A Defense Planning Model for a Power System Against Coordinated Cyber-physical Attack

Peiyun Li, Jian Fu, Kaigui Xie, Senior *Member*, *IEEE*, Bo Hu, *Member*, *IEEE*, Yu Wang, Changzheng Shao, *Member*, *IEEE*, Yue Sun, and Wei Huang

***Abstract*—This paper proposes a tri-level defense planning model to defend a power system against a coordinated cyber-physical attack (CCPA). The defense plan considers not only the standalone physical attack or the cyber attack, but also coordinated attacks. The defense strategy adopts coordinated generation and transmission expansion planning to defend against the attacks. In the process of modeling, the upper-level plan represents the perspective of the planner, aiming to minimize the critical load shedding of the planning system after the attack. The load resources available to planners are extended to flexible loads and critical loads. The middle-level plan is from the viewpoint of the attacker, and aims at generating an optimal CCPA scheme in the light of the planning strategy determined by the upper-level plan to maximize the load shedding caused by the attack. The optimal operational behavior of the operator is described by the lower-level plan, which minimizes the load shedding by defending against the CCPA. The tri-level model is analyzed by the column and constraint generation algorithm, which decomposes the defense model into a master problem and subproblem. Case studies on a modified IEEE RTS-79 system are performed to demonstrate the economic efficiency of the proposed model.**

***Index Terms*—Coordinated cyber-physical attack, flexible load, column-and-constraint generation, defense planning, robust optimization.**

I. Introduction

With large-scale application of computer and network communication in the modern power system, it has evolved into a complex cyber-physical system (CPS). During operation, the power system may face threats from natural disasters and random failure of equipment, and artificial and malicious cyber or physical attacks. For example, the blackout in Ukraine in 2015 was caused by a cyber attack on the power system. This is the first serious blackout in the world triggered by hacking [1], causing power losses to over 225 000 customers and significant economic losses to Ukraine. Hence, modeling and simulating various malicious attacks, quantifying their impacts, and devising effective countermeasures have become urgent issues in the modern power system.

There has been a lot of research on mathematical modeling and simulation of various malicious attacks and defense measures [2]. Two important aspects of malicious attacks are the attack target and the defense measure. The attack targets can be divided into three categories as described below.

The first category is the physical attack against primary equipment. A successful physical attack against equipment can cause equipment to be out of operation [2]–[5], such as transmission lines [2]–[4], substations, generators, buses, etc. [5].

The second category is the cyber attack against information systems. This is an attack that exploits the vulnerabilities and security defects of the communication networks of power systems and attacks the system resources by invading information and control systems without permission [6]. Relevant studies have mainly focused on the load redistribution (LR) attack, which is an attack form in which the attacker maliciously modifies the load measurements in the power system to mislead the operator to make unscientific scheduling, causing great losses to the system [7]. The damage of the LR attack is mainly in two aspects. First, it misleads the operator to make improper scheduling to shed load by modifying the data of load measurements [7]–[9]. Second, it causes line overload and leads to the outage of transmission lines by modifying the data of load measurements. This can even lead to cascading failure in severe cases [10], [11].

The third category is coordinated cyber-physical attack (CCPA) against the whole power system. A coordinated attack scheme including LR attack and physical attack against lines as discussed, in which LR attack is

Received: October 14, 2023
Accepted: March 10, 2024
Published Online: September 1, 2024
Peiyun Li, Kaigui Xie (corresponding author), Bo Hu, Yu Wang, Changzheng Shao, and Wei Huang are with the State Key Laboratory of Power Transmission Equipment & System Security and New Technology, Chongqing University, Chongqing 400044, China (e-mail: 1437779281@qq.com; kaiguixie@vip.163.com; hboy8361@163.com; yu_wang@cqu.edu.cn; cshao@cqu.edu.cn; 17866628985@163.com).

Jian Fu is with the State Grid Chengdu Power Supply Company, State Grid Sichuan Electric Power Co., Ltd., Chengdu 610041, China (e-mail: 504971494@qq.com).

Yue Sun is with the China Yangtze Power Co., Ltd, Yichang 443002, China (e-mail: sun_yue3@ctg.com.cn).
DOI: 10.23919/PCMP.2023.000476

used to modify the load and line measurement data to mislead the operator into believing there is no fault with the lines in the system, thereby providing cover for the physical attack [12]. Thus, the model aims to identify the most disruptive and undetectable physical attack against lines that satisfies the constraint for the total attack budget. In [13], the coordinated attacks composed of either LR attack and attacking lines, or LR attack and attacking generators, are studied. The simulation results show that the attack effects of coordinated attacks are more serious than those of standalone attacks.

At present, relevant research on coordinated attack defense measures mainly focuses on 2 aspects. The first is to transform defense planning into a two-stage model, namely, the attacker-defender model. Reference [14] proposes a two-stage optimization problem for allocating defense resources to maximize the grid's immunity to malicious attacks. In [15], based on the attack and defense strategy with complete information, a two-stage collaborative attack mode considering voltage control is constructed. Reference [16] proposes a new dynamic defense strategy against dynamic load altering attack. This uses a multi-stage game between attacker and defender and is learned by minimax-Q.

The second aspect is to transform defense planning into a three-stage model, namely, the defender-attacker-defender (DAD) model. In [17], a defense-attack-defense (DAD) model is proposed to derive effective protection planning, in which a line switching operation is regarded as an effective post-emergency method. A robust optimization (RO) model for defense resource planning and allocation against multi-cycle attacks is proposed in [18], in which the custom column and constraint generation (C&CG) algorithm is used to solve the problem. Reference [19] studies the DAD model of multiple attack scenarios to develop effective defense strategies for power systems, while considering the uncertainty of attack resources. RO and stochastic programming are combined to analyze the model. In [20], network attacks against an intrusion protection relay communication network are included with the three-level optimization model to optimize defense resource allocation. Looking at transmission capacity expansion planning, reference [21] considers post-distributed mobile distributed generators participating in defense planning.

The main findings and characteristics from the above literature review can be summarized as:

1) The defense strategy against LR attacks does not take into account the scheduling optimization process adopted by system operators and the possible line overload caused by LR attacks. This scheduling is designed to reduce load shedding after being misled by false data.

2) In the defense strategy against coordinated attacks, previous studies have included the power generator in the allocation of defense resources, but not the load side.

Coordinated generation and transmission expansion planning (CGTEP) has been widely used to solve various problems of power systems in many respects, such as increase of generation capacity, grid structure enhancement, reliability improvement, and promoting the accommodation of renewable energy. In the future, malicious attacks should also be considered in CGTEP. In the existing studies, CGTEP can defend against physical attacks, such as transmission line attacks and generator attacks [22]–[25]. At the same time, a new question arises: Whether cyber-attack or coordinated attacks can also be defended effectively by CGTEP? It is reasonable to defend against coordinated attacks through CGTEP considering that cyber-attack is more common and coordinated attacks are more harmful in the modern power system.

This paper considers CGTEP as the defense method for the CCPA defense. CCPA is investigated and a coordinated defense strategy is developed against the line, generator, and LR attacks. A tri-level defense planning model is proposed to optimize the CGTEP scheme. In this tri-level model, the upper model represents the planner with the aim of optimizing the planning strategy for the newly built lines and generators with the minimum load shedding. This defense plan takes into account the load curtailments caused by CCPA, the impact of false data of load measurements, and the effect of false active power flow of lines caused by an LR attack. The attacker's strategy is modeled at the middle level, which aims at optimizing the CCPA scheme to instigate as high load shedding as possible. The lower model represents the action of the operator, aiming at the minimum load shedding. The tri-level model can be described as a master problem and subproblem, which are solved iteratively using the C&CG algorithm. Case studies based on a modified IEEE RTS-79 system are carried out to verify the effectiveness of the proposed defense planning model.

The defense strategy is to prevent the coordinated attacks along with the above concept. The main features of this study distinguishing it from previous work are:

1) The load and power flow data for scheduling considered by the operator are false data due to the attack. In contrast, in previous studies, the system scheduling by the operator is based on real data.

2) Previous studies focus on the situation that the planner considers only the impact on the operator by the physical attack scheme. In this paper, we also consider the situation that the planner is aware of the erroneous scheduling behavior of the operator.

3) This paper considers the case where flexible loads are included in the resources at the disposal of planners. In contrast, previous studies only included power sources and lines into the overall framework.

The remainder of this paper is organized as follows. Section II describes the mechanism of an LR attack and the defense effect of CGTEP, while Section III introduces the three-layer model of defense planning in detail. Section IV introduces the solution of the model. In Section V, the experimental evaluation of defense planning model is presented, and Section VI presents the main conclusions of the paper.

II. Problem Description

This paper uses CGTEP to defend the power system against CCPA. This section describes the mechanism of an LR attack and the defense effect of CGTEP.

In the study of defense planning against malicious attacks, the subjects involved include the planner, the operator (defender), and the attacker. The role of each is:

1) The planner is to defend against malicious attacks by coming up with a defense strategy.

2) An attack scheme is launched against the power system by the attacker.

3) The operator implements optimal scheduling to minimize the system loss after an attack. System information can be obtained from the measurements.

The decision-making objectives of each participant are different. That of the attacker depends on the planning strategy of the planner, while that of the operator depends on the attack scheme of the attacker, and vice versa. Malicious attacks on the power system have strong subjectivity. A rational attacker usually launches the attack to maximize the system damage. Thus, the most conservative system expansion planning strategy under the worst CCPA scheme should be selected to deal with the uncertainty of attack schemes when formulating the defense planning model. The defense of an LR attack by CGTEP can be described in terms of load shedding reduction and avoidance of overload lines.

Figure 1 illustrates the role of CGTEP in load shedding reduction. The diagram is a simple 2-bus system with generator G1 connected to bus 1 and generator G2 connected to bus 2. Generator outputs are limited to $P_{1\max}=18$ MW and $P_{2\max}=28$ MW. The capacity of transmission line L12 is 5 MW, the load data of both bus 1 and bus 2 are $L_1=L_2=20$ MW. Figure 1(a) is the initial operating state of the system, where the outputs of G1 and G2 are $P_1=18$ MW and $P_2=22$ MW.

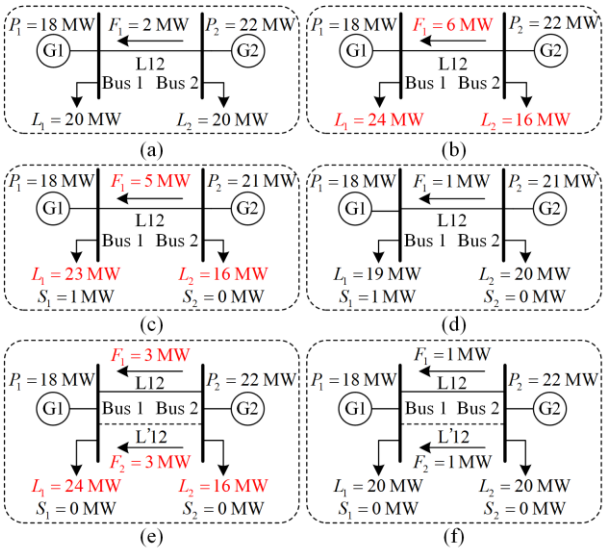

Fig. 1. Diagram of CGTEP in load shedding reduction. (a) Initial system state. (b) System state after LR attack. (c) Load shedding due to LR attack. (d) Actual operation. (e) Optimization operation after building new lines. (f) Actual operation after building new lines.

A. Load Shedding Reduction

Suppose that the attacker attacks the system at the initial operating state of Fig. 1(a) with the LR attack. Then the measured loads of bus 1 and bus 2 are changed, assuming the false data injected into the load are $\Delta L_1=-4$ MW and $\Delta L_2=4$ MW.

Note that $\Delta L_1+\Delta L_2=0$ MW, then the false loads of the two buses measured by the operator after the LR attack are 24 MW and 16 MW, respectively. The system enters the state shown in Fig. 1(b). The data represented in red denote the false data obtained by the operator, rather than the actual data.

In Fig. 1(b), if the system still operates following the state of Fig. 1(a), the active power flow F_1 is 6 MW, which may cause line overload. So the operator can be misled to make improper scheduling, such that the output of G2 becomes 21 MW and the load shedding of bus 1 is 1 MW, i.e., $S_1=1$ MW. Figure 1(c) shows the changes.

The actual operation of the system is shown in Fig. 1(d). The load at bus 1 is curtailed by 1 MW under LR attack, although the actual load is not altered before the false operation. This indicates that the LR attack causes the change of load measurement reading, thus the load shedding, rather than the actual load.

If the planner adopts a defense planning strategy, which is to build a new line L'12 between bus 1 and bus 2 with the same electrical parameters as that of L12, the system will induce to be dispatched according to Fig. 1(e) after the same LR attack scheme is implemented. The actual operation of the planning system is shown in Fig. 1(f). No-load shedding occurs in both cases. Similarly, the same objective can be achieved by building a new generator at bus 1.

B. Avoidance of Line Overload

Suppose that the attacker attacks the system in the initial operating state of Fig. 2(a) with an LR attack. The false data injected into the load are $\Delta L_1=-10$ MW and $\Delta L_2=10$ MW. The false load of L_1 measured by the operator after LR attack is 10 MW and that of L_2 is 30 MW. The system enters the state of Fig. 2(b). This leads to line overload and the power flow of L12 to return to the normal state via optimal scheduling by the operator.

If the operator wants the active power flow of L12 to be as small as possible, Fig. 2(c) depicts the state to be obtained. At this time, the load shedding is zero and the active power flow of L12 from the view of the operator is the smallest. However, the actual operational state as shown in Fig. 2(d) indicates that the actual active power flow of L12 is 8 MW, which is larger than its maximum allowable active power flow. Thus, the line is overloaded and out of operation.

If the transmission expansion plan is carried out according to the strategy in Fig. 1, the problem of line

overload can be alleviated. As shown in Fig. 2(e), at the LR attack, the system dispatch shows that the false power flows of L12 and L'12 are 1 MW each. Moreover, the actual power flows of L12 and L'12 are 4 MW each, as shown in Fig. 2(f). It can be concluded that both cases are in normal operation.

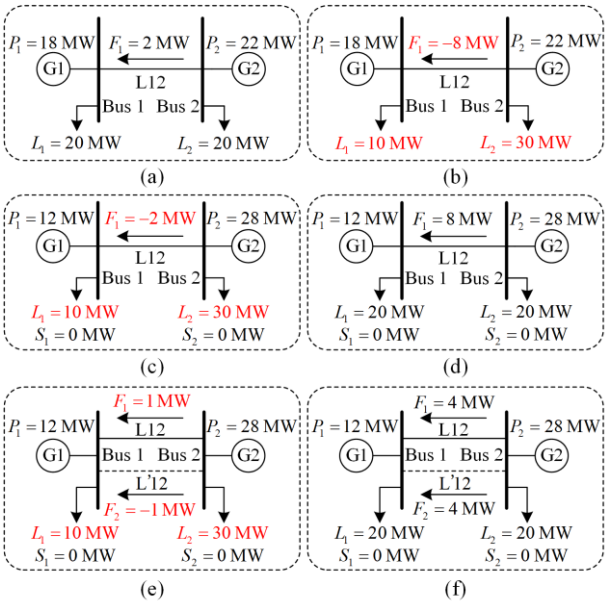

Fig. 2. Diagram of CGTEP in line overload avoidance. (a) Initial system state. (b) System state after LR attack. (c) Generation increasing due to LR attack. (d) Actual operation. (e) Optimization operation after building new lines. (f) Actual operation after building new lines.

Figures 1 and 2 show that the increase in redundancy of generators and lines after building new generators or lines reinforces the ability of power systems to cope with the physical attack on lines or generators. Both show that CGTEP is effective in defending the power system against LR attacks. It has been reported [22]–[25] that CGTEP is also effective against physical attacks. These results motivate us to investigate the effectiveness of CGTEP against CCPA, while the main concern is on determining the generators or transmission lines to be built to make the power system most effective against coordinated attacks.

III. Defense Planning Model

The proposed defense planning model adopts a robust optimization model to cope with the uncertainty of attack schemes. Figure 3 depicts this tri-level model based on the planner-attacker-operator framework. The planner is the upper level, the attacker is the middle level, and the operator is the lower level. The attacker can organize the coordinated cyber-physical attack at the middle level to maximize the load shedding. On the other hand, the planner and the operator develop the planning and scheduling strategies to defend against the attack to minimize load shedding.

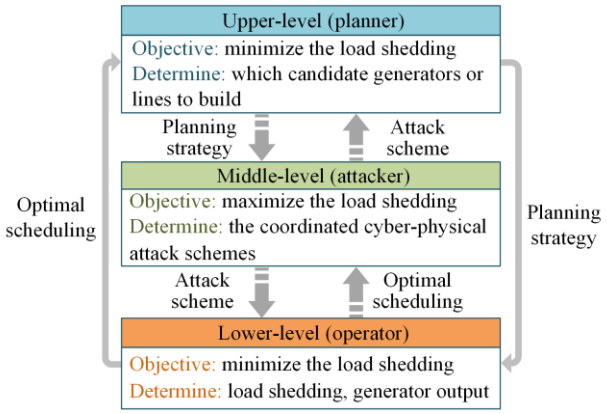

Fig. 3. The proposed tri-level defense-attack model.

This study makes the following assumptions in establishing the defense planning model against CCPA:

1) LR attack, line attack, and generator attack can be conducted simultaneously;

2) The newly added lines and generators determined by CGTEP are reinforced, so the physical attack is ineffective;

3) The attacker can obtain the data such as system topology and electrical parameters of the equipment;

4) The attacker can modify all the load measurements during the LR attack.

A. The Upper-level Model

The upper-level model is an integer optimization model. We focus on the defense effect, which aims at reducing the load shedding caused by attacks as much as possible through CGTEP. For cost-benefit analysis, we can refer to [26] by modifying the objective function of the upper-level model in this paper. However, the weighting factor for the cost of deliberate attacks in the objective function of [26] cannot be determined scientifically. This can easily cause large errors. Reliability will be improved and the load that can be supplied will increase after the system is expanded. This will also bring economic benefits. This shows that the objective function of [26] is not necessarily complete. Therefore, we emphasise the defense effect rather than the economic cost, whereas from the viewpoint of the planner, the objective is to minimize the load shedding of the planning system caused by an attack. The decision variables are the constructed candidate transmission lines and generators, which are described by binary variables.

The building of the upper-level model ensures that the actual power flow of transmission lines in the planning system does not exceed the limit after the planning system is attacked by CCPA determined by the middle-level model and, at the same time, experiences the optimal scheduling determined by the lower-level model.

The upper-level model can be expressed as:

$$\min \sum_{d \in \Omega_D} S_c \tag{1}$$

which is subject to:

$$\sum_{l\in\Omega'_{\mathrm{L}}} x_{\mathrm{L}-l}C_{\mathrm{L}-l} + \sum_{g\in\Omega'_{\mathrm{G}}} x_{\mathrm{G}-g}C_{\mathrm{G}-g} \leqslant C_{\mathrm{total}} \tag{2}$$

$$\sum_{g\in\Omega_{\mathrm{G}}\cup\Omega'_{\mathrm{G}},g\in\Omega_{\mathrm{G}_b}} P_g - \sum_{l\in\Omega_{\mathrm{L}}\cup\Omega'_{\mathrm{L}},i=b} F_l + \sum_{l\in\Omega_{\mathrm{L}}\cup\Omega'_{\mathrm{L}},j=b} F_l - \sum_{d\in\Omega_{\mathrm{D}}} \boldsymbol{K}(b,d)(L_d - S_d) = 0,\ b\in\Omega_{\mathrm{B}} \tag{3}$$

$$F_l = B_l(\theta_i - \theta_j)v_{\mathrm{L}-l},\ l\in\Omega_{\mathrm{L}} \tag{4}$$

$$F_l = B_l(\theta_i - \theta_j)x_{\mathrm{L}-l},\ l\in\Omega'_{\mathrm{L}} \tag{5}$$

$$\sum_{d\in\Omega_{\mathrm{D}}} S_{\mathrm{d}} = \sum_{d\in\Omega_{\mathrm{D}}} S_{\mathrm{c}} + \sum_{d\in\Omega_{\mathrm{D}}} S_{\mathrm{f}} \tag{6}$$

$$\theta_b^{\min} \leqslant \theta_b \leqslant \theta_b^{\max},\ b\in\Omega_{\mathrm{B}} \tag{7}$$

$$\theta_{\mathrm{r}} = 0 \tag{8}$$

$$-F_l^{\max} \leqslant F_l \leqslant F_l^{\max},\ l\in\Omega_{\mathrm{L}}\bigcup\Omega'_{\mathrm{L}} \tag{9}$$

where *l, g, b,* and *d* are the indices of transmission lines, generators, buses, and load buses, respectively; S_{c} refers to the load shedding in the critical load; S_{f} refers to the load shedding in the flexible load; $x_{\mathrm{L}-l}$ and $x_{\mathrm{G}-g}$ are the binary variables indicating whether the candidate line *l* and the candidate generator *g* are built (1: built, 0: not built); C_{total} is the total investment cost (M$); L_d and S_d represent the initial load and the load shedding at load bus *d* (MW), respectively; F_l is the active power flow and $F_l^{\max}$ is the maximum capacity of line *l* (MW); B_l is the susceptance of line *l*. θ_b; $\theta_b^{\max}$, and $\theta_b^{\min}$ are the phase angle, the upper bound, and the lower bound for the phase angle, respectively; *i* and *j* are the sending bus and the receiving bus of line *l*; P_g and $P_g^{\max}$ represent the power output and the capacity of generator *g*, respectively; Ω_{L}, Ω_{G}, Ω'_{L}, Ω'_{G}, Ω_{B} and Ω_{D} are respectively the set of existing transmission lines, generators, candidate lines, candidate generators, buses, and load buses; Ω_{G_b} is the set of generators connected to bus *b*; θ_{r} represents the phase angle of reference bus; $\boldsymbol{K}$ is the bus-load incidence matrix; and $\boldsymbol{K}(b, d)$ denotes the (b, d) element of $\boldsymbol{K}$.

The objective function of the upper-level problem shown in (1) minimizes the load shedding in the planning system caused by CCPA. The inequality constraint (2) is used to limit the investment cost of CGTEP. In the process of modeling, DC power flow is adopted in the power flow model, and constraint (3) expresses the node power balance. The output of generators and load shedding are the scheduling results obtained by the operator misled by the false data when the system is attacked. After the scheduling of the operator, the actual load of bus *d* is $(L_d - S_d)$. Constraints (4) and (5) indicate that the active power flow of the attacked lines and the unconstructed candidate lines is zero. Constraint (6) represents load resources of planners including flexible and critical loads. Constraint (7) expresses the upper and lower bounds of bus voltage angles, and the angle of the reference bus is set to zero in constraint (8). Constraints (4)–(8) are about the power flow after the system is attacked by CCPA, while constraint (9) limits the active power flow of transmission lines to avoid the problem of cascading failure caused by overloaded lines.

B. The Middle-level Model

The middle-level model adopts the perspective of the attacker, and the most serious CCPA scheme is selected through optimization based on the defense planning strategy determined by the upper-level model. The objective function is to maximize the load shedding caused by an attack. The decision variables are: whether to launch a physical attack on generators and lines (described by binary variables), and the amount of false data injected into load measurements by LR attack (described by continuous variables).

The middle-level problem is formulated as follows:

$$\max \sum_{d\in\Omega_{\mathrm{D}}} S_d \tag{10}$$

which is subject to:

$$\sum_{d\in\Omega_{\mathrm{D}}} \Delta L_d = 0\,. \tag{11}$$

$$-\tau L_d \leqslant \Delta L_d \leqslant \tau L_d,\ d\in\Omega_{\mathrm{D}} \tag{12}$$

$$\sum_{l\in\Omega_{\mathrm{L}}} (1 - v_{\mathrm{L}-l})\mathrm{R}_{\mathrm{L}-l} + \sum_{g\in\Omega_{\mathrm{G}}} (1 - v_{\mathrm{G}-g})\mathrm{R}_{\mathrm{G}-g} \leqslant R^{\max} \tag{13}$$

$$-(N_{\mathrm{B}} - 1)v_{\mathrm{L}-l} \leqslant f_l \leqslant (N_{\mathrm{B}} - 1)v_{\mathrm{L}-l},\ l\in\Omega_{\mathrm{L}} \tag{14}$$

$$\sum_{l\in\Omega_{\mathrm{L}}} \boldsymbol{A}(b,l)f = \begin{cases} N_{\mathrm{B}} - 1, & b = r \\ -1, & b\in\Omega_{\mathrm{B}} \text{ and } b\neq r \end{cases} \tag{15}$$

where ΔL_d denotes the false data injected into load measurement at bus *d* and is positive if the measured load increases; The attack intensity of load measurement is denoted by τ; $v_{\mathrm{L}-l}$ and $v_{\mathrm{G}-g}$ are binary variables representing whether the existing line *l* and the existing generator *g* are attacked, respectively (1: not attacked, 0: attacked); $R_{\mathrm{L}-l}$ and $R_{\mathrm{G}-g}$ denote the resources required to attack the existing line *l* and existing generator *g*, respectively; $R^{\max}$ is the upper bound of resource attacking generators and lines; f_l is the single commodity flow [46] on the existing line *l* to check if there are isolated islands in the power system; N_{B} is the total number of buses; $\boldsymbol{A}$ is the bus-branch incidence matrix of the original system, and $\boldsymbol{A}(b, l)$ denotes the element of the *b*th row and *l*th column of $\boldsymbol{A}$.

Objective (10) corresponds to the objective function of maximizing the load shedding by an attack. The injected false data into all the measurements at load buses are summed to zero to ensure the active power balance of the system after the LR attack by (11). Constraint (12) limits the attacking amounts within certain ranges, in order to avoid excessive changes being detected by the operator. The total physical attack resource consumed by

the attacker is limited in (13). Constraints (14)–(15) apply the single commodity flow method to ensure that isolated islands will not be produced by the attack, because the attack scheme in this situation will be easily detected by the operator, causing the attack to fail [11].

C. The Lower-level Model

The lower-level model is used to optimize the scheduling of generators and load shedding based on load measurements by the information system (the obtained load measurements will be changed by LR attack) and topological data, when the defense planning strategy of the upper-level and attack scheme of the middle-level are given and implemented. The objective function is to minimize load shedding after the attack. The decision variables are the output of each generator and load shedding at every load bus. The lower-level problem is formulated by (16)–(25), as:

$$\min \sum_{d\in\Omega_{\mathrm{D}}} S_d \tag{16}$$

which is subject to:

$$\tilde{F}_l = B_l(\tilde{\theta}_i - \tilde{\theta}_j)v_{\mathrm{L}-l},\ l\in\Omega_{\mathrm{L}} \tag{17}$$

$$\tilde{F}_l = B_l(\tilde{\theta}_i - \tilde{\theta}_j)x_{\mathrm{L}-l},\ l\in\Omega'_{\mathrm{L}} \tag{18}$$

$$\sum_{g\in\Omega_{\mathrm{G}}\cup\Omega'_{\mathrm{G}},g\in\Omega_{\mathrm{G}_b}} P_g - \sum_{l\in\Omega_{\mathrm{L}}\cup\Omega'_{\mathrm{L}},i=b} \tilde{F}_l + \sum_{l\in\Omega_{\mathrm{L}}\cup\Omega'_{\mathrm{L}},j=b} \tilde{F}_l - \sum_{d\in\Omega_{\mathrm{D}}} \boldsymbol{K}(b,d)(L_d + \Delta L_d - S_d) = 0,\ b\in\Omega_{\mathrm{B}} \tag{19}$$

$$\tilde{\theta}_{\mathrm{r}} = 0 \tag{20}$$

$$-F_l^{\max} \leqslant \tilde{F}_l \leqslant F_l^{\max},\ l\in\Omega_{\mathrm{L}}\cup\Omega'_{\mathrm{L}} \tag{21}$$

$$0 \leqslant P_g \leqslant v_{\mathrm{G}-g}P_g^{\max},\ g\in\Omega_{\mathrm{G}} \tag{22}$$

$$0 \leqslant P_g \leqslant x_{\mathrm{G}-g}P_g^{\max},\ g\in\Omega'_{\mathrm{G}} \tag{23}$$

$$0 \leqslant S_d \leqslant L_d + \Delta L_d,\ d\in\Omega_{\mathrm{D}} \tag{24}$$

$$\theta_b^{\min} \leqslant \tilde{\theta}_b \leqslant \theta_b^{\max},\ b\in\Omega_{\mathrm{B}} \tag{25}$$

where $\tilde{F}_l$ and $\tilde{\theta}_b$ are the false active power flow of line l and false phase angle of bus b calculated by the operator using the measured load data after the power system is attacked by CCPA, respectively; $\tilde{\theta}_i$ and $\tilde{\theta}_j$ are the phase angle of bus i and bus j.

The minimum load shedding is determined by the operator after the attack in (16). Constraint (17) limits the active power flow of the existing transmission lines, in which the physically attacked lines are out of operation and the corresponding active power flow is 0. Constraint (18) limits the active power flow of the candidate lines whereas the active power flow of the unconstructed lines is zero. Constraint (19) is the node power balance, in which the load of the load bus d measured by the operator is $L_d + \Delta L_d$. The active power flow of the transmission line corresponding to constraints (17)–(19) is false. Constraint (20) limits the angle of the reference bus to 0. Constraints (21)–(25) limit the active power flow of all transmission lines, the outputs of the existing generators and candidate generators, the load shedding of load buses, and the voltage angle of the buses.

In fact, the successful physical attack to shut down the power system equipment, the successful intrusion of the information system, and the successful tampering of load measurement data are all high-impact and low-probability events. Thus, it is not cost-effective to significantly expand the power generation and transmission system to deal with such attacks. From the economic perspective, such cost is not effective.

IV. Solution Methodology

The optimization model proposed in this paper is for a mixed-integer optimization problem [27]. The Benders and C&CG (column and constraint generation) algorithms are two widely used solution methods. Since the C&CG algorithm is a unified approach to deal with optimality and feasibility, it is adopted to analyze the proposed tri-level model [28], [29].

The C&CG algorithm decomposes the tri-level optimization model into a master problem and a subproblem [27]–[29]. The master problem determines the optimal defense planning strategy under given attack schemes. The most serious CCPA scheme under the selected planning strategy is optimized by the subproblem, which corresponds to a bi-level optimization model. It can be solved via the transformation into a single-level optimization model by the Karush-Kuhn-Tucker (KKT) conditions [7].

The solution process based on the C&CG algorithm is described in the following steps and depicted in the flow chart in Fig. 4.

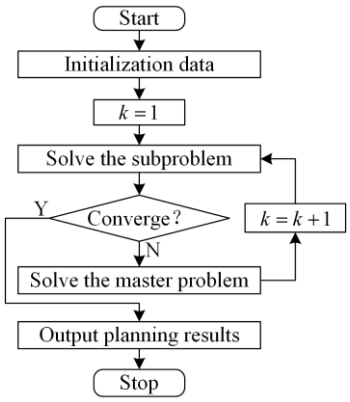

Fig. 4. Flow chart for solutions of the defense planning model.

Step 1: Input grid topology, generators, transmission lines, and other electrical parameters of the original power system, and the position, electrical and economic parameters of candidate lines and candidate generators. Set $U_{\mathrm{B}} = \sum_{d\in\Omega_{\mathrm{D}}} L_d$, $L_{\mathrm{B}} = 0$, where U_{B} means upper bound and L_{B} means lower bound. The iteration counter k =1. Initialize the convergence accuracy ε and the optimal decision variable vectors $\boldsymbol{X}_{\mathrm{L}}^{(k)} = [x_{\mathrm{L}-1}^{(k)}\ x_{\mathrm{L}-2}^{(k)}\ \cdots\ x_{\mathrm{L}-N'_{\mathrm{L}}}^{(k)}]^{\mathrm{T}}$ and $\boldsymbol{X}_{\mathrm{G}}^{(k)} = [x_{\mathrm{G}-1}^{(k)}\ x_{\mathrm{G}-2}^{(k)}\ \cdots\ x_{\mathrm{G}-N'_{\mathrm{G}}}^{(k)}]^{\mathrm{T}}$. Let $\boldsymbol{X}_{\mathrm{G}}^{(1)} = 0, \boldsymbol{X}_{\mathrm{L}}^{(1)} = 0,$ where

N'_{L} is the number of candidate lines and N'_{G} the number of candidate generators. The superscript (k) denotes the kth iteration.

Step 2: Substitute $\boldsymbol{X}_{\mathrm{G}}^{(k)}$ and $\boldsymbol{X}_{\mathrm{L}}^{(k)}$ into the subproblem to find the optimal CCPA scheme: $\boldsymbol{V}_{\mathrm{L}}^{(k)}=[v_{\mathrm{L}-1}^{(k)}\ v_{\mathrm{L}-2}^{(k)}\ \cdots\ v_{\mathrm{L}-N_{\mathrm{L}}}^{(k)}]^{\mathrm{T}}$, $\boldsymbol{V}_{\mathrm{G}-1}^{(k)}=[v_{\mathrm{G}-1}^{(k)}\ v_{\mathrm{G}-2}^{(k)}\ \cdots\ v_{\mathrm{G}-N_{\mathrm{G}}}^{(k)}]^{\mathrm{T}}$, and $\Delta\boldsymbol{L}^{(k)}=[\Delta L_1^{(k)}\ \Delta L_2^{(k)}\ \cdots\ \Delta L_{N_{\mathrm{D}}}^{(k)}]^{\mathrm{T}}$.

Let $U_{\mathrm{B}}=\min\left\{U_{\mathrm{B}},\sum_{d\in\Omega_{\mathrm{D}}}S_d^{(k)}\right\}$.

Step 3: Check, if $U_{\mathrm{B}}-L_{\mathrm{B}}\leqslant\varepsilon$, go to Step 6; otherwise go to Step 4.

Step 4: Solve $\boldsymbol{X}_{\mathrm{G}}^{(k+1)}$ and $\boldsymbol{X}_{\mathrm{L}}^{(k+1)}$ in the master problem by substituting $\boldsymbol{V}_{\mathrm{L}}^{(k)}$, $\Delta\boldsymbol{L}^{(k)}$ and $\boldsymbol{V}_{\mathrm{G}}^{(k)}$ as known quantities. Update L_{B} as $L_{\mathrm{B}}=\alpha$.

Step 5: Let $k=k+1$ and go to Step 2.

Step 6: Output $\boldsymbol{X}_{\mathrm{G}}^{(k)}$, $\boldsymbol{X}_{\mathrm{L}}^{(k)}$ and other results of the model.

V. Case Studies

The modified IEEE RTS-79 test system is used to illustrate the effectiveness of the proposed model. Figure 5 shows the diagram of the system, which consists of 24 buses, 17 load buses, 38 transmission lines, and 32 generators. The total generation capacity is 3405 MW and the peak load is 2850 MW. Detailed information about the RTS-79 system can be found in [30].

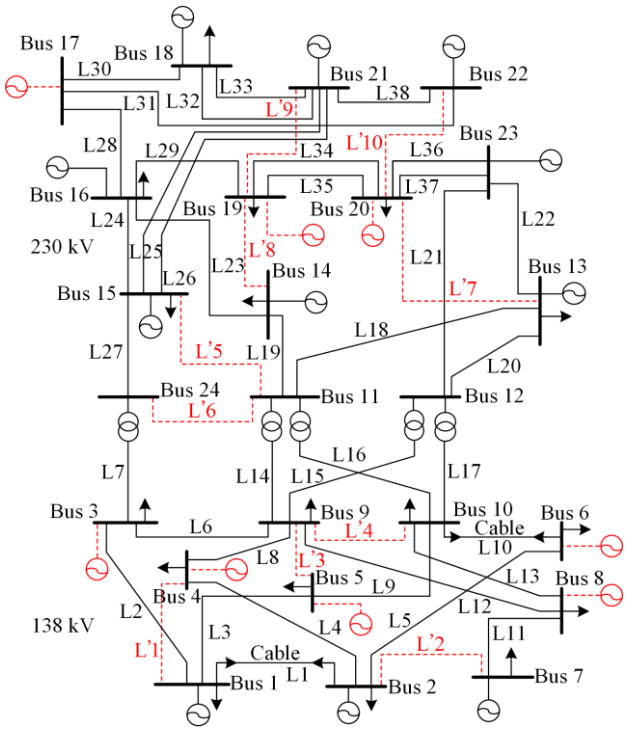

Fig. 5. The modified IEEE RTS-79 system.

In Fig. 5, the red dotted lines denote the candidate lines and the generators in red are the candidate generators. Electrical and economic parameters of the candidate lines and generators are shown in Table I and Table II, respectively. The candidate lines can be constructed as single-circuit or double-circuit lines, while each type of candidate generator can be built at every candidate bus for power plant construction.

TABLE I
Data of Candidate Transmission Lines

No.	Candidate line	Reactance (Ω/km)	Length (km)	Capacity (MW)	Investment (10^3\$/km)	Based voltage (kV)
1	1–4	0.392	150	30	163.49	138
2	2–7	0.392	150	25	163.49	138
3	5–9	0.392	150	40	163.49	138
4	9–10	0.392	150	25	163.49	138
5	11–15	0.412	300	65	459.90	230
6	11–24	0.412	300	50	459.90	230
7	13–20	0.412	300	100	459.90	230
8	14–19	0.412	300	30	459.90	230
9	19–21	0.412	300	75	459.90	230
10	20–22	0.412	300	50	459.90	230

TABLE II
Data of Candidate Generators

No	Capacity (MW)	Investment (\$)	Candidate buses for power plant construction
1	30	2.7×10^7	
2	75	7.5×10^7	3, 4, 5, 6, 8, 17, 19, 20
3	135	1.485×10^8	

In the case studies, the maximum investment cost C_{total} is $\$2\times10^8$. Bus 1 with a base capacity of 100 MVA is set to be the reference bus. The intensity of attack τ of load measurements in the LR attack is 50%. The upper bound of angle is $+\pi/2$ and the lower bound is $-\pi/2$. Suppose that the capacity of each existing transmission line drops to 70% of that of the original line. The convergence accuracy in the C&CG algorithm is set to $\varepsilon=10^{-6}$.

In the actual power system, different lines and generators encounter distinctive physical attacks because of the geographical locations and other factors. To simplify the case studies, this paper assumes that the physical attack resource required to attack any lines or generators successfully is 1 and the maximum physical attack resource $R^{\max}$ is also 1.

The studies are implemented on a PC with 3.40 GHz Intel Core i5-7500 and 8 GB RAM. The MILP model is analyzed by Gurobi with Yalmip toolbox in Matlab 2020.

A. Analysis of Case Study Results

Case studies investigate the effectiveness of the proposed tri-level defense planning model based on CGTEP to defend the power system against CCPA. Seven cases are conducted and shown in Table III.

Cases 1–4 consider either the LR attack or the physical attacks, while Cases 5–7 consider the CCPA. For example, Case 7 deals with the LR attack, line attack, and generator attack.

TABLE III
ATTACKS OF EACH CASE STUDY

Cases	LR attack	Line attack	Generator attack
1			√
2		√	
3	√		
4		√	√
5	√		√
6	√	√	
7	√	√	√

Performance of the conventional hardening strategy against the attacks in Table III is also assessed for comparison purposes. Based on this, Table IV shows the optimal results of the seven cases using the CGTEP defense strategy. In Table IV, L'x indicates the newly built transmission lines and the number of candidate transmission lines listed in Table I. For example, L'8 denotes that transmission line 14-19 is built. Similarly, G'x denotes the newly built generators and the number of candidate generators listed in Table II, whereas the numbers in the bracket are the bus numbers connected to it. For example, G'2(6, 8) denotes that two 75 MW generators are built at bus 6 and bus 8, with one for each bus.

TABLE IV
OPTIMAL RESULTS OF DIFFERENT CASES BY THE CGTEP STRATEGY

Cases	Load shedding before CGTEP (MW)	Load shedding after CGTEP (MW)	Built transmission lines	Built generators
1	0	0		
2	13.50	0	L'5	G'1(5, 6, 17, 19)
3	63.41	0	L'1; L'3; L'4; L'5	G'3(6)
4	13.50	0	L'5	G'1(5, 6, 17, 19)
5	112.14	0	L'3; L'5; L'8	G'3(6)
6	345.51	0	L'1; L'2; L'4; L'5	G'1(3, 6, 8); G'2(6)
7	345.51	6.50	L'8	G'1(3); G'2(6, 8)

Some observations from Table IV are given below.

1) Results of Cases 1 and 2 show that the load shedding caused by generator attack is smaller than that by line attack. This is because, for the modified IEEE-RTS system, the adequacy of transmission capacity is poorer than that of the generation capacity.

2) Cases 1–6 show that the load shedding caused by the single-type attack, whether it is the LR, line, or generator attack, is significantly less than that caused by the coordinated attack.

3) The load shedding of Cases 6 and 7 before CGTEP are the same. This result shows that a line attack causes much more damage than a generator attack. Thus, under the circumstance of $R^{\max}=1$, the priority of the physical attack strategy in the coordinated attack of Case 7 is to perform the line attack. There is no need to perform the generator attack because no additional damage will be induced. Consequently, both attack strategies result in the same load shedding results. Note that the load shedding after CGTEP in Case 7 is greater than that in Case 6 at the same maximum investment cost. This indicates that the coordinated attacks comprising the generator, line, and LR attacks are more serious than those of the line and LR attacks.

4) The load shedding after applying CGTEP is zero or close to zero. The results demonstrate that the proposed defense planning based on CGTEP successfully defends the power system against the physical attack, the LR attack, and CCPA.

Performance comparison between the CGTEP strategy and the hardening strategy can be obtained from Tables IV and V. It can be seen from Cases 1, 2, and 4 in Tables IV and V that both defense strategies are effective in defending the individual physical attacks. They all result in zero load shedding. However, this is not the case for LR attacks or coordinated attacks. This is shown in the results of Cases 3, 5, 6, and 7, although the load shedding is reduced but not eliminated by the hardening strategy. In contrast, the CGTEP strategy can lower the load shedding to zero under the LR attack and most coordinated attacks. The only exception is the CCPA with all three attacks. Nevertheless, the load shedding is significantly reduced in comparison to the hardening strategy. Therefore, it can be concluded that the proposed defense plan is much more effective than the hardening strategy in dealing with CCPA.

Table VI is a comparison of new lines and generators with and without flexible load. As can be seen, the number of newly added units and lines decreases after considering flexible load. Accordingly, the cost of CGTEP also decreases.

TABLE V
OPTIMAL RESULTS OF DIFFERENT CASES BY THE CONVENTIONAL HARDENING STRATEGY

CASES	Load shedding before hardening (MW)	Load shedding after hardening (MW)	Hardened transmission lines	Hardened generators
1	0	0		
2	13.50	0	L5; L10	
3	63.41	63.41		
4	13.50	0	L5; L10	
5	112.14	67.88		G1; G2; G3; G4; G5; G6; G7; G8; G9; G10; G11; G22; G23; G32
6	345.51	63.41	All transmission lines	
7	345.51	69.37	L5; L7; L8; L9; L10; L13; L14; L15; L16; L17; L18; L20; L21; L22; L27	G1; G2; G3; G4; G5; G6; G7; G8; G9; G10; G11; G23; G32

TABLE VI
OPTIMAL RESULTS OF DIFFERENT CASES BY THE PROPOSED CGTEP STRATEGY

Cases	Load shedding after CGTEP (MW)		Built transmission lines		Built generators	
	Without FL	With FL	Without FL	With FL	Without FL	With FL
1	0	0				
2	0	0	L'5		G'1(5, 6, 17, 19)	G'1(5, 17, 19)
3	0	0	L'1; L'3; L'4; L'5		G'3(6)	G'3(6)
4	0	0	L'5		G'1(5, 6, 17, 19)	G'1(5, 6, 17, 19)
5	0	0	L'3; L'5; L'8		G'3(6)	G'3(6)
6	0	0	L'1; L'2; L'4; L'5	L'4	G'1(3, 6, 8); G'2(6)	G'1(3, 6, 8); G'2(6)
7	6.50	0	L'3		G'1(3); G'2(6, 8)	G'1(3); G'2(6, 8)

B. Analysis of Maximum Investment Cost on CGTEP Strategy

This section investigates the impact of maximum investment cost and the attack intensity on the proposed CGTEP strategy. Table VII shows the impact of investment cost on load shedding of the planning system.

The cost of hardening is about 10% of the cost of the corresponding generator or transmission line. System parameters in the simulation include the costs of a generator at 10^6\$/MW and a line at 4×10^5\$/km. The cost of hardening a transformer branch is set to $\$2\times10^6$.

It is observed from Table VII that, the load shedding in each case declines along with the rise of maximum investment cost. When the maximum investment is higher than the proposed planning system enables zero load-shedding against all the attack schemes. It is worth noting that the smaller the load shedding caused by attacks, the stronger the system's ability to defend against attacks. Zero load shedding indicates that the planning system can effectively defend against attacks by reducing the load shedding to 0 after being attacked. This means that CGTEP can effectively defend the power system against CCPA provided sufficient funds are available.

TABLE VII
IMPACT OF INVESTMENT COST ON LOAD SHEDDING OF THE PLANNING SYSTEM

Cases	Maximum investment cost ($)					
	0	100	200	300	400	500
1	0	0	0	0	0	0
2	1.35×10^7	0	0	0	0	0
3	6.341×10^7	0	0	0	0	0
4	1.35×10^7	0	0	0	0	0
5	1.1214×10^8	0	0	0	0	0
6	3.4551×10^8	5.15×10^7	0	0	0	0
7	3.4551×10^8	5.446×10^7	6.5	0	0	0

C. Impact of $R^{\max}$ and τ on Attack Effects and Defense Planning Results

The load shedding of the original system and that of the planning system of Case 7 caused by the most vicious attack scheme are recorded in Fig. 6 considering a different physical attack resource $R^{\max}$ and attack intensity of load measurement τ in the LR attack. It is seen from Fig. 6 that the load shedding increases along with the increase of $R^{\max}$ as well as the rise of τ. In particular, the load shedding increases substantially when $R^{\max}$ increases.

For fixed τ, the increase of $R^{\max}$ allows the rise in the number of line attacks and generator attacks. As a result, more load shedding is caused by the coordinated attack. At the same time, the capacity of newly constructed lines and generators must be raised adequately to defend against the attacks. However, because of the limitation of the total investment in the optimization process, the capacity is limited. This leads to the increase in the load shedding of the planning system.

For fixed $R^{\max}$, larger τ means that a wider range of false data are injected into the load measurements. Thus, system operators are more likely to be misled with false information. Consequently, the load shedding of both systems caused by the attack tends to rise.

Under different $R^{\max}$ and τ, the load shedding of the planning system caused by CCPA is significantly lower than that of the original system. This further demonstrates that the proposed defense planning strategy based on CGTEP in this paper is effective in coping with CCPA.

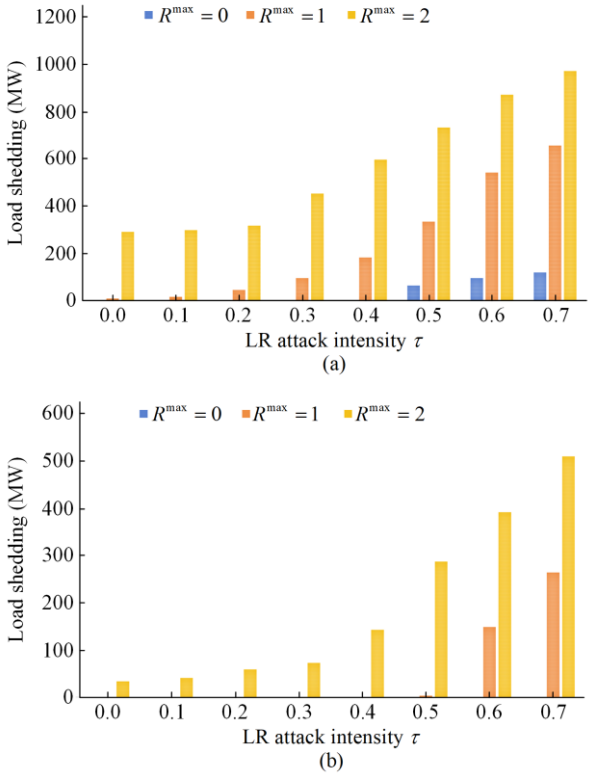

Fig. 6. Impact of $R^{\max}$ and τ on load shedding caused by the attack. (a) The original system. (b) The defense planning system.

VI. Conclusion

In this paper, a coordinated defense planning model against CCPA is proposed. The CGTEP based tri-level model is optimized from the perspectives of the planner, attacker, and operator. The model solutions including the master problem and the subproblem solved by the C&CG algorithm are presented. Simulation results on the modified IEEE RTS-79 test system demonstrate:

1) CCPA consisting of LR, line and generator attacks is a much more serious attack scheme than the single attack or the combination of LR and line attacks. It leads to the largest load reduction in the power system, and requires higher investment costs to address.

2) The proposed defense planning strategy based on CGTEP is effective for the power system to resist CCPA.

3) Adding flexible load to planners' resources is effective for defending against network physical coordinated attacks on the power system and can save costs.

4) Load measurement in an LR attack, the attack intensity of τ, and the physical attack resource $R^{\max}$ have important influence on the load reduction and system planning caused by attacks.

Acknowledgment

Not applicable.

Authors' Contributions

Peiyun Li: conceptualization, methodology, validation, formal analysis, writing-original draft, and writing-review & editing. Jian Fu: conceptualization, methodology, validation, and writing-review & editing. Kaigui Xie: conceptualization, writing-review & editing, and supervision. Bo Hu: supervision. Yu Wang: validation and writing-review & editing. Changzheng Shao: Supervision and writing-review & editing. Yue Sun: formal analysis. Wei Huang: formal analysis. All authors read and approved the final manuscript.

Funding

This work is partially supported by the National Natural Science Foundation of China (No. 52022016).

Availability of Data and Materials

Not applicable.

Declarations

Competing interests: The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this article.

Authors' Information

Peiyun Li received the B.S. degree in electrical engineering and its automation from Hunan University, Changsha, China, in 2021 and is pursuing the M.S. degree in electrical engineering from Chongqing University. Her current research interests include cyber-physical attack and its defense model.

Jian Fu received the M.S. degree with the School of Electrical Engineering, Chongqing University, Chong-

qing, China. His research interests include power system reliability and power system planning and optimal operation. He is currently working at State Grid Chengdu Power Supply Company, State Grid Sichuan Electric Power Co., Ltd., Chengdu, China.

Kaigui Xie received a Ph.D. degree in electrical engineering from Chongqing University, China, in 2001. He is currently working as a full professor at the School of Electrical Engineering in Chongqing University. His main research interests include power system reliability, planning, and analysis.

Bo Hu received his Ph.D. degree in electrical engineering from Chongqing University, Chongqing, China, in 2010. Currently, he is a professor in the School of Electrical Engineering at Chongqing University, China. His research interests include power system reliability, and parallel computing techniques in power systems.

Yu Wang received the Ph.D. degree in electrical engineering from Nanyang Technological University, Singapore. He is currently working as a professor at the School of Electrical Engineering at Chongqing University. His main research interests include power system planning.

Changzheng Shao received the B.S. degree in electrical engineering from Shandong University and the Ph. D degree in electrical engineering from Zhejiang University in 2015 and 2020, respectively. He is currently an assistant professor at Chongqing University, Chongqing, China. His research interests include the operation optimization and reliability evaluation of the integrated energy system.

Yue Sun received a M.S. degree with the School of Electrical Engineering, Chongqing University, Chongqing, China. His research interests include power system reliability and power system planning and optimal operation. He is currently working at China Yangtze Power Co., Ltd, Yichang, China.

Wei Huang is working toward a Ph.D. degree with the School of Electrical Engineering, Chongqing University, Chongqing, China. His current research interests include Power system reliability and power system planning and optimal operation.

REFERENCES

[1] J. E. Sullivan and D. Kamensky, "How cyber-attacks in Ukraine show the vulnerability of the US power grid," *The Electricity Journal*, vol. 30, no. 3, pp. 30-35. Apr. 2017.

[2] J. M. Arroyo, "Bilevel programming applied to power system vulnerability analysis under multiple contingencies," *IET Generation*, *Transmission &. Distribution*, vol. 4, no. 2, pp. 178-190, Feb. 2010.

[3] S. Sayyadipour, G. R. Yousefi, and M. A. Latify, "Mid-term vulnerability analysis of power systems under intentional attacks," *IET Generation*, *Transmission & Distribution*, vol. 10, no. 15, pp. 3745-3755, Nov. 2016.

[4] J. Yan, H. He, and X. Zhong *et al*., "Q-learning-based vulnerability analysis of smart grid against sequential topology attacks," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 1, pp. 200-210, Jan. 2017.

[5] Y. Wang and R. Baldick, "Interdiction analysis of electric grids combining cascading outage and medium-term impacts," *IEEE Transactions on Power Systems*, vol. 29, no. 5, pp. 2160-2168, Sept. 2014.

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

[7] Y. Yuan, Z. Li, and K. Ren, "Modeling load redistribution attacks in power systems," *IEEE Transactions on Smart Grid,* vol. 2, no. 2, pp. 382-390, Jun. 2011.

[8] X. Liu and Z. Li, "Local load redistribution attacks in power systems with incomplete network information," *IEEE Transactions on Smart Grid*, vol. 5, no. 4, pp. 1665-1676, Jul. 2014.

[9] Y. Xiang, Z. Ding, and Y. Zhang *et al*., "Power system reliability evaluation considering load redistribution attacks," *IEEE Transactions on Smart Grid*, vol. 8, no. 2, pp. 889-901, Mar. 2017.

[10] L. Che, X. Liu, and Z. Shuai *et al*., "Cyber cascades screening considering the impacts of false data injection attacks," *IEEE Transactions on Power Systems*, vol. 33, no. 6, pp. 6545-6556, Nov. 2018.

[11] L. Che, X. Liu, and Z. Li *et al*., "False data injection attacks induced sequential outages in power systems," *IEEE Tranactions on Power System*, vol. 34, no. 2, pp. 1513-1523, Mar. 2019.

[12] Z. Li, M. Shahidehpour, and A. Alabdulwahab *et al*., "Bilevel model for analyzing coordinated cyber-physical attacks on power systems," *IEEE Transactions on Smart Grid*, vol. 7, no. 5, pp. 2260-2272, Sept. 2016.

[13] Y. Xiang, L. Wang, and N. Liu, "Coordinated attacks on electric power systems in a cyber-physical environment," *Electric Power Systems Research*, vol. 149, pp. 156-168, Aug. 2017.

[14] A. Costa, D. Georgiadis, and T. Ng *et al*., "An optimization model for power grid fortification to maximize attack immunity," *International Journal of Electrical Power & Energy Systems*, vol. 99, pp. 594-602, Jul. 2018.

[15] H. Nemati, M. A. Latify, and G. R. Yousefi, "Coordinated generation and transmission expansion planning for a power system under physical deliberate attacks," *International Journal of Electrical Power & Energy Systems*, vol. 96, pp. 208-221, Mar. 2018.

[16] Y. Guo, L. Wang, and Z. Liu *et al*., "Reinforcement-learning-based dynamic defense strategy of multistage game against dynamic load altering attack," *In-*

ternational Journal of Electrical Power & Energy Systems, vol. 131, pp. 107-113, Oct. 2021.

[17] W. Yuan and B. Zeng, "Cost-effective power grid protection through defender-attacker-defender model with corrective network topology control," *Energy System*, vol. 11, pp. 811-837, Jul. 2019.

[18] H. Lei, S.Huang, and Y. Liu *et al*., "Robust optimization for microgrid defense resource planning and allocation against multi-period attacks," *IEEE Transactions on Smart Grid*, vol.10, no. 5, pp.5841-5850, Sept. 2019.

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

[20] L. Lai, M. Illindala, and K. Subramaniam, "A tri-level optimization model to mitigate coordinated attacks on electric power systems in a cyber-physical environment," *Applied Energy*, vol. 235, pp. 204-218, Feb. 2019.

[21] H. He, S. Huang, and Y. Liu *et al*., "A tri-level optimization model for power grid defense with the consideration of post-allocated DGs against coordinated cyber-physical attacks," *International Journal of Electrical Power & Energy Systems*, vol. 130, Sept. 2021.

[22] H. Nemati, M. A. Latify, and G. R. Yousefi, "Coordinated generation and transmission expansion planning for a power system under physical deliberate attacks," *International Journal of Electrical Power & Energy Systems*, vol. 96, pp. 208-221, Mar. 2018.

[23] M. Carrin, J. M. Arroyo, and N. Alguacil, "Vulnerability-constrained transmission expansion planning: a stochastic programming approach," *IEEE Transactions on Power Systems*, vol. 22, no. 4, pp. 1436-1445, Nov. 2007.

[24] H. Nemati, M. A. Latify, and G. R. Yousefi, "Tri-level transmission expansion planning under intentional attacks: virtual attacker approach-part I: formulation," *IET Generation*, *Transmission &. Distribution*, vol. 13, no.3, pp. 390-398, Feb. 2019.

[25] H. Nemati, M. A. Latify, and G. R. Yousefi, "Optimal coordinated expansion planning of transmission and electrical energy storage systems under physical intentional attacks," *IEEE Systems Journal*, vol. 14, no. 1, pp. 793-802, Mar. 2020.

[26] X. Liu, Z. Li, and Z. Li, "Optimal protection strategy against false data injection attacks in power systems," *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1802-1810, Jul. 2017.

[27] J. Alvarez Lopez, K. Ponnambalam, and V. H. Quintana, "Generation and transmission expansion under risk using stochastic programming," *IEEE Transactions on Power Systems*, vol. 22, no. 3, pp. 1369-1378, Aug. 2007.

[28] B. Zeng and L. Zhao, "Solving two-stage robust optimization problems using a column-and-constraint generation method," *Operation Research*. *Letters*, vol. 41, no. 5, pp. 457-461, Sept. 2013.

[29] C. Ruiz and A. J. Conejo, "Robust transmission expansion planning," *European Journal of Operation Research*, vol. 242, no. 2, pp. 390-401, Apr. 2015.

[30] P. M. Subcommittee, "IEEE reliability test system," *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-98, no. 6, pp. 2047-2054, Nov. 1979.