Profit-Oriented False Data Injection on Electricity Market: Reviews, Analyses, and Insights

Qiwei Zhang, *Student Member, IEEE*, Fangxing Li, *Fellow, IEEE*, Qingxin Shi, *Member, IEEE*, Kevin Tomsovic, *Fellow, IEEE*, Jinyuan Sun, *Member, IEEE*, and Lingyu Ren, *Member, IEEE*

***Abstract*—The rapid evolution of sensor technologies and communication networks is tightly coupling the cyber and physical layers of power systems. Because a few power grids have fallen victim to cyber intrusions causing unexpected device failure and large-scale power outages, enhancing power system cybersecurity is the utmost focus of power grid development today. Financially, the deregulation of the electricity market opens the gate to profit-oriented cyberattacks. Real-time market auctions rely heavily on the accuracy of state estimation, which is susceptible to cyberattacks. Extensive reviews have been conducted on modern power system cybersecurity. However, the lack of a comprehensive and in-depth review of electricity market cyberattacks prevents independent system operators from systematically analyzing the financial consequences of cyberattacks and limits public awareness of the significant monetary loss. This article briefly summarizes previous review works and analyzes the two-settlement market design from a cybersecurity perspective. Then the current achievements of electricity market cyberattacks are discussed, and state-of-the-art works are analyzed based on their contributions. Additionally, a few possible improvements and future directions are presented.**

***Index Terms*—Day-ahead (DA) market, false data injection, real-time (RT) market, state estimation, two-settlement market.**

NOMENCLATURE

Sets and Indicis

T	Set of time periods.
N_b	Set of system buses.
L	Set of transmission lines.

Parameters

$SC_{i,t}$	Start-up cost for unit i at time t.
$\mathrm{NLC}_{i,t}$	No-load cost for unit i at time t.
$C_{i,t}$	Generation cost for unit i at time t.
$D_{i,t}$	Load at a specific bus i at time t.
d	Total load.
$F^{\max}{}_l$, $F^{\min}{}_l$	Upper and lower transmission capacity for line l.
$\mathrm{GSF}_{l\text{-}i}$	Generation shift factor matrix.
$P^{\max}{}_i$, $P^{\min}{}_i$	Upper and lower generation capacity for unit i.
δ	Fluctuation parameter (usually 0.001).
z	Raw measurements for state estimation.
$h(x)$	Function describing the relationship between measurement z and states x.
H	Linearized $h(x)$.
R	Variance matrix for measurement z.
e	Measurement error.
r	Residual vector.
S	Sensitivity matrix.

Variables

$s_{i,t}$, $on_{i,t}$	Start-up decision and status for unit i at time t.
P_i	Generation of unit i.
ΔP_i	Hypothetical incremental generation of unit i.
ΔD_i	Dispatch loads.
ν	Lagrange multiplier for power balance constraint.
$\kappa^+{}_l$, $\kappa^-{}_l$	Lagrange multipliers for transmission capacity constraints.
$\eta^+{}_i$, $\eta^-{}_i$	Lagrange multipliers for generator capacity constraints.
z_{com}	Compromised measurements.
z_a, Δa	Attack vector for measurements and bids.

Manuscript received December 23, 2019; revised August 16, 2020 and September 21, 2020; accepted October 25, 2020. Date of publication November 6, 2020; date of current version June 16, 2021. This work was supported in part by the US Department of Energy CEDS Project "Watching Grid Infrastructure Stealthily Through Proxies (WISP)" under Award DE-OE0000899 and in part by the CURENT which is a US NSF/DOE Engineering Research Center funded by NSF Award EEC-1041877. Paper no. TII-19-5433. *(Corresponding author: Fangxing Li.)*

Qiwei Zhang, Fangxing Li, Qingxin Shi, Kevin Tomsovic, and Jinyuan Sun are with the Department of Electrical Engineering and Computer Science, The University of Tennessee, Knoxville, TN 37996 USA (e-mail: qzhang41@vols.utk.edu; fli6@utk.edu; qshi1@vols.utk.edu; tomsovic@tennessee.edu; jysun@utk.edu).

Lingyu Ren is with the Raytheon Technologies Research Center, East Hartford, CT 06108 USA (e-mail: renlingy@utrc.utc.com).

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

Digital Object Identifier 10.1109/TII.2020.3036104

I. INTRODUCTION

THE GROWTH of the Internet profoundly impacts everyday life and industrial developments. A global and interconnected communication network introduces both opportunities and threats to the development of the modern power grid. With the traditional power industry evolving towards a smart grid scheme, the complex coupling between cyber and physical power systems operation challenges the existing cyber protection measures. A few real-world cases have demonstrated the current capability of cyberattacks: in 2003, a Slammer worm disabled the safety monitoring of an Ohio nuclear plant for five

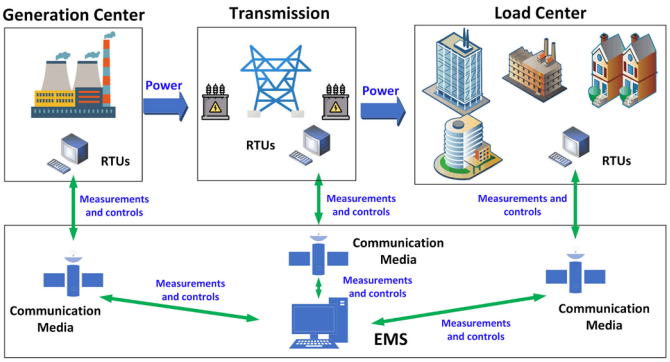


Fig. 1. Power flow and data flow network.

hours [1]; in 2010, a virus called Stuxnet invaded an Iranian Supervisory Control & Data Acquisition (SCADA) system to delay the nuclear program [1]; in 2015 an illegal third-party entry into a SCADA system in Ukraine caused a large-scale power outage over three regions [2]. These cases invalidate the traditional belief that cyberattacks are unable to penetrate real-world industrial systems.

Beyond the physical damage, some attackers target financial arbitrage advantages brought by false data injection attacks (FDIAs) [3]. Under the deregulated power market, electricity prices are extremely volatile and heavily reliant on real-time (RT) data gathering. The independent system operator (ISO) collects bids and offers from various market participants. The state estimation results construct the RT network model [4]. The locational marginal prices (LMPs) are then calculated to clear the market. Fig. 1 depicts the power flow and data communication flow for electricity market operations. The remote terminal units (RTUs) at substations and generators transmit the raw measurements, such as power flow, power injection, and bus voltage to the SCADA system. Then the state estimation calculates the best estimate of the system states. The electricity market-clearing model is formulated using state estimation results.

Therefore, a profit-oriented FDIA targets the SCADA system to modify state estimation results and compromise the RT market LMPs accordingly. In [5], the impacts of FDIAs on the electricity market are first thoroughly analyzed. The authors form a stealthy FDIA against state estimation and realize the monetary gain by up-to-congestion transactions (UTCs). Subsequently, a significant amount of research has been conducted on this topic.

The state-of-the-art works on profit-oriented electricity market FDIAs have been categorized in Table I. Research works [5]–[32] include most of the profit-oriented attack strategies on the electricity market. Research works [33]–[42] cover the defense of attack routes related to the electricity market since there is a lack of direct market-level defense. Nine research directions have been identified based on their contributions.

Works on power system cybersecurity have been reviewed extensively: in [1] and [44], the literature on FDIAs is classified into three topics: the design of FDIAs, the impact of FDIAs, and defense against FDIAs; literature [43] categorizes current

TABLE I
ELECTRICITY MARKET CYBERATTACK LITERATURE CATEGORY

Type	Research Direction	Reference
Attack strategies for monetary gain	Attacker and defender interaction	[6][7][8][9]
	Attack strategies with imperfect topology information	[10][11][12][13]
	Congestion pattern attack strategies	[5][14][15][16][17]
	Topology attack strategies	[18] [19][20]
	New attack paths	[21][22][23][24][25] [26][27]
	Sensitivity analysis	[28][29][30][31][32]
Defense strategies	Securing pre-selected sensors	[33][34] [35][36]
	Improving state estimation algorithms	[37][38][39] [40]
	Other defense algorithms	[41][42]

cybersecurity works based on different attack paths, such as smart home device or SCADA system; in [45], the prevailing structures and characteristics of FDIAs and countermeasures are discussed; literature [46] reviews the role of data streaming in the smart grid and key techniques for data authentication.

However, review works focusing on the financial impacts of cyberattacks are not well categorized or clarified. In [3], the literature on electricity market FDIAs is summarized individually, but the categorization is broadly divided without analyzing connections. The focuses of review works [[1], [43]]–[45] are on FDIAs in general, and only a few studies of market FDIAs are mentioned.

The contributions of this review article are summarized as follows.

1) The two-settlement market mechanism is presented from a cybersecurity perspective.
2) The state-of-the-art works on electricity market cyberattacks are summarized and further categorized based on previous works.
3) The current achievements on this topic are presented, and a comprehensive review is provided where research works are divided by their contributions.
4) A number of potential future research directions are discussed.

The rest of this article is organized as follows. Section II presents an overview of electricity market models and analyzes their vulnerabilities. Section III analyzes market cyberattacks based on where they attack, how they avoid detection, how they gain profits, and what the impacts are. In Section IV, research works are categorized and analyzed according to their research directions. In Section V, countermeasures and defense strategies are presented. Section VI discusses a few potential future research directions. Finally, Section VII concludes this article.

II. Electricity Market Operation

Wholesale electricity markets in the U.S. are organized by ISOs/RTOs and usually consist of day-ahead (DA) and RT markets. The offers and bids from generator companies and load aggregators are collected by ISOs. Unit commitment and DA economic dispatch are solved to determine DA unit dispatches and LMPs. DA LMPs are calculated based on 24-h advance load forecasting. The purpose of the RT market is to offer adjustments for load forecasting differences between RT and DA. The RT market is cleared based on RT operation conditions obtained from state estimation. Therefore, attacking the DA market is less feasible because ISOs have plenty of time to detect and analyze. A significant number of profit-oriented attacks perform FDIA on state estimation to affect RT LMP calculations. The prevailing market operation models are presented in the following sections.

A. DA Electricity Market Model

The DA dispatch schedule is determined through simultaneous optimization of energy and reserves by the least-cost security-constrained unit commitment (SCUC) and security-constrained economic dispatch (SCED) [47]. A simplified SCUC model is shown in (1)–(7):

$$\min_{on,\text{start},p_{i,t}} \sum_i \sum_t \text{SC}_{i,t} s_{i,t} + \text{NLC}_{i,t} on_{i,t} + C_{i,t}(P_{i,t}) \quad (1)$$

$$\sum_i P_{i,t} - d_t = 0 \forall t \in T \quad (2)$$

$$F_l{}^{\max} \geq F_l \geq F_l{}^{\min} \forall l \in L \quad (3)$$

$$P_{i,t}^{\min} on_{i,t} \leq P_{i,t} \forall t \in T \quad \forall i \in N_b \quad (4)$$

$$P_{i,t} \leq P_{i,t}^{\max} on_{i,t} \forall t \in T \; \forall i \in N_b \quad (5)$$

$$s_{i,t} \leq on_{i,t} \leq s_{i,t} + on_{i,t-1} \; \forall t \in T \forall i \in N_b \quad (6)$$

$$s_{i,t} \text{ and } on_{i,t} \text{ are binary } \forall t \in T \forall i \in N_b. \quad (7)$$

After the unit commitment is fixed, the SCED is formulated at each period (8)–(12)

$$\min \sum_i C_i(P_i) \quad (8)$$

$$\sum_i P_i - d = 0 \quad (9)$$

$$P^{\min}{}_i \leq P_i \leq P^{\max}{}_i \; \forall i \in N_b \quad (10)$$

$$\sum_{i=1}^{N_b} \text{GSF}_{l-i}(P_i - D_i) \leq F_l{}^{\max} \; \forall l \in L \quad (11)$$

$$\sum_{i=1}^{N_b} \text{GSF}_{l-i}(P_i - D_i) \geq F_l{}^{\min} \; \forall l \in L. \quad (12)$$

Lagrange multipliers are assigned to each constraint to formulate the Lagrange function. The LMP at bus i is defined as the effect of incremental load on the cost function, as shown in the following equation:

$$\text{LMP}_i = v - \sum \text{GSF}_{l-i} \kappa^+{}_l + \sum \text{GSF}_{l-i} \kappa^-{}_l. \quad (13)$$

It is theoretically possible to perform a man-in-the-middle (MITM) attack to modify bids or offer signals through the market gateway so that the ISOs clear the market based on incorrect information. However, cyberattacks on the DA market are unlikely to happen because of the following reasons.

1) The DA market is cleared a day before RT operation, during which market participants and ISOs have plenty of time to detect such anomalies.
2) The DA market-clearing results are based on both the unit commitment and the economic dispatch, which complicate the computation of attack vectors.
3) The profitability of such attacks is largely impacted by RT operation conditions. Therefore, attacking the DA market is less viable.

B. RT Electricity Market Model

The RT market is designed to balance actual demand and satisfy RT system conditions. The RT market price is unknown until the operation hour is approaching. Thus, RT LMPs are extremely volatile.

Two primary approaches to calculate RT LMPs are the *ex-ante* method (e.g., NYISO) and the *ex-post* method (e.g., PJM) [48]. In the *ex-ante* model, generation dispatches and LMPs are calculated based on the forecasted conditions for the next trading period. The price is settled in a near RT estimate. The *ex-ante* model formulation is shown in the following equations:

$$\min \sum_i C_i^{RT}(P_i) \quad (14)$$

$$\sum_i P_i - d^{RT} = 0 \quad (15)$$

$$P^{RT\,\min}{}_i \leq P_i \leq P^{RT\,\max}{}_i \; \forall i \in N_b \quad (16)$$

$$\sum_{i=1}^{N_b} \text{GSF}_{l-i}(P_i - D_i^{RT}) \leq F_l{}^{\max} \; \forall l \in L \quad (17)$$

$$\sum_{i=1}^{N_b} \text{GSF}_{l-i}(P_i - D_i^{RT}) \geq F_l{}^{\min} \; \forall l \in L. \quad (18)$$

The *ex-post* model is purely a price-setting model. Generation dispatch is determined via the *ex-ante* model, while the nodal price is calculated by the *ex-post* model (19)–(24) [48]. The *ex-post* model is an incremental model based on RT system conditions. If the generators and load perform exactly as instructed, then LMPs from the *ex-ante* model and LMPs from the *ex-post* model converge

$$\min \sum_i^{N_b} C_i^{RT}(\Delta P_i) - \sum_i^{N_b} \text{d}_i(\Delta D_i) \quad (19)$$

$$\sum_i^{N_b} \Delta P_i = \sum_i^{N_b} \Delta D_i \quad (20)$$

$$\sigma {P_i}^{RT\max} \le \Delta P_i \le \sigma {P_i}^{RT\min} \ \forall i \in N_b \tag{21}$$

$$\sum_{i=1}^{N_b} \mathrm{GSF}_{l-i}(\Delta P_i - \Delta D_i) \le \sigma {F_l}^{RT\max} \ \forall l \in L \tag{22}$$

$$\sum_{i=1}^{N_b} \mathrm{GSF}_{l-i}(\Delta P_i - \Delta D_i) \ge \sigma {F_l}^{RT\min} \ \forall l \in L. \tag{23}$$

The formulation of RT nodal prices is similar to (13).

In the RT market model, constraints are formulated through state estimation. For example, the congestion pattern L is decided by line flow results from state estimation. Raw measurement data, such as line flow, power injection, and voltage magnitude, is measured and transmitted through RTUs to control centers. This remote connection allows an attacker to compromise the data streaming between RTUs and control centers and manipulate the state estimation results. Additionally, attackers have more profitability in an RT market attack. The *ex-post* model provides LMPs for the previous period. Thus, when the attack applies, there is lower uncertainty affecting the profitability of such an attack. Consequently, a large amount of profit-oriented attack strategies target at RT market operations.

III. Analysis of Electricity Market Cyberattacks

Different from traditional malicious data intrusions, cyberattacks on the electricity market consider the following.

1) The attackers' participation in the market-clearing.
2) The profitability of the attack strategies.
3) Bypassing control center detection, such as bad data identification.

In this section, market cyberattacks are analyzed based on where they attack, how they avoid detections, how they gain profits, and what the impacts are.

A. Where to Attack

The construction of RT market model is mainly based on the result of state estimation and parameters from the market gateway. Therefore, two main attack paths are: 1) the measurement data, which may alter the result of state estimation; and 2) the market gateway where generators and loads submit bids and offers.

1) State Estimation: The majority of the market cyberattacks in the literature are performed on state estimation.

The basic principle of state estimation is presented in the following equations:

$$z = h(x) + e \tag{24}$$

$$x = (x_1, x_2, \ldots, x_n)^T \tag{25}$$

$$z = (z_1, z_2, \ldots, z_m)^T \tag{26}$$

where x is a system states vector, z is a measurement vector, and e is the random noise vector. Function $h(x)$ describes the relationship between the system states and measurements. As shown in Fig. 2, attackers perform a MITM attack to compromise data streaming between the control center and local RTUs. In this way, vector z is modified by the attacker.

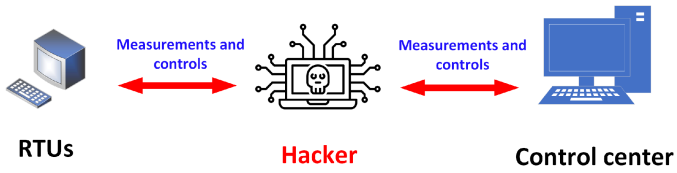


Fig. 2. MITM attack between RTU and control center.

The weighted least square method is commonly adopted in the control center to constructs the ac state estimation problem [50]. The weighted least square is described in (27), where W is the weight matrix for measurements. When z is manipulated by an attacker, x is affected accordingly

$$\min J(x) = \frac{1}{2}(z - h(x))^T W (z - h(x)). \tag{27}$$

Few research works on market cyberattack apply the ac state estimation model. Most works utilize the approximated dc model, e.g., [5]–[31]. The dc model simplifies (24) as (28). The estimated states and measurements are calculated as (29), (30)

$$z = Hx + e \tag{28}$$

$$\tilde{x} = (H^T R^{-1} H)^{-1} H^{\mathrm{T}} R^{-1} z \tag{29}$$

$$\tilde{z} = H(H^T R^{-1} H)^{-1} H^{\mathrm{T}} R^{-1} z. \tag{30}$$

When the attack vector (31) is added, the estimated state and state estimation results change as in (32) and (33)

$$z_{\mathrm{com}} = z + z_a \tag{31}$$

$$\tilde{x} = (H' R^{-1} H)^{-1} H' R^{-1} z_{\mathrm{com}} \tag{32}$$

$$\tilde{z} = H(H' R^{-1} H)^{-1} H' R^{-1} z_{\mathrm{com}}. \tag{33}$$

By manipulating the estimated line flow, the congestion pattern is compromised. The Lagrange multiplier associated with the compromised line is changed to 0 or from 0 to a positive number, and thus LMPs are modified. The new set of Lagrange multipliers are obtained by resolving the Karush–Kuhn–Tucker (KKT) conditions.

However, it is inaccurate to claim that LMPs are manipulated by such attacks. Manipulation of the line congestion pattern is not the same as the manipulation of LMPs. First, attackers are unable to calculate the new Lagrange multipliers. Second, attackers can only create price differences but are unable to change LMPs to a specified value.

A potential method for manipulating LMPs is to compromise the bids and offers through the market gateway.

2) Market Participant Interface: The relationship between the bidding information and LMPs can be inferred by formulating the stationary (34) in market model KKT conditions

$$\frac{\partial C_i(p_i)}{\partial P_i} - v + \sum_{l=1}^{L} \mathrm{GSF}_{l-i}(\kappa^+{}_l - \kappa^-{}_l) + \eta^+{}_i - \eta^-{}_i = 0. \tag{34}$$

Then, (34) is reformed to (35) by separating the bid term $\partial C_i(p_i)/\partial P_i$ with the Lagrange multipliers

$$\frac{\partial C_i(p_i)}{\partial P_i} = v - \sum_{l=1}^{N_L} \kappa^+{}_i \mathrm{GSF}_{l-i} + \sum_{l=1}^{N_L} \kappa^-{}_i \mathrm{GSF}_{l-i} - \eta^+{}_i + \eta^-{}_i. \tag{35}$$

Therefore, the relation between bid information and LMPs is developed in the following equations:

$$\frac{\partial C_i(p_i)}{\partial P_i} = LMP_i - \eta^+{}_i + \eta^-{}_i. \tag{36}$$

Attackers manipulate bid information when the RT market gateway is compromised, as in (37). It worth noting that the results of such an attack depend on the marginal unit patterns

$$\frac{\partial C_i(p_i)}{\partial P_i} + \Delta a = \mathrm{LMP}^{\mathrm{new}}{}_i - \eta^{\mathrm{new}+}{}_i + \eta^{\mathrm{new}-}{}_i. \tag{37}$$

Scenario 1: when the marginal unit's bids are modified, and the attack vector is small enough to maintain the original marginal unit patterns, LMPs are manipulated by such an attack as follows:

$$\eta^+{}_i = 0, \eta^-{}_i = 0 \tag{38}$$

$$\frac{\partial C_i(p_i)}{\partial P_i} + \Delta a = \mathrm{LMP}^{\mathrm{new}}{}_i = \mathrm{LMP}_i + \Delta a. \tag{39}$$

Scenario 2: when marginal units stay the same, and the non-marginal unit is attacked, this attack is inactive until an amount of Δa large enough to alter the marginal unit pattern, as in the following equations:

$$\frac{\partial C_i(p_i)}{\partial P_i} + \Delta a = \mathrm{LMP}_i - \eta^{\mathrm{new}+}{}_k + \Delta a \leq \mathrm{LMP}_i \tag{40}$$

$$\frac{\partial C_i(p_i)}{\partial P_i} + \Delta a = \mathrm{LMP}_i + \eta^{\mathrm{new}-}{}_k - \Delta a = \mathrm{LMP}_i. \tag{41}$$

Scenario 3: the modified bids turn a marginal unit to a non-marginal unit or a nonmarginal unit to a marginal unit. The bid of the new marginal unit will contribute to the LMPs, as in the following equation:

$$\mathrm{LMP}_i = \sum_{j \in MG_{new}} \mathrm{LMP}_j \frac{\partial P_j}{\partial D_i}. \tag{42}$$

Therefore, the identification of marginal units is crucial to perform such an attack. Most attackers may not have enough information to estimate which unit is the marginal unit. An efficient algorithm for marginal unit estimation combined with this cyberattack may cause significant financial loss.

There are other unconventional attack paths in the market operation: such as communication at the demand side [25] and line rating information manipulation [27]. Further explanations of those attacks are included in Section IV-E.

B. Where to Gain Profit

To gain profit from the electricity market, the attackers have to participate in the market operation. However, owning a generation resource or cooperating with the generator company may reveal attackers' identity to control centers.

Therefore, a virtual bidding transaction best fits the attackers' needs. Virtual bidding is an arbitrage from the DA market to the RT market to increase liquidity in market operations. Normally, three types of virtual bidding are offered in the U.S.: increment offers (INCs), decrement bids (DECs), and UTCs [49]. In an INC, the bidder sells a certain amount of power at a node in the DA market and buys it back at the RT market. This trade is profitable when the DA LMP exceeds the RT LMP

$$\mathrm{Pay} = (\mathrm{LMP}_{DA} - \mathrm{LMP}_{RT})P. \tag{43}$$

DECs are performed in the opposite way to INCs

$$\mathrm{Pay} = (\mathrm{LMP}_{RT} - \mathrm{LMP}_{DA})P. \tag{44}$$

UTCs are performed to gain profit via the congestion and loss difference between the RT market and the DA market

$$\mathrm{Pay} = \left[(\mathrm{LMP}^A{}_{DA} - \mathrm{LMP}^B{}_{DA}) - (\mathrm{LMP}^A{}_{RT} - \mathrm{LMP}^B{}_{RT})\right] P. \tag{45}$$

Furthermore, (45) is reformulated as follows:

$$\sum_{l=1}^{N_L} (\kappa^+{}_l - \kappa^-{}_l)(\mathrm{GSF}_{l-A} - \mathrm{GSF}_{l-B}) + (\mathrm{LMP}^A{}_{DA} - \mathrm{LMP}^B{}_{DA})P. \tag{46}$$

Virtual bidding is a purely financial transaction that requires no physical power delivery or consumption. Thus, virtual bidding is the preferred way for an attacker to gain profit. As stated in Section III-A, LMPs are not fully manipulatable, but the created price difference can guarantee attackers' profit if the following conditions are satisfied [5].

1) Careful selection of bus A and B in the DA market (47)

$$(\mathrm{LMP}^A{}_{DA} - \mathrm{LMP}^B{}_{DA}) \geq 0. \tag{47}$$

2) For lines that $\mathrm{GSF}_{l-A} > \mathrm{GSF}_{l-B}$, those lines are modified to non-negative congested lines

$$\sum_{l=1}^{N_L} (\kappa^+{}_l - \kappa^-{}_l) \geq 0. \tag{48}$$

3) For lines that $\mathrm{GSF}_{l-A} < \mathrm{GSF}_{l-B}$, those lines are modified to nonpositive congested lines

$$\sum_{l=1}^{N_L} (\kappa^+{}_l - \kappa^-{}_l) \leq 0. \tag{49}$$

Depending on the attack model, different virtual transactions could be selected. For example, literature [14] and [27] consider DECs at a pre-selected bus. In [5] and [26], the UTC is applied to gain profit.

C. How to Avoid Detection

The market operator typically collects data from two sources: state estimation and market gateway. Research works on market FDIAs have been focusing on avoiding the state estimation level detections. Measurements transmitted from RTUs are imperfect due to the finite accuracy of meters or communication systems.

With sufficient redundancy of measurements, a typical module of bad data detection is expected to filter out the errors. Therefore, the injection of false data could be identified by the bad data detection module. Most research works on market cyberattacks consider bypassing bad data detection. The largest normalized residual test is a prevailing model for bad data detection to find the anomalies in a measurement set. The difference between estimated measurement data and raw measurement data is calculated in (50). Then, (51) describes the relationship between residuals and errors. The obtained residuals are normalized by (52) and (53). If the calculated $r_i{}^N$ exceeds a certain threshold (54), the measurement i is identified as bad data

$$r = z - \tilde{z} \tag{50}$$

$$\mathrm{r} = (I - H(H^T R^{-1} H)^{-1} H^{\mathrm{T}} R^{-1})(h(x) + e) \tag{51}$$

$$S = I - H(H^T R^{-1} H)^{-1} H^{\mathrm{T}} R^{-1} \tag{52}$$

$$r_i{}^N = \frac{r_i}{\sqrt{S_{ii} R_{ui}}} \tag{53}$$

$$\left\| r_i{}^N \right\|_2 > \text{threshold } \forall i \in M. \tag{54}$$

To avoid the detection, the additional residual induced by FDIAs, as in (55), needs to be controlled. Thus, if the resulting res is less than a threshold, the attack is assumed to be undetectable

$$\mathrm{res} = (I - H_{\mathrm{act}}(H'_{\mathrm{act}} R^{-1} H_{\mathrm{act}})^{-1} H'_{\mathrm{act}} R^{-1}) z_a. \tag{55}$$

D. Impact of Profit-Oriented FDIAs on Market Operations

The profit-oriented FDIAs on the electricity market aims to bring financial arbitrages to some market participants. However, such FDIAs are also detrimental to the overall market operation, regardless of the profit-oriented objective. In [5]–[17], the congestion price is modified by manipulating the congestion patterns. Thus, the compromised congestion price between certain nodes creates profits for targeted market players. However, the change in congestion prices inevitably changes the LMPs at other nodes. Some of the normal market players may suffer from a significant loss, and some of the normal market players may receive a "free-ride" profit due to the FDIA. In either way, the social-welfare suffers from an inevitable loss because the FDIA deviates the financial settlement from the original equilibrium. Further, in [18]–[20] and [27], the topological information is manipulated by the attacker to create price deviations. Although the physical topology or line rating is unchanged, the compromised information induces erroneous generation dispatches, which may cause transmission line physical overload and outage. In [22]–[24], the load side management is compromised to manipulate LMPs. An erroneous load forecast or demand response induces excessive ancillary services, which not only diminishes social-welfare but also delivers incorrect signals for contingency analysis. In general, any fake parameters in the RT dispatch model may lead to social welfare loss and erroneous dispatches. Further, in the long-term, consecutively compromised LMPs deliver false signals to grid planning and investment decisions.

Market operation is a crucial part of supporting an economical and reliable grid operation. Although the intended impact of profit-oriented FDIAs is only to create profits for the targeted market players, the influence on market settlements leads to a chain reaction in the system. Therefore, the impact of such FDIAs is not limited to the profitability of certain market players. Profit-oriented FDIAs induce catastrophic consequences in grid operations, both financially and physically.

IV. Categorizing the Literature by Research Directions

In this section, the current FDIA efforts are reviewed in detail based on their contributions. Many works have investigated the impact of cyberattacks on the electricity market. State-of-the-art works on market FDIAs are summarized and analyzed in this section. Major research directions are identified and are shown in Fig. 3.

A. Attacker and Defender Interaction

The attacker's goal is to compromise market prices while the control center tries to identify and mitigate the attacks. Thus, the interaction between an attacker and a control center (defender) is intrinsically a zero-sum game. Esmalifalak *et al.* [6] model the Nash equilibrium of the attacker and defender, where the attacker and defender compete to increase/decrease the power flow from state estimation. Attackers and defenders are assumed to have a mixed strategy where the players randomly select moves. The possible outcome of this game is decided via (56) where a represent the outcome, and y and w are the action indicators selected by the attacker and defender

$$J(y, w) = \sum_{i=1} \sum_{j=1} y_i a_{ij} w_j = y' A w. \tag{56}$$

The defender tries to minimize $J(y,w)$, as in (57), while the attacker prefers to maximize $J(y,w)$, as in (58), and they both do not influence the other party's selections

$$V_{df} = \min_{Y} \max_{w} J(y, w) \tag{57}$$

$$V_{att} = \max_{w} \min_{Y} J(y, w). \tag{58}$$

Then the equilibrium point of the attacker and defender is found in the following equation:

$$V_{df} = V_{att}. \tag{59}$$

Instead of assuming that the attacker and defender act simultaneously, in [7], dynamic interaction is further modeled through multiact dynamic game theory. In [8] and [9], the attacker and defender are competing for measurements in PMU and substations, which causes loss of loads and misleads the economic dispatch eventually. The zero-sum game in the above-mentioned literature models the interaction of a single attacker and a single control center well. A more realistic setting could be provided by further modeling multiple attacker players and multiple defender players.

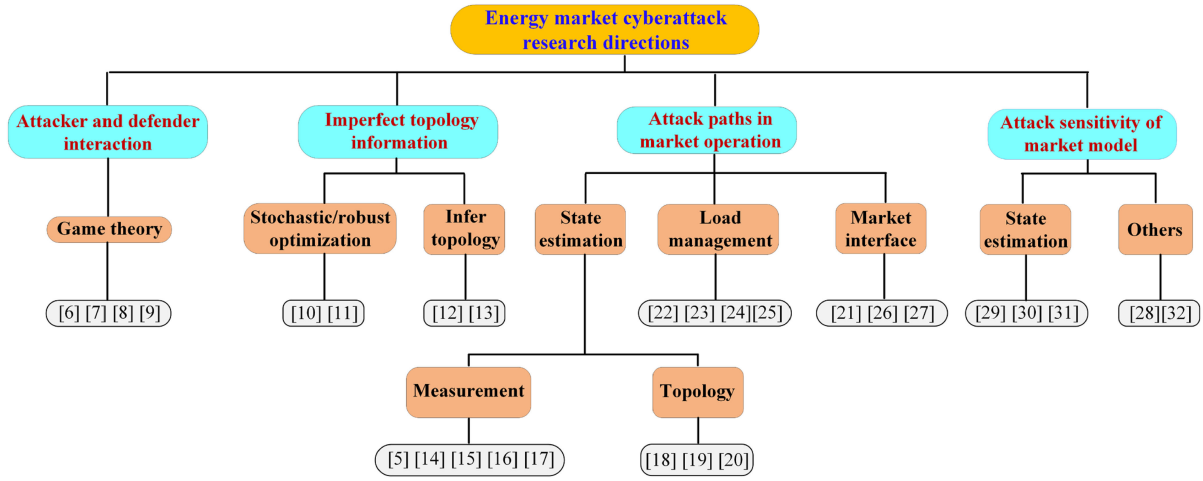


Fig. 3. Schematic picture of cyberattack research directions in electricity markets.

B. Imperfect Topology Information

As shown in (55), if the system topology matrix H is known, the extra residual induced by FDIAs can be reduced to zero by a careful selection of the attack vector. However, the system topology is extensive and volatile, and the attacker is unable to have the full topology information. Under this scenario, attacks are more likely to be detected by bad data detection.

Some research works launch profitable attacks without full grid information. In [10] and [11], the attacker is assumed to have partial access to topology information. To ensure profitability under the topology information uncertainty, research work [10] proposes a robust FDIA to guarantee worst-case profits. Research work [11] further models FDIAs through stochastic programming, where (55) is modified to a chance constraint as in (60), which means the possibility of passing bad data detection is larger than a confidence level η. The overall attack procedure is similar to attack strategies that have full information, but solving the chance constraint requires model reformulation and more computations.

$$P\left(\left\|(I - H(H'R^{-1}H)^{-1}H'R^{-1})z_{\text{com}}\right\|_2 < \text{thresh}\right) \geq \eta. \tag{60}$$

In [12], the attack vector is constructed without inferring H. The subspace of H is tracked by the measurement data, and thus, as long as the attack vector lies in the subspace of H, (55) is always satisfied.

The above-mentioned works focus on utilizing mathematic techniques to infer grid information or construct the attack vector by analyzing the relation between the state estimation and attack vectors. Kekatos *et al.* [13] provides a new path in which the topology matrix is inferred by observing successive RT LMPs.

C. Congestion Pattern Attack

Congestion pattern modification is the most commonly referred attack strategy in market cyberattacks. The true status of line flow f_l is at its maximum (61) while the attacker injects false data to relieve the congestion

$$f_l = {f_l}^{\max} \ \forall l \in L_{\text{taget}}. \tag{61}$$

The after-attack line flow becomes (62), which is usually used as a constraint in the attack model

$$f_l - (H'R^{-1}H)^{-1}H'R^{-1}z_a < {f_l}^{\max} \ \forall l \in L_{-\max}. \tag{62}$$

The modification of the congestion pattern changes the dual variables associated with line flow constraints, which modify the LMP.

In [14], both the financial gains and the possible blackout caused by modifying congestion patterns are discussed. In [15], an attacker adds or removes a transmission line from a contingency list to affect SCED. In [16], bogus trading in the DA market is combined with congestion pattern modifications to generate profit. Research work [17] presents an attack strategy which not only avoids bad data detection but also maximizes profits. It should be noted that relieving a congested line is much easier than congesting an uncongested line in terms of finding a valid attack vector. For example, a line is congested at its upper limit 200 MW, and the attack vector only needs to make a slight change to de-congest the line (e.g., reducing the line flow by 1 MW). As such, the attack vector leads to a very small change to the value of *res* in (55) and still causes a change in the congestion pattern, which eventually changes the value of LMPs.

D. Topology Attack

Similar to congestion pattern attacks, the topology attack modifies the digital information of break or switch status sent to topology processors. Thus, the optimal power flow calculation is significantly altered. Different from congestion pattern attacks, which normally relieve line congestions, topology attacks can add or switch off lines. From a market-clearing perspective, congestion pattern attacks take away particular line limits, but topology attacks change the generation shift factors. Therefore, the topology error can cause more damage than the congestion pattern attack. Current topology attack strategies focus on damaging market operations and social welfare. Profitable topology

attack strategies considering the altered dispatch are an area for future research. The topology attack literature is reviewed as follows to provide insights for further developments. The economic impact of adding, removing, and switching a line in a topology processor is provided in [18]. In [19], topology attacks and general FDIAs are combined to disturb the Australian electricity market LMP calculation, and the huge financial loss caused by such an attack is demonstrated. Further, research work [20] investigates the necessary information set under which the topology attack is undetectable.

E. New Attack Paths

Other than traditional attack strategies that focus on state estimations, market attackers have shown other attack paths to gain illegal profit.

In [21], an MITM attack is performed to modify the bid information of load aggregators and generator companies. A load redispatch (LR) attack compromises only load measurement and line flow measurement to affect power generation, as proposed in [22]. Research work [23] further applies the LR attack to produce desired congestion patterns, and thus the RT LMPs are controlled. Most existing RT market cyberattack works perform an attack on the *ex-post* market while research work [24] formulates an attack strategy performing on the very-short-term load forecasting. Thus, the *ex-ante* unit dispatch schedule is misguided, and the actual power generation is significantly affected, which gives the corrupted generator owner benefits. Instead of focusing on compromising data streaming between a control center and RTUs, research work [25] investigates the possibility of attacking communication between responsive demand and aggregators to disturb RT LMPs. In [26], the inter-temporal generator ramping constraint is compromised to withhold generator capacity. In this scenario, look-ahead dispatch is applied instead of the static SCED. The extra dual variables associated with the ramping constraint inevitably influence the LMPs, and thus modifying the ramping limit achieves a similar effect when modifying the congestion pattern. In [27], the transmission line ratings, namely the lower/upper bounder of line flow constraints, are compromised to ensure the profit of some market players.

F. Sensitivity Analysis

Performing cyberattacks or defending cyberattacks on the electricity market is a complicated task. An attacker prefers to inject as small of an amount of bad data as possible or compromise as few sensors as possible but generate a monetary gain as large as possible. Similarly, a defender wishes to protect sensors and mitigate attacks with the least amount of effort. To balance this tradeoff, sensitive analysis is paramount to potential attackers and defenders. In [28], the sensitivity between the price signal to responsive load and the power imbalance is developed. Research work [29] derives the mathematical representation between the congestion cost and topology errors, and thus the topology errors' impact on LMPs is formulated. In [30], both the error in system state and topology impact on LMPs are analyzed. It is shown that RT LMPs experience more variation if a topology error is combined with bad meter data. Further, in [31], the insensitivity between the attack vectors in critical measurements and system states is demonstrated, which leads to a long-term impact on LMPs. In [32], an opportunity for attackers to withhold distributed generator generation to gain profit is discussed, and the impact sensitivity of curtailment and profit is analyzed.

V. Electricity Market Attack Defense Algorithm

There is a lack of literature on market-level cyberattack detection mechanisms, such as how to detect cyber intrusions based on abnormal LMPs. The attack paths of market cyber intrusion normally lay in state estimation, as stated in Section III. Therefore, by enhancing state estimation, cyberattacks on the electricity market are less likely to happen. Some representative defense strategies that may contribute to the future development of market-level attack defense are summarized as follows.

A. Securing Preselected Sensors

As stated in [1], if the insecure sensor number K is larger than the difference between measurement number M plus one and bus number N, an undetectable FDIA is always feasible

$$K \geq M - N + 1. \tag{63}$$

Thus, if the defender can have at least M-N+1 sensor immune to attackers, the attack can no longer bypass the bad data detection [33]. Further, the protection of a sensor is assumed to have a defense budget. Based on this observation, a least-budget defense strategy is proposed in [34] to protect the system while spending the least on defense. Similarly, in [35], a graphical method is applied to identify a minimum number of measurements, and which is assumed secure so that none of the system states can be compromised.

Other than physically securing the basic measurement unit, replacing basic measurement units with phasor measurement units (PMUs) enhances data collection security. PMUs synchronize global time information with buses distributed over the system, which reduces the risk of being attacked. In [36], a greedy algorithm is proposed to place PMUs in a system efficiently, and if more than 1/3 of buses are equipped with a PMU, any attack vector largely increases the bad data detection residual.

B. Improving State Estimation Algorithms

Different from securing sensor measurements, works [37]–[39] develop algorithms facilitating bad data detection. Random noise in the raw measurements has consistent statistical distributions, but the maliciously added attack vector does not follow the distribution. Therefore, there is a possibility of differentiating the attack vector from the random noise via pretuned statistic algorithms. Based on this observation, Huang *et al.* [37] provide an adaptive cumulative sum method to determine the change of statistic properties. Similarly, in [38], a Kullback-Leibler distance is applied to calculate the similarity between two distributions. The measurement variations are obtained first, and then the historical error probability distribution is compared with probability distribution in RT operation to detect the FDIA.

Further, research work [39] observes that temporal system measurement typically has a low dimension structure, and the attack vector is normally sparse. Thus, a matrix separation method is proposed to detect the FDIA. In [40], a new detector is proposed to replace the classic largest normalized residue test based on the minimum mean square error to detect FDIAs.

C. Other Defense Algorithms

There are other defense methods against market cyberattacks, apart from enhancing state estimation. In [41], the reactance information of a preselected transmission line set is hidden from attackers, which significantly increase bad data detection possibilities. Based on this observation, an optimal line selection problem is formulated. Solving the problem gives the minimum line information to be hidden. In [42], the vulnerability of state estimation is improved from a communication security point of view, such as enhancing routing and data authentication.

VI. Future Directions

Based on the above-mentioned analysis and review of current research on electricity market cyberattacks, the following research directions are believed to be worth investigating.

A. Defense Strategies on the Market-Level, Such as Detecting Attacks Via Abnormal LMPs

Most of the research works have been developing defense strategies on state estimation. However, there is a lack of investigation in defense strategies based on market-level behaviors. The FDIA could induce inconsistency between modified LMPs, congestion patterns, system loading levels, generation cost, etc. As in [51], an attack model only bypassing bad data detection could induce abnormal step changes in LMPs, which is an easy-to-detect signal for ISOs. More market-level defense strategies could be further developed to provide direct protection against market cyberattacks.

B. Vulnerability Analysis of the Market-Clearing Process in Terms of Profit-Oriented Cyberattacks

Although the market cyberattacks could come from various attack paths, the eventual targets are already known, which are the parameters of the market-clearing model. Therefore, a vulnerability analysis for the market-clearing process could evaluate the possibility of each parameter being attacked. Existing research works have been elaborating on a specific attack path. There is a lack of comprehensive analysis on which attack path produces the most profits (i.e., the most vulnerable attack path).

C. Modeling of Interactions between Multiple Attackers and Single/Multiple Defenders

Current research works only model the interactivity between a single defender and a single attacker. In reality, multiple entities could be preparing to gain illegal profits or protecting the system. Thus, a two-party zero-sum game fails to represent this complicated scenario. Attackers may also be cooperative or noncooperative with each other, but defenders are always cooperative with each other. However, equilibrium in this multiattacker setting is computationally hard. A tentative way is to separate the multiplayer game into multiple subgames because different attackers may target LMPs at different buses, which could make the game separable. Further, the interaction model becomes more realistic if the impact of unexpected contingency events is incorporated.

D. Profitability and Feasibility of the Proposed FDIA Strategies Under AC State Estimations

Most of the electricity market cybersecurity literature consider bypassing bad data detection in dc state estimation. However, the real system runs under ac state estimation. Research work [50] demonstrates that the residuals of FDIAs targeting the dc model increases quadratically with attack magnitude when applied in the ac model. A possible successful market attack in ac state estimation manipulates congestion, which only needs a small deviation to relieve congested lines. For example, a line at its limit of 200 MW is relieved to 199 MW. Thus, conceptually a reasonable FDIA for congestion manipulation always exists to pass bad data detection in ac state estimation if we keep reducing the modification amount. Therefore, a further investigation is the profitability jurisdiction if the attacks only relieve congestion. Further, it is more difficult to implement an FDIA in a large system because of high redundancy and complicate topology. Market FDIAs on large-scale test cases with full ac state estimation can be investigated for both profitability and feasibility.

E. Possibility and Profitability of Compromising Communication at Distribution-Levels

Most research works on cyberattacks at the distribution-level focus on sabotaging microgrid operations or renewable generation controls. Profitable attacks at distribution-levels are still under investigation. Similar to the wholesale market, distribution-level attacks also bring significant monetary gains. For example, distribution-level economic dispatch and distribution-level LMPs have been proposed to encourage distributed generations (DGs) [53]. Financial arbitrages could be given to particular DGs by compromising the communication between distribution system operators (DSOs) and DGs. It is worth noting that congestion rarely occurs at the distribution-level, and thus congestion manipulation may not be preferable. Some possible attack paths could be reactive power limits, dispatch signals from DSOs to distribution aggregators, and demand response programs.

VII. Conclusion

The evolving communication techniques strongly couple the cyber and physical electricity market operations. The cybersecurity of market operations is an indispensable part of smart grid developments.

This article provided a comprehensive and in-depth review and analysis of, and insights on profit-oriented electricity market cyberattacks. First, electricity market models were reviewed and the vulnerability was analyzed from a cybersecurity perspective.

Second, current works of literature on where attacks occur, how attacks avoid detection, how attackers gain profit, and the impacted of attacks in market operation were analyzed. Then the literature was summarized and categorized by research directions. Finally, a few potential future directions were also discussed.

Disclaimer

References

[1] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1630–1638, Jul. 2017.

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

[3] M. A. Rahman and G. K. Venayagamoorthy, "A survey on the effects of false data injection attack on energy market," in *Proc. Clemson Univ. Power Syst. Conf.*, 2018, pp. 1–6.

[4] F. Li, "Continuous locational marginal pricing (CLMP)," *IEEE Trans. Power Syst.*, vol. 22, no. 4, pp. 1638–1646, Nov. 2007.

[5] 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.

[6] 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, Mar. 2013.

[7] J. Ma, Y. Liu, L. Song, and Z. Han, "Multiact dynamic game strategy for jamming attack in electricity market," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2273–2282, Sep. 2015.

[8] Q. Wang, W. Tai, Y. Tang, M. Ni, and S. You, "A two-layer game theoretical attack-defense model for a false data injection attack against power systems," *Int. J. Elect. Power Energy Syst.*, vol. 104, pp. 169–177, Jan. 2019.

[9] Y. Xiang and L. Wang, "A game-theoretic study of load redistribution attack and defense in power systems," *Elect. Power Syst. Res.*, vol. 151, pp. 12–25, Oct. 2017.

[10] M. R. Mengis and A. Tajer, "Data injection attacks on electricity markets by limited adversaries: Worst-case robustness," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 5710–5720, Nov. 2020.

[11] A. Tajer, "False data injection attacks in electricity markets by limited adversaries: Stochastic robustness," *IEEE Trans. Smart Grid*, vol. 10, no. 1, pp. 128–138, Jan. 2019.

[12] S. Tan, W.-Z. Song, M. Stewart, J. Yang, and L. Tong, "Online data integrity attacks against real-time electrical market in smart grid," *IEEE Trans. Smart Grid*, vol. 9, no. 1, pp. 313–322, Jan. 2018.

[13] V. Kekatos, G. B. Giannakis, and R. Baldick, "Online energy price matrix factorization for power grid topology tracking," *IEEE Trans. Smart Grid*, vol. 7, no. 3, pp. 1239–1248, May 2016.

[14] 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.*, Apr. 2010, pp. 2468–2472.

[15] J.-W. Kang, I.-Y. Joo, and D.-H. Choi, "False data injection attacks on contingency analysis: Attack strategies and impact assessment," *IEEE Access*, vol. 6, pp. 8841–8851, 2018.

[16] R. Moslemi, A. Mesbahi, and J. M. Velni, "Design of robust profitable false data injection attacks in multi-settlement electricity markets," *IET Gener., Transmiss. Distrib.*, vol. 12, no. 6, pp. 1263–1270, Mar. 2018.

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

[18] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "A framework for cyber-topology attacks: Line-switching and new attack scenarios," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 3820–3829, Mar. 2017.

[19] G. Liang, S. R. Weller, F. Luo, J. Zhao, and Z. Y. Dong, "Generalized FDIA-based cyber topology attack with application to the Australian electricity market trading mechanism," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 3820–3829, Jul. 2017.

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

[21] K. Khanna, B. K. Panigrahi, and A. Joshi, "Bid modification attack in smart grid for monetary benefits," in *Proc. IEEE Int. Symp. Nanoelectron. Inf. Syst.*, 2016, pp. 224–229.

[22] 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.

[23] 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.

[24] C. Liu, M. Zhou, J. Wu, C. Long, and D. Kundur, "Financially motivated FDI on SCED in real-time electricity markets: Attacks and mitigation," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 1949–1959, Dec. 2017.

[25] H. S. Karimi, K. Jhala, and B. Natarajan, "Impact of real-time pricing attack on demand dynamics in smart distribution systems," in *Proc. North Amer. Power Symp.*, 2018, pp. 1–6.

[26] D. H. Choi and L. Xie, "Ramp-induced data attacks on look-ahead dispatch in real-time power markets," *IEEE Trans. Smart Grid*, vol. 4, no. 3, pp. 1235–1243, Sep. 2013.

[27] H. Ye, Y. Ge, X. Liu, and Z. Li, "Transmission line rating attack in two-settlement electricity markets," *IEEE Trans. Smart Grid*, vol. 7, no. 3, pp. 1346–1355, May 2016.

[28] J. Giraldo, A. Cárdenas, and N. Quijano, "Integrity attacks on real-time pricing in smart grids: Impact and countermeasures," in *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2249–2257, Sep. 2017.

[29] D.-H. Choi and L. Xie, "Impact of power system network topology errors on real-time locational marginal price," *J. Modern Power Syst. Clean Energy*, vol. 5, no. 5, pp. 797–809, Sep. 2017.

[30] L. Jia, J. Kim, R. J. Thomas, and L. Tong, "Impact of data quality on real-time locational marginal price," *IEEE Trans. Power Syst.*, vol. 29, no. 2, pp. 627–636, Mar. 2014.

[31] H. Xu, Y. Lin, X. Zhang, and F. Wang, "Power system parameter attack for financial profits in electricity markets," *IEEE Trans. Smart Grid*, vol. 11, no. 4, pp. 3438–3446, Jul. 2020.

[32] N. A. Ruhi, K. Dvijotham, N. Chen, and A. Wierman, "Opportunities for price manipulation by aggregators in electricity markets," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 5687–5698, Nov. 2018.

[33] 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 *Proc. 1st Workshop Secure Control Syst.*, Apr. 2010, pp. 18–26.

[34] R. Deng, G. Xiao, and R. Lu, "Defending against false data injection attacks on power system state estimation," *IEEE Trans. Ind. Informat.*, vol. 13, no. 1, pp. 198–207, Aug. 2015.

[35] 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.

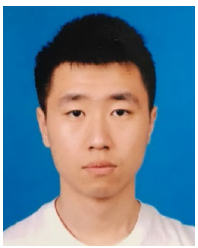
[36] T. T. Kim and H. V. Poor, "Strategic protection against data injection attacks on power grids," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 326–333, Jun. 2011.

[37] Y. Huang, J. Tang, Y. Cheng, H. Li, K. A. Campbell, and Z. Han, "Real-time detection of false data injection in smart grid networks: An adaptive CUSUM method and analysis," *IEEE Syst. J.*, vol. 10, no. 2, pp. 532–543, Jun. 2016.

[38] G. Chaojun, P. Jirutitijaroen, and M. Motani, "Detecting false data injection attacks in AC state estimation," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2476–2483, Sep. 2015.

[39] L. Liu, M. Esmalifalak, Q. Ding, V. A. Emesih, and Z. Han, "Detecting false data injection attacks on power grid by sparse optimization," *IEEE Trans. Smart Grid*, vol. 5, no. 2, pp. 612–621, Mar. 2014.

[40] 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.
[41] 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.
[42] O. Vukovic, 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.
[43] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, "A survey of IoT-enabled cyberattacks: Assessing attack paths to critical infrastructures and services," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3453–3495, Oct./Dec. 2018.
[44] R. Deng, G. Xiao, R. Lu, H. Liang, and A. V. Vasilakos, "False data injection on state estimation in power systems—Attacks, impacts, and defense: A survey," in *IEEE Trans. Ind. Informat.*, vol. 13, no. 2, pp. 411–423, Apr. 2017.
[45] Q. Wang *et al.*, "Review of the false data injection attack against the cyber-physical power system," *IET Cyber-Phys. Syst., Theory Appl.*, vol. 4, no. 2, pp. 101–107, 2019 .
[46] H. Jiang, K. Wang, Y. Wang, M. Gao, and Y. Zhang, "'Energy big data: A survey,"' *IEEE Access*, vol. 4, pp. 3844–3861, 2016.
[47] Q. Zhang, W. Feng, M. M. M. Kamel, B. Wang, and F. Li, "Extended LMP under high-penetration wind power," in *Proc. IEEE PES Trans. Distrib. Conf. Exhib. Latin Amer.*, 2018, pp. 1–6.
[48] F. Li, Y. Wei, and S. Adhikari, "Improving an unjustified common practice in ex post LMP calculation," *IEEE Trans. Power Syst.*, vol. 25, no. 2, pp. 1195–1197, May 2010.
[49] PJM Interconnection, "Virtual transactions in the PJM energy markets," 2015. [Online]. Available: http://www.pjm.com/media/documents/reports/20151012-virtual-bid-repor t.ashx
[50] J. Liang, O. Kosut, and L. Sankar, "Cyber attacks on AC state estimation: Unobservability and physical consequences," in *Proc. IEEE PES Gen. Meet. Conf. Expo.*, Jul. 2014, pp. 1–5.
[51] Q. Zhang, F. Li, H. Cui, R. Bo, and L. Ren, "Market-level defense against FDIA and a new LMP-disguising attack strategy in real-time market operations," *IEEE Trans. Power Syst.*, in-press, doi: 10.1109/TPWRS.2020.3020870.
[52] J. Schoene *et al.*, "Quantifying performance of distribution system state estimators in supporting advanced applications," *IEEE Open Access J. Power Energy*, vol. 7, pp. 151–162, 2020.
[53] F. Ding, Y. Zhang, J. Simpson, A. Bernstein, and S. Vadari, "Optimal energy dispatch of distributed PVs for the next generation of distribution management systems," *IEEE Open Access J. Power Energy*, vol. 7, pp. 287–295, 2020.



Qiwei Zhang (Student Member, IEEE) received the B.S. degree from North China Electrical Power University, Beijing, China, in 2016, and the M.S. degree in 2018 from The University of Tennessee Knoxville, Knoxville, TN, USA, where he is currently working towards the Ph.D. degree with the Department on Electrical Engineering and Computer Science, all in electrical engineering.

His research interest includes cyber security in power systems, power system optimization, and market operation.

Fangxing Li (Fellow, IEEE) received the B.S. and M.S. degrees in electrical engineering from Southeast University, Nanjing, China, in 1994 and 1997, respectively, and the Ph.D. degree in electrical and computer engineering from Virginia Tech, Blacksburg, VA, USA, in 2001.

He is currently the James W. McConnell Professor in electrical engineering and the Campus Director of CURENT with the University of Tennessee, Knoxville, TN, USA. His current research interests include renewable energy integration, demand response, distributed generation and microgrid, energy markets, and power system computing.

Prof. Li is currently serving as the Editor-In-Chief of IEEE OPEN ACCESS JOURNAL OF POWER AND ENERGY (OAJPE) and the Chair of IEEE/PES Power System Operation, Planning, and Economics (PSOPE) Committee.

Qingxin Shi (Member, IEEE) received the B.S. degree from Zhejiang University, Hangzhou, China, in 2011, and the M.Sc. degree from University of Alberta, Edmonton, AB, Canada, in 2014. He received the Ph.D. degree from University of Tennessee, Knoxville, TN, USA, in 2019, all in electrical engineering.

He is currently working as a Research Assistant Professor with University of Tennessee. His research interests include demand response and distribution system resilience.

Kevin Tomsovic (Fellow, IEEE) received the B.S. degree from Michigan Technological University, Houghton, MI, USA, in 1982, and the M.S. and Ph.D. degrees from the University of Washington, Seattle, WA, USA, in 1984 and 1987, respectively, all in electrical engineering.

He is currently CTI Professor with the Department of Electrical Engineering and Computer Science, University of Tennessee, Knoxville, TN, USA, and Director of the NSF/DOE ERC called CURENT. He was on the faculty of Washington State University from 1992 to 2008. He held the Advanced Technology for Electrical Energy Chair at Kumamoto University, Kumamoto, Japan, from 1999 to 2000, and was an NSF Program Director in the ECS division of the engineering directorate from 2004 to 2006.

Jinyuan Sun (Member, IEEE) received the B.Sc. degree in computer information systems from Beijing Information Science and Technology University, Beijing, China, in 2003, the M.A.Sc. degree in computer networks from Ryerson University, Toronto, ON, Canada, in 2005, and the Ph.D. degree in electrical and computer engineering from the University of Florida, Gainesville, FL, USA, in 2010.

She was a Network Test Developer with RuggedCom Inc., Concord, Canada, in 2005–2006. She was an Assistant Professor with the Department of Electrical Engineering and Computer Science, University of Tennessee, Knoxville, TN, USA, from 2010 to 2016, and has been an Associate Professor since 2016. Her research interests include security and privacy of cyber-physical systems, wireless networks, and mobile systems.

Dr. Sun is a member of the ACM.

Lingyu Ren (Member, IEEE) received the Ph.D. degree in electrical engineering from the University of Connecticut, Mansfield, CT, USA, in 2017.

She is currently a Senior Engineer at Raytheon Technologies Research Center, East Hartford, CT, USA. Her current research interest is in cybersecurity and big data analysis in smart grids.