False Data Injection on State Estimation in Power Systems—Attacks, Impacts, and Defense: A Survey

Ruilong Deng, *Member, IEEE*, Gaoxi Xiao, *Member, IEEE*, Rongxing Lu, *Senior Member, IEEE*, Hao Liang, *Member, IEEE*, and Athanasios V. Vasilakos, *Senior Member, IEEE*

***Abstract*—The accurately estimated state is of great importance for maintaining a stable running condition of power systems. To maintain the accuracy of the estimated state, bad data detection (BDD) is utilized by power systems to get rid of erroneous measurements due to meter failures or outside attacks. However, false data injection (FDI) attacks, as recently revealed, can circumvent BDD and insert any bias into the value of the estimated state. Continuous works on constructing and/or protecting power systems from such attacks have been done in recent years. This survey comprehensively overviews three major aspects: constructing FDI attacks; impacts of FDI attacks on electricity market; and defending against FDI attacks. Specifically, we first explore the problem of constructing FDI attacks, and further show their associated impacts on electricity market operations, from the adversary's point of view. Then, from the perspective of the system operator, we present countermeasures against FDI attacks. We also outline the future research directions and potential challenges based on the above overview, in the context of FDI attacks, impacts, and defense.**

***Index Terms*—Cyber security, electricity market, false data injection (FDI), smart grid, state estimation.**

I. Introduction

THE power system is a complex and interconnected system for delivering electricity from generation to consumers. The electricity grid is consistently operated and monitored by supervisory control and data acquisition (SCADA) system to guarantee a normal running state. Specifically, state variables of power systems are estimated from meter measurements; and the system operator will leverage the estimated state to control the physical space [1]–[3].

With the incorporation of cyber space such as information and communications technology, the power system is making strides toward smart grid [4]–[8]. However, potential threats in terms of cyber attacks would be introduced into the system [9]–[18]. Taking false data injection (FDI) attacks, for example, which can circumvent bad data detection (BDD) and insert any bias into the value of the estimated state stealthily [19], [20]. FDI attacks were first named in 2009 by Liu *et al.* [19]. After that, they are widely recognized to be new cyber attacks on power system state estimation. Due to historical reasons, FDI attacks are also known as stealthy deception attacks, load redistribution (LR) attacks, malicious data attacks, data integrity attacks, and so on, proposed by different research groups at different time. Compared with the traditional physical attacks, FDI attacks can be launched multiple times without being detected. If FDI attacks are well-coordinated with physical attacks, line outages initiated by physical attacks could be masked [16], [17]. Therefore it is of critical importance to analyze the attack model of adversaries[1] such that the corresponding defense can be proposed to secure power systems from FDI attacks.

As shown in Fig. 1, the building blocks of a power system include generation, transmission, distribution, consumers, and control center, with two-way communications among them. The power system employs remote terminal units (RTUs), such as meters, sensors, and actuators, to collect meter measurements through communication networks, including power injections on buses and power flows on branches. The control center is equipped with SCADA system, whose functionalities include BDD, state estimation, unit commitment, economic dispatch, fault or disturbance analysis, power flow optimization, load forecasting, etc. With meter measurements, the value of state variables representing the operating condition of power systems are estimated, including phase angles of bus voltages. Then the control center will leverage the estimated state to control the

Manuscript received June 24, 2016; revised August 30, 2016; accepted September 24, 2016. Date of publication September 28, 2016; date of current version April 18, 2017. This work was supported in part by the EEE Cybersecurity Research Program at Nanyang Technological University, in part by the Alberta Innovates – Technology Futures postdoctoral fellowship, in part by a research grant from the Natural Science and Engineering Research Council of Canada, and in part by the Open Research Project of the State Key Laboratory of Industrial Control Technology, Zhejiang University, China (ICT1600168). Paper no. TII-16-0563. *(Corresponding author: R. Lu.)*

R. Deng and H. Liang are with the Department of Electrical and Computer Engineering, University of Alberta, Edmonton, AB T6G 1H9, Canada (e-mail: ruilong@ualberta.ca; hao2@ualberta.ca).

G. Xiao is with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore 639798 (e-mail: egxxiao@ntu.edu.sg).

R. Lu is with the Faculty of Computer Science, University of New Brunswick, Fredericton, NB E3B 5A3, Canada (e-mail: rlu1@unb.ca).

A. V. Vasilakos is with the Department of Computer Science, Electrical and Space Engineering, Lulea University of Technology, Lulea 97187, Sweden (e-mail: athanasios.vasilakos@ltu.se).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TII.2016.2614396

[1]Throughout the paper, "adversary" and "attacker" are used interchangeably.

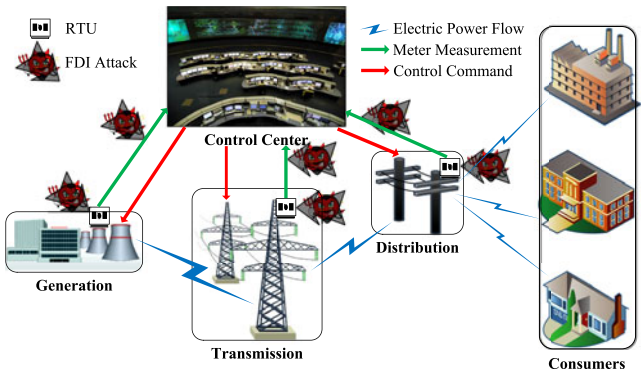


Fig. 1. FDI attacks on state estimation in a power system.

power grid. If the adversary has the capability to manipulate meter measurements coordinately, he/she could launch FDI attacks to bias the estimated state. Meter measurements can be manipulated by either compromising RTUs directly or tampering with the data reported from the meter to the control center.

The concept of FDI attacks, as a new type of cyber attacks on state estimation in smart grid, was first developed in 2009 by Liu *et al.* [19], [20]. After that, continuous works on constructing and/or defending against such attacks have been done in recent years. For the purpose of quantifying the potential threat to a power grid, two classes of security indices are introduced by Sandberg *et al.* [21], corresponding to two different types of FDI attacks, namely sparse attacks and small magnitude attacks, respectively. One of such security metrics is used by Teixeira *et al.* [22] to show limitations of linear attack policies on the nonlinear ac power flow model. Besides, they further propose a generalized approach to construct deception attacks on state estimation in smart grid, with specific target constraints [23]. More references on constructing FDI attacks can be found in [24]–[28].

Dán *et al.* [29] consider clusters of meters at the same attack cost for the adversary to compromise, and propose greedy algorithms for perfect and partial countermeasures against FDI attacks. The concept of LR attacks was first introduced in 2011 by Yuan *et al.* [30], [31] as a special class of FDI attacks. Kosut *et al.* [32]–[35] investigate two different regimes of FDI attacks on state estimation in smart grid, and investigate how FDI attacks will interfere electricity market operations, because the biased state estimation result will be used for economic dispatch. Xie *et al.* [36], [37] show that the adversary can launch FDI attacks for continuous financial arbitrage, e.g., virtual bidding at selected pairs of buses. Jia *et al.* [38], [39] consider making profit for the generator at a specific bus by launching FDI attacks on the real-time market. Besides, they further investigate three different scenarios: the adversary may have full, partial, or zero knowledge of real-time measurements [40]. Bi and Zhanget al. [41] show that by fabricating a fake transmission congestion pattern, FDI attacks can manipulate real-time electricity price at any target bus. More references on how FDI attacks will impact electricity market can be found in [42] and [43].

Bobba *et al.* [44] explore how to detect FDI attacks: One way is to secure basic measurements which are selected strategically, while the other way is to verify state variables independently which are selected strategically. Kim and Poor [45] investigate constructing FDI attacks on the power grid based on linearized measurement models, and propose strategic countermeasures against such attacks, by either immunizing a small number of meter measurements or deploying phasor measurement units (PMUs). Giani *et al.* [46], [47] consider unobservable data integrity attacks on power systems, and also present corresponding defense approaches by means of PMUs. More references on both constructing FDI attacks and defending against them can be found in [48]–[51].

Bi and Zhang [52] propose countermeasures against FDI attacks by protecting critical state variables. After characterizing the problem into a Steiner tree in graph theory, graphical methods are leveraged to select the minimum number of meter measurements [53]. In addition, they further propose a mixed protection strategy, in case that either fails to obtain the defense objective [54], [55]. Göl and Abur [56], [57] identify the vulnerability of state estimation against cyber attacks and provide two PMU-based countermeasures, by either converting critical measurements to redundant ones or eliminating the leveraging effect of leverage measurements. More references on defending against FDI attacks can be found in [58]–[66].

In summary, the topic of FDI attacks has drawn considerable attention in the field of smart grid cyber security during past few years. As there exist considerable contributions on this research issue, a comprehensive survey is in urgent need to address the challenges. Up to now, only three surveys on FDI attacks are found in [67]–[69]. However, they only review a few literatures, and do not touch much technical depth on FDI attacks. Besides, how FDI attacks impact electricity market has not been thoroughly analyzed either. Therefore, in this paper, we intend to survey all literatures to our best knowledge, disclose the mathematical details on FDI attacks and defense, and further investigate their associated impacts on electricity market operations. To sum up, the main contributions of this paper are as follows:

1) This paper intends to provide a comprehensive survey to date on all FDI literatures to the best knowledge.
2) Besides, this paper summarizes the detailed mathematical and theoretical depths on FDI attacks and defense.
3) Further more, this paper thoroughly surveys the impact of FDI attacks on electricity market for the first time.
4) Finally, this paper classifies existing literatures on FDI attacks, impacts, and defense into sophisticated categories.

The rest of this survey is organized as follows. From the adversary's point of view, we explore and understand how to construct FDI attacks in Section II. In Section III, we further show and demonstrate the impacts of FDI attacks on electricity market. In Section IV, from the perspective of the system operator, we present and analyze defense and countermeasures against FDI attacks. From the above overview, potential extension opportunities are outlined in Section V. In Section , we draw concluding remarks.

II. Constructing FDI Attacks

This section will explore and understand the problem of constructing FDI attacks from the perspective of the adversary.

A. FDI Attacks

We focus on a steady-state and lossless power transmission system with $n+1$[2] buses and a set $\mathcal{M}=\{1,2,\ldots,m\}$ of meters. The state of a power system is usually composed of bus voltage magnitudes and phase angles. The meter data of a power system typically includes active and reactive parts of bus power injection and branch power flow measurements. Based on the ac power flow model, the relationship between the meter data $\boldsymbol{z}$ and the system state $\boldsymbol{x}$ is [3, ch. 2]

$$\boldsymbol{z}=\boldsymbol{h}\left(\boldsymbol{x}\right)+\boldsymbol{e} \tag{1}$$

where $\boldsymbol{h}\left(\boldsymbol{x}\right)$ is the nonlinear measurement function of $\boldsymbol{x}$ and $\boldsymbol{e}$ is the additive noise with covariance matrix $\boldsymbol{R}$. For large power systems, state estimation using the nonlinear ac power flow model would be computationally expensive and even not always converge to an optimal solution in many cases. Thus, power system engineers sometimes use a linearized dc power flow model to approximate the ac model. The dc model is less accurate, but simpler and more robust than the ac model. Besides, the dc model is often used in real-time operations such as the computation of real-time local marginal price. In the dc model, the system state can reduce to just bus phase angles, and the meter data can reduce to only the active part of bus power injection and branch power flow measurements. The nonlinear measurement function $\boldsymbol{h}\left(\boldsymbol{x}\right)$ is linearized around the operating point. In the dc model, state estimation is to estimate the value of state variables $\boldsymbol{x}\in\mathbb{R}^{n\times 1}$ from meter measurements $\boldsymbol{z}\in\mathbb{R}^{m\times 1}$, in face of independent and uncertain measurement noises (errors) $\boldsymbol{e}\in\mathbb{R}^{m\times 1}$, assumed to follow distributions with zero mean and diagonal covariance matrix $\boldsymbol{R}$. The n state variables are the n bus phase angles $\boldsymbol{x}=\boldsymbol{\theta}$, and the m meter measurements are the observed active power injections (power generation minus load) on buses and the observed active power flows on branches. Based on the dc power flow model, the relationship between meter measurements $\boldsymbol{z}$ and state variables $\boldsymbol{x}$ is [3, ch. 2]

$$\boldsymbol{z}=\boldsymbol{H}\boldsymbol{x}+\boldsymbol{e} \tag{2}$$

where $\boldsymbol{H}\in\mathbb{R}^{m\times n}$ is the measurement Jacobian matrix.

The state estimation problem is to find an estimate $\hat{\boldsymbol{x}}$ of state variables $\boldsymbol{x}$ that is the best fit of meter measurements $\boldsymbol{z}$. Based on the ac power flow model (1) and the weighted least-squares (WLS) criterion, the state estimation problem is to find an estimate $\hat{\boldsymbol{x}}$ that minimizes the WLS error

$$\hat{\boldsymbol{x}}=\arg\min_{\boldsymbol{x}}\left[\boldsymbol{z}-\boldsymbol{h}\left(\boldsymbol{x}\right)\right]^{\intercal}\boldsymbol{W}\left[\boldsymbol{z}-\boldsymbol{h}\left(\boldsymbol{x}\right)\right] \tag{3}$$

where the weight matrix $\boldsymbol{W}\triangleq\boldsymbol{R}^{-1}$ (i.e., a diagonal matrix whose entries are reciprocals of the variances of measurement errors $\boldsymbol{e}$). In practice, the ac state estimation is nonlinear and implemented iteratively [70, ch. 10]. For example, the Gauss–Newton iteration or Newton–Raphson iteration can be used until the solution converges. The process is time consuming and does not guarantee convergence to the global optimal value. Based on the dc power flow model (2) and the WLS criterion, the state estimation problem is to find an estimate $\hat{\boldsymbol{x}}$ that minimizes the WLS error

$$\hat{\boldsymbol{x}}=\arg\min_{\boldsymbol{x}}\left(\boldsymbol{z}-\boldsymbol{H}\boldsymbol{x}\right)^{\intercal}\boldsymbol{W}\left(\boldsymbol{z}-\boldsymbol{H}\boldsymbol{x}\right). \tag{4}$$

The dc state estimation is linear with a closed-form solution [70, ch. 3]

$$\hat{\boldsymbol{x}}=\left(\boldsymbol{H}^{\intercal}\boldsymbol{W}\boldsymbol{H}\right)^{-1}\boldsymbol{H}^{\intercal}\boldsymbol{W}\boldsymbol{z}\triangleq\boldsymbol{E}\boldsymbol{z} \tag{5}$$

where

$$\boldsymbol{E}\triangleq\left(\boldsymbol{H}^{\intercal}\boldsymbol{W}\boldsymbol{H}\right)^{-1}\boldsymbol{H}^{\intercal}\boldsymbol{W} \tag{6}$$

is the dc state estimator, also referred to as the "pseudo-inverse" of $\boldsymbol{H}$ since $\boldsymbol{E}\boldsymbol{H}=\boldsymbol{I}$. Besides the WLS criterion, some other statistical estimation criteria, such as the maximum likelihood criterion and the minimum variance criterion, are also commonly used in the dc state estimation [71, ch. 12]. These criteria will result in the identical optimal state estimator $\boldsymbol{E}$, if measurement errors are assumed to follow the normal distribution with zero mean [19]. If $\boldsymbol{H}$ is of full column rank or equivalently $\boldsymbol{H}^{\intercal}\boldsymbol{W}\boldsymbol{H}$ is nonsingular, the unique state estimation $\hat{\boldsymbol{x}}$ can be derived. To obtain a unique state estimation, at least n meter measurements are required, since $\operatorname{rank}\left(\boldsymbol{E}\right)=\operatorname{rank}\left(\boldsymbol{H}\right)=n<m$ typically holds. We refer to the minimum set of meter measurements needed to obtain a unique state estimation as the essential/basic meter measurements. The other $(m-n)$ redundant meter measurements can be leveraged by the control center to deal with the random measurement noises.

The estimated state variables $\hat{\boldsymbol{x}}$ can be used to estimate meter measurements by

$$\hat{\boldsymbol{z}}=\boldsymbol{H}\hat{\boldsymbol{x}}=\boldsymbol{H}\left(\boldsymbol{H}^{\intercal}\boldsymbol{W}\boldsymbol{H}\right)^{-1}\boldsymbol{H}^{\intercal}\boldsymbol{W}\boldsymbol{z}\triangleq\boldsymbol{K}\boldsymbol{z} \tag{7}$$

where $\boldsymbol{K}\triangleq\boldsymbol{H}\boldsymbol{E}$ is the so-called "hat matrix."

Caused by meter failures or malicious attacks, errors could be introduced into meter measurements. The current power systems use the residual-based detector for BDD to protect state estimation [70, ch. 8]. The measurement residual is the difference between the observed measurements $\boldsymbol{z}$ and the estimated measurements $\hat{\boldsymbol{z}}$, i.e.,

$$\boldsymbol{r}=\boldsymbol{z}-\hat{\boldsymbol{z}}=\left(\boldsymbol{I}-\boldsymbol{K}\right)\boldsymbol{z}. \tag{8}$$

The largest normalized residual (LNR) test is to compare the $\mathcal{L}_2$ norm $\left\|\boldsymbol{r}\right\|_2$ (gross errors or bias) with a predetermined threshold τ to identify bad measurements (outliers). Precisely, if $\left\|\boldsymbol{r}\right\|_2>\tau$, then bad measurements are assumed to exist; otherwise $\boldsymbol{z}$ is taken as normal measurements. The independent random measurement errors are assumed to follow the normal distribution with zero mean. Then, through mathematical derivation, $\left\|\boldsymbol{r}\right\|_2^2$ follows the chi-square distribution with $(m-n)$ degrees of freedom, i.e., χ^2_{m-n} (recall that state estimation is only determined by n independent equations). According to [70, ch. 8], τ is predetermined by a hypothesis test $\Pr\left\{\left\|\boldsymbol{r}\right\|_2^2\geq\tau^2\right\}=\alpha$ with a significance level (false alarm probability) α. In other words, $\left\|\boldsymbol{r}\right\|_2>\tau$ detects bad measurements with a false alarm probability α.

[2]An arbitrary bus is chosen as the slack (reference) bus whose phase angle is set as zero.

Let $\boldsymbol{z}_a = \boldsymbol{z} + \boldsymbol{a}$, where $\boldsymbol{a} \in \mathbb{R}^{m\times 1}$ denotes the attack vector (malicious data injected into meter measurements). In other words, $\boldsymbol{z}_a$ is the bad measurements with the malicious data $\boldsymbol{a}$. The biased measurement residual of $\boldsymbol{z}_a$ is

$$\begin{aligned}\boldsymbol{r}_a &= \boldsymbol{z}_a - \hat{\boldsymbol{z}}_a = (\boldsymbol{z}+\boldsymbol{a}) - \boldsymbol{K}(\boldsymbol{z}+\boldsymbol{a}) \\ &= (\boldsymbol{z}-\hat{\boldsymbol{z}}) + (\boldsymbol{I}-\boldsymbol{K})\boldsymbol{a} = \boldsymbol{r} + (\boldsymbol{I}-\boldsymbol{K})\boldsymbol{a}.\end{aligned} \tag{9}$$

In general, if the malicious data $\boldsymbol{a}$ is unstructured, the attack vector is likely to be detected by BDD. However, some well-structured attack vectors, as revealed in [19], could circumvent BDD without being detected. For example,

$$\boldsymbol{a} = \boldsymbol{H}\boldsymbol{c} \tag{10}$$

where $\boldsymbol{c} \in \mathbb{R}^{n\times 1}$ is an arbitrary nonzero vector. The reason is as follows. Let $\hat{\boldsymbol{x}}_a$ denote the estimate of $\boldsymbol{x}$ using $\boldsymbol{z}_a$, i.e.,

$$\hat{\boldsymbol{x}}_a = \boldsymbol{E}\boldsymbol{z}_a = \boldsymbol{E}(\boldsymbol{z}+\boldsymbol{a}) = \boldsymbol{E}\boldsymbol{z} + \boldsymbol{E}\boldsymbol{H}\boldsymbol{c} = \hat{\boldsymbol{x}} + \boldsymbol{c}. \tag{11}$$

Then, the $\mathcal{L}_2$ norm of the measurement $\boldsymbol{z}_a$ residual is

$$\begin{aligned}\|\boldsymbol{r}_a\|_2 &= \|\boldsymbol{z}_a - \boldsymbol{H}\hat{\boldsymbol{x}}_a\|_2 = \|(\boldsymbol{z}+\boldsymbol{a}) - \boldsymbol{H}(\hat{\boldsymbol{x}}+\boldsymbol{c})\|_2 \\ &= \|(\boldsymbol{z}-\boldsymbol{H}\hat{\boldsymbol{x}}) + (\boldsymbol{a}-\boldsymbol{H}\boldsymbol{c})\|_2 = \|\boldsymbol{z}-\boldsymbol{H}\hat{\boldsymbol{x}}\|_2 = \|\boldsymbol{r}\|_2.\end{aligned} \tag{12}$$

That is, the derived measurement residual is the same as that without malicious data $\boldsymbol{a}$. Thus, $\boldsymbol{z}_a$ will not be detected as long as the original measurements $\boldsymbol{z}$ can pass BDD.

FDI attacks are referred to as those with the attack vector $\boldsymbol{a} = \boldsymbol{H}\boldsymbol{c}$. Since FDI attacks target data integrity, they are different from traditional cyber attacks that target data availability or confidentiality, such as denial-of-service, jamming, flooding, and eavesdropping attacks. Besides, FDI attacks can circumvent BDD such that the injection measurements will not be detected. Thus, they are different from other types of attacks on injection measurements where the unstructured attack vector is likely to be detected by BDD. Since the control center cannot distinguish $\hat{\boldsymbol{x}}_a$ from $\hat{\boldsymbol{x}}$, FDI attacks are also referred to as "unobservable" attacks. Under such attacks, the biased $\hat{\boldsymbol{x}}_a$ is mistaken by the system operator as the valid value of the estimated state. That is, the adversary could circumvent BDD and inject any bias $\boldsymbol{c}$ into state estimation $\hat{\boldsymbol{x}}$. To successfully launch FDI attacks, the attacker requires access to the $\boldsymbol{H}$ matrix that is configured by the power network topology and transmission line susceptance. Besides, the adversary needs the capability to manipulate meter measurements, by either compromising the device itself or tampering with the data reported from the meter to the control center.

FDI attacks on the dc state estimation can be similarly extended to the ac state estimation. If the attack vector $\boldsymbol{a}$ is well-structured as

$$\boldsymbol{a} = \boldsymbol{h}(\hat{\boldsymbol{x}}+\boldsymbol{c}) - \boldsymbol{h}(\hat{\boldsymbol{x}}) \tag{13}$$

then, the $\mathcal{L}_2$ norm of the measurement $\boldsymbol{z}_a$ residual is

$$\begin{aligned}\|\boldsymbol{r}_a\|_2 &= \|\boldsymbol{z}_a - \boldsymbol{h}(\hat{\boldsymbol{x}}_a)\|_2 = \|(\boldsymbol{z}+\boldsymbol{a}) - \boldsymbol{h}(\hat{\boldsymbol{x}}+\boldsymbol{c})\|_2 \\ &= \|\boldsymbol{z} - \boldsymbol{h}(\hat{\boldsymbol{x}})\|_2 = \|\boldsymbol{r}\|_2.\end{aligned} \tag{14}$$

Thus, $\boldsymbol{z}_a$ could circumvent BDD without being detected.

B. Constructing FDI Attacks

The concept of FDI attacks was first developed in 2009 by Liu *et al.* [19], [20]. The authors investigate two practical conditions: One is that the adversary is restrained to compromise certain meters, while the other is that the attack budget is limited. In both scenarios, it is demonstrated that the adversary can figure out FDI attack vectors in an efficient way. This research indicates that in face of the potential FDI attacks, the existing protection of smart grid needs to be revisited.

The adversary has to manipulate a number of meter measurements simultaneously to stealthily launch FDI attacks. Obviously the more state variables the adversary intends to bias, the more meter measurements he/she has to manipulate. In the first scenario, Liu *et al.* [19], [20] let $\mathcal{K}$ denote the set of k specific meters ($0 < k < m$) that the adversary can compromise. To launch an FDI attack successfully, the adversary has to construct an attack vector $\boldsymbol{a} = \boldsymbol{H}\boldsymbol{c}$ restrained by

$$a_i = 0 \quad \forall i \notin \mathcal{K}. \tag{15}$$

If k is too small, then possibly the attack vector $\boldsymbol{a}$ does not exist. However, the authors prove that as long as the adversary can compromise $k \geq m - n + 1$ meters, the attack vector $\boldsymbol{a}$ could always be figured out. In the second scenario, Liu *et al.* [19], [20] consider that the attack budget of the adversary is limited and he/she could manipulate at most k meters. Such an attack vector is called k-*sparse*, with up to k nonzero entries. In both scenarios, the authors provide detailed guidance on constructing attack vectors, to launch FDI attacks on random or targeted state variables without being detected. Simulation results demonstrate that by compromising only four meters, the adversary can construct a random FDI attack vector, since the power system matrices $\boldsymbol{H}$ are often sparse. Besides, by compromising at most 27 m in the IEEE 300-bus test case, the adversary can insert any bias into any target state variable.

Two security indices are proposed by Sandberg *et al.* [21] for state estimation in smart grid. These indices quantify the least effort required to launch stealthy deception attacks without triggering bad-data alarms. The authors show that measurement redundancy improves security indices in terms of large attack vector magnitudes, but the attack vector can be still relatively sparse.

Since to just compromise one single meter will typically trigger bad-data alarms, Sandberg *et al.* [21] investigate how many, and by how much, other meters need to be cooperatively compromised to avoid being detected. A meter i that requires more and severer collusion to be compromised in stealth is consider more secure, denoted by higher security indices. For the first security index α_i (*minimum sparsity*), the authors consider how sparse the attack vector $\boldsymbol{a} = \boldsymbol{H}\boldsymbol{c}$ could be to compromise the meter i without triggering alarms:

$$\alpha_i = \min_{\boldsymbol{c}} \quad \|\boldsymbol{H}\boldsymbol{c}\|_0 \tag{16}$$

$$\text{s.t.} \quad a_i = \boldsymbol{h}_i\boldsymbol{c} = 1 \tag{17}$$

where $\|\boldsymbol{H}\boldsymbol{c}\|_0$ means the number of nonzero entries, and $\boldsymbol{h}_i$ for the ith row of $\boldsymbol{H}$. The constraint $a_i = 1$ means that the

attack goal is to inject one unit malicious data into the meter i's measurement. Such a security metric is used by Teixeira *et al.* [22] to show limitations of linear attack policies on the ac power flow model. The experiment results indicate that information concerning operating conditions and saturation limits is needed for successful stealthy deception attacks on nonlinear model. The other security index β_i (*minimum magnitude*) is introduced for a tradeoff between sparsity and magnitude of attack vectors. The $\mathcal{L}_1$ norm of $\boldsymbol{a}$ denotes the metric of total malicious data injected into meter measurements $\boldsymbol{z}$. The minimal magnitude attack vector $\boldsymbol{a} = \boldsymbol{H}\boldsymbol{c}$ that compromises the meter i in stealth is based on convex optimization

$$\beta_i = \min_{\boldsymbol{c}} \quad \|\boldsymbol{H}\boldsymbol{c}\|_1 \tag{18}$$

$$\text{s.t.} \quad a_i = \boldsymbol{h}_i \boldsymbol{c} = 1. \tag{19}$$

The convex optimization framework is easy to extend including multiple attack goals and model derivations.

Teixeira *et al.* [23] propose a generalized approach to construct deception attacks on state estimation in smart grid, with specific target constraints. The attack vector $\boldsymbol{a} = \boldsymbol{H}\boldsymbol{c}$ is solved by

$$\gamma_i = \min_{\boldsymbol{c}} \quad \|\boldsymbol{H}\boldsymbol{c}\|_p \tag{20}$$

$$\text{s.t.} \quad a_i = \boldsymbol{h}_i \boldsymbol{c} = 1 \tag{21}$$

which corresponds to the "*least-effort*" attack in p-norm sense. For example, for the case of $p = 0$, the adversary constructs an attack vector with minimal sparsity, i.e., the number of meters that the attacker needs to manipulate is minimum, corresponding to the security index α_i in [21]. Teixeira *et al.* [23] also consider scenarios when the adversary only has limited knowledge of the power system, e.g., a partial model or an out-dated (perturbed) model. The authors demonstrate that the more knowledge of the power system the adversary has, the more severe stealthy deception attacks he/she could launch without being detected.

Dán and Sandberg [29] consider clusters of meters at the same attack cost for the adversary to compromise. Similar to the security index α_i in [21], the minimum cost FDI attack on the meter i is to solve the problem

$$\alpha_i = \min_{\boldsymbol{c}} \quad \|\boldsymbol{H}\boldsymbol{c}\|_0 \tag{22}$$

$$\text{s.t.} \quad \begin{cases} a_i = \boldsymbol{h}_i \boldsymbol{c} = 1 \\ a_k = \boldsymbol{h}_k \boldsymbol{c} = 0 \ \forall k \in \mathcal{P} \end{cases} \tag{23}$$

where $\mathcal{P}$ is the set of meters to be protected. The solution can be calculated if the adversary knows the network topology graph of the power system.

Kosut *et al.* [32] investigate two different regimes of FDI attacks on state estimation in smart grid. The *strong attack regime* is that a sufficiently large number of meters are compromised to guarantee the power network state is unobservable to the system operator. For the strong attack regime, the graph theoretic method is leveraged to determine the smallest set of meters that the adversary needs to manipulate to make the power system unobservable. The problem is formulated by the submodular graph function minimization, which could be efficiently tackled. The number of meters that the attacker manipulates in the *weak attack regime* is smaller than that in the strong attack regime. The problem is addressed by the adversary from a decision theoretic point of view [33]–[35]. The tradeoff between reducing the detection probability and raising the state estimation error is investigated. Based on the minimum energy leakage, the authors construct a balanced attack vector for the adversary.

The aforementioned two attack regimes are distinguished by the number k^* (*security index*) of meters that the adversary need compromise at least to launch an "unobservable" attack. Equivalently, for certain $\boldsymbol{c}$

$$k^* = \min_{\boldsymbol{a}} \quad \|\boldsymbol{a}\|_0 \tag{24}$$

$$\text{s.t.} \quad \boldsymbol{a} = \boldsymbol{H}\boldsymbol{c} \tag{25}$$

where $\|\boldsymbol{a}\|_0$ means the number of nonzero entries in $\boldsymbol{a}$ (k in the k-sparse attack vector $\boldsymbol{a}$). Kosut *et al.* [32] show the equivalence between unobservable attacks and network unobservability. That is, for the k-sparse unobservable attack vector $\boldsymbol{a}$, the power network will become unobservable when the k compromised meters are removed; or the $(m-k) \times n$ submatrix of $\boldsymbol{H}$ will no longer be of full column rank. Based on the equivalence, unobservable attacks can be constructed under the ac power flow model, though much harder. Kosut *et al.* [32] determine the minimum number k^* to launch unobservable attacks though the graph theoretic method. Based on graph theoretic model, if let $\mathcal{V}$ denote the set of buses and $\mathcal{E}$ for the set of transmission lines, then an undirected graph $(\mathcal{V}, \mathcal{E})$ can represent a power system. For a subset of branches $\mathcal{A} \subset \mathcal{E}$, let $g(\mathcal{A})$ denote the set of meters on $\mathcal{A}$'s branches and adjacent buses. In the graph $(\mathcal{V}, \mathcal{E} \backslash \mathcal{A})$, let $h(\mathcal{A})$ denote the number of interconnected modules. Let $|\cdot|$ denote the set cardinality, then the security index k^* can be calculated by

$$k^* = \min_{\mathcal{A} \subset \mathcal{E}} \left[|g(\mathcal{A})| - h(\mathcal{A}) + 2 \right]. \tag{26}$$

For the weak attack regime, the adversary's optimal attack is to maximize estimation error while limit detection probability. The minimum residue energy attack is proposed to approximate the tradeoff problem.

III. Impacts of FDI Attacks on Electricity Market

This section will show and demonstrate the impacts of FDI attacks on electricity market from the perspective of the adversary.

A. Electricity Market Operations

The deregulated electricity market is operated by the independent system operators (ISOs), like ISO-New England and PJM, which are the third-party regulators independent of power suppliers and users. To determine the market-clearing electricity price is one of the major responsibilities of ISOs. Currently, the locational marginal price (LMP) method is widely adopted by ISOs to calculate day-ahead/real-time price and manage transmission congestion [72]. A unified Ex Ante and Ex Post method is primarily used to calculate the real-time LMP based on the dc lossless optimal power flow (OPF) model [73]–[75].

1) Ex Ante Dispatch: The Ex Ante LMP and power generation dispatch instruction are determined by the real-time dispatch software of ISOs—unit dispatch system (UDS). The Ex Ante LMP gives generators an incentive to follow the generation dispatch instruction to avoid transmission congestion. The Ex Ante dispatch usually takes place 5 min prior to real time, by solving a security constrained economic dispatch (SCED) problem, since the OPF solution needs to satisfy transmission security constraint. *Ex Ante Dispatch*

$$\min_{\boldsymbol{s}} \sum_{j=1}^{n} c_j s_j \tag{27}$$

$$\text{s.t.} \begin{cases} \sum_{j=1}^{n} s_j = \sum_{j=1}^{n} d_j & (\lambda) \\ f_l^{\min} \le \sum_{j=1}^{n} G_{lj}\left(s_j - d_j\right) \le f_l^{\max} \quad \forall l \in \mathcal{L} & \left(\mu_l^{\min}, \mu_l^{\max}\right) \\ s_j^{\min} \le s_j \le s_j^{\max} \quad \forall j \in \mathcal{N} & \left(\nu_j^{\min}, \nu_j^{\max}\right) \end{cases} \tag{28}$$

where s_j is the power generation at bus j, c_j is the corresponding generation cost, d_j is the forecasted load at bus j, G_{lj} is the shift factor (with respect to the reference bus) from bus j to branch l, $f_l^{\min}$ and $f_l^{\max}$ are the power flow limits for transmission line l, $s_j^{\min}$ and $s_j^{\max}$ are the lower and upper bounds of the power generation at bus j, and $\boldsymbol{s} = [s_1, s_2, \ldots, s_n]^\intercal$. The objective function is to minimize the aggregated generation cost, and the constraints are supply-demand balance constraint, transmission constraint, and generation constraint, respectively. The Lagrangian multipliers (dual variables) λ, $\mu_l^{\min}$, $\mu_l^{\max}$, $\nu_j^{\min}$, $\nu_j^{\max}$ are associated with each constraint, respectively. It has been well known that the optimal solution must satisfy the Karush–Kuhn–Tucker (KKT) conditions [76, Sec. 5.5.3]. The Ex Ante LMP is byproduct of the optimal solution. Based on marginal cost pricing theory, the Ex Ante LMP is interpreted as shadow prices [73], [74]

$$\begin{aligned} \text{LMP}_j^{\text{EA}} &= \lambda^* + \sum_{l \in \mathcal{L}} \mu_l^{\min *} G_{lj} - \sum_{l \in \mathcal{L}} \mu_l^{\max *} G_{lj} \\ &= c_j - \nu_j^{\min *} + \nu_j^{\max *}, \end{aligned} \tag{29}$$

where λ^* is shadow price of power generation at the reference bus, $\mu_l^{\min *}$ and $\mu_l^{\max *}$ are shadow (congestion) prices associated with transmission constraint. The power generation dispatch command S^* is assigned to all generators as a reference to follow. The generator at bus j will receive $LMP_j^{EA} \times s_j^*$ revenue.

2) Ex Post Dispatch: Based on state estimation at the end of each interval, ISO estimates $\hat{s}_j$ and $\hat{d}_j$ for the power generation and load at bus j. Further more, ISO computes the estimated power flow $\hat{f}_l = \sum_{j=1}^{n} G_{lj}\left(\hat{s}_j - \hat{d}_j\right)$ through each transmission line l. If the estimated power flow exceeds the flow limits, then the branch is considered to be congested. Let $\hat{\mathcal{C}}^-$ and $\hat{\mathcal{C}}^+$ denote the sets of the estimated negatively and positively congested branches, respectively, [37], [41]

$$\begin{cases} \hat{\mathcal{C}}^- \triangleq \left\{ l : \hat{f}_l \le f_l^{\min} \right\} \\ \hat{\mathcal{C}}^+ \triangleq \left\{ l : \hat{f}_l \ge f_l^{\max} \right\}. \end{cases} \tag{30}$$

The Ex Post LMP is produced by the LMP calculator, based on the estimated system operating condition. The objective is to provide generators with the enhanced incentive to follow the power generation dispatch instruction to alleviate transmission congestion. The estimated system state is used as a starting point for solving an incremental economic dispatch program in a small range around. *Ex Post Dispatch*

$$\min_{\Delta \boldsymbol{s}} \sum_{j=1}^{n} c_j \times \Delta s_j \tag{31}$$

$$\text{s.t.} \begin{cases} \sum_{j=1}^{n} \Delta s_j = 0 & (\lambda) \\ \sum_{j=1}^{n} G_{lj} \times \Delta s_j \ge 0 \quad \forall l \in \hat{\mathcal{C}}^- & \left(\mu_l^{\min}\right) \\ \sum_{j=1}^{n} G_{lj} \times \Delta s_j \le 0 \quad \forall l \in \hat{\mathcal{C}}^+ & \left(\mu_l^{\max}\right) \\ \Delta s_j^{\min} \le \Delta s_j \le \Delta s_j^{\max} \quad \forall j \in \mathcal{N} & \left(\nu_j^{\min}, \nu_j^{\max}\right) \end{cases} \tag{32}$$

where Δs_j is the incremental power generation at bus j, $\Delta s_j^{\min}$ and $\Delta s_j^{\max}$ are the lower and upper bounds for incremental power generation at bus j (e.g., approximately 2 MW down and 0.1 MW up [75]), and $\Delta \boldsymbol{s} = [\Delta s_1, \Delta s_2, \ldots, \Delta s_n]^\intercal$. Similarly, the Ex Post LMP is interpreted as shadow prices [73], [74]

$$\begin{aligned} \text{LMP}_j^{\text{EP}} &= \hat{\lambda} + \sum_{l \in \hat{\mathcal{C}}^-} \hat{\mu}_l^{\min} G_{lj} - \sum_{l \in \hat{\mathcal{C}}^+} \hat{\mu}_l^{\max} G_{lj} \\ &= c_j - \hat{\nu}_j^{\min} + \hat{\nu}_j^{\max}. \end{aligned} \tag{33}$$

To simplify the notations, define $\hat{\mu}_l^{\min} = 0$ for $\forall l \notin \hat{\mathcal{C}}^-$, $\hat{\mu}_l^{\max} = 0$ for $\forall l \notin \hat{\mathcal{C}}^+$, $\hat{\boldsymbol{\mu}}^{\min} = \left[\hat{\mu}_1^{\min}, \hat{\mu}_2^{\min}, \ldots, \hat{\mu}_L^{\min}\right]^\intercal$, and $\hat{\boldsymbol{\mu}}^{\max} = [\hat{\mu}_1^{\max}, \hat{\mu}_2^{\max}, \ldots, \hat{\mu}_L^{\max}]^\intercal$. Then, the Ex Post LMP can be simplified as

$$\text{LMP}_j^{\text{EP}} = \hat{\lambda} + G_j^\intercal \left(\hat{\boldsymbol{\mu}}^{\min} - \hat{\boldsymbol{\mu}}^{\max}\right) \tag{34}$$

where G_j is the jth column of the shift factor matrix G. By complementary slackness, the Ex Post LMP can be viewed as an increasing step function of $\Delta \hat{s}_j$

$$\text{LMP}_j^{\text{EP}} = \begin{cases} c_j - \hat{\nu}_j^{\min} & \text{if } \Delta \hat{s}_j = \Delta s_j^{\min} \\ c_j & \text{if } \Delta s_j^{\min} < \Delta \hat{s}_j < \Delta s_j^{\max} \\ c_j + \hat{\nu}_j^{\max} & \text{if } \Delta \hat{s}_j = \Delta s_j^{\max}. \end{cases} \tag{35}$$

The Ex Post LMP is produced by the LMP calculator, based on the estimated system operating condition. The objective is to provide generators with the enhanced incentive to follow the power generation dispatch instruction to alleviate transmission congestion. The estimated system state is used as a starting point for solving an incremental economic dispatch program in a small range around. *Ex Post Dispatch*

The Ex Post LMP is produced by the LMP calculator, based on the estimated system operating condition. The objective is to provide generators with the enhanced incentive to follow the power generation dispatch instruction to alleviate transmission congestion. The estimated system state is used as a starting point for solving an incremental economic dispatch program in a small range around. *Ex Post Dispatch*

The generator at bus j will receive $\text{LMP}_j^{\text{EP}} \times \Delta \hat{s}_j$ revenue.

If each generator exactly follows the instruction of generation dispatch and the load forecast is accurate, there would be no congested branches and thus the Ex Ante LMP is identical to the Ex Post one [72]. Note that the Ex Post LMP is totally determined by the estimated transmission congestion pattern, i.e., $\hat{\mathcal{C}} \triangleq \left\{\hat{\mathcal{C}}^-, \hat{\mathcal{C}}^+\right\}$. Therefore, if the adversary has the ability to fabricate a biased transmission congestion pattern, he/she could manipulate electricity price at a specific bus, and further make financial profit from launching attacks. The above electricity market operations are based on state estimation, and thus vulnerable to FDI attacks, which cannot be detected by the system operator.

B. Impacts of FDI Attacks on Electricity Market

The concept of LR attacks was first introduced in 2011 by Yuan *et al.* [30], [31], where only load bus power injection and branch power flow measurements are attackable. The reason is that the generation subsystems are generally well protected and generator output measurements can be easily verified by direct communications between power plants and the control center, while load and power flow meters are widely distributed and more vulnerable to cyber attacks. For easy of presentation, we rearrange $\boldsymbol{z} \triangleq (\boldsymbol{z}_s; \boldsymbol{z}_d; \boldsymbol{z}_f)$, $\boldsymbol{a} \triangleq (\boldsymbol{a}_s; \boldsymbol{a}_d; \boldsymbol{a}_f)$, and $\boldsymbol{H} \triangleq (\boldsymbol{H}_s; \boldsymbol{H}_d; \boldsymbol{H}_f)$, in a certain ordering of rows. The subscript s denotes the part corresponding to generation buses, the subscript d denotes the part corresponding to load buses, and the subscript f denotes the part corresponding to branches. In addition to $\boldsymbol{a} = \boldsymbol{H}\boldsymbol{c}$, LR attacks require $\boldsymbol{a}_s = \boldsymbol{0}$ since generation bus power injection measurements cannot be attacked, and $\boldsymbol{1}^{\mathsf{T}}\boldsymbol{a}_d = 0$ to guarantee the equality of power generation and consumption. The effect is actually LR, i.e., increasing load at some buses and reducing load at other buses while maintaining the total load unchanged.

The impact of LR attacks on electricity market operations is quantitatively modeled by the raised operation cost, resulted from a fake SCED. From the adversary's perspective, two different attack objectives based on the damage analysis are proposed: *immediate* and *delayed* LR attacks. Immediate attacks aim at maximizing the operation cost instantly; while delayed attacks target at maximizing the operation cost after the overloaded transmission lines trip. For the immediate attack objective, the most damaging LR attacks are characterized by a maximin bilevel framework between the attacker and defender, and solve by the KKT-based method.

Xie *et al.* [36], [37] show that the adversary can launch FDI attacks for continuous financial arbitrage, e.g., virtual bidding at chosen buses. In the day-ahead market, the adversary buys and sells virtual power P at bus j_1 and j_2 at price $\mathrm{LMP}_{j_1}^{\mathrm{EA}}$ and $\mathrm{LMP}_{j_2}^{\mathrm{EA}}$, respectively. In the real-time market, after injecting attack vector $\boldsymbol{a}$ to manipulate nodal prices, the adversary sells and buys virtual power P at bus j_1 and j_2 at price $\mathrm{LMP}_{j_1}^{\mathrm{EP}}$ and $\mathrm{LMP}_{j_2}^{\mathrm{EP}}$, respectively. From this virtual bidding, the profit that the adversary could make is

$$\left(\mathrm{LMP}_{j_1}^{\mathrm{EP}} - \mathrm{LMP}_{j_2}^{\mathrm{EP}} + \mathrm{LMP}_{j_2}^{\mathrm{EA}} - \mathrm{LMP}_{j_1}^{\mathrm{EA}}\right) P. \tag{36}$$

First, in the day-ahead market, $\mathrm{LMP}_{j_2}^{\mathrm{EA}} > \mathrm{LMP}_{j_1}^{\mathrm{EA}}$ can be easily satisfied. Second, if define two sets $\mathcal{L}_1 \triangleq \{l : G_{lj_1} > G_{lj_2}\}$ and $\mathcal{L}_2 \triangleq \{l : G_{lj_2} > G_{lj_1}\}$, to let

$$\begin{aligned}\mathrm{LMP}_{j_1}^{\mathrm{EP}} - \mathrm{LMP}_{j_2}^{\mathrm{EP}} &= (G_{j_1} - G_{j_2})^T \left(\hat{\boldsymbol{\mu}}^{\min} - \hat{\boldsymbol{\mu}}^{\max}\right) \\ &= \sum_{l\in\mathcal{L}_1} (G_{lj_1} - G_{lj_2}) \left(\hat{\mu}_l^{\min} - \hat{\mu}_l^{\max}\right) \\ &\quad + \sum_{l\in\mathcal{L}_2} (G_{lj_2} - G_{lj_1}) \left(\hat{\mu}_l^{\max} - \hat{\mu}_l^{\min}\right) \\ &> 0\end{aligned} \tag{37}$$

heuristically, one sufficient condition is $\hat{f}_l < f_l^{\max}$ (i.e., $\hat{\mu}_l^{\max} = 0$) for $\forall l \in \mathcal{L}_1$ and $\hat{f}_l > f_l^{\min}$ (i.e., $\hat{\mu}_l^{\min} = 0$) for $\forall l \in \mathcal{L}_2$. Under an attack vector $\boldsymbol{a}$, the biased power flow estimation is $\hat{\boldsymbol{f}}_a = \boldsymbol{H}_f \boldsymbol{E} \boldsymbol{z}_a$, where $\boldsymbol{H}_f$ is part of $\boldsymbol{H}$ corresponding to power flow. The authors define that an attack vector $\boldsymbol{a}$ is called δ-*profitable* if

$$\begin{cases} \hat{f}_l \le f_l^{\max} - \delta & \forall l \in \mathcal{L}_1 \\ \hat{f}_l \ge f_l^{\min} + \delta & \forall l \in \mathcal{L}_2. \end{cases} \tag{38}$$

A large value of the margin δ could ensure the sufficient condition holds with large probability. The biased measurement residual under an attack vector $\boldsymbol{a}$ is $\boldsymbol{r}_a = \boldsymbol{r} + (\boldsymbol{I} - \boldsymbol{K})\,\boldsymbol{a}$. By triangle inequality, $\|\boldsymbol{r}_a\|_2 \le \|\boldsymbol{r}\|_2 + \|(\boldsymbol{I} - \boldsymbol{K})\,\boldsymbol{a}\|_2$. The authors also define that an attack vector $\boldsymbol{a}$ is referred to as ϵ-*feasible* when

$$\|(\boldsymbol{I} - \boldsymbol{K})\,\boldsymbol{a}\|_2 \le \epsilon. \tag{39}$$

An attack with a smaller ϵ will more likely bypass BDD. From the adversary's perspective, the optimal attacking strategy is to determine an ϵ-feasible attack vector $\boldsymbol{a}$ with the maximum margin δ, or a δ-profitable attack vector $\boldsymbol{a}$ with the minimum ϵ. The authors consider two possible scenarios: the subset of compromised meters is fixed; and the total number of compromised meters is upper bounded. These scenarios are formulated as or relaxed to convex optimization problems and can be efficiently solved.

Jia *et al.* [38], [39] consider making profit for the generator at a specific bus by launching FDI attacks on the real-time market, where the attacker can manipulate electricity price at a specific bus by fabricating a biased transmission congestion pattern. The real-time gain of the generator at bus j is $\mathrm{LMP}_j^{\mathrm{EP}} \times \Delta\hat{s}_j$. Under an attack vector $\boldsymbol{a}$, the biased power generation estimation is $\hat{\boldsymbol{s}}_a = \boldsymbol{H}_s \boldsymbol{E} \boldsymbol{z}_a$, where $\boldsymbol{H}_s$ is part of $\boldsymbol{H}$ that corresponds to power generation. The adversary should balance between reducing the probability of being detected and increasing the profit. Take the expected profit as the goal

$$\max_{\boldsymbol{a}} \left[1 - P_d\left(\boldsymbol{a}\right)\right] \mathrm{LMP}_j^{\mathrm{EP}} \left(\boldsymbol{H}_s \boldsymbol{E}\right)_j \boldsymbol{a} \tag{40}$$

where $\left(\boldsymbol{H}_s \boldsymbol{E}\right)_j$ is the jth row of $\boldsymbol{H}_s \boldsymbol{E}$, and the detection probability $P_d\left(\boldsymbol{a}\right)$ is a function of $\boldsymbol{a}$ (in the weak attack regime [32]). The optimal attacking strategy is obtained by optimizing the quasiconcave objective function.

Jia *et al.* [40] further consider three different scenarios: the adversary may have full, partial, or zero knowledge of real-time measurements. Bayesian formulation is adopted in the analysis. The distribution of the system state is known to the adversary, treated as the priori knowledge. Based on the full, partial, or zero real-time measurements, the attacker will make the posteriori estimation of the system state, and then make the attack decision. Since a state estimate $\hat{\boldsymbol{x}}$ is corresponding to a transmission congestion pattern $\hat{\mathcal{C}}$, and thus a real-time price $\mathrm{LMP}_j^{\mathrm{EP}}(\hat{\mathcal{C}})$ at bus j. Let $x(\hat{\mathcal{C}})$ denote the region of system states that make the transmission congestion pattern as $\hat{\mathcal{C}}$. The available set of transmission congestion patterns that the attack's detection probability is less than a threshold $\bar{P}_d$, is

denoted by $\Gamma \triangleq \{\hat{\mathcal{C}} : \exists \boldsymbol{a}, \hat{\boldsymbol{x}}_a \in x(\hat{\mathcal{C}}), P_d(\boldsymbol{a}) \leq \bar{P}_d\}$. The desirable transmission congestion pattern is chosen as

$$\hat{\mathcal{C}}^* = \arg\max_{\hat{\mathcal{C}} \in \Gamma} \text{LMP}_j^{\text{EP}}(\hat{\mathcal{C}}) \tag{41}$$

and the optimal attacking strategy is the arbitrary one that makes the transmission congestion pattern as $\hat{\mathcal{C}}^*$.

Kosut *et al.* [32] investigate how FDI attacks have impact on electricity market operations, since the biased state estimation result will be used for economic dispatch without being detected. In the day-ahead market, the generator at bus j will receive $\text{LMP}_j^{\text{EA}} s_j^*$ revenue. In the real-time market, the generator at bus j will receive $\text{LMP}_j^{\text{EP}} \times \Delta\hat{s}_j$ revenue. Note that $\Delta\hat{s}_j$ is calculated based on state estimation, and thus may be influenced by the adversary. Under an attack vector $\boldsymbol{a}$, the biased power generation estimation is $\hat{\boldsymbol{s}}_a = \boldsymbol{H}_s \boldsymbol{E} \boldsymbol{z}_a$, where $\boldsymbol{H}_s$ is part of $\boldsymbol{H}$ corresponding to power generation. The biased real-time gain of the generator at bus j is $\text{LMP}_j^{\text{EP}} (\boldsymbol{H}_s \boldsymbol{E})_j \boldsymbol{a}$, where $(\boldsymbol{H}_s \boldsymbol{E})_j$ is the jth row of $\boldsymbol{H}_s \boldsymbol{E}$. In such as way the adversary can inject the attack vector $\boldsymbol{a}$ to potentially make financial profit.

Bi and Zhang [41] show that by fabricating a fake transmission congestion pattern, FDI attacks can manipulate real-time price at arbitrary target bus. They further show how to determine an effective transmission congestion pattern which only biases the estimated state a little. LR attacks, a special type of FDI attacks that induce fake estimation of load, are also leveraged to realize the desirable transmission congestion pattern. Both resource constrained and unconstrained "neighborhood" LR (NLR) attacks are derived, which also have impact on future electricity market.

Suppose that the attack goal is to decrease the electricity price at bus j. Since the Ex Post LMP LMP_j^{EP} is an increasing step function of $\Delta\hat{s}_j$, an rational adversary should launch attacks when $\Delta\hat{s}_j = \Delta s_j^{\max}$ (i.e., when $\text{LMP}_j^{\text{EP}} = c_j + \hat{\nu}_j^{\max}$). Thus, an effective transmission congestion pattern, denoted by $\left\{\hat{\mathcal{C}}_a^-, \hat{\mathcal{C}}_a^+\right\}$ under an attack vector $\boldsymbol{a}$, should cause the ISO to yield biased $\Delta\hat{s}_j \in \left[\Delta s_j^{\min}, \Delta s_j^{\max}\right)$. This is obtained by Ex Post dispatch under the following constraints:

$$\begin{cases} \sum_{j=1}^{n} \Delta s_j = -\beta \\ \sum_{j=1}^{n} G_{lj} \times \Delta s_j \geq -G_{lj}\beta \ \forall l \in \hat{\mathcal{C}}_a^- \\ \sum_{j=1}^{n} G_{lj} \times \Delta s_j \leq -G_{lj}\beta \ \forall l \in \hat{\mathcal{C}}_a^+ \\ \Delta s_j^{\min} \leq \Delta s_j \leq \Delta s_j^{\max} \ \ \forall j \in \mathcal{N} \end{cases} \tag{42}$$

where $\beta \in \left[\Delta s_j^{\min}, \Delta s_j^{\max}\right)$ is a tuning coefficient. Intuitively, obtaining a feasible $\left\{\hat{\mathcal{C}}_a^-, \hat{\mathcal{C}}_a^+\right\}$ requires enumerating all possible combinations. Bi and Zhang [41] propose an "add-then-remove" heuristic algorithm to solve the problem at a low computational cost. Then the authors realize the desirable transmission congestion pattern through LR attacks. The biased power flow estimation under LR attacks is $\hat{\boldsymbol{f}}_a = \boldsymbol{H}_f \boldsymbol{E} \boldsymbol{z}_a$, where $\boldsymbol{H}_f$ is part of $\boldsymbol{H}$ corresponding to power flow. The goal of an adversary is to realize the desirable transmission congestion pattern while inserting a little bias into the estimated state

$$\min_{\boldsymbol{a}} \|\boldsymbol{E}\boldsymbol{a}\|_2 \tag{43}$$

$$\text{s.t.} \begin{cases} \boldsymbol{a} = \boldsymbol{H}\boldsymbol{c} \\ \hat{f}_l \leq f_l^{\min} & \forall l \in \hat{\mathcal{C}}_a^- \\ \hat{f}_l \geq f_l^{\max} & \forall l \in \hat{\mathcal{C}}_a^+ \\ f_l^{\min} \leq \hat{f}_l \leq f_l^{\max} & \forall l \in \mathcal{L} \backslash \hat{\mathcal{C}}_a^+ \backslash \hat{\mathcal{C}}_a^-. \end{cases} \tag{44}$$

Furthermore, the authors propose a concept of cost-aware NLR attacks, where the adversary's capacity is constrained to manipulate the power load measurements at the target bus and those within one hop, and its k-hop power flow measurements. These formulations are convex optimization problems which can be easily solved.

IV. Defending Against FDI Attacks

From the perspective of the system operator, this section will present and analyze countermeasures against FDI attacks.

Bobba *et al.* [44] explore how to detect FDI attacks: One way is to secure basic measurements which are selected strategically, while the other way is to verify state variables independently which are selected strategically. Specifically, the authors show that protecting basic measurements is sufficient and necessary for the detection of FDI attacks. The protection on meter measurements includes both physical and software methods, for example, guard patrolling, video monitoring, tamper-proof communication systems, sophisticated authentication protocols, asymmetric encryption mechanisms, etc.

To detect FDI attacks in smart grid, a naive approach is to protect all meter measurements from being manipulated; which is, however, not cost-effective. Let $\mathcal{P}$ denote the set of p protected meters. Bobba *et al.* [44] show that it is necessary but not sufficient to protect at least n meters for the detection of FDI attacks. The possibility to reduce such burden is to independently verify values of certain state variables. One way is through the deployment of PMUs, which can directly measure the bus voltage phasor (including magnitudes and phase angles) with global positioning system (GPS) timestamp. Note that PMUs may have the vulnerability since the GPS signal can be spoofed [77]–[81]. The results in [82]–[84] are some existing countermeasures against GPS spoofing attacks on PMUs in smart grid. Let $\mathcal{Q}$ denote the set of q state variables that can be verified by PMUs. To launch FDI attacks stealthily, the adversary has to construct an attack vector $\boldsymbol{a} = \boldsymbol{H}\boldsymbol{c}$ restrained by

$$\begin{cases} a_i = 0 \ \forall i \in \mathcal{P} \\ c_j = 0 \ \forall j \in \mathcal{Q}. \end{cases} \tag{45}$$

The defender needs to identify the set $\mathcal{P}$ of protected meter measurements, and the set $\mathcal{Q}$ of verifiable state variables, such that the adversary cannot find any possible attack vector. Ideally, the smallest such sets are desirable. Bobba *et al.* [44] first try a straightforward brute-force approach to identify optimal $\mathcal{P}$ and $\mathcal{Q}$, by searching through $C_m^p C_n^q$ combinations for all possible choices of p and q. This approach is reducible to the hint set

problem which is $\mathcal{NP}$-complete. Bobba *et al.* [44] then provide an alternative approach by leveraging the concept of basic measurements that ensure observability of a power network [70, ch. 7]. The conclusion is that without PMUs, it is sufficient and necessary to protect all basic measurements for the detection of FDI attacks; while if there are q PMUs, it is sufficient and necessary to protect a subset of basic measurements corresponding to the remaining $(n-q)$ state variables to defend against FDI attacks.

Dán and Sandberg [29] propose greedy algorithms for perfect and partial countermeasures against FDI attacks. Perfect defense means no FDI attacks are possible. Due to so many meters in power systems, to make all devices encrypted overnight is not possible. Since the defense budget π might not be sufficient for perfect countermeasures, the control center would consider to protect a subset $\mathcal{P}$ of meters to maximize the increased system security. The authors consider two possible protection metrics: maximizing the minimal attack cost among all meters

$$\max_{\mathcal{P}} \quad \min_{i\in\mathcal{M}} \alpha_i \tag{46}$$

$$\text{s.t.} \quad c(\mathcal{P}) \le \pi \tag{47}$$

where $c(\mathcal{P})$ denotes the cost of protecting the set $\mathcal{P}$ of meters; and maximizing the average attack cost of meters

$$\max_{\mathcal{P}} \quad \frac{1}{m}\sum_{i\in\mathcal{M}} \alpha_i \tag{48}$$

$$\text{s.t.} \quad c(\mathcal{P}) \le \pi. \tag{49}$$

These protection strategies could be heuristically computed by greedy algorithms.

Kosut *et al.* [32] consider two regimes of FDI attacks on state estimation in smart grid, where for the weak attack regime, the number of meters that the attacker manipulates is smaller than that in the strong attack regime. The problem is addressed by the adversary from a decision theoretic point of view [33]–[35]. For the system operator, a generalized likelihood ratio test (GLRT) detector is devised with incorporation of historical data. The Bayesian formulation can take advantage of priori information to preserve and trace the likely state of the system. Compared with the $J(\hat{\boldsymbol{x}})$ detector, numerical simulations show that the proposed GLRT detector is asymptotically optimal in terms of detection performance. Kosut *et al.* [32] also prove that the GLRT detector is the same as the LNR detector under the case of only one compromised meter.

Kim and Poor [45] propose strategic countermeasures against FDI attacks on the power grid based on linearized measurement models. They first propose a new low-complexity attacking strategy. Then, a greedy approach is designed to protect a number of meter measurements for defense. Finally, they also develop the other greedy approach to promote the PMU deployment to defend against such attacks.

Giani *et al.* [46], [47] consider unobservable data integrity attacks on power systems. First, an efficient approach is presented to obtain all sparse attacks where a modest number of meter measurements are compromised. Known-secure PMUs are used as countermeasures against such cyber attacks. How to find the minimum number of necessary PMUs at carefully chosen buses is finally analyzed for defense.

TABLE I
CLASSIFICATION OF FDI ATTACKS AND THEIR DEFENSE

Types	References
FDI attacks	[19]–[28], [36]–[43]
Defense/detection/countermeasures	[44], [52]–[66]
Both attack and defense	[29]–[35], [45]–[51]

TABLE II
CLASSIFICATION OF FDI ATTACKS BASED ON THEIR IMPACTS

Target	Impact	References
SCADA (dc model)	biased state estimation	[19]–[21], [24], [25] [27]–[29], [45]–[51]
SCADA (ac model)	biased state estimation	[22], [23], [26], [39]
Electricity market	potential financial loss	[30]–[43]

TABLE III
CLASSIFICATION OF COUNTERMEASURES AGAINST FDI ATTACKS

Countermeasure	References
Protecting meter measurement	[29]–[35], [48]–[55], [60]–[66]
PMU for securing state variable	[46], [47], [56]–[59]
Protecting measurement and state	[44], [45]

Bi and Zhang [52] propose countermeasures against FDI attacks by protecting critical state variables. To this end, the authors carefully select a minimum number of meter measurements to be protected. Both optimal and the complexity-reduced suboptimal approaches are provided to obtain the defense objective at the minimum cost. After characterizing such a problem into a Steiner tree in graph theory, graphical methods are leveraged to select the minimum number of meter measurements [53]. In addition, by jointly considering the conventional protecting meter measurements and the covert topological information, they further propose a mixed protection strategy, in case that either of them fails to obtain the defense objective [54], [55].

V. FUTURE RESEARCH DIRECTIONS

From the above, we have reviewed extensive literatures on FDI attacks on state estimation in power systems, and their impacts and defense. We now categorize the aforementioned literatures as follows. In Table I, we classify existing FDI attacks and their defense, including literatures merely on attacks, merely on defense/detection/countermeasures, or both on attack and defense. In Table II, we classify existing FDI attacks based on their associated impacts on smart grid. For example, some FDI attacks target dc or ac SCADA to introduce arbitrary errors into power system state estimation, while others target electricity market to manipulate electricity price, resulting in potential financial loss. In Table III, we classify existing countermeasures against FDI attacks, in terms of protecting meter measurements,

TABLE IV
SUMMARY OF IMPORTANT CONCEPTS IN FDI ATTACKS AND DEFENSE ON POWER SYSTEM STATE ESTIMATION

Concept	Mathematical description	Description or explanation
AC power flow model	$\boldsymbol{z} = \boldsymbol{h}(\boldsymbol{x}) + \boldsymbol{e}$	$\boldsymbol{h}(\boldsymbol{x})$ is nonlinear measurement function of $\boldsymbol{x}$
DC power flow model	$\boldsymbol{z} = \boldsymbol{H}\boldsymbol{x} + \boldsymbol{e}$	$\boldsymbol{H}$ is measurement Jacobian matrix
DC State estimation	$\hat{\boldsymbol{x}} = \boldsymbol{E}\boldsymbol{z}$	based on WLS criterion
DC State estimator	$\boldsymbol{E} \triangleq (\boldsymbol{H}^\intercal \boldsymbol{W} \boldsymbol{H})^{-1} \boldsymbol{H}^\intercal \boldsymbol{W}$	"pseudo-inverse" of $\boldsymbol{H}$ since $\boldsymbol{E}\boldsymbol{H} = \boldsymbol{I}$
Estimated measurement	$\hat{\boldsymbol{z}} = \boldsymbol{H}\hat{\boldsymbol{x}} = \boldsymbol{K}\boldsymbol{z}$	$\boldsymbol{K} \triangleq \boldsymbol{H}\boldsymbol{E}$ is "hat matrix"
Measurement residual	$\boldsymbol{r} = \boldsymbol{z} - \hat{\boldsymbol{z}}$	$\boldsymbol{r} = (\boldsymbol{I} - \boldsymbol{K})\boldsymbol{z}$
Bad measurement	$\boldsymbol{z}_a = \boldsymbol{z} + \boldsymbol{a}$	$\boldsymbol{a}$ is attack vector (malicious data)
Biased state estimation	$\hat{\boldsymbol{x}}_a = \boldsymbol{E}\boldsymbol{z}_a$	$\hat{\boldsymbol{x}}_a = \hat{\boldsymbol{x}} + \boldsymbol{E}\boldsymbol{a}$
Biased estimated measurement	$\hat{\boldsymbol{z}}_a = \boldsymbol{H}\hat{\boldsymbol{x}}_a$	$\hat{\boldsymbol{z}}_a = \boldsymbol{K}\boldsymbol{z}_a$
Biased measurement residual	$\boldsymbol{r}_a = \boldsymbol{z}_a - \hat{\boldsymbol{z}}_a$	$\boldsymbol{r}_a = \boldsymbol{r} + (\boldsymbol{I} - \boldsymbol{K})\boldsymbol{a}$
FDI attack on dc state estimation	$\boldsymbol{a} = \boldsymbol{H}\boldsymbol{c}$	$\boldsymbol{r}_a = \boldsymbol{r}$ since $(\boldsymbol{I} - \boldsymbol{K})\boldsymbol{a} = \boldsymbol{0}$
LR attack on dc state estimation	$(\boldsymbol{a}_s; \boldsymbol{a}_d; \boldsymbol{a}_f) = \boldsymbol{H}\boldsymbol{c}$ with $\boldsymbol{a}_s = \boldsymbol{0}$ and $\boldsymbol{1}^\intercal \boldsymbol{a}_d = 0$	s: generation buses, d: load buses, f: branches
Security index (minimum sparsity)	$\alpha_i = \min_{\boldsymbol{c}} \|\boldsymbol{H}\boldsymbol{c}\|_0$ s.t. $a_i = \boldsymbol{h}_i \boldsymbol{c} = 1$	$\boldsymbol{h}_i$ is ith row of $\boldsymbol{H}$
Security index (minimum magnitude)	$\beta_i = \min_{\boldsymbol{c}} \|\boldsymbol{H}\boldsymbol{c}\|_1$ s.t. $a_i = \boldsymbol{h}_i \boldsymbol{c} = 1$	$\boldsymbol{h}_i$ is ith row of $\boldsymbol{H}$
Security index ("least-effort" in p-norm sense)	$\gamma_i = \min_{\boldsymbol{c}} \|\boldsymbol{H}\boldsymbol{c}\|_p$ s.t. $a_i = \boldsymbol{h}_i \boldsymbol{c} = 1$	$\boldsymbol{h}_i$ is ith row of $\boldsymbol{H}$
Biased power generation estimation	$\hat{\boldsymbol{s}}_a = \boldsymbol{H}_s \boldsymbol{E}\boldsymbol{z}_a$	$\boldsymbol{H}_s$ is part of $\boldsymbol{H}$ w.r.t. power generation
Biased power flow estimation	$\hat{\boldsymbol{f}}_a = \boldsymbol{H}_f \boldsymbol{E}\boldsymbol{z}_a$	$\boldsymbol{H}_f$ is part of $\boldsymbol{H}$ w.r.t. power flow

PMU placement for securing state variables, as well as jointly protecting meter measurements together with state variables.

Although FDI attacks, impacts, and defense have already drawn a large quantity of attention from the academic and research community, this topic is still worth exploring in face of certain unsolved issues. The potential future research directions as well as possible challenges are listed as below.

First, most existing works on FDI attacks and defense are employing the approximated dc power flow model, that is easy for the adversary and system operator due to the linear approximation. The ac power flow model is comprised of nonlinear equations and includes both the active and reactive power, which is more complicated and time consuming. However, the ac power flow model is more precise than the dc model, especially for the distribution subsystem. Currently, there have been relatively rare studies on FDI attacks based on the ac power flow model. Driven by the advance in nonlinear optimization and super computing, the research on the ac power flow model will become a potential direction. On the other hand, most existing researches focus on the centralized FDI attack and defense, but works on the distributed approach is less. However, the centralized FDI attacks require that the attacker knows the information of the network topology and configuration of the power system. Besides, for the large-scale power grid, the centralized FDI countermeasures may result in incomplete and inefficient detection. Thus, the research on distributed FDI attack and defense will be gradually necessary.

Second, the interplay between the attacker and defender has not been well investigated in the context of cyber security in smart grid. From the game theoretic point of view, the defender takes the first action, by deploying defense resources to secure the power system as much as possible; and the adversary takes the second action, by attacking on the weakest target of the system. For simplicity, the two-player interaction can be modelled by a static zero-sum game. One interesting thing is that the attacker may not, partially, or fully know the defender's strategy, but the defender has zero knowledge of the attacker's strategy beforehand. How the information asymmetry will have impact on the FDI attack and defense performance is a problem worth studying. Besides, considering the scenario of multiple defenders and multiple attackers, some hierarchical games, such as Stackelberg games, shall be taken advantage of to provide insight into the complicated interactions. Furthermore, if we view the attack–defense interaction more realistically as a continuous process instead of only a one-time event, some dynamic games, such as Markov games, shall be leveraged to characterize the transient state evolution process. The related works in the area of power system physical security can be based on, but the transition is not trivial, since cyber attacks are quite different from the traditional physical attacks.

Finally, most existing countermeasures against FDI attacks have assumed that the adversary cannot compromise some meter measurements no matter how powerful he/she is. Such an assumption is impractical for realistic situations. To be more realistic, assume that whether or not the adversary can compromise a meter depends on how much protection the defender deploys on the meter. In this viewpoint, one direction is to devise the cost-efficient protection approach to defend the power system against cyber attacks. Another direction extends to determine protecting which meters and deploying how much protection on them, such that any state variable cannot be modified by the adversary. Although some pioneering works have made a trial in this context, more efforts are still needed to shed light on immunizing power systems from FDI attacks in practical applications.

VI. CONCLUSION

Recently, FDI attacks have emerged as a new type of cyber attacks threatening state estimation in power systems. Significant research efforts have been made in constructing and/or defending against such attacks in the context of cyber security in smart grid. To unify the knowledge, a literature overview of

FDI attacks, impacts, and defense is presented in this paper. Specifically, this overview includes three folds:

1) constructing FDI attacks;
2) impacts of FDI attacks on electricity market; and
3) defending against FDI attacks.

One direction is from the perspective of the adversary, to explore the problem of constructing FDI attacks, and further show their associated impacts on electricity market operations. Another direction is from the perspective of the system operator, to present countermeasures against FDI attacks. From the overview of existing works, we also outline some future research directions such as distributed detection based on the ac power flow models, attack-defense game interactions, and more realistic assumptions. To conclude, some aforementioned important concepts in the context of FDI attacks, impacts, and defense are summarized in Table IV. However, due to so many research activities in these areas, we might have missed some literatures and would like to apologize for that.

REFERENCES

[1] F. F. Wu, "Power system state estimation: A survey," *Int. J. Elect. Power Energy Syst.*, vol. 12, no. 2, pp. 80–87, 1990.

[2] A. Monticelli, "Electric power system state estimation," *Proc. IEEE*, vol. 88, no. 2, pp. 262–282, 2000.

[3] A. Abur and A. G. Exposito, *Power System State Estimation: Theory and Implementation*. Boca Raton, FL, USA: CRC Press, 2004.

[4] V. C. Gungor et al., "Smart grid technologies: Communication technologies and standards," *IEEE Trans. Ind. Informat.*, vol. 7, no. 4, pp. 529–539, Nov. 2011.

[5] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid—the new and improved power grid: A survey," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 944–980, Fourth Quater 2012.

[6] R. Deng, Z. Yang, J. Chen, N. R. Asr, and M.-Y. Chow, "Residential energy consumption scheduling: A coupled-constraint game approach," *IEEE Trans. Smart Grid*, vol. 5, no. 3, pp. 1340–1350, May 2014.

[7] R. Deng, Z. Yang, M.-Y. Chow, and J. Chen, "A survey on demand response in smart grids: Mathematical models and approaches," *IEEE Trans. Ind. Inform.*, vol. 11, no. 3, pp. 570–582, Jun. 2015.

[8] C. Zhao, J. He, P. Cheng, and J. Chen, "Consensus-based energy management in smart grid with transmission losses and directed communication," *IEEE Trans. Smart Grid*, vol. PP, no. 99, pp. 1–13, to be published, doi: 10.1109/TSG.2015.2513772.

[9] Y. Mo *et al.*, "Cyber–physical security of a smart grid infrastructure," *Proc. IEEE*, vol. 100, no. 1, pp. 195–209, Jan. 2012.

[10] J. Liu, Y. Xiao, S. Li, W. Liang, and C. P. Chen, "Cyber security and privacy issues in smart grids," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 981–997, Fourth Quarter 2012.

[11] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," *IEEE Commun. Surveys Tutorials*, vol. 14, no. 4, pp. 998–1010, Fourth Quarter 2012.

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

[13] Y. Yamaguchi, A. Ogawa, A. Takeda, and S. Iwata, "Cyber security analysis of power networks by hypergraph cut algorithms," in *Proc. IEEE Int. Conf. Smart Grid Commun.*, 2014, pp. 824–829.

[14] S. Mousavian, J. Valenzuela, and J. Wang, "A probabilistic risk mitigation model for cyber-attacks to PMU networks," *IEEE Trans. Power Syst.*, vol. 30, no. 1, pp. 156–165, Jan. 2015.

[15] H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal DoS attack scheduling in wireless networked control system," *IEEE Trans. Control Syst. Technol.*, vol. 24, no. 3, pp. 843–852, May 2016.

[16] 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.

[17] Z. Li, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, "Analyzing locally coordinated cyber-physical attacks for undetectable line outages," *IEEE Trans. Smart Grid*, vol. PP, no. 99, pp. 1–12, to be published, doi: 10.1109/TSG.2016.2542925.

[18] R. Deng, G. Xiao, and R. Lu, "Defending against false data injection attacks on power system state estimation," *IEEE Trans. Ind. Informat.*, vol. PP, no. 99, pp. 1–10, to be published, doi: 10.1109/TII.2015.2470218.

[19] 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.

[20] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, pp. 21–32, 2011.

[21] H. Sandberg, A. Teixeira, and K. Johansson, "On security indices for state estimators in power networks," in *Proc. Preprints 1st Workshop Secure Control Syst., CPSWEEK*, 2010, pp. 1–6.

[22] A. Teixeira, G. Dán, H. Sandberg, and K. H. Johansson, "A cyber security study of a SCADA energy management system: Stealthy deception attacks on the state estimator," *IFAC World Congr.*, vol. 18, no. 1, pp. 11 271–11 277, 2011.

[23] A. Teixeira, S. Amin, H. Sandberg, K. H. Johansson, and S. S. Sastry, "Cyber security analysis of state estimators in electric power systems," in *Proc. IEEE Conf. Decision Control*, 2010, pp. 5991–5998.

[24] M. Esmalifalak, H. Nguyen, R. Zheng, and Z. Han, "Stealth false data injection using independent component analysis in smart grid," in *Proc. IEEE Int. Conf. Smart Grid Commun.*, 2011, pp. 244–248.

[25] K. C. Sou, H. Sandberg, and K. H. Johansson, "Electric power network security analysis via minimum cut relaxation," in *Proc. IEEE Conf. Decision Control Eur. Control Conf.*, 2011, pp. 4054–4059.

[26] G. Hug and J. A. Giampapa, "Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1362–1370, Sep. 2012.

[27] M. Ozay, I. Esnaola, F. T. Yarman Vural, S. R. Kulkarni, and H. V. Poor, "Distributed models for sparse attack construction and state vector estimation in the smart grid," in *Proc. IEEE Int. Conf. Smart Grid Communic.*, 2012, pp. 306–311.

[28] M. Ozay, I. Esnaola, F. T. Yarman Vural, S. R. Kulkarni, and H. V. Poor, "Sparse attack construction and state estimation in the smart grid: Centralized and distributed models," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 7, pp. 1306–1318, Jul. 2013.

[29] G. Dán and H. Sandberg, "Stealth attacks and protection schemes for state estimators in power systems," in *Proc. IEEE Int. Conf. Smart Grid Commun.*, 2010, pp. 214–219.

[30] 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.

[31] 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.

[32] 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.

[33] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Limiting false data attacks on power system state estimation," in *Proc. IEEE Annu. Conf. Inf. Sci. Syst.*, 2010, pp. 1–6.

[34] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "On malicious data attacks on power system state estimation," in *Proc. IEEE Int. Univ. Power Eng. Conf.*, 2010, pp. 1–6.

[35] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures," in *Proc. IEEE Int. Conf. Smart Grid Commun.*, 2010, pp. 220–225.

[36] L. Xie, Y. Mo, and B. Sinopoli, "False data injection attacks in electricity markets," in *Proc. IEEE Int. Conf. Smart Grid Commun.*, 2010, pp. 226–231.

[37] L. Xie, Y. Mo, and B. Sinopoli, "Integrity data attacks in power market operations," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 659–666, Dec. 2011.

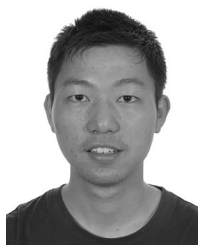
[38] L. Jia, R. J. Thomas, and L. Tong, "Malicious data attack on real-time electricity market," in *Pro. IEEE Int. Conf. Acoust., Speech Signal Process.*, 2011, pp. 5952–5955.

[39] L. Jia, R. J. Thomas, and L. Tong, "On the nonlinearity effects on malicious data attack on power system," in *Proc. IEEE Power Energy Soc. Gen.Meeting*, 2012, pp. 1–8.

[40] L. Jia, R. J. Thomas, and L. Tong, "Impacts of malicious data on real-time price of electricity market operations," in *Proc. IEEE Hawaii Int. Conf. Syst. Sci.*, 2012, pp. 1907–1914.

[41] S. Bi and Y. J. Zhang, "False-data injection attack to control real-time price in electricity market," in *Proc. IEEE Global Commun. Conf.*, 2013, pp. 772–777.

[42] M. Esmalifalak, Z. Han, and L. Song, "Effect of stealthy bad data injection on network congestion in market based power system," in *Proc. IEEE Wireless Commun. Netw. Conf.*, 2012, pp. 2468–2472.
[43] J. Lin, W. Yu, X. Yang, G. Xu, and W. Zhao, "On false data injection attacks against distributed energy routing in smart grid," in *Proc. IEEE/ACM Int. Conf. Cyber-Phys. Syst.*, 2012, pp. 183–192.
[44] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. J. Overbye, "Detecting false data injection attacks on DC state estimation," in *Preprints 1st Workshop Secure Control Syst., CPSWEEK*, 2010.
[45] 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.
[46] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla, "Smart grid data integrity attacks: Characterizations and countermeasures," in *Proc. IEEE Int. Conf. Smart Grid Commun.*, 2011, pp. 232–237.
[47] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla, "Smart grid data integrity attacks," *IEEE Trans. Smart Grid*, vol. 4, no. 3, pp. 1244–1253, Sep. 2013.
[48] S. Cui, Z. Han, S. Kar, T. T. Kim, H. V. Poor, and A. Tajer, "Coordinated data-injection attack and detection in the smart grid: A detailed look at enriching detection solutions," *IEEE Signal Process. Mag.*, vol. 29, no. 5, pp. 106–115, 2012.
[49] Y. Huang *et al.*, "Bad data injection in smart grid: Attack and defense mechanisms," *IEEE Commun. Mag.*, vol. 51, no. 1, pp. 27–33, 2013.
[50] M. Esmalifalak, G. Shi, Z. Han, and L. Song, "Bad data injection attack and defense in electricity market using game theory study," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 160–169, Jan. 2013.
[51] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang, and W. Zhao, "On false data-injection attacks against power system state estimation: Modeling and countermeasures," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 3, pp. 717–729, Mar. 2014.
[52] S. Bi and Y. J. Zhang, "Defending mechanisms against false-data injection attacks in the power system state estimation," in *Proc. IEEE GLOBECOM Workshops*, 2011, pp. 1162–1167.
[53] 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.
[54] S. Bi and Y. J. Zhang, "Mitigating false-data injection attacks on dc state estimation using covert topological information," in *Proc. IEEE Global Commun. Conf.*, 2013, pp. 766–771.
[55] S. Bi and Y. J. Zhang, "Using covert topological information for defense against malicious attacks on DC state estimation," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 7, pp. 1471–1485, Jul. 2014.
[56] M. Göl and A. Abur, "Identifying vulnerabilities of state estimators against cyber-attacks," in *Proc. IEEE Grenoble PowerTech*, 2013, pp. 1–4.
[57] M. Göl and A. Abur, "Effective measurement design for cyber security," in *Proc. IEEE Power Syst. Comput. Conf.*, 2014, pp. 1–8.
[58] A. Tarali and A. Abur, "Bad data detection in two-stage state estimation using phasor measurements," in *Proc. 2013 23rd IEEE PES Int. Conf. Exhib. Innovative Smart Grid Technol. Eur.*, 2012, pp. 1–8.
[59] V. Kekatos and G. Giannakis, "Distributed robust power system state estimation," *IEEE Trans. Power Syst.*, vol. 28, no. 2, pp. 1617–1626, May 2013.
[60] Y. Huang, H. Li, K. Campbell, and Z. Han, "Defending false data injection attack on smart grid network using adaptive CUSUM test," in *Proc. IEEE Annu. Conf. Inf. Sci. Syst.*, 2011, pp. 1–6.
[61] A. Tajer, S. Kar, H. V. Poor, and S. Cui, "Distributed joint cyber attack detection and state recovery in smart grids," in *Proc. IEEE Int. Conf. Smart Grid Commun.*, 2011, pp. 202–207.
[62] F. Pasqualetti, R. Carli, and F. Bullo, "A distributed method for state estimation and false data detection in power networks," in *Proc. IEEE Int. Conf. Smart Grid Commun.*, 2011, pp. 469–474.
[63] F. Pasqualetti, R. Carli, and F. Bullo, "Distributed estimation via iterative projections with application to power network monitoring," *Automatica*, vol. 48, no. 5, pp. 747–758, 2012.
[64] O. Vuković, K. C. Sou, G. Dán, and H. Sandberg, "Network-layer protection schemes against stealth attacks on state estimators in power systems," in *Proc. IEEE Int. Conf. Smart Grid Commun.*, 2011, pp. 184–189.
[65] O. Vuković, K. C. Sou, G. Dán, and H. Sandberg, "Network-aware mitigation of data integrity attacks on power system state estimation," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 6, pp. 1108–1118, Jul. 2012.
[66] T. Liu, Y. Gu, D. Wang, Y. Gui, and X. Guan, "A novel method to detect bad data injection attack in smart grid," in *Proc. IEEE INFOCOM Workshop*, 2013, pp. 3423–3428.
[67] Q. Yang, J. Yang, and X. Ma, "Research on false data injection attacks in power systems," *Microelectron. Comput.*, vol. 28, no. 12, pp. 1–5, 2011.
[68] D. Wang, X. Guan, T. Liu, Y. Gu, Y. Sun, and Y. Liu, "A survey on bad data injection attack in smart grid," in *Proc. IEEE PES Asia-Pac. Power Energy Eng. Conf.*, 2013, pp. 1–6.
[69] Z. Guan, N. Sun, Y. Xu, and T. Yang, "A comprehensive survey of false data injection in smart grid," *Int. J. Wirel. Mob. Comput.*, vol. 8, no. 1, pp. 27–33, 2015.
[70] A. Monticelli, *State Estimation in Electric Power Systems: A Generalized Approach*. Berlin, Germany: Springer, 1999.
[71] A. J. Wood and B. F. Wollenberg, *Power Generation, Operation and Control*. Hoboken, NJ, USA: Wiley, 1996.
[72] F. Li, Y. Wei, and S. Adhikari, "Improving an unjustified common practice in Ex Post LMP calculation: An expanded version," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, 2010, pp. 1–4.
[73] A. L. Ott, "Experience with PJM market operation, system design, and implementation," *IEEE Trans. Power Syst.*, vol. 18, no. 2, pp. 528–534, May 2003.
[74] T. Zheng and E. Litvinov, "Ex post pricing in the co-optimized energy and reserve market," *IEEE Trans. Power Syst.*, vol. 21, no. 4, pp. 1528–1538, Nov. 2006.
[75] D. B. Patton, P. LeeVanSchaick, and J. Chen, "Assessment of the ISO New England Electricity Markets," 2014. [Online]. Available: http://www.iso-ne.com/static-assets/documents/2015/06/isone_2014_emm_report_6_16_2015_final.pdf
[76] S. P. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.
[77] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner Jr, "Assessing the spoofing threat: Development of a portable GPS civilian spoofer," in *Proc. Int. Tech. Meeting Satell. Div. Inst. Navig.*, 2008, pp. 2314–2325.
[78] Q. Yang, D. An, and W. Yu, "On time desynchronization attack against IEEE 1588 protocol in power grid systems," in *Proc. IEEE Energytech*, 2013, pp. 1–5.
[79] Z. Zhang, S. Gong, A. D. Dimitrovski, and H. Li, "Time synchronization attack in smart grid: Impact and analysis," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 87–98, Mar. 2013.
[80] X. Jiang, J. Zhang, B. J. Harding, J. J. Makela, and A. D. Domınguez-Garcıa, "Spoofing GPS receiver clock offset of phasor measurement units," *IEEE Trans. Power Syst.*, vol. 28, no. 3, pp. 3253–3262, Aug. 2013.
[81] S. Barreto, A. Suresh, and J.-Y. Le Boudec, "Cyber-attack on packet-based time synchronization protocols: The undetectable delay box," in *Proc. IEEE Int. Instrum. Meas. Technol. Conf.*, 2016, pp. 1–6.
[82] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "GPS vulnerability to spoofing threats and a review of antispoofing techniques," *Int. J. Navig. Obs.*, vol. 2012, 2012, Art. no. 127072.
[83] J. Magiera and R. Katulski, "Accuracy of differential phase delay estimation for GPS spoofing detection," in *Proc. IEEE Int. Conf. Telecommun. Signal Process.*, 2013, pp. 695–699.
[84] Y. Fan, Z. Zhang, M. Trinkle, A. D. Dimitrovski, J. B. Song, and H. Li, "A cross-layer defense mechanism against GPS spoofing attacks on PMUs in smart grids," *IEEE Trans. Smart Grid*, vol. 6, no. 6, pp. 2659–2668, Nov. 2015.



Ruilong Deng (S'11–M'14) received the B.Sc. and Ph.D. degrees in control science and engineering from Zhejiang University, Hangzhou, China, in 2009 and 2014, respectively.

He was a Visiting Scholar at Simula Research Laboratory, Norway, in 2011, and the University of Waterloo, Canada, from 2012 to 2013. He was a Research Fellow at Nanyang Technological University, Singapore, from 2014 to 2015. He is currently an AITF Postdoctoral Fellow in the Department of Electrical and Computer Engineering, University of Alberta, Edmonton, AB, Canada. His research interests include smart grid, cyber security, and wireless sensor network.

Dr. Deng currently serves as an Editor of the IEEE/KICS JOURNAL OF COMMUNICATIONS AND NETWORKS, and a Guest Editor for IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTING, and *Hindawi Journal of Computer Networks and Communications*. He also serves/served as a technical program committee member for the IEEE GLOBECOM, IEEE ICC, IEEE SmartGridComm, EAI SGSC, and others.

Gaoxi Xiao (M'99) received the B.S. and M.S. degrees in applied mathematics from Xidian University, Xi'an, China, in 1991 and 1994, respectively, and the Ph.D. degree in computing from the Hong Kong Polytechnic University, Hong Kong, in 1998.

He was an Assistant Lecturer in Xidian University during 1994–1995, a Postdoctoral Research Fellow in Polytechnic University, Brooklyn, NY, USA, in 1999; and a Visiting Scientist in the University of Texas at Dallas during 1999–2001. He joined the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, in 2001, where he is currently an Associate Professor. His research interests include complex systems and networks, communication networking, system resilience and robustness, smart grids and cyber security.

Dr. Xiao is serving or has served as an Editor or Invited Editor for *PLOS ONE*, *The European Physical Journal B*, *Advances in Complex Systems*, and others, and a TPC member for conferences including IEEE ICC, GLOBECOM, and INFOCOM.

Rongxing Lu (S'09–M'11–SM'15) received the Ph.D. degree from the Department of Electrical and Computer Engineering, University of Waterloo, ON, Canada, in 2012, for which he received the prestigious Governor General's Gold Medal.

Since August 2016, he has been an Assistant Professor in the Faculty of Computer Science, University of New Brunswick, Fredericton, NB, Canada. Before that, he was an Assistant Professor in the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, from May 2012 to August 2016. He was a Postdoctoral Fellow at the University of Waterloo from May 2012 to April 2013. He has published extensively in his areas of expertise (with more than 7500 citations from Google Scholar). His research interests include applied cryptography, privacy enhancing technologies, and IoT–Big Data security and privacy.

Dr. Lu received the 8th IEEE Communications Society Asia Pacific Outstanding Young Researcher Award in 2013, the Student Best Paper Award, ITS Summit Singapore 2015 (with his students and colleagues), the IEEE IES Student Best Paper Award in 2014, the Best Paper Awards of *Tsinghua Science and Technology Journal* in 2014, IEEE ICCC in 2015, IEEE WCNC in 2013, BodyNets in 2010, and IEEE ICCCN in 2009. He is currently a senior member of the IEEE Communications Society. He was/is on the editorial boards of several international refereed journals, e.g., IEEE NETWORK, and currently serves as the Technical Symposium Co-chair of the IEEE GLOBECOM'16 and many technical program committees of the IEEE and other international conferences, including IEEE INFOCOM and ICC. In addition, he is currently organizing a special issue on "security and privacy issues in fog computing" in *Elsevier Future Generation Computer Systems* and a special issue on "big security challenges in big data era" in IEEE INTERNET OF THINGS. He currently serves as the Secretary of the IEEE Communications and Information Security Technical Committee.

Hao Liang (S'09–M'14) received the Ph.D. degree from the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada, in 2013.

Since 2014, he has been an Assistant Professor in the Department of Electrical and Computer Engineering, University of Alberta, Edmonton, AB, Canada. From 2013 to 2014, he was a Postdoctoral Research Fellow in the Broadband Communications Research Lab and Electricity Market Simulation and Optimization Lab, University of Waterloo. His current research interests include the areas of smart grid, wireless communications, and wireless networking.

Dr. Liang received the Best Student Paper Award from the IEEE 72nd Vehicular Technology Conference (VTC Fall-2010), Ottawa, ON, Canada. He serves/served as an Editor for *IET Communications*, and a Guest Editor for IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTING and *Hindawi Journal of Computer Networks and Communications*. He has been a Technical Program Committee (TPC) Member for major international conferences in both information/communication system discipline and power/energy system discipline, including IEEE International Conference on Communications, IEEE Global Communications Conference, IEEE VTC, IEEE Innovative Smart Grid Technologies Conference, and IEEE International Conference on Smart Grid Communications. He was the System Administrator of the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY (2009–2013).

Athanasios V. Vasilakos (M'00–SM'11) is currently a Professor with the Lulea University of Technology, Lulea, Sweden.

Prof. Vasilakos served or is serving as an Editor for many technical journals, such as the IEEE TRANSACTIONS ON NETWORKS AND SERVICES MANAGEMENT, IEEE TRANSACTIONS ON CLOUD COMPUTING, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, IEEE TRANSACTIONS ON CYBERNETICS, IEEE TRANSACTIONS ON NANOBIOSCIENCE, IEEE TRANSACTIONS ON INFORMATION TECHNOLOGY IN BIOMEDICINE, *ACM Transactions on Autonomous and Adaptive Systems*, and IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS. He is also the General Chair of the European Alliances for Innovation (www.eai.eu).