IEEE Access
Multidisciplinary ⁝ Rapid Review ⁝ Open Access Journal

Received December 16, 2018, accepted December 25, 2018, date of publication January 4, 2019, date of current version January 29, 2019.

Digital Object Identifier 10.1109/ACCESS.2018.2890604

Multilevel Programming-Based Coordinated Cyber Physical Attacks and Countermeasures in Smart Grid

MENG TIAN[1], (Member, IEEE), MINGJIAN CUI[2], (Senior Member, IEEE), ZHENGCHENG DONG[3], XIANPEI WANG[1], SHENGFEI YIN[2], (Member, IEEE), and LE ZHAO[1]

[1]Electronic Information School, Wuhan University, Wuhan 430072, China
[2]Department of Electrical Engineering, Southern Methodist University, Dallas, TX 75275, USA
[3]School of Electrical Engineering and Automation, Wuhan University, Wuhan 430072, China

Corresponding author: Mingjian Cui (mingjian.cui@ieee.org)

This work was supported by the National Natural Science Foundation of China under Grant 51707135 and Grant 51807143.

ABSTRACT Since the Ukraine blackout in 2015, coordinated cyber-physical attacks (CCPAs) have been emerging and are used to mask line outages in the smart grid. In this paper, we investigate the features of CCPAs and constitute the mathematic formulation with respect to topologies and electric parameters of a power grid before and after attacks. With the objective of maximizing the number of overloaded lines, a bilevel programming model is developed to describe the interaction between the adversary and the control center. The most damaging CCPA can be determined by transforming the developed bilevel model to a single mixed-integer linear programming problem using the Karush–Kuhn–Tucker conditions. Based on the features of the bilevel model, the countermeasure is expressed as a trilevel model with one leader and multiple followers. The implicit enumeration-based searching strategy is proposed to solve the trilevel model to identify the protected meters. Both the implementation of CCPAs and the effectiveness of the developed countermeasure are verified on the modified IEEE 14-bus system.

INDEX TERMS Bilevel programming, coordinated cyber physical attacks (CCPAs), trilevel programming, smart grid.

NOMENCLATURE

Sets and Indices:

$\boldsymbol{O}/d$	Bus set / bus index.
$\boldsymbol{G}/g$	Generation set / generation index.
$\boldsymbol{L}/l$	Transmission line set / transmission line index.

Variables:

$\boldsymbol{z}/\boldsymbol{z}_A$	Received meter measurement vector of control center before / after CCPAs.
$\boldsymbol{\theta}$	System state vector.
$\boldsymbol{F}/\boldsymbol{F}_A$	Received active power flow of control center before / after CCPAs.
$\boldsymbol{G}/\boldsymbol{G}_A$	Received generation output of control center before / after CCPAs.
$\boldsymbol{D}/\boldsymbol{D}_A$	Received load demand of control center before / after CCPAs.
S_d	Load shedding of bus d.
P_g	Output of generator g.
F_l	Power flow of line l.
$\boldsymbol{a}_D$	Injected data to demand measurements.
$\boldsymbol{a}_F$	Injected data to power flow measurements.
$\delta_{F,l}/\delta_{D,d}$	Indicators. If line l or bus d is attacked, $\delta_{F,l} = 1$ or $\delta_{D,d} = 1$; otherwise, both are set to 0.
$\gamma_{L,l}/\gamma_{D,d}$	Indicators. If line l or bus d is protected, $\gamma_{L,l} = 1$ or $\gamma_{D,d} = 1$; otherwise, both are set to 0.
k_l	Indicators. If line l overloads, $k_l = 1$; otherwise, $k_l = 0$.
μ_l	Lagrange multipliers associated with the power flow equation of line l.
λ_d	Lagrange multipliers associated with the power balance equation of load d.
$\underline{\kappa}_g/\overline{\kappa}_g$	Lagrange multipliers associated with lower and upper bounds for output of generation g.

$\underline{\omega}_l/\overline{\omega}_l$ Lagrange multipliers associated with lower and upper bounds for power flow of line l.

$\underline{\alpha}_d/\overline{\alpha}_d$ Lagrange multipliers associated with lower and upper bounds for load shedding of load d.

$\xi_g^{\underline{\kappa}}/\xi_g^{\overline{\kappa}}$ Additional binary variables associated with the complementary slackness conditions for the generation output constraints of generator g.

$\xi_l^{\underline{\omega}}/\xi_l^{\overline{\omega}}$ Additional binary variables associated with the complementary slackness conditions for power flow constraints of line l.

$\xi_d^{\underline{\alpha}}/\xi_d^{\overline{\alpha}}$ Additional binary variables associated with the complementary slackness conditions for the load shedding of bus d.

Parameters:

$\boldsymbol{H}/\boldsymbol{H}_A$ Received measurement Jacobin matrix of control center before / after CCPAs.

$\mathbf{SF}/\mathbf{SF}_A$ Received shifting factor matrix of control center before / after CCPAs.

$\mathbf{KD}/\mathbf{KD}_A$ Received bus-load incidence matrix of control center before / after CCPAs.

$\mathbf{KG}/\mathbf{KG}_A$ Received bus-generator incidence matrix of control center before / after CCPAs.

$N_d/N_l/N_g$ Number of buses / transmission lines / generations.

τ Maximum percentage of change for load measurement attacks.

C_g/C_{sd} Generation cost (in \$/MWh) of generator g / load shedding cost (in \$/MWh) of bus d.

B_{MVA} System MVA base.

γ Threshold for lines whose flows are closed to the rating.

x_l Reactance of line l.

D_d Maximal demand for bus d.

$P_g^{\min}$ / $P_g^{\max}$ Minimum / maximum output of generator g.

$F_l^{\max}$ Maximum power flow capacity of line l.

A_{dl} Element of network incidence matrix. A_{dl} is equal to 1 if bus d is the sending bus of line l; -1 if bus d is the receiving bus of line l; and 0 otherwise.

R_p/R_a Defend cost / attack cost.

Other notations are defined in the text.

I. INTRODUCTION

Cyber security and structural vulnerability are increasingly concerned issues in the smart grid [1]–[4], due to the wide introduction of information communication technologies to smart grid and intensive interconnection of regional power networks. For the former, adversaries can attack power systems (e.g., the Israe's Electric Authority was tampered by computer virus in 2016 [5]) by leveraging software bugs, failures, etc. For the latter, structure failures can seriously affect the security of smart grid. Furthermore, the outage of transmission lines or substations may cause cascading failures (e.g., the electrical blackout in Italy on September 28, 2003 [4]). Recently, a new type of cyber attacks, namely coordinated cyber physical attacks (CCPAs), is emerging due to the Ukraine blackout in 2015 [6].

Cyber security and structural vulnerability have been separately studied for a long time. In the area of cyber security, confidentiality, integrity, and availability (the CIA triad) are the basic high-level security objectives for the smart grid. As it is still challenging to enumerate all possible cyber attacks due to large-scale and complex structures of the smart grid, many research efforts have been taken on cyber attacks targeting the CIA [2]. For confidentiality attacks, Ismail *et al.* [7] formulated the attacks as a non-cooperative game and analyzed the behavior of one attacker and defender in the Advanced Metering Infrastructure. Targeting the integrity, false data injection attacks, which may lead to load shedding [8] and line overload [9], were proposed based on the traditional power system state estimation [10]. As the distributed denial-of-service (DDoS) attack is one of the most dangerous availability attacks, Ma *et al.* [11] modeled the interaction between providers and attackers as a Markov game to identify their optimal strategies.

Structural vulnerability analysis is also one of the most concerned topics in the smart grid. Yan *et al.* [12] utilized the Q-learning algorithm to identify grid vulnerability under sequential attacks. Nezamoddini *et al.* [13] developed an optimization model to determine the optimal investment decision for the resilient design of power systems against physical attacks. Alam *et al.* [14] proposed a new algorithm for multiple line outage identification using PMU (Phasor Measurement Unit) with bad data. After the emergency of complex network science [15], it is shown that structural features (e.g., small-world and scale-free networks) play a key role in the robustness of power grids [16]. For example, by modeling a power grid and supervisory control and data acquisition system as an interdependent network, Buldyrev *et al.* [4] found that a broader degree distribution increased the vulnerability of interdependent networks to random failures. Considering power flows in power grids, Salmeron *et al.* [17] proposed a bilevel programming model to identify critical system components under terrorist threat. Furthermore, the defender-attacker-defender model [18]–[20] is adopted to identify countermeasures.

Since line outages can be easily masked by cyber attacks, CCPAs attract increasing attention after the Ukraine blackout in 2015. It caused approximately 225,000 customers to lose power across areas [6]. In this blackout, the ON/OFF states of several circuit breakers are maliciously altered (i.e., physical attacks). The modified KillDisk and DDoS (i.e., cyber attacks) are coordinately used to erase the master boot record and frustrate the call center. It is still an open issue to model and defend against CCPAs in recent years. It is shown that CCPAs can be successfully constructed by exploiting RTU (Remote Terminal Unit) [21], [22] and PMU [23], [24], even when attackers can not obtain complete information of power systems [25], [26]. For example, Li *et al.* [21] and Liu *et al.* [23] demonstrated that single and multiple line outages can be masked by disrupting the PMU-based and RTU-based outage detections with false data, respectively. Brown and Demarco [26] found that attackers can cause system-wide unstable oscillations and trips of generators by altering only local control characteristics of customer loads. To better defend against CCPAs, multiple countermeasures have been proposed by researchers. Li *et al.* [21] constructed a single level optimization model to identify protected meters based on the single commodity method. Deng *et al.* [24] shown that CCPAs could be detected through known-secure PMUs and online tracking of the power system equivalent impedance. Soltan *et al.* [27] exploited linear algebra and graph theory to retrieve grid state information following CCPAs. It should be noted that CCPAs also exist in other cyber physical systems [28], [29]. However, the aforementioned strategies do not consider the interaction between defenders and adversaries. In addition, when overloaded lines are triggered under abnormal conditions, a cascading failure blackout may occur. Hence, the worst-case scenario should be considered if adversaries aim at maximizing the number of overloaded lines through CCPAs.

In the current research of CCPAs, physical attacks are used to trip transmission lines. Simultaneously, undetectable attacks [30] are exploited to mask physical attacks for fear of being detected by power system state estimation. In this paper, we use the multilevel programming to model CCPAs and countermeasures. The major contributions of this paper are summarized as follows:

1) A new concise formulation of CCPAs is proposed based on measurements from the supervisory control and data acquisition (SCADA) system.

2) A bilevel programming model is developed to describe the interaction between the control center and adversaries aiming at maximizing the number of overloaded transmission lines. It is transformed to a single-level mixed-integer linear programming problem by using Karush-Kuhn-Tucker (KKT) conditions.

3) A trilevel programming model with one leader and multiple followers is developed to defend against CCPAs. The middle and lower levels of this model are transformed to a single level model according to KKT conditions. Then the implicit enumeration algorithm is utilized to identify protected meters.

The remainder of this paper is organized as follows. Section II describes undetectable attacks and the developed CCPAs. Section III presets the bilevel programming model for CCPAs. Section IV formulates the trilevel programming model to identify protected meters. Section V presents and analyzes the numerical results in the modified IEEE 14-bus system. Relevant conclusions and future work are summarized in Section VI.

II. ATTACK MODEL

A. UNDETECTABLE ATTACKS

A power grid can be represented as an undirected graph $G = (V, E)$, where V and E represent the set of system buses and transmission lines connecting system buses, respectively. In this paper, the widely used DC power flow model in SCADA is adopted [31], where only active power injections in buses and active power flows in lines are considered to estimate bus phase angles. The DC power flow model follows the linear relationship, given by:

$$z = \boldsymbol{H}\boldsymbol{\theta} + \boldsymbol{e}, \quad \boldsymbol{e} \sim \mathrm{N}(0, \Sigma_e) \tag{1}$$

where $z = (z_1, z_2, \cdots, z_m)^T$ is composed of active power flow and bus injection measurements from RTUs. $\boldsymbol{\theta} = (\theta_1, \theta_2, \cdots, \theta_n)^T$ is composed of voltage phase angles at all buses except the reference bus where the voltage phase angle is represented as 0. The measurement Jacobin matrix $\boldsymbol{H} \in \boldsymbol{R}^{m\times n}$ relates to the power system topology and branch reactance. $\boldsymbol{e}$ is the Gaussian measurement noise with a diagonal covariance matrix Σ_e. m and n represent the number of meter measurements and state variables, respectively.

To detect bad data caused by random disturbances in the communication medium, various algorithms (e.g., χ^2-test method [31]) have been developed based on the measurement residual vector defined as $\boldsymbol{r} = z - \boldsymbol{H}\hat{\boldsymbol{\theta}}$. For the DC power flow model, analog measurements and topology information can be tampered without being detected. It is assumed that original measurements z can pass the bad measurement detection. The malicious measurements $z_A = z + \boldsymbol{a}$ can also pass the bad measurement detection if the injected data $\boldsymbol{a}$ into measurements is a linear combination of the column vectors $\boldsymbol{H}$, i.e., $\boldsymbol{a} = \boldsymbol{H}\boldsymbol{c}$, where $\boldsymbol{a}$, named as a false data injection attack (FDIA), is the malicious injected data into measurements and $\boldsymbol{c}$ is an arbitrary nonzero vector [10]. The power grid topology is controlled by various switches and line breakers with the ON/OFF status represented as binary variables. If only ON/OFF statuses of switches and line breakers are tampered, they can be easily detected by bad data detection methods [31]. However, when ON/OFF statuses and meter measurements are simultaneously tampered with a well-matched formulation, the topology change cannot be detected by the control center, presuming that the power system operates normally. Without regard to the measurement noise, the following formulation for topology status-based undetectable attacks can be obtained and the attack framework of CCPAs is shown in Fig. 1.

Definition 1 ([32, Definition 2.2]): An attack to modify G to G_A with the attack vector $\boldsymbol{a}$ is considered to be undetectable if $z + \boldsymbol{a} \in \mathrm{Col}(\boldsymbol{H}_A)$ and $\forall z \in \mathrm{Col}(\boldsymbol{H})$, where $\boldsymbol{H}$ and $\boldsymbol{H}_A$ are the measurement matrices for G and G_A, respectively, $\mathrm{Col}(\boldsymbol{H})$ and $\mathrm{Col}(\boldsymbol{H}_A)$ are the column space of $\boldsymbol{H}$ and $\boldsymbol{H}_A$, respectively.

B. COORDINATED CYBER PHYSICAL ATTACKS

When a power system operates normally, measurements z received by the control center include the active power flow $\boldsymbol{F}$, generation output $\boldsymbol{G}$, and load demand $\boldsymbol{D}$. Without considering the measurement noise, measurements z are

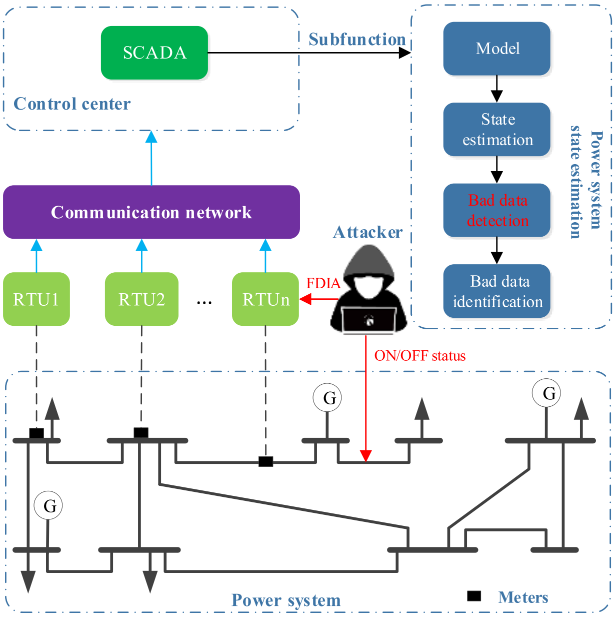


FIGURE 1. The attack framework of CCPAs.

satisfied by $z = \boldsymbol{H\theta}$, which can also be formulated as:

$$\boldsymbol{F} = \mathbf{SF} \times \mathbf{KG} \times \boldsymbol{G} - \mathbf{SF} \times \mathbf{KD} \times \boldsymbol{D} \tag{2}$$

When transmission lines are triggered by an adversary, it is assumed that the reactances of attacked lines become infinite to guarantee the topology integrity of the power system. Due to the CCPAs, the control center will obtain false topology statuses and measurements and presume that the system still operates normally. Actual measurements z_A received by the control center include the active power flow $\boldsymbol{F}_A$, generation output $\boldsymbol{G}_A$, and load demand $\boldsymbol{D}_A$. In the absence of the measurement noise, measurements z_A are satisfied by $z_A = \boldsymbol{H}_A\boldsymbol{\theta}$, which can also be formulated as:

$$\boldsymbol{F}_A = \mathbf{SF}_A \times \mathbf{KG}_A \times \boldsymbol{G}_A - \mathbf{SF}_A \times \mathbf{KD}_A \times \boldsymbol{D}_A \tag{3}$$

Without the mask of undetectable attacks, the attacked lines can be directly detected [31]. If the adversary wants to successfully break down the lines without being detected, two conditions should be satisfied, i.e., changing the topology statuses of failed lines from OFF to ON and tampering meter measurements by injecting data $\boldsymbol{a}_F$ and $\boldsymbol{a}_D$ to measurements $\boldsymbol{F}_A$ and $\boldsymbol{D}_A$, i.e., $\boldsymbol{F} = \boldsymbol{F}_A + \boldsymbol{a}_F$ and $\boldsymbol{D} = \boldsymbol{D}_A + \boldsymbol{a}_D$. Taking one line tripped as an example, the equations $\mathbf{KG} = \mathbf{KG}_A$ and $\mathbf{KD} = \mathbf{KD}_A$ hold. According to Definition 1, after injecting $\boldsymbol{a}_F$ and $\boldsymbol{a}_D$ to measurements, Eq. (2) should still hold, given by:

$$\boldsymbol{F}_A + \boldsymbol{a}_F = \mathbf{SF} \times \mathbf{KG} \times \boldsymbol{G} - \mathbf{SF} \times \mathbf{KD} \times (\boldsymbol{D}_A + \boldsymbol{a}_D) \tag{4}$$

Since generator output measurements cannot be attacked [8], namely $\boldsymbol{G} = \boldsymbol{G}_A$, the following formulation can be obtained based on (3) and (4):

$$\boldsymbol{a}_F = (\mathbf{SF} - \mathbf{SF}_A)\,(\mathbf{KG} \cdot \boldsymbol{G} - \mathbf{KD} \cdot \boldsymbol{D}) - \mathbf{SF} \cdot \mathbf{KD} \cdot \boldsymbol{a}_D \tag{5}$$

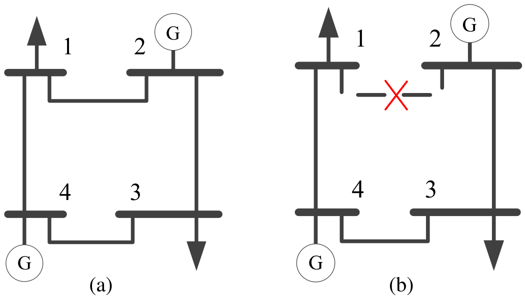


FIGURE 2. Topology of the 4-bus power system before and after attacks. Line connecting bus 1 and 2 is tripped by an adversary in (b).

Fig. 2 shows an example of one CCPA in a 4-bus power system before and after attacks. Reactances of all transmission lines are set to 1. Bus 2 is chosen as the reference bus. Fig. 2a shows the topology under the normal condition. It is assumed that the transmission line connecting bus 1 and 2 is triggered by an adversary shown in Fig. 2b. However, due to the CCPA, the control center will presume that the system still operates normally shown in Fig. 2a. Before attacks,

$$\mathbf{SF} = \begin{bmatrix} 0.75 & 0.25 & 0.5 \\ 0.25 & -0.25 & -0.5 \\ -0.25 & -0.75 & -0.5 \\ -0.25 & 0.25 & -0.5 \end{bmatrix},$$

$$\mathbf{KD} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix},$$

and

$$\mathbf{KG} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 1 \end{bmatrix}.$$

After attacks,

$$\mathbf{SF}_A = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ -1 & -1 & -1 \\ -1 & 0 & -1 \end{bmatrix}.$$

According to (5), the relations between $\boldsymbol{a}_F$ and $\boldsymbol{a}_D$ can be identified.

Generally, the bus injection measurements of zero injection buses in the network cannot be attacked. Attacks that cause load measurements to deviate far from their true values should be under suspicion. The complete formulation of CCPAs on determined lines can be described as follows:

$$\begin{aligned} \textstyle\sum_{d=1}^{N_d} a_{D,d} &= 0 - \tau D_d \le a_{D,d} \le \tau D_d, \quad \forall d \in \boldsymbol{O} \\ \boldsymbol{a}_F &= (\mathbf{SF} - \mathbf{SF}_A)\,(\mathbf{KG} \cdot \boldsymbol{G} - \mathbf{KD} \cdot \boldsymbol{D}) \\ &\quad - \mathbf{SF} \cdot \mathbf{KD} \cdot \boldsymbol{a}_D \end{aligned} \tag{6}$$

where $a_{D,d}$ is the dth element of $\boldsymbol{a}_D$. It is noted that the load redistribution attack without triggering lines [8] is a special category of the developed CCPAs.

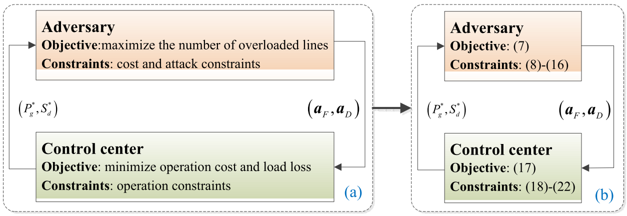

Adversary
Objective:maximize the number of overloaded lines
Constraints: cost and attack constraints
(P_g^*, S_d^*)
$(\boldsymbol{a}_F, \boldsymbol{a}_D)$
Control center
Objective: minimize operation cost and load loss
Constraints: operation constraints
(a)
Adversary
Objective: (7)
Constraints: (8)-(16)
(P_g^*, S_d^*)
$(\boldsymbol{a}_F, \boldsymbol{a}_D)$
Control center
Objective: (17)
Constraints: (18)-(22)
(b)

FIGURE 3. Bilevel model for CCPAs.

III. BILEVEL MODEL FOR CCPAS AND THE SOLUTION

A. BILEVEL PROGRAMMING MODEL

When an adversary manipulates the topology statuses and measurements, the control center would execute the false security-constrained economic dispatch (SCED) using the tampered topology statuses and measurements. As shown in Fig. 3a, the interaction between the adversary and control center can be constructed as a bilevel programming model. The upper level represents the adversary's action aiming at maximizing the number of overloaded lines with cost and attack constraints. The lower level represents the control center's response aiming at minimizing the operation cost and load loss with operation constraints.

The bilevel programming model can be formulated as follows.

$$\max\ \sum\nolimits_{l=1}^{N_l} k_l \tag{7}$$

$$\text{s.t.}\ \sum\nolimits_{d=1}^{N_d} a_{D,d} = 0 \tag{8}$$

$$-\tau D_d \le a_{D,d} \le \tau D_d, \quad \forall d \in \boldsymbol{O} \tag{9}$$

$$\boldsymbol{a}_F = (\mathbf{SF} - \mathbf{SF}_A)\,(\mathbf{KG}\cdot \boldsymbol{G} - \mathbf{KD}\cdot \boldsymbol{D}) - \mathbf{SF}\cdot \mathbf{KD}\cdot \boldsymbol{a}_D \tag{10}$$

$$a_{F,l} = 0 \iff \delta_{F,l} = 0, \quad \forall l \in \boldsymbol{L} \tag{11}$$

$$a_{D,d} = 0 \iff \delta_{D,d} = 0, \quad \forall d \in \boldsymbol{O} \tag{12}$$

$$\sum\nolimits_{d=1}^{N_d} \delta_{D,d} + 2\sum\nolimits_{l=1}^{N_l} \delta_{F,l} \le R_a \tag{13}$$

$$F_l' = (\mathbf{SF}_A\cdot \mathbf{KG})_l\, \boldsymbol{P}^* - (\mathbf{SF}_A\cdot \mathbf{KD})_l\left(\boldsymbol{D} - \boldsymbol{S}^*\right) \tag{14}$$

$$-\gamma F_{\max} \ge F_l',\ F_l' \ge \gamma F_{\max} \iff k_l = 1 \tag{15}$$

$$\delta_{F,l}, \delta_{D,d}, k_l \in \{0, 1\} \tag{16}$$

$$\left\{P_g^*, S_d^*\right\} = \arg\ \min \sum\nolimits_{g=1}^{N_g} C_g P_g + \sum\nolimits_{d=1}^{N_d} C_{sd} S_d \tag{17}$$

$$\text{s.t.}\quad F_l = B_{\text{MVA}}\frac{1}{x_l}\sum_{d\in \boldsymbol{O}} A_{dl}\theta_d, \quad \forall l \in \boldsymbol{L} \quad (\mu_l) \tag{18}$$

$$\sum_{g\in \boldsymbol{G}_d} P_g - \sum_{l\in \boldsymbol{L}} A_{dl}F_l + S_d = D_d + a_{D,d},\ \forall d \in \boldsymbol{O} \quad (\lambda_d) \tag{19}$$

$$P_g^{\min} \le P_g \le P_g^{\max}, \forall g \in \boldsymbol{G}\ \left(\underline{\kappa}_g, \overline{\kappa}_g\right) \tag{20}$$

$$-F_l^{\max} \le F_l \le F_l^{\max}, \quad \forall l \in \boldsymbol{L}\ \left(\underline{\omega}_l, \overline{\omega}_l\right) \tag{21}$$

$$0 \le S_d \le D_d + a_{D,d}, \quad \forall d \in \boldsymbol{O}\ \left(\underline{\alpha}_d, \overline{\alpha}_d\right) \tag{22}$$

In this bilevel model shown in Fig. 3b, the attack model is represented by the upper level problem (7)–(16) including variables $\boldsymbol{a}_F$, $\boldsymbol{a}_D$, k_l, $\delta_{F,l}$, $\delta_{D,d}$, and F_l'. The adversary aims at maximizing the number of overloaded lines, as shown in (7). Constraints (8)–(10) ensure that the false data can be injected to measurements without being detected. Constraints (11)–(12) are the logical relationship between the attack vector and used attack resources. Constraint (13) represents the maximum attack resources exploited by the adversary. Constraint (14) denotes the actual power flow F_l' in line l after attacks. Constraint (15) indicates whether the line is overloaded or not. The SCED model of the control center is represented by the lower level problem (17)–(22) including variables P_g, S_d, F_l and θ_d. The objective (17) is to minimize both the generation operation cost and the load loss. Constraints (18)–(22) are the operation conditions of power systems. As can be seen, the lower level is parameterized in terms of the upper-level decision variable $\boldsymbol{a}_D$. The upper level is parameterized by the lower-level decision variables P_g^* and S_d^*.

B. SOLUTION METHODOLOGY

In the logical constraint (11), the symbol '$\iff$' represents the necessary and sufficient conditions. If $a_{F,l} = 0$, then $\delta_{F,l} = 0$; and if $\delta_{F,l} = 0$, then $a_{F,l} = 0$. The constraint can be linearized as follows:

$$\begin{cases} a_{F,l} \le \delta_{F,l}M \\ a_{F,l} \ge -\delta_{F,l}M \\ a_{F,l} + (-M - \varepsilon)\,\delta_{L,l}' \ge -M \\ a_{F,l} + (M + \varepsilon)\,\delta_{L,l}'' \le M \\ \delta_{L,l}' + \delta_{L,l}'' - \delta_{F,l} = 0 \\ \delta_{L,l}', \delta_{L,l}'' \in \{0, 1\} \end{cases} \tag{23}$$

where M and ε are the sufficiently large and small positive constants, respectively. $\delta_{L,l}'$ and $\delta_{L,l}''$ are auxiliary binary variables, respectively.

Similarly, the logical constraint (12) can be linearized by increasing auxiliary binary variables $\delta_{D,l}'$ and $\delta_{D,l}''$, given by:

$$\begin{cases} a_{D,d} \le \delta_{D,d}M \\ a_{D,d} \ge -\delta_{D,d}M \\ a_{D,d} + (-M - \varepsilon)\,\delta_{D,d}' \ge -M \\ a_{D,d} + (M + \varepsilon)\,\delta_{D,d}'' \le M \\ \delta_{D,d}' + \delta_{D,d}'' - \delta_{D,d} = 0 \\ \delta_{D,d}', \delta_{D,d}'' \in \{0, 1\} \end{cases} \tag{24}$$

For the logical constraint (15), if $-\gamma F_{\max} \ge F_l'$ or $F_l' \ge \gamma F_{\max}$, then $k_l = 1$; and if $k_l = 1$, then $-\gamma F_{\max} \ge F_l'$ or $F_l' \ge \gamma F_{\max}$. It can be linearized by increasing auxiliary binary variables k_l' and k_l'', given by:

$$\begin{cases} F_l' - \gamma F_{\max} \le Mk_l' - \varepsilon\left(1 - k_l'\right) \\ F_l' - \gamma F_{\max} \ge -M\left(1 - k_l'\right) \\ F_l' + \gamma F_{\max} \ge -Mk_l'' + \varepsilon\left(1 - k_l''\right) \\ F_l' + \gamma F_{\max} \le M\left(1 - k_l''\right) \\ k_l = k_l' + k_l'' \\ k_l', k_l'' \in \{0, 1\} \end{cases} \tag{25}$$

If the objective and constraints in the lower level of a bilevel programming model are linear and convex, a major approach to solve the bilevel optimization is to merge the upper and lower levels into one-single-level problem by using either the KKT conditions or strong duality theorem. Although the strong duality theorem is more efficient in some physical attack problems for large systems [33], it is not suitable for our proposed bilevel model. Since the upper-level decision variables $\boldsymbol{a}_D$ are continuous, the strong duality equality in strong duality theorem cannot be linearized. The Benders decomposition method is also adopted to solve bilevel problems [34]. However, the variables in the objective (7) are binary, which means that the partial derivative of the objective (7) with respective to the objective (17) does not exist. Hence, the KKT conditions are used to replace the lower level (17)–(22) and the Fortuny-Amat and McCarl method [35] is adopted to linearize the nonlinear complementary slackness conditions in KKT conditions. Finally, the KKT conditions of the lower level are obtained as follows.

$$\textstyle\sum_{l\in \boldsymbol{L}} \frac{1}{x_l} B_{\mathrm{MVA}} \mu_l A_{dl} = 0,\ d \in \boldsymbol{O} \tag{26}$$

$$C_g - \lambda_d|_{g\in \boldsymbol{G}_d} - \underline{\kappa}_g + \overline{\kappa}_g = 0,\ g \in \boldsymbol{G} \tag{27}$$

$$-\mu_l + \textstyle\sum_{d\in \boldsymbol{O}} \lambda_d A_{dl} - \underline{\omega}_l + \overline{\omega}_l = 0,\ l \in \boldsymbol{L} \tag{28}$$

$$C_{sd} - \lambda_d - \underline{\alpha}_d + \overline{\alpha}_d = 0,\ d \in \boldsymbol{O} \tag{29}$$

$$\underline{\kappa}_g \le M\xi_g^{\underline{\kappa}},\ g \in \boldsymbol{G} \tag{30}$$

$$P_g - P_g^{\min} \le M\left(1 - \xi_g^{\underline{\kappa}}\right),\ g \in \boldsymbol{G} \tag{31}$$

$$\overline{\kappa} \le M\xi_g^{\overline{\kappa}},\ g \in \boldsymbol{G} \tag{32}$$

$$P_g^{\max} - P_g \le M\left(1 - \xi_g^{\overline{\kappa}}\right),\ g \in \boldsymbol{G} \tag{33}$$

$$\underline{\omega}_l \le M\xi_l^{\underline{\omega}},\ l \in \boldsymbol{L} \tag{34}$$

$$F_l + F_l^{\max} \le M\left(1 - \xi_l^{\omega}\right),\ l \in \boldsymbol{L} \tag{35}$$

$$\overline{\omega}_l \le M\xi_l^{\overline{\omega}},\ l \in \boldsymbol{L} \tag{36}$$

$$F_l^{\max} - F_l \le M\left(1 - \xi_l^{\overline{\omega}}\right),\ l \in \boldsymbol{L} \tag{37}$$

$$\underline{\alpha}_d \le M\xi_d^{\underline{\alpha}},\ d \in \boldsymbol{O} \tag{38}$$

$$S_d \le M\left(1 - \xi_d^{\underline{\alpha}}\right),\ d \in \boldsymbol{O} \tag{39}$$

$$\underline{\alpha}_d \le M\xi_d^{\underline{\alpha}},\ d \in \boldsymbol{O} \tag{40}$$

$$D_d + a_{D,d} - S_d \le M\left(1 - \xi_d^{\underline{\alpha}}\right),\ d \in \boldsymbol{O} \tag{41}$$

$$\xi_g^{\underline{\kappa}} + \xi_g^{\overline{\kappa}} \le 1,\ g \in \boldsymbol{G} \tag{42}$$

$$\xi_l^{\underline{\omega}} + \xi_l^{\overline{\omega}} \le 1,\ l \in \boldsymbol{L} \tag{43}$$

$$\xi_d^{\underline{\alpha}} + \xi_d^{\overline{\alpha}} \le 1,\ d \in \boldsymbol{O} \tag{44}$$

$$\xi_g^{\underline{\kappa}}, \xi_g^{\overline{\kappa}}, \xi_l^{\underline{\omega}}, \xi_l^{\overline{\omega}}, \xi_d^{\underline{\alpha}}, \xi_d^{\overline{\alpha}} \in \{0, 1\} \tag{45}$$

$$\underline{\kappa}_g, \overline{\kappa}_g, \underline{\omega}_l, \overline{\omega}_l, \underline{\alpha}_d, \overline{\alpha}_d \ge 0 \tag{46}$$

where $\boldsymbol{G}_d$ is the set of generators connecting to bus d. Constraints (26)–(29) are the dual feasibility constraints. Constraints (30)–(44) express the complementary slackness conditions. Note that all the constraints are linear. Considering the primary feasibility conditions (18)–(22), the bilevel optimization can be transformed to a single-level mixed-integer linear programming problem as follows.

$$\begin{cases} \max\ \ \sum_{l=1}^{N_l} k_l \\ s.t.\ (8)-(10),\ (13),\ (14) \\ (16),\ (18)-(46) \end{cases} \tag{47}$$

It should be noted that the solution of a bilevel problem can not be directly obtained by KKT conditions. Because the KKT conditions are not computing methods but equivalence conditions for the bilevel and single-level problems. The most computationally expensive operation in the procedure is to solve the single-level mixed-integer linear programming problem to optimality. In our implementation, the single-level mixed-integer linear programming problem is solved through the solver Cplex. The algorithm complexity is dependent on the computing method in Cplex. Although KKT conditions add more variables, they do not change the complexity of the computing method in Cplex.

IV. TRILEVEL MODEL FOR COUNTERMEASURE AND THE SOLUTION METHODOLOGY

A. TRILEVEL MODEL

In this paper, the protected bus d and line l are represented by binary variables $\gamma_{D,d}$ and $\gamma_{L,l}$, respectively. If a meter on bus d is protected, it can be expressed as $\gamma_{D,d} = 1$; otherwise, $\gamma_{D,d} = 0$. If a meter on line l is protected, it can be expressed as $\gamma_{L,l} = 1$; otherwise, $\gamma_{L,l} = 0$. Considering the limitation of defend cost R_p, the following formulation should be satisfied:

$$\textstyle\sum_{d=1}^{N_d} \gamma_{D,d} + \sum_{l=1}^{N_l} \gamma_{L,l} \le R_p \tag{48}$$

Moreover, if lines and buses are protected, corresponding meters cannot be attacked and can be described as:

$$\begin{cases} \gamma_{L,l} + \delta_{F,l} \le 1, & \forall l \in \boldsymbol{L} \\ \gamma_{D,d} + \delta_{D,d} \le 1, & \forall d \in \boldsymbol{O} \end{cases} \tag{49}$$

The developed bilevel model for CCPAs can identify the most damaging attack corresponding to a determined line l. If the defender of the power system wants to defend against CCPAs associated with all lines, the defender has to conflict with N_l non-cooperative adversaries, which can be modeled as a trilevel model with one leader and multiple followers shown in Fig. 4a. The upper level in the blue block represents the defender's countermeasure. The middle level in the yellow block represents the actions of N_l adversaries. The lower level in the green block is the SCED model of the control center.

The proposed bilevel model (7)–(22) for a determined attacked line l can be abstracted as:

$$\max_{y,k}\ F\left(k\right) \tag{50}$$

$$\text{s.t. } G\left(x_l^*, y, k\right) \le 0 \tag{51}$$

$$H\left(x_l^*, y, k\right) = 0 \tag{52}$$

$$k \in \{0, 1\} \tag{53}$$

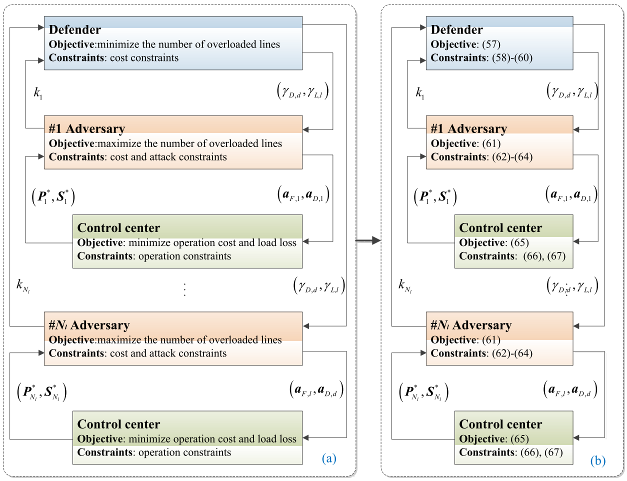

Defender
Objective:minimize the number of overloaded lines
Constraints: cost constraints
k_1
$(\gamma_{D,d},\gamma_{L,l})$
#1 Adversary
Objective:maximize the number of overloaded lines
Constraints: cost and attack constraints
$(\boldsymbol{P}_1^*,\boldsymbol{S}_1^*)$
$(\boldsymbol{a}_{F,1},\boldsymbol{a}_{D,1})$
Control center
Objective: minimize operation cost and load loss
Constraints: operation constraints
k_{N_l}
$(\gamma_{D,d},\gamma_{L,l})$
#N_l Adversary
Objective:maximize the number of overloaded lines
Constraints: cost and attack constraints
$(\boldsymbol{P}_{N_l}^*,\boldsymbol{S}_{N_l}^*)$
$(\boldsymbol{a}_{F,l},\boldsymbol{a}_{D,d})$
Control center
Objective: minimize operation cost and load loss
Constraints: operation constraints
(a)
Defender
Objective: (57)
Constraints: (58)-(60)
k_1
$(\gamma_{D,d},\gamma_{L,l})$
#1 Adversary
Objective: (61)
Constraints: (62)-(64)
$(\boldsymbol{P}_1^*,\boldsymbol{S}_1^*)$
$(\boldsymbol{a}_{F,1},\boldsymbol{a}_{D,1})$
Control center
Objective: (65)
Constraints: (66), (67)
k_{N_l}
$(\gamma_{D,d},\gamma_{L,l})$
#N_l Adversary
Objective: (61)
Constraints: (62)-(64)
$(\boldsymbol{P}_{N_l}^*,\boldsymbol{S}_{N_l}^*)$
$(\boldsymbol{a}_{F,l},\boldsymbol{a}_{D,d})$
Control center
Objective: (65)
Constraints: (66), (67)
(b)

FIGURE 4. Trilevel model for countermeasures.

$$x_l^* = \arg\min_{x} f_l(x) \tag{54}$$

$$\text{s.t. } g_l(x, y, k) \le 0 \tag{55}$$

$$h_l(x, y, k) = 0 \tag{56}$$

where x and y are the continuous variables in the upper and lower levels, respectively, k is the binary variable in the upper level. Eqs. (50) and (54) represent the adversary's and control center's objectives, respectively. Constraints (51) and (55) represent the inequality constraints in the upper and lower levels, respectively. Constraints (52) and (56) denote the equality constraints in the upper and lower levels, respectively. According to the definition of the model with one leader and multiple followers [36], the formulation of the trilevel model in Fig. 4a can be expressed as:

$$\min \sum_{i=1}^{N_l} F_i^*\left(\delta_{F,l}, \delta_{D,d}\right) \tag{57}$$

$$\text{s.t. } \sum_{d=1}^{N_d} \gamma_{D,d} + \sum_{l=1}^{N_l} \gamma_{L,l} \le R_p \tag{58}$$

$$\gamma_{L,l} + \delta_{F,l} \le 1, \quad \forall l \in \boldsymbol{L} \tag{59}$$

$$\gamma_{D,d} + \delta_{D,d} \le 1, \quad \forall d \in \boldsymbol{O} \tag{60}$$

$$F_i^*\left(\delta_{F,l}, \delta_{D,d}\right) = \arg\max_{y,k} F_i\left(\delta_{F,l}, \delta_{D,d}\right), \quad i = 1, \cdots, N_l \tag{61}$$

$$\text{s.t. } G_i\left(x^*, y, \delta_{F,l}, \delta_{D,d}\right) \le 0 \tag{62}$$

$$H_i\left(x^*, y, \delta_{F,l}, \delta_{D,d}\right) = 0 \tag{63}$$

$$\delta_{F,l}, \delta_{D,d} \in \{0, 1\} \tag{64}$$

$$x^* = \arg\min_{x} f_i(x) \tag{65}$$

$$\text{s.t. } \quad g_i(x, y) \le 0 \tag{66}$$

$$h_i(x, y) = 0 \tag{67}$$

where the defender and adversary have conflicting objectives shown in (57) and (61). The defender allocates R_p resources to minimize the number of overloaded lines, while the adversary has the opposite goal. As shown in Fig. 4b, the defend problem is represented by the upper level (57)–(60). Constraint (58) is the defend cost limitation. Constraints (59) and (60) determine meters that could be attacked by the adversary. The middle level (61)–(64) and lower level (65)–(67) represent the adversary's action and control center's SCED model. Both of them are the same as the bilevel model (7)–(22). Note that there is one upper model (57)–(60) and N_l bilevel models (61)–(67) for the trilevel model.

Algorithm 1 IE-Based Searching Strategy

```
1  Initialize: $\boldsymbol{P} \leftarrow \varnothing, \boldsymbol{I} \leftarrow \varnothing, l \leftarrow 1$, and $i \leftarrow 0$
2  while $l \le N_l$ do
3      Solve bilevel problem (61)–(67) corresponding to line $l$ and obtain the set of injected meters $\boldsymbol{S}_l$ composed of $\delta_{F,l}$ and $\delta_{D,d}$.
4      if bilevel problem (61)–(67) is feasible then
5          $\boldsymbol{I} = \boldsymbol{I} \cup \boldsymbol{S}_l$
6      else
7          finish this loop and start the next loop.
8      end
9  end
10 Count the number of bilevel models containing a specific meter in the set $\boldsymbol{I}$ and denote the meter with the largest number as $k$.
11 if multiple meters with the largest number then
12     randomly select one: $\boldsymbol{P} \leftarrow k$
13 end
14 $i \leftarrow i + 1$
15 if the $k$-th meter represents bus then
16     add the cut $\delta_{D,k} \le 0$ to the bilevel model (61)–(67).
17 else
18     add the cut $\delta_{F,k} \le 0$ to the bilevel model (61)–(67).
19 end
20 Check the defend resources $R_p$:
21 if $i \le R_p$ then
22     return to the step in Line 2–9.
23 else
24     exit and return the set of protected meters $\boldsymbol{P}$.
25 end
```

B. SOLUTION METHODOLOGY

Based on the aforementioned solution methodology in Section III-B, the trilevel model (57)–(67) can be transformed to a bilevel model by using KKT conditions to replace the lower level. However, the transformed bilevel model is an NP-hard problem, though there are only binary variables $\gamma_{L,l}$ and $\gamma_{D,d}$ in the upper level. Since the column-and-constraint generation method (C&CG method) was proposed in [37], it has become the mainstream method to solve trilevel problems. However, it requires that the lower-level problem includes both upper-level and middle-level variables [20]. In the proposed trilevel model, the variables $\gamma_{D,d}$ and $\gamma_{L,l}$ in the upper-level problem do not exist in the lower-level problem. Hence, the C&CG method is not suitable to solve the proposed trilevel model in this paper. To identify protected meters, the implicit enumeration (IE) algorithm is used based on the Observation 1 in the bilevel model of the r-interdiction median problem with fortification [38].

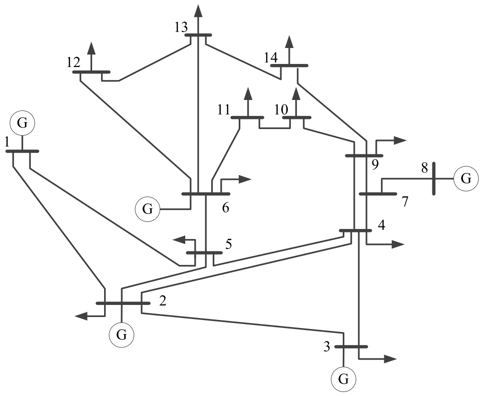


FIGURE 5. IEEE 14-bus System.

Observation 1: Let $\boldsymbol{I}$ be the set of R_a interdictions in the optimal solution to the lower-level interdiction problem without fortification. Then the optimal set of R_p fortifications selected by the leader must include at least one of the R_a facilities in $\boldsymbol{I}$.

It can be easily explained that if none of meters in the R_a interdictions are protected, it is still possible to interdict the measurements in the worst-case vector $\boldsymbol{I}$. If there are no solutions for the bilevel model (61)–(67) corresponding to a determined line l, it means that the line l is either well protected or impossibly attacked by CCPAs under R_a attack resources. The IE-based searching strategy is illustrated in Algorithm 1. An upper bound of the number of bilevel models which are solved by the algorithm is provided in the following proposition.

Proposition: The IE-based searching strategy solves at most $N_l + [(N_l \cdot R_a)^{R_p+1} - N_l \cdot R_a]/(N_l \cdot R_a - 1)$ bilevel problems in the worst case.

Proof: See Appendix.

Actually, the number of bilevel problems that should be solved is less than $N_l + [(N_l \cdot R_a)^{R_p+1} - N_l \cdot R_a]/(N_l \cdot R_a - 1)$. Because some measurements may appear serval times in the set A_i^j. Another reason is that some lines have been protected. Hence, the number of alternative measurements in set A_i^j is less than $N_l \cdot R_a$.

V. CASE STUDIES AND RESULTS

In this section, the implementation of CCPAs and the effectiveness of the proposed countermeasures are demonstrated by using the modified IEEE 14-bus system [8] shown in Fig. 5. The system is fully measured with m=54 measurements in total. The transmission capacity of line L1 is set to 160 MW and capacities of other lines are set to 60 MW [8]. Generator parameters are shown in Table 1. Other configurations of this system are obtained from the MATPOWER package [39]. The indices of transmission lines in the modified IEEE 14-bus system are adopted in accordance with the original IEEE 14-bus system in MATPOWER, e.g., line L1 connects bus 1 and 2. Meters with number 1-14 are set on buses, and others with number 15-54 are set on lines.

TABLE 1. Generator parameters.

Index	Bus	Pmax (MW)	Pmin (MW)	Cg($/MWh)
1	1	300	0	20
2	2	50	0	30
3	3	30	0	40
4	6	50	0	50
5	8	20	0	35

TABLE 2. Simulation results in the uncongested scenario.

AL	M_l	PA	Overloaded lines under CCPAs		
			25	20	15
1	0.75	2,7	/	/	/
2	1	1,3,4,5	1,3,4,5	1,3,4,5	/
3	1	2,4,6,7	2,4,5,6,7	2,4,5,6,7	/
4	0.79	2,3,5,7	2,3,5,7	2,3,5,7	/
5	0.60	2,3,4	2,3,4	2,3,4	/
6	0.34	3	1,2,3	2,3	/
7	0.83	3,4	/	/	/
8	0.26	2,3	2,3	2,3	/
9	0.22	2,3	2,3	2,3	2,3
10	0.64	2,3,7,15	/	/	/
11	0.07	2,3	2,3	2,3	2,3
12	0.12	2,3	2,3	2,3	2,3
13	0.27	2,3	2,3	2,3	2,3
14	0.33	2,3	2,3	2,3	2,3
15	0.60	2,3	/	/	/
16	0.14	2,3	2,3	2,3	/
17	0.19	2,3	2,3	2,3	/
18	0.01	2,3	2,3	2,3	2,3
19	0.02	2,3	2,3	2,3	2,3
20	0.06	2,3	2,3	2,3	2,3

Without loss of generality, the parameter γ is set to 0.95. The CPLEX solver is used to solve the bilevel and trilevel models in MATLAB R2017a platform.

A. SOLUTION OF THE BILEVEL MODEL

Two scenarios are performed on the modified IEEE 14-bus system: one with original rating representing an uncongested system and the other one with reduced rating representing a congested system. The congested system is modeled with all branch ratings decreased by 50%. In both cases, the attack resource R_a is set as 25, 20, and 15, respectively. To indicate the power flow margin of line l, the fraction M_l for line l is defined as $M_l = \left|F_l'\right| / F_{\max}$.

Table 2 and Table 3 show the simulation results in the uncongested and congested systems, respectively. In the tables, AL represents indices of attacked lines, and PA represents indices of overloaded lines only caused by physical attacks (i.e., tripping a line). In Table 2 and Table 3, due to the limitation of attack resource and the system structure, the most damaging attacks may not exist for some lines (e.g., L1). It is observed that when attack resources of CCPAs are large enough (e.g., R_a=25), the most damaging attack is to trip line L3. Tripping line L3 makes 5 lines (i.e., L2, L4, L5, L6, and L7) and 6 lines (i.e., L2, L4, L5, L6, L7, and L15) overloaded in the uncongested and congested scenarios, respectively. It is also found that the adversary tends to make transmission lines with larger fraction M_l overloaded in

TABLE 3. Simulation results in the congested scenario.

AL	M_l	PA	Overloaded lines under CCPAs		
			25	20	15
1	0.6	2,7	/	/	/
2	1	1,3,4,5,15	1,3,4,5,15	1,3,4,5,15	/
3	1	2,4,5,6,7	2,4,5,6,7,15	2,4,5,6,7,15	/
4	0.9	2,3,5,7,15	2,3,5,7,15	2,3,5,7,15	/
5	0.71	2,3,4,15	2,3,4,15	2,3,4,15	/
6	0.19	2,3,5	2,4,7,15	2,3,7,15	2,4,7,15
7	1	3,4	/	/	/
8	0.31	2,3	2,3,4,7	2,3,7	2,3,7
9	0.32	2,3,15	2,3,4,7,15	2,3,4,7,15	2,3,7,15
10	0.45	2,3,4,7,15	2,3,4,7,8,15	/	/
11	0.35	2,3,4,7,15	2,3,4,7,15	2,3	/
12	0.27	2,3,7,15	2,3,4,7,15	2,4,7,15	2,3,7,15
13	0.64	2,3,7,15	2,3,4,7,15	2,3,7,15	2,3,7,15
14	0.67	2,3,7,15	2,3,4,7,15	2,3,4,7,15	2,3,4,7,15
15	0.98	2,3	/	/	/
16	0.07	2,3,7,15	2,3,4,7,15	2,3,4,7	2,4,7,15
17	0.24	2,3	2,3,4,7	2,3,7	2,3,7
18	0.23	2,3,7,15	2,3,4,7,15	2,3,7,15	2,3,15
19	0.07	2,3,7,15	2,3,4,7	2,3,4,7	2,4,7,15
20	0.26	2,3,7,15	2,3,4,7,15	2,4,7,15	2,4,7,15

the most damaging attacks. For instance, when the line L3 is tripped in the uncongested scenario with R_a=25, the M_l of overloaded lines L2, L4, L5, L6, and L7 are 1, 0.79, 0.60, 0.34, and 0.83, respectively, which rank high in all lines.

In both uncongested and congested scenarios, it can be observed that the most damaging attacks are dependent on attack resources. When attack resources are relatively small, the number of tripped lines caused by CCPAs is decreased. For example, when L2 is attacked in Table 3, there are 5 overloaded lines given attack resources 25 and 20, respectively. While tripping the line L2 cannot be masked by cyber attacks when attack resource is 15. It means that an adversary can damage a power system with available attack resources. Comparing the uncongested and congested scenarios, it is found that the congested power grid is more vulnerable than the uncongested one given the same attack resources. For example, when L12 is attacked, there are 5 overloaded lines (i.e., L2, L3, L4, L7, and L15) in the congested scenario, while the number of overloaded lines is 2 (i.e., L2, and L3) in the uncongested scenario. Because reducing ratings of all lines decreases their margins and correspondingly creates a more stressful system. Thus, the most damaging CCPAs are significantly dependent on attack resources and the rating of lines.

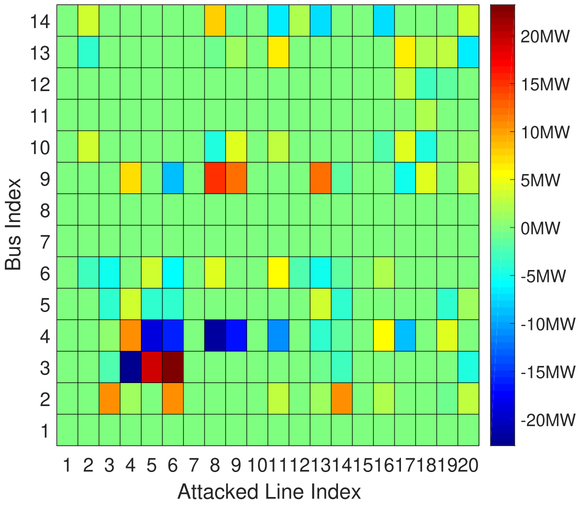


FIGURE 6. Distribution of injected powers in the uncongested scenario.

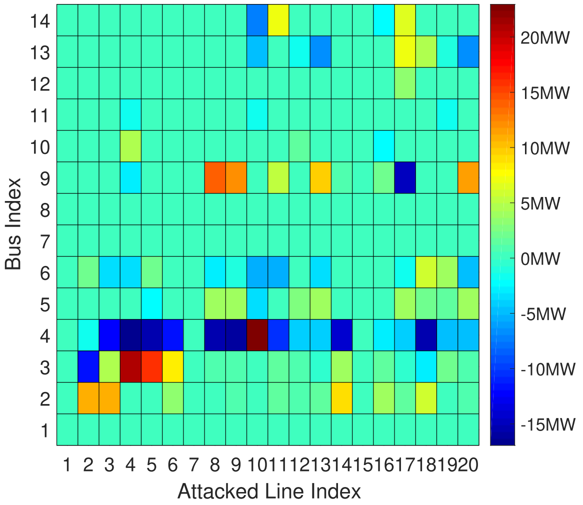


FIGURE 7. Distribution of injected powers in the congested scenario.

Furthermore, Fig. 6 and Fig. 7 show the distributions of injected powers (i.e., $\boldsymbol{a}_D$) to all loads with respect to tripping each line in uncongested and congested scenarios with R_a=25, respectively. In both scenarios, we can find that loads are redistributed by CCPAs according to injecting false data $\boldsymbol{a}_D$ to measurements. Taking the worst case as an example, when line L3 is tripped in the uncongested scenario, the injected powers in buses 2, 3, 4, 5, and 6 are 10.85 MW, −2.57 MW, 0.73 MW, −3.8 MW, and −5.21 MW as shown in Fig. 6, respectively. It means that the loads in buses 3, 5, and 6 are transferred to buses 2 and 4. Surprisingly, when Table 2 is recalled, it is noted that most ends of overloaded lines are affected by the malicious injected false data. For example, the affected ends of overloaded lines L2 (connecting buses 1 and 5), L4 (connecting buses 2 and 4), L5 (connecting buses 2 and 5), L6 (connecting buses 3 and 4), and L7 (connecting buses 4 and 5) are 2, 3, 4, 5, and 6, which are attacked. This phenomenon can also be observed in the congested scenario in Fig. 7. When line L3 is attacked in the congested scenario, the false data 10.85 MW, 4.8 MW, −12.22 MW, and −3.43 MW are injected to the measurements in buses 2, 3, 4, and 6, which are the ends of overloaded lines (i.e., L2, L4, L5, L6, L7, and L15) shown in Table 3. Hence, by injecting false data into the measurements in buses, CCPAs can make the lines connecting these buses overloaded.

Finally, we compare the results caused by physical attacks and CCPAs. The load shedding for the congested scenario corresponding to different R_a is shown in Fig. 8. In Table 2 and Table 3, it is shown that the numbers of overloaded

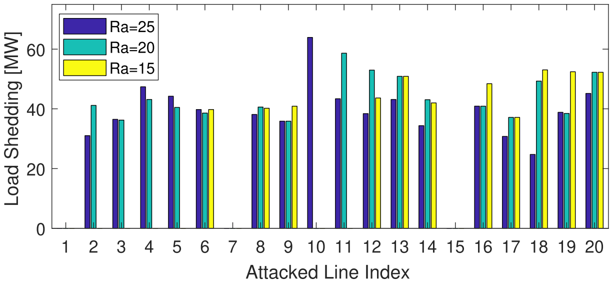


FIGURE 8. Distribution of load shedding in the congested system.

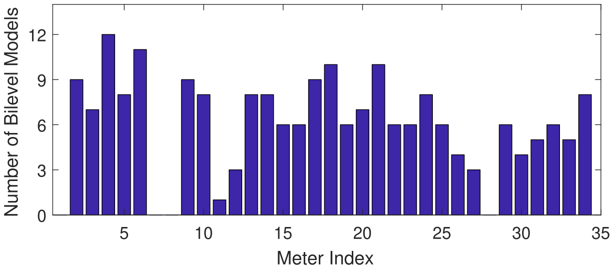


FIGURE 9. Number of bilevel models, where solutions contain an specific measurement.

TABLE 4. Countermeasures for IEEE 14-Bus system.

Iteration	Protected Meters	Total Number of Tampered measurements	Overload Lines
1	/	205	41
2	4	157	38
3	4,6	149	32
4	4,6,9	117	20
5	4,6,9,14	94	15
6	4,6,9,14,24	71	12
7	4,6,9,14,24,30	37	6
8	4,6,9,14,24,30,26	30	6
9	4,6,9,14,24,30,26,25	9	2
10	4,6,9,14,24,30,26,25,5	0	0

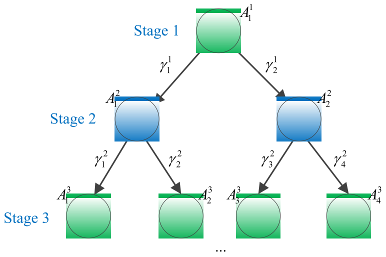


FIGURE 10. Tree for IE-based searching strategy.

lines caused by physical attacks and CCPAs are almost the same. However, different from the physical attacks, CCPAs can directly cause load shedding, especially when the system is congested. Taking R_a=25 in Table 3 as an example, the number of overloaded lines caused by physical attacks is 5 (i.e., L2, L4, L5, L6, and L7) corresponding to triggering line L3, while it is 6 (i.e., L2, L4, L5, L6, L7, and L15) for CCPAs. There is no load shedding only with physical attacks, while the load shedding is 36.40 MW with CCPAs corresponding to triggering line L3 shown in Fig. 8. Because the power flow in all transmission lines can be balanced by the automatic generation control (AGC) without load shedding in the first step when only physical attacks trip lines [40]. However, the control center may dispatch normally since physical attacks are well masked by CCPAs. This phenomenon can lead to the overload of some lines and significant load shedding. When any reasonable actions for attacks are not taken in time, cascading failures may occur.

B. COUNTERMEASURES

The proposed countermeasures are testified in the modified IEEE 14-bus system under the uncongested scenario with R_p=25.

Firstly, we make an explanation to identify a protected meter in each iteration of Algorithm 1. In the first step without any protection, the number of meters which are parts of solutions of different bilevel programming models corresponding to triggering different lines is shown in Fig. 9. Meters 1-34 are shown for the sake of comparison. It can be observed that the solutions of 12 bilevel models contain meter 4. According to Observation 1, if the meter 4 is protected, it can affect as many as 12 bilevel models. However, there are no bilevel models, whose solutions contain meters 1, 7, 8, and 28. It means that CCPAs do not inject false data into measurements in meters 1, 7, 8, and 28, when different lines are triggered. Thus, it is unnecessary to protect them in the first step. Hence, our proposed method is to protect the meter, which appears most frequently in the solutions of bilevel models in each step.

The solution process is shown in Table 4. The second column shows protected meters. The third and fourth columns are the total number of tampered measurements and overloaded lines, respectively. In the first iteration, there are no protected meters. The total numbers of tampered measurements and overloaded lines are 205 and 41, respectively. In the second iteration, meter 4 is protected. The total numbers of tampered measurements and overloaded lines decrease to 157 and 38, respectively. After 9 iterations, the protected meters are 4, 6, 9, 14, 24, 30, 26, 25, and 5. The total numbers of tampered measurements and overloaded lines are zero. It means that the minimum number of protected meters is 9, including meters in buses 4, 5, 6, 9, 14 and meters in lines 24, 25, 26, 30. At this time, the adversary cannot attack the power system by using CCPAs.

The developed countermeasures are compared with the complete protection strategies, which are also used to defend against CCPAs in [21]. The complete protection strategies are based on the single commodity method, which needs to guarantee the connectivity of power systems. This method is independent with electric parameters (e.g., capacities of lines and reactance), since it only needs the topology information and the distribution of buses without loads. The results of the complete protection strategies in Table 7 are directly used for comparison [21]. It is found that the complete protection strategies contain 15 protected meters. However, only

9 meters are needed for the developed countermeasures in this paper. The reason is that the process to obtain protected measurements in [21] is static, but ours is dynamic. Because iterations are adopted to identify protected measurements in our proposed countermeasures. From the dynamical perspective, some measurements need not be protected. Because they are not contained in solutions of bilevel models in our proposed method, when some other measurements are protected. For example, meter 15 (line L1 connecting bus 1 and 2) should be protected in the plan 2 shown in Table VII [21]. In Fig. 9, meter 15 is contained in solutions of 6 bilevel models corresponding to line L2, L3, L4, L5, L14, and L16, when there are no protected meters. However, when meters in buses 4, 5, 6, 9, 14 and meters in lines 24, 25, 26, 30 are protected, the meter 15 is not contained by any solutions of all bilevel models. This is because all the bilevel models are infeasible. Thus, the effectiveness of our developed countermeasures is well verified.

VI. CONCLUSION

In this paper, the formulation describing the relationship between the injected data into measurements and parameters (i.e., topology and reactance) of a power system under CCPAs is first constructed. A bilevel programming model is built to find the most damaging attack corresponding to a specific transmission line. The KKT conditions are used to transform the bilevel model to a single mixed-integer linear programming problem. To defend against CCPAs, a trilevel programming model is developed to identify protected measurements. The IE-based searching strategy is used to solve the trilevel model. The implementation of the developed CCPAs and the effectiveness of the countermeasures are verified in the modified IEEE 14-bus system. The future work is to analyze CCPAs in more sophisticated environments, such as measurements full of noise and AC power flow. Also, some efficient algorithms are needed to quickly identify protected measurements in the future.

APPENDIX

PROOF OF PROPOSITION

According to [38], the IE-based searching strategy can be formulated as a tree shown in Fig. 10. Both the green and blue nodes represent the points where bilevel problems are solved. γ_i^k represents the ith measurement that should be protected in stage k. A_i^j represents the attacked measurement set in stage j after measurement γ_i^k is protected. In the worst case, there are $N_l \cdot R_a$ attacked measurements in the set A_i^j in each stage. It is easy to see that the enumeration tree built in this fashion has as many levels as the number of defend cost R_p, i.e., the depth of the tree is R_p. In the first stage, N_l bilevel optimizations have to be solved. In the second stage, $N_l \cdot R_a$ bilevel optimizations have to be solved. The process will be iterated until the number of stages becomes $R_p + 1$. Finally, the sum of bilevel optimizations that have to be solved is $N_l + N_l \cdot R_a + (N_l \cdot R_a)^2 + \ldots + (N_l \cdot R_a)^{R_p}$, which is equivalent to $N_l + [(N_l \cdot R_a)^{R_p+1} - N_l \cdot R_a]/(N_l \cdot R_a - 1)$. Hence, the IE-based searching strategy solves at most $N_l + [(N_l \cdot R_a)^{R_p+1} - N_l \cdot R_a]/(N_l \cdot R_a - 1)$ bilevel problems in the worst case.

ACKNOWLEDGMENT

The authors would like to thank Prof. Jianhui Wang with the Department of Electrical Engineering, Southern Methodist University, Dallas, TX USA, for his suggestions of writing this paper.

REFERENCES

[1] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," *Comput. Netw.*, vol. 57, no. 5, pp. 1344–1371, 2013.

[2] H. He and J. Yan, "Cyber-physical attacks and defences in the smart grid: A survey," *IET Cyber-Phys. Syst., Theory Appl.*, vol. 1, no. 1, pp. 13–27, 2016.

[3] G. A. Pagani and M. Aiello, "The power grid as a complex network: A survey," *Phys. A, Statist. Mech. Appl.*, vol. 392, no. 11, pp. 2688–2700, 2013.

[4] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, "Catastrophic cascade of failures in interdependent networks," *Nature*, vol. 464, pp. 1025–1028, Apr. 2010.

[5] The Times of Israel. *Steinitz: Israel's Electric Authority Hit by 'Severe' Cyber-Attack*. Accessed: Jan. 27, 2016. [Online]. Available: https://www.timesofisrael.com/steinitz-israels-electric-authority-hit-by-severe-cyber-attack/

[6] E-ISAC/SANS. *Analysis of the Cyber Attack on the Ukrainian Power Grid*. Accessed: Mar. 18, 2016. [Online]. Available: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

[7] Z. Ismail, J. Leneutre, D. Bateman, and L. Chen, "A game theoretical analysis of data confidentiality attacks on smart-grid AMI," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 7, pp. 1486–1499, Jul. 2014.

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

[9] J. Liang, L. Sankar, and O. Kosut, "Vulnerability analysis and consequences of false data injection attack on power system state estimation," *IEEE Trans. Power Syst.*, vol. 31, no. 5, pp. 3864–3872, Sep. 2016.

[10] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 13, pp. 1–33, May 2011.

[11] C. Y. T. Ma, D. K. Y. Yau, and N. S. V. Rao, "Scalable solutions of Markov games for smart-grid infrastructure protection," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 47–55, Mar. 2013.

[12] J. Yan, H. He, X. Zhong, and Y. Tang, "Q-learning-based vulnerability analysis of smart grid against sequential topology attacks," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 1, pp. 200–210, Jan. 2017.

[13] N. Nezamoddini, S. Mousavian, and M. Erol-Kantarci, "A risk optimization model for enhanced power grid resilience against physical attacks," *Electr. Power Syst. Res.*, vol. 143, pp. 329–338, Feb. 2017.

[14] M. Alam, B. Mishra, and S. S. Thakur, "A new approach of multiple line outage identification using phasor measurement unit (PMU) with bad data," in *Proc. Int. Conf. Current Trends Towards Converg. Technol. (ICCTCT)*, Mar. 2018, pp. 1–6.

[15] M. E. J. Newman, *Networks: An Introduction*. New York, NY, USA: Oxford Univ. Press, 2011.

[16] S. Boccaletti *et al.*, "The structure and dynamics of multilayer networks," *Phys. Rep.*, vol. 544, no. 1, pp. 1–122, 2014.

[17] 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.

[18] Y. Xiang and L. Wang, "An improved defender-attacker-defender model for transmission line defense considering offensive resource uncertainties," *IEEE Trans. Smart Grid*, to be published.

[19] C. Wang *et al.*, "Robust defense strategy for gas–electric systems against malicious attacks," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 2953–2965, Jul. 2017.

[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] 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.

[22] 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.

[23] X. Liu, Z. Li, X. Liu, and Z. Li, "Masking transmission line outages via false data injection attacks," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 7, pp. 1592–1602, Jul. 2016.

[24] R. Deng, P. Zhuang, and H. Liang, "CCPA: Coordinated cyber-physical attacks and countermeasures in smart grid," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2420–2430, Sep. 2017.

[25] 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.

[26] H. E. Brown and C. L. Demarco, "Risk of cyber-physical attack via load with emulated inertia control," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 5854–5866, Nov. 2018.

[27] S. Soltan, M. Yannakakis, and G. Zussman, "Power grid state estimation following a joint cyber and physical attack," *IEEE Trans. Control Netw. Syst.*, vol. 5, no. 1, pp. 499–512, Mar. 2018.

[28] Y. Chen, S. Kar, and J. M. F. Moura, "Cyber-physical attacks with control objectives," *IEEE Trans. Autom. Control*, vol. 63, no. 5, pp. 1418–1425, May 2018.

[29] K. Huang, C. Zhou, Y.-C. Tian, S. Yang, and Y. Qin, "Assessing the physical impact of cyberattacks on industrial cyber-physical systems," *IEEE Trans. Ind. Electron.*, vol. 65, no. 10, pp. 8153–8162, Oct. 2018.

[30] 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.

[31] A. Abur and A. G. Expósito, *Power System State Estimation: Theory and Implementation*. New York, NY, USA: CRC Press, 2004.

[32] J. Kim and L. Tong, "On topology attack of a smart grid: Undetectable attacks and countermeasures," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 7, pp. 1294–1305, Jul. 2013.

[33] J. M. Arroyo, "Bilevel programming applied to power system vulnerability analysis under multiple contingencies," *IET Generat., Transmiss. Distrib.*, vol. 4, no. 2, pp. 178–190, Feb. 2010.

[34] Y. Yuan, Z. Li, and K. Ren, "Quantitative analysis of load redistribution attacks in power systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 9, pp. 1731–1738, Sep. 2012.

[35] J. M. Arroyo and F. D. 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.

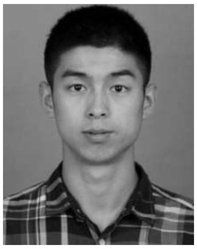
[36] J. Lu, J. Han, Y. Hu, and G. Zhang, "Multilevel decision-making: A survey," *Inf. Sci.*, vols. 346–347, pp. 463–487, Jun. 2016.

[37] B. Zeng and L. Zhao, "Solving two-stage robust optimization problems using a column-and-constraint generation method," *Oper. Res. Lett.*, vol. 41, no. 5, pp. 457–461, 2013.

[38] M. P. Scaparra and R. L. Church, "A bilevel mixed-integer program for critical infrastructure protection planning," *Comput. Oper. Res.*, vol. 35, no. 6, pp. 1905–1923, 2008.

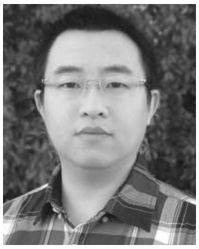
[39] R. D. Zimmerman, C. E. Murillo-Sánchez, and R. J. Thomas, "MATPOWER: Steady-state operations, planning, and analysis tools for power systems research and education," *IEEE Trans. Power Syst.*, vol. 26, no. 1, pp. 12–19, Feb. 2011.

[40] M. J. Eppstein and P. D. H. Hines, "A 'random chemistry' algorithm for identifying collections of multiple contingencies that initiate cascading failure," *IEEE Trans. Power Syst.*, vol. 27, no. 3, pp. 1698–1705, Aug. 2012.



MENG TIAN (M'17) received the B.S. and Ph.D. degrees from the Electronic Information School, Wuhan University, Wuhan, China, in 2011 and 2016, respectively.

He holds a Postdoctoral position with Wuhan University and a Visiting Scholar with Southern Methodist University. His research interests include security of cyber physical power systems and cascading failures of multilayer networks.



MINGJIAN CUI (S'12–M'16–SM'18) received the B.S. and Ph.D. degrees in electrical engineering and automation from Wuhan University, Wuhan, China, in 2010 and 2015, respectively.

He was a Postdoctoral Research Associate with the University of Texas at Dallas, from 2016 to 2017. He was a Visiting Scholar with the Transmission and Grid Integration Group, National Renewable Energy Laboratory, Golden, CO, USA, from 2014 to 2015. He is currently a Postdoctoral Research Associate with Southern Methodist University. He has published over 50 journal and conference papers. His research interests include power system operation, wind and solar forecasts, machine learning, data analytics, and statistics.

ZHENGCHENG DONG received the M.S. and Ph.D. degrees from Wuhan University, Wuhan, China, in 2013 and 2016, respectively.

He holds a Postdoctoral position with the School of Electrical Engineering and Automation, Wuhan University. His research interests include complex networks, interdependent infrastructures, and smart grid.

XIANPEI WANG received the B.S. degree from North China Electric Power University, in 1984, and the M.S. and Ph.D. degrees from Wuhan University, in 1991 and 1999, respectively.

He is currently a Professor with the Electronic Information School, Wuhan University. He has authored or co-authored over 100 papers in international and domestic journals. His research interests include security of cyber physical power systems, intelligent monitoring technique for power system, system reliability analysis, and fault diagnosis of high-voltage equipment.

SHENGFEI YIN (M'16) received the B.S. degree in electrical engineering from the College of Electrical and Information Engineering, Hunan University, Changsha, China, in 2016, and the M.Sc. degree in electrical engineering from the Illinois Institute of Technology, Chicago, IL, USA, in 2017.

He is currently pursuing the Ph.D. degree with Southern Methodist University, Dallas, TX, USA. His research interests include power market operation/optimization and data analysis in power systems.

LE ZHAO received the B.S. and M.S. degrees from the Electronic Information School, Wuhan University, Wuhan, China, in 2014 and 2016, respectively.

He is currently pursuing the Ph.D. degree with Wuhan University. His research interests include image processing and fault diagnosis in power systems.