4]. The abovementioned proactive defense technologies have made considerable progress in theory, but the disadvantage is that it needs to take a huge cost to build a system with the above defense attributes, which is often unbearable. For the sake of solving this problem, many scholars have applied game theory to network security defense, but so far, there have been fewer reports on game theory that can be employed to solve security problems in the real power production systems.

In this paper, we firstly introduce some related typical works in the field of active and proactive defense. Secondly, a single and dual game model between the hackers and defenders of the power systems, based on the introduction of game theory, is constructed. Then, the established attack and

defense model is verified by the production environment attack data from a real power systems subnet. Finally, the model that matches the real production environment is used to predict the hostile attack strategy in the next month and the key defense points of the power systems under the current situation are given.

The significant contribution of this article is to provide a qualitative method for evaluating external attacks for the power systems, which is as follows: the idea with the revenue of the power systems being robbed is proposed for the first time; taking a subnet in a real power systems as an example, three single and dual attack and defense models are discussed in detail, respectively; the theoretical model in line with the real production environment was established and verified by the attack data in actual production; the best revenues of the attack and defense sides are calculated separately, and the best defense modes for the power systems when facing different attack scales are given. Overall, the main contributions of our works are as follows:

- (1) Compared with the mimic defense and moving target defense methods in the current industry, we propose a relatively low-cost proactive defense method based on game theory.
- (2) By calculating the best benefits of the attacker and defender in the game, we can predict the most likely attack behavior and provide more targeted defense strategy for the power systems.
- (3) We have evaluated the benefits of the three combined attack strategies that are closer to the actual attack situations for both the attacker and defender and verified it with actual attack data.

2. Related Work

Currently, there are many related reports on active defense on active network defense, mainly including moving target defense (MTD), mimic security defense (MSD), end information hopping (EIH), game theory defense technologies (GTD), and information theory approach (ITA) [5, 6]. Deformation networks, adaptive computer networks, self-cleaning networks, and open-flow random host conversion technologies are widely reported in MTD, and the essence of them is to make it difficult for an attacker to accurately grasp the information of the target systems by proactively changing its relevant configuration within a certain time interval. The advantage of this theory is that it can improve the security of the systems attacked by forcing the attacker to continuously increase attack cost, but the pain points inside are needing a huge available configuration space to support the operation of this defense technology. The concept of MSD is fairly similar to that of MTD. Both technologies enable defenders to realize rapid migration in a diverse environment, thereby augmenting the difficulty degree of the hackers. Compared with MTD, MSD has more heterogeneous redundant architectures with the disadvantages that require huge investment cost, while MTD provides limited heterogeneous redundant architectures, which can be regarded as a special case of MTD. EIH, composed of

early warning, collaborative control, information management, and task switching function modules, mainly protects the two communication parties by changing crucial information such as the protocol, address, and port between the two communication ends. GTD is a network defense technology based on game theory, which belongs to the theory of beforehand decision analysis and has been used in the field of network security for many years. Although the abovementioned methods have a certain effect on the actual environment, the common problem is that these designs are expensive.

Game theory is an ideal solution to the problem of high cost in proactive defense methods. Many scholars have done a lot of research on it. Radha et al. proposed a game theory optimization routing framework for wireless networks, which provided a solution for the realization of low-energy routing [7]. Zhu and Basar explored the game mechanism of the optimal cross-layer flexible control system to enhance the robustness and security of the cyber-physical system [8]. Zhao et al. studied the game theory model based on the distribution market and solved the problem of the coordinated operation of multiple microgrids [9]. Rass and Zhu analyzed the defense-in-depth strategy of advanced persistent threats and proposed a method to deal with the threats [10]. Chen et al. used dynamic game theory to design a network protection and recovery system for infrastructure to ensure reliable service provision [11]. Miao et al. established a zero-sum mixed state random game model to solve different types of attacks on cyber-physical systems [12].

The abovementioned method based on game theory does solve many relevant network security problems. However, it neither calculates the value of offense and defense benefits nor does it use real-world attack data of power systems to verify its theoretical model. Therefore, the problem solved in this paper is how to use game theory to model real industrial control systems and how to qualitatively give the best protection strategy for power systems.

3. Preliminaries

3.1. Bayesian Game Theory. Bayesian game is also called incomplete information game, which means that at least one player among multiple players is not completely clear about the revenues or revenue functions of the remaining players. In this article, incomplete information means that the defender on the power systems does not know the method and purpose of the hackers. Similarly, the hackers are not fully aware of the power systems. Thus, we need to introduce the Bayesian game model to analyze the possible behaviors and revenues of both parties. Bayesian game is not repeated here because the existing literature is very detailed about it [13, 14].

3.2. Attack and Defense Model Construction of the Power Systems. Many factors that affect the safe operation of the power systems and the main targets that most likely to be attacked are focused on, including the host, network, and management. Here, we primarily build the single and dual

models of the power systems among which the single models include host, network, and management model and the dual models include host and network, host and management, and network and management model.

Under normal circumstances, a considerable revenue, recorded as the total revenue s , can be obtained by defenders from their assets inside the power systems. In consideration of the assets characteristics with wide coverage and multifaceted feature, there will always exist potential security vulnerabilities and this part, denoted as l , is defined as the inherent loss. The hackers frequently utilize various vulnerabilities in an attempt to reduce the defender's revenue. At this time, the hackers' benefit and cost are proportional to the attack size. When the defense side detects that the malicious forces from outside are attempting to damage the power system, it will consume a certain cost and adopt corresponding defense strategies to intercept. Once the power system is severely damaged, it needs at a significant cost to repair it. In this paper, the deliberate attack scale from the outside world is divided into three categories: large-scale, small-scale, and no-attack. The defense strategy in the power systems is divided into complete-defense, partial-defense, and no-defense. Judging from the data about the centralized attacks on the power systems organized by government departments every year, the main targets of the attack are the host, network, and management. The corresponding risk levels are 2, 3 and 2, respectively. According to the respective damage levels, specific values are assigned to the parameters in the models, as shown in Figure 1, and the specific meaning is listed in Table 1. Besides, the original benefits in the adversarial sides are increased by 10 to be convenient for processing data.

3.3. Single Attack-Defense Models

3.3.1. Host Attack-Defense Model. Considering that each attack/defense is a frequently organized and complicated process, all kinds of costs and revenues here are relative values and greater than zero. The expenditure cost from the hackers on large-scale, small-scale, and no-attack can be expressed as a matrix s_a , and the expenditure cost of the power systems on complete-, partial-, and no-defense can be expressed as a matrix s_d :

$$\begin{aligned} s_a &= \begin{bmatrix} -t \\ -(t - \Delta t) \\ 0 \end{bmatrix}, \\ s_d &= \begin{bmatrix} -p \\ -(p - \Delta p) \\ 0 \end{bmatrix}. \end{aligned} \quad (1)$$

There are three defense modes for the power systems to choose each time, and every defense mode may face any attack strategies from outside. In the following, the overall revenue matrix s_e obtained by the hackers is given in detail, among which the complete-, partial-, and no-defense in the power systems are taken as row vectors and the large-scale,

FIGURE 1: The value of different variables.

small-scale, and no-attack from the attackers are used as column vectors, respectively:

$$s_e = \begin{bmatrix} q & q + \Delta q & q + n^* \Delta q \\ \Delta q & q & q + \Delta q \\ 0 & 0 & 0 \end{bmatrix}. \quad (2)$$

At this time, according to the abovementioned discussion of various parameters in both sides, the total revenue of the hackers under different attack strategies corresponding to the different defense modes can be calculated, as shown in Figure 2. In the complete-defense mode, Figure 2(a) shows that the gained revenue by the hackers reaches maximum when they adopt large-scale strategy, with the result that the revenue in the power systems is forced to drop to the bottom, but the cost paid by the hackers is also huge. In partial-defense mode, Figure 2(b) reveals that the two sides reach the Nash equilibrium when the hackers use small-scale strategy. In no-defense mode, Figure 2(c) indicates that both sides also reach the Nash equilibrium when the hackers employ a small-scale strategy. It can be concluded that the probability of adopting small- and large-scale strategies for the hackers, respectively, is 2/3 and 1/3 corresponding to the three defense modes that the defender can choose. Therefore, the small-scale attack should be paid close attention to in-host attack and defense model.

3.3.2. Network Attack and Defense Model. The construction process of the network attack and defense model is the same as that of the host, and the cost of both sides is exactly the same as the matrix (1). Considering the openness and accessibility of the network, the extent of injury from an attacker via the network is slightly higher than that of the host, so its specific revenue is shown in the following matrix:

$$s'_e = \begin{bmatrix} 2q & 2q + \Delta q & 2q + n^* \Delta q \\ n^* \Delta q & 2q & 2q + \Delta q \\ 0 & 0 & 0 \end{bmatrix}. \quad (3)$$

TABLE 1: Summary of symbols and meaning.

Symbols	Meaning
t	The cost of a large-scale attack
$t - \Delta t$	The cost of a small-scale attack
$p - \Delta p$	The cost of a partial-defense
q	The benefit made by the attacker with launching a large-scale attack when the defender is in a state of complete-defense
$q + \Delta q$	The benefit made by the attacker with launching a large-scale attack when the defender is in a state of partial-defense
$q + n^* \Delta q$	The benefit made by the attacker with launching a large-scale attack when the defender is in a state of no-defense
q	The benefit made by the attacker with launching a small-scale attack when the defender is in a state of partial-defense
$q + \Delta q$	The benefit made by the attacker with launching a small-scale attack when the defender is in a state of no-defense
l	Inherent loss
s	The total benefit obtained by the defender using its own assets

FIGURE 2: Under (a), (d), and (g) complete-defense mode, (b), (e), and (h) partial-defense mode, and (c), (f) and (i) no-defense mode, both sides benefit when the hackers launch different attack strategies.

Next, according to the cost of both sides and the revenue obtained by the hackers, we have calculated their total revenues in different states, as shown in Figure 2. Although the defender chooses complete-defense mode in Figure 2(d), the hackers still make very considerable gains by using large-scale strategy, owing to the network openness and its own various flaws such as protocol loopholes. Furthermore, the hacker revenue in Figure 2(d) is higher than that of the power systems and both sides have reached the Nash equilibrium, but considering the cost, this attack strategy will only be employed at a particular moment; in partial-defense mode, both sides reach the Nash equilibrium when the hackers adopt the small-scale strategy, and the revenue of the hackers is greater than that of the power systems, as shown in Figure 2(e); in no-defense mode, Figure 2(f) displays that the two sides also reach the Nash equilibrium when the hackers use small-scale strategy. At this moment, the hackers reach the optimal value in terms of costs and revenues.

In these three defense modes, the probability of small-scale strategy (2/3) is greater than the probability of large-scale strategy (1/3). It is worth noting that the conditions for the emergence of large-scale strategy are that the defender must select complete-defense mode and the hackers are willing to be at all costs.

3.3.3. Management Attack and Defense Model. The construction of the management attack and defense model is also similar to the network and the cost of both sides is identical with matrix (1). Different from the above-mentioned network attack and defense model, the degree of attack severity through management defects is lower than that of the host, and its specific revenue is presented in the following matrix:

$$s_e'' = \begin{bmatrix} q^{1/2} & q^{1/2} + \Delta q & q^{1/2} + n^* \Delta q \\ \Delta q^{1/2} & q^{1/2} & q^{1/2} + \Delta q \\ 0 & 0 & 0 \end{bmatrix}. \quad (4)$$

Then, based on the known costs and the gains obtained, the total revenues of the attack and defense parties in different states can be calculated, as shown in Figure 2. The data in Figure 2(g) indicate that the cost paid by the hackers is far higher than their revenues when large- and small-scale strategies are adopted. It can be inferred from the above that the best attack strategy of the hackers is to keep a static state and then both sides reach the Nash equilibrium with the defender being in complete-defense mode. In partial-defense mode, the hackers would try to remain stationary since Figure 2(h) indicates that the revenue of the hackers, although higher than in other cases, is still minimal with large-scale attacks. As a result, the power systems achieve the maximum revenue with a state of Nash equilibrium. Obviously, the situation in Figure 2(i) is similar to Figure 2(h).

In the management attack and defense model, it is fairly difficult for the hackers to find out a breakthrough point to invade the power systems because the various management measures on it are relatively complete. Therefore, the smartest choice for an attacker is to use a static observation strategy.

3.4. Dual Attack and Model

3.4.1. Host and Network Attack and Defense Model. In the general host and network policy configuration process, the security policy configuration of the host or network is usually completed first, and then the rest of the policy settings are completed in turn. The default security policy setting order in this part is host network. It is known that many security policies are often universal. Here, the security policies that have been set in the host and can be used in the network are recorded as cost savings. The following lists the cost savings matrix s_s of the host in complete-, partial-, and no-defense:

$$s_s = \begin{bmatrix} \tau & \\ \tau - \Delta\tau & \\ 0 & \end{bmatrix}. \quad (5)$$

According to the cost saved by matrix (5), it can be calculated that the defense cost paid by the power systems in the case of complete-, partial-, and no-defense of the host is displayed in the matrix s_1 , s_2 , and s_3 :

$$\begin{aligned} s_1 &= \begin{bmatrix} -p + \tau & \\ -(p - \Delta p) + \tau & \\ \tau & \end{bmatrix}, \\ s_2 &= \begin{bmatrix} -p + \tau - \Delta\tau & \\ -(p - \Delta p) + \tau - \Delta\tau & \\ \tau - \Delta\tau & \end{bmatrix}, \\ s_3 &= \begin{bmatrix} -p & \\ -(p - \Delta p) & \\ 0 & \end{bmatrix}, \end{aligned} \quad (6)$$

that the overall revenue required by various attack methods minus its cost is the ultimate revenue of the attack side. The final revenue on the power systems is that its total revenue subtracts the inherent loss, defense cost, and the plundered revenue. Thus, under the complete-, partial-, and no-defense of the host, the total revenue of the attack side can be gotten via the calculation process provided above, which is the average of the sum of the revenues of the corresponding host and network single model, as shown in the following matrix:

$$s_{hc}^I = \begin{bmatrix} \frac{3q}{2} & \frac{(3q + 2\Delta q)}{2} & \frac{(3q + 2n\Delta q)}{2} \\ \frac{(n+1)\Delta q}{2} & \frac{3q}{2} & \frac{(3q + 3\Delta q)}{2} \\ 0 & 0 & 0 \end{bmatrix}. \quad (7)$$

Facing the three defense modes of the power systems, Figure 3 analyzes the final revenue that an attacker can achieve by using three different attack strategies. In the first place, we discuss the revenues of the attack and defense sides when the host is in complete-defense mode: with the network being complete-defense, the most likely outcome is

FIGURE 3: Under (a) Complete-defense of host and network, (b) complete-defense of host and partial-defense of network, (c) complete-defense of host and no-defense of network, (d) partial-defense of host and complete-defense of network, (e) partial-defense of host and network, (f) partial-defense of host and no-defense of network, (g) no-defense of host and complete-defense of network, (h) no-defense of host and partial-defense of network, and (i) no-defense of host and network, both sides benefit when the hackers launch different attack strategies.

that the attack side would adopt large-scale strategy to maximize its revenue, which is very close to the value of the power systems in Figure 3(a). In Figure 3(b), the revenue obtained by the hackers using small-scale strategy is almost equal to that obtained with large-scale strategy, and the two sides reach the Nash equilibrium; therefore, the possibility of suffering small-scale attack is the greatest in the case of network partial-defense; Figure 3(c) shows that the attack revenue is higher than that of the other two strategies when

small-scale strategy is employed by an attacker to destroy the power systems, which enable the two sides to reach the Nash equilibrium, it is why most of the outside invaders launch small-scale strategy when the network is in no-defense.

Afterwards, we discuss the revenue made by the attack and defense sides when the host is in partial-defense mode: as shown in Figure 3(d), small-scale strategy is the most unfavorable tactic for the hackers and its revenue is negative, while large-scale strategy makes the hackers' revenue

basically equal to that of the power systems and the both sides reach the Nash equilibrium. The data in Figure 3(d) indicates that the power systems are more likely to be subjected to large-scale attacks when the network is set as complete-defense mode; obviously, small-scale strategy makes the revenue of the attack and defense parties achieve the Nash equilibrium, as shown in Figure 3(e), which demonstrates that the most probable attack strategy is to launch a small-scale attack when the network is in partial-defense mode; the situation in Figure 3(f) is extremely similar to Figure 3(e).

Finally, we discuss the revenues of the attack and defense sides when the host is in no-defense mode: it can be seen from Figure 3(g) that small-scale strategy not only fails to break the defense of the power systems but also makes the attack side pay a huge price. On the contrary, large-scale strategy can maintain the revenues of both parties at a balanced point. Consequently, it must be alert to large-scale attack from the enemy when the network adopts complete-defense; the hackers utilize small-scale strategy to receive the same revenue as the power systems, and the two sides have reached the state of Nash equilibrium, as shown in Figure 3(h), when the network adopts partial-defense. At this time, we must pay more attention to the loss caused by small-scale strategy adopted by the attack side; when the network adopts no-defense, Figure 3(i) displays that small-scale strategy launched by the hackers has the largest gain and is also the most desirable strategy compared with the cost paid by large-scale strategy. Thus, small-scale strategy remains the focus of attention.

Based on the above discussion, this part lists nine possible combinations in host and network attack and defense model among which the probability that the hackers may adopt large- and small-scale strategies is 3/9 and 6/9, respectively. Therefore, it is critical to be aware of small-scale strategy implemented by the attack side for most of the time. In special circumstances, the possibility of an attacker launching a large-scale strategy is not ruled out.

3.4.2. Host and Management Attack and Defense Model. The possibility of an attacker carrying out a malicious attack on the host and management is also bound to exist. The main discussion here is to consider the establishment of host and management attack and defense model when the host security policy has been completed. In view of the low cross degree of the security strategy between the host and management, the cost saving matrix s'_s of the host during complete, partial-, and no-defense is as follows:

$$s'_s = \begin{bmatrix} \tau^{1/2} \\ \tau^{1/2} - \Delta\tau^{1/2} \\ 0 \end{bmatrix}. \quad (8)$$

Similarly, according to the cost saved in matrix (8), the defense costs paid by the side of the power systems in the above three cases (complete-, partial-, and no-defense) can be calculated, respectively, as the matrix s'_1 , s'_2 , and s'_3 as follows:

$$\begin{aligned} s'_1 &= \begin{bmatrix} -p + \tau^{1/2} \\ -(p - \Delta p) + \tau^{1/2} \\ \tau^{1/2} \end{bmatrix}, \\ s'_2 &= \begin{bmatrix} -p + \tau^{1/2} - \Delta\tau^{1/2} \\ -(p - \Delta p) + \tau^{1/2} - \Delta\tau^{1/2} \\ \tau^{1/2} - \Delta\tau^{1/2} \end{bmatrix}, \\ s'_3 &= \begin{bmatrix} -p \\ -(p - \Delta p) \\ 0 \end{bmatrix}. \end{aligned} \quad (9)$$

The calculation process of the total revenue of the hackers in this type of model is similar to matrix (7). The total revenue here is the average of the sum of the corresponding host and management single model, as shown in the following matrix:

$$s_{hm}^I = \begin{bmatrix} \frac{q + q^{1/2}}{2} & \frac{q + q^{1/2} + \Delta q + \Delta q^{1/2}}{2} & \frac{(q + 2n\Delta q + q^{1/2})}{2} \\ \frac{(\Delta q + \Delta q^{1/2})}{2} & \frac{q + q^{1/2}}{2} & \frac{(q + 2\Delta q + q^{1/2})}{2} \\ 0 & 0 & 0 \end{bmatrix}. \quad (10)$$

Under the three defense modes on the power systems, Figure 4 analyzes in detail the final revenues made by the attack and defense sides when the hackers adopt three different attack strategies. For the host in complete-defense mode, the final revenue of the both sides is revealed in Figures 4(a) and 4(c), respectively: when the management is in complete-defense, the average revenue of the three different attack strategies of the hackers is 9.66, which is significantly

lower than the situation where the management is in partial- and no-defense, as described in Figure 4(a). At this time, the hacker's choice of large-scale strategy can effectively prevent the power systems from maximizing its revenue, but the own revenue performance of the attack side is fairly poor so that there are two possible options for the hackers: large-scale attack or no-attack; when the management is in partial-defense, small-scale strategy used by the attack side makes the

FIGURE 4: Under (a) complete-defense of host and management, (b) complete-defense of host and partial-defense of management, (c) complete-defense of host and no-defense of management, (d) partial-defense of host and complete-defense of management, (e) partial-defense of host and management, (f) partial-defense of host and no-defense of management, (g) no-defense of host and complete-defense of management, (h) no-defense of host and partial-defense of management, and (i) no-defense of host and management, both sides benefit when the hackers launch different attack strategies.

most significant contribution to its overall revenue, and the two sides have reached the Nash equilibrium. In this defense mode, the hackers are most likely to employ a small-scale strategy, as shown in Figure 4(b), as shown in Figure 4(c), the revenue of small-scale strategy is not only close to that of large-scale strategy but also the paid cost from small-scale strategy is much smaller than that of the large-scale strategy. From the perspective of maximizing revenue, the attack side will still choose a small-scale strategy when the management side is in no-defense.

For the host in partial-defense mode, the final revenues of both sides are displayed in Figures 4(d) and 4(f), respectively: in Figure 4(d), the revenue from utilizing small-scale strategy is about half that of the power systems, and it is the least of the three attack strategies. In view of that, the hackers have two options along with the management being in complete-defense: one is to be forced to adopt large-scale strategy when necessary to suppress the revenue of the power systems to reach maximum, and the other is to remain stationary to avoid its own loss; in Figure 4(e), the

defender achieves the biggest revenue when the hackers employ small-scale strategy, while the hackers get the maximum revenue with large-scale strategy. However, the maximum revenue obtained by the hackers through large-scale strategy is very close to the value obtained by small-scale strategy. To minimize cost and maximize revenue, the hackers have the highest probability of choosing small-scale strategy when the management side is in partial-defense; in Figure 4(f), the attack and defense parties arrive the Nash equilibrium when the hackers launch a small-scale strategy. Taking into account the respective costs and game issues, at this time, the revenues of both parties also reach each maximum value.

For the host in no-defense mode, the final revenues of the both sides are described in Figures 4(g) and 4(i), respectively: from Figure 4(g), it can be inferred that the revenue inside the power systems is obviously lower than that in Figures 4(a) and 4(d) in order when the management side is set as complete-defense mode; similarly, the revenue inside the power systems in Figure 4(h) is lower than Figures 4(b) and 4(e); it is also suitable for the revenue inside the power systems of Figure 4(i), lower than Figures 4(c) and 4(f). That manifests that the revenue of the power systems is more easily plundered by the hackers with the host being no-defense; the data in Figure 4(g) point that only when the attack side adopts large-scale strategy can the revenue of the power systems reach the maximization. When the management side is set as complete-defense, the hackers also have two options: launching large-scale attack when necessary to reach the Nash equilibrium or continuing to remain silent to avoid any losses; when the management side is in partial- and no-defense, as shown in Figures 4(h) and 4(i), both sides will reach the Nash equilibrium with small-scale strategy adopted by the hackers. Therefore, in the above three defense modes, the hackers are more likely to launch a small-scale strategy.

In summary, this part discusses nine possible combinations in host and management attack and defense model among which the occurrence probability of large-scale, small-scale, and no-attack strategy is 3/12, 6/12, and 3/12, respectively. So, it is critical to be aware of small-scale strategy implemented by the attack side most of the time. Under special conditions, the possibility of the attackers launching a large-scale and no-attack strategy is not excluded.

3.4.3. Network and Management Attack and Defense Model.

The third possible combination is network and management attack. Whenever a huge amount of cost is invested and a certain level of authorizations is still not available through the network path, the hackers will choose to use social engineering to seek management loopholes to breakthrough. When a certain authorization is obtained by means of management defects or a specific Trojan horse is implanted in a specific location, the hackers will successfully conduct the attack via the network path. The setting order of security policies here is the network management. Given that management vulnerabilities can often provide vital support for network attacks, the cost savings when the network is in complete-, partial-, and no-defense are denoted as $\tau/2$, $(\tau - \Delta\tau)/2$, and 0, respectively. In the light of the cost savings, the paid defense costs in the above three cases can be calculated, as exhibited, respectively, in matrix s_1' , s_2' , and s_3' :

$$\begin{aligned} s_1'' &= \begin{bmatrix} -p + \frac{\tau}{2} \\ -(p - \Delta p) + \frac{\tau}{2} \\ \tau^{1/2} \end{bmatrix}, \\ s_2'' &= \begin{bmatrix} -p + \frac{(\tau - \Delta\tau)}{2} \\ -(p - \Delta p) + \tau^{1/2} - \Delta\tau^{1/2} \\ \tau^{1/2} - \Delta\tau^{1/2} \end{bmatrix}, \\ s_3'' &= \begin{bmatrix} -p \\ -(p - \Delta p) \\ 0 \end{bmatrix}. \end{aligned} \quad (11)$$

The calculation process of the total revenue of the hackers in this type of model is similar to matrix (9); the total revenue here is equal to the average of the sum of the corresponding single network and management model, as displayed in the following matrix:

$$s_{cm}^I = \begin{bmatrix} \frac{2q + q^{1/2}}{2} & \frac{2q + q^{1/2} + 2\Delta q}{2} & \frac{(2q + (n+1)\Delta q + q^{1/2})}{2} \\ \frac{(n\Delta q + \Delta q^{1/2})}{2} & \frac{2q + q^{1/2}}{2} & \frac{(2q + 2\Delta q + q^{1/2})}{2} \\ 0 & 0 & 0 \end{bmatrix}. \quad (12)$$

FIGURE 5: Under (a) complete-defense of network and management, (b) complete-defense of network and partial-defense of management, (c) complete-defense of network and no-defense of management, (d) partial-defense of network and complete-defense of management, (e) partial-defense of network and management, (f) partial-defense of network and no-defense of management, (g) no-defense of network and complete-defense of management, (h) no-defense of network and partial-defense of management, and (i) no-defense of network and management, both sides benefit when the hackers launch different attack strategies.

Next, we calculate the final revenues of the both sides that the revenue of the hackers acquired by various attack methods minus the attack cost is its ultimate value. That the total revenue on the power systems minus the inherent loss, defense cost, and plundered revenue is its final revenue. Under the three defense modes on the power systems, Figure 5 analyzes in detail the final revenues made by both sides when the hackers utilize three different attack strategies. For the network in complete-defense mode, the final revenues of the two sides are presented in

Figures 5(a) and 5(c), respectively: when the management side is set as complete-defense mode, Figure 5(a) indicates that the hackers can only obtain the maximum revenue by adopting large-scale strategy due to the rigorous defense on the power systems. At the same time, that strategy can effectively stop the power systems reaching its top value with the two sides being the Nash equilibrium, which demonstrates that large-scale strategy needs the most attention; when the management side is set as partial-defense mode, the two sides reach the Nash equilibrium

FIGURE 6: A certain production subnet in the power systems.

with the hackers using small-scale strategy, which expresses that the probability of small-scale attacks is the highest; The data in Figure 5(c) show that not only do the revenues of the two parties get the maximum value but both sides also reach a state of Nash equilibrium when the hackers launch small-scale attacks, which represents that small-scale strategy should be highly attached importance. For the network in partial-defense mode, the final revenues of the both sides are shown in Figures 5(d) and 5(f), respectively: when the management side is set as complete-defense, in order to suppress the emergence of the maximum gain on the power systems, the only option for the hackers is to employ large-scale strategy, as illustrated in Figure 5(d), so it is necessary to hinder large-scale attacks; when the management side is set as partial-defense, the attack side is more likely to seek small-scale attacks because under this situation, as presented in Figure 5(e), its output cost is fairly low and the revenue is only 0.1% lower than large-scale attack; when the management side is set as no-defense, Figure 5(f) indicates that the revenues of both sides have reached respective peaks and the state of Nash equilibrium with small-scale attacks by the hackers. For the network in no-defense mode, the final revenues of both sides are shown in Figures 5(g) and 5(i), respectively; when the management

side is set as complete-defense, the situation in Figure 5(g) is the same as that in Figure 5(d). At this time, the probability of the hackers being forced to adopt large-scale attack strategy is greater; the data trends in Figures 5(h) and 5(i) are respectively similar to those in Figures 5(e) and 5(f), and both sides have acquired each optimal value and reached the Nash equilibrium with small-scale strategy.

Based on the above discussion, here we list nine possible combinations in network and management attack and defense model among which the probability of the large- and small-scale strategy is $3/9$ and $6/9$, implying that the probability that the hackers will implement small-scale strategy is far greater than the probability of large-scale and no-attack strategy most of the time.

4. Experiment Analysis

First of all, the experimental part of this article is to verify the dual attack and defense model established previously to ensure that the constructed model can be applied to the power production systems. Then, we predict the best defense strategy on the power systems in the next month according to the construction model.

FIGURE 7: (a) The probability of high-, medium-, and low-risk events in the power systems; (b) the type of attack events that occurred.

A production subnet in the power systems is taken as an example, as shown in Figure 6. The entire production systems network is an internal private network, divided into multiple subareas, and its terminals of each subarea include personal PCs, cameras, electric vehicles, and temperature detectors. As can be seen from Figure 6, Web Application Firewall (WAF), the admission device, and other security devices are respectively connected at the core switching layer with the purpose to monitor abnormal traffics and prevent malicious attacks on the power systems.

4.1. Model Validation. WAF is one of the most commonly used network security protection devices in the power systems and is well known for its ability to detect malicious attacks in accordance with rules in a timely manner. To accurately predict the probability of attacks of different scales every day, a total of 454 sets of real-time data are extracted with a time step of 10 minutes.

The average value of the high-, medium-, and low-risk events in the WAF is used as the basis for judging, so as to

infer the frequency of various attacks inside the power systems every day. Here, the high-, medium-, and low-risk attacks correspond to the large-, small-, and no-attack strategies of the hackers in turn. The calculated daily probability of high-, medium-, and low-risk attack events is 48%, 51%, and 1%, as shown in Figure 7(a). A total of 27 possible combined attacks are discussed in this article among which the odds of launching large-scale, small-scale, and no-attack by attackers are 9/30, 18/30, and 3/30, with the conclusion that the basic attack strategy of the hackers is mainly small-scale strategy combining with large-scale and no-attack strategy followed occasionally. The probability of high- and medium-risk events in Figure 7(a) is 48% and 51% higher than the probability of no security event, respectively. The data in Figure 7(a) show that the probability of no-attack on the power systems is extremely small, which is very close to the change trend inferred from the theoretical model. Obviously, the actual attack data in the power systems also confirm the results of the attack and defense model, which indicates that the models constructed in the article are consistent with the actual production environment.

FIGURE 8: Under (a) complete-defense of host, (b) partial-defense of host, and (c) no-defense of host, both sides benefit when the hackers launch different attack strategies; under (d) complete-defense of host, (e) partial-defense of host, and (f) no-defense of host, both sides benefit when the hackers launch different attack strategies; under (g) complete-defense of network, (h) partial-defense of network, and (i) no-defense of network, both sides benefit when the hackers launch different attack strategies.

Figure 7(b) reveals 17 types of attack events that occurred in 454 sets of data, which are recorded by waf in the experimental stage.

4.2. Building Revenue Function. Taking the value of the above risk types as empirical values, the monthly revenue function formula (13) of both the sides is given, and then we discuss how the power systems should take precautions to maximize its revenue:

$$f(I) = 30 * (0.48x + 0.51y + 0.1z). \quad (13)$$

Among which, x , y , and z correspond to the final revenues obtained by the attack side using large-scale, small-scale, and no-attack. Assuming that the attack plan chosen by the hackers is the same within one month, thus the total monthly revenue of the power systems can be calculated. Considering that in actual production, the hackers are less likely to launch an attack on a single target and most of them would take the form of a combined attack. Therefore, this article only discusses the revenues of the both parties in the dual model.

In the first place, the revenues of both parties in the host and network attack defense model are discussed. The three

models corresponding to complete-, partial-, and no-defense of the host are described in Figures 8(a) and 8(c), respectively. The changes in the three figures are exactly the same, both of them reach the Nash equilibrium during partial-defense. The probability of this situation in Figure 8(c) in the actual production environment is almost zero. Thus, only when the host is in complete-defense and the network is in partial-defense can the power systems gain abundant revenues. Therefore, this defense mode should be the main one in the next month.

Then, the revenues of both parties in the host and management attack and defense model are discussed. The three models corresponding to complete-, partial-, and no-defense of the host are shown in Figures 8(d) and 8(f), respectively. The data trends in the three figures are the same as those in Figure 8, which implies that the power systems have the largest gain when the host side is in complete-defense and management side is in partial-defense. It is clear that this defense mode should be dominated in the next month.

Finally, the revenues of both parties in network and management attack and defense model are discussed. The three models corresponding to complete-, partial-, and no-defense of the network are shown in Figures 8(g) and 8(i), respectively. The data trends in the three figures are the same as in Figures 8(d) and 8(f), which also means that the power systems have the largest gain when the network side is in complete-defense and the management side is in partial-defense. In the next month, this defense mode should be the optimal choice in the power systems.

5. Conclusions and Future Work

In summary, the idea of modeling cyber-attack and defense as contending for power system benefit is proposed for the first time. Then, we have taken a subnet of the power systems as a case and employed the attack data in the actual production environment to verify the 27 dual attack-defense models constructed in this paper. By this approach, we derive the monthly benefit function applicable to this environment and calculated the benefits of both sides and the best defense mode on the power systems in the next month. Additionally, this paper analyzes in detail the possible attacks from the perspective of the attackers and evaluates the impact on the power systems, thereby changing its defense strategy from passive to proactive; we explored the optimum proactive defense strategy for the power systems from the angle of the game between the attacker and defender. In the next step, we will combine with actual production business processes to further study more specific proactive strategies to achieve the transition from qualitative defense to quantitative defense strategies.

Data Availability

No dataset was used in this experiment. The supporting data for the experimental results are all from WAF equipment, and the data template on the official website cannot be seen (the link may have expired). See the hyperlink (<https://pan.baidu.com/s/1cxUE51JPnwS3KG5i0VE-Ew>; Extraction code: Jw25) for the specific data the authors extracted.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

- [1] C. Kang, J. Huang, Z. Zhang et al., "An automatic algorithm of identifying vulnerable spots of internet data center power systems based on reinforcement learning," *International Journal of Electrical Power & Energy Systems*, vol. 121, Article ID 106145, 2020.
- [2] N. Moreira, E. Molina, J. Lázaro, E. Jacob, and A. Astarloa, "Cyber-security in substation automation systems," *Renewable and Sustainable Energy Reviews*, vol. 54, pp. 1552–1562, 2016.
- [3] J. X. Jacob, X. Zhang, and X. Q. Zhu, "The exploration of mobile target defense method in a diversified environment," *Electric Power Information and Communication Technology*, vol. 16, no. 6, pp. 1–5, 2018.
- [4] M. Hu, H. K. Boddapati, and S. Prakriya, "Performance off cluster-based multi-hop underlay networks with energy harvesting nodes," *IET Communications*, vol. 14, no. 9, pp. 1476–1484, 2020.
- [5] S. Vuppala, A. E.-D. Mady, and A. Kuenzi, "Moving target defense mechanism for side-channel attacks," *IEEE Systems Journal*, vol. 14, no. 2, pp. 1810–1819, 2020.
- [6] C. X. Liu, X. S. Ji, and J. X. Wu, "A mimic defense mechanism for mobile communication user data based on MSISDN virtualization," *Chinese Journal of Computers*, vol. 41, pp. 275–287, 2018.
- [7] S. Radha, G. J. Bala, and P. Nagabushanam, "FRAME routing with game theory optimization for wireless networks," *International Journal of Communication Systems*, 2019.
- [8] Q. Y. Zhu and T. Basar, "Game-theoretic methods for robustness, security, and resilience of cyberphysical control systems: games-in-games principle for optimal cross-layer resilient control systems," *IEEE Control Syst Mag*, vol. 35, no. 1, pp. 46–65, 2015.
- [9] Y. Zhao, J. L. Yu, and M. F. Ban, "A distribution-market based game-theoretical model for the coordinated operation of multiple microgrids in active distribution networks," *International Transactions on Electrical Energy Systems*, vol. 30, pp. 1–11, 2020.
- [10] S. Rass and Q. Zhu, "GADAPT: a sequential game-theoretic framework for designing defense-in-depth strategies against advanced persistent threats," *Lecture Notes in Computer Science*, vol. 9996, pp. 314–326, 2016.
- [11] J. T. Chen, C. Touati, and Q. Y. Zhu, "A dynamic game analysis and design of infrastructure network protection and recovery," *Electrical Engineering and Systems Science*, vol. 45, pp. 125–128, 2017.
- [12] F. Miao, Q. Zhu, M. Pajic, and G. J. Pappas, "A hybrid stochastic game for secure control of cyber-physical systems," *Automatica*, vol. 93, pp. 55–63, 2018.
- [13] R. Pappas, Q. Chen, L. Chen, J. Xiong, and D. Wu, "A privacy-preserving personalized service framework through Bayesian game in social IoT," *Wireless Communications and Mobile Computing*, vol. 2020, Article ID 8891889, 13 pages, 2020.
- [14] J. Xiong, M. Zhao, M. Z. A. Bhuiyan, L. Chen, and Y. Tian, "An AI-enabled three-party game framework for guaranteed data privacy in mobile edge crowdsensing of IoT," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 2, pp. 922–933, 2019.