Bilevel Model for Protection-Branch Measurements-Based Topology Attack Against DC and AC State Estimations

Gao, Shibin; He, Zonglun; Wei, Xiaoguang; Liu, Yigu; Huang, Tao ; Lei, Jieyu

DOI
10.1109/JSYST.2022.3181066

Publication date
2022

Document Version
Final published version

Published in
IEEE Systems Journal

Citation (APA)
Gao, S., He, Z., Wei, X., Liu, Y., Huang, T., & Lei, J. (2022). Bilevel Model for Protection-Branch Measurements-Based Topology Attack Against DC and AC State Estimations. *IEEE Systems Journal*, *16*(4), 5369-5379. Article 9801080. https://doi.org/10.1109/JSYST.2022.3181066

Bilevel Model for Protection-Branch Measurements-Based Topology Attack Against DC and AC State Estimations

Shibin Gao, Zonglun He, Xiaoguang Wei, Yigu Liu, Tao Huang, and Jieyu Lei, *Student Member, IEEE*

***Abstract*—A topology attack, as a special class of false data injection attacks, tampers with topology information of a system to mislead the decision of the control center. This article conducts an in-depth study on topology attacks that aim to interfere with the judgment in topology information and pose potential damage by tampering with measurement data and protection information on branches, namely, protection-branch measurements-based topology attacks (PBT attacks). To achieve PBT attacks in actual networks, we study the protection settings and mechanisms in term of branches including transformers and transmission lines. Then, for the first time, we develop a bilevel model based on the protection configuration from the perspective of security-constrained economic dispatch. Meanwhile, since a bilevel model is constructed against dc state estimation, a conversion method in constructing attack vectors under PBT attacks against ac power system is proposed, which makes PBT attacks more suitable for actual power systems and more concealed. In a set of case studies on an IEEE 14-bus system, the simulation results verify the effectiveness of the model we proposed, analyze the vulnerability of network under PBT attacks, and then identify some critical branches that are defended to cope with PBT attacks. In addition, the comparison between PBT attacks and traditional cyber-overloaded attacks also shows a stronger threat of the studied attacks.**

***Index Terms*—Bilevel model, conversion method, protection information, topology attack.**

I. Introduction

With the continuous development and innovation on information and communication technologies and operation technologies, cyber privacy and security issues arouse increasing attention in today's smart grids [1], [2]. As to a normal-operating complex power system, massive operational data (e.g., measurements of power system) and control information are being exchanged in real time to monitor the actual status and perform optimal generation dispatch arrangements. The information network ensures reliable and efficient electricity delivery in the system. However, it also introduces new cyber-related vulnerabilities to power systems. In 2010, hacker groups injected the Stuxnet worm virus to invade a supervisory control and data acquisition (SCADA) system and attacked uranium-enrichment equipment, causing Iran's nuclear power plants to postpone power generation [3]. Meanwhile, blackout caused by attackers' remote control of the substation circuit breakers led to wide-area power outages in the Ukraine power grid in 2015 [4]. The above events have caused serious economic losses and social impacts, so it is crucial to thoroughly investigate the mechanism and influence of cyber attacks to better enhance the system security.

As a special cyber attack, the false data injection (FDI attack) has received widespread attention from scholars, which was first proposed in [5]. The attacks are capable of intruding into SCADA systems, which transmit protection information, circuit breaker statuses, and measurement data between control center and remote terminal units (RTUs), and because the injected false data are precisely designed, they can bypass bad data detection of state estimation successfully [6]. Therefore, the attackers can cooperatively contaminate state estimation results to manipulate security-constrained economic dispatch (SCED) solutions in a predicted way which may mislead operators' control decisions and lead smart grids to uneconomic operating conditions accompanied with load shedding, and even cause emergencies such as line outages and cascading failures [7], [8].

The risk of FDI attacks on smart grids is increasing in recent years. According to attack mechanism and implementation methods, the existing research on FDI attacks can be divided into the following categories: cyber-overloaded attacks, coordinated cyber–physical attacks, and topology attacks. As a basic and pervasive form of FDI attacks, the cyber-overloaded attacks [i.e., load redistribution (LR) attack] were proposed by Yuan *et al.* [9], [10] in which the immediate attacks and delayed attacks were formulated as a bilevel attacker–defender model and a trilevel attacker–defender–defender model, respectively. In cyber-overloaded attacks, the attackers attempt to maximize the system disruption penalties in load shedding, while the defenders (i.e., system operators) tend to minimize the attack effectiveness collectively. On this basis, some studies explored how to maximize the effect and improve efficiency of the immediate attacks. A bilevel linear programming model was constructed to cause line overloading and maximize the total loadings in

Manuscript received 30 April 2021; revised 8 September 2021; accepted 1 June 2022. Date of publication 20 June 2022; date of current version 9 December 2022. This work was supported by the National Natural Science Foundation of China under Grant 51877181. (*Corresponding author: Jieyu Lei.*)

Shibin Gao, Zonglun He, Xiaoguang Wei, and Jieyu Lei are with the School of Electrical Engineering, Southwest Jiaotong University, Chengdu 611756, China (e-mail: gao_shi_bin@126.com; hzlin_swjtu@163.com; wei_xiaoguang@126.com; leijieyu_swjtu@126.com).

Yigu Liu is with the Department of Electrical Sustainable Energy, Delft University of Technology, 2628CD Delft, The Netherlands (e-mail: liuyigu_a@126.com).

Tao Huang is with the Department of Energy, Politecnico di Torino, 10129 Torino, Italy (e-mail: tao.huang@polito.it).

Digital Object Identifier 10.1109/JSYST.2022.3181066

all overloaded lines [11]. A fast solution in determining the attack vectors by just solving one linear programing problem was presented in [12]. In addition, recent research discussed the cascading failures caused by delayed cyber attacks. Che *at al.* [13] analyzed an optimal mechanism which can identify critical lines and by tripping them, it can cause high risk subsequent failures. Che *et al.* [14] studied the increasing occurrence probabilities of initiating contingencies caused by cyber attacks against key lines overloads which increased the grid vulnerability to cascading failures. Furthermore, some research adopt machine learning techniques to process system history information, and then extract attack characteristics to detect FDI attacks [15]–[18]. Some scholars also focused on the defense approaches to reduce the damage of cyber-overloaded attacks through formulating trilevel models [19]–[22].

Meanwhile, to broaden the impact of FDI attacks, some articles collectively consider both cyber attacks and physical attacks. The coordinated cyber–physical attacks could tamper with system data through cyber attacks to fabricate unobservable physical attacks. Zhang and Sankar [22] formulated a two-stage optimization model to analyze the physical consequences of the undetectable state-and-topology cyber–physical attacks. Similarly, a bilevel model of the coordinated cyber–physical attacks was constructed in [23] to identify the most damaging and undetectable physical attacks masked by cyber attacks. A stochastic game-theoretic approach was also proposed in [24], which could be adopted to protect the cyber–physical grids against coordinated attacks.

However, the feasibilities of the above two attacks are questionable when they are implemented in realistic attack scenarios. First, both attacks require to inject false data into bus-load measurements. Unfortunately, due to the existence of load forecast, the attacks could be easily detected after bus-load measurements are maliciously changed. Furthermore, the coordinated attack is not practical because of the difficulty in real-time coordinating and implementation.

Therefore, some scholars extend the idea of FDI attack to topology attacks that could perturb the operators' perceptions of network topologies through altering data from branch measurements and network switches. Rahman *et al.* [25] proposed a verification-based framework to analyze the impact of stealthy topology attacks on optimal power flow routines. Liang *et al.* [26] developed optimal attack models for three kinds of cyber-topology attack scenarios and used the natural aggregation algorithm to solve the models.

Considering that with the continuous expansion of large-scale cyber–physical systems, topology attacks exacerbate the vulnerabilities of smart grids. The existing research did not consider the difference in protection settings between the line and the transformer. Similarly, the processes between the attackers and the operators are also not given. In addition, most of the existing studies are based on dc state estimation; however, ISO/RTO is generally adopted in ac state estimation that is generally described by complex nonlinear mathematical models.

Based on the above background, we consider the special class of topology attacks that causes false tripping on branches. This article explores the vulnerabilities under such attack and the mechanism and interaction process are also analyzed. We also consider the conversion method of attack vectors against ac state estimation. The main contributions of this article are summarized as follows:

1) This article studies protection-branch measurements-based topology attacks (PBT attacks) by cooperatively tampering with protection scheme and branch power flow measurements. Meanwhile, the proposed PBT attacks can be also implemented based on incomplete information analyzed in case studies.
2) This article employs a bilevel model to construct PBT attack from the perspective of SCED. To the best knowledge of the authors, this article is the first of its kind. This article also conducts the comparison with the traditional bilevel model-based cyber-overloaded attack, and the comparison results show that the PBT attacks are more threatening to the system.
3) This article proposes a conversion method that can convert the attack vectors obtained by solving mixed integer linear programming (MILP) problem under dc state estimation into the attack vectors for ac state estimation, which is more applicable to the complex reality. Such method improves the universality of analytical procedures against FDI attacks in ac-based analysis.

The rest of the article is organized as follows: we describe the mechanisms of the existing FDI attacks and the protection schemes on branches in Section II. In Section III, we develop the bilevel model for PBT attacks which can be reformulated in MILP form by Karush–Kuhn–Tucker (KKT) method. Section IV discusses PBT attacks against ac state estimation. Case studies are performed in Section V to quantitatively analyze the harmfulness of PBT attacks and discuss the corresponding defense strategies. Finally, conclusions are drawn in Section VI.

II. Motivation

In this section, the principle and the modeling methodology of the PBT attacks are discussed. Considering that the PBT attacks we discuss is a special class of FDI attacks, we investigate the differences between the PBT attacks and the other FDI attacks from the perspective of branch overload/outage in Section II-A. On this basis, the principle of the PBT attacks is discussed in Section II-B. Last, the protection schemes on branches in modern power grids are discussed.

A. Overview of Security Issues Under FDI Attack

In existing literature, the available entries for FDI attackers include measurement, protection units, and the communication networks in SCADA system [5], [27]. For measurement and protection units, the attackers can exploit the inherent vulnerabilities in encryption and authentication mechanisms to invade the hardware of the field devices physically and tamper with their data through hardware Trojan, etc. On the other hand, weaknesses in communication protocols and schemes and network vulnerabilities can also be exploited by attackers to intrude into SCADA system to tamper with the data transformed between

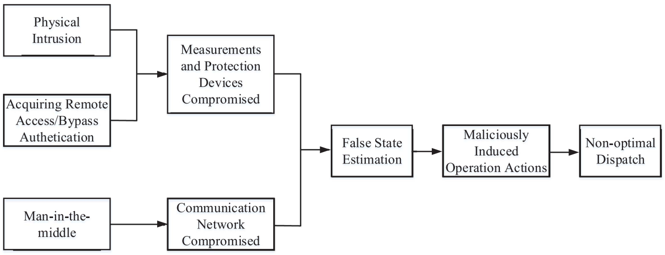
Physical Intrusion
Acquiring Remote Access/Bypass Authetication
Man-in-the-middle
Measurements and Protection Devices Compromised
Communication Network Compromised
False State Estimation
Maliciously Induced Operation Actions
Non-optimal Dispatch

Fig. 1. Attack mechanism schematic diagram of FDI attacks.

TABLE I
MEASUREMENT AND INFORMATION AN ATTACKER NEED TO CAPTURE

Captured data: Class of the attack:	Network topology	Protection information	Bus-load measurement	Branch power flow measurement
Cyber-overloaded attack	√		√	√
Coordinated cyber-physical attack	√	√	√	√
LR-topology coordinated attack	√	√	√	√
PBT attack	√	√		√

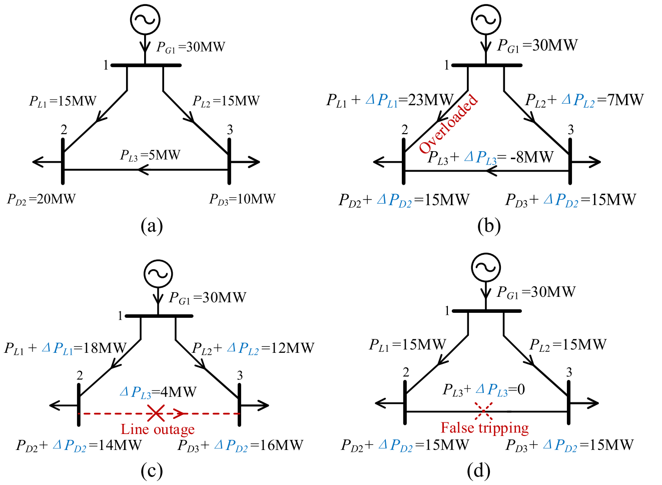
P_{G1}=30MW
1
P_{L1}=15MW
P_{L2}=15MW
2
3
P_{L3}=5MW
P_{D2}=20MW
P_{D3}=10MW
(a)
P_{G1}=30MW
1
P_{L1} + ΔP_{L1}=23MW
P_{L2}+ ΔP_{L2}=7MW
Overloaded
2
3
P_{L3}+ ΔP_{L3}= -8MW
P_{D2}+ ΔP_{D2}=15MW
P_{D3}+ ΔP_{D2}=15MW
(b)
P_{G1}=30MW
1
P_{L1} + ΔP_{L1}=18MW
P_{L2}+ ΔP_{L2}=12MW
2
3
ΔP_{L3}=4MW
Line outage
P_{D2}+ ΔP_{D2}=14MW
P_{D3}+ ΔP_{D2}=16MW
(c)
P_{G1}=30MW
1
P_{L1}=15MW
P_{L2}=15MW
2
3
P_{L3}+ ΔP_{L3}=0
False tripping
P_{D2}+ ΔP_{D2}=15MW
P_{D3}+ ΔP_{D2}=15MW
(d)

Fig. 2. Simple cases of existing three types of FDI attacks in three-bus system.

the units and the control center, and attackers can also employ man-in-the-middle attacks to deflect the data from their original values [19], [28]. Based on the above analysis and research [29], an attack mechanism schematic diagram of FDI attacks can be drawn as Fig.1. The potential attack paths and detailed data tampering process depend on the specific components and characteristics of the infrastructure and network which are out of the scope of this article.

Furthermore, FDI attacks are generally developed against dc state estimation. To bypass the bad data detection in dc state estimation, the injected attack vector $\boldsymbol{a}$ need to satisfy $\boldsymbol{a} = \boldsymbol{Hc}$, where $\boldsymbol{H}$ represents Jacobian matrix of dc state estimation and $\boldsymbol{c}$ represents false state vector. By injecting $\boldsymbol{a}$, the load distribution of entire network can be disrupted to make system fall into insecure operating state. At present, there are three ways to result in branch overload/outage under FDI attacks.

1) Cyber-Overloaded Attacks: The cyber-overloaded attacks inject false data which are deliberately designed according to the topology and capacity of the network to make branches appear to be overloaded. The false data mixed with the measurement data are uploaded to induce the control center to believe that some of the transmission lines are actually overloaded.

2) Coordinated Cyber–Physical Attacks: The coordinated cyber–physical attack could lead to undetected outages. An attacker could cause branch outages of the network by physical attack first, and then injects false data into bus-load measurements, branch power flow measurements, and protection information (including circuit breaker statuses) by cyber attacks, which could preserve the network topology and mask the outage states.

3) LR-Topology Coordinated Attacks: The LR-topology coordinated attack is the original form of topology FDI attack. The mechanism of the attack which aims to fake physical outages on branches is contrary to that of coordinated cyber–physical attack [30]. In such cyber attack, an adversary requires to modify bus-load measurements, branch power flow measurements, and protection information to mislead the control center with an incorrect topology estimate, which interferes operation security.

As shown in Table I, the above three classes of FDI attacks all launch cyber attacks by injecting false data, but the measurements and information that the attackers need to capture are quite different. A simple three-bus system example is shown in Fig. 2(a), in which bus 1 is a generator bus, and bus 2 and bus 3 are load buses. There are three branches in the system whose capacity limits are $0 \leq P_{L1} \leq 20$ MW, $0 \leq P_{L2} \leq 25$ MW, and $0 \leq P_{L3} \leq 10$ MW, respectively. We assume that the original system state is $P_{G1} = 30$ MW, $P_{L1} = P_{L2} = 15$ MW, $P_{L3} = 5$ MW, $P_{D2} = 20$ MW, and $P_{D3} = 10$ MW. Fig. 1(b)–(d) shows the mechanism of the above three FDI attacks, respectively. Fig. 2(b) is the false overload state of branch $L1$ which is caused by data injection against measurements in the whole system. Fig. 2(c) represents a real outage on branch $L3$ caused by physical attack which is masked by injecting false power flow and load. Fig. 2(d) shows a fake outage on branch $L3$ caused by injecting false data into measurements and protection information uploaded to the control center. Under these attacks, SCED will readjust generator outputs or even initiate load shedding based on false state estimation results, which lead the system to insecure operation states.

B. Principle of the PBT Attack

From the analysis in the previous subsection, we can see that the above three classes of FDI attacks require the allocation of attack resources to bus-load measurements of the system. However, it is impossible to tamper with the bus-load measurements by a big margin. Once the bus-load measurements are drastically changed, the control center will easily detect anomalies because the false load measurements deviate significantly from the predictable value calculated by load forecasting methods in energy management system (EMS). On the other hand, minor change of the load measurements may not be sufficient to make system fall into unsecure operation. Therefore, tampering with bus-load measurements is not an optimal choice. Compared with above three classes of FDI attacks, the PBT attacks just need to cooperatively tamper with branch power flow measurements and protection information without tampering with bus-load measurements, which use fewer attack resources and are less likely to be detected by the operator. The goal of PBT attacks is to fake outages on branches. When the false outages on branches are uploaded to the control center, SCED will be triggered to redistribute the power flow of the whole network by adjusting generator outputs and even removing load.

The details of the PBT attacks are discussed as follows. The original state of the network needs to satisfy

$$\boldsymbol{P}^{(0)} = \boldsymbol{SF}^{(0)} \cdot \boldsymbol{KG}^{(0)} \cdot \boldsymbol{G}^{(0)} - \boldsymbol{SF}^{(0)} \cdot \boldsymbol{KD}^{(0)} \cdot \boldsymbol{D}^{(0)} \quad (1)$$

where $\boldsymbol{P}^{(0)}$, $\boldsymbol{G}^{(0)}$, and $\boldsymbol{D}^{(0)}$ are the branch power flow measurement vector, generator measurement vector, and bus-load measurement vector in normal operation state, respectively. Shift factor matrix $\boldsymbol{SF}^{(0)}$, bus-generator incidence matrix $\boldsymbol{KG}^{(0)}$, and bus-load incidence matrix $\boldsymbol{KD}^{(0)}$ represent the network topology information in normal operation state, separately. Suppose the set of branches $\boldsymbol{TL}$ is falsely tripped by injecting false attack vector $\Delta\boldsymbol{P}$ under PBT attack. The corrupted power flow measurement vector $\boldsymbol{P}^{(1)}$ of postattack is

$$\boldsymbol{P}^{(1)} = \begin{bmatrix} \boldsymbol{P}_{\boldsymbol{TL}}^{(1)} \\ \bar{\mathbf{P}}_{\boldsymbol{TL}}^{(1)} \end{bmatrix} = \begin{bmatrix} \mathbf{0} \\ \boldsymbol{SF}^{(1)} \cdot \boldsymbol{KG}^{(1)} \cdot \boldsymbol{G}^{(0)} - \boldsymbol{SF}^{(1)} \cdot \boldsymbol{KD}^{(1)} \cdot \boldsymbol{D}^{(0)} \end{bmatrix} \quad (2)$$

where $\boldsymbol{P}_{\boldsymbol{TL}}^{(1)}$ represents the corrupted power flow measurement vector of branches $\boldsymbol{TL}$. Obviously, since branches $\boldsymbol{TL}$ is tripped falsely, $\boldsymbol{P}_{\boldsymbol{TL}}^{(1)} = 0$. $\bar{\mathbf{P}}_{\boldsymbol{TL}}^{(1)}$ represents the corrupted power flow measurement vector of other branches and $\boldsymbol{SF}^{(1)}$, $\boldsymbol{KG}^{(1)}$, and $\boldsymbol{KD}^{(1)}$ denote network topology information of postattack. In (2), because PBT attack does not take load measurements as the target, to make the network reach equilibrium, $\bar{\mathbf{P}}_{\boldsymbol{TL}}^{(1)}$needs to be determined by corrupted network topology information. According to (1) and (2), we can calculate the attack vector $\Delta\boldsymbol{P}$ as shown in (3a) and (3b) at the bottom of this page, where $\boldsymbol{SF}_{\boldsymbol{TL}}^{(0)}$, $\boldsymbol{KG}_{\boldsymbol{TL}}^{(0)}$, and $\boldsymbol{KD}_{\boldsymbol{TL}}^{(0)}$ represent the topology information related to branches $\boldsymbol{TL}$; and $\overline{\boldsymbol{SF}}_{\boldsymbol{TL}}^{(0)}$, $\overline{\boldsymbol{KG}}_{\boldsymbol{TL}}^{(0)}$, and $\overline{\boldsymbol{KD}}_{\boldsymbol{TL}}^{(0)}$ represent the topology information related to other branches. In (3), the attack vectors consist of two parts: attack vector $\Delta\boldsymbol{P}_{TL}$ related to falsely tripped branches $\boldsymbol{TL}$ and attack vector $\Delta\bar{\mathbf{P}}_{TL}$ related to other branches.

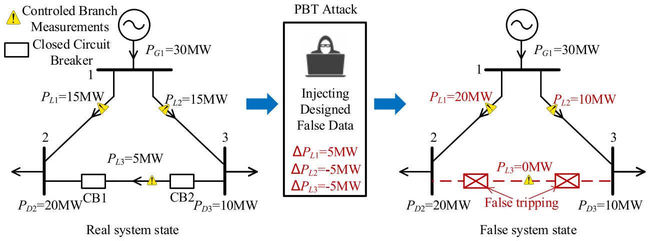

Fig. 3. Principle and a simple case of PBT attack.

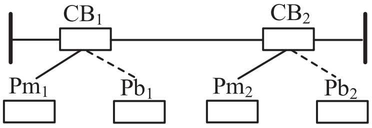

Fig. 4. Main and local backup protections in transmission line.

A simple case of PBT attacks based on the three-bus system mentioned above is shown in Fig. 3. In this case, the attacker aims to falsely trip the branch L_3. Therefore, to ensure the false balance of the system, the attack vector injected into branch measurements can be calculated:$\Delta\boldsymbol{P} = [5 \; -5 \; -5]^T$ MW. At the same time, the statuses of the two circuit breakers on L_3 are also tampered with cooperatively. After the control center receives the tampered data and the false tripping status of circuit breakers uploaded, it will mistakenly believe that the branch $L3$ has been tripped, so that SCED is urgently started to readjust the generator outputs and redistribute the load, resulting in uneconomic or even unsecure operating state.

C. Analysis of Attack Against Protection Schemes

In order to study the intrusion mechanism of PBT attacks against protection, the actual multilevel protection schemes including primary protection and backup protection are discussed.

Since the research object of this article is transmission system, the remote backup protections are not adopted for the branches [31]. The simple diagram of main protections and local backup protections on transmission line is shown in Fig. 4. There are two main protections (Pm1 and Pm2) and two local backup protections (Pb1 and Pb2) at both ends of the branch. When the branch fails, both the main protections and the local backup protections will be activated. Under normal circumstances, the main protection will trip the circuit breakers at both ends of the branches, and the local backup protection will return. When the main protections fail, the local backup protections will trip the circuit breakers after a delay.

Therefore, the PBT attacker in this article forges the main protection actions to trip the circuit breakers, and we assume

$$\Delta\boldsymbol{P} = \boldsymbol{P}^{(1)} - \boldsymbol{P}^{(0)} = \begin{bmatrix} -\boldsymbol{P}_{\boldsymbol{TL}}^{(0)} \\ \bar{\mathbf{P}}_{\boldsymbol{TL}}^{(1)} - \bar{\mathbf{P}}_{\boldsymbol{TL}}^{(0)} \end{bmatrix} \quad \text{(3a)}$$

$$\Delta\boldsymbol{P} = \begin{bmatrix} -\boldsymbol{SF}_{\boldsymbol{TL}}^{(0)} \cdot \boldsymbol{KG}_{\boldsymbol{TL}}^{(0)} & \boldsymbol{SF}_{\boldsymbol{TL}}^{(0)} \cdot \boldsymbol{KD}_{\boldsymbol{TL}}^{(0)} \\ \boldsymbol{SF}^{(1)} \cdot \boldsymbol{KG}^{(1)} - \overline{\boldsymbol{SF}}_{\boldsymbol{TL}}^{(0)} \cdot \overline{\boldsymbol{KG}}_{\boldsymbol{TL}}^{(0)} & -\boldsymbol{SF}^{(1)} \cdot \boldsymbol{KD}^{(1)} + \overline{\boldsymbol{SF}}_{\boldsymbol{TL}}^{(0)} \cdot \overline{\boldsymbol{KD}}_{\boldsymbol{TL}}^{(0)} \end{bmatrix} \begin{bmatrix} \boldsymbol{G}^{(0)} \\ \boldsymbol{D}^{(0)} \end{bmatrix} \quad \text{(3b)}$$

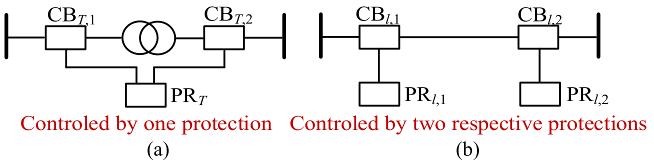

Fig. 5. Protection schemes in transformer and transmission line.

that the attacker can fabricate the start and return information of the local backup protections at the same time.

Meanwhile, in order to make the control center believe that the circuit breakers of the selected branches have been tripped, the attacker needs to cooperatively tamper with the action information $\boldsymbol{\psi}$ of protection devices and status information $\boldsymbol{\xi}$ of the corresponding circuit breakers while the branches are falsely tripped. However, in actual power system, the protection schemes set for branches are different. Therefore, it is necessary to discuss the intrusive method of transformer and transmission line under PBT attacks, respectively.

Transformer Protection Schemes: As shown in Fig. 5(a), a transformer has one main protection PR_T and two circuit breakers CB1 and CB2 at both ends. When the transformer fails, the protection PR_T will act to trip the circuit breakers $\text{CB}_{T,1}$ and $\text{CB}_{T,2}$. Therefore, when an attacker attempts to falsely trip the transformer, it is necessary to simultaneously tamper with one main protection information and two circuit breaker statuses according to

$$\psi_T^{(0)}=0\Rightarrow\psi_T^{(1)}=1\rightarrow\begin{cases}\boldsymbol{\xi}_{T,1}^{(0)}=0\Rightarrow\boldsymbol{\xi}_{T,1}^{(1)}=1\\ \boldsymbol{\xi}_{T,2}^{(0)}=0\Rightarrow\boldsymbol{\xi}_{T,2}^{(1)}=1\end{cases},T\in\boldsymbol{TL} \tag{4}$$

where ψ_T represents main protection action status of false tripped transformer $T\in\boldsymbol{TL}$. $\boldsymbol{\xi}_{T,1}$ and $\boldsymbol{\xi}_{T,2}$ represent two circuit breaker statuses of false tripped transformer $T\in\boldsymbol{TL}$. 0 means the uploaded status of circuit breaker is closed (protection does not act, $\psi_T^{(0)}=0$) and 1 means open (protection act, $\psi_T^{(1)}=1$).

Branch Protection Schemes: Different from transformer, there are two sets of main protection devices for a transmission line, and each main protection controls one corresponding circuit breaker. As shown in Fig. 5(b), when the transmission line fails, the two main protections $\text{PR}_{l,1}$ and $\text{PR}_{l,2}$ will act to trip the circuit breakers $\text{CB}_{l,1}$ and $\text{CB}_{l,2}$, respectively. Therefore, the attacker requires to invade two protection devices and manipulate the states of two circuit breakers to successfully implement a topology information tampering on a transmission line according to

$$\begin{cases}\psi_{l,1}^{(0)}=0\Rightarrow\psi_{l,1}^{(1)}=1\rightarrow\boldsymbol{\xi}_{l,1}^{(0)}=0\Rightarrow\boldsymbol{\xi}_{l,1}^{(1)}=1\\ \psi_{l,2}^{(0)}=0\Rightarrow\psi_{l,2}^{(1)}=1\rightarrow\boldsymbol{\xi}_{l,2}^{(0)}=0\Rightarrow\boldsymbol{\xi}_{l,2}^{(1)}=1\end{cases},l\in\boldsymbol{TL} \tag{5}$$

where $\psi_{l,1}$, and $\psi_{l,2}$ represent two main protection action statuses, and $\xi_{l,1}$, and $\xi_{l,2}$ represent the corresponding circuit breaker states, respectively. Obviously, compared with transformer, an attacker needs to tamper with more protection information after transmission line is falsely tripped.

III. Bilevel Model of PBT Attack

The essence of PBT attacks is to make a system fall into nonoptimal and even unsecure operation. Therefore, PBT attacks are formulated as a bilevel optimization model from the perspective of SCED. The upper level constructs the attack model whose purpose is to maximize the generation dispatch and load shedding cost through injecting attack vector $\Delta\boldsymbol{P}$ and tampering with protection $\boldsymbol{\psi}$ and circuit breaker $\boldsymbol{\xi}$ information to original system operation state. Based on $\Delta\boldsymbol{P}$, $\boldsymbol{\psi}$, and $\boldsymbol{\xi}$ delivered from upper level, the operator represented by the lower level implements SCED emergently to redispatch generators outputs $\boldsymbol{G}$ and even shed load $\boldsymbol{S}$ based on the corrupted data. The mathematical model of PBT attacks is shown as follows:

$$\text{Max}:\sum_{k=1}^{N_b}c_k\cdot G_k^{(1)}+\sum_{k=1}^{N_b}d_k\cdot S_k^{(1)} \tag{6}$$

subject to

$$\begin{aligned}\Delta P_h=&-\boldsymbol{SF}_h^{(0)}\cdot\boldsymbol{KG}_h^{(0)}\cdot\boldsymbol{G}^{(0)}\\&+\boldsymbol{SF}_h^{(0)}\cdot\boldsymbol{KD}_h^{(0)}\cdot\boldsymbol{D}^{(0)},\end{aligned}\quad\forall h\in\boldsymbol{TL} \tag{7a}$$

$$\begin{aligned}\Delta P_h=&\left(\boldsymbol{SF}_h^{(1)}\cdot\boldsymbol{KG}_h^{(1)}-\boldsymbol{SF}_h^{(0)}\cdot\boldsymbol{KG}_h^{(0)}\right)\boldsymbol{G}^{(0)}\\&-\left(\boldsymbol{SF}_h^{(1)}\cdot\boldsymbol{KD}_h^{(1)}-\boldsymbol{SF}_h^{(0)}\cdot\boldsymbol{KD}_h^{(0)}\right)\boldsymbol{D}^{(0)},\\&\forall h\in\boldsymbol{L}-\boldsymbol{TL}\end{aligned} \tag{7b}$$

$$\Delta P_h=-P_h^{(0)}\Leftrightarrow\delta_h=0,\ \delta_h\in\{0,1\},\ \forall h\in\boldsymbol{L} \tag{8a}$$

$$\sum_{h=1}^{N_L}(1-\delta_h)\le R,\ \forall h\in\boldsymbol{L} \tag{8b}$$

$$|\Delta P_h|\le\varepsilon\Leftrightarrow\sigma_h=0,\ \sigma_h\in\{0,1\},\ \forall h\in\boldsymbol{L} \tag{9a}$$

$$\sum_{h=1}^{N_L}(1-\delta_h)+\sum_{h=1}^{N_L}\sigma_h\le Z \tag{9b}$$

$$h\in\boldsymbol{L_T}\Leftrightarrow\psi_h=1,\xi=2 \tag{10a}$$

$$h\in\boldsymbol{L_l}\Leftrightarrow\psi_h=2,\xi=2 \tag{10b}$$

$$\psi_h\in\{1,2\},\ \forall h\in\boldsymbol{L} \tag{10c}$$

$$\sum_{h=1}^{N_L}(1-\delta_h)(\psi+\xi)\le W \tag{10d}$$

$$\delta_h=0\Leftrightarrow y_{ij}=0,\ \forall h\in\boldsymbol{L},i,j\in\boldsymbol{B} \tag{11a}$$

$$\sum_{j\neq i^*,j=1}^{N_b}y_{i^*j}=-N_b+1 \tag{11b}$$

$$\sum_{j=1}^{N_b}y_{ij}=1,\ \forall i\in\boldsymbol{B}i\neq i^* \tag{11c}$$

$$-N_b+1\le y_{ij}\le N_b-1\forall i,j\in\boldsymbol{B} \tag{11d}$$

$$\left\{P_k^{(1)},S_k^{(1)}\right\}$$

$$= \arg\left\{\underset{P_k, S_k}{\text{Min}} \sum_{k=1}^{N_b} c_k \cdot G_k + \sum_{k=1}^{N_b} d_k \cdot S_k\right\} \tag{12}$$

subject to

$$\theta_1 = 0 \tag{13a}$$

$$P_{kq} = \delta_h \cdot \frac{1}{x_h}(\theta_k - \theta_q),\ \forall h = kq \in \boldsymbol{L},\ \ k, q \in \boldsymbol{B} \tag{13b}$$

$$G_k - \sum_{q=1}^{N_b} P_{kq} = D_k - S_k, \forall kq \in \boldsymbol{L}, k, q \in \boldsymbol{B} \tag{13c}$$

$$\sum_{k=1}^{N_k} G_k = \sum_{k=1}^{N_b} (D_k^{(0)} - S_k) \tag{13d}$$

$$0 \le G_k \le G_{k\max}, \ \forall k \in \boldsymbol{B} \tag{14a}$$

$$-P_{kq\max} \le P_{kq} \le P_{kq\max}, \ \forall kq \in \boldsymbol{L} \tag{14b}$$

$$0 \le S_k \le D_k^{(0)}, \ \forall k \in \boldsymbol{B}. \tag{14c}$$

Upper-Level Model: The upper-level model is constructed in (6)–(11). Equation (6) is the objective function of the upper-level model. The attacker's goal is to maximize the total operation cost of the system adjusted by SCED, including generation costs of all generators and load shedding costs of all buses, where c_k and d_k are the generation cost and load shedding cost of bus k. G_k and S_k represent the generator outputs and load shedding on bus k. In addition, it is noted that if bus k does not directly connect to any generator or load, $G_k = 0$ or $S_k = 0$.

A set of attacker constraints are shown in (7)–(11). Constraint (7) represents the attack vector which is injected into branch measurements, where ΔP_h represents the false data injected into the hth branch power flow measurement. $\boldsymbol{SF}_h^{(0)/(1)}$, $\boldsymbol{KG}_h^{(0)/(1)}$, and $\boldsymbol{KD}_h^{(0)/(1)}$ represent topology information related to branch h. For the falsely tripped branches (***TL***), the false data values injected into the measurement are the opposite of the original power data which can be calculated through by (7a). For other branches (***L-TL***), it is also necessary to design false data calculated by (7b) to maintain the balance of false power in the system, so that the attack cannot be detected.

Constraints (8)–(10) are the limitations of attack resources. Since it is difficult to realize falsely breaking branches in practice, constraint (8) guarantees that the number of falsely tripped branches cannot exceed R, where δ_h is the binary variable which is equal to 0 if branch h is tripped falsely. Constraint (9) ensures the number of tampered branch measurements does not exceed Z, where σ_h is the binary variable which is equal to 0 if the false power quantity injected into the hth branch measurement does not exceed a small constant ε. In addition, when the false data quantity injected into a branch measurement is very small, the false quantity can be neglected, which can be viewed as the measurement error, due to the allowable error of measurement data in the state estimation process. Constraints (10a)–(10c) indicate the number of protection devices and circuit breakers that require to be tampered with for the falsely tripped branches that include the transformer and the transmission lines.

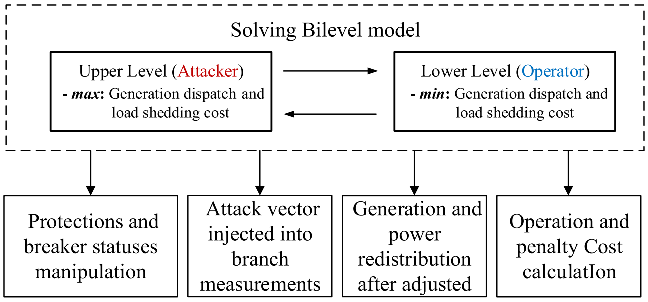
Solving Bilevel model
Upper Level (Attacker)
- max: Generation dispatch and load shedding cost
Lower Level (Operator)
- min: Generation dispatch and load shedding cost
Protections and breaker statuses manipulation
Attack vector injected into branch measurements
Generation and power redistribution after adjusted
Operation and penalty Cost calculatIon

Fig. 6. Block diagram of the proposed bilevel model.

Equation (10d) limits the number of tampered protection devices and circuit breakers to no more than W, which achieves a further constraint on the choice of the tripped branches, where ψ_h is the integer variable of main protection which is equal to 1 if branch h is a transformer and is equal to 2 if branch h is a line according to (4) and (5). ξ represents the integer variable of circuit breakers.

Constraint (11) adopts the method of single commodity flow to ensure the tampered network topology is connected instead of islanding after being attacked so as not to be suspected by control center. If the network is split into several islands, each island may face power imbalance in which case the attacker must maintain the dynamic balance of the system, which is more difficult to mask and easily detected by operator. In single commodity method, constraint (11a) is set to ensure the consistency of topology information, where i and j are the start bus and end bus of branch h. y_{ij} is the continuous decision variable set for virtual single commodity flow on branch $i \rightarrow j$ to guarantee the integrity of the network. Constraint (11b) assumes that $N_b - 1$ units of power are supplied by the reference bus i^*. Every other bus acts as a receiver which must have a positive incoming from i^* and each of them undertakes a load valued one unit which is shown in constraint (11c). Constraint (11d) stipulates the value of variable y_{ij} should be less than $N_b - 1$ for any branch $i \rightarrow j$. If all the above constraints can be met, then the network should be connected.

Lower-Level Model: The target of lower level that represents the operator by the model of SCED as shown in (12) is to minimize the system operating cost which contrasts with problem (6). Constraint (13a)–(13b) shows the calculation formula of branch power after SCED adjustment where x_h is the electrical reactance on branch $h.\theta_k$ and θ_q are the adjusted voltage angle of bus k and q based on fixing the voltage angle of the reference bus θ_1 to 0. The power balance equations for any bus and the whole system are shown in constraints (13c) and (13d). Constraints (14a)–(14c) limit the adjusted results of generator outputs, power flow on branches, and load shedding at buses, respectively, where $G_{k\max}$ and $P_{kq\max}$ indicate the maximum output of generator k and capacity of branch kq separately, and $D_k^{(0)}$ represents the load in normal operating state.

Based on the aforementioned discussion, we can concurrently summarize the block diagram of the proposed bilevel model as shown in Fig. 6 to show the results that can be obtained by solving the model.

IV. PBT Attack Against AC State Estimation

The above bilevel model based PBT is constructed based on dc state estimation. Since ac state estimation is generally adopted in ISO/RTO, it is necessary to extend PBT attack against ac state estimation. However, it is impractical to directly convert the dc-based bilevel model to an ac-based one due to the nonlinearity of ac method leading to high computational complexity. To overcome above problem, we first employ the dc-based bilevel model to screen the set of falsely tripped branches $\boldsymbol{TL}$, and then construct the ac-based attack vector according to these branches. To bypass the bad data detection in the ac-based state estimation, the attack vector

$$\dot{\boldsymbol{a}} = \boldsymbol{H}_{\text{ac}}\left(\hat{\dot{\boldsymbol{x}}} + \dot{\boldsymbol{c}}\right) - \boldsymbol{h}_{\text{ac}}\left(\hat{\dot{\boldsymbol{x}}}\right) \tag{15}$$

where $\boldsymbol{H}_{\text{ac}}$ and $\boldsymbol{h}_{\text{ac}}$ represent Jacobian matrix of ac state estimation after and before attack, and $\hat{\dot{\boldsymbol{x}}}$ and $\dot{\boldsymbol{c}}$ represent the estimated states and false states in ac state estimation. $\boldsymbol{H}_{\text{ac}}(\hat{\dot{\boldsymbol{x}}} + \dot{\boldsymbol{c}})$ and $\boldsymbol{h}_{\text{ac}}(\hat{\dot{\boldsymbol{x}}})$ represent estimated measurements, which consist of estimated load measurements, generator measurements, and branch measurements. Therefore, (15) can be written as

$$\begin{aligned}\dot{\boldsymbol{a}} &= \boldsymbol{H}_{AC}\left(\hat{\dot{\boldsymbol{x}}} + \dot{\boldsymbol{c}}\right) - \boldsymbol{h}_{AC}\left(\hat{\dot{\boldsymbol{x}}}\right)\\ &= \begin{pmatrix}\hat{\boldsymbol{P}}_G + j\hat{\boldsymbol{Q}}_G\\ \hat{\boldsymbol{P}}_D + j\hat{\boldsymbol{Q}}_D\\ \hat{\boldsymbol{P}}_L + j\hat{\boldsymbol{Q}}_L\end{pmatrix} - \begin{pmatrix}\hat{\boldsymbol{p}}_G + j\hat{\boldsymbol{q}}_G\\ \hat{\boldsymbol{p}}_D + j\hat{\boldsymbol{q}}_D\\ \hat{\boldsymbol{p}}_L + j\hat{\boldsymbol{q}}_L\end{pmatrix}\end{aligned} \tag{16}$$

where $\hat{\boldsymbol{P}}_{G/D/L}$ and $\hat{\boldsymbol{p}}_{G/D/L}$ represent estimated generator/load/branch active power flow measurements after and before attack, respectively. $\hat{\boldsymbol{Q}}_{G/D/L}$ and $\hat{\boldsymbol{q}}_{G/D/L}$ represent estimated generator/load/branch reactive power flow measurements after and before attack, respectively.

Because an attacker can obtain $\boldsymbol{h}_{\text{ac}}$ and real-time measurements $\dot{\boldsymbol{z}}$ from SCADA system, the attacker can employ $\dot{\boldsymbol{z}}$ and $\boldsymbol{h}_{\text{ac}}$ to estimate $\boldsymbol{h}_{\text{ac}}(\hat{\dot{\boldsymbol{x}}})$ by

$$\boldsymbol{h}_{\text{ac}}\left(\hat{\dot{\boldsymbol{x}}}\right) = \begin{pmatrix}\hat{\boldsymbol{p}}_G + j\hat{\boldsymbol{q}}_G\\ \hat{\boldsymbol{p}}_D + j\hat{\boldsymbol{q}}_D\\ \hat{\boldsymbol{p}}_L + j\hat{\boldsymbol{q}}_L\end{pmatrix} : \hat{\dot{\boldsymbol{x}}} = \arg\min\left\|\dot{\boldsymbol{z}} - \boldsymbol{h}_{\text{ac}}\left(\hat{\dot{\boldsymbol{x}}}\right)\right\| \tag{17}$$

where (17) can be solved by least squares method. Since PBT attack does not tamper with load and generator measurements, estimated load and generator measurements of preattack and postattack are identical as follows:

$$\hat{\boldsymbol{P}}_G + j\hat{\boldsymbol{Q}}_G = \hat{\boldsymbol{p}}_G + j\hat{\boldsymbol{q}}_G \tag{18a}$$

$$\hat{\boldsymbol{P}}_D + j\hat{\boldsymbol{Q}}_D = \hat{\boldsymbol{p}}_D + j\hat{\boldsymbol{q}}_D. \tag{18b}$$

Since $\hat{\boldsymbol{P}}_G + j\hat{\boldsymbol{Q}}_G$ and $\hat{\boldsymbol{P}}_D + j\hat{\boldsymbol{Q}}_D$ are precise value after estimation, $\hat{\boldsymbol{P}}_L + j\hat{\boldsymbol{Q}}_L$ can be directly calculated as follows according to ac power flow calculation:

$$\hat{\boldsymbol{P}}_L + j\hat{\boldsymbol{Q}}_L = \boldsymbol{H}'_{\text{ac}}\left(\hat{\boldsymbol{P}}_G + j\hat{\boldsymbol{Q}}_G, \hat{\boldsymbol{P}}_D + j\hat{\boldsymbol{Q}}_D\right) \tag{19}$$

where $\boldsymbol{H}'_{\text{ac}}$ represents the Jacobian matrix of ac power flow calculation after attack. In summary, according to (16)–(19), the attack vector $\dot{\boldsymbol{a}}$ can be calculated as

$$\begin{aligned}\dot{\boldsymbol{a}} &= \begin{pmatrix}\hat{\boldsymbol{p}}_G + j\hat{\boldsymbol{q}}_G\\ \hat{\boldsymbol{p}}_D + j\hat{\boldsymbol{q}}_D\\ \boldsymbol{H}'_{\text{ac}}\left(\hat{\boldsymbol{p}}_G + j\hat{\boldsymbol{q}}_G, \hat{\boldsymbol{p}}_D + j\hat{\boldsymbol{q}}_D\right)\end{pmatrix} - \begin{pmatrix}\hat{\boldsymbol{p}}_G + j\hat{\boldsymbol{q}}_G\\ \hat{\boldsymbol{p}}_D + j\hat{\boldsymbol{q}}_D\\ \hat{\boldsymbol{p}}_L + j\hat{\boldsymbol{q}}_L\end{pmatrix}\\ &= \begin{pmatrix}\boldsymbol{0}\\ \boldsymbol{0}\\ \boldsymbol{H}'_{\text{ac}}\left(\hat{\boldsymbol{p}}_G + j\hat{\boldsymbol{q}}_G, \hat{\boldsymbol{p}}_D + j\hat{\boldsymbol{q}}_D\right) - \left(\hat{\boldsymbol{p}}_L + j\hat{\boldsymbol{q}}_L\right)\end{pmatrix}.\end{aligned} \tag{20}$$

Based on (20), the PBT attack can be extended to estimation ac after the dc-based false data injected to branch power flow measurements are captured by the proposed bilevel model as showed in Fig. 7.

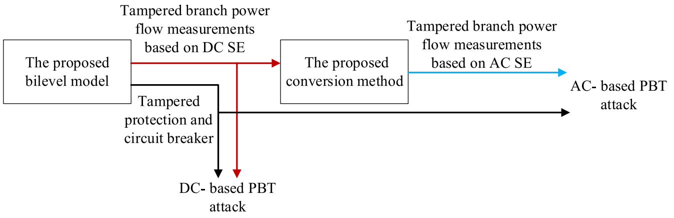
The proposed bilevel model
Tampered branch power flow measurements based on DC SE
The proposed conversion method
Tampered branch power flow measurements based on AC SE
AC- based PBT attack
Tampered protection and circuit breaker
DC- based PBT attack

Fig. 7. Goal of the conversion method against ac state estimation.

TABLE II
Parameters for Generators and Branches

Generator bus	Generator capacity (MW)	Generator cost ($/MWh)	Branch	Capacity (MW)
1	250	30	1-2	200
2	60	40	1-5,2-3,4-5	100
3	25	50	2-4,2-5,5-6	80
6	25	50	3-4,4-7,7-9	60
8	25	50	Others	40

V. Case Studies

In this section, we choose the IEEE 14-bus system to demonstrate the feasibility of the mathematical model above and analyze system vulnerabilities and defense strategies. The simulation is implemented by MATLAB R2018a (version number: 9.4.0.813654) on a 2.60 GHz personal laptop with an Intel Core i5-4210M CPU and 8 GB RAM.

A. Test on IEEE 14-Bus System

The IEEE 14-bus system which includes 14 buses and 5 generators connected through 20 branches is a classic case whose basic data are obtained from [32]. The additional parameters of generators and branches we set are shown in Table II. From the topology information of the IEEE-14 bus system, branches 5–6, 4–7, and 4–9 are transformer branches and the others are transmission lines. In addition, load shedding cost is set as 100 $/MWh.

When the attack resources are limited under PBT attack, the attack with $R = 1$ can be considered as the most resource-saving one. The simulation results under $R = 1$ are presented in Fig. 8 and Tables III and IV. In the figure, we can observe that to falsely trip the branch 1–2, the attacker needs to tamper with the breaker status. Meanwhile, to bypass the bad data detection, the other branch measurements also need to be tampered with

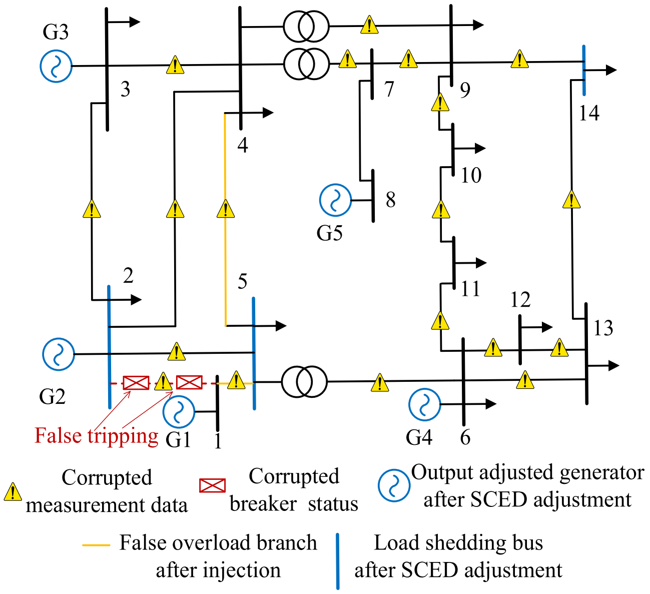
G3
3
4
7
9
14
10
8
G5
2
5
11
12
13
G2
False tripping
G1
1
G4
6
⚠ Corrupted measurement data
Corrupted breaker status
Output adjusted generator after SCED adjustment
False overload branch after injection
Load shedding bus after SCED adjustment

Fig. 8. PBT attack process and effect schematic diagram ($R = 1$).

TABLE III
FALSE POWER FLOW RESULT ON BRANCHES (MW)

Branch	δ_h	$P_h^{(0)}$	$P_h^{(1)}$	$P_h^{(1)}$	$P_h^{(2)}$
1-2	**0**	147.84	-147.84	**0.00**	**0.00**
1-5	1	71.16	147.84	**219.00**	100.00
2-3	1	70.01	-24.93	45.09	37.11
2-4	1	55.15	-52.17	2.98	10.53
2-5	1	40.97	-70.74	-29.77	-7.84
3-4	1	-24.19	-24.93	-49.11	-32.09
4-5	1	-61.75	-73.65	**-135.40**	-76.49
4-7	1	28.36	-2.01	26.35	1.39
4-9	1	16.55	-1.43	15.12	5.74
5-6	1	42.79	3.45	46.23	15.67
6-11	1	6.73	2.08	8.80	8.82
6-12	1	7.61	0.30	7.91	6.67
6-13	1	17.25	1.07	18.32	13.97
7-8	1	0.00	0.00	0.00	-25.00
7-9	1	28.36	-2.01	26.35	26.39
9-10	1	5.77	-2.08	3.70	3.68
9-15	1	9.64	-1.37	8.27	-1.04
10-11	1	-3.23	-2.08	-5.30	-5.32
12-13	1	1.51	0.30	1.81	0.57
13-14	1	5.26	1.37	6.63	1.04

TABLE IV
GENERATION AND LOAD ADJUSTMENT RESULT ON BUSES (MW)

Bus	$G_k^{(0)}$	$G_k^{(1)}$	$D_k^{(0)}$	S_k	$D_k^{(1)}$
1	219.00	100.00	0.00	0.00	0.00
2	40.00	60.00	21.70	1.50	20.20
3	0.00	25.00	94.20	0.00	94.20
4	/	/	47.80	0.00	47.80
5	/	/	7.60	7.60	0.00
6	0.00	25.00	11.20	0.00	11.20
7	/	/	0.00	0.00	0.00
8	0.00	25.00	0.00	0.00	0.00
9	/	/	29.50	0.00	29.50
10	/	/	9.00	0.00	9.00
11	/	/	3.50	0.00	3.50
12	/	/	6.10	0.00	6.10
13	/	/	13.50	0.00	13.50
14	/	/	14.90	14.90	0.00
Total cost	8170.00$	9150.00$	/	2400.00$	/

cooperatively. In addition, the branch 4–5 can be falsely overloaded to lead to SCED adjustment after the branch 1–2 is falsely tripped. Table III shows the falsely tripped branch δ_h, injected attack vector $P_h^{(1)}$, the tampered data uploaded to the control center $P_h^{(1)}$, and the error results of power flow $P_h^{(2)}$ after SCED adjustment. According to the proposed bilevel model, branch 1–2 is chosen as the falsely tripped one whose original power flow measurement value $P_{1-2}^{(0)}$ is 147.84 MW, and the injected power flow data ΔP_{1-2} is -147.84 MW accordingly. Since the original power flow of branch 1–2 is heavier than any other branches in the system, we infer that the disconnecting of the branch will cause the worst impact on LR of entire network. On the basis, in order to bypass the bad data detection successfully, attack vectors on measurements of the other branches are well designed as shown in the fourth column of Table III which is conditioned by the system topology and configuration. The verification shows that the false power of the system after injection of the attack vector is still balanced and no island appears.

As mentioned above, certain errors are undetectable in residual analysis of state estimation. In this case, we set the value of allowable error constant ε as 0.05 MW. We can find the false power flow injected into branch 7–8 does not exceed 0.05 MW. Therefore, branch 7–8 need not to be deliberately injected to false power flow which can be viewed as measurement error. Through the analysis of tampered power flow measurements $P_h^{(1)}$ received by the control center, we can find that the false tripping of branch 1–2 causes the tampered power flow over branches 1–5 and 4–5 to exceed the capacity limit after LR of entire network. From the perspective of the operator, to avoid resulting in the tripping of more circuit breakers and even cascading failures, SCED needs to urgently regulate generator outputs and redistribute the load to make the power flow on those branches back to secure range that leads to the error results under PBT attack. Table IV shows original generation outputs $G_k^{(0)}$, original load $D_k^{(0)}$, and generation outs $G_k^{(1)}$, load $D_k^{(1)}$, and load shedding S_k after SCED adjustment. The false tripping of branch 1–2 causes five generators redispatch and load shedding on bus 2, 3, and 14 whose values are 1.5, 7.6, and 14.9 MW, respectively. Furthermore, we investigate the operating cost of system as shown under PBT attack. In normal operating state, the original SCED solution should be a total generator output of 259 MW supplied by generator bus 1 and 2 which causes an operation cost of 8170 $ in all. Undoubtedly, the attack leads to a nonoptimal generation dispatch with unnecessary load shedding, which leads to a high operation cost of 11550 $ including 9150 $ of generation output cost and 2400 $ of load shedding cost. In summary, it can be considered that the PBT attack model is correct and effective.

Moreover, the simulation results of PBT attack under the situation of different number of false tripped branches R are given in Table V. When R reaches 5, the maximum load loss whose value is 128.50 MW occurs in the system, with a maximum operation cost of 17765 $/h which is more than twice the cost in normal operation state. We can also find that as R increases in the range of 1–5, the system takes more load shedding measures,

TABLE V
SIMULATION RESULTS FOR DIFFERENT NUMBER OF TRIPPED BRANCHES

R	Tripped branches	Total load shedding (MW)	Resources used (units)	Operation cost（$）	Cost performance ($/unit)
1	1-2	24.00	3+19	11550.00	525.00
2	2-3,4-5	39.88	6+19	12061.48	482.46
3	1-5,2-3,2-4	82.30	9+19	15031.00	536.82
4	2-3,2-4,4-5, 6-11	114.39	12+19	16777.26	541.20
5	2-3,2-4,4-5, 6-12,6-13	128.50	15+19	17765.00	522.50
6	1-2,2-3,2-4, 4-5,6-11, 6-12	128.50	18+19	17765.00	480.14
7	1-5,2-3,2-4, 4-5,4-7, 6-11,6-12	128.50	22+19	17765.00	433.29

*Resources used: resources used for protection information and breaker statuses; +resources used for branch power flow measurements.

TABLE VI
SIMULATION RESULTS OF TRADITIONAL CYBER-OVERLOADED ATTACK

Injected load vector on buses (MW)	[0.00, –10.02, 19.02, 18.28, –3.31, 3.94, 0.00 0.00, –14.21, –3.85, –1.55, –0.97, 0.005, –7.33]
Injected power flow vector on branches (MW)	[–39.01, 39.01, 3.31, –2.70, –39.62, 3.31,10.65, –16.74, 6.70, 10.04, 5.78, 4.13, 0.13, 0.00, –16.74, –5.78, –4.26, –5.78, 4.13, 4.26]
Adjusted power flow data in false SCED(MW)	[174.21, 75.79, 78.70, 54.88, 37.94, –34.52, –73.13, 17.31, 10.10, 36.33, 2.03, 6.01, 13.15, 0.00, 17.31, 5.07,7.04, –0.08, 0.88, 0.52]
Resources used (unit)	11+19
False overloaded branches	Branch 1–5 (110.18MW)
Total load Shedding (MW)	0.00
Adjusted Generator output (MW)	250 (generator bus 1) 9 (generator bus 2)
Generation cost ($/h）	7860

*Resources used: resources used for bus-load measurements; +resources used for power flow measurements.

TABLE VII
$R = 1$ AC-BASED INJECTED FALSE POWER FLOW ON BRANCHES

Branch	Real power flow (MW)	Reactive power flow (MVar)	Branch	Real power flow (MW)	Reactive power flow (MVar)
1	–156.88	20.40	11	3.56	0.57
2	185.46	34.09	12	0.48	0.01
3	–25.16	3.09	13	1.86	0.34
4	–54.34	24.76	14	0.00	–4.69
5	–73.09	39.99	15	–3.63	0.79
6	–23.86	21.00	16	–3.48	–0.40
7	–72.64	51.38	17	–2.28	–0.23
8	–3.63	–4.03	18	–3.48	–0.38
9	–2.13	–1.51	19	0.47	–0.01

and operating costs also increase accordingly. However, when the number of false tripped branches is more than 5 and less than 7, the attack cannot make the system perform more additional load shedding. When $R \geq 8$, the attacker could not find the optimal solution, i.e., the system will be falsely disconnected and divided into several islands after attack.

In addition, we assume that the attacker needs to consume one-unit resource for tampering protection information and circuit breaker status on each protection device, respectively, and injecting false data into a branch power flow measurement also requires one. Therefore, the results of attack resources with different *R* values can be calculated after attack in Table V. We can find that the number of tampered branch measurements are identical, all of which require 19 resource units with *R* increases. But the number of tampered protection devices are different, which increases with increasing *R*. Obviously, when the cost of acquiring attack resources is exorbitant, the attacker needs to consider how to achieve a stronger attack effect by using fewer attack resources. To investigate the cost performances under different attack resources, we use operating cost divided by attack resources as an index as shown in Table V. The results indicate that with *R* increasing, the cost performances of PBT attack show a trend of decreasing. Therefore, tripping one branch falsely is a reasonable choice in term of considering both attack resources and operating cost.

B. Comparison With Traditional Cyber-Overloaded Attack

To investigate the advantage of PBT attacks, we compare the studied attack with traditional bilevel-based cyber-overloaded (BCO) attack, which are obtained from [9]. In BCO attacks, the magnitude of injected false data for load measurement at each bus is restricted within 50% of its normal measurement. The initial state and parameters of the system are the same as the IEEE 14-bus system in subsection A. As shown in Table VI, BCO attack causes branch 1–5 to be false overloaded by cooperatively tampering with load measurements and power flow measurements. From the adjustment results of SCED, we can find that although the attack leads to the false overload on branch 1–5, the system does not adopt a load shedding under the regulation of SCED. Compared with traditional BCO attack, the PBT attack we discussed has the following serious threats: 1) Strong attack effect on system: the break of the branches, especially the branches with heavy loads, will cause serious overloads on other branches due to the LR of entire network. Therefore, faking tripping under PBT attack under will cause more generator dispatches and load shedding than pure cyber overload under BCO attack on branches. 2) Saving in attack resources used: the most significant feature of PBT attack is that it does not require to tamper with the load measurement data on buses. To sum up, it is considered that the PBT attack can cause more serious economic and secure impact on the system.

C. Conversion Method Against AC Power System

We adopt the proposed method to reconstruct the PBT attack vector in the case of $R = 1$ against ac-based state estimation, and the conversion results (FDI of real and reactive power flow on branches measurements) are shown in Table VII. Compared with the dc-based results in Table III, although the active power flow results on branch 2 are quite different, there are few changes in the injected data of the other branches. It is inferred that the inherent resistance leads to the load loss on branches which finally causes the redistribution of power flow to a limited extent, and the results can prove the effectiveness of the method we proposed. Therefore, the dc-based attack vector can be quickly converted through this method to effectively target the ac power system.

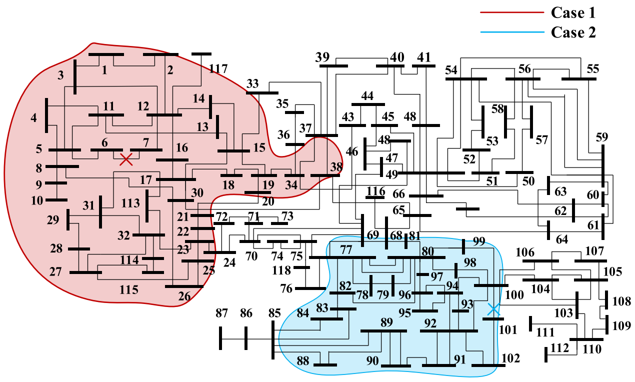

Fig. 9. Network topology and invaded branches distributions in two cases.

D. Corresponding Defense Strategy Analysis

According to the characteristics of PBT attacks, the research on defense strategies is against key branches that are more likely to be selected as the falsely tripped goals, such as branches 1–22–32–44–56–12 in the IEEE 14-bus test system. Methods of key branches strengthening range from intensifying physical security (e.g., conducting physical perimeter control) to enhancing communication security (e.g., equipping with PMUs instead of RTUs). In addition, software measures can be adopted to improve the network security such as upgrading the enhanced firewalls, developing the function of real-time attack characteristics extracting.

As long as the tampering of the measurement data on one key branch fails, the attack can be detected by control center immediately. Therefore, the defense measures for key branches can effectively ensure the economic and safe operation of power systems.

E. Attack Feasibility Under Incomplete Information

A more practical situation is that the attackers do not have the ability to invade all branches of the entire network, that is, PBT attacks can only tamper with the branch measurement data that has been controlled by the attackers. Therefore, this section will discuss the feasibility of PBT attacks under incomplete information through two tests in IEEE 118-bus system [32].

The system topology including 186 branches is shown in Fig. 8. We severally choose branch 6–7 (case 1) and branch 100–101(case 2) as the falsely tripped one and studied the attack vectors in the two cases. Same as subsection A, the false data injected into the branch measurements with a value less than 0.05 MW can be considered as an allowable and regardless error. After simulation and statistics, there are 49 branches whose measurement data are tampered with in case 1, while the number of that in case 2 is 38. In addition, the distributions of the invaded branches in two cases can be observed in Fig. 9. Therefore, it can be considered that PBT attacks can be successfully implemented when the attackers possess incomplete system information and only intrude into some of the branch measurement. Obviously, the amount and distribution of information obtained by the attackers are the decisive factors for the attacker to select the falsely tripped branches. And when the information available to attackers are seriously insufficient, the PBT attack cannot be implemented.

VI. Conclusion

This article proposes a bilevel model to quantitatively analyze the damage of PBT attacks through the increase in operating cost caused by a false SCED result. Noted that the actual protection configuration on branches is fully considered and distinguished to accurately calculate the required attack resources. The test results indicate the PBT attacks can cause serious load shedding, and as the number of tripped branches increases, the damage of the attack gradually increases until the system is disconnected falsely. Compared with traditional cyber attacks, PBT attacks have the characteristics of strong system adaptability and high attack cost performance that poses a greater threat to the system security. In addition, defense strategies and ac-based attack vector conversion method are also analyzed. At last, cases are performed in IEEE 118-bus system to verify the feasibility of the attack under incomplete information.

In the future, the false cascading failure under PBT attacks and the fault correlation will be explored by the authors.

Appendix

The bilevel model as described in this article is mixed integer nonlinear program form which requires to be transformed to MILP problems in this subsection to be solved in optimization solution techniques.

The MILP formulation of logical constraint (8a) that indicates the correlation between logical variable δ_h and continuous variable ΔP_h on faking tripping branches can be expressed as follows:

$$P_h^{(0)} + \delta_h \cdot M \geq 0,\ \forall h \in \boldsymbol{L} \tag{21a}$$

$$P_h^{(0)} - \delta_h \cdot M \leq 0,\ \forall h \in \boldsymbol{L} \tag{21b}$$

$$P_h^{(0)} - (M + \mu) \cdot {\delta'}_h \geq -M,\ \forall h \in \boldsymbol{L} \tag{21c}$$

$$P_h^{(0)} + (M + \mu) \cdot {\delta''}_h \leq M,\ \forall h \in \boldsymbol{L} \tag{21d}$$

$${\delta'}_h + {\delta''}_h - \delta_h{=}0,\ \forall h \in \boldsymbol{L} \tag{21e}$$

$${\delta'}_h, {\delta''}_h \in \{0, 1\},\ \forall h \in \boldsymbol{L} \tag{21f}$$

where ${\delta'}_h$ and ${\delta''}_h$ are additional binary variables defined. M and μ denote a sufficiently large positive constant and a sufficiently small positive constant separately.

Constraint (9a) can also be linearized as follows:

$$\Delta P_h - \sigma_h \cdot M \leq \varepsilon,\ \forall h \in \boldsymbol{L} \tag{22a}$$

$$\Delta P_h + \sigma_h \cdot M \geq -\varepsilon,\ \forall h \in \boldsymbol{L} \tag{22b}$$

$$\Delta P_h - (M + \mu) \cdot {\sigma'}_h \geq -M + \varepsilon,\ \forall h \in \boldsymbol{L} \tag{22c}$$

$$\Delta P_h + (M + \mu) \cdot {\sigma''}_h \leq M - \varepsilon,\ \forall h \in \boldsymbol{L} \tag{22d}$$

$${\sigma'}_h + {\sigma''}_h - \sigma_h = 0,\ \forall h \in \boldsymbol{L} \tag{22e}$$

$${\sigma'}_h, {\sigma''}_h \in \{0, 1\},\ \forall h \in \boldsymbol{L}. \tag{22f}$$

In addition, note that the constraint (13b) in which the logical binary variable δ_h multiplies the continuous decision variable

$\theta_k - \theta_q$that represents the difference between two bus angles associated with corresponding branch also requires to be converted to a linear form.

We define $\theta_{kq} = \theta_k - \theta_q$, and the nonlinear term of constraint (13b) can be expressed as $\gamma_h = \delta_h \cdot \theta_{kq}$. No need to consider its nonlinearity, the bilinear terms can be transformed to the following linear constraints:

$$-\delta_h \cdot M \le \gamma_h \le \delta_h \cdot M, \forall h \in \boldsymbol{L} \tag{23a}$$

$$-(1-\delta_h) \cdot M \le \theta_{kq} - \gamma_h \le (1-\delta_h) \cdot M, \forall h = kq \in \boldsymbol{L},\, k, q \in \boldsymbol{B}. \tag{23b}$$

Consequently, we could obtain the MILP formulations of bilevel model which can be transformed to an equivalent single level problem solved by KKT method.

REFERENCES

[1] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 645–658, Dec. 2011.

[2] J. Liu, Y. Xiao, S. Li, W. Liang, and C. L. P. Chen, "Cyber security and privacy issues in smart grids," *IEEE Commun. Surv. Tut.*, vol. 14, no. 4, pp. 981–997, Oct.–Dec. 2012.

[3] D. Kushner, "The real story of stuxnet," *IEEE Spectr.*, vol. 50, no. 3, pp. 48–53, Mar. 2013.

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

[5] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proc. 16th ACM Conf. Comput. Commun. Secur.*, 2009, pp. 21–32.

[6] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "False data injection attacks targeting DC model-based state estimation," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, 2017, pp. 1–5.

[7] B. M. Horowitz and K. M. Pierce, "The integration of diversely redundant designs dynamic system models and state estimation technology to the cyber security of physical systems," *Syst. Eng.*, vol. 16, no. 4, pp. 401–412, Jan. 2013.

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

[9] 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.

[10] 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.

[11] Y. Tan, Y. Li, Y. Cao, M. Shahidehpour, and Y. Cai, "Severe cyber attack for maximizing the total loadings of large-scale attacked branches," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 6998–7000, Nov. 2018.

[12] X. Liu, Z. Li, Z. Shuai, and Y. Wen, "Cyber attacks against the economic operation of power systems: A fast solution," *IEEE Trans. Smart Grid*, vol. 8, no. 2, pp. 1023–1025, Mar. 2017.

[13] L. Che, X. Liu, and Z. Li, "Mitigating false data attacks induced overloads using a corrective dispatch scheme," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 3081–3091, May 2019.

[14] L. Che, X. Liu, T. Ding, and Z. Li, "Revealing impacts of cyber attacks on power grids vulnerability to cascading failures," *IEEE Trans. Circuits Syst. II: Exp. Brief*, vol. 66, no. 6, pp. 1058–1062, Jun. 2019.

[15] L. Che, X. Liu, and Z. Li, "Fast screening of high-risk lines under false data injection attacks," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 4003–4014, Jul. 2019.

[16] T. C. Gulcu, V. Chatziafratis, Y. Zhang, and O. Yaĝan, "Attack vulnerability of power systems under an equal load redistribution model," *IEEE / ACM Trans. Netw.*, vol. 26, no. 3, pp. 1306–1319, Jun. 2018.

[17] X. Wei, J. Zhao, T. Huang, and E. Bompard, "A novel cascading faults graph based transmission network vulnerability assessment method," *IEEE Trans. Power Syst.*, vol. 33, no. 3, pp. 2995–3000, May 2018.

[18] Y. Zhu, J. Yan, Y. Tang, Y. L. Sun, and H. He, "Resilience analysis of power grids under the sequential attack," *IEEE Trans. Inf. Forensics Secur.*, vol. 9, no. 12, pp. 2340–2354, Dec. 2014.

[19] R. Deng, G. Xiao, and R. Lu, "Defending against false data injection attacks on power system state estimation," *IEEE Trans. Ind. Inform.*, vol. 13, no. 1, pp. 198–207, Feb. 2017.

[20] X. Liu and Z. Li, "Trilevel modeling of cyber attacks on transmission lines," *IEEE Trans. Smart Grid*, vol. 8, no. 2, pp. 720–729, Mar. 2017.

[21] A. Abusorrah, A. Alabdulwahab, Z. Li, and M. Shahidehpour, "Minimax-regret robust defensive strategy against false data injection attacks," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 2068–2079, Mar. 2019.

[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] 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.

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

[25] M. A. Rahman, E. Al-Shaer, and R. Kavasseri, "Impact analysis of topology poisoning attacks on economic operation of the smart power grid," in *Proc. IEEE 34th Int. Conf. Distrib. Comput. Syst.*, 2014, pp. 649–659.

[26] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "A framework for cyber-topology attacks: Line-switching and new attack scenarios," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 1704–1712, Mar. 2019.

[27] T. T. Kim and H. V. Poor, "Strategic protection against data injection attacks on power grids," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 326–333, Jun. 2011.

[28] J. Hull, H. Khurana, T. Markham, and K. Staggs, "Staying in control: Cybersecurity and the modern electric grid," *IEEE Power Energy Mag.*, vol. 10, no. 1, pp. 41–48, Jan./Feb. 2012.

[29] Y. Liu, S. Gao, J. Shi, and X. Wei, "Pre-overload-graph-based vulnerable correlation identification under load redistribution attacks," *IEEE Trans. Smart Grid*, vol. 11, no. 6, pp. 5216–5226, Nov. 2020.

[30] 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.

[31] J. Yang and Z. He, "Power systems alarm processing technology and fault diagnosis based on petri nets with timing contraints," *Proc. CSEE*, vol. 36, no. 2, pp. 250–256, Feb. 2012.

[32] "Power system simulation package," MATPOWER, A MATLAB, 2020. [Online]. Available: http://www.pserc.cornell.edu/matpower/

Shibin Gao received the Ph.D degree in electrical engineering from Southwest Jiaotong University, Chengdu, China, in 2004.

He is currently a Professor with the School of Electrical Engineering, Southwest Jiaotong University, Chengdu, China. His research interest includes power system protection and automation, online monitoring of electrical equipment, traction power supplies, railway electrification, and power system security.

Zonglun He is currently working toward the M.S. degree in electrical engineering from Southwest Jiaotong University, Chengdu, China.

His research interest includes cyber-physical power systems and power system security.

Xiaoguang Wei received the Ph.D. degree in electrical engineering from Southwest Jiaotong University, Chengdu, China, in 2019.

He is currently an Assistant Professor with the School of Electrical Engineering, Southwest Jiaotong University, Chengdu, China. His research interest includes power market and energy system security.

Yigu Liu received the M.S. degree in electrical engineering from Southwest Jiaotong University, Chengdu, China, in 2020. He is currently working toward the Ph.D. degree in electrical engineering from the Department of Electrical Sustainable Energy, Delft University of Technology, Delft, Netherlands.

His research interest includes vulnerability assessment of cyber-physical systems and synthetic networks.

Tao Huang received the Ph.D. degree in electrical engineering from Politecnico di Torino, Turin, Italy, in 2011.

He is currently a Researcher with the Department of Energy, Politecnico di Torino. His research interests include vulnerability assessment, electricity markets, smart grids, and artificial intelligence in power systems.

Jieyu Lei (Student Member, IEEE) is currently working toward the Ph.D. degree in electrical engineering with the Southwest Jiaotong University, Chengdu, China.

His research interest includes power market and cyber-physical power systems.