Defensive Resource Allocation Method for Improving Survivability of Communication and Information System in CPPS Against Cyber-attacks

Yingjun Wu, Hao Xu, and Ming Ni

***Abstract*—With the widespread use of communication and information technology, power system has been evolving into cyber-physical power system (CPPS) and becoming more vulnerable to cyber-attacks. Therefore, it is necessary to enhance the ability of the communication and information system in CPPS to defend against cyber-attacks. This paper proposes a method to enhance the survivability of the communication and information system in CPPS. Firstly, the communication and information system for critical business of power system is decomposed into certain types of atomic services, and then the survivability evaluation indexes and their corresponding calculation method for the communication and information system are proposed. Secondly, considering the efficacy and cost defensive resources, a defensive resource allocation model is proposed to maximize the survivability of communication and information system in CPPS. Then, a modified genetic algorithm is adopted to solve the proposed model. Finally, the simulation results of CPPS for an IEEE 30-node system verify the proposed method.**

***Index Terms*—Cyber-physical power system (CPPS), cyber-attacks, survivability evaluation, communication and information system, defensive resource.**

I. Introduction

WITH the large-scale application of modern advanced communication and information technology, power system has been evolving into cyber-physical power system (CPPS) [1]. Modern advanced communication and information technology not only enhances the safety and efficiency of power system operations [2], [3], but also makes the power system more vulnerable to cyber-attacks due to its critical businesses which are increasingly dependent on the communication and information system. In such case, by weakening or even destroying the functions of the communication and information system, cyber-attacks will threaten the safe and stable operation of power systems [4], [5].

In recent years, many researches on the decision making of real-time defense strategy against cyber-attacks have been reported. The behavior and purpose of cyber-attacks are analyzed in [6], [7], and a corresponding detection and identification method for cyber-attacks is proposed in [8]. The forms and the propagation processes of cyber-attacks are studied in [9], [10]. Based on these researches, [11] proposes a method to deploy security countermeasures to protect an organization by its attack graph, and [5] uses a graph-theoretical formulation for attacks of false data injection in smart grids and proposes the defense mechanisms to mitigate this type of attacks. However, these defensive methods are targeting for one or several types of cyber-attacks, and there is no guarantee that these defenses will succeed. So, even with the defense strategy, the communication and information system is still facing the security risks [12]. For example, the "Stuxnet" virus attacked a nuclear power plant in Iran and the plant stopped operating in 2010. A cyber-attack attacked the power grid in Ukraine and finally resulted in a large-scale blackout in 2015 [13]. And the corresponding defense countermeasures were implemented in time after a cyber-attack occurred in Israel in 2016, which blocked the spread of the cyber-attack effect and avoided a large-scale blackout, but cost a lot in economic terms [14].

Therefore, for existing power systems and their auxiliary communication and information system, there may be cyber-attacks that cannot be defended or can be defended but costly even with cyber-attack defense measures. This problem can only be solved by optimizing the defense resource allocation and improving the inherent survivability of CPPS. Many researchers have proposed some resource allocation methods for improving the survivability of CPPS. References [15] and [16] explore the survivability of the communication and information system and the effect of survivability in the process of defending against cyber-attacks. References [17]-[22] propose some survivability defensive methods for improving the vulnerability of the communication and information system in smart grids. However, the above references only investigate the methods to improve the survivability of communication and information system in CPPS, and do not

Manuscript received: March 7, 2019; accepted: August 26, 2019. Date of CrossCheck: August 26, 2019. Date of online publication: March 26, 2020.

This work was supported by "Research on Operation Situation Awareness and Proactive Defense of Power Cyber-Physical System Against Cyber Attacks" and the Fundamental Research Funds for the Central Universities (No. 2018B05814).

Y. Wu (corresponding author) is with the College of Energy and Electrical Engineering, Hohai University, Nanjing, China, and he is also with the College of Automation & College of Artificial Intelligence, Nanjing University of Posts and Telecommunications, Nanjing, China (e-mail: ywu_ee@vip.163.com).

H. Xu is with the College of Automation and College of Artificial Intelligence, Nanjing University of Posts and Telecommunications, Nanjing, China (e-mail: xuhao6592@163.com).

M. Ni is with NARI Group Corporation (State Grid Electric Power Research Institute), Nanjing, China (e-mail: ni-ming@sgepri.sgcc.com.cn).

DOI: 10.35833/MPCE.2019.000148

consider how to maximize the survivability from a systemic perspective. There is still no effective optimization model of defense resource allocation to improve the survivability of the communication and information system in CPPS.

Targeting at improving the survivability of the communication and information system in CPPS, this paper proposes a model and the method for the defense resource allocation. Firstly, based on the analysis of the evaluation of the survivability in CPPS, each critical power business of CPPS is broken down into many atomic services. Then, a set of survivability indexes of atomic services and the corresponding calculation methods are proposed, and the defense resources for improving different survivability are given. Secondly, a defensive resource allocation model to decide the kind and number of defensive measures for enhancing the survivability of atomic services is established. The main contributions of this paper are as follows.

1) The goal of cyber-attack defense is to guarantee the key power businesses undertaken by the communication and information system in CPPS, but these critical businesses are difficult to be guaranteed. By decomposing the critical businesses into more operational atomic services, the critical businesses can be guaranteed by enhancing the survivability of these atomic services.

2) From the perspectives of attack identification ability at the beginning of the cyber-attacks, the resistance during the effect propagation of cyber-attacks and the recovering ability of critical businesses after cyber-attacks, the defensive resource allocation model for enhancing the survivability of the atomic services is established.

The rest of this paper is organized as follows. The method for assessing the survivability of communication and information system is given in Section II. A defensive resource allocation model for improving the survivability of communication and information system is proposed in Section III. An improved genetic algorithm for solving the optimal configuration of defensive resources is introduced in Section IV. Section V shows the simulations and Section VI draws the conclusion.

II. Survivability Evaluation of Communication and Information System in CPPS

A. *Definition of Survivability for Communication and Information System*

The main mission of the communication and information system in CPPS is to complete the power businesses. According to the regulations issued by the Economic and Trade Commission of the People's Republic of China [23] and the Electricity Regulatory Commission [24], the power businesses are classified into four major security areas. Area 1 contains safety and stability system (SSS), relay protection (RP) and power dispatch (PD). Area 2 contains protection management information system (PMIS) and electricity market (EM), etc. Area 3 contains hydrological information system (HIS) and lightning positioning system (LPS), etc. Area 4 contains shared resource management (SRM) and official document approval business (ODAB), etc. The businesses that the power system will not function properly after their failures are called critical businesses such as SSS, RP and PD in Area 1. In this paper, the survivability of the communication and information system in CPPS is defined as the ability to ensure the critical businesses of power system after cyber-attacks.

B. *Decomposition of Power Businesses into Atomic Services*

The power businesses are difficult to be guaranteed. In this section, the concept of atomic service is defined as the smallest independent unit of power business and can be implemented by one or several communication and information elements. Therefore, the consequences of attacking atomic services are independent of each other [25] and the critical businesses can be guaranteed by enhancing the survivability of these atomic services.

C. *Survivability Indexes of Atomic Services*

Three indexes are selected based on the time scale which are defined as follows.

1) Identifiability index: the ability of CPPS to identify cyber-attack at the beginning.

2) Resistibility index: the ability of CPPS to ensure critical businesses during the effect propagation of cyber-attack.

3) Recoverability index: the ability of CPPS to recover the critical businesses after cyber-attack.

D. *Framework of Survivability Evaluation*

In this section, the framework of survivability evaluation is proposed, as shown in Fig. 1. Firstly, the critical businesses are selected which need to be guaranteed according to the specific needs of the survivability in power system. Secondly, based on the concept of atomic service, the critical businesses are decomposed into the smallest independent unit that can impose the measures to enhance the survivability. Finally, the survivability of atomic services is evaluated for the perspectives of the ability to identify cyber-attacks at the beginning, the ability to ensure critical businesses during the effect propagating of cyber-attacks, and the ability to recover the critical businesses after cyber-attacks.

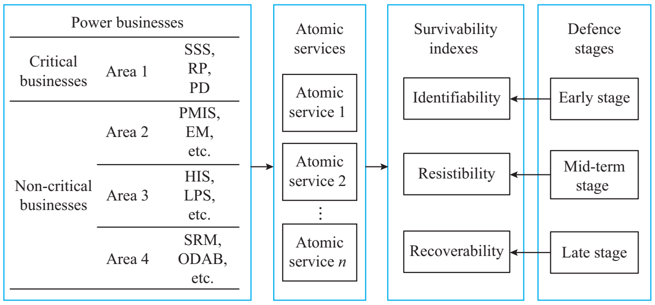


Fig. 1. Framework of survivability evaluation by decomposing power businesses into atomic services.

E. *Calculation Method of Survivability Evaluation Indexes*

1) *Effect of Defensive Measures for Calculating Survivability Evaluation Index*

The effect of defensive measures is needed to calculate the survivability evaluation indexes of atomic services. In order to calculate the survivability index, the effect of defensive measures is collected through the simulation after the defense resources are configured. The steps shown in Fig. 2 are given as follows.

Step 1: based on the steps for the execution process of critical businesses, the critical businesses are decomposed into atomic services. The cyber-attacks are selected to form a cyber-attack library according to the degree of cyber-attack threat to different atomic services. The cyber-attack library includes the probability that different attacks choose different types of atomic services as targets.

Step 2: an unselected cyber-attack is selected in the cyber-attack library randomly.

Step 3: based on the characteristics of cyber-attacks, the consequences of cyber-attacks on the system are simulated for multiple times. And the basic data used to calculate the evaluation indexes are collected.

Step 4: judge if all cyber-attacks in the cyber-attack library have been selected. If yes, *Step 5* is executed. Otherwise, go back to *Step 2*.

Step 5: calculate the expectation values of the collected data used to calculate the evaluation indexes.

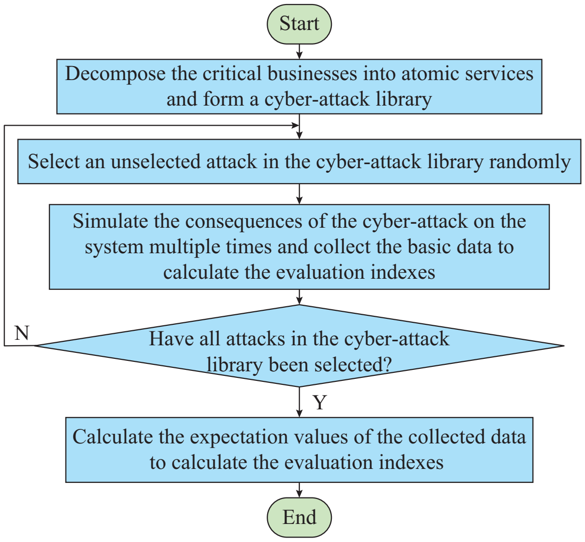

Start
Decompose the critical businesses into atomic services and form a cyber-attack library
Select an unselected attack in the cyber-attack library randomly
Simulate the consequences of the cyber-attack on the system multiple times and collect the basic data to calculate the evaluation indexes
N
Have all attacks in the cyber-attack library been selected?
Y
Calculate the expectation values of the collected data to calculate the evaluation indexes
End

Fig. 2. Process of data acquisition.

2) *Calculation of Survivability Evaluation Indexes*

This section quantifies the survivability indexes. The attack hazard index and the attack impedance rate index are used to evaluate the resistibility. The indexes of attack identification rate and the attack identification time are adopted to evaluate the identifiability while the indexes of attack recovery time and the attack recovery rate are utilized to evaluate the recoverability.

1) Calculation of identifiability index

The index of attack identification rate for the j^{th} atomic service in the m^{th} critical business atomic service is:

$$RI_{A,mj}=\sum_{i=1}^{K} RI_{mji}\cdot P_{D,mji} \tag{1}$$

$$RI_{mji}=\begin{cases}1 & \text{attack can be identified}\\ 0 & \text{attack cannot be identified}\end{cases} \tag{2}$$

where RI_{mji} is the identification result when j^{th} atomic service in the m^{th} critical business suffers the i^{th} cyber-attack; $P_{D,mji}$ is the probability that the j^{th} atomic service in the m^{th} critical business suffers the i^{th} cyber-attack; i is the number of cyber-attacks; and K is the total number of attacks in the attack library.

The attack identification rate indexes of the m^{th} critical business and the entire system are $RI_{S,m}$ and RI_S, respectively.

$$RI_{S,m}=\sum_{j=1}^{N_m} RI_{A,mj}\cdot W_{A,mj} \tag{3}$$

$$RI_S=\sum_{m=1}^{M} RI_{S,m}\cdot W_{S,m} \tag{4}$$

where N_m is the total number of atomic services included in the m^{th} critical business; M is the total number of critical businesses; $W_{A,mj}$ is the relative weight of the j^{th} atomic service in the m^{th} critical business; and $W_{S,m}$ is the relative weight of the m^{th} critical business. The sum of the relative weights of all atomic services is 1. The size of the weight depends on the impact of atomic service fault on the critical business. The sum of the relative weights of all critical businesses is 1. The weight depends on the impact of critical business failures on system security and stability.

The index of attack identification time for the j^{th} atomic service in the m^{th} critical business $TI_{A,mj}$ is:

$$TI_{A,mj}=\sum_{i=1}^{K} TI_{mji}\cdot P_{D,mji} \tag{5}$$

$$TI_{mji}=\begin{cases}1.0 & T_{mji}\le 10\ \text{s}\\ 0.8 & 10\ \text{s}<T_{mji}\le 1\ \text{min}\\ 0.5 & 1\ \text{min}<T_{mji}\le 5\ \text{min}\\ 0.2 & 5\ \text{min}<T_{mji}\le 10\ \text{min}\\ 0 & T_{mji}>10\ \text{min}\end{cases} \tag{6}$$

where TI_{mji} is the rate of T_{mji}; and T_{mji} is the attack identification time when the j^{th} atomic service in the m^{th} critical business suffers the i^{th} cyber-attack.

The indexes of attack identification time for the m^{th} critical business and the entire system are $TI_{S,m}$ and TI_S, respectively.

$$TI_{S,m}=\sum_{j=1}^{N_m} TI_{A,mj}\cdot W_{A,mj} \tag{7}$$

$$TI_S=\sum_{m=1}^{M} TI_{S,m}\cdot W_{S,m} \tag{8}$$

2) Calculation of resistibility index

The extent to which an atomic service is destroyed by an attack is:

$$AD_{A,mj}=\sum_{i=1}^{K} AD_{mji}\cdot P_{D,mji} \tag{9}$$

$$AD_{mji}=\begin{cases}1 & \text{atomic service cannot work}\\ 0 & \text{atomic service works properly}\end{cases} \tag{10}$$

where $AD_{A,mj}$ is the attack hazard index of the j^{th} atomic service in the m^{th} critical business; and AD_{mji} is the attack result when the j^{th} atomic service in the m^{th} critical business suffers the i^{th} cyber-attack.

The attack hazard index of the m^{th} critical business with N_m atomic services is:

$$AD_{S,m} = \sum_{j=1}^{N_m} AD_{A,mj} \cdot W_{A,mj} \tag{11}$$

The attack hazard index of the entire system is:

$$AD_S = \begin{cases} 1 & \exists AD_{S,m} \ge 1 \\ \sum_{m=1}^{M} AD_{S,m} \cdot W_{S,m} & \text{else} \end{cases} \tag{12}$$

The probability that an atomic service is attacked successfully is:

$$AS_{A,mj} = \sum_{i=1}^{K} AS_{mji} \cdot P_{D,mji} \tag{13}$$

where AS_{mji} is the probability that the i^{th} cyber-attack will be succeed in the j^{th} atomic service of the m^{th} critical business.

The probability of successful attack on the m^{th} critical business with N_m atomic services is:

$$AS_{S,m} = \sum_{j=1}^{N_m} AS_{A,mj} \cdot W_{A,mj} \tag{14}$$

The probability of successful attack on the entire system is:

$$AS_S = \begin{cases} 1 & \exists AS_{S,m} \ge 1 \\ \sum_{m=1}^{M} AS_{S,m} \cdot W_{S,m} & \text{else} \end{cases} \tag{15}$$

The attack impedance index for the entire system is:

$$AP_S = 1 - AS_S \tag{16}$$

3) Calculation of recoverability index

The attack recovery time index of atomic service is:

$$RT_{mji} = \begin{cases} T_{R,mji}/T_{0,mj} & T_{R,mji} \le T_{0,mj} \\ 1 & T_{R,mji} > T_{0,mj} \end{cases} \tag{17}$$

$$RT_{A,mj} = \sum_{i=1}^{K} RT_{mji} \cdot P_{D,mji} \tag{18}$$

where $RT_{A,mj}$ is the index of attack recovery time for the j^{th} atomic service in the m^{th} critical business; RT_{mji} is the recovery time index when the j^{th} atomic service in the m^{th} critical business suffers the i^{th} cyber-attack; $T_{R,mji}$ is the actual recovery time when the j^{th} atomic service in the m^{th} service suffers the i^{th} cyber-attack; and $T_{0,mj}$ is the demand recovery time of the j^{th} atomic service in the m^{th} critical business.

The indexes of attack recovery time for critical business and the entire system are:

$$RT_{S,m} = \sum_{j=1}^{N_m} RT_{A,mj} \cdot W_{A,mj} \tag{19}$$

$$RT_S = \sum_{m=1}^{M} RT_{S,m} \cdot W_{S,m} \tag{20}$$

where $RT_{S,m}$ is the index of attack recovery time for the m^{th} critical business; and RT_S is the index of attack recovery time for the entire system.

The index of attack recovery rate for critical business is:

$$RR_{S,m} = \frac{\sum_{i=1}^{K} Q_{R,i} P_{D,mji}}{Q_0} \tag{21}$$

where $Q_{R,i}$ is the system suffering from the i^{th} cyber-attack; and Q_0 is the number of atomic services involved in the m^{th} critical business during normal operation. The number of atomic services involved in the m^{th} critical business after the system is restored.

The index of attack recovery rate for the entire system is:

$$RR_S = \sum_{m=1}^{M} RR_{S,m} \cdot W_{S,m} \tag{22}$$

4) Fusion of survivability assessment indexes

The fusion index can directly reflect the survivability of the system. Among all the above indexes, the smaller the AD_S and RT_S, the better the system survivability, and the larger the RI_S, TI_S, AP_S and RR_S, the better the system survivability. The relationship between unified indexes and survivability is that the composition vector $\boldsymbol{R}$= [RI_S, TI_S, AP_S, RR_S, 1−AD_S, 1−RT_S]. The formula for calculating the fusion index is:

$$h(\boldsymbol{R}) = a\frac{1}{E}\|\boldsymbol{R}\|_1 + b\|\boldsymbol{R}\|_\infty \tag{23}$$

where a and b are the weight coefficients which satisfy $a + b = 1$, and this paper takes $a = b = 0.5$; E is the total number of indexes; and $\|\boldsymbol{R}\|_1$ and $\|\boldsymbol{R}\|_\infty$ are the 1 norm and the infinite norm of the vector $\boldsymbol{R}$, respectively.

$$\begin{cases} \|\boldsymbol{R}\|_1 = \sum_{e=1}^{E} |R_e| \\ \|\boldsymbol{R}\|_\infty = \max|R_e| \end{cases} \tag{24}$$

where R_e is the e^{th} element in vector $\boldsymbol{R}$.

F. Defensive Resources for Improving Survivability

Defensive resources are defense measures (hardware or software) equipped in CPPS to enhance its survivability. Corresponding to the survivability assessment indexes, the defensive resources are divided into three categories, which are respectively used to enhance the corresponding survivability [19]-[22].

1) Identifiability defensive resources are used to enhance the system recognizability. Commonly-used defensive measures include intrusion detection technology, honeypot technology [19], [20]. The cost is:

$$C_{ide1} n_{ide1,mj} + C_{ide2} n_{ide2,mj} = C_{ide,mj} \tag{25}$$

where C_{ide1} is the cost of adding an intrusion detection software to the atomic service; C_{ide2} is the cost of adding a honeypot component to the atomic service; $n_{ide1,mj}$ is the number of intrusion detection software on the j^{th} atomic service in the m^{th} critical business; $n_{ide2,mj}$ is the number of honeypot components on the j^{th} atomic service in the m^{th} critical business; and $C_{ide,mj}$ is the identifiability defensive resource cost of the j^{th} atomic service in the m^{th} critical business.

2) Resistibility defensive resources are used to enhance the system resistance ability. Commonly-used defensive measures are firewall technology, access control technology, and the deployment of camouflage components [19], [21]. The

cost is:

$$C_{res1}n_{res1,mj}+C_{res2}n_{res2,mj}+C_{res3}n_{res3,mj}=C_{res,mj} \tag{26}$$

where C_{res1} is the cost of adding a firewall to the atomic service; $n_{res1,mj}$ is the number of firewalls on the j^{th} atomic service in the m^{th} critical business; C_{res2} is the cost of adding a right control software to the atomic service; $n_{res2,mj}$ is the number of right control software on the j^{th} atomic service in the m^{th} critical business; C_{res3} is the cost of adding a camouflage component to the atomic service; $n_{res3,mj}$ is the number of camouflage components on the j^{th} atomic service in the m^{th} critical business; and $C_{res,mj}$ is the resistibility defensive resource costs of the j^{th} atomic service in the m^{th} critical business.

3) Recoverability defensive resources are used to enhance the system recoverability capabilities. Commonly-used defensive measures include the creation of redundant components, data backup and recovery technology [22]. The cost is:

$$C_{rec1}n_{rec1,mj}+C_{rec2}n_{rec2,mj}=C_{rec,mj} \tag{27}$$

where C_{rec1} is the cost of adding a spare component to the atomic service; $n_{rec1,mj}$ is the number of spare components on the j^{th} atomic service in the m^{th} critical business; C_{rec2} is the cost of adding a data backup and recovery component to the atomic service; $n_{rec2,mj}$ is the number of data backup and recovery components on the j^{th} atomic service in the m^{th} critical business; and $C_{rec,mj}$ is the recoverability defensive resource costs of the j^{th} atomic service in the m^{th} critical business.

III. Model of Defensive Resource Allocation

Different defense effects can be achieved by configuring different numbers and types of defensive measures on the atomic service. Considering the constraints of defense resource configuration, we configure different numbers and types of defensive measures on all atomic services, and form different configuration schemes of defense resources. The optimization variables in the model are the number and type of defense measures on atomic services. The consequences of cyber-attacks are simulated and the survivability defense effect is evaluated by calculating the indexes.

A. Objective Function

Quantify system survivability through survivability fusion indexes based on (23). The objective function is:

$$\max F(\boldsymbol{L})=h(\boldsymbol{R}) \tag{28}$$

where $\boldsymbol{L}$ is the atomic service defensive measure allocation matrix. The number of columns in $\boldsymbol{L}$ represents different atomic services. The number of rows in $\boldsymbol{L}$ represents the type of defensive measures. The elements in $\boldsymbol{L}$ represent the number of types of defensive measures configured on different atomic services.

B. Constraints

Resource allocation in the system is subject to the following conditions.

1) The total amount of defensive resources is limited as:

$$\sum_{m=1}^{M}\sum_{j=1}^{N_m}(C_{ide,mj}+C_{res,mj}+C_{rec,mj})\le C_0 \tag{29}$$

where C_0 is the total cost of defensive resources.

2) Each defensive resource configurable on each atomic service also has a cost cap as:

$$\begin{cases} C_{ide,mj}\le C_{ide0} \\ C_{res,mj}\le C_{res0} \quad j=1,2,...,N_m, m=1,2,...,M \\ C_{rec,mj}\le C_{rec0} \end{cases} \tag{30}$$

where C_{ide0} is the upper limit of the cost of identifiability defensive resource on atomic services; C_{res0} is the upper limit of the cost of resistibility defensive resource on atomic services; and C_{rec0} is the upper limit of the cost of identifiability defensive resource on atomic services.

IV. Modified Genetic Algorithm for Proposed Model

A. Improvement of Genetic Algorithm

This paper uses an improved genetic algorithm [26]. The specific improvements are as follows:

1) In the encoding process, the decimal encoding is adopted.

2) The objective function of the proposed model is not directly selected as the fitness function. The following fitness function is used.

$$H=\begin{cases} F-F_{\min}+\dfrac{1}{1+\mathrm{e}^{-t}}(F_{\max}-F_{\min}) & \dfrac{F-\bar{F}}{\bar{F}-F_{\min}}<k \\ \dfrac{F}{1+\mathrm{e}^{t}} & \dfrac{F-\bar{F}}{\bar{F}-F_{\min}}\ge k \end{cases} \tag{31}$$

where H is an improved fitness function; F is the objective function value in (28); $F_{\max}$ and $F_{\min}$ are the maximum and minimum values of the objective function without consideration of constraints, respectively; $\bar{F}$ is the average of the maximum and minimum values of the objective function; and t is an evolutionary algebra with different values depending on the environment.

3) Roulette selection operator, adaptive crossover operator and adaptive mutation operator are adopted.

4) Chaotic perturbations are added to the algorithm. After performing selection, crossover, and mutation operations, we add some individuals with low fitness to the progeny population. Therefore, it is difficult for the group to fall into the local optimal solution.

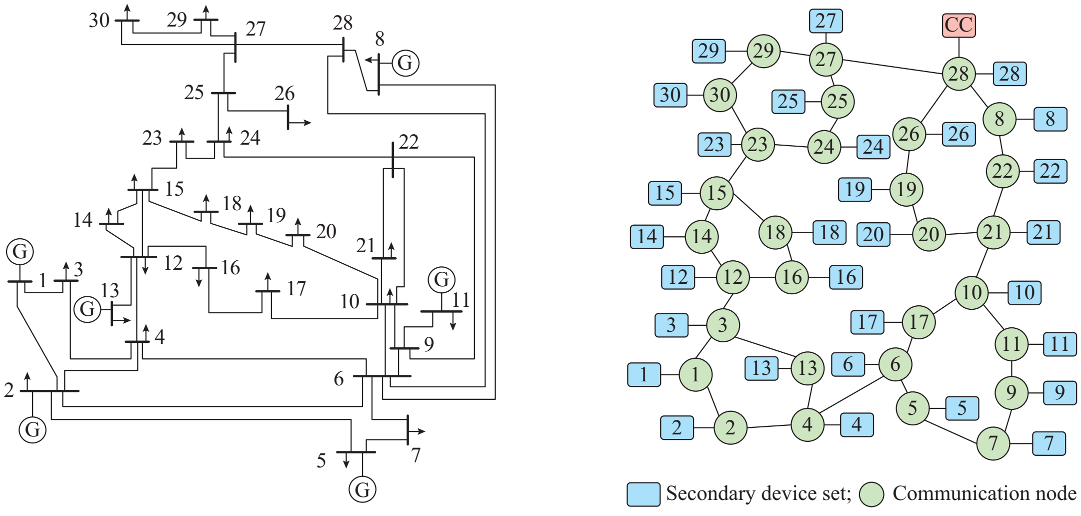
B. Algorithm Flow

The specific process of applying improved genetic algorithm to the survivability defensive resource allocation of the communication and information system is given in Algorithm 1.

V. Simulations

This section takes IEEE 30-node system as an example. The single-line diagram and its communication and information system are given in Fig. 3.

```
Algorithm 1: improved genetic algorithm
Input the maximum number of iterations $\lambda$; the weight of critical business in the system $W_{S,m}$; the weight of atomic services in critical business $W_{A,mj}$; the group size $M_G$; the individual coding method $C$; the terminate evolutionary algebra $T$; the crossover probability $P_c$; and the variation probability $P_v$. Configure the defense effect of different defense measures.
Output the defensive measure configuration scheme.
Initialize the number of iterations $t = 0$ and the defensive measure configured on the atomic service.
Repeat
    Step 1: randomly assign different numbers and types of defensive measures on atomic services within the constraints. The nodes are sorted by the number when encoding. Encode the number of defensive resources on the atomic service to obtain the individual gene $C_g$ and generate the initial population $Q_0$.
    Step 2: defensive effect data are brought into account based on the number and the type of defensive measures on the atomic service. Calculate the survivability assessment indexes $AP_S$, $RI_S$, $TI_S$, $RR_S$, $AD_S$, $RT_S$ according to the formula in Section II. Calculate the fusion index and the fitness function. Get the individual fitness $H$.
    Step 3: perform crossover, selection, and mutation operations. The individual $C_n$ that does not meet the constraint of defense resource cost is deleted, and the progeny population $R_t$ is generated.
    Step 4: perform chaotic perturbation operations, randomly add individuals that have been eliminated due to low fitness, ensure the population diversity, and obtain the population $Q_{t+1}$.
    Step 5: if the termination condition is satisfied, the termination condition that the maximum number of iterations reach, go to Step 6. Else go back to Step 2.
    Step 6: calculate the fitness of the resulting population and obtain the optimal solution set.
End
```



(a)

(b)

Fig. 3. Diagram of IEEE 30-node system and its communication network. (a) IEEE 30-node system. (b) Communication network.

A. Basic Introduction of System

1) Atomic services of critical businesses

The functions of SSS include: data collection (DC) on the power nodes such as frequency, voltage, and power data, data uploading (DU) to the substation, substation processing (SP) of the data, transmitting data to control center (CC) through communication nodes (CNs) by the substation, making decisions by CC, transmitting orders to substation through CNs by CC, substation analysis (SA) of orders, substation sending orders (SI), controlling the action (CA) of electric components to adjust the power output of power plant. Based on these functions, the SSS can be decomposed into the following atomic services, as shown in Fig. 4.

The functions of RP include: DC (current, voltage, and phase data), DU, SP, CN, CC, CN, SA, SI, CA (adjusting the power output of the power plant). Based on these functions, the RP can be decomposed into the following atomic services, as shown in Fig. 5.

The functions of PD include: DC (frequency, voltage, and power data), DU, SP, CN, CC, CN, SA, SI, CA (adjusting power to power plants and loads). Based on these functions, the PD can be decomposed into the following atomic services, as shown in Fig. 6.

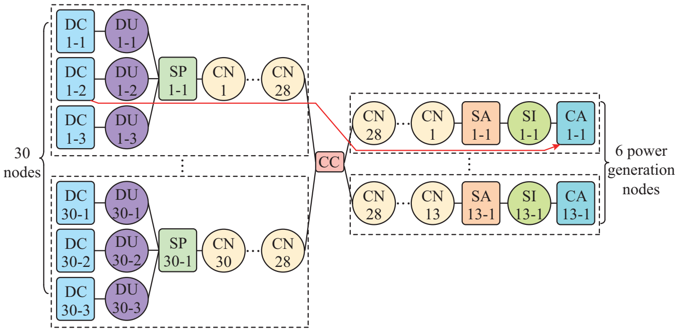


Fig. 4. Schematic diagram of SSS decomposition into atomic services.

According to the functions of atomic services, they are classified into three categories: data acquisition atomic services (DCAS), data transfer and processing atomic services (DTPAS) and control action atomic services (CAAS). The number of atomic services of all power businesses are shown in Table I.

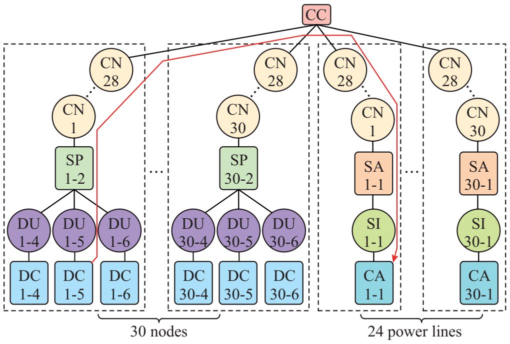


Fig. 5. Schematic diagram of RP decomposition into atomic services.

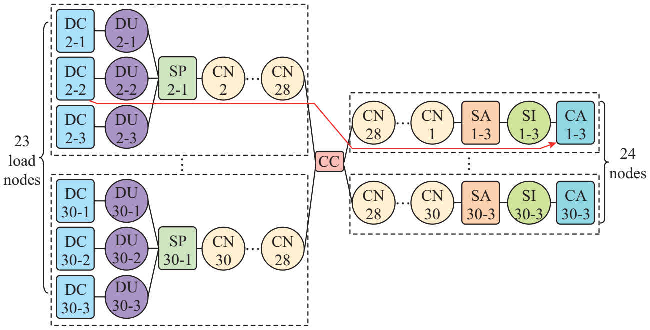


Fig. 6. Schematic diagram of PD decomposition into atomic services.

TABLE I
NUMBER OF ATOMIC SERVICES FOR ALL POWER BUSINESSES

Power business	Atomic service	Number
SSS	DCAS	90
	DTPAS	162
	CAAS	6
RP	DCAS	90
	DTPAS	198
	CAAS	24
PD	DCAS	69
	DTPAS	170
	CAAS	24

ALL the CN critical services are in the same topology. The DCAS in PD and part of the DCAS in SSS are the same. In summary, there are 180 DCAS, 378 DTPAS, 54 CAAS, and a total of 612 atomic services.

2) Cyber-attack library

Three various cyber-attacks F1, F2, and F3 are set in the simulation. The probabilities of each atomic service being attacked by these cyber-attacks are given in Table II [17].

3) Defensive resource library

Seven defensive measures of three defensive resource are adopted for enhancing the survivability of atomic services. Since the cost of these defensive measures is difficult to determine, this paper does not quantify the specific value of defensive measures. The cost and cost caps for all types of defensive measures are shown in Table III [20]-[23].

TABLE II
PROBABILITY OF THREE ATOMIC SERVICES SUFFERING FROM THREE CYBER-ATTACKS

Atomic service	Probability (%)		
	F1	F2	F3
DCAS	50	25	25
DTPAS	25	50	25
CAAS	25	25	50

TABLE III
DEFENSIVE RESOURCE COMPOSITION AND THEIR COSTS

Defensive resource	Defensive measure	Cost	Defensive resource cost cap on atomic services	Defensive resource cost cap on system
Resistibility defensive measure	Firewall technology	1	8	12000
	Access control technology	1		
	Deployment of camouflage components	2		
Identifiability	Intrusion detection technology	1	6	
	Honeypot technology	2		
Recoverability	Redundant components	3	10	
	Data backup and recovery technology	2		

4) Weights of atomic services for power business

Different atomic services have different degrees of impact on the survivability of power business. The weights of atomic services in Table IV [27] are used in calculating the survivability evaluation indexes.

TABLE IV
WEIGHTS OF ATOMIC SERVICES FOR DIFFERENT POWER BUSINESSES

Atomic service	W_{A1j} (SSS)	W_{A2j} (RP)	W_{A3j} (PD)
DC	0.003	0.0025	0.0030
DU	0.003	0.0025	0.0030
SP	0.005	0.0035	0.0035
CN	0.005	0.0045	0.0040
SA	0.010	0.0045	0.0060
SI	0.010	0.0040	0.0050
CA	0.010	0.0040	0.0050

B. Simulation Results and Analysis

1) Effect of defensive measures

Firstly, the effect of defensive measures used to calculate the indexes is collected by simulation. There are three types of atomic services, and each type of atomic services can suffer from three types of cyber-attacks, with a total of nine attack scenarios. In Fig. 7, the abscissa is the number of different defensive measures (NDM), and the ordinate is divided into three groups from left to right: ① the effect of configuring firewall technology, access control technology, and camouflage components on AD_S and AP_S; ② the effect of configuring intrusion detection technology and honeypot technology on RI_S and TI_S; ③ the effect of configuring redundant components, data backup and recovery technologies on RT_S and RR_S.

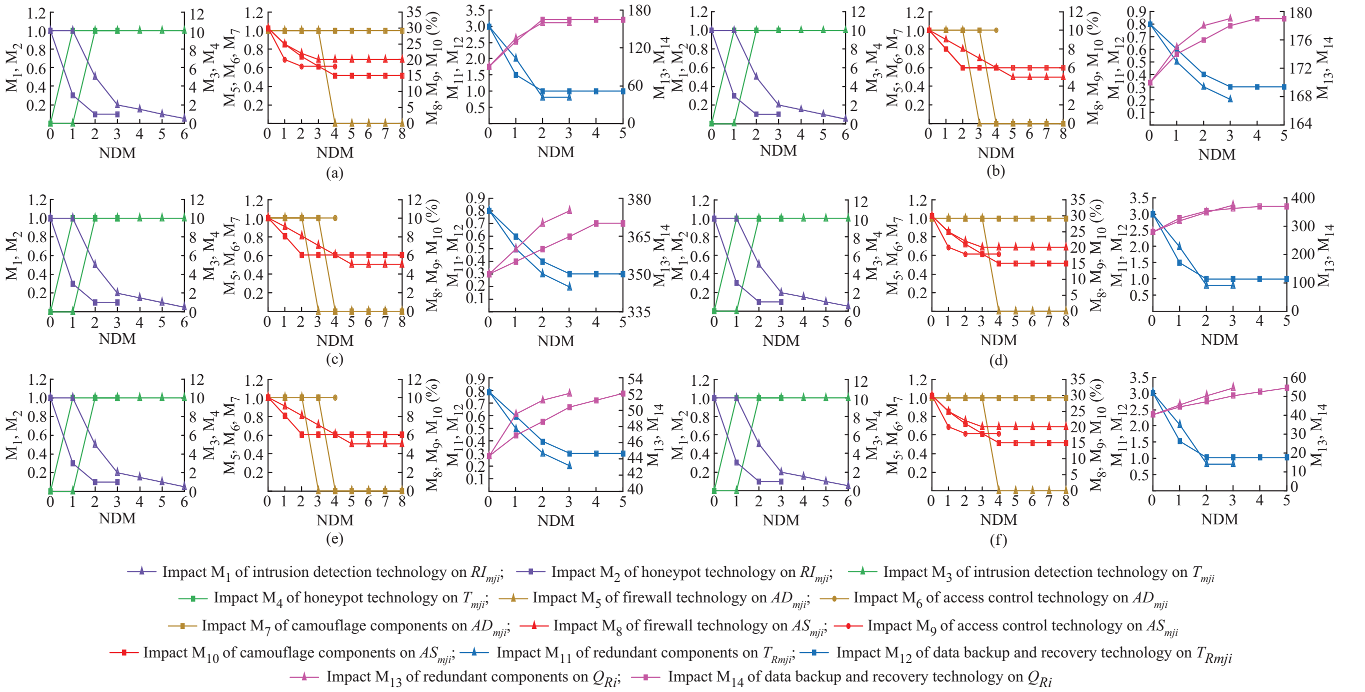


Fig. 7. Effect of defensive measures. (a) In the case of DCAS attacked by F1. (b) In the case of DCAS attacked by F2 or F3. (c) In the case of DTPAS attacked by F1 or F3. (d) In the case of DTPAS attacked by F2. (e) In the case of CAAS attacked by F1 or F2. (f) In the case of CAAS attacked by F3.

2) Allocation scheme of defense resources

With the data in Fig. 7, the survivability assessment indexes can be calculated. Then, the model of defensive resource allocation can be solved by the improved genetic algorithm. The defense resource configuration scheme is shown in Fig. 8. Vectors are used to represent the number of defensive measures. For example, [*a*, *b*, *c*, *d*, *e*, *f*, *g*] indicates the numbers of firewall technology, access control technology, camouflage components, intrusion detection technology, honeypot technology, redundant components and data backup and recovery technologies, respectively.

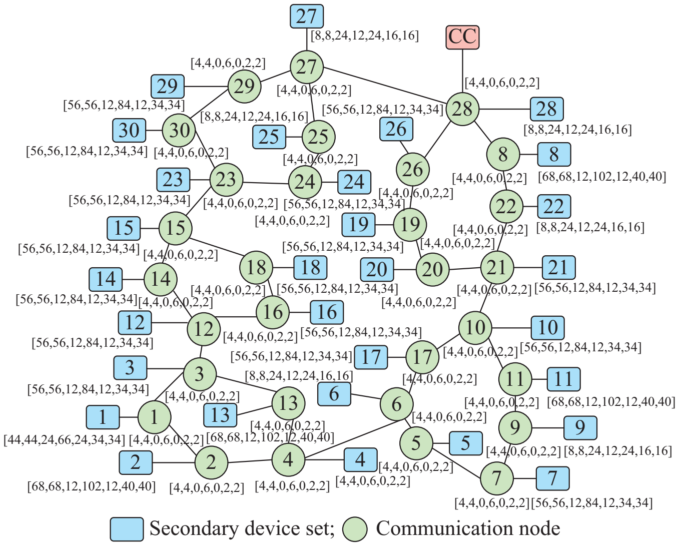


Fig. 8. Overall allocation of defensive resources.

As shown in Fig. 8, a large number of defense resources are allocated at all CNs because the execution of all critical businesses requires CN. Also, a large number of defense resources are allocated on the atomic services connected to the load nodes or generator nodes because the data collected on the load nodes or generator nodes are used for the SSS and the PD. The greatest number of defensive resources are allocated on the atomic services connected to the nodes conceded with both loads and generators. The specific allocation scheme of defense resources on atomic services of the SSS, the RP and the PD is shown in Fig. 9.

3) Effect of survivability improvement

A total 1000 simulations have been performed, in which the system configured with defensive resources are attacked by a randomly selected cyber-attack. As a comparison, 1000 simulations have been also performed for the system without defense resources. Then, the objective function of the proposed model and the fusion indexes are calculated based on these simulations. The results are shown in Fig. 4. It can be seen from Table V that after the defensive resources are configured, the survivability of the system increases significantly, which proves the effectiveness of the proposed method.

VI. Conclusion

Considering there may be cyber-attacks that cannot be defended or can be defended but costly for the existing power systems and their auxiliary communication and information system, even with cyber-attack defense measures, a method of defense resource allocation is proposed to enhance the survivability of the communication and information system in CPPS.

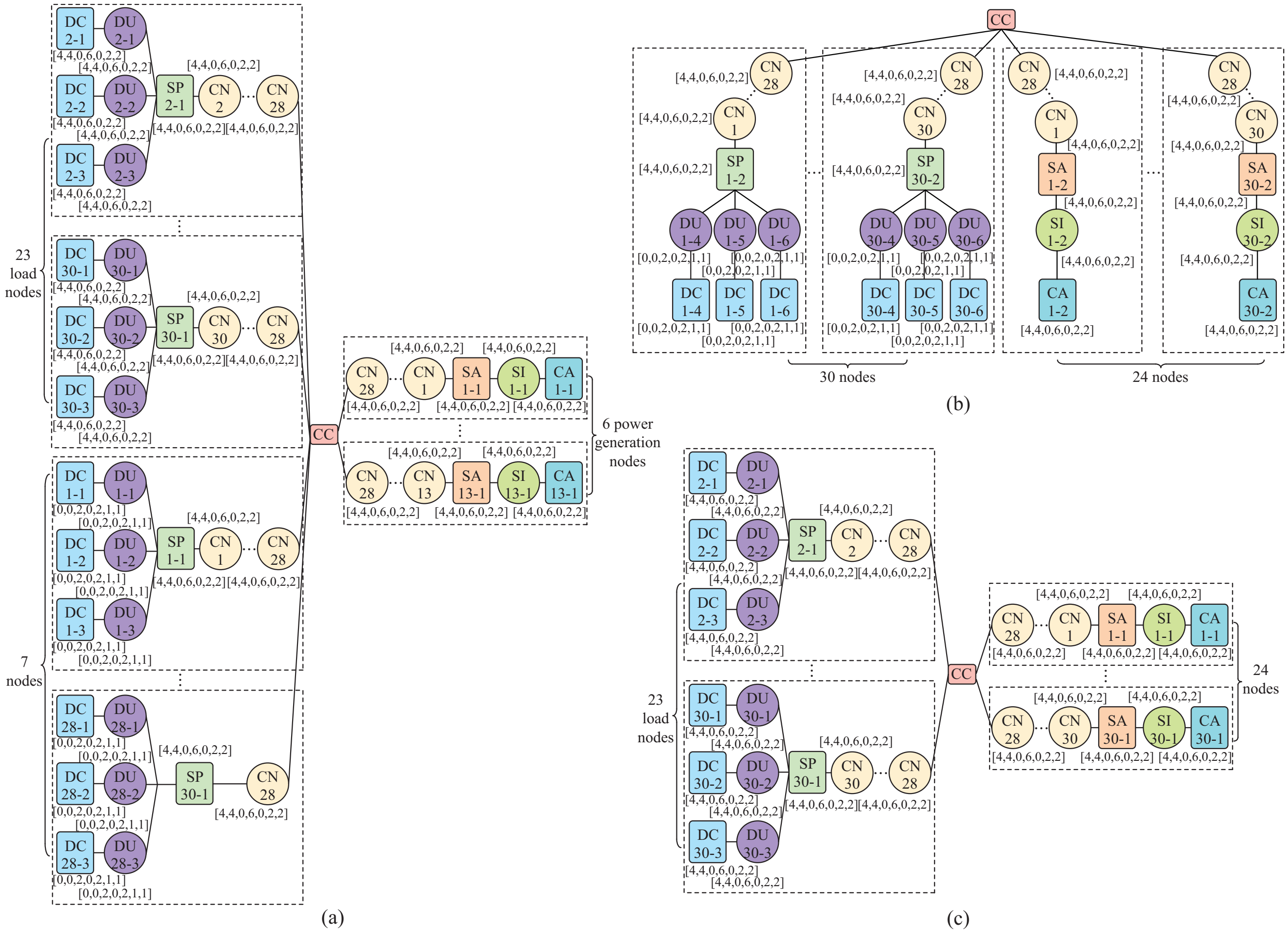


Fig. 9. Specific allocation of defensive resources on atomic services. (a) SSS. (b) RP. (c) PD.

TABLE V
SURVIVABILITY COMPARISON

Whether to configure defensive resources	Fusion index
No	0.5938
Yes	0.7413

Simulation results show that the method of defense resource allocation is effective to enhance the inherent survivability of the CPPS. This paper is a preliminary study on the research methods of cyber-attack defense resource allocation. In the future, it can be further studied from the following aspects: ① after configuring defense resources on atomic services, the survivability of atomic services can be enhanced. But the degree of improvement is still quantified by the simulation. In the future, the effect of defensive measures can be obtained through actual experiments to make the optimization result more realistic; ② this paper focuses on how to enhance the survivability by configuring defense resources on atomic services (that is, configuring defense resources on the nodes of the communication and information system). One of the most noteworthy aspects of future research is how to optimize the topology of the communication and information system to enhance its survivability.

REFERENCES

[1] Y. Han, C. Guo, S. Ma *et al.*, "Modeling cascading failures and mitigation strategies in PMU based cyber-physical power systems," *Journal of Modern Power Systems and Clean Energy*, vol. 6, no. 5, pp. 944-957, Sept. 2018.

[2] Z. Su, L. Xu, S. Xin *et al.*, "A future outlook for cyber-physical power system," in *Proceedings of IEEE Conference on Energy Internet and Energy System Integration*, Beijing, China, Nov. 2017, pp. 1-4.

[3] K. D. Kim and P. R. Kumar, "Cyber-physical systems：a perspective at the centennial," *Proceedings of the IEEE*, vol. 100, pp. 1287-1380, May 2012.

[4] Y. Tang, Q. Chen, M. Li *et al.*, "Overview on cyber-attacks against cyber physical power system," *Automation of Electric Power Systems*, vol. 40, no. 17, pp. 59-69, Sept. 2016.

[5] M. H. Ansari, V. T. Vakili, B. Bahrak *et al.*, "Graph theoretical defense mechanisms against false data injection attacks in smart grids," *Journal of Modern Power Systems and Clean Energy*, vol. 6, no. 5, pp. 860-871, Sept. 2018.

[6] G. Liang, J. Zhao，F. Luo *et al.*, "A review of false data injection attacks against modern power systems," *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1630-1638, Jul. 2017.

[7] S. Amini, F. Pasqualetti, and H. Mohsenian-Rad, "Dynamic load altering attacks against power system stability: attack models and protection schemes," *IEEE Transactions on Smart Grid*, vol. 9, no. 4, pp. 2862-2872, Oct. 2016.

[8] N. Živkovic and A. T. Saric, "Detection of false data injection attacks using unscented Kalman filter," *Journal of Modern Power Systems and Clean Energy*, vol. 6, no. 5, pp. 847-859, Sept. 2018.

[9] J. Zhao, G. Zhang, M. L. Scala *et al.*, "Short-term state forecasting-aided method for detection of smart grid general false data injection attacks," *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1580-1590, Jul. 2017.

[10] J. Letchford and Y. Vorobeychik, "Optimal interdiction of attack

plans," in *Proceedings of International Conference on Autonomous Agents and Multi-Agent Systems*, Saint Paul, USA, May 2013, pp. 199-206.

[11] A. K. Nandi, H. R. Medal, and S. Vadlamani, "Interdicting attack graphs to protect organizations from cyber attacks: a bi-level defender-attacker model," *Computers & Operations Research*, vol. 75, pp. 118-131, Nov. 2016.

[12] S. Mei, Y. Wang, and L. Chen, "Overviews and prospects of the cyber security of smart grid from the view of complex network theory," *High Voltage Engineering*, vol. 37, no. 3, pp. 672-679, Mar. 2011.

[13] Q. Guo, S. Xin, J. Wang *et al*., "Comprehensive security assessment for a cyber physical energy system: a lesson from Ukraine's blackout," *Automation of Electric Power Systems*, vol. 40, no. 5, pp. 145-147, Mar. 2016.

[14] Z. Li, W. Tong, and X. Jin, "Construction of cyber security defense hierarchy and cyber security testing system of smart grid: thinking and enlightenment for network attack events to national power grid of Ukraine and Israel," *Automation of Electric Power Systems*, vol. 40, no. 8, pp. 147-151, Apr. 2016.

[15] X. Yi and Y. Zhang, "Survivability of information system," in *Proceedings of International Conference on Information, Communications and Signal Processing*, Bangkok, Thailand, Dec. 2005, pp. 1551-1555.

[16] I. Garasym, "Information security system survivability assessment method based on logical-probabilistic models," in *Proceedings of International Conference on the Experience of Designing and Application of CAD Systems in Microelectronics (CADSM)*, Polyana-Svalyava, Ukraine, Feb. 2011, pp. 160-161.

[17] A. K. Srivastava, T. A. Ernster, R. Liu *et al*., "Graph-theoretic algorithms for cyber-physical vulnerability analysis of power grid with incomplete information," *Journal of Modern Power Systems and Clean Energy*, vol. 6, no. 5, pp. 887-899, Sept. 2018.

[18] H. Abie, R. Savola, J. Bigham *et al*., "Self-healing and secure adaptive messaging middleware for business-critical systems," *International Journal on Advances in Security*, vol. 3, no. 1 & 2, 2010.

[19] Z. Bao, "Active defense of security risk in train control system," Ph. D. dissertation, Beijing Jiaotong University, Beijing, China, 2017.

[20] X. Dong, L. Lin, X. Zhang *et al*., "The application of active defense technology in the communication network," *Information Security & Technology*, no. 1, Jan. 2016.

[21] S. Huang, H. Zhang, J. Wang *et al*., "Markov differential game for network defense decision-making method," *IEEE Access*, vol. 6, pp. 39621-39634, Jun. 2018.

[22] L. Zhang, "Research on network information system survivability technology," Ph. D. dissertation, Harbin Engineering University, Harbin, China, 2008.

[23] Power Grid and Power Plant Computer Monitoring System and Dispatching Data Network Security Protection Rules, Order No. 30 of the National Economic and Trade Commission of the People's Republic of China, 2002.

[24] Power Secondary System Security Protection Regulations, State Electricity Regulatory Commission Order No. 5, 2005.

[25] D. Chen, S. Han, M. Munro *et al*., "An analytic model of atomic service for services descriptions," in *Proceedings of International Conference on Service Sciences (ICSS)*, Hangzhou, China, May 2010, pp. 197-202.

[26] P. Wei, M. Yan, Y. Tan *et al*.,"Micro variation Chaos genetic algorithm," in *Proceedings of Chinese Control and Decision Conference (CCDC)*, Shenyang, China, Jun. 2018, pp. 4523-4528.

[27] T. L. Saaty, "How to make a decision: the analytic hierarchy process," *European Journal of Operational Research*, vol. 48, no. 1, pp. 9-26, Jan. 1990.

Yingjun Wu received the B. S. degree from Nanchang University, Nanchang, China, in 2007, the M.S. degree from Southeast University, Nanjing, China, in 2009, and the Ph.D. degree from Politecnico di Torino, Torino, Italy, in 2013, all in electrical engineering. He is currently an Associate Professor with the College of Energy and Electrical Engineering, Hohai University, Nanjing, China. His research interests include active distribution networks and microgrids, power system economics and markets, and electric power cyber-physical systems.

Hao Xu received the B. S. degree in electrical engineering from Nanjing University of Posts and Telecommunications, Nanjing, China, in 2017, where he is currently pursuing the M. S. degree. His research interests include cyber-security in cyber-physical power systems.

Ming Ni received the B. S. and Ph. D. degrees from Southeast University, Nanjing, China, in 1991 and 1996, respectively. He is currently the Chief Expert of Power System Planning and Analysis with the State Grid Electric Power Research Institute, a Researcher Level Senior Engineer with NARI Group Corporation, and an Adjunct Professor with the School of Electrical Engineering, Southeast University, Nanjing, China. His research interests include power system planning, analysis and control, and cyber-physical systems.