IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received January 4, 2020, accepted January 30, 2020, date of publication February 10, 2020, date of current version February 18, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2973030

Modeling an Attack-Mitigation Dynamic Game-Theoretic Scheme for Security Vulnerability Analysis in a Cyber-Physical Power System

BOYU GAO AND LIBAO SHI, (Senior Member, IEEE)
National Key Laboratory of Power Systems in Shenzhen, Shenzhen International Graduate School, Tsinghua University, Shenzhen 518055, China
Corresponding author: Libao Shi (shilb@sz.tsinghua.edu.cn)

ABSTRACT The rapid development of advanced information and communication technology has made modern power systems evolve into more complicated cyber-physical power systems (CPPSs) with mutual coupling characteristics between cyber systems and power systems, and at the same time, the CPPSs have to confront some newly emerged risks owing to cyber system unreliability or cyberattacks. In this paper, regarding the cyber and physical attacks in a CPPS, the operation risks and vulnerabilities of transmission lines are discussed in detail by building relevant game-theoretic models. Under two possible cyberattack scenarios, namely time delay of system recovery and distributed denial of service, a three-stage defender-attacker-defender tri-level mathematical programming model is proposed based on dynamic game theory of complete information. In particular, the objective functions and corresponding constraint conditions in each level are analyzed and constructed elaborately. For the solution of this proposed tri-level programming model, a solution method based on an improved particle swarm optimization approach combined with sequential quadratic programming technique is applied during analysis. Finally, the proposed model is validated through two case studies, and some preliminary concluding remarks are summarized.

INDEX TERMS Cyber-physical power system, dynamic game with complete information, tri-level programming, vulnerability analysis, particle swarm optimization.

I. INTRODUCTION

The rapid development of today's smart grid has undergone tremendous changes and innovations in recent years. In particular, with increasing automation in the power system, more and more information networks, communication technologies, and sensing devices are widely applied. As deep integration of physical power system and information network, the modern power system is no longer a purely traditional power grid consisting of a large number of power devices, but a cyber-physical power system(CPPS) composed of virtual cyberspace and traditional entity physical network. Compared with the traditional power grid, CPPS integrating advanced information communication technology and control algorithm, greatly improves the efficiency and reliability of the power system. However, at the same time, it also brings new problems and challenges. Insecure cyber networks and increasing cyber intrusion activities could result in different consequences on power systems from inappropriate disclosure of confidential information to disastrous blackouts.

Recently, the threat of cyberattacks against power system cyber networks is increasing dramatically. Regarding the malicious attacks by terrorists, besides those attacks aiming at physical parts, causing line interruption or component failure, the cyberattacks which can also lead to severe consequences are involved as well [1]. In December 2015, an unprecedented hack attack on Ukraine's power grid caused thousands of homes to lose power. It was the first known instance of hacker-induced power outages around the world [2]. Moreover, in December of the following year, hackers launched another attack, causing a severe power outage in Ukraine [3]. In 2017, it was reported that there were cyberattacks on the Irish power grid. The attackers installed software on the routers and were able to see encrypted communications

The associate editor coordinating the review of this manuscript and approving it for publication was Arup Kumar Goswami.

protocols [4]. Furthermore, the cyberattack in Venezuela in March 2019 caused blackouts for more than five days [5]. Confronting such cyberattack threat, it is of great practical significance to analyze the operational risk of the power system and identify the vulnerable components.

It is known that game theory is widely used to analyze the vulnerability in a CPPS. The competition between attackers and system operators has always been modeled as Markov games and leader-follower Stackelberg games. In a Markov game [6]–[10], the competition was regarded as a continual process in which the participants choosed their strategies in each state. And the interaction in each state can be regarded as a zero-sum static stochastic game. Different from Markov games, leader-follower Stackelberg games were one-time events but always have two stages, in which the players choosed their strategies to maximize their payoffs subject to other players' action behaviors [11]–[17]. In a Stackelberg game, the attackers were always regarded as the leaders who determined the components to be attacked so that the damage was maximized, and the system operator was the follower with the aim of minimizing the damages caused by the disruptive agent. This attack-mitigation process can be transformed into a mixed integer bi-level optimization problem, which can be solved by converting into a single-level linear programming problem [12] or Benders decomposition [13]. Thereafter, a tri-level programming model was proposed, which was more realistic, considering the defender's configuration before the attacker's action behavior [17]–[21]. The tri-level programming problem can be solved by the decomposition algorithm [17], [18]. In a tri-level programming model, the allocation strategy of the resource was discrete, which only simply used the binary value to measure whether the attack would cause component failure. In practice, even if the component was in a protected state, some attack towards it may also succeed, which means that whether the attack was successful or not should be a probabilistic event. Furthermore, in subsequent researches, the continuity of resources was elaborately investigated. In [22], the resources were divided into K parts for distribution. In addition, Shi L et al. set power failure caused by the attack as a probabilistic event, where the vulnerability of the line in the test system was analyzed by dynamic game. In [23], the defensive strategies were completely continuous, and the influence of the defense resources on the system recovery time was introduced.

The models mentioned above mainly focused on physical attacks in power systems. There were also some researches on the cyberattacks in CPPS. The false data injection attacks can affect the state estimation, further affect the power flow calculation [24] and even the power market [25]. The attackers can also launch undetectable cyberattacks through load redistribution attack, which can redistribute individual bus loads in the system without changing the overall load demands [26]. The corresponding mathematical models were established to analyze such cyberattacks [27], [28]. However, there are few researches analyzing the vulnerability of the power grid with cyberattacks.

In this paper, a CPPS vulnerability assessment framework that represents a tri-level mathematical programming model under various cyberattack scenarios is established based on dynamic game theory. For this proposed nonlinear programming model, an improved particle swarm optimization (PSO) approach is applied to identify the critical system components in a studied CPPS. Finally the simulations are performed on two test systems to demonstrate the effectiveness and validity of the proposed model and method.

The rest of the paper is organized as follows. Section II describes the problem to be studied and proposes the defense-attack-mitigation optimization model based on the dynamic game method. Section III discusses the corresponding solution method. Case studies are carried out and analyzed in Section IV. Finally, the concluding remarks and future works are presented in Section V.

II. PROBLEM FORMULATION

As aforementioned, we aim to carry out vulnerability assessments of power components and to identify critical system components based on the dynamic game under physical attacks and cyberattacks. In this paper, the interaction between the attacker and the defender is envisaged as a game of complete information.

The following basic assumptions are listed for formulating the attack-mitigation scheme.

(a) The attacker is accessible to the topology and all parameters of the entire network.

(b) The attacker knows the defense strategies applied by the defender, namely the allocation of physical resources and defense resources.

(c) The attacker knows the measures that the defender would take if attacks succeed.

(d) The attacker has knowledge of the final losses of the power grid if attacks succeed.

(e) The defender would take the attacker's possible attacks into consideration before allocating defense resources.

(d) Fault tolerant of the CPPS is ignored.

A. DEFENSE-ATTACK-MITIGATION SCENARIO

In this paper, we only consider such a scenario involving one operator and one attacker. As shown in Fig.1, the attacker maliciously attacks the transmission lines and prevents the defender taking mitigation measures. The defense-attack-mitigation process can be described as follows:

(1) The grid operator allocates limited defense resources to harden physical components and cyber elements, aiming at reducing the probability of components failure.

(2) The attacker launches physical attacks and then cyberattacks according to the operator's defense strategies. Here, the physical attacks mainly refer to those attacks which would cause the line tripping. While the cyberattacks refer to those attacks on cyber elements, which may lead to recovery time delay or the distributed denial of service (DDoS).

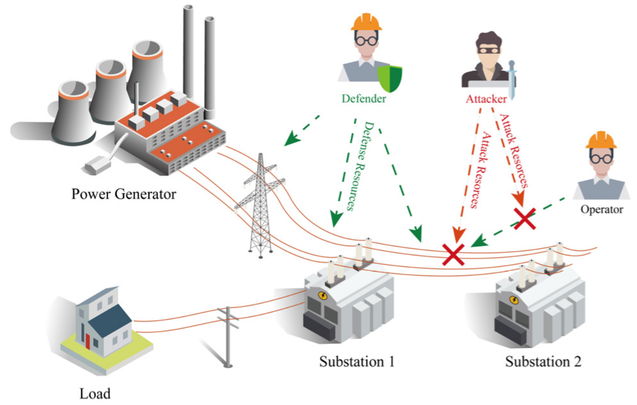

FIGURE 1. Defense-attack-mitigation scenario.

(3) The operator tries to reduce the losses of the system and maintain system stability by means of load shedding and line tripping, if necessary.

Based on the game theory, the aforementioned defense-attack-mitigation scenario can be modeled as a dynamic game model through a triple $\Gamma =< I, S, U >$:

(a) I = (defender, attacker) is the player space which includes the CPPS defender and the attacker.

(b) $S = (S_{\text{attacker}}, S_{\text{defender}})$ is the strategy space. And $S_{\text{defender}} = (d_{p,1}, d_{p,2}, \ldots, d_{p,i}, \ldots, d_{p,N}, d_{c,1}, d_{c,2}, \ldots, d_{c,i}, \ldots, d_{c,N'})$, $S_{\text{attacker}} = (a_{p,1}, a_{p,2}, \ldots, a_{p,i}, \ldots, a_{p,M}, a_{c,1}, a_{c,2}, \ldots, a_{c,i}, \ldots, a_{c,M'})$, where $d_{c,i}, d_{p,i}$ represent the cyber and physical defense resources allocated on component i, respectively; $a_{c,i}, a_{p,i}$ represent the cyber and physical attack resources allocated on component i, respectively; N, N' denote that the defender can protect N physical components and N' cyber elements. M, M' denote that the attacker can attack M physical components and M' cyber elements.

(c) Let $U_{\text{defender}}(S_{\text{attacker}}, S_{\text{defender}}): S_{\text{defender}} \rightarrow \mathbb{R}$, $U_{\text{attacker}}(S_{\text{attacker}}, S_{\text{defender}}): S_{\text{attacker}} \rightarrow \mathbb{R}$ represent the payoffs to the defender and the attacker, respectively. In this paper, the U_{attacker} means the load losses of CPPS, while $U_{\text{defender}} = -U_{\text{attacker}}$. Thereofre, the entire game process constitutes a zero-sum game. What's more, the calculation of the payoff would be described in the following sections.

(d) Game stage: The game model is a two-stage model, where the CPPS defender allocates defense resource at the first stage, while the attacker would lunch the physical and cyber attacks at the second stage. It is worth mentioning that that the attacker acts after the defender, therefore the strategy of the defender would be observed by the attacker.

1) RESOURCES SETTINGS

In practice, the resources include manpower, device technology, software level and so on. In our work, the details of the resources are ignored, and the resources are quantified by using unit "1" during analysis.

Regarding the resources settings, the further assumptions are listed as follows:

(a) The defender and the attacker both have limited resources D and A, respectively.

(b) Physical resources are independent of each other.

(c) The defender and the attacker can allocate their resources on the components in the system continuously.

Then we can get:

$$\begin{aligned} A_c + A_p &= A = \text{const} \\ D_c + D_p &= D = \text{const} \\ A_c, A_p, D_c, D_p &= \text{const} \end{aligned} \tag{1}$$

where A_c and D_c denote the amount of cyber resources owned by the attacker and the defender, respectively. A_p and D_p denote the amount of physical resources owned by the attacker and the defender, respectively.

Particularly, we have:

$$\begin{aligned} &\sum_{i=1}^{N} d_{p,i} = D_p, \quad \sum_{i=1}^{N'} d_{c,i} = D_c \\ &\sum_{j=1}^{M} a_{p,j} = A_p, \quad \sum_{j=1}^{M'} a_{c,j} = A_c \end{aligned} \tag{2}$$

2) PHYSICAL ATTACK

In this paper, the physical attacks mainly refer to attacking the transmission lines in CPPS. In general, the attacker and the defender will influence the vulnerability of components via allocating the physical and cyber resources. Regarding the monotonic and marginal effects, we propose the following simplified equation on the failure probability of transmission line i based on the allocations of physical resources $a_{p,i}$ and $d_{p,i}$ of both attacker and defender:

$$p_{p,i} = \frac{a_{p,i}}{1 + a_{p,i}} \cdot \frac{1}{1 + d_{p,i}} \tag{3}$$

Equation (3) shows that the line i would be tripped easily when fewer defense resources or more attack resources are allocated on it. And the value of the probability will decrease as the allocated physical resources increase.

When M transmission lines are attacked simultaneously, if the attack causes S lines tripped, let $\boldsymbol{SP} = \{SP_1, SP_2, \ldots, SP_w\}$ represent the collection of possible S tripped lines. For each of these cases, the corresponding probability of its occurrence can be calculated by:

$$P_{p,SP_k} = \prod_{i \in SPA} p_{p,i} \cdot \prod_{j \in FPA} (1 - p_{p,j}) \quad k = 1, 2, \ldots, w \tag{4}$$

where SPA represents the set of failure lines, FPA denotes the set of other lines.

3) TWO KINDS OF CYBERATTACKS

In this paper, two kinds of cyberattacks, namely recovery time delay attack and DDoS attack, are mainly considered during analysis. For different types of cyberattacks, the allocation of cyber and defense resources has different effects on the vulnerability of components.

First, regarding the recovery time delay attack, when a component in a system is attacked and eventually failed, it takes time for the system operator for such a situation. What is more, repairing the failure also takes a certain amount of time. Hence, the attackers can launch cyberattacks to extend the recovery time [29], which can expand the losses of the system.

The recovery time of component i depends on the allocated defense and attack resources. It can be calculated by the following expression:

$$t_{d,i} = \frac{a_{c,i}}{1+a_{c,i}} \cdot \frac{1}{1+d_{c,i}} \tag{5}$$

Similar to (3), equation (5) also considers the monotonic and marginal effects.

When several components need to be recovered after a physical attack, for the sake of simplicity, we assume the sum of the recovery time of all components as the total recovery time T_d:

$$T_d = \sum_{i \in SPA} t_{d,i} \tag{6}$$

Besides launching recovery time delay attack, cyber attackers can also cause the expansion of system losses via preventing the system operator from taking defensive measures. For instance, when the system operator wants to maintain the stability of the system by means of load shedding, the DDoS attacks can prevent the system operator from shedding load, which may make the system more unstable.

For DDoS attacks, the impacts of the allocation of cyberattack and defense resources on the vulnerability of components are still reflected by the success probability of the attack. The probability of a cyberattack causing a component to refuse an action can be modeled as:

$$p_{c,i} = \frac{a_{c,i}}{1+a_{c,i}} \cdot \frac{1}{1+d_{c,i}} \tag{7}$$

When M' cyber components are attacked simultaneously, if the attack causes S components to refuse action at the same time, let $\boldsymbol{SC}$=$\{SC_1, SC_2, \ldots, SC_w\}$ represent the collection of all possible S faulty components, then for each of these cases, the corresponding probability of its occurrence can be described as:

$$P_{c,SC_k} = \prod_{i \in SCA} p_{c,i} \cdot \prod_{j \in FCA} \left(1 - p_{c,j}\right) \tag{8}$$

where SCA represents the set of components that refuse action due to cyberattacks, while FCA represents the set of other cyber components.

B. TRI-LEVEL PROGRAMMING MODEL

After establishing the dynamic game model, the Nash equilibrium can be calculated by applying a two-stage backward induction approach, which can be described as follows:

1. Analyze the attacker's strategies, who must choose his dominant strategy in the second stage. And establish the best-response correspondence of the attacker.
2. Analyze the defender's strategies with the best-response correspondence of the attacker taken into account.

Therefore, the game model constructed in Section II can be transformed into a tri-level programming problem by establishing corresponding objective function and constraints in each level respectively. In the lower level programming model, the losses of the system can be obtained if the target transmission lines are tripped. The middle level programming model can be viewed as the best-response correspondence of the attacker when the defender's strategy is given. Furthermore, the Nash equilibrium solution of the dynamic game can be obtained by solving the upper level programming model. Then the vulnerability assessment can be further conducted on transmission lines based on the final resource allocations of both the attacker and the defender.

1) LOWER LEVEL PROGRAMMING MODEL

In our work, there are following major concerns in establishing the lower level programming model. When transmission lines are tripped due to the attacker's physical attack, the system operator needs to operate load shedding to maintain system stability. Therefore, the corresponding amount of load shed will become the key point of constructing the lower level model.

In this paper, the product of the amount of load shedding and the recovery time is leveraged to represent the losses of the power grid caused by the attack. In fact, when the tripped lines are determined, the recovery time of these tripped lines is determined as well. Then for the defender, reducing the losses of power grid can be equivalent to minimum load shedding. Therefore, the objective function in the lower level programming model is defined to minimize the total load shedding amount:

$$\left[\boldsymbol{P}^{Gen}, \boldsymbol{\theta}\right] = \arg\left\{\min \sum_{i \in \boldsymbol{I}} S_i\right\} \tag{9}$$

where $\boldsymbol{P}^{Gen}$ is the active power of generator; $\boldsymbol{\theta}$ is the phase angle of each node; $\boldsymbol{I}$ is the set of load nodes; S_i is the loads to be shed.

For (9), the following constraints must be satisfied:

$$P_l = \frac{\theta_{o(l)} - \theta_{d(l)}}{x_l} \tag{10}$$

$$P_i^{Gen} - \sum_{l|o(l)=i} P_l^{Line} + \sum_{l|d(l)=i} P_l^{Line} = d_i - S_i \tag{11}$$

$$0 \le P_g^{Gen} \le \overline{P}_g^{Gen} \tag{12}$$

$$-\overline{P}_l^{Line} \le P_l^{Line} \le \overline{P}_l^{Line} \tag{13}$$

$$0 \le S_i \le d_i \tag{14}$$

Equation (10) describes the power flow constraints on line l base on DC technique. Where the subscripts $o(l)$ and $d(l)$ denote the from-end and to-end of line l respectively, and x_l represents the impedance of line l. Equation (11) describes the power balance at the bus i. Equations (12) and (13) denote the upper and lower limits of generator outputs and line power flows. Equation (14) shows that the amount of load shedding at bus i cannot exceed its given load demand.

2) MIDDLE LEVEL PROGRAMMING MODEL

For the middle level modeling concerns, the second step in the game is that the attacker allocates attack resources according to the defender's defensive strategies, aiming at causing the greatest losses in the system. In our work, the losses caused by the attack are defined as the product of the amount of load shedding and the recovery time. When a set of components $SP_k \in \boldsymbol{SP}$ fail due to the attack, the final losses can be described as:

$$Y_{SP_k} = T \cdot mLS \tag{15}$$

where the mLS (the minimum load shedding amount) can be obtained by solving the aforementioned lower level programming model, while the total recovery time T mainly consists of the basic recovery time and the delay time caused by cyberattacks, which can be described as:

$$T = \alpha T_{base} + (1-\alpha) T_d, \quad 0 \le \alpha \le 1 \tag{16}$$

where α is a weighted coefficient which would be set as 0.1 in this paper, and the total basic recovery time T_{base} is:

$$T_{base} = \sum_{l \in SPA} t_{base,l} \tag{17}$$

In this paper, we assume that the basic recovery time of a single transmission line is proportional to its reactance:

$$t_{base,l} = k_l \cdot x_l \tag{18}$$

where we take $k_l = 1$ in this paper.

In the middle level programming model, the attacker should reasonably allocate the resources so as to implement the maximum system losses, while it is imperative to consider the influence of the probability of a successful attack. In our work, the risk theory [30] is employed to construct the objective function of the middle level programming model.

Based on the risk theory, the attacker's payoff function can be modeled as the product of accident losses caused by component failure and the probability of component failure. When the attacker attacks a single transmission line, the payoff function U_1 pertinent to the attacker can be expressed as:

$$U_1 = p_{p,l} \cdot Y_l \tag{19}$$

where Y_l denotes the losses of system when line l is tripped, and $p_{p,1}$ represents the failure probability of line l.

When the attacker attacks two lines simultaneously, the corresponding payoff function U_2 can be expressed as:

$$U_2 = P_{p,l_1} \cdot Y_{l_1} + P_{p,l_2} \cdot Y_{l_2} + P_{p,\{l_1,l_2\}} \cdot Y_{\{l_1,l_2\}} \tag{20}$$

And according to (4), here is:

$$\begin{aligned} P_{p,l_1} &= p_{p,l_1} \cdot \left(1 - p_{p,l_2}\right) \\ P_{p,l_2} &= \left(1 - p_{p,l_1}\right) \cdot p_{p,l_2} \\ P_{p,\{l_1,l_2\}} &= p_{p,l_1} \cdot p_{p,l_2} \end{aligned} \tag{21}$$

Likewise, when the attacker attacks M lines in the system, the payoff function can be expressed as:

$$U_M = \sum_{S=1}^{M} \sum_{SP_k \in SP} P_{p,SP_k} \cdot Y_{SP_k} \tag{22}$$

Then the objective function of the middle level programming model can be expressed as:

$$\left[a_c, a_p\right] = \arg \left\{ \max_{d_p, d_c} U_M \right\} \tag{23}$$

Moreover, the constraints are given as follows, that means the attacker bears limited attack resources:

$$\begin{cases} \sum_{i=1}^{M} a_{p,i} = A_p = \text{const} \\ \sum_{i=1}^{M'} a_{c,i} = A_c = \text{const} \end{cases} \tag{24}$$

where M' is different from M, that means the number of cyberattack targets is not necessarily the same as the number of physical attack targets.

3) UPPER LEVEL PROGRAMMING MODEL

The upper level programming model is pertinent to the strategy of the defender. The defender aims to maximally reduce the losses of power grid through allocating defense resources when the power grid is attacked. The objective function of the upper level programming model is similar to that of the middle level programming model, except that the modeling of middle level programming is for the attacker to maximize U_M while the modeling of upper level programming is for the defender to minimize U_M through making strategies.

The corresponding objective function of the upper level programming model can be expressed as:

$$\left[d_c, d_p\right] = \arg \left\{ \min_{a_p^*, a_c^*} U_M \right\} \tag{25}$$

Similarly, the constraints are given as follows, that means the defender bears limited defense resource:

$$\begin{cases} \sum_{i=1}^{N} d_{p,i} = D_p = \text{const} \\ \sum_{i=1}^{N'} d_{c,i} = D_c = \text{const} \end{cases} \tag{26}$$

III. SOLUTION APPROACH

A. SOLUTIONS OF LOWER LEVEL AND MIDDLE LEVEL PROGRAMMING MODELS

First, for the lower level programming model, it can be seen from (9) that the objective function is linear, and its constraints (10)-(14) are also linear. Therefore, we use the sequential quadratic programming (SQP) [31] to solve the lower level programming model.

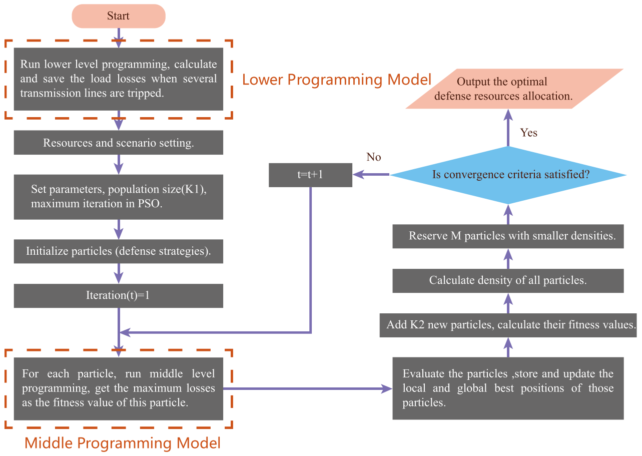
Start
Run lower level programming, calculate and save the load losses when several transmission lines are tripped.
Lower Programming Model
Resources and scenario setting.
Set parameters, population size(K1), maximum iteration in PSO.
Initialize particles (defense strategies).
Iteration(t)=1
For each particle, run middle level programming, get the maximum losses as the fitness value of this particle.
Middle Programming Model
Evaluate the particles ,store and update the local and global best positions of those particles.
Add K2 new particles, calculate their fitness values.
Calculate density of all particles.
Reserve M particles with smaller densities.
Is convergence criteria satisfied?
No
t=t+1
Yes
Output the optimal defense resources allocation.

FIGURE 2. Flow chart of solutions of the proposed tri-level programing model by using PSO Algorithm.

For the middle level programming model, it can be regarded as a nonlinear programming problem with continuously differentiable objective function. The SQP technique can also be used to solve the middle level programming model.

B. SOLUTIONS OF UPPER LEVEL PROGRAMMING MODEL

For the upper level programming model, there may be certain discontinuities in the objective function and constraints, which are very difficult to be solved by traditional optimization approaches. In this paper, the particle swarm optimization (PSO) approach [32] is applied to solve the upper level programming model.

PSO belongs to a kind of metaheuristic search algorithm, which can be abstractly understood as foraging behavior of birds or fish schools. The basic principle of PSO can be briefly described that particles in the particle swarm move to the optimal value direction according to the global search and their own experiences. PSO algorithm does not require the continuity and differentiability of the objective function and can be used to solve a large number of complex optimization problems with nonlinear and non-differentiable properties.

When PSO is used to solve the tri-level programming model, the particles are regarded as the strategies of the defender, which are the allocation of the defense resources. The fitness function value is selected as the optimal value of the middle programming model after that defense strategies are determined. Fig.2 gives the details of solving the tri-level programming model by using PSO algorithm.

In summary, the proposed CPPS vulnerability assessment framework under attack-mitigation scenario based on the relevant theory of dynamic game can be described as follows:

1. Set defense-attack-mitigation scenario.
2. Set the attack and defense resources.
3. Solve the lower level programming model for all possible accidents caused by attacks.
4. Solve the upper level programming model by using PSO algorithm, and for every particle in particle swarm, solve the corresponding middle level programming model.
5. Get the optimal allocations of defense resources by solving the upper level programming model.

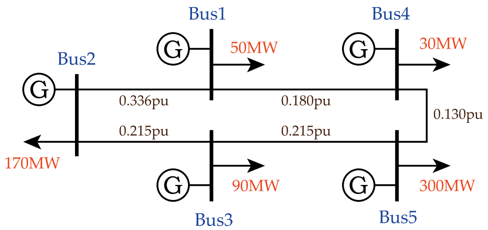

FIGURE 3. Single line diagram of 5-generator-5-bus system.

TABLE 1. Parameters of 5-Generator-5-Bus system.

Parameter	Value
Generator Capacity (MW)	0-150
Transmission Line Thermal Capacity Limits (MW)	100

C. VULNERABILITY ANALYSIS OF TRANSMISSION LINES

By applying the assessment framework as mentioned above, we can get the equilibrium $S^* = (S^*_{\text{attacker}}, S^*_{\text{defender}})$ of the proposed game model. S^*_{attacker} denotes the optimal sum of the physical defense resources allocated on each transmission line. Furthermore, we can evaluate the vulnerabilities of transmission lines based on the defender's strategy S^*_{attacker}, that is, the more physical resources allocated on the line, the higher the vulnerability of the line.

IV. CASE STUDY

In this section, the proposed CPPS vulnerability assessment framework based on the dynamic game is analyzed and validated by conducting case studies pertinent to two test systems.

A. 5-GENERATOR-5-BUS TEST SYSTEM

The 5-generator-5-bus test system and some parameters are shown in Fig.3. This system consists of five buses and six transmission lines, and each node has a generator and a load.

The system parameters are given in Table 1.

1) DEFENSE-ATTACK-MITIGATE SCENARIO

For the 5-generator-5-bus test system, we only consider the recovery time delay attacks. The basic attack-defense scenario and resources settings have been introduced in section II. In the 5-Generator-5-Bus test system, the scenario settings need to be refined further, mainly including the followings details:

- Resources settings: we assume that the targets of attack and defense are the six transmission lines. Therefore, let $N = N' = M = M' = 6$ in (2).
- Attack and defense process: The process of attack and defense is basically the same as that described in section II, and in this case, the process will be further refined. The physical and cyber attacks are considered to be

TABLE 2. The allocations of attack and defense resources on 5-Generator-5-Bus test system.

Line	Allocation of resources			
	Physical defense	Cyber defense	Physical attack	Cyber attack
1-2	0.6395	0.8350	0.9177	0.9467
1-3	0.4554	0.8511	0.8462	0.9522
1-4	0	0.6966	0.5480	0.8978
2-3	0.3835	0.8414	0.8172	0.9489
3-5	2.0181	1.3349	1.3681	1.1109
4-5	2.5034	1.4410	1.5027	1.1436

TABLE 3. The rank of transmission line risk on the 5-Generator-5-Bus test system.

Rank	Line
1	4-5
2	3-5
3	1-2
4	1-3
5	2-3
6	1-4

carrying out at the same time. Although the cyberattack may be useless when the physical attacks failed. However, regarding that this test system size is relatively small, the corresponding assumptions would not produce much error in the ranking of transmission line vulnerabilities.

By utilizing the proposed CPPS vulnerability assessment framework, the vulnerability assessment results can be obtained by solving the proposed tri-level programming model. The final allocations of defense and attack resources are shown in Table 2.

The risk of transmission lines can be ranked according to the last physical defense resource allocations, as shown in Table 3.

B. IEEE 39-BUS TEST SYSTEM

For the IEEE 39-Bus test system, both the recovery time delay and DDoS attacks are considered during simulations. The topology of the IEEE 39-Bus system is shown in Fig.4. For the sake of simplicity, the upper limit of the active power for each line is set to 1.5 times active power of normal operation, and the upper limit of the generator output is set to 1.5 times output of normal operation.

1) RECOVERY TIME DELAY ATTACKS

In this case, we assume that the defender can protect all lines whether physical or cyberattacks. Hence, we set $N = N' = 46$ and $D_p = D_c = 46$ in (2). For the sake of simplicity, we also assume that the attacker can only attack two lines in physical attacks. Furthermore, the more determined and well-informed attackers are considered during analysis. That is, attackers will select the target to attack in cyberattack based on the results of physical attacks, which can be considered as a more effective way. For instance, when an attacker launches physical attacks on line 1 and line 2, if line 1 is finally broken but line 2 not, the attacker will only perform cyberattack on line 1 to extend the recovery time of line 1. Therefore, it is further assumed that there is a relevance between the attacker's physical resources and cyber resources:

$$A_p + \beta \cdot A_c = A = 4 \tag{27}$$

where β is a conversion factor that considers the difference between the unit "1" in physical resources and cyber resources. In this paper, let $\beta = 1$.

Regarding that the attackers can only attack two transmission lines, therefore we have:

$$\sum_{i=1}^{2} a_{p,i} = A_p, \sum_{i=1}^{M'} a_{c,i} = A_c \tag{28}$$

The attack and defense process is shown in Fig.5.

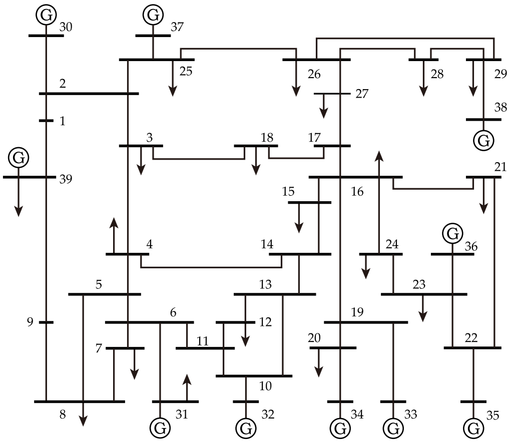

FIGURE 4. Single line diagram of IEEE 39-bus system.

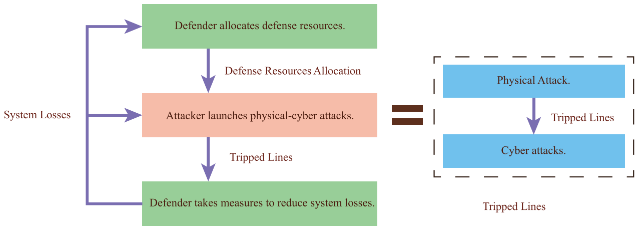
Defender allocates defense resources.
Defense Resources Allocation
System Losses
Attacker launches physical-cyber attacks.
Tripped Lines
Defender takes measures to reduce system losses.
Physical Attack.
Tripped Lines
Cyber attacks.
Tripped Lines

FIGURE 5. The scenario based on recovery time delay attack (IEEE 39-bus test system).

It can be seen from Fig.5 that it is a four-step dynamic game. However under the assumption that the sum of the attacker's physical resources and cyber resources is a constant and the cyberattacks follow the physical attacks, the two-step process including physical attacks and cyberattacks can be regarded as a one step process. The four-step game process can be equivalent to a tri-step game.

By solving the tri-level programming model, the vulnerabilities of transmission lines are divided into eight levels according to the physical resource allocation in the defense strategies, as shown in Fig.6. Different levels are

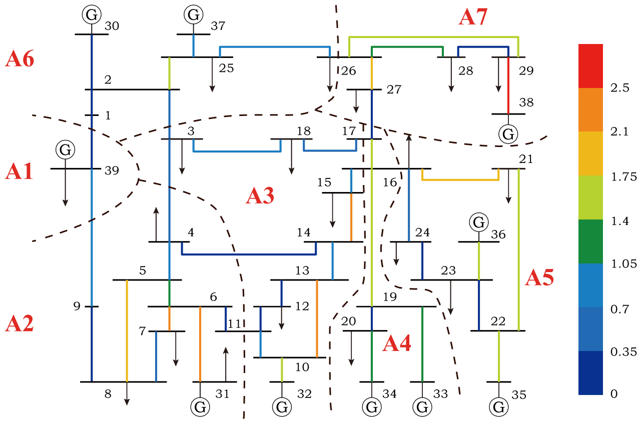

FIGURE 6. Visualized results of line vulnerability assessment based on recovery time delay attack.

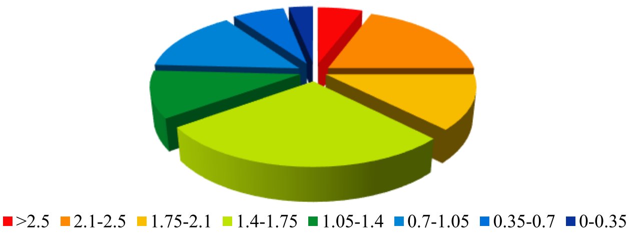

FIGURE 7. Defense resource allocation based on recovery time delay attack.

distinguished by different colors, and the warmer the color, the higher the risk of the transmission line, and the heavier the losses after an attack.

The IEEE 39-bus system can be divided into seven areas as shown in Fig.6. From Fig.6, we can get some conclusions.

- The vulnerabilities at the outlets of generators are generally high. From the viewpoint of the allocation of physical defense resources, all the resource distributions at the outlets of generators are more than 1.05. What is more, the risks of line 29-38 and line 6-31 have already been in level one or level two. In fact, from the viewpoint of the system, the disconnections at the generator outlets will cause the generators to detach from the system. When the generator outlets are tripped, the operator must cut down more loads to keep the system stable, and it would cause heavier system losses.
- It is worth mentioning that line 2-30 and line 25-37 are outlets of generators, however their risks are not high, it can be understood that they are in the same area, and when a generator is detached from the system, the other one can also meet the load demand in the area. What is more, the loads at bus 25 and bus 26 are relatively small, therefore the risks of the outlets of these two generators are not such high as others.
- The vulnerabilities of those lines which connect two different areas are relatively low. Line 1-39, line 9-39, line 4-14, line 2-3 and line 17-27 belong to the lines that connect two different areas. It can be understood that the supply and demand in each area can be balanced according to the partition, therefore when these lines are tripped, the generator output and load demand can still be balanced in each region.
- Some lines that are away from generators have relatively high risks. For instance, the line 26-27 is connected to the load at the bus 27, and the load at bus 27 is mainly supplied by node 38. While the bus 27 is away from other generators. Therefore, when line 26-27 is tripped, the supply of bus 27 will be interrupted, which will cause lots of losses. Similar situations also occur on lines line 6-7, line 14-15 and line 16-21.

According to the aforementioned levels of physical resource allocation divided, a pie chart as shown in Fig.7 is plotted to further illustrate that the defense resources are distributed evenly across the various levels, and with the exception of the highest risk level and two lowest risk levels, the other levels have essentially the same defensive physical resources.

2) DDOS ATTACK

Different from the recovery time delay attack, in a DDoS attack, the attacker's targets are the bus nodes. The attacker would like to prevent the system operator from shedding load through cyberattacks. The following details of the attack-defense scenario are discussed.

First, the defender needs to defend against a total of 46 lines. Regarding that the targets of cyberattacks are the load nodes, the defender also needs to deploy cyber defense resources for the 19 load nodes in the test system. Hence for the defender, we set $N = 46, N' = 19$ and $D_p = 46, D_c = 19$ in (2).

Moreover, we assume that the attacker can launch physical attacks on two lines and cyberattack on one cyber component, that is:

$$\sum_{i=1}^{2} a_{p,i} = A_p, \quad \sum_{i=1}^{1} a_{c,i} = A_c \tag{29}$$

And like (27), we assume:

$$A_p + \beta' \cdot A_c = A = 4 \tag{30}$$

where $\beta' = 1$ in this case.

In a DDoS attack, the total recovery time does not include recovery time delay caused by cyberattacks. It is only related to the characteristics of the lines themselves. However, the load shedding also includes the amount of load shedding after the components refuse to act owing to cyberattacks.

In this case, we consider another game process. Regarding that the attacker shall launch cyberattacks based on the defender's strategies after launching physical attacks, the cyberattacks should be launched after the defender's operation. What is more, the defender needs to take measures to reduce the losses according to the attacker's cyberattacks, including further shedding load or actively disconnecting some lines to maintain system stability. Meanwhile,

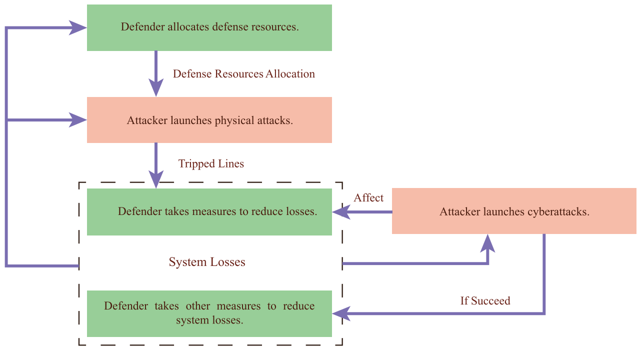
Defender allocates defense resources.
Defense Resources Allocation
Attacker launches physical attacks.
Tripped Lines
Defender takes measures to reduce losses.
Affect
Attacker launches cyberattacks.
System Losses
If Succeed
Defender takes other measures to reduce system losses.

FIGURE 8. The scenario based on DDoS attack (IEEE 39-bus system).

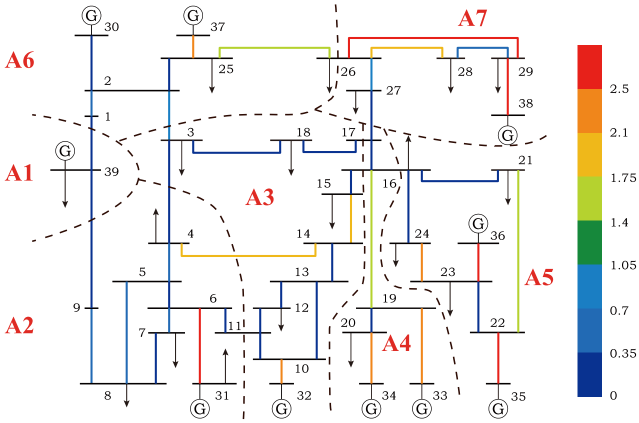

FIGURE 9. Visualized results of line vulnerability assessment based on DDoS attack.

the attacker will also consider the subsequent cyberattacks before launching physical attacks.

This dynamic game process is shown in Fig.8.

Similarly, the visualized results pertinent to the vulnerabilities of transmission lines are shown in Fig.9.

C. COMPARISONS BETWEEN TWO CYBERATTACK MODLES

Comparing to Fig.6 and Fig.9, the results based on DDoS attack and recovery time delay attack are similar, and the details are discussed as follows:

- The outlets of generators are in a high-risk position.
- Those lines whose vulnerabilities are relatively high based on recovery time delay attack also have relatively high risks based on DDoS attack.
- Those lines whose risks are relatively low are basically the same in the two cyberattack modes.

However, there are still some differences between the two cyberattack modes. Similarly, according to the cyber resource allocation, a pie chart as shown in Fig.10 is plotted to further illustrate the defense resource allocation results (There are no lines whose cyber defense resources are between 1.05 and 1.4). The corresponding physical resource allocation results based on the two different cyberattack modes are given in Fig.11. In contrast to Fig.7 and Fig.10, and referring to Fig.11, we can see that the critical lines take more physical resources based on DDoS attack. Hence, the analysis based on the DDoS attack can highlight the critical transmission lines in the test system.

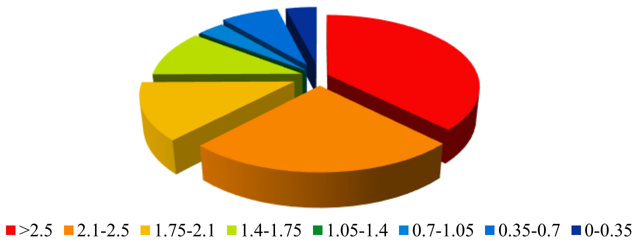

FIGURE 10. Defense resource allocation based on DDoS attack.

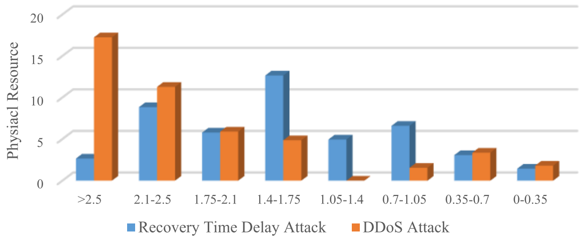

FIGURE 11. Physical resource allocation results in different cyberattack modes.

We can also find that the risks of some lines in different cyberattack modes are different as well. For instance, line 4-14 shows higher importance in DDoS attack mode. Because if the attacker attacks line 4-14 and causes it failure, the defender needs to remove some loads at bus 4 to maintain system stability. However, if the attacker launches DDoS attack to prevent the defender from shedding load, then the defender must disconnect the transmission lines connected to bus 4 to ensure that the system is stable. In this case, the defender will automatically disconnect the line 4-5 and line 3-4, causing greater losses to the system.

V. CONCLUSION

A CPPS vulnerability assessment framework is proposed and discussed in detail by applying relevant game-theoretic models. Based on the recovery time delay and DDoS attack scenarios, a tri-level programming model is established in accordance with dynamic game theory with complete information. An improved PSO approach combined with sequential quadratic programming technique is leveraged to solve the proposed optimization model. Finally, the simulations are performed on two cases to illustrate the validity and effectiveness of the proposed model and method. The results demonstrate that the model proposed in this paper can effectively point out vulnerable transmission lines in the system. Most lines show the same high vulnerability in the results of the models based on different attack scenarios. While the analysis based on the DDoS attack pays more attention to those lines with higher vulnerabilities. Currently, this paper mainly focuses on the vulnerability assessment method of power grid components under certain attack-mitigation scenarios. The future work can be carried out on the risks of cyber elements and other physical components in CPPS.

REFERENCES

[1] K. Chatterjee, V. Padmini, and S. A. Khaparde, ''Review of cyber attacks on power system operations,'' in *Proc. IEEE Region 10 Symp. (TENSYMP)*, Cochin, India, Jul. 2017, pp. 1–6.

[2] (Jan. 5, 2016). *First Known Hacker-Caused Power Outage Signals Troubling Escalation(ArsTechnia)*. [Online]. Available: https://arstechnica.com/i

[3] (Jan. 12, 2017). *Hackers Trigger Yet Another Power Outage in Ukraine(ArsTechnia)*. [Online]. Available: https://arstechnica.com/

[4] (Aug. 8, 2017). *Irish Power Grid Compromised Foreign Actor: Report(The Hill)*. [Online]. Available: http://thehill.com/

[5] (Mar. 11, 2019). *Venezuela Power Cut: Lootings as Desperation Grows(BBC)*. [Online]. Available: https://www.bbc.com/

[6] 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.

[7] Y. Li, L. Shi, P. Cheng, J. Chen, and D. E. Quevedo, ''Jamming attacks on remote state estimation in cyber-physical systems: A game-theoretic approach,'' *IEEE Trans. Autom. Control*, vol. 60, no. 10, pp. 2831–2836, Oct. 2015.

[8] Y. Li, D. E. Quevedo, S. Dey, and L. Shi, ''SINR-based DoS attack on remote state estimation: A game-theoretic approach,'' *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 3, pp. 632–642, Sep. 2017.

[9] H. Li, L. Lai, and R. C. Qiu, ''A denial-of-service jamming game for remote state monitoring in smart grid,'' in *Proc. 45th Annu. Conf. Inf. Sci. Syst.*, Baltimore, MD, USA, Mar. 2011, pp. 1–6.

[10] K. Ding, S. Dey, D. E. Quevedo, and L. Shi, ''Stochastic game in remote estimation under DoS attacks,'' *IEEE Control Syst. Lett.*, vol. 1, no. 1, pp. 146–151, Jul. 2017.

[11] A. Motto, J. Arroyo, and F. Galiana, ''A mixed-integer lp procedure for the analysis of electric grid security under disruptive threat,'' *IEEE Trans. Power Syst.*, vol. 20, no. 3, pp. 1357–1365, Aug. 2005.

[12] J. Arroyo and F. Galiana, ''On the solution of the bilevel programming formulation of the terrorist threat problem,'' *IEEE Trans. Power Syst.*, vol. 20, no. 2, pp. 789–797, May 2005.

[13] J. Salmeron, K. Wood, and R. Baldick, ''Worst-case interdiction analysis of large-scale electric power grids,'' *IEEE Trans. Power Syst.*, vol. 24, no. 1, pp. 96–104, 2009.

[14] J. Arroyo, ''Bilevel programming applied to power system vulnerability analysis under multiple contingencies,'' *IET Gener. Transm. Distrib.*, vol. 4, no. 2, p. 178, 2010.

[15] J. Salmeron, K. Wood, and R. Baldick, ''Analysis of electric grid security under terrorist threat,'' *IEEE Trans. Power Syst.*, vol. 19, no. 2, pp. 905–912, May 2004.

[16] A. Sanjab and W. Saad, ''Data injection attacks on smart grids with multiple adversaries: A game-theoretic perspective,'' *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 2038–2049, Jul. 2016.

[17] G. Brown, M. Carlyle, J. Salmerón, and K. Wood, ''Defending critical infrastructure,'' *Interfaces*, vol. 36, no. 6, pp. 530–544, Nov. 2006.

[18] Y. Yao, T. Edmunds, D. Papageorgiou, and R. Alvarez, ''Trilevel optimization in power network defense,'' *IEEE Trans. Syst., Man, Cybern. C, Appl. Rev.*, vol. 37, no. 4, pp. 712–718, Jul. 2007.

[19] N. Alguacil, A. Delgadillo, and J. M. Arroyo, ''A trilevel programming approach for electric grid defense planning,'' *Comput. Oper. Res.*, vol. 41, pp. 282–290, Jan. 2014.

[20] 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.

[21] X. Liu and Z. Li, ''Trilevel modeling of cyber attacks on transmission lines,'' *IEEE Trans. Smart Grid*, vol. 8, no. 2, pp. 720–729, Mar. 2015.

[22] S. H. I. Libao and J. I. A. Zhou, ''Vulnerability assessment of cyber physical power system based on dynamic attack-defense game model,'' *Autom. Electr. Power Syst.*, vol. 40, no. 17, pp. 99–105, 2016.

[23] G. Chen, Z. Y. Dong, D. J. Hill, and Y. S. Xue, ''Exploring reliable strategies for defending power systems against targeted attacks,'' *IEEE Trans. Power Syst.*, vol. 26, no. 3, pp. 1000–1009, Aug. 2011.

[24] Q. Yang, D. Li, W. Yu, Y. Liu, D. An, X. Yang, and J. Lin, ''Toward data integrity attacks against optimal power flow in smart grid,'' *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1726–1738, Oct. 2017.

[25] R. Deng, G. Xiao, R. Lu, H. Liang, and A. V. Vasilakos, ''False data injection on state estimation in power systems—Attacks, impacts, and defense: A survey,'' *IEEE Trans. Ind. Informat.*, vol. 13, no. 2, pp. 411–423, Apr. 2017.

[26] Z. Li, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, ''Analyzing locally coordinated cyber-physical attacks for undetectable line outages,'' *IEEE Trans. Smart Grid*, vol. 9, no. 1, pp. 35–47, Jan. 2018.

[27] Z. Li, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, ''Bilevel model for analyzing coordinated cyber-physical attacks on power systems,'' *IEEE Trans. Smart Grid*, vol. 7, no. 5, pp. 2260–2272, Sep. 2016.

[28] Y. Xiang, L. Wang, and N. Liu, ''Coordinated attacks on electric power systems in a cyber-physical environment,'' *Electr. Power Syst. Res.*, vol. 149, pp. 156–168, Aug. 2017.

[29] J. Zhang and L. Sankar, ''Physical system consequences of unobservable state-and-topology cyber-physical attacks,'' *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 2016–2025, Jul. 2016.

[30] M. Ni, J. D. McCalley, V. Vittal, and T. Tayyib, ''Online risk-based security assessment,'' *IEEE Power Eng. Rev.*, vol. 18, no. 1, pp. 258–265, Feb. 2003.

[31] S. Sivasubramani and K. Swarup, ''Sequential quadratic programming based differential evolution algorithm for optimal power flow problem,'' *IET Gener. Transm. Distrib.*, vol. 5, no. 11, p. 1149, 2011.

[32] Y. Gao and S. L. Xie, ''Particle swarm optimization algorithms with immunity,'' *Comput. Eng. Appl.*, vol. 6, pp. 4–6, Jun. 2004.

BOYU GAO received the B.S. degree in electrical engineering from Tsinghua University, Beijing, China, in 2017. He is currently pursuing the M.Sc. degree with the National Key Laboratory of Power Systems in Shenzhen, Shenzhen International Graduate School, Tsinghua University.

His main research interests include the risk assessment of cyber-physical power systems.

LIBAO SHI (Senior Member, IEEE) received the B.S., M.Sc., and Ph.D. degrees from the Department of Electrical Engineering, Chongqing University, Chongqing, China, in 1994, 1997, and 2000, respectively.

He was a Postdoctoral Research Associate at The University of Hong Kong, China, from August 2004 to June 2006. He is currently an Associate Professor with the National Key Laboratory of Power Systems in Shenzhen, Shenzhen International Graduate School, Tsinghua University, Shenzhen, China. His research interests include complementary and coordinated dispatch technologies with multienergy source structure, cyber-physical power systems, power system cascading failure and restoration control, as well as AI technologies and its application in power systems.

Dr. Shi is a member of the IET.