IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received July 5, 2020, accepted July 21, 2020, date of publication August 11, 2020, date of current version August 21, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3014785

Risk Assessment of Cyber Attacks on Power Grids Considering the Characteristics of Attack Behaviors

BIYUN CHEN[1], ZHIHAO YANG[1], YIYI ZHANG[1], (Member, IEEE), YANNI CHEN[1], AND JUNHUI ZHAO[2], (Member, IEEE)

[1]Guangxi Key Laboratory of Power System Optimization and Energy Technology, Guangxi University, Nanning 530004, China
[2]Department of Electrical and Computer Engineering, University of New Haven, West Haven, CT 06516, USA

Corresponding authors: Yiyi Zhang (yiyizhang@gxu.edu.cn) and Junhui Zhao (jzhao@newhaven.edu)

This work was supported by the National Natural Science Foundation of China under Grant 51767002.

ABSTRACT The quick development of smart grids coupled with IoT devices has opened breaches of security leading to cyberattacks done by attackers with different purposes. In this study, a behavior model is proposed to investigate the risk of cyber attacks on power grids, where the utility value is determined by subjective attack attitude and characteristics of candidate targets firstly, and then the behaviors of attack target selection and attack resource allocation are described by the probability response and utility attenuation model respectively based on data analysis of historical events. The simulation results on RTS79 system indicate that the risk and the vulnerable nodes of the power grid vary with the characteristics of attack behaviors and characteristic attributes of targets, which should be considered in the cyber security defense dynamically.

INDEX TERMS Attack behaviors, probability response model, risk assessment, utility attenuation model, utility value.

I. INTRODUCTION

With the quick development of Internet of Things and communication technologies, the coverage of intelligent devices allocated in power grids is expanding [1], [2] and the interaction between external and internal parts of the system is booming. Massive terminal interfaces and open protocols opened breaches of cyber security and attracted serious concerns [3]–[5]. Cyberattacks with different purposes and of different classes, such as false data injection [6], [7], GPS spoofing [8], denial-of-service (DoS) [9], attacks against breaks [10], and etc., are one kind of the primary risks of cyber systems. The Ukraine Blackout in Dec 2015 is considered to be a milestone and the first known successful cyberattack on a power grid [11]. The Venezuelan Blackout in Mar 2019 reminds the world again that smart grids are at severely heightened risk of cyberattacks and it is of great significance to take recognition and precaution measures against the risk.

There has been a number of studies on risk assessment for cyberattacks on power systems with different models of implementation process, intention and strategies of cyberattacks. Topological models are most commonly used to simulate the implementation of cyberattack in evaluation of system risk or component vulnerability, such as Bayesian models [10], attack graph [12], tree model [13] and limited stochastic Petri net graph [14]. In order to investigate the attack process in more detail, digital simulation platforms are also employed to construct the interdependencies between cyber and power systems [15], [16] and get some deep insight into transmit mechanism within cyber systems and between cyber and physical systems [17], [18]. Analysis based on topological models or simulation platforms always focus on implementation scheme rather than the decision strategies of the attack and so the intention of the attacker and other subjective factors are generally omitted. Some studies concerning with attack intention employed game theory and multilevel programming to model attack-and-defense competition with optimal strategies, such as Static game for attack probability modeling [19]–[21], Colonel Blotto game and Stackelberg game for optimal attack resource

The associate editor coordinating the review of this manuscript and approving it for publication was Pietro Varilone.

allocation [22], [29], Markov game for dynamic attack modeling [23]–[25], Tri-level programming model for vulnerability assessment and component protection [26]–[28]. However, the factors affecting attack decision making and the diversity of attack intention have not been fully coved in existing studies, primarily due to the difficulty of data acquisition of necessary information for characterizing the attack behaviors in detail.

Nowadays, the development of big data technologies cast a new light on this problem to gain a more precise adjustment of defensive scheme against cyberattacks and construct a more secure power system. In this paper, a behavior model is proposed to investigate the risk of cyberattacks on power grids. Firstly, utility function is built to measure attacker's satisfaction, which is related with subjective attitude and characteristics of the cyber and physical system, and the utility value is used to reflect attackers' behaviors, including attack target selection and attack resource allocation. Secondly, According to the regional characteristic of attacks, the probability response model and utility attenuation model are proposed to analyze the attack target selection behavior based on utility value and data analysis of historical events, then the attack resource allocation behavior are analyzed based on the result of selection, and the probabilities of successful attacks are calculated based on attack-defense efficiency analysis; With the uncertainty of the attack capability and number of attack targets, a risk assessment method considering the characteristics of attack behaviors is presented finally, showing the risk distribution of the system when confronting different attacking behaviors.

II. ATTACK ON CYBER SYSTEM

Supervisory Control and Data Acquisition (SCADA) system is the heart of cyber system in a power grid. As shown in Figure 1, a typical SCADA system consists of control center local area network (LAN), multiple substation LANs and communication links between control center and substations [10].

Hackers may attack any feasible access point of the SCADA system to make impacts on the physical grid [10], including:

1) Attacks on Control Center. Attackers bypass the firewall with advanced intrusion tools and scan the hosts and services of the network. Once obtaining the root privilege of the application server, trip commands can be directly sent to the IEDs or RTUs.

2) Attacks on Substation Networks. Attackers identify IP addresses of substations by port-scanning tool and log on routers by brute-force password attacks. After bypassing the firewall and gaining access to the network of the substation, IP scanning can be deployed for different user interface intrusions to execute unauthorized operations, such as reconfiguring parameters of field devices, manipulating measurement data and GPS time, sending incorrect trip commands to IEDs or RTUs.

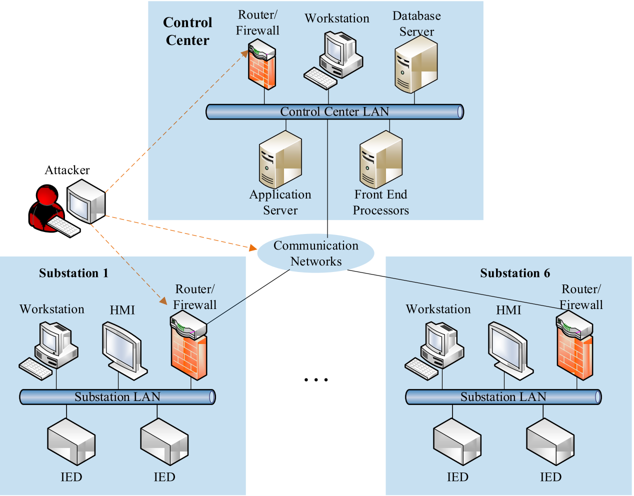


FIGURE 1. A typical cyber architecture of the SCADA system.

3) Attacks on Communication Links Between the Control Center and Substations. By accessing the communication network, attackers eavesdrop messages and analyze traffic to complete attacks. After intercepting and decoding the messages in the communication links, attackers can replace some actual measurement, state or control data and replay the fabricated data into the network [12]. When false measurements and state data are sent to the state estimation module, the control decisions may be misguided and cause incorrect trips or load shedding [10]. Another way to hide events and status of the power grid is to delay/interrupt messages from reaching their intended destination through a DoS attack on communication network [9]. The DoS attack can make the control center fail to predict, perceive, and take prompt actions against sustained or imminent failures, resulting in a significant increase of failure rates and repair times on the power grid.

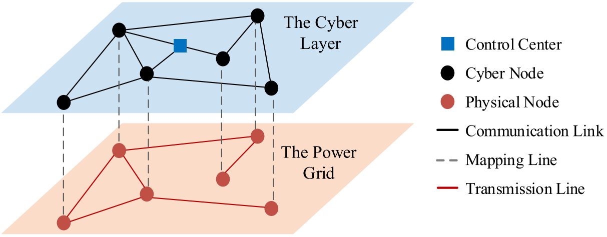


FIGURE 2. Cyber-physical architecture of the CPPS.

To simplify the analysis, a station-level LAN can be expressed as a cyber node. Cyber nodes and control center communicate with each other through the communication network which is usually structured as double-star network and the mesh network [30]. As shown in Figure 2, a physical node in the power grid usually represents a bus in practical, and one cyber node mappings one or more buses to monitor/control the physical components connected to their mapping buses [30]. Thus attacking cyber nodes is an effective way to compromise physical components.

III. ATTACK BEHAVIORS

Cyberattack is a two-phase process, including preparation and implementation. In the preparation phase, attacker selects attack targets to reach his purpose. In implementation phase, attacker invests resources to break through targets and make the attack successful. The attack behavior can be described as the action of selecting $n(1 \leq n \leq T)$ targets from T candidates and investing resources to make attack successful on the selected targets. In this work, cyber nodes are candidate targets, which can be represented by a candidate set $\boldsymbol{E} = \{e_t | t = 1, 2, \ldots, T\}$, where T is the total number of candidates and e_t is the tth candidate, while the control center can be neglected in the following analysis due to its extremely low risk of being broken through directly by cyberattacks [10].

As a behavioral subject with different attitudes, attacker always makes decisions depending on personal satisfaction or preference. Measurement of personal satisfaction or preference is one of the key issues in the study of attack behavior. According to the theory of utilitarianism and decision [31], [32], the criteria for decision among alternatives is based on numerical representation of satisfaction or preference of the decision maker, and utility is a commonly accepted concept to measure the satisfaction or preference. Typically, each alternative is assessed for desirability on a number of scored criteria and utility function is used as a transformation of alternative's performance measured in natural units into an equivalent value of satisfaction or preference of the decision-maker [32]. And then utility value, containing the attacker's subjective attitude, is used to analyze the behavior of target selection and resource allocation on the candidate targets.

A. UTILITY VALUES OF TARGETS

Utility function has been widely used as an effective method in the field of economics, finance, management and artificial intelligence, etc., such as modeling of consumer's preference ordering over a choice set, or investor's satisfaction over different portfolios. In the field of artificial intelligence, different utility functions are used to convey the value of various outcomes to intelligent agents. However, expression of utility function is a complex problem. It can be treated as either cardinal or ordinal, or have a more precise representation through big data analysis.

Since the utility value of each alternative attacking decision is assessed according to multiple scored criteria and subjective attitudes, scoring criteria in this paper, defined as characteristic attribute, can be used to reflect certain performances of the target candidate, and the attacker's attitude toward the characteristic attributes is defined as preference.

1) CHARACTERISTIC ATTRIBUTES

Generally, there are three types of purposes to launch cyberattacks on power grid: Power Destruction, Political Intimidation and Difficulty Aversion [19], [21]. Different purposes make attackers focus on different characteristic attributes of the candidate targets. Attackers measure candidate target's characteristic attributes, including Attack Complexity, Topology Relationship and Influence of Public Opinion, and makes decision in favor of accomplishing his purpose. The above attributes can be divided into two categories according to their role in achieving expected effect: 1) Benefit Attribute, having positive impact on the attack, and being more beneficial with higher value. 2) Cost Attribute, having negative impact on the attack, and being less acceptable with higher value.

i) Attack Complexity, a cost attribute, refers to the degree of difficulty in breaking through the candidate target successfully. Given limited attack resources, the stronger the defense, the harder the attack. From the view of difficulty aversion, Lower difficulty of candidate target is more attractive to the attacker. The attribute value can be quantified as the defensive effect by exponential function [35]:

$$x_t^{\text{diff}} = 1 - e^{\alpha_t s_t^{\text{d}}} \tag{1.1}$$

where e_t is the amount of defense resources allocated on the tth candidate target S_i^{a}, which can be quantized hierarchically [39]–[41] or monetarily [19]. $\alpha_t = -\ln(DF_t)/DC_t$ is the defense conversion coefficient, where DC_t is the defender's elimination cost to reduce vulnerability and increase defensive strength of S_i^{a}, $DF_t \in (0, 1]$ is the defender's elimination fraction, defined as the percentage of availability for elimination cost allocated on S_i^{a}.

ii) Topology Relationship, a beneficial attribute, refers to the closeness of the relationships between one candidate target and the others. Based on the communication network of the cyber nodes, the more the associated nodes, the more critical the candidate. From the view of power destruction, higher topology criticality is more attractive to the attacker. The attribute value can be quantified as the betweenness for the ith node [30]:

$$x_t^{\text{topol}} = \sum_{i}^{T} \sum_{j}^{T} \frac{\sigma_{i,j}(t)}{\sigma_{i,j}} \tag{1.2}$$

where $\sigma_{i,j}(t)$ is the number of shortest paths between nodes i and j through node t and $\sigma_{i,j}$ is the total number of shortest paths between nodes i and j.

iii) Influence of Public Opinion, a beneficial attribute, refers to the influencing degree of power outage or insufficient power supply on politics, economy, and social activities in a specific area due to an attack. From the view of political intimidation, the greater influential, the more attractive. The influence of public opinion can be quantified in terms of the economic or social value of the load loss, which can be determined as the function of load level and social impact coefficient [19]:

$$x_t^{\text{senti}} = \mu_t D_t \tag{1.3}$$

where D_t is the load of the physical node mapping with S_i^{a}, μ_t is the social impact coefficient of S_i^{a}, whose value can reference operation manual [38] shown in TABLE 1.

TABLE 1. μ_t **in different power supply periods.**

	general period	special periods	tertiary period	secondary period	primary period
value	1.0	1.2	1.4	1.6	2.0

Since candidate targets are part of the CPPS, the characteristic attributes can reflect background information of the power system which can be considered as constant in a short-term perspective, while characteristic attribute values can also be open to change in a long-term perspective.

2) ATTACK PREFERENCES

Commonly, those candidate targets with characteristic attributes matching the attacking purpose better will be more preferable to the attacker, which means that the same candidate has different utilities for attackers due to different preferences. Generally, attackers can be divided into three types according to different purposes [19], [21]:

i) Terror attackers. Terror attackers are organizations or individuals who use violent means to disrupt social security and stability, and have obvious destructive intentions and political purposes, who may sometimes carry out political intimidation in a certain area at all costs. As to preferences, Attack Complexity is not the key attribute claiming their attention. They focus more on the Topology Relationship and the Influence of Public Opinion.

ii) Efficient attackers. This type of attackers aims to destroy the power grid but has limited resources and has to aim at the targets being relatively important and having weaker cyber defense to obtain high efficiency with limited resources. As to preferences, efficient attackers focus more on the Topology Relationship and the Attack Complexity. In the efficient attack, the target on important position but with poor or medium defense will be attacked.

iii) Ordinary attackers. There are also such attackers who have poor attack skills and fewer resources. In the ordinary attack, attacker seeks and hack on vulnerabilities of the cyber system without detail information about the physical system. As to preferences, ordinary attackers focus on the Attack Complexity.

When measuring the utility of candidate targets, the characteristic attribute will be transformed value from their natural units into an equivalent value of attacker's satisfaction according to their preference attitudes. If one of the attributes is preferred by the attacker, it will be scored higher, or it will be scored lower. Thus, the attack preferences can be taken as the form of weights for attribute value in the utility measurement.

3) UTILITY VALUE CALCULATION

Since utility is calculated according to multiple attributes, a multi-attribute utility function is needed, which is an extension conception of Utility theory developed to help decision-makers assign utility values, considering their decision-making preferences, and combine the assignments to obtain overall utility measures. There are different multi-attribute utility functions suitable for different decision-making problems, whose axioms and additive independence have been proved in some articles [31]. To construct an effective framework for multi-factor behavior modeling of cyber-attack, an implementable and practical utility function, which have been applied in other research topics and proved to be effective [32], is adopted here as expressed in equation (1.4).

$$u_t = \sum\nolimits_{k=1}^{K} w_k v_{t,k} \tag{1.4}$$

$$v_{t,k} = \begin{cases} \dfrac{x_{t,k} - x_k^{\min}}{x_k^{\max} - x_k^{\min}}, & x_{t,k} \textit{ is Benefit Attribute value} \\ \dfrac{x_k^{\max} - x_{t,k}}{x_k^{\max} - x_k^{\min}}, & x_{t,k} \textit{ is Cost Attribute value} \end{cases} \tag{1.5}$$

where u_t is the utility value of e_t, K is the number of characteristic attributes for each candidate target, w_k is the utility weight, which can be calculated by the Analytic Hierarchy Process, representing the degree of preference for the kth characteristic attribute. $x_{t,k}$ is the quantized value of the kth characteristic attribute for e_t, and $v_{t,k}$ is the normalization value of $x_{t,k}$. $x_k^{\max}$ and $x_k^{\min}$ are the maximum and the minimum values of the kth attribute respectively.

B. SELECTION OF ATTACK TARGETS

Historical cases of cyber-attacks show that, most of the multi-target attacks aim at targets inside some specific area and with relatively close connection between each other, which implies that the targets out of some specific area is less attractive to the attacker. However, even if the attacker aims at some specific zone with preference, the target selection within the zone is still rather uncertain, which means that it cannot be modeled precisely by mechanism methods and the numerical-simulation model based on data analysis of historical events is more preferable. Therefore, considering that attackers select targets according to the utility value and carry out multi-target attacks around some center point of the attack area, the behavior of multi-target selection can be described as the selection of one primary target from the candidate target set $\boldsymbol{E}$ at the first step and the selection of other associated attack targets according to their connection relationships at the second step.

Based on utility value, the Logit model and the utility attenuation model are built to analyze the probability of a candidate being selected as the primary target and the selection of the other targets.

1) LOGIT MODEL AND PROBABILITY RESPONSE

Here, probabilistic model is built for target selection from a strategic viewpoint. Logit model, having a firm theoretical foundation in utility theory, is a common probabilistic model to investigate the decision behaviors of humans [33].

The probability of e_t being selected as a primary attack target can be determined based on the utility value and the Logit model, and is denoted as the response probability.

$$p_t^{\mathrm{R}} = \frac{e^{\lambda u_t}}{\sum_{e_t \in \boldsymbol{E}} e^{\lambda u_t}} \tag{2.1}$$

where $\lambda(\lambda \geq 0)$ is the attacker's response sensitivity to the utility value of candidate target. A high value of λ means a significant inclination of primary attack target selection, where the attacker has radical choice behavior, and is more sensitive to the utility difference between the candidate targets and more inclined to choose the candidate target with higher utility value. A low value of λ means an unclear inclination of primary attack target selection, where attacker chooses the primary attack target with great caution. All candidate targets have the same response probability when λ is zero. Application of Logit model in behavior studies has been investigated in some articles, such as [33], where λ can be obtained by statistical analysis of history data. In this paper, given the utility values of target sets $\boldsymbol{u}$ and historical records of attack targets, where the records are approximate to be independent and have the same response probability, λ can be determined based on Maximum Likelihood Estimation (MLE):

$$\widehat{\lambda} = \arg\max_{\lambda} \ln L(\lambda|\boldsymbol{u}) \tag{2.2}$$

$$L(\lambda|\boldsymbol{u}) = \prod_{j=1}^{N} p_{t_j}^{\mathrm{R}}(\lambda|\boldsymbol{u}) \tag{2.3}$$

$$\ln L(\lambda|\boldsymbol{u}) = \sum_{j=1}^{N} \ln \left[p_{t_j}^{\mathrm{R}}(\lambda|\boldsymbol{u}) \right] \tag{2.4}$$

where $L(\lambda|\boldsymbol{u})$ is the MLE function for λ, N is the number of historical records of the attacker's primary attack target choices, t_j represents the scene that the e_t is chosen as primary attack target in the jth historical record, and $p_{t_j}^{\mathrm{R}}(\lambda|\boldsymbol{u})$ is the probability of e_t being selected as primary attack target in the jth historical record. Let N_t be the number of the cases that e_t was selected as primary attack target. Then we have:

$$\ln L(\lambda|\boldsymbol{u}) = \sum_{t=1}^{T} N_t \ln \left[p_t^{\mathrm{R}}(\lambda|\boldsymbol{u}) \right] \tag{2.5}$$

$$= \sum_{t=1}^{T} N_t \ln \left[\frac{e^{\lambda u_t}}{\sum_{k=1}^{T} e^{\lambda u_k}} \right] \tag{2.6}$$

$$= \lambda \sum_{t=1}^{T} N_t u_t - N \ln \left(\sum_{k=1}^{T} e^{\lambda u_k} \right) \tag{2.7}$$

Information security technologies, such as Security Information and Event Management, Honeypots, Big Data Mining and etc., are under study and have made meaningful progresses in the cyber security area. Based on the wide application of these technologies in the future on cyber attack monitoring, tracing and analyzing, relevant data analysis of historical records can be achieved more easily and more accurately.

2) UTILITY ATTENUATION MODEL

When the primary target is locked, attacker will undergo the second selection process to choose other attack targets mostly according to the associated relationship of candidates, which can be measured by adjacent topology, where the attack range is denoted by topology distance in cyberspace. As the targets out of the range are less attractive to the attacker, the variation of satisfaction with the increase of distance from primary target is described as a decrease of utility attenuation of the candidate. In other word, the utility value of each candidate changes with its adjacent topology relationship and its topology distance to the primary target.

When the bth candidate target is chosen as the primary attack target, denoted as e_b, the utility value of e_t changes from u_t to $u_{b,t}$. To make it easy to distinguish, we name u_t the former utility value of e_t, and name $u_{b,t}$ the post utility value of e_t on e_b.

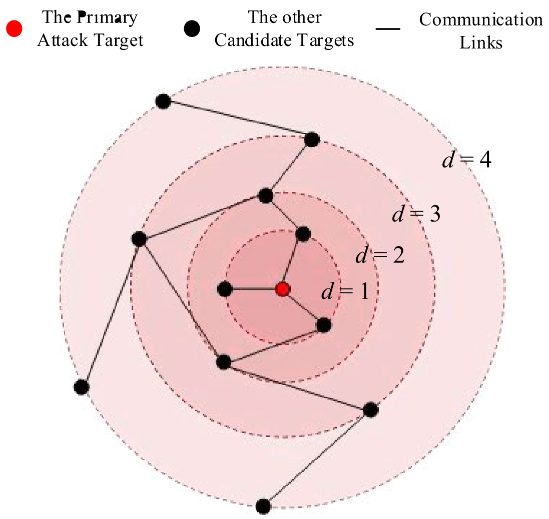


FIGURE 3. Schematic diagram of topological distance.

Figure 3 shows an example of topology relationship of candidate targets (i.e. cyber nodes), where the topology connection between two targets is a communication link between cyber nodes. The farther from the primary target, the less attractive to the attacker. Defined the topology distance $d_{b,t}$ (from e_b to e_t) as the number of links contained in the shortest topology path from e_b to e_t, the utility value $u_{b,t}$ is calculated as

$$u_{b,t} = \varepsilon_{b,t} u_t \tag{3.1}$$

$$\varepsilon_{b,t} = e^{-d_{b,t}} \tag{3.2}$$

where $\varepsilon_{b,t}$ is the distance attenuation coefficient. Obviously, when b is equal to t, $d_{b,t}$ is 0 and $\varepsilon_{b,t}$ is 1, the utility value of the primary target doesn't change in the second selection process. Although, there may be some other factors having influence on the second target selection process, here are the considerations for taking topology relationship as the major factor: 1) Since numerical model based on data analysis of historical events is more preferable for target selection simulation, the model with single parameter, number of communication links due to adjacent topology relationship, can be easily obtained from statistics of historical attacks; 2) The number, rather than the length, of communication link is considered due to the distance in cyberspace is different from that in the physical space, attackers can implement remote attack without geographical restrictions, and consequently without significant difference in the cost, attackers care more about whether there is a cyber path to the target than the cost due to the distance; 3) the simplified representation can also reflect the characteristic that attacker aims at targets inside specific area, and pays less attention to those targets far away from the primary one.

When attackers attempt to choose $n(1 \leq n \leq T)$ targets from T candidates, once the primary target e_b is decided, the other $T-1$ candidates will be re-ranked in order of their $u_{b,t}$ and the top $n-1$ ones will be selected out.

C. NUMBER OF ATTACK TARGETS

The number of attack targets is limited by attack capabilities, generally measured by attack resources [20]–[22], including personnel or hackers assigned to the attack and technological resources, such as advanced tools or malwares [22], [24]. Since the total amount of resources S^{a} is usually random in natural, the number of attack targets n is also a random variable associated with S^{a}. The probability distributions of n and S^{a} can be obtained by historical event analysis and statistics. Considering n with an uneven probability distribution, the probability of n targets within $\boldsymbol{E}$ being selected can be simulated based on Poisson distribution model.

$$p_n^{\mathrm{N}} = \frac{\xi^n}{n!}e^{-\xi}, \quad n = 1, 2, \ldots, n_{\max} \tag{4.1}$$

$$\xi = \frac{S^{\mathrm{a}}}{S^{\mathrm{base}}} \tag{4.2}$$

where ξ is equal to the expected value of n and also to its variance, S^{base} is the basic amount of attack resources required to attack a target successfully, $n_{\max}(1 \leq n_{\max} \leq T)$ is the maximum expected number of attack targets. S^{base} and $n_{\max}$ can be obtained by post evaluation.

Suppose that S^{a} obeys Normal distribution $N(\mu, \sigma^2)$, where μ and σ are parameters related to the characteristics of attackers and μ represents the average amount of attack resources to perform a task. The empirical rule of Normal distribution shows that 99% of the data will be distributed within interval $[\mu - 3\sigma, \mu + 3\sigma]$. In order to concentrate on the modeling process and simplify the analysis, as shown in TABLE 2, an extended interval $[\mu - 3.5\sigma, \mu + 3.5\sigma]$ is discretized into seven subintervals, each of which is represented by a median value, as $\mu - 3\sigma$, $\mu - 2\sigma$, $\mu - \sigma$, μ, $\mu + \sigma$, $\mu + 2\sigma$, $\mu + 3\sigma$, respectively. The ith possible value of resource amount is denoted as S_i^{a}, and its probability is p_i^{A}.

TABLE 2. The seven discretization representative values and corresponding probabilities for S^{a}.

Number	Representative value for S^{a}	Value interval and probability
1	$S_1^{\mathrm{a}} = \mu - 3\sigma$	$p_1^{\mathrm{A}} = P(\mu - 3.5\sigma \leq S^{\mathrm{a}} \leq \mu - 2.5\sigma)$
2	$S_2^{\mathrm{a}} = \mu - 2\sigma$	$p_2^{\mathrm{A}} = P(\mu - 2.5\sigma \leq S^{\mathrm{a}} \leq \mu - 1.5\sigma)$
3	$S_3^{\mathrm{a}} = \mu - \sigma$	$p_3^{\mathrm{A}} = P(\mu - 1.5\sigma \leq S^{\mathrm{a}} \leq \mu - 0.5\sigma)$
4	$S_4^{\mathrm{a}} = \mu$	$p_4^{\mathrm{A}} = P(\mu - 0.5\sigma \leq S^{\mathrm{a}} \leq \mu + 0.5\sigma)$
5	$S_5^{\mathrm{a}} = \mu + \sigma$	$p_5^{\mathrm{A}} = P(\mu + 0.5\sigma \leq S^{\mathrm{a}} \leq \mu + 1.5\sigma)$
6	$S_6^{\mathrm{a}} = \mu + 2\sigma$	$p_6^{\mathrm{A}} = P(\mu + 1.5\sigma \leq S^{\mathrm{a}} \leq \mu + 2.5\sigma)$
7	$S_7^{\mathrm{a}} = \mu + 3\sigma$	$p_7^{\mathrm{A}} = P(\mu + 2.5\sigma \leq S^{\mathrm{a}} \leq \mu + 3.5\sigma)$

D. RESOURCE ALLOCATION AND PROBABILITY OF SUCCESSFUL ATTACK

When a candidate target is selected, attacker will allocate resources to ensure success. Meanwhile, defender will launch defense resources against the attack, such as security personnel, firewall, encryption device, antivirus software and intrusion detection system and so on. From the viewpoint of attack-defense competition, the success probability of an attack is decided by the competition between the attacker and the defender, so the resources invested in the competition by the two adversaries can be used to model the success probability [34], [35]. Consequently, when the tth candidate e_t is selected as an attack target, the success probability of this attack can be calculated based on an exponential function [34], [35]:

$$p_t^{\mathrm{S}} = p_t^{\mathrm{a}}(1 - p_t^{\mathrm{d}}) \tag{5.1}$$

$$p_t^{\mathrm{a}} = 1 - e^{-\beta_t s_t^{\mathrm{a}}} \tag{5.2}$$

$$p_t^{\mathrm{d}} = 1 - e^{-\alpha_t s_t^{\mathrm{d}}} \tag{5.3}$$

where p_t^{S} is the success probability of attack on e_t, s_t^{a} is the amount of attack resources allocated on e_t, s_t^{d} is the amount of defense resources allocated on e_t, p_t^{a} and p_t^{d} are the attack efficiency and the defense efficiency of attack on e_t respectively, β_t and α_t are the attack conversion coefficient and the defense conversion coefficient, respectively. β_t can be calculated as $\beta_t = -\ln(1 - AF_t)/AC_t$ [35], where AC_t is the minimum attack resources to increase the probability of destruction of e_t, $AF_t \in (0, 1]$ is the fraction of attack resources assigned on e_t to AC_t.

Considering that attackers allocate resources according to utility value $u_{b,t}$, when primary target $e_b$is locked, s_t^{a} is calculated as

$$s_t^{\mathrm{a}} = \frac{S^{\mathrm{a}} e^{\lambda u_{b,t}}}{\sum_{e_t \in \boldsymbol{E}^{\mathrm{a}}} e^{\lambda u_{b,t}}} \tag{6}$$

where $\boldsymbol{E}^{\mathrm{a}}$ is the set of attack targets. Since attack targets are determined by attack capability and attack preference, the attack resources allocation and the success probability alters in different scenarios.

IV. RISK ASSESSMENT MODEL

A. SCENARIO PROBABILITY

Due to the uncertainty of attack resources and target selection, there may be multiple attack scenarios. Given an attack scenario $Q_{t,i,n}$ with selected primary target e_t, total attack target number n, and attack resources S_i^{a}, the occurrence probability of $Q_{t,i,n}$ is calculated as

$$p_{t,i,n}^{\mathrm{Q}} = p_t^{\mathrm{R}} p_i^{\mathrm{A}} p_n^{\mathrm{N}} \tag{7}$$

There is attack target set $\boldsymbol{E}_{t,i,n}^{\mathrm{a}}$ for $Q_{t,i,n}$. Obviously, whether an attack on a target succeeds or not has uncertainty, so are the schemes to be successful. It is assumed that there are M independent successful attack schemes for $Q_{t,i,n}$, and the mth ($m = 1, 2, \ldots, M$) successful scheme is denoted by $Z_{t,i,n,m}$, the set including targets attacked successfully in $Z_{t,i,n,m}$ is $\boldsymbol{E}_{t,i,n,m}^{\mathrm{a}}(\boldsymbol{E}_{t,i,n,m}^{\mathrm{a}} \subset \boldsymbol{E}_{t,i,n}^{\mathrm{a}})$. The occurrence probability of $Z_{t,i,n,m}$ is

$$p_{t,i,n,m}^{\mathrm{Z}} = \prod\nolimits_{e_t \in \boldsymbol{E}_{t,i,n,m}^{\mathrm{a}}} p_t^{\mathrm{S}} \prod\nolimits_{e_t \in \boldsymbol{E}_{t,i,n}^{\mathrm{a}}, e_t \notin \boldsymbol{E}_{t,i,n,m}^{\mathrm{a}}} (1 - p_t^{\mathrm{S}}) \tag{8}$$

B. ATTACK CONSEQUENCE

Once a target is accessible, attacker will carry out his implementation plan by one or more technical methods, such as sending incorrect tripping commands, injecting false data, delaying or interrupting the transmittal messages and so on. The resulting consequences of cyberattacks on power system can be analyzed by simulation modeling of power system, where Optimal Power Flow model is widely adopted and the consequences can be quantified by the sum of the load loss L^{direct} directly caused by attacks and the load shedding L^{shed} caused by operation constraints of the power grid [36].

$$L = L^{\mathrm{direct}} + L^{\mathrm{shed}} \tag{9.1}$$

where L^{shed} can be calculated by the optimal load shedding model as follow.

$$L^{\mathrm{shed}} = \min \sum\nolimits_{i=1}^{N_{\mathrm{b}}} P_{\mathrm{C},i} \tag{9.2}$$

$$\text{s.t. } \boldsymbol{P}_{\mathrm{L}} = \boldsymbol{B}_{\mathrm{L}} \boldsymbol{A} \boldsymbol{B}^{-1} (\boldsymbol{P}_{\mathrm{G}} - \boldsymbol{P}_{\mathrm{D}} + \boldsymbol{P}_{\mathrm{C}}) \tag{9.3}$$

$$\sum\nolimits_{k=1}^{N_{\mathrm{b}}} P_{\mathrm{G},k} = \sum\nolimits_{i=1}^{N_{\mathrm{b}}} (P_{\mathrm{D},i} - P_{\mathrm{C},i}) \tag{9.4}$$

$$-\bar{P}_{\mathrm{L},j} \leq P_{\mathrm{L},j} \leq \bar{P}_{\mathrm{L},j} \tag{9.5}$$

$$P_{\mathrm{G},k} \leq P_{\mathrm{G},k} \leq \bar{P}_{\mathrm{G},k} \tag{9.6}$$

$$0 \leq P_{\mathrm{C},i} \leq P_{\mathrm{D},i} \tag{9.7}$$

where N_{b} is the bus number of power grid, $\boldsymbol{P}_{\mathrm{L}}$ is the power flow vector of transmission lines, $\boldsymbol{P}_{\mathrm{G}}$ is the vector of active power injections to the buses, $\boldsymbol{P}_{\mathrm{D}}$ is the vector of load demands at buses, $\boldsymbol{P}_{\mathrm{C}}$ is the vector of load shedding at buses, $\boldsymbol{B}_{\mathrm{L}}$ is diagonal matrix of the admittance of transmission lines, $\boldsymbol{A}$ is the incidence matrix, $\boldsymbol{B}$ is the admittance matrix. Equation (9.2) is the objective function. Equation (9.3) and (9.4) are DC model of power flow equation. The capacity limits of transmission lines and generators are given in constraint (9.5) and (9.6), respectively. Constraint (9.7) guarantees that the load shedding is less than or equal to load demand.

C. DEFINITION OF RISK INDEX

In risk assessment, risk index of a scenario is usually expressed as the product of probability and consequence of the scenario and risk of a system is the sum of the risks of all scenarios. Given the probabilities of attack behaviors and related consequences, the risk of attack scenario $Q_{t,i,n}$ is calculated as

$$r_{t,i,n} = \sum\nolimits_{m=1}^{M_{t,i,n}} p_{t,i,n,m}^{\mathrm{Z}} L_{t,i,n,m} \tag{10}$$

where $L_{t,i,n,m}$ is the consequence of $Z_{t,i,n,m}$. Discretizing the attack resources into 7 levels and scoring them, assuming a maximum number of attack targets $n_{\max}$, the risk of the tth target scenario with primary attack target e_t can be calculated as

$$R_t = \sum\nolimits_{i=1}^{7} \sum\nolimits_{n=1}^{n_{\max}} p_{t,i,n}^{\mathrm{Q}} r_{t,i,n} \tag{11}$$

The total risk of one type of attack behaviors on the power grid is accumulated.

$$R = \sum\nolimits_{t=1}^{T} R_t \tag{12}$$

D. RISK ASSESSMENT PROCESS

The Non-sequential Monte Carlo method is used here to generate attack scenarios, and the risk assessment process is shown in Figure 4. The main steps are described as follows:

1) Input parameters including the set of candidate targets, values of characteristic attribute, and grid parameters, etc. Let $i = 1, n = 1, t = 1$.

2) Let e_t be the primary attack target and calculate p_t^{R}.

3) Obtain S_i^{a} and calculate p_i^{A}.

4) Obtain n attack targets to constitute $\boldsymbol{E}^{\mathrm{a}}$ and calculate p_n^{N}.

5) Calculate the success probability of each target within $\boldsymbol{E}^{\mathrm{a}}$.

6) Select a successful scheme randomly based on the Non-sequential Monte Carlo simulation.

7) Calculate the consequence of the successful scheme by the optimal load shedding model and update $r_{t,i,n}$.

8) If the stopping criterion of $r_{t,i,n}$ is satisfied, go to step 9); otherwise, return to step 6).

9) Update R_t according to formula (11).

10) Let $n = n + 1$, if n is greater than $n_{\max}$, go to step 11); otherwise, return to step 4).

11) Let $i = i + 1$, if i is greater than 7, go to step 12); otherwise, Let $n = 1$ and return to step 3).

12) Update R according to formula (12).

13) Let $t = t + 1$, if t is greater than T, go to step 14); otherwise, Let $n = 1$, $i = 1$ and return to step 2).

14) Output risk assessment results.

E. VULNERABILITY CALCULATION

After evaluating the influence of a certain kind of attackers on the power grid, we take kinds of attackers into account and the vulnerability evaluation is one of the key methods to identify which candidate targets are more easy-access. In formulas (13.1)-(13.3), the vulnerability of target e_t is

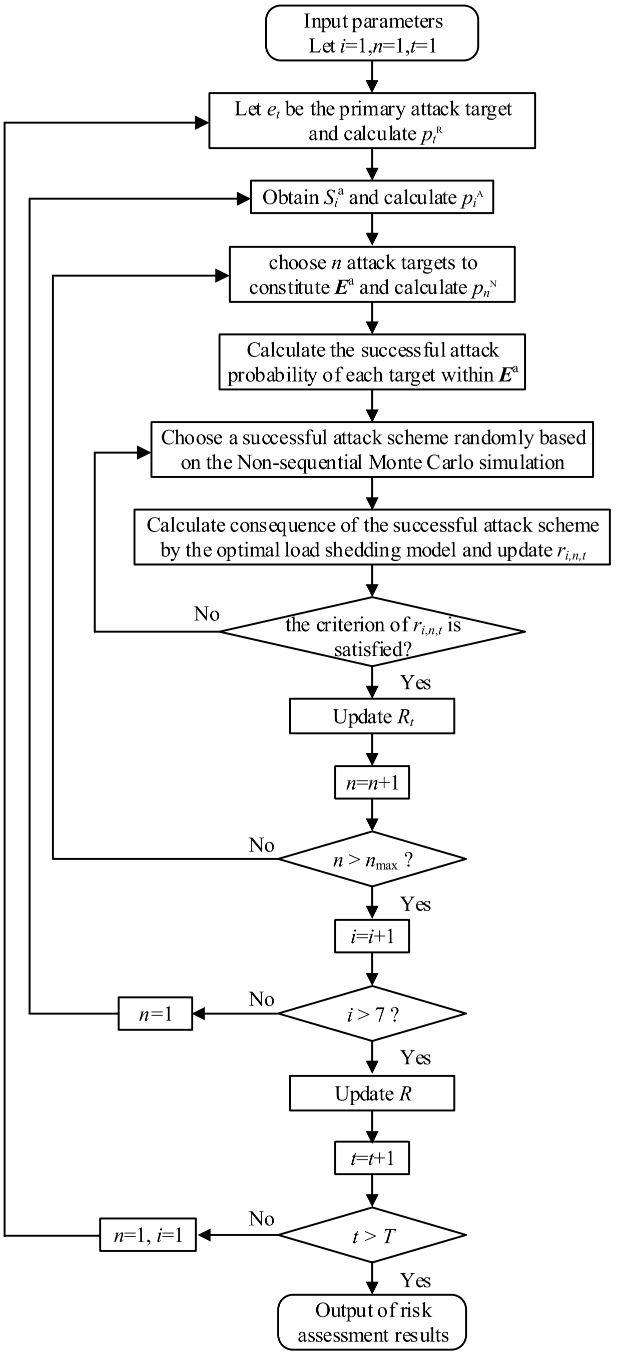

Input parameters
Let i=1,n=1,t=1
Let e_t be the primary attack target and calculate p_t^R
Obtain S_i^a and calculate p_i^A
choose n attack targets to constitute E^a and calculate p_n^N
Calculate the successful attack probability of each target within E^a
Choose a successful attack scheme randomly based on the Non-sequential Monte Carlo simulation
Calculate consequence of the successful attack scheme by the optimal load shedding model and update $r_{i,n,t}$
the criterion of $r_{i,n,t}$ is satisfied?
No
Yes
Update R_t
n=n+1
$n > n_{max}$?
No
Yes
i=i+1
$i > 7$?
No
n=1
Yes
Update R
t=t+1
$t > T$
No
n=1, i=1
Yes
Output of risk assessment results

FIGURE 4. Risk assessment process.

defined as the expected success probability of all the attacks on the target.

$$V_t = \frac{1}{N_S}\sum\nolimits_{i=1}^{N_S} P^S_{t,i} \tag{13.1}$$

$$P^S_{t,i} = \begin{cases} 0, & I_{t,i} = 0 \\ \left(1 - e^{-\beta_t s^a_{t,i}}\right)\left(e^{-\alpha_t s^a_t}\right), & I_{t,i} = 1 \end{cases} \tag{13.2}$$

$$s^a_{t,i} = \sum\nolimits_{b=1}^{B} s^a_{t,i,b} \tag{13.3}$$

where N_S is the number of attack scenarios on e_t, B is the number of attackers, $I_{t,i}$ is a binary variable. When the tth candidate target is selected in the ith scenario, $I_{t,i}$ is 1, otherwise $I_{t,i}$ is 0. $s^a_{t,i,b}$ is the attack resource that the bth attacker allocate to the tth candidate target in the ith scenario. Non-sequential Monte Carlo method is also applied here to generate attack scenarios and the main steps of vulnerability index calculation are as follows:

1) Sampling the attackers for one scenario based on the probability of different types of attackers.

2) Sampling attack resources based on the Normal distribution of attack resources in one task.

3) Sampling number of attack targets based on the Poisson distribution of target number in one task.

4) Sampling primary attack target based on response probability.

5) Determining other targets based on the second target selection model.

6) Determining attack resources allocation.

7) Calculating success probability of attacks on each target according formulas (13.1)-(13.3).

8) Repeating step 1)-7) until satisfying terminating criterion.

It should be noted that one simulated scenario is generated after executing step 1) – 6), and the probability distribution of each type of attackers can be acknowledged from historical statistics.

The risk of cyberattack on the certain cyber node depends both on its vulnerability and on the consequence once it is intruded, which is expressed as

$$W_t = V_t L_t \tag{14}$$

where L_t is the consequence when the tth candidate target is intruded successfully. The CPPS has weak resilience on the tth candidate target when W_t has high value.

V. NUMERICAL SIMULATIONS

Numerical simulations are carried out to show the analyzing results by the proposed methods and show the influences on risk by different characteristics attack behaviors. Generally, it is not easy for attackers to make actual damage on physical system by injecting false measurement data or interrupting transmittal messages depends on limited knowledge of the operation parameters and operation status of the power grid, while sending incorrect control commands to trip physical components can damage the power grid directly. So it is assumed that once an attack on certain cyber node succeeds, the correlated physical components (such as transformers, generators and transmission lines) connected to its mapping bus would be tripped by incorrect commands [10].

Simulations are carried out on the IEEE RTS79 system [37] with an 18-node mesh cyber network [17], [30] as shown in Figure 5. There are 18 candidate targets and it is assumed that the maximum number of attack targets in one attack is three i.e. $n_{\max} = 3$. Besides, we refer to the behavior characteristics of the three types of attackers in practice and

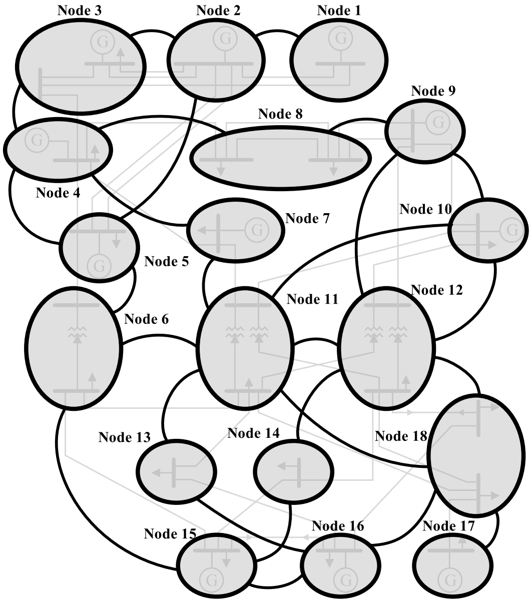


FIGURE 5. IEEE-RTS79 system with cyber topology.

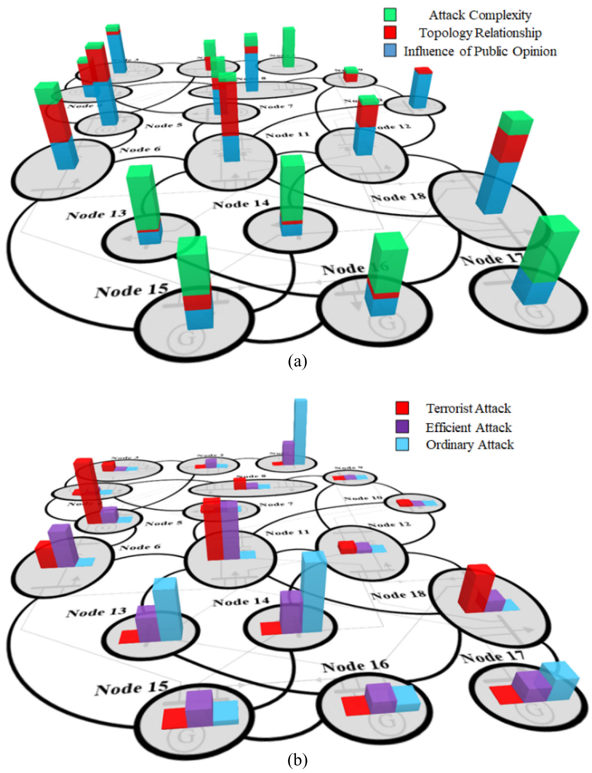
use analytic hierarchy process to obtain their corresponding utility weight parameters as shown in TABLE 3 which will be used to show how different attack behaviors influence the risk and vulnerability assessment.

TABLE 3. Utility weights of different types of attackers.

Type of Attackers	w for the Attack Complexity	w for the Topology Relationship	w for the Influence of Public Opinion
Terror Attacker	0.0588	0.4706	0.4706
Efficient Attacker	0.4706	0.4706	0.0588
Ordinary Attacker	0.8824	0.0588	0.0588

A. RESPONSE PROBABILITY AND SCENARIO RISK

Assume that S^{base} is 40, μ is 5, σ is 1, and λ is 10, all of which are unit values, the normalization values of characteristic attributes and the response probabilities of candidate targets being selected as the primary attack target by different types of attacks are shown in Figure 6, where e_1, e_{13}, e_{14}, e_{17} have weaker defense and lower attack complexity while e_{10} has the highest attack complexity. e_{11}, e_6, e_5, e_4, e_{12} are in critical topology position and e_3, e_5, e_8, e_{10}, e_{18} have great public opinion influence. Since different types of attackers have different preferences for target attributes, the utility value of the same candidate target varies under different attacks, so does the response probability. Figure 7 depicts the risk of scenario with different cyber nodes selected as the primary attack target under different types of attacks.



(a)

(b)

FIGURE 6. Behavioral response to targets' characteristic attributes. (a) normalization values of characteristic attributes; (b) response probabilities of the primary attack targets for three types of attacks.

As shown in Figure 6, terror attackers focus more on the topology relationship attribute and influence of public opinion attribute, and tend to choose target in critical topology position or having great public opinion influence as the primary attack target, such as e_5, e_{11} and e_{18}, the response probabilities of which are higher than the other targets. Usually, these targets have significant impact on load supplying too. So it can be seen from Figure 7 (a) that, when these targets mentioned above are chosen as primary target, the risks are higher.

As to efficient attacks, attackers focus more on the attack complexity and the topology relationship of candidate targets, and incline to launch attacks on targets with low attack complexity or in critical topology position, such as e_{11} (in the most critical topology position) and e_1 (with the lowest attack complexity). Although efficient attacks will not cause extreme serious risk scenarios like terror attacks in general, they have higher success rate in some cases. Comparing (a) and (b) in Figure 7, this risk distribution for efficient attacks are more even and affected area is wider.

As to ordinary attacks, attackers pay less attention to the topology relationship and influence of public opinion of candidates, but tend to select targets with low attack complexity. Since the attack complexities of e_1, e_{13}, e_{14} are far lower than the other targets, as shown in Figure 6, where e_1 is the one with lowest attack complexity and the highest response probability, ordinary attackers will more likely to

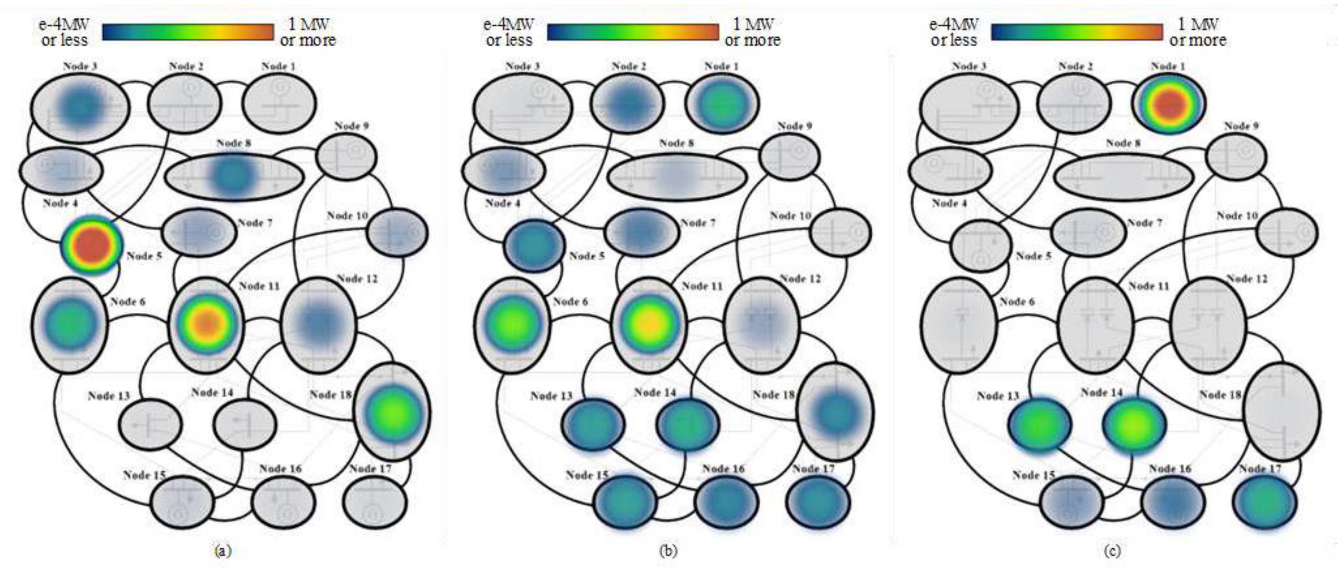


FIGURE 7. Risk of target scenario under different types of attacks. (a) terror attacks; (b) efficient attacks; (c) ordinary attacks.

launch attacks on these targets with weaker defense and cause higher risk on them as observed in Figure 7 (c).

B. SYSTEM RISK

Assuming that $\mu \in [6, 12]$, $\lambda \in [20, 80]$, comparison of system risks caused by different types of attackers with different attack resources, response sensitivities is depicted in Figure 8, and given characteristic attribute values in Figure 6 are. It is found that, in either case, risk index increases with attack resources, and risk of terror attack or efficient attack is much higher than that of ordinary attacks. The reason is that terror attackers tend to launch attacks on targets in critical topology position or with great public opinion influence, and efficient attackers favor to allocate attack resources more effectively, while weak-defense targets that ordinary attackers mostly concern are comparatively of less importance in the system.

It can be also observed that, the risk of terror attack or ordinary attack seems unchanged with λ, while the risk of efficient attack increases with λ less than 60, and holds constant with λ greater than 60. This is because of the higher value of λ implying the higher likelihood of allocating attack resources to the targets with high utility values. Due to the marginal effect of attack resource, unit resource will bring fewer attack efficiency on target when the amount of attack resource assigned to the target increases continuously, which results in a convergence value of the probability of successful attacks.

The targets e_5, e_{11} and e_{18}, in more critical topology position and having greater public opinion influence have high utilities to terror attackers; targets e_1, e_{13} and e_{14}, with lower attack complexity have high utilities to ordinary attackers, the amount of attack resource assigned to these targets increase significantly with λ, while the scenario probability and scenario risk will not vary obviously due to the marginal effect on attack resource. However, there are not great differences between the targets' utilities during efficient attacks, and attack resources are not concentrated on several targets so the marginal effect of attack resource is not obviously. Thus, when the amount of attack resource assigned to preferable targets increase significantly with λ, the scenario probability and scenario risk will increase vary obviously during efficient attacks.

C. VULNERABILITY OF TARGET

Assuming that S^{base} is 40, μ is 5, σ is 1, $\lambda = 10$, and probability of each type of attack is 0.05, all of which are unit values, the target vulnerabilities for different types of attacks are shown in Figure 9. The vulnerable point distributions are totally different for different attack behaviors. Overall, the candidate target with weaker defense (such as e_1, e_{13}, e_{14}) is vulnerable, but targets with stronger defense may be more vulnerable than those with weaker defense in certain attack scenario, such as e_1 and e_5 in terror attack scenario, for it mostly depends on attack preferences.

Moreover, targets' characteristic attribute values as part of the utility definition also have influence on vulnerability index. For example, if Public Opinion attribute and Attack Complexity attribute of e_5 decrease while those of e_{13} and e_{14} increase due to social or economic activity or defensive system rearrangement, named as comparative case in Figure 9, terror attackers will shift their attention from e_5 to e_{13} and e_{14}, while efficient attackers will focus on e_5 instead, and ordinary attackers will pay more attention to e_1 due to the decrease of defensive weakness of other candidates. As a result, e_{13} and e_{14} are vulnerable for terror attacks but relatively reliable for efficient attacks and

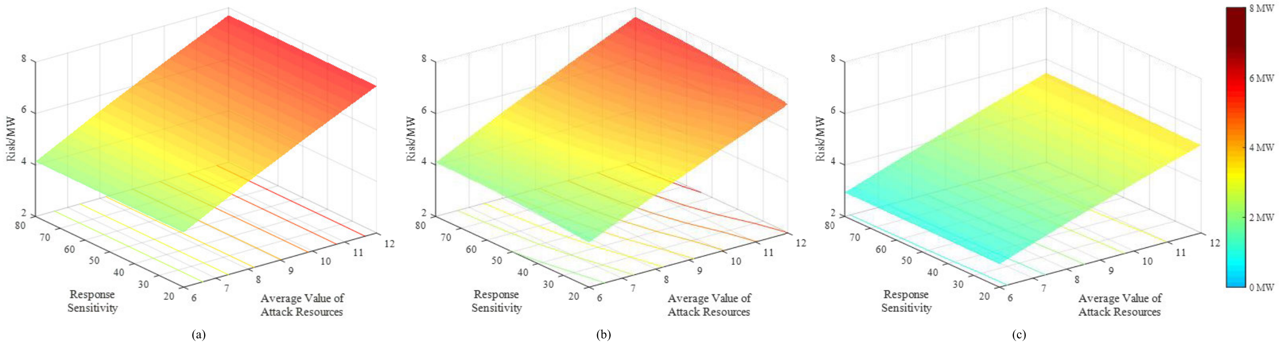


FIGURE 8. Risk of power system under different types of attacks. (a) terror attacks; (b) efficient attacks; (c) ordinary attacks.

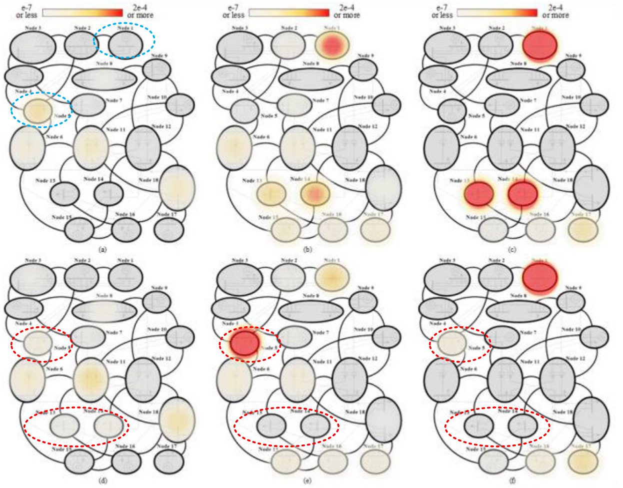


FIGURE 9. Vulnerability distribution for different types of attacks. (a) terror attack; (b) efficient attack; (c) ordinary attack; (d) terror attack for comparative case; (e) efficient attack for comparative case; (f) ordinary attack for comparative case.

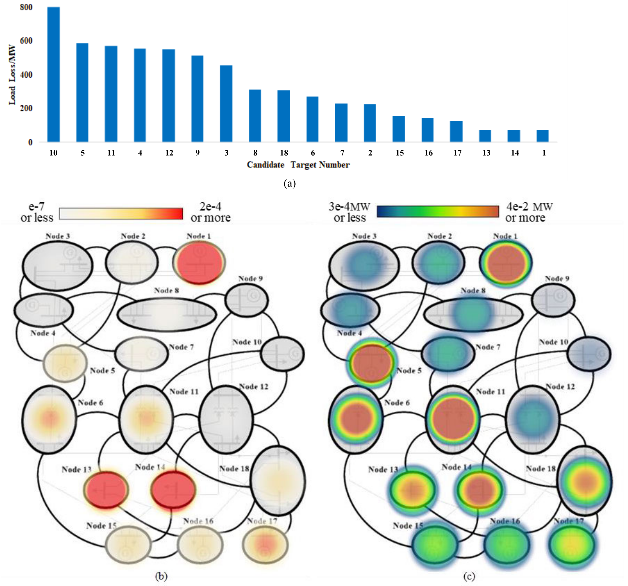


FIGURE 10. Vulnerability and risk distribution considering combined effects of different attack behaviors. (a) consequence ranking; (b vulnerability distribution; (c) risk distribution.

ordinary attacks, while e_5 becomes more vulnerable when encountering efficient attacks.

In general, comparing the three types of attacks, terror attacks have the least probability but the highest resources; while ordinary attacks have the least resources but the highest probability. To observe the combined effects of different attack behaviors, Figure 10 depicts the comparison of consequence, vulnerability and risk of different candidate targets superposing all kinds of attacks. Assume that λ is 10, the probabilities of terror attacks, efficient attacks and ordinary attacks are 0.02, 0.04, 0.05, and the average amounts of attack resources per unit are 12, 9 and 5, respectively, It can be seen that, e_1, e_{14}, and e_{13} with rather high vulnerability are the major weaknesses of the system. Compared the vulnerability distribution for combined attacks with those for single type of attacks in Figure 9 (a) (b) (c), the ordinary attacks and efficient attacks obviously play the decisive role. The consequence of primary attacks on e_{10} is the most serious, then e_5 and e_{11}, however, cyberattacks on e_5, e_{11} have higher risk to the system than that on e_{10} since the vulnerability of the former two points are much higher than that of the latter. Similarly, attacks on e_1, e_{14} with lower consequence have higher risk to the system due to their high vulnerability. These points mentioned above deserve special attention to take precautions against the risk.

D. MODEL COMPARISON

To further illustrate the significance of considering attack behaviors on the risk and vulnerability assessment, we benchmark our model against the model without distinction of attack behaviors proposed in [29].

Given the total amount of attack resources as 5 units and $n_{\max} = 3$, the resource allocation scheme of [29] determined by optimal attack strategies is shown in TABLE 4.

Assume that λ is 10, the probabilities of terror attacks, efficient attacks and ordinary attacks are 0.02, 0.04, 0.05, and the total amounts of attack resources are 5 for each attacker,

TABLE 4. The resource allocation scheme of [29].

Number of Attack Targets	Attack Target	Resource
1	e_{18}	5.0000
2	e_7, e_8	2.5002,24998
3	e_7, e_8, e_{17}	1.7537,1.6429,1.6033

calculate the risk considering combined effects of different attack behaviors. On the other hand, replace the all three types of attack behaviors above with behavior proposed in [29], and calculate the risk index without distinction of attack behaviors for comparison under the same calculation conditions. The comparison of risk indices based on the above two models is shown in TABLE 5.

TABLE 5. Comparison of risk indices based on different models.

Ref. [29]	Considering Combined Effects of Different Attack Behaviors
0.4198MW	0.3157MW

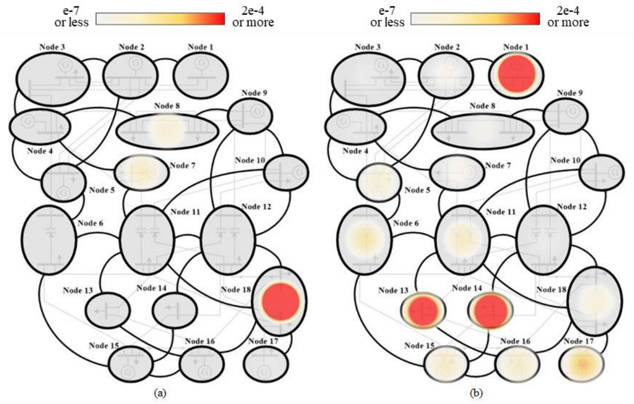


FIGURE 11. Vulnerability distribution (a) based on model without distinction of attack behaviors; (b) considering combined effects of different attack behaviors.

As shown in TABLE 5, the risk based on our model is lower than the one based on the model in [29]. This is because different behaviors rather than the only optimal attack behaviors are considered in our model. Comparing (a) and (b) in Figure 11, e_7, e_8, e_{17}, e_{18} are the weaknesses according to the optimal attack behaviors in [29] while there are more other weaknesses under different behaviors in (b). The optimal attack behaviors are always considered to evaluate the risk in the worst-case scenario, but it cannot recognize the varied vulnerabilities under different attack behaviors. In fact, it is hard for attackers to obtain enough expertise and information of the power system to implement the optimal attack strategy. Attackers are most likely to carry out attack according to their preferences and available characteristic attributes of the system, which make the weakness vary. Thus, considering characteristic and diversity of attack behavior is significant for risk and vulnerability assessment.

VI. CONCLUSION

In this paper, a behavior model is proposed to investigate the risk of cyberattacks on power grids, where the utility value and utility attenuation model are adopted to describe different subjective attack attitudes and characteristics of candidate targets. Simulation results based on IEEE RTS79 system illustrate that: a) The risk of being invaded through specific cyber node is totally different when suffering different kinds of attackers, which means that the weak points of the cyber-physical power system will change with the time since different type of attack behaviors surges obviously during different periods, and this will help to identify the vulnerability of the system more precisely and coordinate defense measurements more effectively. b) The parameters of behavior modeling have certain impact on the evaluated risk indices of the system. The parameters are supported by big data analysis on cyber-attack monitoring, tracing and analyzing, which is now deeply concerned and making continuous progresses in the cyber security area. However, due to the constraint of practical data source, the model adopted here may not be a precise one but just an implementable one with lower precise. With the development and industrial application of big data technology, more accurate models can be constructed in the future work and get better results in the risk assessment of cyberattacks. Besides, coordinated cyber-attacks and complicated physical failure modes, such as cascading outages, have not been considered in this work, which need to be further studied in the future.

REFERENCES

[1] H. Chen, X. Wang, Z. Li, W. Chen, and Y. Cai, "Distributed sensing and cooperative estimation/detection of ubiquitous power Internet of Things," *Protection Control Mod. Power Syst.*, vol. 4, no. 1, pp. 151–158, Jun. 2019.

[2] B. Appasani and D. K. Mohanta, "A review on synchrophasor communication system: Communication technologies, standards and applications," *Protection Control Mod. Power Syst.*, vol. 3, no. 1, pp. 383–399, Dec. 2018.

[3] M. Cui, J. Wang, and B. Chen, "Flexible machine learning-based cyberattack detection using spatiotemporal patterns for distribution systems," *IEEE Trans. Smart Grid*, vol. 11, no. 2, pp. 1805–1808, Mar. 2020.

[4] S. Xin, Q. Guo, H. Sun, B. Zhang, J. Wang, and C. Chen, "Cyber-physical modeling and cyber-contingency assessment of hierarchical control systems," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2375–2385, Sep. 2015.

[5] Y. Zhang, Q. Chen, B. Chen, J. Liu, H. Zheng, H. Yao, and C. Zhang, "Identifying hotspots of sectors and supply chain paths for electricity conservation in China," *J. Cleaner Prod.*, vol. 251, Apr. 2020, Art. no. 119653, doi: 10.1016/j.jclepro.2019.119653.

[6] A. S. Bretas, N. G. Bretas, and B. E. B. Carvalho, "Further contributions to smart grids cyber-physical security as a malicious data attack: Proof and properties of the parameter error spreading out to the measurements and a relaxed correction model," *Int. J. Electr. Power Energy Syst.*, vol. 104, pp. 43–51, Jan. 2019.

[7] A. S. Bretas, N. G. Bretas, B. Carvalho, E. Baeyens, and P. P. Khargonekar, "Smart grids cyber-physical security as a malicious data attack: An innovation approach," *Electr. Power Syst. Res.*, vol. 149, pp. 210–219, Aug. 2017.

[8] P. Risbud, N. Gatsis, and A. Taha, "Vulnerability analysis of smart grids to GPS spoofing," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 3535–3548, Jul. 2019.

[9] C. Yang, W. Yang, and H. Shi, "DoS attack in centralised sensor network against state estimation," *IET Control Theory Appl.*, vol. 12, no. 9, pp. 1244–1253, Jun. 2018.

[10] Y. Zhang, L. Wang, Y. Xiang, and C.-W. Ten, "Power system reliability evaluation with SCADA cybersecurity considerations," *IEEE Trans. Smart Grid*, vol. 6, no. 4, pp. 1707–1721, Jul. 2015.

[11] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 ukraine blackout: Implications for false data injection attacks," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 3317–3318, Jul. 2017.

[12] N. Liu, J. Zhang, H. Zhang, and W. Liu, "Security assessment for communication networks of power control systems using attack graph and MCDM," *IEEE Trans. Power Del.*, vol. 25, no. 3, pp. 1492–1500, Jul. 2010.

[13] J. Hong, R. F. Nuqui, A. Kondabathini, D. Ishchenko, and A. Martin, "Cyber attack resilient distance protection and circuit breaker control for digital substations," *IEEE Trans. Ind. Informat.*, vol. 15, no. 7, pp. 4332–4341, Jul. 2019.

[14] R. Fu, X. Huang, Y. Xue, Y. Wu, Y. Tang, and D. Yue, "Security assessment for cyber physical distribution power system under intrusion attacks," *IEEE Access*, vol. 7, pp. 75615–75628, 2019.

[15] D. Bian, M. Kuzlu, M. Pipattanasomporn, S. Rahman, and Y. Wu, "Real-time co-simulation platform using OPAL-RT and OPNET for analyzing smart grid performance," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, Denver, CO, USA, Jul. 2015, pp. 1–5.

[16] S. Poudel, Z. Ni, and N. Malla, "Real-time cyber physical system testbed for power system security and control," *Int. J. Electr. Power Energy Syst.*, vol. 90, pp. 124–133, Sep. 2017.

[17] R. Liu, C. Vellaithurai, S. S. Biswas, T. T. Gamage, and A. K. Srivastava, "Analyzing the cyber-physical impact of cyber events on the power grid," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2444–2453, Sep. 2015.

[18] J. Fei, Y. Ma, X. Huang, Z. Liu, Q. Wang, and Y. Tang, "The research on cyber-attack testbed with hardware-in-loop," in *Proc. IEEE Conf. Energy Internet Energy Syst. Integr. (EI2)*, Beijing, China, Nov. 2017, pp. 1–6.

[19] E. Bompard, C. Gao, R. Napoli, A. Russo, M. Masera, and A. Stefanini, "Risk assessment of malicious attacks against power systems," *IEEE Trans. Syst., Man, Cybern. A, Syst. Humans*, vol. 39, no. 5, pp. 1074–1085, Sep. 2009.

[20] Z. Jian, L. Shi, L. Yao, and B. Masoud, "Electric grid vulnerability assessment under attack-defense scenario based on game theory," in *Proc. IEEE PES Asia–Pacific Power Energy Eng. Conf. (APPEEC)*, Kowloon, China, Dec. 2013, pp. 1–5.

[21] L. Wei, A. H. Moghadasi, A. Sundararajan, and A. I. Sarwat, "Defending mechanisms for protecting power systems against intelligent attacks," in *Proc. 10th Syst. Syst. Eng. Conf. (SoSE)*, San Antonio, TX, USA, May 2015, pp. 12–17.

[22] Y. Zhang, L. Wang, Y. Xiang, and C.-W. Ten, "Inclusion of SCADA cyber vulnerability in power system reliability assessment considering optimal resources allocation," *IEEE Trans. Power Syst.*, vol. 31, no. 6, pp. 4379–4394, Nov. 2016.

[23] C. Y. T. Ma, D. K. Y. Yau, X. Lou, and N. S. V. Rao, "Markov game analysis for attack-defense of power networks under possible misinformation," *IEEE Trans. Power Syst.*, vol. 28, no. 2, pp. 1676–1686, May 2013.

[24] L. Wei, A. I. Sarwat, W. Saad, and S. Biswas, "Stochastic games for power grid protection against coordinated cyber-physical attacks," *IEEE Trans. Smart Grid*, vol. 9, no. 2, pp. 684–694, Mar. 2018.

[25] Y. Xiang and L. Wang, "A game-theoretic study of load redistribution attack and defense in power systems," *Electr. Power Syst. Res.*, vol. 151, pp. 12–25, Oct. 2017.

[26] X. Wu and A. J. Conejo, "An efficient tri-level optimization model for electric grid defense planning," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 2984–2994, Jul. 2017.

[27] Y. Xiang and L. Wang, "An improved defender–attacker–defender model for transmission line defense considering offensive resource uncertainties," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 2534–2546, May 2019.

[28] M. Tian, M. Cui, Z. Dong, X. Wang, S. Yin, and L. Zhao, "Multilevel programming-based coordinated cyber physical attacks and countermeasures in smart grid," *IEEE Access*, vol. 7, pp. 9836–9847, 2019.

[29] P. Li, Y. Liu, H. Xin, and D. Qi, "Vulnerability assessment for cyber-physical system of distribution network in distributed cooperative control mode," *Autom. Electr. Power Syst.*, vol. 42, no. 10, pp. 28–35, May 2018.

[30] Y. Cai, Y. Cao, Y. Li, T. Huang, and B. Zhou, "Cascading failure analysis considering interaction between power grids and communication networks," *IEEE Trans. Smart Grid*, vol. 7, no. 1, pp. 530–538, Jan. 2016.

[31] M. Abdellaoui and C. Gonzales, "Multiattribute utility theory," in *Decision-Making Process*. London, U.K.: Wiley, 2009, pp. 579–616.

[32] J. R. S. C. Mateo, "Utility theory and decision theory," in *Multi Criteria Analysis in the Renewable Energy Industry*. London, U.K.: Springer, 2012, pp. 63–72.

[33] X. Li, "Study on traffic assignment models and algorithms based on extended logit model," Ph.D. dissertation, School Traffic Transp., Beijing Jiaotong Univ., Beijing, China, 2014.

[34] Y. Zhang, L. Wang, and Y. Xiang, "Power system reliability analysis with intrusion tolerance in SCADA systems," *IEEE Trans. Smart Grid*, vol. 7, no. 2, pp. 669–683, Mar. 2016.

[35] W. I. Al Mannai and T. G. Lewis, "A general defender-attacker risk model for networks," *J. Risk Finance*, vol. 9, no. 3, pp. 244–261, 2008.

[36] B. Chen, H. Chen, Y. Zhang, J. Zhao, and E. Manla, "Risk assessment for the power grid dispatching process considering the impact of cyber systems," *Energies*, vol. 12, no. 6, p. 1084, Mar. 2019.

[37] P. Subcommittee, "IEEE reliability test system," *IEEE Trans. Power App. Syst.*, vol. PAS-98, no. 6, pp. 2047–2054, Nov. 1979.

[38] *Guide on Operational Risk Evaluation of China Southern Power Grid*, Standard Q/CSG 11104002, 2012.

[39] *Information Security Technology—Risk Assessment Specification for Information Security*, Standard GB/T 20984, 2007.

[40] *Information Technology—Security Techniques—Information Security Management Systems-Overview and Vocabulary*, Standard ISO IEC 27000, 2018.

[41] *Information Security Technology—Baseline for Classified Protection of Cybersecurity*, Standard GB/T 22239, 2019.

BIYUN CHEN was born in Beihai, China, in 1978. She received the B.E. degree in electrical engineering from the South China University of Technology, Guangzhou, China, in 1999, the M.S. degree from the College of Electrical Engineering, Guangxi University, Nanning, China, in 2003, and the Ph.D. degree in electrical engineering from the South China University of Technology, in 2006. She was an Associate Dean of the College of Electrical Engineering, Guangxi University, where she is currently an Associate Professor. Her research interests include smart grid operation and planning, and power system cyber-security.

ZHIHAO YANG was born in Yulin, China, in 1994. He received the B.E. degree from the School of Mechatronics Engineering, Guilin University of Electronic Technology, Guilin, in 2017. He is currently pursuing the M.S. degree with the Guangxi Key Laboratory of Power System Optimization and Energy Technology, Guangxi University. His current research interest includes power system risk assessment.

YIYI ZHANG (Member, IEEE) was born in Guangxi, China, in 1986. He received the bachelor's degree in electrical engineering from Guangxi University, Nanning, China, in 2008, and the Ph.D. degree from Chongqing University, Chongqing, China, in 2014. In 2014, he joined Guangxi University, where he is an Associate Professor with the College of Electrical Engineering. He was awarded by the Guangxi Thousand Teachers Talent (the young teacher talents in Guangxi province) and the Bagui Young Talent Scholar (the young talent in Guangxi province), in 2017 and 2019, respectively. He hosts over ten projects and has authored or coauthored over 60 papers published in SCI/EI journals and conferences. His current research interests include power system risk assessment and intelligent diagnosis for transformers.

YANNI CHEN was born in Quanzhou, China, in 1997. She received the B.E. degree from the Electrical and Electronics Engineering Institute, North China Electric Power University, Beijing, in 2019. She is currently pursuing the M.S. degree with the Guangxi Key Laboratory of Power System Optimization and Energy Technology, Guangxi University. Her current research interest includes power system reliability.

JUNHUI ZHAO (Member, IEEE) was born in Henan, China. He received the M.Sc. degree in electrical engineering from Chongqing University, Chongqing, China, in 2009, and the Ph.D. degree in electrical engineering from Wayne State University, Detroit, MI, USA, in 2014. From 2009 to 2014, he was a Graduate Research Assistant at the Center for Integration of Electric Vehicle and Smart Grid, Wayne State University. He is currently an Assistant Professor with the University of New Haven, USA. He has authored or coauthored over 30 papers published in journals and conferences. His current research interests include modeling and control of distributed generation (DG) sources, the operation of smart grid with high penetration of DG and energy storage, and the voltage stability of power systems. He is an Associate Editor of *Intelligent Automation and Soft Computing* (Autosoft Journal).