

A Flow Graph-Based Scalable Critical Branch Identification Approach for AC State Estimation Under Load Redistribution Attacks

Wei, Xiaoguang; Liu, Yigu; Shi, Jian; Gao, Shibin; Li, Xingpeng; Han, Zhu

DOI

[10.1109/TII.2023.3320402](https://doi.org/10.1109/TII.2023.3320402)

Publication date

2023

Document Version

Final published version

Published in

IEEE Transactions on Industrial Informatics

Citation (APA)

Wei, X., Liu, Y., Shi, J., Gao, S., Li, X., & Han, Z. (2023). A Flow Graph-Based Scalable Critical Branch Identification Approach for AC State Estimation Under Load Redistribution Attacks. *IEEE Transactions on Industrial Informatics*, 20(3), 4079-4091. <https://doi.org/10.1109/TII.2023.3320402>

Important note

To cite this publication, please use the final published version (if applicable). Please check the document version above.

Copyright

Other than for strictly personal use, it is not permitted to download, forward or distribute the text or part of it, without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license such as Creative Commons.

Takedown policy

Please contact us and provide details if you believe this document breaches copyrights. We will remove access to the work immediately and investigate your claim.







Green Open Access added to TU Delft Institutional Repository

'You share, we take care!' - Taverne project

<https://www.openaccess.nl/en/you-share-we-take-care>

Otherwise as indicated in the copyright section: the publisher is the copyright holder of this work and the author uses the Dutch legislation to make this work public.

A Flow Graph–Based Scalable Critical Branch Identification Approach for AC State Estimation Under Load Redistribution Attacks

Xiaoguang Wei , Yigu Liu , Jian Shi , Senior Member, IEEE, Shibin Gao , Xingpeng Li , Senior Member, IEEE, and Zhu Han , Fellow, IEEE

Abstract—This article offers a novel perspective on identifying the critical branches under load redistribution (LR) attacks. Compared to the existing literature that is largely disruption-driven and based on dc state estimation, we propose to address the threat from LR attacks on a more fundamental level by modeling and analyzing the circulation of false data within the cyber network resulting from the coordinated branch and node measurement manipulation based on ac state estimation. We reveal the underlying mechanism that disturbing the coordinated and reconciled interactions among false data injections can effectively sever the completeness and consistency of the LR attack, thus reducing its damaging effect. We then develop a scalable and computationally efficient critical branch identification approach that evaluates and ranks branches in terms of their criticality according to the graph model of the false data circulation. Case studies are conducted on IEEE 14-, 39-, 118-bus systems and several large-scale models to validate the effectiveness and computational efficiency of the proposed approach. Simulation results show that the proposed approach scales well with the size of the system and can effectively mitigate the damaging effects of the LR attack in terms of operation cost and load shedding.

Index Terms—Critical branch identification, cyber-physical power systems, flow graph, load redistribution (LR) attack.

Manuscript received 12 December 2022; revised 9 August 2023; accepted 23 September 2023. Date of publication 10 October 2023; date of current version 23 February 2024. This work was supported by the National Natural Science Foundation of China under Grant 52307143. Paper no. TII-22-5050. (Corresponding author: Yigu Liu.)

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

Yigu Liu is with the Department of Electrical Sustainable Energy, Delft University of Technology, 2628 CD Delft, The Netherlands (e-mail: y.liu-18@tudelft.nl).

Jian Shi is with the Department of Engineering Technology, University of Houston, Houston, TX 77004 USA (e-mail: jshi14@uh.edu).

Xingpeng Li is with the Department of Electrical and Computer Engineering, University of Houston, Houston, TX 77204 USA (e-mail: xingpeng.li@asu.edu).

Zhu Han is with the Department of ECE, University of Houston, Houston, TX 77004 USA, and also with the Department of Computer Science and Engineering, Kyung Hee University, Seoul 446-701, South Korea (e-mail: hanzhu22@gmail.com).

Color versions of one or more figures in this article are available at <https://doi.org/10.1109/TII.2023.3320402>.

Digital Object Identifier 10.1109/TII.2023.3320402

I. INTRODUCTION

A. Background

ADVANCING cyber security is a major priority for today's power grid. As a complex network that is increasingly monitored and controlled using digital devices and information technologies, such as smart meters and sensors, massive data are exchanged at high speeds over the cyber network of the energy transmission and delivery infrastructure to enable real-time monitoring and control of millions of physical processes and devices. This extensive information network provides critical benefits for the efficient, reliable, and secure operation of the power system; however, it also suggests that the power system has become more accessible to potential adversaries and harms from malicious events and attackers [1], [2]. Following emerging cyber security events, such as the two Ukraine blackouts in 2015 and 2016 that caused wide-area power outages, concerted efforts have been made by the government, industry, and research community to properly respond to, mitigate, and recover from cyber threats and hazards [3], [4].

This article examines the load redistribution (LR) attack [5], [6], a realistic form of false data injection (FDI) attacks [7], [8], [9] which target the power system measurement data in the supervisory control and data acquisition (SCADA) system. Under an LR attack, the attacker (i.e., cyber intruder) first attempts to gain unauthorized access to the measurement units and communication networks. Then, by cooperatively injecting false measurement data at multiple locations, the attacker could cause deviations between the measurement model and factual system operation model, trigger LR of the network, and further drive the system into a nonoptimal (i.e., uneconomic) or even insecure operating state. Meanwhile, according to the two white papers from E-ISAC SANS [3], [4], it has been proved that the adversaries are capable of organizing long-term reconnaissance to collect the necessary materials, e.g., network topology, key parameters, email addresses, etc. By combining all the collected materials, the weaponization and delivery can be finished. Then, by taking advantage of the state-of-the-art common vulnerability and exposures, which is open access, the adversaries are capable of finishing the cyber kill chain and pose great threats to the power grids by initializing sophisticated LR attacks. As concluded in [1], [5], and [9], the threat posed by the

LR attack is three-fold: first, in an LR attack, the false data vector injected by the attacker is undetectable by the state estimator (SE), which makes the attack highly stealthy and can effectively bypass the existing bad data detection (BDD), a key security module of the SE. Second, the successful execution of an LR attack requires less access to meters and resources. Thus, the LR attack is more attractive than other types of FDI attacks for cyber intruders with limited attack resources. Finally, the line overloading effect of LR attacks is equivalent to that of a physical attack on transmission lines [10], [11]. Therefore, it represents a severe security risk to the security and integrity of the power grid in which physical infrastructure is increasingly intertwined with cyber components [12].

B. Motivation and Aim

To analyze the underlying mechanism of LR attacks and protect the power system from their adverse effects on operation economy and security, it was first proposed in [13] that it is possible to prevent the system from entering the uneconomic and high-risk operation state by strengthening (i.e., defending) a certain number of critical branches. Simulation results from [13] have shown that once the cyber security for these branches is strengthened preventively and their measurement units can no longer be tampered with by the cyber intruder, the damaging effect of the LR attack on the whole network may be effectively mitigated. However, the identification of such critical branches is nontrivial. While the existing literature has offered valuable insights on safeguarding the system from the threat of LR attacks from the perspectives of system observability and attacker-defender interactions, they are limited in different ways, especially regarding computational efficiency.

In this article, we attempt to offer a brand-new perspective on identifying the critical branches under the LR attacks. Compared with the conventional approaches, we propose to address the threat from LR attacks on a more fundamental level by modeling and analyzing the false data circulation that resulted from the coordinated branch and node measurement manipulation. Moreover, we develop a systematic approach based on the min-cut max-flow theorem to identify and rank key pathways in the network that carry the heaviest false data transmission. These key pathways, i.e., critical branches, can then be strengthened to separate the reconciled interactions among FDIs and sever the completeness and consistency of the LR attack. Our approach does not require taking into account the complex sequential interactions between different agents and their distinct objectives involved in the LR attack, thus leading to a more scalable and computationally efficient solution.

C. Related Literature

So far, the identification of critical branches has been primarily studied from two perspectives in the literature. The first category focused on identifying a set of essential measurements that meet the “observable” conditions of the power system to secure in the face of FDIs [13], [14], [15], [16], [17]. A power system is considered observable if the measurement set yields a unique solution of all state variables in the SE. Greedy algorithms were

proposed in [14] and [15] to select a subset of critical measurements to protect, such that no FDI attack can be launched to compromise any set of state variables. A similar effort was presented in [16], where a mixed-integer linear programming (MILP) model was constructed and solved using a tree-pruning approach to protect the minimum number of measurements. In [17], a bilevel MILP problem that is subject to practical constraints was formulated to identify the least number of critical measurements to be protected. A common limitation shared by the above literature was that they formulated the defense problem as a network/device configuration problem with an emphasis on determining the optimal placement of measurement devices to improve state estimation based on system observability. The operation conditions of the power system under an FD attack, on the other hand, have not been fully incorporated. Moreover, the dynamic interactions between the attacker and the defender were also not considered in the methods mentioned above.

The secondary category of critical branch identification (CBI) approaches evaluated the damaging effects of an LR attack as a multilevel optimization problem in which an attacker seeks to maximize the power grid *disruption penalty* in the form of unmet demand or load shedding [18], whereas a defender (i.e., system operator) attempts to mitigate and minimize the effectiveness of any attack attempts [5], [6], [10], [11], [13], [19], [20], [21]. The interactions between the attacker and defender can be described as a bilevel attacker-defender problem (i.e., the attacker disrupts the network and the defender reacts to the disruption) or a trilevel defender-attacker-defender problem (i.e., the defender deploys countermeasures considering all possible attacking scenarios, attacker disrupts the network, and defender reacts). This process can then be formulated and solved as an optimal attack/defense resource allocation problem to determine the most vulnerable branches to strengthen.

To this end, a minimax-regret decision rule was proposed in [19] to determine the optimal measurement units to secure that reduce the maximum economic loss based on a multilevel optimization model. A nonlinear mixed-integer model was formed in [20] to select the meter measurements to secure considering the defense budget so that the attack cost can be maximized. In [21], a fast-screening approach was proposed to identify the high-risk branches with heavy power flow under LR attacks. Similar efforts were made in [22] and [23] to identify and strengthen critical branches that would prevent the network from overloading based on vulnerability correlations. In addition, as distributed flexible ac transmission (D-FACTS) devices are increasingly integrated into the transmission networks [24], [25], [26] to control the power flow, the concept of *moving target defense* has been proposed to use D-FACTS devices to intentionally perturb the susceptance of branches, so the Jacobian matrix \mathbf{H} can be modified to make it more unpredictable for cyber attackers. A major challenge of the disruption-driven CBI approaches lies in their computational complexity. As pointed out in [27], both bilevel and trilevel optimization problems can be computationally expensive to solve or even intractable, especially for large-scale systems. More specifically, the bilevel model is commonly transformed to the equivalent single-level MILP model by replacing the lower-level linear programming

problem with its Karush–Kuhn–Tucker conditions, which is known to be computationally inefficient. Similarly, the trilevel model also requires MILP reformulation, yielding additional computational burdens.

Within the context above, the contributions of this article can be summarized as follows.

- 1) While most of the existing LR literature is based on dc SE [5], [6], [7], [10], [11], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21], [23], [28], [29], in this article, we develop the proposed approach based on ac SE, which is more consistent with the current practice in the power industry.
- 2) This article offers a novel perspective of studying LR attacks based on the completeness and consistency of the false data circulation within the cyber network. The proposed approach is fundamentally different from the conventional disruption-driven LR attack models [5], [6], [10], [11], [13], [19], [20], [21]. To the best knowledge of the authors, our work is the first of its kind.
- 3) This article develops a systematic approach to identify, rank, and evaluate the key pathways involved in false data circulation with significantly enhanced computational efficiency, based on which effective mitigation measures can be derived promptly, especially for large-scale systems in which conventional disruption-driven CBI approaches quickly become computationally difficult or even infeasible to solve.

The rest of this article is organized as follows. We describe the mechanism of false data flow in Section II. In Section III, we develop the flow graph model for a power network under LR attacks and present the proposed CBI and ranking approach. Case studies are performed in Section IV to evaluate the performance of the proposed CBI approach. Finally, Section V concludes this article.

II. FALSE DATA CIRCULATION UNDER AN LR ATTACK

A. Threat Model of the LR Attack

As shown in Fig. 1(a), LR attacks aim to exploit the SE of an electrical network by compromising entry points, including 1) the distributed measurement units and 2) the data communication networks involved in the SCADA system. In terms of measurement units, such as intelligent electronic devices, RTUs, and smart meters, attackers can gain illegal/unauthorized access to them to physically tamper with the hardware of the field devices and inject false data into their measurements through means such as hardware trojan and malware. Other issues, such as inadequate controls on software and encryption integrity, unprotected internet access, and vendor/protocol-specific cryptographic vulnerabilities of these devices, can also be exploited to distort the measurement data. For the SCADA communication networks, attackers can leverage the weakness in authentication and security configuration, the inadequate network segmentation and perimeter protection, and other cyber vulnerabilities of the communication protocols to invade, intercept, and deflect the data transmission between field devices and the control center (e.g., man-in-the-middle attacks and man-on-the-side attacks)

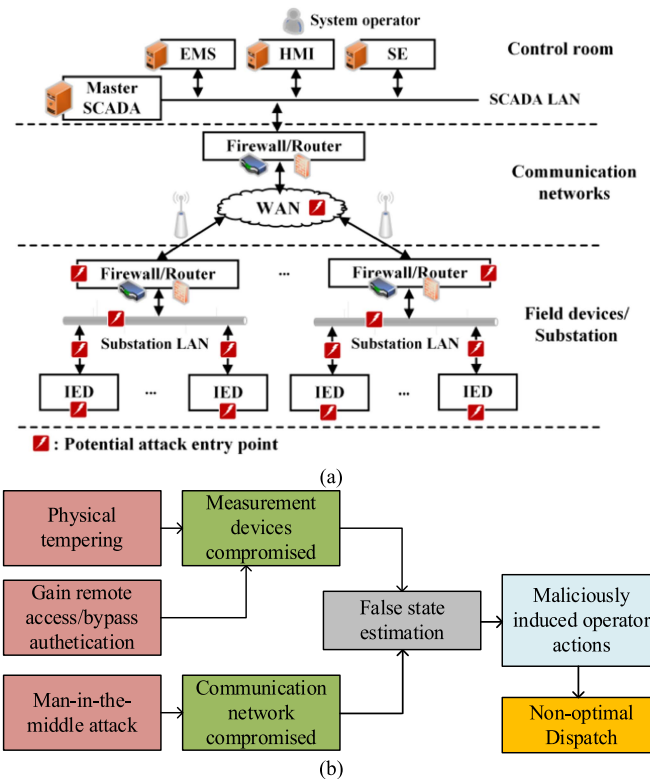


Fig. 1. (a) Concept diagram of LR attacks. (b) Representative attack tree for the LR attack.

[23]. A representative attack tree for the LR attack is shown in Fig. 1(b), in which the light red box suggests that the subtree below is omitted for brevity. Note that the detailed number of possibilities and potential attack paths depend on the specific components and structure of the infrastructure and are out of the scope of this manuscript.

Once the attacker gains access to the measurement data, they can start maliciously manipulating the measurements taken at different locations of the power grid by injecting a set of synthesized telemetered measurements (i.e., false data). Different than the conventional FDI attacks, according to [5] and [6], an LR attack considers the following two practical constraints: 1) the attacker can only tamper with load-bus measurements and line power measurements. The measurements of generator output cannot be manipulated due to their advanced security settings. 2) The FDI at a load bus cannot deviate too much from its normal value so that it does not draw attention from the system operator. To construct a successful attack, the attacker would need full information privilege to the configuration and cost information of the targeted power system as well, including network parameters, line capacity, detailed generator information (i.e., generation output, cost, and capacity), load shedding information, as well as the real-time measurement data [5], [6], [10], [11], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21], [26], [27], [28], [29], [30], [31], [32], [33]. Note that in cases where an attacker has no direct knowledge of the network topology, i.e., the attacker cannot capture the Jacobian matrix

$\mathbf{H}(\cdot)$ directly, various data-driven approaches [34], [35], [36], [37] exist that estimate $\mathbf{H}(\cdot)$ based on measurement data. The approximated $\mathbf{H}(\cdot)$ can then be used to launch the stealthy attack [38], [39].

Once an LR attack is constructed and launched, the contaminated measurement data would mislead the outcome of the SE and distort the solutions of the security-constrained economic dispatch (SCED) and other energy management system (EMS) applications in the control center. The falsified SCED solution can increase the system operation cost and drive the system to an uneconomic operating state. An LR attack may further lead the system to an insecure operating state where one or more transmission lines can experience being tripped offline due to overloading. Without immediate corrective actions, these line outages may lead to wide load shedding, and in the worst-case scenarios, cascading failures [28], [29].

Based on the cyber vulnerabilities identified above, once the critical branches to defend are identified, the defender can deploy enhancements to improve the cyber security of the measurement units and their communication links contained in the SCADA network [24], [25], such as:

- 1) fortify the measurement device with tamper-resistant and fail-safe hardware and tamper alarms to ensure physical prevention of FDI attacks;
- 2) apply advanced encryption, authentication, and validation measures to protect the confidentiality and integrity of the measurement data; or
- 3) deploy intrusion detection and prevention modules along the communication channels, so the alteration of messages can be detected.

Note that the list above is not comprehensive and readers can refer to [40] for a more in-depth discussion about the cyber-enhancement procedure. Also, note that similar to previous literature on FDI/LR attacks [11], [21], [22], [23], we assume in the following analysis that once a branch is strengthened, its measurement data is secured and can no longer be manipulated by the attacker.

B. Modeling of LR Attacks Against AC State Estimation

For an LR attack, the goal of the attacker is to redistribute the active power flow of the transmission network by injecting a vector of false active load power measurement, denoted by $\Delta\mathbf{P}_D$, to the vector of factual active load power measurements \mathbf{P}_D . Since the generator output measurements cannot be manipulated [5], $\Delta\mathbf{P}_D$ should satisfy (1), i.e., the sum of false active load power measurements injected to all load buses is equal to zero to ensure the total active load power measurement remains unchanged following the attack and the magnitude of $\Delta\mathbf{P}_D$ cannot exceed τ of normal active load to prevent the attack from being detected

$$\mathbf{1}^T \Delta\mathbf{P}_D = 0, -\tau\mathbf{P}_D \leq \Delta\mathbf{P}_D \leq \tau\mathbf{P}_D. \quad (1)$$

To bypass the BDD mechanism embedded in ac SE, it is evident that the branch power flow measurements need to be cooperatively manipulated with the load injection measurements [30], [31]. Hence, the general form of the attack vector can be

described as $\mathbf{a} = [\Delta\mathbf{P}_D, \Delta\mathbf{p}, \Delta\mathbf{q}]^T$, where $\Delta\mathbf{p}$ and $\Delta\mathbf{q}$ denote the vectors of false measurements injected to the vectors of factual active and reactive branch power measurements \mathbf{p} and \mathbf{q} , respectively. More specifically, as revealed in [38], following the injection of the attack vector \mathbf{a} , the 2-Norm of measurement residual $\|\mathbf{r}_a\|$ needs to satisfy (2) to bypass the BDD module

$$\|\mathbf{r}_a\| = \|\mathbf{z} + \mathbf{a} - \hat{\mathbf{z}}_a\| \leq \delta \quad (2a)$$

where

$$\hat{\mathbf{z}}_a = \mathbf{H}(\hat{\mathbf{x}} + \mathbf{c}). \quad (2b)$$

In (2), \mathbf{z} and $\hat{\mathbf{z}}_a$ denote the real-time measurements and the estimated false measurements, respectively, δ represents the detection threshold of the measurement residual, and $\hat{\mathbf{x}}/\mathbf{c}$ represent the estimated normal states/false states, respectively [33]. With the knowledge of $\mathbf{H}(\cdot)$ and the real-time measurements \mathbf{z} from the SCADA system, the attacker can estimate $\mathbf{H}(\hat{\mathbf{x}})$ by

$$\mathbf{H}(\hat{\mathbf{x}}) : \hat{\mathbf{x}} = \arg \min \|\mathbf{z} - \mathbf{H}(\mathbf{x})\| \quad (3)$$

where (3) can be solved by the least-squares method (LSM) in ac SE. As $\mathbf{H}(\cdot)$ is composed of two submatrices: bus-based Jacobian matrix $\mathbf{H}_B(\cdot)$ and branch-based Jacobian matrix $\mathbf{H}_L(\cdot)$, i.e., $\mathbf{H}(\cdot) = [\mathbf{H}_B(\cdot), \mathbf{H}_L(\cdot)]^T$, (2) can be divided into the following equations:

$$\Delta\mathbf{P}_D = \mathbf{H}_B(\hat{\mathbf{x}} + \mathbf{c}) - \mathbf{H}_B(\hat{\mathbf{x}}) \quad (4a)$$

$$\Delta\mathbf{p} + j\Delta\mathbf{q} = \mathbf{H}_L(\hat{\mathbf{x}} + \mathbf{c}) - \mathbf{H}_L(\hat{\mathbf{x}}). \quad (4b)$$

As indicated in (4a), we can calculate $\hat{\mathbf{x}} + \mathbf{c}$ based on $\Delta\mathbf{P}_D$, and by substituting the value of $\hat{\mathbf{x}} + \mathbf{c}$ into (4b), $\Delta\mathbf{p}$ and $\Delta\mathbf{q}$ can be determined. This suggests that once $\Delta\mathbf{P}_D$ is arbitrarily constructed according to (1) by an attacker, it can employ (3) and (4) to calculate $\Delta\mathbf{p}$ and $\Delta\mathbf{q}$, and the resulting attack vector can bypass the BDD mechanism in ac SE without being detected.

C. Modeling False Data Injection Flow

To illustrate the flow of the false data, we take the following electrical network with one generator and three loads as an example in Fig. 2. Under the *normal state*, the load injection measurements are (P_{D1}, Q_{D1}) , (P_{D2}, Q_{D2}) , and (P_{D3}, Q_{D3}) , respectively, as shown in Fig. 2(a), where Q_{D1} , Q_{D2} , and Q_{D3} denote reactive load power measurement injections. Meanwhile, the branch power flow measurements on branches (2,3), (2,4), and (2,5) are denoted as (p_1, q_1) , (p_2, q_2) , and (p_3, q_3) , respectively. Following a successful LR attack, we assume that the attacker injects ΔP_{D1} , ΔP_{D2} , and ΔP_{D3} to the meters at load buses 3, 4, and 5, respectively, so their measurements become $(P_{D1} + \Delta P_{D1}, Q_{D1})$, $(P_{D2} + \Delta P_{D2}, Q_{D2})$, and $(P_{D3} + \Delta P_{D3}, Q_{D3})$ following the attack. Then, according to (1), ΔP_{D1} , ΔP_{D2} , and ΔP_{D3} need to satisfy $\Delta P_{D1} + \Delta P_{D2} + \Delta P_{D3} = 0$. Without loss of generality, we assume $\Delta P_{D1} > 0$, $\Delta P_{D2} < 0$, and $\Delta P_{D3} < 0$. In addition, the attacker needs to cooperatively temper with the branch power measurements, i.e., (p_1, q_1) , (p_2, q_2) , and (p_3, q_3) , based on (4) to make the attack stealthy. We denote the falsified branch power flow measurements following the injection as $(p_1 + \Delta p_1, q_1 + \Delta q_1)$, $(p_2 + \Delta p_2, q_2 + \Delta q_2)$, and $(p_3 + \Delta p_3, q_3 + \Delta q_3)$. This is shown in Fig. 2(b). We name this

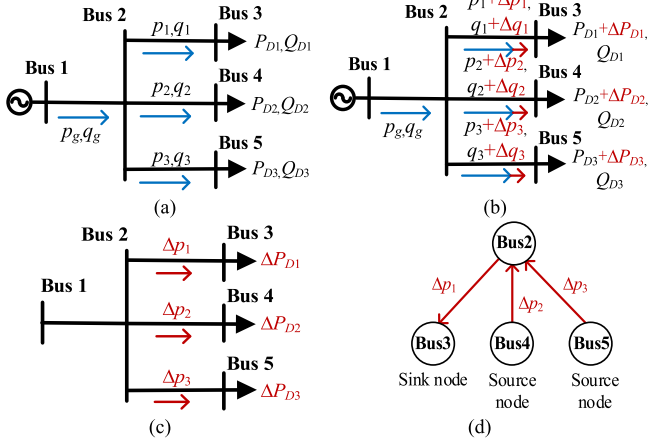


Fig. 2. Pathway for normal and false power measurement data flow. Blue arrows represent factual data flow, red arrows represent the false data flow. (a) Normal state, (b) Post attack state, (c) FDI state, (d) False load measurements divided into source nodes and sink nodes.

state the “*post-attack state*.” Generally, for an ac transmission network, the increments of branch power flow between two buses can be approximated as

$$\Delta p_{ij} \approx -b_{ij} (\Delta \theta_i - \Delta \theta_j). \quad (5)$$

The detailed approximation process is found in the Appendix.

According to (5), it is apparent that the vector of injected branch active power flow measurements Δp , where $\Delta p = [\Delta p_1, \Delta p_2, \Delta p_3]^T$ is approximately linearly dependent on the vector of injected active load power measurement ΔP_D , where $\Delta P_D = [\Delta P_{D1}, \Delta P_{D2}, \Delta P_{D3}]^T$. In addition, as ΔP_D has a negligible effect on the vector of injected reactive branch power flow measurements Δq as shown in the Appendix, where $\Delta q = [\Delta q_1, \Delta q_2, \Delta q_3]^T$, the post-attack state can be further simplified and decomposed into the normal state before the attack occurs, as shown in Fig. 2(a), and an *FDI state*, as shown in Fig. 2(c). In particular, since the FDI $\Delta P_{D2} < 0$ and $\Delta P_{D3} < 0$, load buses 4 and 5 can be seen as generating sources that inject $-\Delta P_{D2}$ and $-\Delta P_{D3}$ into the network, respectively. We name such load buses “*source nodes*.” On the other hand, we name load bus 3 “*sink nodes*.” In this way, based on the sign of the injected active load power measurement ΔP_D , all the load buses being manipulated by the attacker can be divided into source nodes and sink nodes, as shown in Fig. 2(d). Therefore, following an LR attack, the FDI state can be viewed as a network of multiple source nodes and multiple sink nodes, where the *false data flow* (FD-flow) circulates from the source nodes to the sink nodes in the form of Δp .

It is worth pointing out that while the approximated form of (8) is derived based on a set of assumptions introduced above, these assumptions are reasonable for a typical ac network [31]. Furthermore, we will show in the results section that the proposed approach is valid to construct stealthy LR attacks against ac SE. In other words, we will show that the attack vector can successfully bypass a non-linear ac SE based on the full-fidelity ac power flow model.

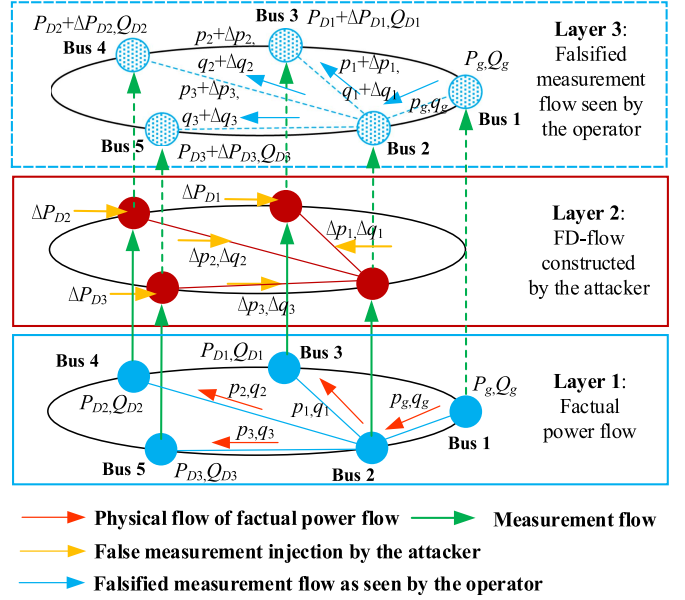


Fig. 3. Decoupled physical and information flow under an LR attack.

Based on the aforementioned discussion, it is evident that for the attacker to construct a successful LR attack, a valid path needs to exist between the source nodes and sink nodes in the FDI state to transmit the FD-flow. If any section of this transmission pathway is fully “*blocked*” or partially “*congested*,” the cooperative manipulations of load injection measurements at various network locations would be impaired. As a result, the threat of false load injections can be reduced or even diminished. This inspires us to study the LR attacks from the perspective of the FD-flow. If the key pathways (i.e., critical branches) that bear the heaviest FD-flow can be identified, their cyber security can be strengthened by the system operator before the attack to disturb the completeness and consistency of the FD-flow, which may lead to the reduction of the system-wide security risk resulted from the LR attack.

With the incorporation of FD-flow, the operation of the cyber-physical power grid under an LR attack can be decomposed into three distinct layers, as labeled in Fig. 3. The first and bottom layer is the physical layer, where factual power flow p and q circulates in the branches. The second layer is a cyber layer, where the stream of network traffic is the FD-flow, i.e., Δp . The third layer is another cyber layer, where the stream of network traffic is the falsified measurement data, i.e., $p + \Delta p$ and $q + \Delta q$, that would be fed into SE and EMS applications. Note that while layers 2 and 3 are both cyber layers, they may have different topologies as well as different natures and characteristics of network traffic.

Fig. 3 indicates that the critical branches involved in the FD-flow are fundamentally different from critical branches quantified using conventional approaches developed in the literature for LR attacks, which are mostly based on the falsified measurement flow on layer 3. For example, research studies [10], [22], [23], and [29] all aimed to identify critical branches based on their overloading conditions determined by the falsified

measurements. Branches are considered critical if they carry heavy power flow and hence are associated with the risk of being overloaded after the LR induced by the FDIs. By comparison, in our approach, the critical branches are identified based on the newly revealed FD-flow layer with a focus on disturbing the coordinated and reconciled network-wide interactions among FDIs required for the attacker to launch a self-consistent LR attack.

III. FD-FLOW-BASED CBI

In this section, we represent the system network as a graph to systematically model and evaluate the FD-flow. Then, we discuss how to identify the critical branches carrying the heaviest flow of false data based on min-cut max-flow theory.

A. FD-Flow Graph

Definition 1 (Map electrical network to a graph): For a given electrical network EN , we define a topology $FN = \langle V, E \rangle$ and a mapping operator f to map EN to FN , i.e., $f: EN \mapsto FN$ and $FN = f(EN)$, where all buses B of EN can be mapped to the vertices V of the graph FN as described in (6a) and all branches L of EN can be mapped to the edges E of the graph FN as described in (6b). Let the incidence function $g: E \mapsto V \times V$ be the mapping relationship between E and V . $\forall E_{mn} \in E$ satisfies (6c), i.e.,

$$V = \{V_b | V_b = f(B_b), B_b \in B, b = 1, 2, \dots, N_B\} \quad (6a)$$

$$E = \{E_{mn} | E_{mn} = f(L_i), L_i \in L, i = 1, 2, \dots, N_L\} \quad (6b)$$

$$g(E_{mn}) = \{V_m, V_n\}, V_m, V_n \in V. \quad (6c)$$

Definition 2 (FD-flow graph): According to Definition 1, the FDI state can be defined as an *FD-flow graph* $FD = \langle V, E, F \rangle$, where F denotes the flow of each edge or each vertex according to Definition 3 and Definition 4.

Definition 3 (Initial flow of edges): For a branch L_i , if $\Delta p(L_i) > 0$, the *initial flow* direction of the associated edge E_{mn} is defined to be from the node V_m to the node V_n , namely, $E_{m \rightarrow n}$, and the *initial flow* amplitude $F(E_{m \rightarrow n})$ is equal to $\Delta p(L_i)$. If $\Delta p(L_i) < 0$, the initial flow direction is defined to be from V_n to V_m , namely, $E_{n \rightarrow m}$, and the initial flow amplitude $F(E_{n \rightarrow m})$ is equal to $-\Delta p(L_i)$.

Definition 4 (Flow of vertices): For the false load measurement $\Delta P_D(B_j)$ injected to the measurement of load node B_j , the flow of the associated vertex VB_j is $F(VB_j)$.

Definition 5 (Source and sink vertices): Using the operator defined in (6a), a sink node B_j (i.e., $\Delta P_D(B_j) > 0$) can be mapped to a *sink vertex* denoted by VB_j^- , i.e., $VB_j^- = f(B_j)$, whereas a source node B_j (i.e., $\Delta P_D(B_j) < 0$) can be mapped to a *source vertex* denoted by VB_j^+ , i.e., $VB_j^+ = f(B_j)$. If $\Delta P_D(B_j) = 0$, it suggests that no false data is injected into node B_j and we thus define it as an *intermediate vertex*. Then, according to (1), the sum of the flow leaving the source vertices and the sum of the

flow ending at the sink vertices need to satisfy

$$\sum_{j_1=1}^{N_D^+} F(VB_{j_1}^+) = \sum_{j_2=1}^{N_D^-} F(VB_{j_2}^-) = K. \quad (7)$$

Definition 6 (Edge capacity): In the proposed FD-flow graph, it is evident that the flow of each edge cannot exceed K as described in (8). If we define F as the *edge capacity* of a particular edge, the *residual capacity* $F^*(E_{n \rightarrow m})$ of the edge $E_{n \rightarrow m}$ can be defined in (9), i.e.,

$$0 \leq F(E_{n \rightarrow m}) \leq K \quad (8)$$

$$F^*(E_{n \rightarrow m}) = K - F(E_{n \rightarrow m}). \quad (9)$$

Equation (9) shows that if an edge carries heavier FD-flow from the source vertex to the sink vertex, its residual capacity would be reduced. Note that the definition of the edge capacity F is different from the transmission line power-carrying capacity. It is rather a measure that captures the amount of FD-flow on an edge. Definition 6 indicates that an edge with lower residual capacity carries heavier initial flow from the source vertices to the sink vertices in the FD-flow graph.

Following Definition 1–Definition 6, we can convert an electric power network into a flow graph. In the following discussion, we study the identification of the critical pathways that link the source nodes (now source vertices) to the sink nodes (now sink vertices). Based on the previous discussion, the system operator can prevent the system from falling prey to the coordinated LR attacks by interfering with the attacker's access to these pathways.

B. FD-Flow Graph With a Single Source and Sink Vertex

To investigate the critical pathway between any pair of source and sink vertices, we first convert the FD-flow graph into an *s-t* network with a single source (s) and sink (t) vertex, namely, *s-t FD-flow graph*, to generate the flow. To do so, we propose to first convert the other source and sink vertices in the network into intermediate vertices as defined in Definition 5. Specifically, to study a pair of source vertex VB_j^+ and sink vertex VB_h^- , we need to perform the following operations.

For each additional source vertex in the network VB_w^+ (i.e., $VB_w^+ \in VB - \{VB_j^+\}$), we add a dummy edge $E_{j \rightarrow w}$ between vertex VB_j^+ and vertex VB_w^+ , and the residual capacity of this dummy edge $F^*(E_{j \rightarrow w})$ is set to 0, i.e., no FDI flows through this dummy edge. For each additional sink vertex VB_w^- (i.e., $VB_w^- \in VB - \{VB_h^-\}$), we add a dummy edge $E_{w \rightarrow h}$ between VB_w^- and VB_h^- , and the residual capacity of this dummy edge $F^*(E_{w \rightarrow h})$ is set to 0. In this way, the source vertices other than VB_j^+ and sink vertices other than VB_h^- can all be converted to intermediate vertices for the pair (VB_j^+, VB_h^-) without losing their original FDI information.

Then, between the pair of source vertex VB_j^+ and sink vertex VB_h^- , the maximum volume of false data that can circulate in between, denoted by $F(VB_j^+, VB_h^-)$, can be defined as

$$F(VB_j^+, VB_h^-) = \min(\tau S(B_j^+), \tau S(B_h^-)) \quad (10)$$

where $VB_i^+ = f(B_i^+)$ and $VB_h^- = f(B_h^-)$. Note that to investigate the maximum false power flow that a branch carries, we assume in (10) that the maximum false load measurements are injected to the pair of (VB_j^+, VB_h^-) , subject to (1). It is thus evident that $F(VB_i^+, VB_h^-)$ is constrained by the volume of FDIs at the source and sink vertices as described in (10).

In this way, we can conveniently evaluate the critical path between any pair of source-sink nodes according to their s - t FD-flow graph.

C. Maximum Flow and Minimum Cut

Definition 7 (Source-sink cut): Let the vertex set \mathbf{V} of a s - t FD-flow graph be partitioned into two sub-sets: \mathbf{A} ($VB_j^+ \in \mathbf{A}$) and \mathbf{B} ($VB_h^- \in \mathbf{B}$), which satisfies $\mathbf{V} = \mathbf{A} \cup \mathbf{B}$ and $\mathbf{A} \cap \mathbf{B} = \emptyset$. If the edge set $\mathbf{C}(VB_j^+ \rightarrow VB_h^-)$ satisfies (11a), then we can define this set as the $VB_j^+ - VB_h^-$ cut. Based on (11a), the cut set $\mathbf{C}(VB_j^+ \rightarrow VB_h^-)$ contains all the possible pathways between VB_j^+ and VB_h^- whose removal will separate the network into 2 disjoint halves \mathbf{A} and \mathbf{B} . In other words, removing the edges in the cut \mathbf{C} will cut off the connectivity between the source VB_j^+ and the sink VB_h^- . Furthermore, we can define the *cut capacity*, $\kappa(\mathbf{C}(VB_j^+ \rightarrow VB_h^-))$, as the sum of residual capacities of all edges contained in $\mathbf{C}(VB_j^+ \rightarrow VB_h^-)$ as shown in (11b):

$$\mathbf{C}(VB_j^+ \rightarrow VB_h^-) = \{E_{m \rightarrow n} | V_m \in \mathbf{A}, V_n \in \mathbf{B}\} \quad (11a)$$

$$\kappa(\mathbf{C}(VB_j^+ \rightarrow VB_h^-)) = \sum_{E_{m \rightarrow n} \in \mathbf{C}} F^*(E_{n \rightarrow m}). \quad (11b)$$

Equation (11) suggests that in the s - t FD-flow graph, if all the edges in the $VB_j^+ - VB_h^-$ cut set are removed, the attacker will not be able to initiate the FDIs to load buses B_j and B_h . Then the goal of the system operator is to determine the *minimum cut*, denoted as $\kappa(\mathbf{C}^*(VB_j^+ \rightarrow VB_h^-))$, that has the lowest possible capacity. Based on (9), the minimum capacity indicates that the sum of the residual capacities of all edges is minimized due to their high initial flow.

Furthermore, based on the max-flow/min-cut theorem proposed by Ford-Fulkerson [41], we can have the following:

$$\kappa(\mathbf{C}^*(VB_j^+ \rightarrow VB_h^-)) = Q^*(VB_j^+ \rightarrow VB_h^-) \quad (12)$$

where $Q^*(VB_j^+ \rightarrow VB_h^-)$ is the maximum amplitude of the feasible flow $Q(VB_j^+ \rightarrow VB_h^-)$ between VB_j^+ and VB_h^- that satisfies the edge capacity and flow conservation. In other words, $Q^*(VB_j^+ \rightarrow VB_h^-)$ captures the maximum amplitude of the FDI flow in the s - t FD-flow graph, and this *maximum flow* is equal to the *minimum cut* as described in (12).

Equation (12) further confirms that the minimum cut can help us identify the pathway in the cut set that carries the largest flow of false data between two load buses in the network. Therefore, the attacker will rely on the branches contained in the min-cut set to circulate the maximum amount of false data from the source vertex to the sink vertex. From the system operator's perspective, strengthening these critical branches could effectively interfere with the coordination of the LR attack.

While all edges in the cut $\mathbf{C}^*(VB_j^+ \rightarrow VB_h^-)$ can be considered critical edges between the source vertex VB_j^+ and sink vertex VB_h^- , due to the limitation of the defense resources, the system operator may not be able to strengthen all of them. Therefore, we need to define a criticality index to rank the critical branches. Specifically, for an individual branch L_i and the associated edge $E_{mn} = f(L_i) \in \mathbf{C}^*(VB_j^+ \rightarrow VB_h^-)$, we define the criticality index for L_i based on the following two considerations tailored specifically to the nature of the FD-flow.

- 1) *Amount of FDI:* The first factor to be taken into consideration is the amount of false measurement data injected into a pair of source and sink buses. If a larger volume of data is injected, it suggests that the pathway between the source and the sink vertices carries a heavier flow in the s - t FD-flow graph, i.e., such a pathway is more critical to the attacker to construct a valid LR attack. Thus, we can quantify the criticality of L_i as

$$I_{VB_j^+, VB_h^-}^1(L_i) = 2F(VB_i^+, VB_h^-). \quad (13)$$

Note that the “ $2F$ ” in (16) represents the combined FDI at the source and sink nodes. According to (16), a greater $I_{VB_j^+, VB_h^-}^1(L_i)$ indicates that more false data is injected into the vertex pair of VB_j^+ and VB_h^- .

- 2) *Initial flow:* for an individual branch in the min-cut, it is evident that if a branch carries heavier false power measurement traffic (i.e., initial flow in the edge as defined in Definition 3, it is more critical according to (12). In this way, we can quantify the criticality of L_i based on its edge capacity as described in the following equation:

$$I_{VB_j^+, VB_h^-}^2(L_i) = |F(E_{mn})|. \quad (14)$$

Combining (13) and (14), we define the overall criticality index for L_i as

$$I_{VB_j^+, VB_h^-}(L_i) = I_{VB_j^+, VB_h^-}^1(L_i) I_{VB_j^+, VB_h^-}^2(L_i). \quad (15)$$

Note that (15) quantifies the criticality of branches for a given pair of source vertex and sink vertex. To expand this index to the entire network, we need to take each source vertex from the set \mathbf{VB}^+ of source vertices and each sink vertex from the set \mathbf{VB}^- of sink vertices (a total number of $N_D \times (N_D - 1)$ combinations) to construct the s - t FD-flow graph and then calculate the criticality index of L_i . In this way, we can obtain $N_D \times (N_D - 1)$ criticality indices of L_i based on different combinations of source vertices and sink vertices. According to these criticality indices, the *global index* $\zeta(L_i)$ can be defined as follows:

$$\begin{aligned} \zeta(L_i) &= \sum_{j=1}^{N_D} \sum_{h=2}^{N_D-1} I_{VB_j^+, VB_h^-}(L_i), VB_j^+ \in \mathbf{VB}^+, VB_h^- \in \mathbf{VB}^-. \end{aligned} \quad (16)$$

Equation (16) determines the overall importance of L_i in carrying false data flow. Based on the rankings calculated from (16), the system operator can determine a list of critical branches

to strengthen. It is evident that by strengthening branches with higher $\zeta(L_i)$, a larger amount of false data circulating among load buses can be severed to interrupt the consistency of the LR attack.

After the set of critical branches CB is identified according to (16), the defender can strengthen one or more of them to sever the key pathway of the false data circulation to disturb the completeness of the LR attack. Ideally, if the system operator has sufficient defensive resources to strengthen all the branches included in a pathway between a given pair of s - t nodes, this pathway can be completely blocked, suggesting no false data can flow through it from the source node to the sink node.

It is worth noting that in the proposed approach, critical branches are investigated based on the input of a particular system operating condition, and a branch's criticality index could potentially vary when the operating conditions of the system change. That said, for a particular system, the system operator can use approaches such as [42] and [43] to select representative operating conditions and perform the proposed analysis to comprehensively evaluate the system's false data flow and gain insight into the patterns of critical branches within the network under different operating conditions, based on which strategic defense plans can be made.

IV. CASE STUDIES

In this section, we employ the IEEE 14-, 39-, and 118-bus systems to demonstrate the effectiveness of the proposed approach. We will also verify the scalability of the proposed approach on several large-scale testing systems. The parameters of the LR model used in the study are set up as follows: $\tau = 20\%$. The simulations are performed on a laptop, which has an Intel i5-7200U CPU @2.50 GHz and 8.00 GB of RAM. Yalmip is used to solve the optimization models in the following discussion.

A. Analysis of AC-Based LR Attack

To verify the capability of the proposed LR attack model in bypassing the BDD module in ac SE, we take the IEEE 14-bus system as an example. We can first count that for this particular system, there is a total of 55 pairs of s - t nodes. We then inject false data attack vectors to each pair of s - t nodes according to (1) and (4). We can determine if the attack is detectable by evaluating the variation of the measurement residuals before and after the attack. The results of this analysis are given in Table I. Note that under the normal state, the measurement residual is 0.0122.

Table I shows that following the injection of attack vectors constructed using the proposed approach, the measurement residuals for all 55 pairs of s - t nodes remain very close to their values before the attack. This observation demonstrates that the proposed LR model can effectively bypass the BDD module in the ac SE without being detected.

It is worth pointing out that due to the high-dimensional non-linear nature of the ac SE, it is challenging to mathematically prove that the residual change resulting from the proposed approach is less than a certain threshold. Therefore, the feasibility of the proposed approach is validated by numerical simulation.

TABLE I
RESIDUALS OF BDD AFTER FALSE DATA INJECTION

VB ^{+/−}	Residual	VB ^{+/−}	Residual	VB ^{+/−}	Residual	VB ^{+/−}	Residual
2,3	0.0135	3,10	0.0116	5,9	0.0166	9,12	0.0144
2,4	0.0135	3,11	0.0146	5,10	0.0151	9,13	0.0104
2,5	0.0164	3,12	0.0143	5,11	0.0121	9,14	0.0180
2,6	0.0134	3,13	0.0120	5,12	0.0109	10,11	0.0118
2,9	0.0150	3,14	0.0114	5,13	0.0104	10,12	0.0145
2,10	0.0137	4,5	0.0198	5,14	0.0115	10,13	0.0121
2,11	0.0176	4,6	0.0133	6,9	0.0163	10,14	0.0104
2,12	0.0115	4,9	0.0194	6,10	0.0102	11,12	0.0139
2,13	0.0129	4,10	0.0182	6,11	0.0119	11,13	0.0157
2,14	0.0139	4,11	0.0174	6,12	0.0143	11,14	0.0117
3,4	0.0151	4,12	0.0119	6,13	0.0107	12,13	0.0192
3,5	0.0140	4,13	0.0178	6,14	0.0161	12,14	0.0136
3,6	0.0174	4,14	0.0195	9,10	0.0165	13,14	0.0178
3,9	0.0135	5,6	0.0109	9,11	0.0199		

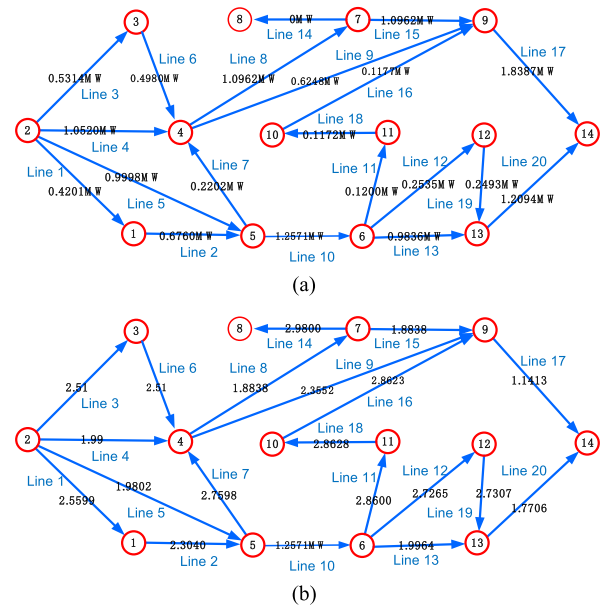


Fig. 4. (a) False data flow and (b) FD-flow graph for IEEE 14-bus system between s - t pair of (2, 14).

This is consistent with the previous LR attack literature based on ac SE [28], [29].

B. Critical Branch Identification for AC State Estimation

We first use the IEEE 14-bus system to analyze the features of the critical branch sets (i.e., min-cut sets) between different source and sink nodes. We inject false data between different source and sink nodes to construct the FD-flow graph. Take s - t pair (2,14) as an example, where the normal load levels of node 2 and node 14 are 27.10 MW and 14.90 MW, respectively. According to, we inject $20\% \times 14.90 \text{ MW} = 2.98 \text{ MW}$ of false data between s - t pair (2,14). The false data flow is shown in Fig. 4(a). Then, the circulation of false data is converted into the FD-flow graph as shown in Fig. 4(b). Similarly, we can construct all FD-flow graphs for 55 pairs of s - t nodes using the above-mentioned procedure. Then, the Min-cuts are calculated according to the FD-flow graphs. The results of the analysis are shown in Table II. Note that in Table II, values with parentheses represent the criticality index of critical branches calculated

TABLE II
MIN-CUT BETWEEN DIFFERENT s - t VERTICES

VB^{s-t}	Min-cut	VB^{s-t}	Min-cut
2,3	3(23.26),6(15.9)	5,9	9(1.16), 10(1.44) ,15(2.04)
2,4	2(7.28), 3(7.33) ,4(14.68),5(10.84)	5,10	10(1.77) ,16(3.26)
2,5	2(1.14), 3(0.65) ,4(1.31),5(1.75)	5,11	11(0.54),16(0.44)
2,6	3(1.59) ,4(3.17), 10(6.84)	5,12	12(1.74),19(1.27)
2,9	9(9.75), 10(11.00) ,15(17.11)	5,13	12(0.75),13(2.91), 17(1.05)
2,10	10(2.36) ,16(4.65)	5,14	10(2.19) ,17(2.82)
2,11	11(0.53),16(0.45)	6,9	10(3.91) ,11(3.74), 17(2.34)
2,12	12(1.73),19(1.27)	6,10	11(3.14),16(3.41)
2,13	3(2.39) ,4(4.78),10(9.33)	6,11	11(0.73),16(0.26)
2,14	10(8.09) , 17(10.96)	6,12	12(1.80),19(1.21)
3,4	3(76.95) , 6(110.51)	6,13	12(1.84),13(7.25), 17(1.15)
3,5	3(2.20) , 6(2.56)	6,14	17(4.97) ,20(5.28)
3,6	3(4.61) , 6(5.71)	9,10	11(0.73),16(5.79)
3,9	3(30.11) , 6(41.36)	9,11	11(0.36),16(0.62)
3,10	10(2.26) ,16(4.71)	9,12	12(1.67),19(1.34)
3,11	11(0.44),16(0.57)	9,13	12(2.00),13(7.75), 17(5.08)
3,12	3(1.36) , 6(1.71)	9,14	17(12.96) ,20(5.22)
3,13	3(6.60) , 6(8.39)	10,11	11(0.25),18(0.73)
3,14	10(7.81) , 17(11.07)	10,12	16(1.62),18(1.36)
4,5	1(0.33),5(0.42),7(3.69), 10(0.24)	10,13	11(2.81),16(3.73)
4,6	10(6.53) ,11(2.15),17(1.34)	10,14	16(4.90),20(2.16)
4,9	8(32.97),9(18.82),10(18.12)	11,12	12(0.57),19(0.42)
4,10	10(2.15) ,16(4.77)	11,13	11(0.67),16(0.31)
4,11	11(0.52),16(0.47)	11,14	11(0.49), 17(0.58)
4,12	12(1.73),19(1.28)	12,13	12(1.26),19(1.74)
4,13	12(2.30),13(8.94),17(3.62)	12,14	12(1.48),20(1.73)
4,14	10(7.52) , 17(11.18)	13,14	17(5.56) ,20(9.34)
5,6	10(3.24) ,11(0.84), 17(0.53)		

*Bold data represents the critical branches.

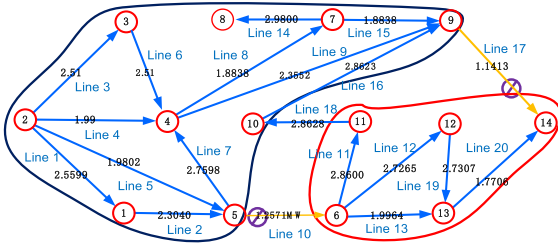


Fig. 5. Min-cut for IEEE 14-bus system between s - t pair of (2, 14).

according to (18). For instance, for s - t pair (2,3), the criticality index of branch 3 is 23.26, and the criticality index for branch 6 is 15.9. Based on the previous discussion in Section III-C, a larger criticality index indicates the branch is more critical for a given s - t pair. Therefore, Branch 3 can be considered more critical for s - t pair (2,3). Similarly, for s - t pair (2,4), the critical branches are branches 2, 3, 4, and 5 with the associated criticality indices of 7.28, 7.73, 14.68, and 10.84, respectively. It is thus evident that branch 4 has the largest criticality index among the four identified branches and can be given priority to defend to block the FD-flow between s - t pair (2,4).

Furthermore, among the set of 55 min-cuts, it can be observed that the criticality indices of branches 3 and 6 are often greater than others. This observation provides us with an estimation that strengthening branches 3 and 6 would provide effective disturbance to the circulation of the FD-flow. Meanwhile, when we examine the min-cuts for the s - t pairs, we can identify that branch 6 (for s - t pairs such as (2,3), (3,4), and (3,9)), 10 (for s - t pairs such as (2,14), (3,14), and (9,13)), 3 (for s - t pairs such as (3,4), (3,9), and (3,13)), and 17 (for s - t pairs such as (3,14), (4,14), and (9,14)) are some of the most noticeable critical pathways that transmit the heaviest FD-flow.

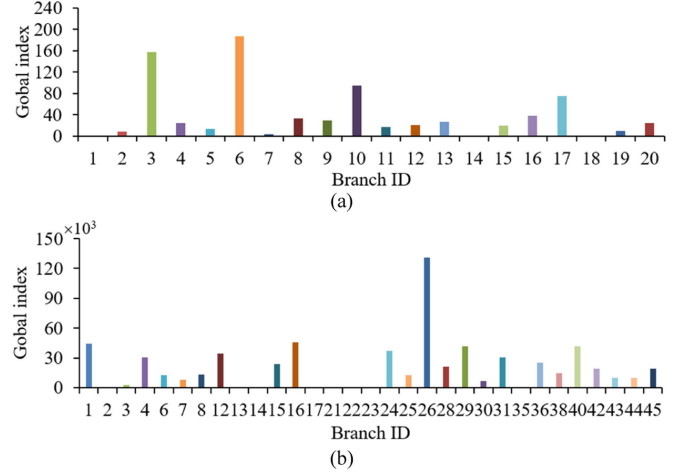


Fig. 6. Global indices for (a) IEEE 14-bus system. (b) IEEE 39-bus system.

In particular, we have shown the min-cut in Fig. 5 between s - t pair (2,14). It can be observed that while there are multiple valid paths for the false data to flow from bus 2 to bus 14, blocking branch 10 (between buses 5 and 6) and branch 17 (between buses 9 and 14) will result in the “complete separation” between (2,14), meaning that it is impossible to establish a valid path that allows the false data to flow from bus 2 to bus 14 given that the false data flow is directional. Based on the flow over branches as shown in Fig. 5, we can observe that the maximum flow for this s - t pair is 1.18 (over branch 10) plus 1.7 (over branch 4), which is roughly 2.88.

Moreover, the global indices of the IEEE 14-bus system are calculated according to the local indices and are shown in Fig. 6(a). We can observe that the top three most critical branches are branches 3, 6, and 10. This observation matches our previous estimation made based on the min-cut results in Table II. Utilizing this information, the system operator can estimate that by strengthening branches 3, 6, and 10, the system can be effectively safeguarded from the measurement temperaments needed to launch the LR attacks. Similarly, the global indices of branches in the IEEE 39-bus system are given in Fig. 6(b). Branches 26, 16, 1, and 29 are ranked the top four most vulnerable branches. Therefore, it is anticipated that these branches can be strengthened to cope with the LR attacks.

Finally, we analyze the impacts of the load shift factor (i.e., τ) on the determination of critical branches. We take $\tau = 10\%$, 15% , 20% , 25% , and 30% to calculate the global indices for the IEEE 14-bus system and the IEEE 39-bus system, respectively. The results are shown in Fig. 7. It can be clearly observed that while the values of the global indices increase when τ increases, the rankings of critical branches have not significantly changed in both cases. In other words, our observation has shown that the selection of τ doesn’t necessarily affect the criticality of branches in the IEEE 14- and 39-bus systems.

C. Performance Verification

Once the set of critical branches is identified for the IEEE 14- and 39-bus systems, we can strengthen a selected number

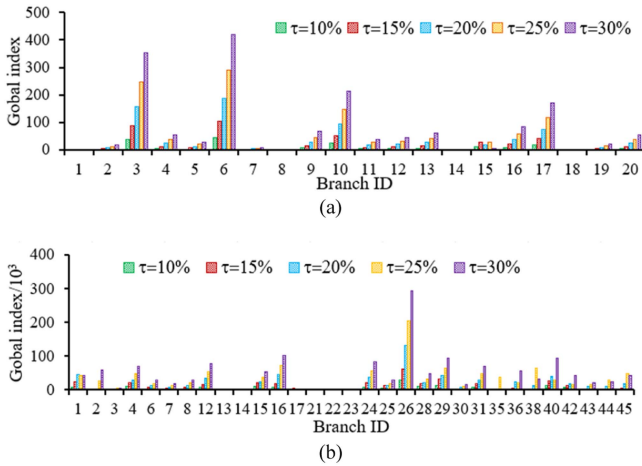


Fig. 7. Impacts of τ on critical branches for the (a) IEEE 14-bus system and (b) IEEE 39-bus system.

of them to interrupt FDI s and verify the system's updated response to the LR attacks. For the IEEE 14-bus system, we focus on evaluating the effect of the proposed approach when the system operator has the defensive resources to strengthen up to five of the most vulnerable branches. For the IEEE 39-bus system, we evaluate the proposed approach when the system operator can afford to strengthen up to ten branches. All critical branches are identified based on their rankings of the global indices. Due to the shortage of comparative approaches based on ac SE in the literature, the performance of the proposed approach is compared with the single-level CBI, the bilevel CBI and the trilevel CBI approaches that were developed based on dc SE. Specifically, the single-level CBI, hereinafter referred to as the SL-CBI, is modeled according to [10], and the bilevel CBI approach, hereinafter referred to as the power flow-based CBI (PF-CBI), ranks critical branches according to their redistributed power flow following an LR attack [5]. On the other hand, the defender-attacker-defender trilevel CBI, hereinafter referred to as the Tri-CBI, is adopted from and modified based on [13]. To investigate the effectiveness of the three CBI approaches, once the critical branches are identified by each approach and strengthened accordingly, we randomly construct 2000 attack vectors and inject them into the system to investigate their damaging effects in terms of average operation cost and load shedding following the redispatch. It is worth pointing out that the operation cost and load shedding determine the overall mitigation effectiveness of a defense strategy following an LR attack. Specifically, a lower operation cost and less load shedding cost is more favorable to the system operator as it indicates that the defense strategy reduces the direct and possible subsequent impacts of the LR attack. The results for the IEEE 14- and 39-bus systems are shown in Fig. 8.

We first analyze the results obtained from the IEEE 14-bus system. As shown in Fig. 8(a) and (b), we can observe that identifying and strengthening more branches would provide better mitigation against LR attacks for all four methods. In particular, we can observe that the proposed method outperforms the other three methods when the operator strengthens one, three, four, and five branches, respectively. After the selected

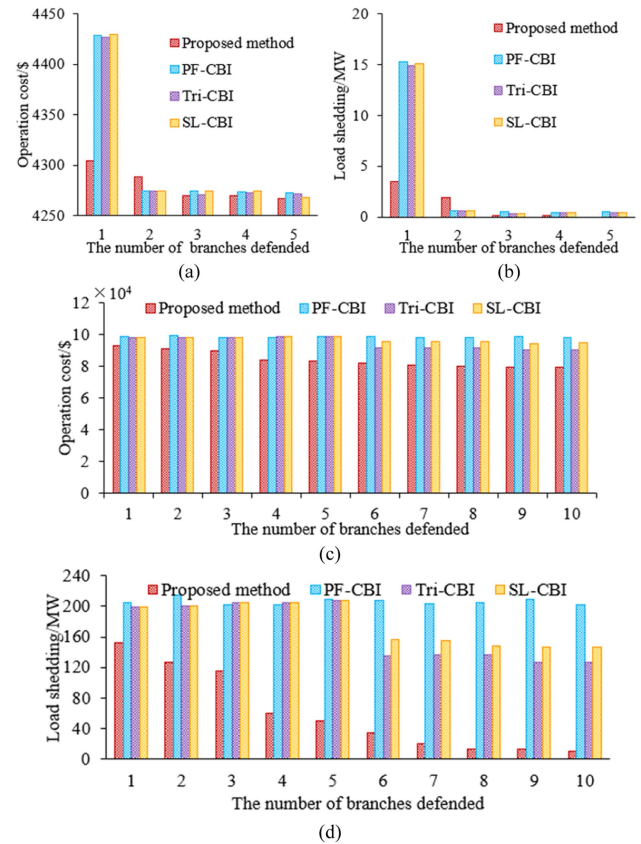


Fig. 8. Operation cost and load shedding after the selected critical branches are strengthened: (a) Operation cost and (b) load shedding for the IEEE 14-bus system. (c) Operation cost and (d) load shedding for the IEEE 39-bus system.

branches are strengthened, the system is capable of remaining operable at a lower average operation cost with less average load shedding in the face of LR attacks. This comparison shows that the proposed approach provides comparable/better overall better mitigation than the conventional BL-CBI, PF-CBI, and Tri-CBI methods. The results for the IEEE 39-bus system are shown in Fig. 8(c) and (d). We can observe that our method offers obvious improvement for average operation cost and load shedding in all cases to improve the operation economy and reduce the risk of blackouts caused by mass loading following the LR attack compared to the other two methods. Based on the above analysis, we can conclude that the proposed CBI strategy is effective in terms of mitigating the adverse impacts of the LR attack.

D. Results for Larger Systems and Computational Efficiency

As mentioned in the previous analysis, another benefit offered by the proposed CBI strategy is its superior scalability, computational efficiency, and ease of deployment, especially compared with the conventional optimization approaches. To illustrate this, we apply the proposed approach to IEEE 118-bus, IEEE 300-bus, and several large-scale system models, including case1354pegase, case1888rte, case1951cfa, case2383wp, and case3375wp models provided in the MatPower package [44].

TABLE III
TOP 10 CRITICAL BRANCHES FOR EACH TESTING SYSTEM

Rank	IEEE 118	IEEE 300	1354 pegase	1888 rte	1951 cfa	2383 wp	3375 wp
1	104	307	68	268	1141	2588	431
2	37	301	1975	269	1145	2614	85
3	121	214	1976	1127	1146	2470	27
4	163	311	1977	1131	272	757	352
5	138	365	1822	1132	273	100	96
6	143	224	1823	442	452	2813	430
7	185	303	400	443	453	2082	348
8	52	44	541	648	1788	2878	443
9	117	321	182	651	1789	763	424
10	66	48	389	652	1790	2245	291

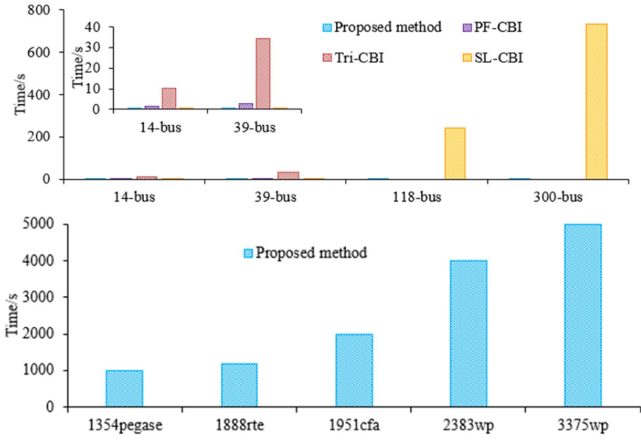


Fig. 9. Comparison of computation efficiencies.

The top 10 critical branches identified for these testing systems are shown in Table III. The computational efficiency of the proposed approach is shown in Fig. 9. We can observe that the proposed CBI approach scales well with the size of the system. Compared with the SL-CBI, the computational complexity of the proposed method and the SL-CBI is not vastly different. However with the increasing size of the system, the computational complexity of the proposed method starts to become lower than that of the SL-CBI. For example, for the 118-bus system, the proposed method only needs 0.152 s while the SL-CBI needs 241 s. In addition, the computational complexity for the PF-CBI and Tri-CBI methods is considerably high (for the IEEE 14- and 39-bus systems) and becomes infeasible when applied to larger systems (for the IEEE 118-bus, IEEE 300-bus, case1354pegase, case1888rte, case1951cfa, case2383wp, and case3375wp systems). This is why their computational performances are not available to report in Fig. 9.

V. CONCLUSION AND FUTURE WORK

This article offers a new perspective on understanding and studying LR attacks based on the flow of FDIs. Unlike the conventional disruption-driven models, our approach focuses on modeling the circulation of the synthesized false measurement data on the cyber-layer of the network and identifying critical branches in the network that carry the heaviest FD-flow. Simulation results show that the proposed CBI approach provides effective mitigation against LR attacks by disrupting

the coordinated and reconciled interactions among FDIs within a network required for the attacker to launch a self-consistent LR attack. The proposed approach is also computationally efficient, showing great potential for large-scale applications. Our work is the first of its kind and lays the groundwork for developing other analyses and mitigation strategies based on the FD-flow graph.

Although the scope of this article focuses on LR attacks, the proposed mechanism of mitigating the threat of a cyber-attack by disrupting the consistency and integrity of false data circulation has the potential to be further extended to other FDI attacks in the smart grid that encompass malicious and coordinated data manipulation. One can also extend this article by evaluating the statistical patterns of false data flow that may result from different attacking scenarios. These patterns can then be used as an additional “risk factor” in determining the critical branches to defend.

APPENDIX

We give the detailed approximation process of the increments of branch power flow as follows.

The increments of branch power flow between two buses are determined by (A1) and (A2) in an ac network:

$$\begin{aligned} \Delta p_{ij} = & (V_i + \Delta V_i)^2 g_{ij} \\ & [-1pt] - (V_i + \Delta V_i) (V_j + \Delta V_j) \\ & \times \left[g_{ij} \cos(\theta_i + \Delta\theta_i - \theta_j - \Delta\theta_j) \right. \\ & \left. + b_{ij} \sin(\theta_i + \Delta\theta_i - \theta_j - \Delta\theta_j) \right] \\ & - V_i^2 g_{ij} + V_i V_j [g_{ij} \cos(\theta_i - \theta_j) \\ & + b_{ij} \sin(\theta_i - \theta_j)] \end{aligned} \quad (\text{A1})$$

$$\begin{aligned} \Delta q_{ij} = & - (V_i + \Delta V_i)^2 b_{ij} \\ & - (V_i + \Delta V_i) (V_j + \Delta V_j) \\ & \times \left[g_{ij} \sin(\theta_i + \Delta\theta_i - \theta_j - \Delta\theta_j) \right. \\ & \left. - b_{ij} \cos(\theta_i + \Delta\theta_i - \theta_j - \Delta\theta_j) \right] \\ & - (-V_i^2 b_{ij} - V_i V_j [g_{ij} \sin(\theta_i - \theta_j) \\ & - b_{ij} \cos(\theta_i - \theta_j)]). \end{aligned} \quad (\text{A2})$$

The following constraints hold for a typical transmission network:

$$\cos(\theta_i - \theta_j) \approx 1; \quad \sin(\theta_i - \theta_j) \approx \theta_i - \theta_j; \quad V_i \approx V_j \approx 1. \quad (\text{A3})$$

Introducing (A1) and (A2) into (A3), we can have

$$\Delta p_{ij} \approx -(1 + \Delta V_i)^2 b_{ij} (\theta_i + \Delta\theta_i - \theta_j - \Delta\theta_j) + b_{ij} (\theta_i - \theta_j) \quad (\text{A4})$$

$$\Delta q_{ij} \approx -(1 + \Delta V_i)^2 g_{ij} (\theta_i + \Delta\theta_i - \theta_j - \Delta\theta_j) + g_{ij} (\theta_i - \theta_j) \quad (\text{A5})$$

Under the common assumption that the resistance of a transmission line is significantly less than its reactance, i.e., $b_{ij} \gg g_{ij}$, (A4) and (A5) confirms that after the false active load power measurement is injected to load buses in the transmission

network, it predominately affects the active power flow distribution of the network Δp_{ij} , and has a negligible effect on the reactive power flow distribution Δq_{ij} . Especially, since we can extend $V_i \approx V_j \approx 1$ to have $V_i + \Delta V_i \approx V_j + \Delta V_j \approx 1$, it suggests that ΔV_i is close to zero, which allows us to further approximate (A4) as

$$\Delta p_{ij} \approx -b_{ij} (\Delta \theta_i - \Delta \theta_j). \quad (\text{A6})$$

REFERENCES

- [1] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1630–1638, Jul. 2017.
- [2] 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.
- [3] R. M. Lee, M. J. Assante, and T. Conway, "Analysis of the cyber attack on the Ukrainian power grid," E-ISAC, Washington, DC, USA, TLP: White, Defense Use Case, Mar. 2016. [Online]. Available: <https://ics.sans.org/ics-library>
- [4] M. J. Assante, R. M. Lee, and T. Conway, "Modular ICS malware," E-ISAC, Washington, DC, USA, TLP: White - ICS Defense Use Case No. 6, Aug. 2017. [Online]. Available: <https://ics.sans.org/ics-library>
- [5] 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.
- [6] 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.
- [7] R. Kaviani and K. W. Hedman, "A detection mechanism against load-redistribution attacks in smart grids," *IEEE Trans. Smart. Grid*, vol. 12, no. 1, pp. 704–714, Jan. 2021.
- [8] C. Chen, Y. Chen, J. Zhao, K. Zhang, M. Ni, and B. Ren, "Data-driven resilient automatic generation control against false data injection attacks," *IEEE Trans. Ind. Inform.*, vol. 17, no. 12, pp. 8092–8101, Dec. 2021.
- [9] L. Yao, N. Peng, and K. R. Michael, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, May 2011, Art. no. 13.
- [10] 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.
- [11] S. Gao, J. Lei, J. Shi, X. Wei, M. Dong, and Z. Han, "Assessment of overloading correlations among transmission lines under load redistribution attacks," *IEEE Trans. Smart Grid*, vol. 13, no. 2, pp. 1570–1581, Mar. 2022.
- [12] C. Pei, Y. Xiao, W. Liang, and X. Han, "Detecting false data injection attacks using canonical variate analysis in power grid," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 971–983, Apr./Jun. 2021.
- [13] 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.
- [14] T. C. Gulcu, V. Chatziafratis, Y. Zhang, and O. Yağın, "Attack vulnerability of power systems under an equal load redistribution model," *IEEE/ACM Trans. Netw.*, vol. 26, no. 3, pp. 1306–1319, Jun. 2018.
- [15] Y. Xiang, Z. Ding, Y. Zhang, and L. Wang, "Power system reliability evaluation considering load redistribution attacks," *IEEE Trans. Smart Grid*, vol. 8, no. 2, pp. 889–901, Mar. 2017.
- [16] C. Pei, Y. Xiao, W. Liang, and X. Han, "PMU placement protection against coordinated false data injection attacks in smart grid," *IEEE Trans. Ind. Appl.*, vol. 56, no. 4, pp. 4381–4393, Jul./Aug. 2020.
- [17] S. Bi and Y. J. Zhang, "Graphical methods for defense against false-data injection attacks on power system state estimation," *IEEE Trans. Smart Grid*, vol. 5, no. 3, pp. 1216–1227, May 2014.
- [18] R. Kaviani and K. W. Hedman, "An enhanced energy management system including a real-time load-redistribution threat analysis tool and cyber-physical SCED," *IEEE Trans. Power Syst.*, vol. 37, no. 5, pp. 3346–3358, Sep. 2022.
- [19] 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. 2068–2019, Mar. 2019.
- [20] X. Liu, Z. Li, and Z. Li, "Optimal protection strategy against false data injection attacks in power systems," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1802–1810, Jul. 2017.
- [21] J. Lei et al., "A reinforcement learning approach for defending against multiscenario load redistribution attacks," *IEEE Trans. Smart Grid*, vol. 13, no. 5, pp. 3711–3722, Sep. 2022.
- [22] Y. Liu, S. Gao, J. Shi, X. Wei, and Z. Han, "Sequential-mining-based vulnerable branches identification for the transmission network under continuous load redistribution attacks," *IEEE Trans. Smart Grid*, vol. 11, no. 6, pp. 5151–5160, Nov. 2020.
- [23] Y. Liu, S. Gao, J. Shi, X. Wei, Z. Han, and T. Huang, "Pre-overload-graph-based vulnerable correlation identification under load redistribution attacks," *IEEE Trans. Smart Grid*, vol. 11, no. 6, pp. 5216–5226, Nov. 2020.
- [24] Z. Zhang, R. Deng, D. K. Y. Yau, P. Cheng, and J. Chen, "Analysis of moving target defense against false data injection attacks on power grid," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 2320–2335, 2020.
- [25] S. Lakshminaryana and D. K. Y. Yau, "Cost-benefit analysis of moving-target defense in power grids," *IEEE Trans. Power Syst.*, vol. 36, no. 2, pp. 1152–1163, Mar. 2021.
- [26] B. Liu and H. Yu, "Optimal D-FACTS placement in moving target defense against false data injection attacks," *IEEE Trans. Smart Grid*, vol. 11, no. 5, pp. 4345–4357, Sep. 2020.
- [27] 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. 18, no. 2, pp. 1023–1025, Mar. 2017.
- [28] L. Che, X. Liu, Z. Shuai, Z. Li, and Y. Wen, "Cyber cascades screening considering the impacts of false data injection attacks," *IEEE Trans. Power Syst.*, vol. 33, no. 6, pp. 6545–6556, Nov. 2018.
- [29] 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.
- [30] G. Chaojun, P. Jirutitharoen, and M. Motani, "Detecting false data injection attacks in AC state estimation," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2476–2483, Sep. 2015.
- [31] R. Jiao, G. Xun, X. Liu, and G. Yan, "A new AC false data injection attack method without network information," *IEEE Trans. Smart Grid*, vol. 12, no. 6, pp. 5280–5289, Nov. 2021.
- [32] M. Jorjani, H. Seifi, and A. Y. Varjani, "A graph theory-based approach to detect false data injection attacks in power system AC state estimation," *IEEE Trans. Ind. Inform.*, vol. 17, no. 4, pp. 2465–2475, Apr. 2021.
- [33] M. Jin, J. Lavaei, and K. H. Johansson, "Power grid AC-based state estimation: Vulnerability analysis against cyber attacks," *IEEE Trans. Autom. Control*, vol. 64, no. 5, pp. 1784–1799, May 2019.
- [34] C. Liu, H. Liang, and T. Chen, "Network parameter coordinated false data injection attacks against power system AC state estimation," *IEEE Trans. Smart Grid*, vol. 12, no. 2, pp. 1626–1639, Mar. 2021.
- [35] H. Zhang, B. Liu, and H. Wu, "Net load redistribution attacks on nodal voltage magnitude estimation in AC distribution networks," in *Proc. IEEE PES Innov. Smart Grid Technol. Europe*, 2020, pp. 46–50.
- [36] M. Esmalifalak, H. Nguyen, R. Zheng, L. Xie, L. Song, and Z. Han, "A stealthy attack against electricity market using independent component analysis," *IEEE Syst. J.*, vol. 12, no. 1, pp. 297–307, Mar. 2018.
- [37] S. Mohammadi, F. Eliassen, Y. Zhang, and H.-A. Jacobsen, "Detecting false data injection attacks in peer to peer energy trading using machine learning," *IEEE Trans. Dependable Secure Comput.*, vol. 19, no. 5, pp. 3417–3431, Sep./Oct. 2022.
- [38] Y. Zhang, J. Wang, and B. Chen, "Detecting false data injection attacks in smart grids: A semi-supervised deep learning approach," *IEEE Trans. Smart Grid*, vol. 12, no. 1, pp. 623–634, Jan. 2021.
- [39] C. Chen et al., "Data-driven detection of stealthy false data injection attack against power system state estimation," *IEEE Trans. Ind. Inform.*, vol. 18, no. 12, pp. 8467–8476, Dec. 2022.
- [40] K. R. Davis et al., "A cyber-physical modeling and assessment framework for power grid infrastructures," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2464–2475, Sep. 2015.
- [41] A. Dwivedi and X. Yu, "A maximum-flow-based complex network approach for power system vulnerability analysis," *IEEE Trans. Ind. Inform.*, vol. 9, no. 1, pp. 81–88, Feb. 2013.
- [42] J. Fang, C. Su, Z. Chen, H. Sun, and P. Lund, "Power system structural vulnerability assessment based on an improved maximum flow approach," *IEEE Trans. Smart Grid*, vol. 9, no. 2, pp. 777–785, Mar. 2018.
- [43] Y. Wang, Q. Chen, C. Kang, and Q. Xia, "Clustering of electricity consumption behavior dynamics toward big data applications," *IEEE Trans. Smart Grid*, vol. 7, no. 5, pp. 2437–2447, Sep. 2016.
- [44] R. D. Zimmerman, C. E. Murillo-Sanchez, "MATPOWER user's manual," Version 7.1. 2020. [Online]. Available: <https://matpower.org/docs/MATPOWER-manual-7.1.pdf>

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. His research interests include 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, The Netherlands.

His current research focuses on vulnerability assessment of cyber-physical systems and synthetic networks.

Jian Shi (Senior Member, IEEE) received the Ph.D. degree in electrical and computer engineering from Mississippi State University, Starkville, MS, USA, in 2014.

He is currently an Assistant Professor with the Engineering Technology Department, University of Houston, Houston, TX, USA. His research interests include microgrid modeling and control, transportation electrification, and cyber-physical power systems.

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. His research interests include power system protection and automation, online monitoring of electrical equipment, traction power supplies, railway electrification, and power system security.

Xingpeng Li (Senior Member, IEEE) received the B.S. degree in electrical engineering from Shandong University, Jinan, China, in 2010, the M.S. degree in electrical engineering from Zhejiang University, Hangzhou, China, in 2013, the second M.S. degree in industrial engineering and the Ph.D. degree in electrical engineering from Arizona State University, Tempe, AZ, USA, in 2016 and 2017, respectively, and the third M.S. degree in computer science from the Georgia Institute of Technology, Atlanta, GA, USA, in 2023.

He is currently an Assistant Professor with the Department of Electrical and Computer Engineering, University of Houston, Houston, TX, USA. He was with ISO New England, Holyoke, MA, USA, and PJM Interconnection, Audubon, PA, USA. Before joining the University of Houston, he was a Senior Application Engineer for ABB (now Hitachi Energy), San Jose, CA, USA. His research interests include power system operations, control and planning, and applications of optimization and machine learning in power systems, energy markets, and microgrids.

Zhu Han (Fellow, IEEE) received the B.S. degree in electronic engineering from Tsinghua University, Beijing, China, in 1997, and the M.S. and Ph.D. degrees in electrical and computer engineering from the University of Maryland, College Park, MD, USA, in 1999 and 2003, respectively.

From 2000 to 2002, he was a Research and Development Engineer with JDSU, Germantown, MD, USA. From 2003 to 2006, he was a Research Associate with the University of Maryland. From 2006 to 2008, he was an Assistant Professor with Boise State University, Boise, ID, USA. He is currently a John and Rebecca Moores Professor with the Electrical and Computer Engineering Department and the Computer Science Department, University of Houston, Houston, TX, USA. He is also with the Department of Computer Science and Engineering, Kyung Hee University, Seoul, South Korea. His research interests include wireless resource allocation and management, wireless communications and networking, game theory, big data analysis, security, and smart grids.

Dr. Han was an IEEE Communications Society Distinguished Lecturer from 2015 to 2018. He has been an AAAS Fellow and an ACM Distinguished Member since 2019. He has been among the 1% of the highly cited researchers since 2017 according to Web of Science. He was the recipient of an NSF Career Award in 2010, the Fred W. Ellersick Prize of the IEEE Communication Society in 2011, the EURASIP Best Paper Award for the Journal on Advances in Signal Processing in 2015, the IEEE Leonard G. Abraham Prize in the field of Communications Systems (Best Paper Award in IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS) in 2016, and several best paper awards in IEEE conferences.