applied sciences

MDPI

Article

Security-Oriented Cyber-Physical Risk Assessment for Cyberattacks on Distribution System

Yuhang Zhang * and Ming Ni

College of Energy and Electrical Engineering, Hohai University, Nanjing 211100, China; mingni_hhu@163.com
* Correspondence: zhangyuhang0826@126.com

Abstract: With the increasing deployment of advanced sensing and measurement devices, the modern distribution system is evolved into a cyber-physical power distribution system (CPPDS). Due to the extensive application of information and communication technology, CPPDS is prevalently exposed to a wide range of cybersecurity threats. In this paper, a novel security-oriented cyber-physical risk assessment method for CPPDS is proposed. Based on the information model composed of logical nodes, an attack graph of privilege promotion by exploiting the cyber vulnerabilities is constructed. The physical consequence caused by cyberattack is analyzed in detail. By using the Markov decision process (MDP) theory, the cyber-physical risk index (CPRI) is calculated. Furthermore, considering the allocation of the finite defense resource, the modified MDP approach with an attack–defense game is presented. The effectiveness of the proposed method is demonstrated with case studies on a four-feeder IEEE-RTBS test system.

Keywords: cyber-physical power distribution system; cybersecurity; risk assessment; Markov decision process; attack–defense game

Citation: Zhang, Y.; Ni, M. Security-Oriented Cyber-Physical Risk Assessment for Cyberattacks on Distribution System. *Appl. Sci.* **2023**, *13*, 11569. https://doi.org/10.3390/app132011569

Academic Editors: Ying Zhang, Zhengcheng Dong and Meng Tian

Received: 14 September 2023
Revised: 12 October 2023
Accepted: 16 October 2023
Published: 23 October 2023

1. Introduction

The cyber-physical power system is a sophisticated intelligent system with advanced information and communication technologies closely integrated with a physical process [1–5]. Nowadays, lots of fundamental functions of power systems heavily rely on cyber equipment for flexible and efficient operation and control, which increase the cybersecurity risk to itself. In recent years, cyberattack events against power systems and communication systems occur frequently. Ukraine's power grid was attacked by using spear-phishing emails with BlackEnergy malware in 2015, resulting in power outages for roughly 230,000 consumers. The European Network of Transmission System Operators for Electricity (ENTSO-E) fell victim to a cyberattack in 2020. Its administrative information systems were compromised by remote control. South Korea suffered a temporary nationwide shutdown of its communication network caused by a large-scale distributed denial-of-service (DDoS) attack. Therefore, power systems are facing the severe risk of cyberattacks, and it is of great importance to take recognition and precaution measures against the risk. Both in academia and the industry area, cybersecurity issues of power systems have attracted more and more attention [6–10].

Traditional security analysis methods and assessment indices only considering the power layer are no longer suitable for modern power systems. It is necessary to propose a cyber-physical security analysis approach considering the effect on physical systems caused by a cyber event. Topological models are generally utilized to describe the process of cyberattacks against power systems, such as attack graph [11–14], Markov chain [15,16], Bayesian network [17–19], and Petri net graph [20,21]. There have been many related works on risk assessment for cyberattacks on power systems. In [22], considering the characteristics of attack behaviors, a risk assessment method on power grids was proposed. In [23], a cyber-physical security evaluation approach and contingency ranking technique for power

infrastructures were proposed. In [24], considering malicious attacks on protection system settings and parameters, a risk evaluation method was presented. In [25], a cyber insurance design considering power system reliability and cyber vulnerability was proposed. For probabilistic cyberattacks against breakers, the impact of a successful attack was analyzed, and a novel adequacy assessment was proposed in [26].

The above studies mainly focus on the risk assessment for a transmission network. With the development of large-scale sensing measurement systems and a more complicated communication network, the modern distribution system has evolved into CPPDS. Due to the openness of the information technologies and terminal equipment, the cybersecurity issue also needs to be brought to attention in CPPDS. However, current studies rarely simultaneously describe the attack process clearly and quantize the physical impacts in detail. In [27], man-in-the-middle and denial-of-service attacks are considered. The impact of different cyber events on a physical power grid is analyzed using an integrated cyber-power modeling and simulation testbed. In [28], a stochastic epidemic network model is developed to evaluate the cyber risk by propagating cyberattacks among graphical vulnerabilities. However, the method lacks a general risk index for cybersecurity assessment. In [29], based on a Bayesian attack graph model, the probability of a remote terminal unit (RTU) potentially being attacked was obtained. The long-term power loss was taken as the physical impact. In [30], the attack path is modeled by a Petri net, and the attack payoff is calculated based on the physical influence coefficients. In [31], a CPDS security assessment method based on the expected failure method and considering combined information attacks is proposed. In [32], an attack probability computation method is proposed. In different possible attack scenarios, the detailed attack model is given. However, these works ignore the cyber reward of the attack process, and the analysis of physical impacts is also not sufficient. The impact of combined information-physical-failure on CPDS is analyzed in [33], but the corresponding attack model is simple and the different attack paths are ignored. In addition, research on risk assessment considering an attack–defense game for CPPDS is rarer, which is also the research focus in this paper. In [34], considering attacker and defender strategies and attack damage, a CPDS risk assessment framework is established. Additionally, a risk assessment and defense resource allocation method based on the game model is proposed. Compared with this literature, our work provides a more comprehensive and detailed attack model and its underlying logic. Furthermore, we have integrated the evaluation of cyber rewards during the attack process into the computation of the assessment index. In addition, our research not only formulates a defense resource allocation strategy but also enables the derivation of a cyber-physical risk index that takes into account the attack–defense game.

In this paper, we investigate the cybersecurity of CPPDS, and an attack graph is proposed to describe the potential attack process. Then we analyze the physical consequence caused by a cyberattack in detail. A novel risk assessment method for CPPDS is proposed. The main contributions of this work are summarized as follows:

1. The cybersecurity of CPPDS is elaborated. Based on the information model containing logical nodes for a distribution station, an attack graph of privilege promotion by exploiting the cyber vulnerabilities is built.
2. The physical consequence caused by a cyberattack is taken as the attack reward. A novel security-oriented cyber-physical risk assessment method based on MDP is proposed. The calculated CPRI values are used to evaluate the risk for a cyberattack.
3. Considering the allocation of the finite defense resource, the attack–defense game MDP model is proposed. The optimal allocation strategy of a defense resource is obtained.

The rest of this paper is organized as follows: Section 2 presents a CPPDS framework. The cybersecurity of CPPDS is analyzed in Section 3. Section 4 presents a novel cyber-physical risk assessment method for CPPDS. Case studies are carried out in Section 5 to demonstrate the effectiveness of the proposed method. Finally, Section 6 concludes this paper.

2. CPPDS Framework

According to the types of connected information equipment and the distinct functions, CPPDS can be divided into three levels: distribution network backbone layer, access layer, and terminal layer. On this basis, the framework of CPPDS as shown in Figure 1 is constructed. The backbone layer includes the main distribution station system, supervisory control and data acquisition (SCADA) server, management information system (MIS) server, etc. The main distribution station and each slave distribution station are connected by synchronous digital hierarchy (SDH) optical communication technology. The access layer uses Ethernet passive optical network (EPON) technology to connect the slave distribution station and each distribution terminal to realize the real-time communication. EPON is composed of an optical line terminal (OLT), optical network unit (ONU) and optical distribution network (ODN). The terminal layer includes feeders, circuit breakers, section switches, and other power components, as well as the feeder remote terminal units (FRTUs) and other intelligent distribution terminals.

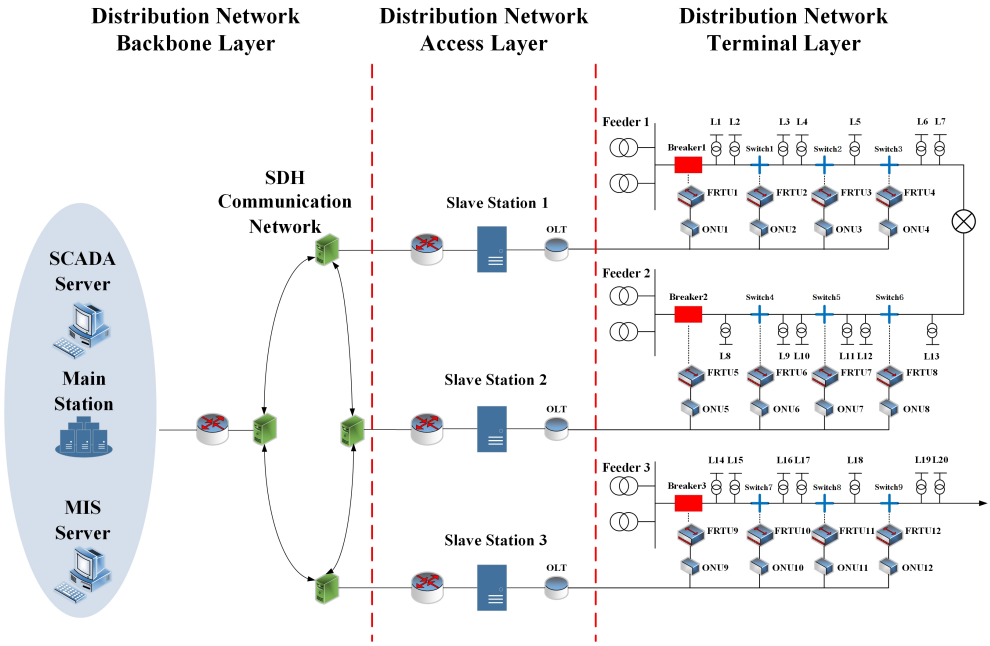

Figure 1. Framework of CPPDS.

From the perspective of cybersecurity, the control center of the power plants or substations usually operates in a closed way with physical isolation. Thus, there are relatively few attack access points that can be exploited by hackers in the control system. Considering the cybersecurity of CPPDS, the main distribution station is usually equipped with relatively complete defense measures, such as the intrusion detection system (IDS), firewalls, and data encryption. However, the terminal units controlled by the slave distribution station lack complete physical protection. In addition, the security of data transmission protocol in the information system of the slave station is relatively low. Consequently, the risk of a cyberattack faced by the slave distribution station is relatively large. Therefore, it is particularly important to accurately evaluate the impact of a cyberattack on it and improve the cybersecurity.

3. Cybersecurity Analysis of CPPDS

In CPPDS, the slave distribution stations are local key information and control hubs that connect the backbone layer and the terminal layer. By communicating with the main station center and remote terminal units in real time, functions such as fault diagnosis, isolation, and recovery in CPPDS are realized. Therefore, we mainly focus on the cybersecurity of the slave distribution stations in CPPDS.

In order to analyze the cyber network of the slave distribution station in more detail, an information system model based on the IEC 61850 standard is constructed, which divides the cyber network into three levels: substation level, bay level, and process level. A cyber-physical system structure diagram of the slave distribution station is shown in Figure 2. The red dash lines denote the possible targets for attacking by intruders. The data, such as the protection setting values, telemetry data, and telesignaling data, are exchanged between the substation level and the bay level by using the Manufacturing Message Specification (MMS) protocol. The data, such as locking control and interlocking information, are transmitted in the bay level by using the Generic Object Oriented Substation Event (GOOSE) protocol. The real-time sampled data of the voltage transformer (VT) and current transformer (CT) in the merging unit are transmitted between the bay level and the process level by using the Sample Value (SV) protocol, and the controlled data of the FRTU, such as the trip signals, switch positions are transmitted by using the GOOSE protocol.

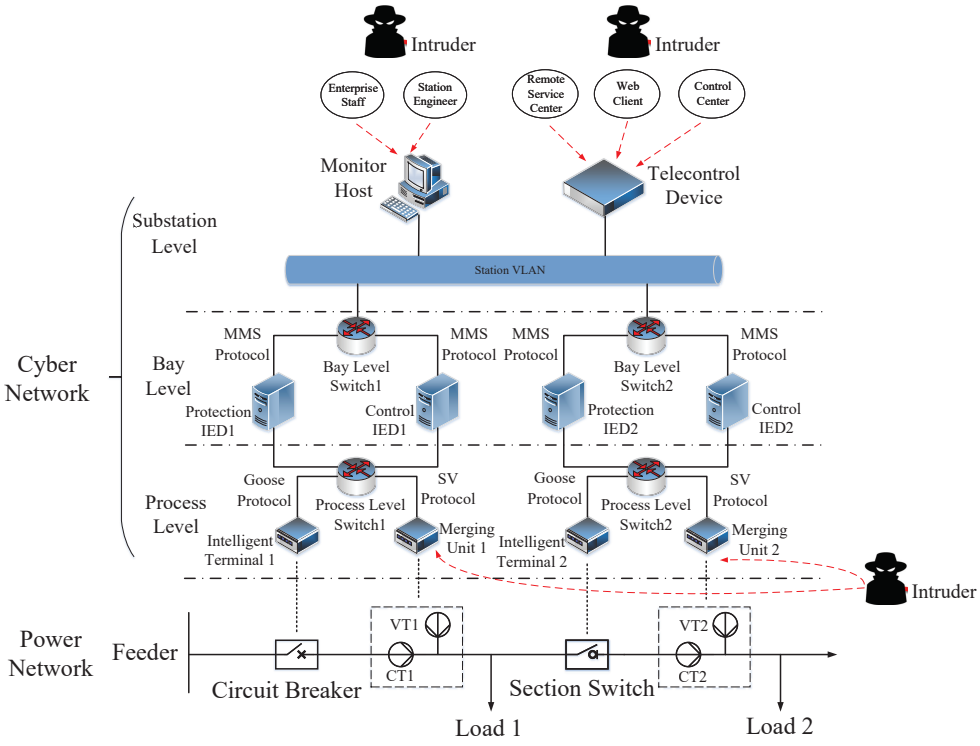

Figure 2. Cyber-physical system structure of the slave distribution station.

On the one hand, the monitoring host, telecontrol devices, and distributed FRTUs in CPPDS lack effective physical isolation protection, and there exist security vulnerabilities that can be exploited by intruders. Some experienced attackers can use these vulnerabilities to invade information devices to obtain corresponding permissions. Then they take this as a springboard to attack other devices, and constantly improve the control authority to achieve the final attack purpose. On the other hand, the security of data transmission protocols used in CPPDS is not high enough, which makes it possible to attack the distribution station. The data packets through MMS, GOOSE, and SV protocols are all transmitted in plaintext through the TCP/IP and Ethernet protocol. In addition, the field devices lack enough encryption protection. The IEC 61850 standard [35] does not consider the corresponding security measures. Therefore, there may be the following risks and threats in CPPDS.

(1) CPPDS lacks complete firewall settings and IDS. The antivirus software is not updated in time, which leads to the low cybersecurity.
(2) The MMS protocol lacks an identity authentication and access control mechanism, and the data are transmitted in plaintext, which will produce serious security risks.

For example, an attacker can exploit the overflow vulnerability of an MMS protocol stack to cause device downtime or offline.

(3) The communication mode of GOOSE and SV protocols is based on subscriber/publisher mode, which requires high real-time transmission. In order to ensure that the function and transmission time of relay protection are not affected, the data packets are encoded by ASN.1. Without any encryption measures, its security cannot be guaranteed, and the data in GOOSE and SV messages exist vulnerabilities, such as tampering, copying, and camouflage.

4. Security-Oriented Cyber-Physical Risk Assessment for CPPDS

4.1. Risk Assessment Based on MDP

Attackers mainly exploit the security vulnerability to invade the information equipment and obtain the authority of the corresponding functional nodes so as to continuously penetrate the information system of CPPDS. Experienced hackers further exploit the vulnerabilities of the communication protocol to tamper with the control instructions and destroy the normal operation of the IEDs, resulting in the power failure of the distribution system. Therefore, we called it cross-domain attack from the information domain to the physical domain.

Generally, each cyberattack path is composed of an escalating series of malicious actions by the attackers. In order to elaborate the cyberattack path, an information model composed of logic nodes for the slave distribution station is built. The corresponding logical node functions and the information flow are illustrated in Figure 3. It is usually necessary to execute a multistep attack to achieve the final purpose. Adversaries first exploit the security vulnerabilities of monitor host, remote interface, or terminal devices to obtain the control authority. Then they further exploit the protocol vulnerabilities to affect the functions of logical nodes and realize the transfer of control states so as to sabotage the fault location, isolation, and service restoration (FLISR).

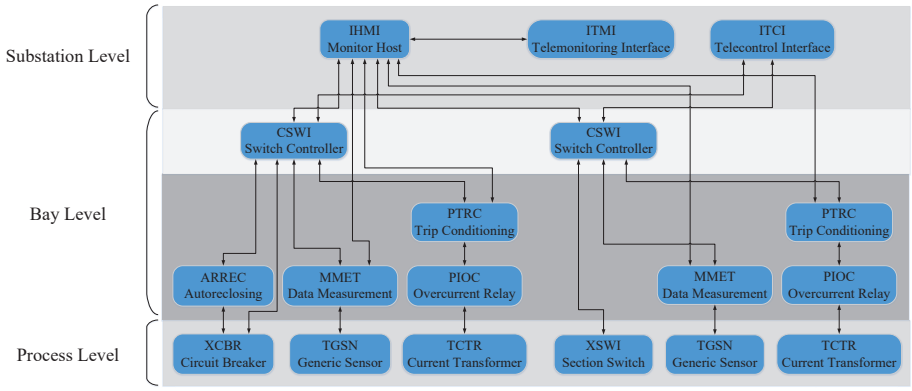

Figure 3. Information model of logical nodes for slave distribution station.

To enumerate all possible attack scenarios, based on the above information model, we model the cyberattack process using a discrete Markov decision process [36]. A standard MDP is denoted as a tuple (S, A, R, P, γ). S is the attack state space. A is the set of the attack actions of adversarial vulnerability exploitations. For each $s \in S$, $A(s) \subset A$ denotes the set of all possible attack actions at state s. R is the reward function. P is the transition probability function. $P(s'|s,a)$ denotes that the probability of state s transferring to state s' when taking an attack action $a \in A(s)$. γ is the discounting factor, commonly $0 < \gamma < 1$.

The MDP state transfer graph is built as shown in Figure 4. The red dashed square denotes the final attack target. The initial state S_0 is set as 'Attacker', and the final target state S_F is 'XCBR' or 'XSWI'. The attack entrances include the monitor host, the remote control interface, and the field terminal devices. The yellow circles denote the security vulnerabilities v_i, which can be exploited in the cyber network. The blue ellipses denote the logic nodes, which are taken as the intermediate states. The current state may transfer

into the other states when an attack action is taken, namely, exploiting the vulnerabilities. The transition probability, namely, the success attack probability is estimated based on the vulnerabilities that are still unpatched in CPPDS. A more realistic probability model considering the age of vulnerability and the CVSS vulnerability scores is established. CVSS is currently the most widely used vulnerability scoring system. It is part of the secure content automation protocol, and is supported by the US national vulnerability library (NVD). The age of vulnerability is modeled by the Pareto distribution. The CVSS vulnerability scores are adopted from a CVSS system. The transition probability is calculated by [13]

$$P(s'|s, a_{v_i}) = \left(1 - \frac{k}{t_{v_i}}\right)^{\alpha} \times AV_{v_i} \times AC_{v_i} \times AT_{v_i} \quad (1)$$

where t_{v_i} is the age of the vulnerability v_i, which is calculated by the released date of CVSS scores. AV_{v_i}, AC_{v_i}, and AT_{v_i} represent the attack vector, attack complexity, and authentication of v_i, respectively. These values are quantified based on Table 1.

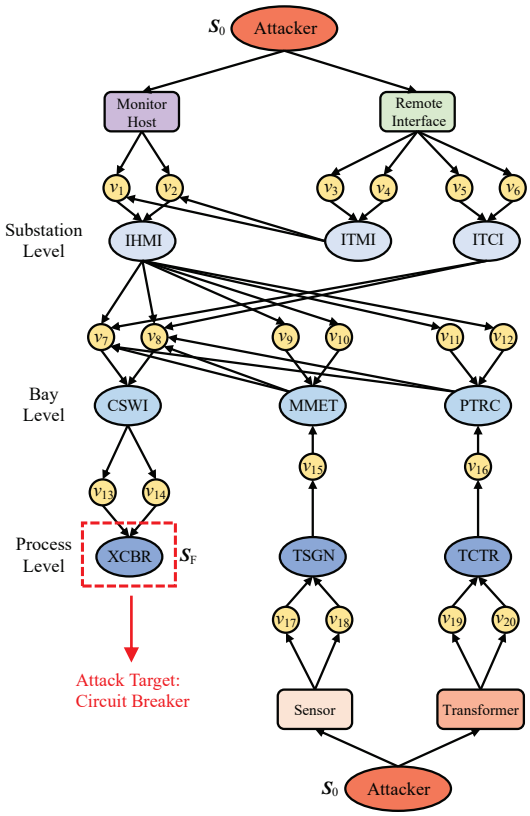

Figure 4. Attack state transfer graph.

During the attack process by exploiting the vulnerabilities, the confidentiality, integrity, and availability of data will be affected so that the privilege of some function will be gained by attackers. We assume that if attackers are successfully exploiting a vulnerability to transfer the state, the cyber reward $R_{cy}(s'|s, a_{v_i})$ is obtained, which is defined by [13]

$$R_{cy}(s'|s, a_{v_i}) = 10.41 \times [1 - (1 - CI_{v_i}) \times (1 - II_{v_i}) \times (1 - AI_{v_i})] \quad (2)$$

where CI_{v_i}, II_{v_i}, and AI_{v_i} are the confidentiality impact, integrity impact, and availability impact of v_i, respectively. These values are quantified based on Table 1, which are adopted from [13].

Table 1. The elements and values of CVSS.

Elements	Level Classification	Quantification
Attack Vector (AV)	Local (L)	0.395
	Adjacent Network (A)	0.646
	Remote Network (N)	1.000
Attack Complexity (AC)	High (H)	0.350
	Medium (M)	0.610
	Low (L)	0.710
Authentication (AT)	Multiple (M)	0.450
	Single (S)	0.560
	None (N)	0.704
Confidentiality Impact (CI)	None (N)	0.000
Integrity Impact (II)	Partial (P)	0.275
Availability Impact (AI)	Complete (C)	0.660

When successfully compromising a section switch or a circuit breaker, the physical reward $R_{ph}(s'|s, a_{v_i})$ is obtained by attackers, which is expressed by Equation (3). The detailed calculation method of $R_{ph}(s'|s, a_{v_i})$ is presented in subsection *C*.

$$R_{ph}(s'|s, a_{v_i}) = \begin{cases} TRcsq, & s' \text{ is XSWI or XCBR} \\ 0, & \text{otherwise} \end{cases} \tag{3}$$

Comprehensively considering the cyber reward, the physical reward, and the attack cost, the net reward obtained by attackers is defined as follows:

$$R_{net}(s'|s, a_{v_i}) = \varepsilon_1 \cdot R_{cy}(s'|s, a_{v_i}) + \varepsilon_2 \cdot R_{ph}(s'|s, a_{v_i}) - \varepsilon_3 \cdot Cost(s'|s, a_{v_i}) \tag{4}$$

where ε_1, ε_2, and ε_3 are the corresponding coefficients. The attack cost is related to the probability of a successful attack [11].

$$Cost(s'|s, a_{v_i}) = -\frac{1}{\rho} ln[P(s'|s, a_{v_i})] \tag{5}$$

From the perspective of the attackers, the cyber-physical risk index (CPRI) for each state s is calculated by solving the following dynamic programming equation:

$$CPRI(s) = \max_{a \in A(s)} \left\{ \sum_{s' \in S} P(s'|s, a_{v_i}) \cdot \left[R_{net}(s'|s, a_{v_i}) + \gamma \cdot CPRI(s') \right] \right\} \tag{6}$$

where $CPRI(s)$ is the MDP's value function, which is related to the cyberattack paths and the net rewards. We take the state "Attacker"'s value $CPRI(s_0)$ as the cyber-physical risk index of attacking one circuit breaker or section switch. In addition, the chosen set of attack actions constitutes the optimal attack policy $\pi(s)$ for each state. The cyber-physical risk assessment algorithm based on MDP is shown as follows:

4.2. Risk Assessment Based on Modified MDP with Attack–Defense Game

Next, from the perspective of the defenders, we further proposed the modified algorithm considering the defense resource allocation. There are a few ways to defend the cyberspace, such as enhancing the security of industrial communication protocols, enhancing the node security (adding access control and identity authentication), enhancing the password security, increasing the encryption complexity, and enhancing the network monitoring (adding the firewalls and improving the IDSs). In order to quantify the degree

of the defense, the defense resource between the transfer states is defined as $d(s'|s)$. The transfer probability needs to be recalculated by multiplying the following formula:

$$P = \frac{1}{\mu_0 + d(s'|s)} \tag{7}$$

where μ_0 is the defense cost coefficient.

We assume that the total defense resource is a constant value and $d(s'|s)$ has its limits. Therefore, the defense resource should satisfy the two constraint conditions as follows:

$$\begin{cases} \sum_{s \in S} d(s'|s) = \text{Constant} \\ d_{\min} \le d(s'|s) \le d_{\max} \end{cases} \tag{8}$$

where $d_{\min}$ and $d_{\max}$ are the lower limit and the upper limit of the defense resource allocation, respectively.

Taking the defense resource into account, the attack–defense game MDP model is given as follows:

$$\min_{d(s'|s)} \max_{a \in A(s)} \left\{ \sum_{s' \in S} \frac{1}{\mu_0 + d(s'|s)} \cdot P\left(s'|s, a_{v_i}\right) \cdot \left[R_{net}\left(s'|s, a_{v_i}\right) + \gamma \cdot CPRI_d\left(s'\right)\right] \right\} \tag{9}$$

The result $CPRI_d(s_0)$ is taken as the risk index considering the defense actions. In addition, we can obtain the optimal defense resource allocation strategy.

4.3. Analysis and Calculation of Physical Consequence under Cyberattack

Cyberattackers often use some known power grid information, such as the power grid topology, the operation mode, and the security defense strategy, to deliberately attack the power system, so as to power off some important users and cause economic losses to the government, industrial enterprises, and commercial enterprises.

4.3.1. Physical Consequence Index

In order to comprehensively measure the physical consequences of power loss caused by cyberattack in CPPDS, they are divided into instantaneous consequences at the time of accident and long-term consequences in a period of time. This paper proposes the following four indicators to measure the physical consequences:

a. Instantaneous consequences

(1) Loss of power load

The total load loss of the jth feeder section on the ith feeder considering the consumer level factor is denoted by

$$C^1_{f_i,j} = \sum_{m \in \varphi(f_i,j)} \mu_m \times L_m \tag{10}$$

where f_i is the ith feeder, $\varphi(f_i, j)$ is the set of consumer units of the jth feeder section on the ith feeder, μ_m is the consumer level factor for the consumer unit m, and L_m is the total load of the consumer unit m.

(2) Loss of power consumers

The total consumer loss of the jth feeder section on the ith feeder considering the consumer level factor is denoted by

$$C^2_{f_i,j} = \sum_{m \in \varphi(f_i,j)} \mu_m \times U_m \tag{11}$$

where U_m denotes all consumers contained in the consumer unit m.

b. Long-term consequences

(1) Loss of energy of power load

The total loss of energy of the power load of the jth feeder section on the ith feeder considering the consumer level factor is denoted by

$$C^3_{f_i,j} = \sum_{m \in \varphi(f_i,j)} \mu_m \times L_m \times T(f,a,b) \tag{12}$$

where $T(f,a,b)$ is the duration of power outage. f, a, and b denote the feeder location, the fault location, and the type of power outage, respectively. If there is no fault, $a = 0$. Three types of $T(f,a,b)$ related to different b are considered as follows:

1. $b = 1$, power supply restoration time caused by cyberattack (undesired tripping).
2. $b = 2$, power supply restoration time for fault areas caused by conventional physical faults.
3. $b = 3$, power supply restoration time for nonfault areas caused by conventional physical faults.

(2) Loss of energy of power consumers

The total loss of energy of power consumers of the jth feeder section on the ith feeder considering the consumer level factor is denoted by

$$C^4_{f_i,j} = \sum_{m \in \varphi(f_i,j)} \mu_m \times U_m \times T(f,a,b) \tag{13}$$

When comprehensively considering the physical consequences caused by a cyberattack, different physical consequence indices have different degrees of impact. Using the benchmark values C^k_{ref}, the four dimensionless indices are denoted by

$$C^{k,R}_{f_i,j} = \frac{C^k_{f_i,j}}{C^k_{ref}} \quad , \quad k = 1,2,3,4 \tag{14}$$

The weight coefficients of the four consequence indices are determined by AHP. The total relative consequence of the jth feeder section on the ith feeder is obtained by

$$C^{TR}_{f_1,j} = \omega_1 \cdot C^{1,R}_{f_i,j} + \omega_2 \cdot C^{2,R}_{f_i,j} + \omega_3 \cdot C^{3,R}_{f_i,j} + \omega_4 \cdot C^{4,R}_{f_i,j} \tag{15}$$

where ω_1, ω_2, ω_3, and ω_4 are the weight coefficients.

4.3.2. Physical Consequence Calculation

When a physical fault occurs on a feeder section, the circuit breaker triggers the protection action. The distribution terminals collect the fault detection information and send it to the slave distribution station. After summarizing the fault information, each slave distribution station sends it to the main distribution station through the SDH communication network. The main station starts the fault location, fault isolation, and power supply recovery process, and issues the orders to control the opening and closing of switches. By destroying the integrity and availability of information, attackers can achieve the purpose of abnormal operation of switches on a feeder, resulting in a certain range of power outage and serious economic losses.

Next, the physical consequence of attacking the circuit breaker (CB) and the section switch (SS) is analyzed.

a. Physical consequences of attacking CB

According to whether a physical fault has occurred in advance, the physical consequences are divided into the consequence caused by a cyberattack directly and cyber-physical combined fault. Depending on the original state of the feeder CB, it can be divided into the undesired-tripping consequence and the failure-to-operate consequence.

(1) Physical consequences of CB undesired tripping

When the power grid is in normal operation, the CB is cyberattacked by tampering with the information of the CB configuration files, resulting in CB undesired tripping. All consumers on this feeder are out of power with type $b = 1$ of power outage.

(2) Physical consequences of CB failure to operate

When a fault occurs in a feeder section, CB and SS are disconnected for fault isolation. After that, CB is cyberattacked and cannot receive the closing command, which makes CB fail to operate. The consumers from the front of the feeder to the fault point are out of power with type $b = 2$ of power outage. As shown in Figure 5, if the fault point is at the third feeder section, after fault isolation, CB1 fails to close by cyberattack. Thus, the consumers on the first and second feeder sections are out of power with type $b = 2$. Considering all combined faults of feeder sections, then sum the physical consequences. The total physical consequence of both CB undesired tripping and failure to operate is calculated by

$$C_{breaker,i} = \sum_{j=1}^{N_{f_i}} C_{f_i,j}^{TR} + \sum_{j=2}^{N_{f_i}} \left(\lambda_{f_i,j} \sum_{k=1}^{j-1} C_{f_i,k}^{TR} \right) \tag{16}$$

where $\lambda_{f_i,j}$ is the failure rate of the jth feeder section on the ith feeder and N_{f_i} is the number of feeder sections. The first item is the physical consequence of undesired tripping. When calculating $C_{f_i,j}^{TR}$, the parameters in $T(f, a, b)$ are set as $f = f_i$, $a = 0$, and $b = 1$. The second item is the physical consequence of failure to operate, and the parameters are set as $f = f_i$, $a = j$, and $b = 2$.

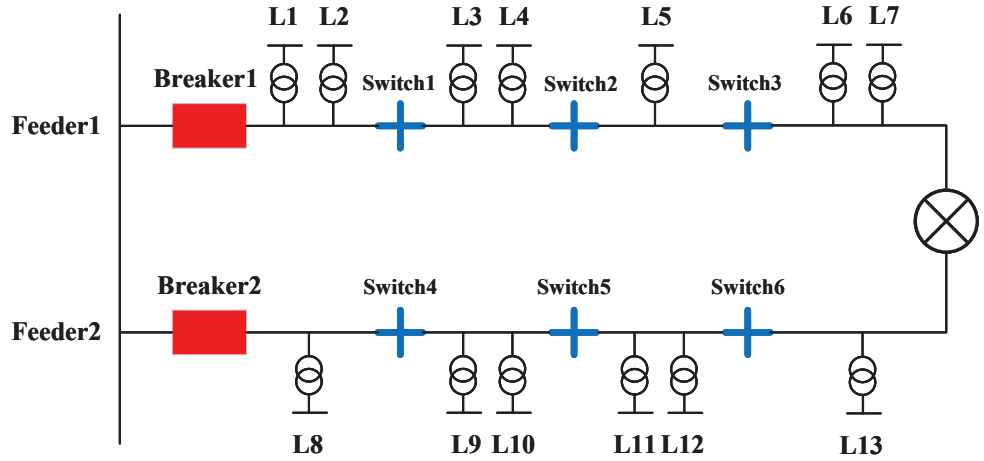

Figure 5. Topology of multisegmented network for distribution system.

b. Physical consequences of attacking SS

SS is the switch on the main feeder, which divides the line into several sections so as to reduce the power outage region in case of a fault. The physical consequences of attacking SS also include the direct faults caused by cyberattack and the combined faults, which are divided into the following three situations:

(1) Physical consequences of SS undesired tripping

When the power grid is in normal operation, one SS is cyberattacked, resulting in undesired tripping. All consumers from this SS position to the feeder back end are out of power with type $b = 1$.

(2) Physical consequences of SS failure to operate

When a fault occurs at a feeder section, the SS that should have been disconnected due to fault isolation fails to operate due to cyberattack. The adjacent SS have to be tripped to ensure the fault isolation; meanwhile, the power outage region is expanded. As shown in Figure 5, assume that a physical fault occurs at feeder section 2, and the attack target is SS 2. The DAS correctly diagnoses the fault position and sends action instructions to SS 1 and SS 2. However, due to the cyberattack on SS 2, it fails to operate. At this time, SS 1 and SS 3 will be disconnected so the power outage region are expanded. For attacking SS 2, the case of the physical fault occurring at feeder section 3 should also be analyzed similarly.

(3) Physical consequences of adjacent switch misoperate

For SS, assume that a physical fault occurs at its front feeder section. During the fault location and diagnosis, because the fault current is detected by the upstream FRTU and not detected by the downstream FRTU, the two SSs at both ends of the fault feeder are disconnected to isolate the fault. Attackers temper with the measurement data of the downstream FRTU of the fault position to mistakenly detect the fault current. Therefore, the new fault position is located in the downstream feeder section adjacent to the actual fault position. The SSs of the downstream feeder section are disconnected to cut off the fault part. Additionally, the consumers of this feeder section are out of power with type $b = 2$. In addition, due to the fact that the actual physical fault has not been removed, the CB of this feeder will disconnect again and maintain the locking state after reclosing. Therefore, the consumers from the CB position to the actual physical fault are out of power with type $b = 2$.

As shown in Figure 5, assume that the attack target is SS 2 and a fault occurs at feeder section 2. According to the above analysis, the fault is mistakenly located at feeder section 3. The consumers on feeder section 3 are out of power with type $b = 2$. The actual physical fault is not removed, so the consumers on feeder sections 1 and 2 are also out of power. It should be pointed out that when calculating the physical consequence caused by a cyberattack, the actual fault consequence need not be included. Similarly, if a fault occurs at feeder section 3, FRTU 2, which should have detected the fault current, does not detect the fault current due to the cyberattack. Thus, the fault position is located at feeder section 2, and the consumers on feeder section 2 are out of power. After the downstream consumers recover power supply by other feeders, the feeder providing the transfer capacity needs to complete another process of fault diagnosis, isolation, and restoration of power supply in nonfault areas due to the remaining existing actual physical fault. The consumers on feeder section 4 of feeder 1 and all consumers on feeder 2 are out of power with type $b = 3$. In conclusion, the total physical consequence of attacking SS is calculated by

$$\begin{aligned} C_{switch,g} = & \sum_{j=g+1}^{N_{f_i}} C_{f_i,j}^{TR} + \lambda_{f_i,g} C_{f_i,g+1}^{TR} + \lambda_{f_i,g+1} C_{f_i,g}^{TR} + \lambda_{f_i,g} \left(\sum_{j=1}^{g+1} C_{f_i,j}^{TR} - C_{f_i,g}^{TR} \right) \\ & + \lambda_{f_i,g+1} \left(C_{f_i,g}^{TR} + \sum_{j=g+2}^{N_{f_i}} C_{f_i,j}^{TR} + \sum_{k=1}^{N_{f_i}^*} C_{f_i,k}^{TR} \right) \end{aligned} \tag{17}$$

In summary, the proposed research framework of a quantitative security risk assessment method for cyberattacks on CPPDS is shown in Figure 6. On the cyber side, we establish a detailed attack model based on the attack graph and vulnerability analysis. On

the physical side, a physical consequence computation method is proposed. In addition, based on MDP, the risk index can be obtained considering both the cyber reward and the physical reward during attacking. Additionally, considering the attack–defense game, the optimal allocation strategy of the defense resource is obtained by our proposed method.

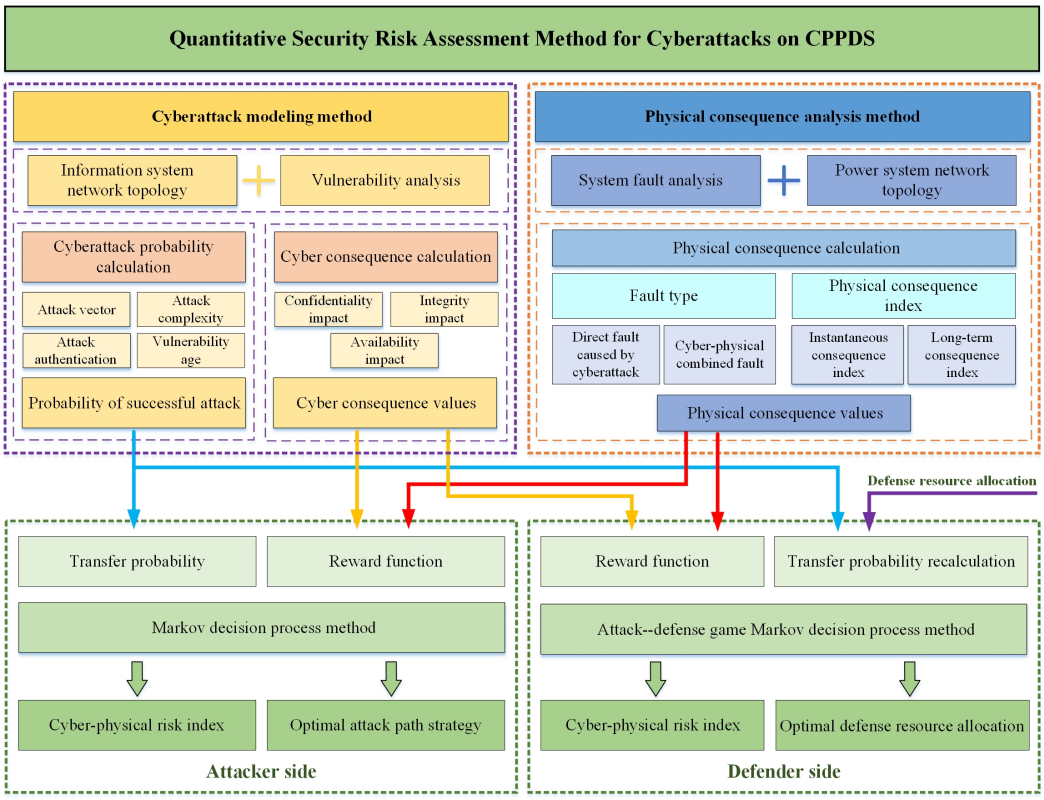

Figure 6. Research framework of quantitative security risk assessment method for cyberattacks on CPPDS.

5. Simulation Results

5.1. Physical Consequence Calculation

Simulation examples are performed on a distribution system for IEEE-RBTS bus 2 [37]. The physical network topology is shown in Figure 7. This test system consists of 4 feeders including 22 load units. The load type and its distribution is shown in Table 2. The other parameters such as load values, consumer numbers of load units, failure rate of feeder sections, and power outage time during FLISR are adopted from the literature [37]. The power outage time caused by a cyberattack in this simulation is modified from the literature [37], as shown in Table 3. There are 4 circuit breakers and 10 section switches, which are considered as the main attack targets. The calculation results of the physical consequences of attacking CB and SS are shown in Tables 4 and 5. It can be seen that the physical consequences of undesired tripping are as serious as those of failure to operate. Therefore, it is meaningful that we both consider the direct consequences caused by a cyberattack and the consequences of cyber-physical combined faults. Specially, feeder 2 only has SS and two feeder sections; we just need to consider load 8 when calculating the physical consequence of failure to operate. Thus, the value is relatively small. From Table 5, it can be found that the physical consequences of undesired tripping of SS, which is close to the feeder front, are more serious. The physical consequences of failure to operate of SS are determined by the load condition of the adjacent feeder section, such as the load value, consumer number, and consumer type. As usual, the physical consequences of adjacent switch misoperate of SS are more serious. During FILSR, the power restoration process of nonfault areas is affected because the actual physical fault is not removed. Thus, the fault areas are expanded even to extend to the adjacent transfer feeders.

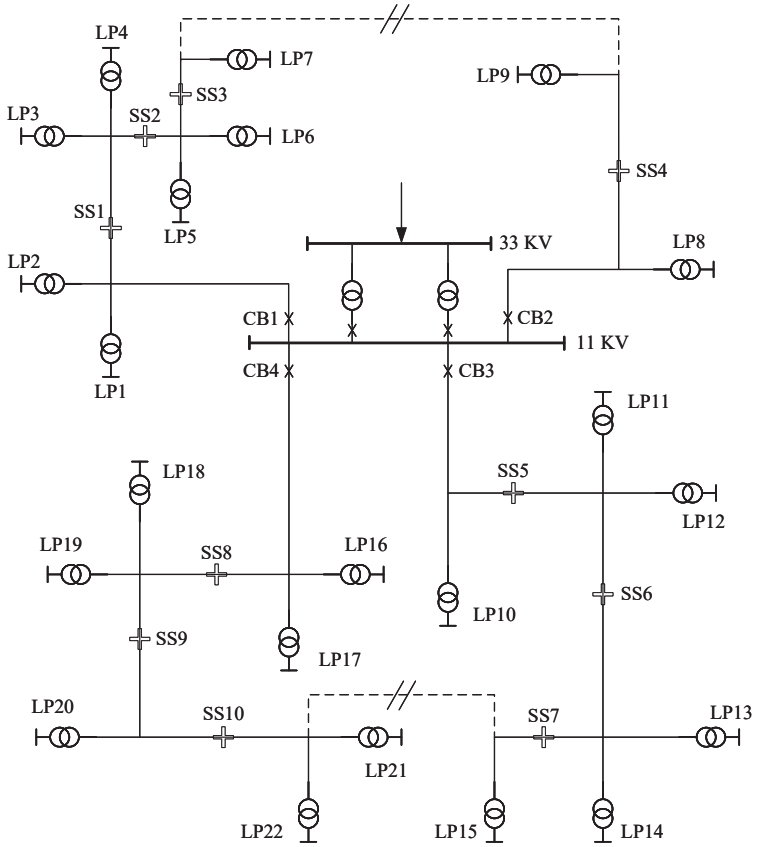

Figure 7. IEEE-RTBS bus 2 system.

Table 2. Load type and level factor.

Load Node	Customer Type	Load Level Factor
1–3, 10–12, 17–19	Residential users	1
4, 5, 13, 14, 20, 21	Government agency	4
8, 9	Industrial users	3
6, 7, 15, 16, 22	Business users	2

Table 3. Power outage time caused by cyberattack.

Feeder Number f_i	Fault Location a	Power Outage Time (hr)		
		$b = 1$	$b = 2$	$b = 3$
Feeder 1	section 1	0.43	1.58	0.12
	section 2	0.29	1.59	
	section 3	0.23	1.59	
	section 4	0.24	1.54	
Feeder 2	section 1	0.52	1.12	0.13
	section 2	0.27	1.03	
Feeder 3	section 1	0.46	1.57	0.15
	section 2	0.22	1.59	
	section 3	0.24	1.52	
	section 4	0.23	1.57	
Feeder 4	section 1	0.48	1.59	0.13
	section 2	0.24	1.57	
	section 3	0.25	1.57	
	section 4	0.27	1.52	

Table 4. Physical consequence values of attacking CB.

Attack Target	Undesired Tripping	Failure to Operate	Sum
CB1	6.9889	8.3064	15.2953
CB2	4.5069	0.3185	4.8254
CB3	6.5133	5.8473	12.3606
CB4	7.3057	7.0592	14.3649

Table 5. Physical consequence values of attacking SS.

Attack Target	Undesired Tripping	Failure to Operate	Adjacent Switch Misoperate	Sum
SS1	3.7552	3.6427	4.5686	11.9665
SS2	1.7455	3.6302	6.0144	11.3901
SS3	0.4794	1.5103	5.5276	7.5173
SS4	1.5081	0.8624	1.8720	4.2425
SS5	3.3518	1.7636	3.2302	8.3456
SS6	2.1425	3.8398	5.8360	11.8183
SS7	0.4676	1.7299	4.7429	6.9404
SS8	3.4688	2.9888	4.4446	10.9022
SS9	2.1968	1.9564	4.0570	8.2102
SS10	1.4101	1.9897	4.6360	8.0358

5.2. Security Risk Assessment for Cyberattacks on CPPDS

The cyberattack graph is shown in Figure 4. According to the practical network experiment in CPPDS, we assume that there are 20 vulnerabilities that can be exploited. The specific vulnerability names and the CVSS values are shown in Table 6. By using Algorithm 1, the risk indexes of terminal equipment and slave stations are calculated based on MDP. As shown in Figures 8 and 9, the difference of CPRI of different terminal equipment is obvious. CPRI shows the risk propagation from the cyber domain to the physical domain. The impacts of a cyberattack are considered. According to the CPRI values, defense measurement can be enhanced contrapuntally against the vulnerable slave distribution stations and terminal equipment.

Algorithm 1 Cyber-physical risk assessment for CPPDS based on MDP

Input:
$CPRI(s)$: initial array values;
γ: discounting factor;
$P(s'|s, a_{v_i})$: state transfer probability;
$R_{net}(s'|s, a_{v_i})$: net reward obtained by attackers;
θ: a small positive threshold determining the accuracy of estimation;
1: **Repeat**
2: $\Delta \leftarrow 0$
3: For each $s \in S$:
4: $temp \leftarrow CPRI(s)$
5: $CPRI(s) \leftarrow \max_{a \in A(s)}\{\sum_{s' \in S} P(s'|s, a_{v_i}) \cdot$
6: $[R_{net}(s'|s, a_{v_i}) + \gamma \cdot CPRI(s')]\}$
7: $\Delta \leftarrow max(\Delta, |temp - CPRI(s)|)$
8: **until** $\Delta < \theta$
Output:
$CPRI(s)$: final cyber-physical risk index;
$\pi(s)^*$: optimal attack path policy that
$\pi(s) = \arg\max_{a \in A(s)} \{\sum_{s' \in S} P(s'|s, a_{v_i}) \cdot [R_{net}(s'|s, a_{v_i}) + \gamma \cdot CPRI(s')]\}$.

Table 6. Vulnerability information.

Number	Name	Vector Values						Age	Transition Probability
		AV	AC	AT	CI	II	AI		
v_1	CVE-2015-4879	N	H	S	P	P	P	1095	0.4164
v_2	CVE-2018-5678	N	M	N	P	P	P	60	0.4016
v_3	CVE-2016-5053	N	L	N	P	P	P	730	0.4829
v_4	CVE-2014-8684	N	L	N	P	P	P	1460	0.4857
v_5	CVE-2012-4879	N	L	N	C	C	C	2190	0.4871
v_6	CVE-2012-4514	N	L	N	C	C	C	2190	0.4871
v_7	CVE-2010-3847	L	L	N	C	C	C	2920	0.1928
v_8	CVE-2012-4056	N	L	N	P	P	P	2190	0.4871
v_9	CVE-2011-4034	N	M	N	C	C	C	2555	0.4190
v_{10}	CVE-2011-3492	N	L	N	C	C	C	2555	0.4876
v_{11}	CVE-2010-0258	N	M	N	C	C	C	2920	0.4193
v_{12}	CVE-2012-0874	N	M	N	P	P	P	2190	0.4185
v_{13}	CVE-2015-1358	N	L	N	P	N	N	1095	0.4846
v_{14}	CVE-2014-4686	N	M	N	P	P	P	1460	0.4173
v_{15}	CVE-2014-5410	N	M	N	N	N	C	1460	0.4173
v_{16}	CVE-2013-4682	N	L	N	P	P	P	1825	0.4865
v_{17}	CVE-2015-4684	N	L	S	P	P	N	1095	0.3855
v_{18}	CVE-2014-3569	N	L	N	N	N	P	1460	0.4857
v_{19}	CVE-2015-4684	N	L	S	P	P	N	1095	0.3855
v_{20}	CVE-2014-3569	N	L	N	N	N	P	1460	0.4857

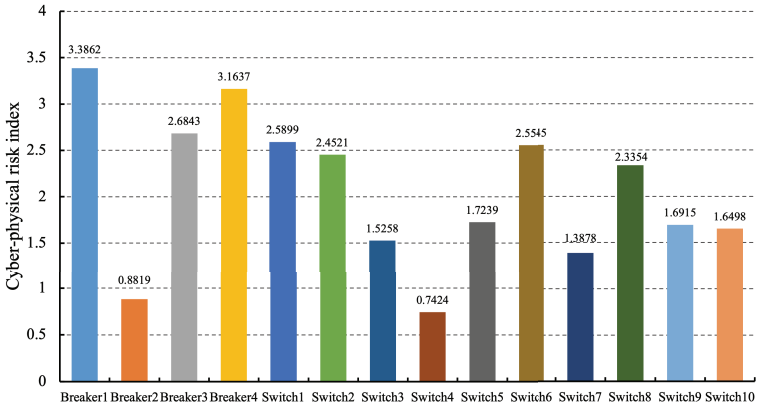

Figure 8. Risk index of different terminal equipment.

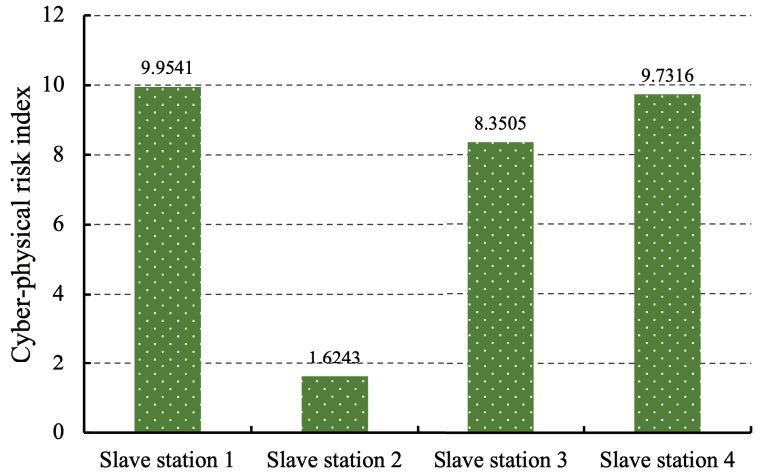

Figure 9. Risk index of different slave distribution stations.

5.3. Security Risk Assessment Based on Attack–Defense Game

In this case, defense resource allocation is taken into account. For convenience, we consider three levels of defense degree, including low, medium, and high. The corresponding quantized values are set as 0.5, 1.0, and 1.5. The total defense resource constant is assumed as 15. There are 15 transfer paths needed to deploy the defense resource. The average value is 1.0. The comparative tests of "no defense", "average defense", and "optimal defense" are completed. The results are shown in Figures 10 and 11. It can be seen that CPRIs decrease due to the defense. Especially, with our proposed attack–defense game MDP model, the CPRIs decrease by about a half. The optimal defense resource allocation scheme is shown in Table 7. The vulnerable parts of the information system can be deployed with more defense resource. Therefore, our method can help defenders maximize the defense resource utilization, and it is efficient to apply into the actual distribution power system to enhance cyber-physical security.

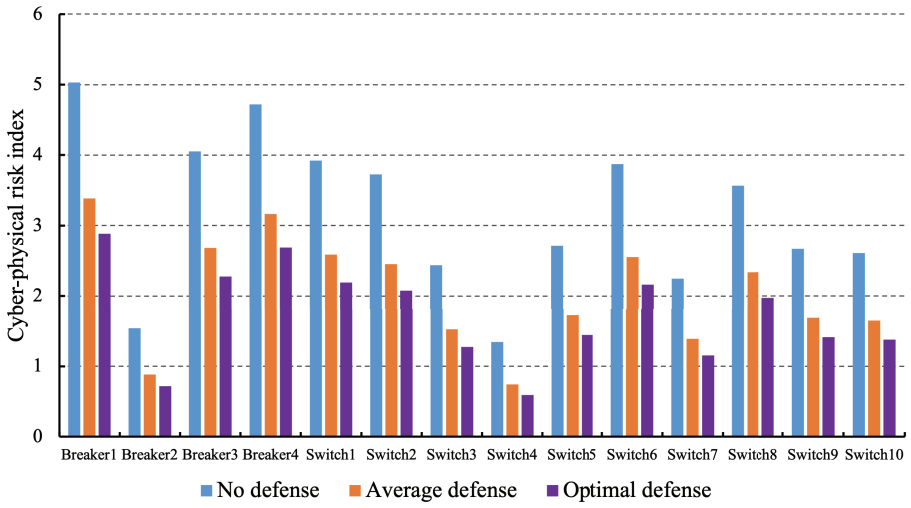

Figure 10. Risk index of different terminal equipment under three defense scenarios.

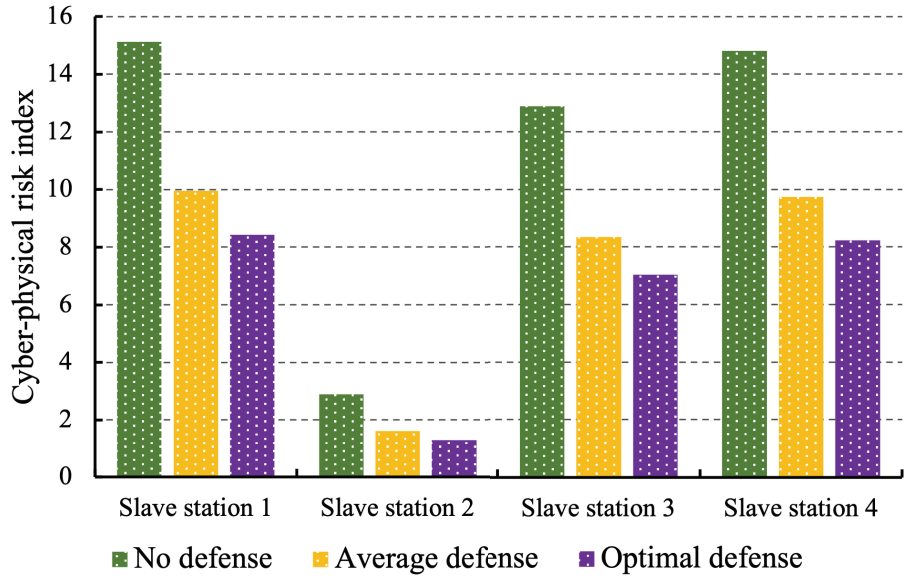

Figure 11. Risk index of different slave distribution stations under three defense scenarios.

Table 7. Result of optimal defense resource allocation.

Transfer Path	Value	Transfer Path	Value
Monitor host → IHMI	1.5	CSWI → XSWI	1.5
Remote interface → ITMI	0.5	MMET → CSWI	0.5
Remote interface → ITCI	1.5	PTRC → CSWI	1.0
IHMI → CSWI	1.0	Transformer → TCTR	1.0
IHMI → MMET	0.5	Sensor → TSGN	1.0
IHMI → PTRC	0.5	TCTR → PTRC	1.0
ITMI → IHMI	0.5	TSGN → MMET	1.5
ITCI → CSWI	1.5	-	-

6. Conclusions

This paper proposes a security-oriented cyber-physical risk assessment method for cyberattacks on CPPDS. Based on MDP, the CPRI values of terminal equipment and distribution stations are calculated. In addition, when considering the allocation of a finite defense resource, the modified MDP method with an attack–defense game is proposed. The simulation results demonstrate that our method can accurately evaluate the risk for a cyberattack so that it can help the system operation and maintenance personnel identify the high-risk equipment and existing cyber vulnerability. According to the obtained optimal defense allocation strategy, the vulnerable part of an information system can be deployed with the defense measurements reasonably so as to most effectively and pertinently improve the security of CPPDS under the consideration of a security defense cost.

Our proposed method only concerned the risk of load shedding resulting from cyberattacks. Other risk factors, such as frequency stability and voltage stability, should also be considered. Concurrently, the growing penetration of renewable energy sources poses new challenges that the risk index computation method should be updated. The distribution system studied in this paper is based on the centralized control mode of master station/slave station. In the following work, the cybersecurity issues under flexible distributed control and distributed fault self-healing will be investigated. What is more, we will explore the identification, early warning, and active defense methods of cyberattacks coordinated by the physical side and the information side.

Author Contributions: Conceptualization, Y.Z. and M.N.; methodology, Y.Z.; software, Y.Z.; validation, Y.Z. and M.N.; formal analysis, M.N.; investigation, Y.Z.; resources, M.N.; data curation, Y.Z.; writing—original draft preparation, Y.Z.; writing—review and editing, Y.Z.; visualization, Y.Z.; supervision, M.N.; project administration, M.N.; funding acquisition, Y.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Postgraduate Research and Practice Innovation Program of Jiangsu Province under Grant No. KYCX20_0429 and by the Fundamental Research Funds for the Central Universities under Grant No. B200203127.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Yu, X.; Xue, Y. Smart Grids: A Cyber–Physical Systems Perspective. *Proc. IEEE* **2016**, *104*, 1058–1070. [CrossRef]
2. Xue, Y.; Yu, X. Beyond smart grid—cyber–physical–social system in energy future [point of view]. *Proc. IEEE* **2017**, *105*, 2290–2292. [CrossRef]
3. Abdelmalak, M.; Venkataramanan, V.; Macwan, R. A Survey of Cyber-Physical Power System Modeling Methods for Future Energy Systems. *IEEE Access* **2022**, *10*, 99875–99896. [CrossRef]
4. Zhang, Y.; Ni, M.; Sun, Y. Fully Distributed Economic Dispatch for Cyber-physical Power System with Time Delays and Channel Noises. *J. Mod. Power Syst. Clean Energy* **2022**, *10*, 1472–1481. [CrossRef]

5. Dong, Z.; Tian, M.; Ding, L. A Framework for Modeling and Structural Vulnerability Analysis of Spatial Cyber-Physical Power Systems From an Attack–Defense Perspective. *IEEE Syst. J.* **2021**, *15*, 1369–1380. [CrossRef]
6. Li, Z.; Shahidehpour, M.; Aminifar, F. Cybersecurity in Distributed Power Systems. *Proc. IEEE* **2017**, *105*, 1367–1388. [CrossRef]
7. Oyewole, P.A.; Jayaweera, D. Power System Security with Cyber-Physical Power System Operation. *IEEE Access* **2020**, *8*, 179970–179982. [CrossRef]
8. Yohanandhan, R.V.; Elavarasan, R.M.; Manoharan, P.; Mihet-Popa, L. Cyber-Physical Power System (CPPS): A Review on Modeling, Simulation, and Analysis With Cyber Security Applications. *IEEE Access* **2020**, *8*, 151019–151064. [CrossRef]
9. Li, M.; Xue, Y.; Ni, M.; Li, X. Modeling and Hybrid Calculation Architecture for Cyber Physical Power Systems. *IEEE Access* **2020**, *8*, 138251–138263. [CrossRef]
10. He, R.; Yang, S.; Deng, J.; Feng, T.; Lai, L.L.; Shahidehpour, M. Reliability Analyses of Wide-Area Protection System Considering Cyber-Physical System Constraints. *IEEE Trans. Smart Grid* **2021**, *12*, 3458–3467. [CrossRef]
11. Liu, N.; Zhang, J.; Zhang, H.; Liu, W. Security Assessment for Communication Networks of Power Control Systems Using Attack Graph and MCDM. *IEEE Trans. Power Deliv.* **2010**, *25*, 1492–1500. [CrossRef]
12. Sen, A.; Madria, S. Risk Assessment in a Sensor Cloud Framework Using Attack Graphs. *IEEE Trans. Serv. Comput.* **2017**, *10*, 942–955. [CrossRef]
13. Wang, H.; Chen, Z.; Zhao, J.; Di, X.; Liu, D. A Vulnerability Assessment Method in Industrial Internet of Things Based on Attack Graph and Maximum Flow. *IEEE Access* **2018**, *6*, 8599–8609. [CrossRef]
14. He, W.; Li, H.; Li, J. Unknown Vulnerability Risk Assessment Based on Directed Graph Models: A Survey. *IEEE Access* **2019**, *7*, 168201–168225. [CrossRef]
15. Sun, F.; Pi, J.; Lv, J.; Cao, T. Network security risk assessment system based on attack graph and Markov chain. *J. Physics Conf. Ser.* **2017**, *910*, 012005. [CrossRef]
16. Qu, Z.; Xie, Q.; Liu, Y.; Li, Y.; Wang, L.; Xu, P.; Zhou, Y.; Sun, J.; Xue, K.; Cui, M. Power Cyber-Physical System Risk Area Prediction Using Dependent Markov Chain and Improved Grey Wolf Optimization. *IEEE Access* **2020**, *8*, 82844–82854. [CrossRef]
17. Zhang, Q.; Zhou, C.; Xiong, N.; Qin, Y.; Li, X.; Huang, S. Multimodel-Based Incident Prediction and Risk Assessment in Dynamic Cybersecurity Protection for Industrial Control Systems. *IEEE Trans. Syst. Man, Cybern. Syst.* **2016**, *46*, 1429–1444. [CrossRef]
18. Zhang, Q.; Zhou, C.; Tian, Y.C.; Xiong, N.; Qin, Y.; Hu, B. A Fuzzy Probability Bayesian Network Approach for Dynamic Cybersecurity Risk Assessment in Industrial Control Systems. *IEEE Trans. Ind. Inform.* **2018**, *14*, 2497–2506. [CrossRef]
19. Zhang, Y.; Wang, L.; Xiang, Y.; Ten, C.W. Power System Reliability Evaluation with SCADA Cybersecurity Considerations. *IEEE Trans. Smart Grid* **2015**, *6*, 1707–1721. [CrossRef]
20. Chen, T.M.; Sanchez-Aarnoutse, J.C.; Buford, J. Petri net modeling of cyber-physical attacks on smart grid. *IEEE Trans. Smart Grid* **2011**, *2*, 741–749. [CrossRef]
21. Ramos, G.; Sanchez, J.L.; Torres, A.; Rios, M. Power systems security evaluation using petri nets. *IEEE Trans. Power Deliv.* **2009**, *25*, 316–322. [CrossRef]
22. Chen, B.; Yang, Z.; Zhang, Y.; Chen, Y.; Zhao, J. Risk Assessment of Cyber Attacks on Power Grids Considering the Characteristics of Attack Behaviors. *IEEE Access* **2020**, *8*, 148331–148344. [CrossRef]
23. Zonouz, S.; Davis, C.M.; Davis, K.R.; Berthier, R.; Bobba, R.B.; Sanders, W.H. SOCCA: A Security-Oriented Cyber-Physical Contingency Analysis in Power Infrastructures. *IEEE Trans. Smart Grid* **2014**, *5*, 3–13. [CrossRef]
24. Liu, X.; Shahidehpour, M.; Li, Z.; Liu, X.; Cao, Y.; Li, Z. Power System Risk Assessment in Cyber Attacks Considering the Role of Protection Systems. *IEEE Trans. Smart Grid* **2017**, *8*, 572–580. [CrossRef]
25. Lau, P.; Wang, L.; Liu, Z.; Wei, W.; Ten, C.W. A Coalitional Cyber-Insurance Design Considering Power System Reliability and Cyber Vulnerability. *IEEE Trans. Power Syst.* **2021**, *36*, 5512–5524. [CrossRef]
26. Xiang, Y.; Wang, L.; Zhang, Y. Power system adequacy assessment with probabilistic cyber attacks against breakers. In Proceedings of the 2014 IEEE PES General Meeting | Conference Exposition, Hong Kong, China, 7–10 December 2014; pp. 1–5. [CrossRef]
27. Liu, R.; Vellaithurai, C.; Biswas, S.S.; Gamage, T.T.; Srivastava, A.K. Analyzing the Cyber-Physical Impact of Cyber Events on the Power Grid. *IEEE Trans. Smart Grid* **2015**, *6*, 2444–2453. [CrossRef]
28. Lau. P.; Wang, L.; Wei, W.; Liu, Z.; Ten, C.-W. A Novel Mutual Insurance Model for Hedging Against Cyber Risks in Power Systems Deploying Smart Technologies. *IEEE Trans. Power Syst.* **2023**, *38*, 630–642. [CrossRef]
29. Dai, Q.; Shi, L.; Ni, Y. Risk Assessment for Cyberattack in Active Distribution Systems Considering the Role of Feeder Automation. *IEEE Trans. Power Syst.* **2019**, *34*, 3230–3240. [CrossRef]
30. Fu, R.; Huang, X.; Xue, Y.; Wu, Y.; Tang, Y.; Yue, D. Security Assessment for Cyber Physical Distribution Power System Under Intrusion Attacks. *IEEE Access* **2019**, *7*, 75615–75628. [CrossRef]
31. Wang, Y.; Feng, C.; Li, Y.; Xu, T.; Zhu, M. Expected Failure Method and Its Analysis for Safety Evaluation in a Cyber-Physical Power System. *IEEE Access* **2022**, *10*, 133348–133356. [CrossRef]
32. Li, M.; Xu, H.; Xu, J.; Ding, Z.; Liu, Q.; Yin, Z. Risk Assessment of Cyber Physical Power System considering Attack Model. In Proceedings of the 2022 IEEE 5th International Electrical and Energy Conference (CIEEC), Nanjing, China, 27–29 May 2022; pp. 4650–4655. [CrossRef]
33. Zhou, X.; Yang, Z.; Ni, M.; Lin, H.; Li, M.; Tang, Y. Analysis of the Impact of Combined Information-Physical-Failure on Distribution Network CPS. *IEEE Access* **2020**, *8*, 44140–44152. [CrossRef]

34. Qin, H.; Weng, J.; Liu, D.; Qi, D.; Wang, Y. Risk assessment and defense resource allocation of cyber-physical distribution system under denial of service attack. *CSEE J. Power Energy Syst.* **2021**, *in press*. [CrossRef]
35. Sidhu, T.S.; Yin, Y. Modelling and Simulation for Performance Evaluation of IEC61850-Based Substation Communication Systems. *IEEE Trans. Power Deliv.* **2007**, *22*, 1482–1489. [CrossRef]
36. Zonouz, S.; Rogers, K.M.; Berthier, R.; Bobba, R.B.; Sanders, W.H.; Overbye, T.J. SCPSE: Security-Oriented Cyber-Physical State Estimation for Power Grid Critical Infrastructures. *IEEE Trans. Smart Grid* **2012**, *3*, 1790–1799. [CrossRef]
37. Allan, R.; Billinton, R.; Sjarief, I.; Goel, L.; So, K. A reliability test system for educational purposes-basic distribution system data and results. *IEEE Trans. Power Syst.* **1991**, *6*, 813–820. [CrossRef]