This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2017.2733346, IEEE Transactions on Smart Grid

False Data Injection Attacks in Electricity Markets by Limited Adversaries: Stochastic Robustness

Ali Tajer, *Senior Member, IEEE*

***Abstract*—Deregulated electricity markets rely on a two-settlement system consisting of day-ahead and real-time markets, across which electricity price is generally volatile. In electricity markets, locational marginal pricing is widely adopted to set electricity prices and manage transmission congestion. Such locational marginal prices (LMPs) strongly hinge on the reliability and accuracy of the state estimation routines, which are designed to provide real-time information about the state of the power grid based on meter measurements. However, state estimation is vulnerable to false data injection attacks (FDIAs), which aim to compromise the readings of measurement meters in order to distort state estimates and, subsequently, mislead the computation of real-time LMPs, and thus carry out financial misconduct. Existing studies show that if the adversaries are *omniscient*, i.e., have *full* and *instantaneous* access to grid topology and state, they can design profitable attack strategies without being detected by the residue-based bad data detectors. This paper focuses on a more realistic FDIA setting, in which the attackers have only *partial* and *imperfect* information due to their limited resources and restricted physical access to the grid. Specifically, the attackers are assumed to have uncertainties about the state of the grid, and the uncertainties are modeled stochastically. Based on this model, this paper offers a framework for characterizing the optimal stochastic guarantees for the effectiveness of the attacks and the associated economic impacts. Designing such attacks is investigated analytically, and is examined in the standard IEEE 14-bus and 118-bus systems.**

***Index Terms*—Electricity market, false data injection attack, locational marginal pricing, stochastic robustness.**

I. Introduction

The power industry is undergoing evolutionary changes by integrating cyber assets with the physical infrastructure for generation, transmission, and distribution control [1, 2]. Compared with the unidirectional power transmission from central resources to vast customers in traditional power grids, modern grid designs involve dynamic bidirectional flows from distributed resources to deliver power, which can significantly enhance efficiency and reliability [3]. However, the increasing reliance on wide-area network results in the potential vulnerability of the power infrastructures to cyber-attacks by malicious adversaries [4].

System monitoring is instrumental to ensuring reliable operation of power grids, the purpose of which is to provide accurate and efficient estimates of power grid states based on meter measurements [5]. However, due to reasons such as unintended measurement abnormalities, grid topology variations, and malicious data attacks, the meter measurements can be distorted, which subsequently, affects the accuracy of state estimates. In particular, in false data injection attacks (FDIAs), as one important class of cyber attacks, an attacker can tamper with the readings of various meters, e.g., phasor measurement units (PMUs), in order to mislead the grid's decision-making process via, e.g., introducing errors into the state estimates [6].

Meanwhile, the electricity market is transitioning from a traditionally monopolized market to a competitive one enabling nation-wide deregulations. In most regions, the operations of the electricity market are monitored, controlled, and coordinated by entities usually referred to as system operators (SOs). Deregulated electricity markets consist of day-ahead (DA) and real-time (RT) markets. These markets are widely adopting the locational marginal pricing methodology (e.g., PJM) as the primary approach for determining electricity prices and managing transmission congestion [7]. In the DA markets, the locational marginal prices (LMPs) are determined based on the DC optimal power flow (DC-OPF) solutions, which are delineated by demand forecasts (which are different from the actual demand), generator capacity, and flow limits [8]. On the other hand, in RT markets the LMPs are computed by solving an incremental OPF based on the actual system operations in real time [7]. Both DA and RT LMPs are used in the final clearing and settlement processes. For determining the LMPs, especially in the RT market, the system state estimates are leveraged in order to characterize the real-time state of the grid [7, 9]. Hence, the accuracy of LMPs strongly hinges on the accuracy of state estimates. Based on this, an adversary can launch FDIAs to manipulate meter measurements, and thereby produce biased load estimates, which in turn leads to non-optimal dispatch and incorrect computation of RT LMPs. This can cause the electricity prices at certain locations in the RT market shift away from their optimal values computed in the DA market, and such price shifts can be leveraged by adversaries to carry out financial misconduct.

A. Previous Work

There exist a number of studies on the potential financial risks that the FDIAs impose on the electricity markets. Specifically, the impacts of the FDIAs on electricity markets through virtual bidding are studied in [10]. The study in [11] presents another FDIA strategy that investigates the generated market revenue for all optimal single attack. Based on the model of multistep electricity pricing (MEP) introduced in [12], the impacts of FDIAs against MEP are investigated in [13]. The study in [14] proposes an FDIA approach based on a geometric characterization of the RT LMPs. Game-theoretic frameworks for modeling the interactions between the attack and defense strategies are studied in [15] and

The Author is with the Department of Electrical, Computer, and Systems Engineering, Rensselaer Polytechnic Institute, Troy, NY.

This research was supported in part by the U. S. National Science Foundation CAREER Award ECCS-1554482.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2017.2733346, IEEE Transactions on Smart Grid

[16]. The effects of incomplete network information on load redistribution attacks and AC state estimates are studiesd in [17] and [18], respectively.

B. Contribution

The common assumption in the aforementioned studies on the FDIAs against electricity markets is that the attacker has *full* and *instantaneous* information about power grids, including its topology and state. In practice, however, grid information is extensive, secured, and temporally volatile, and the attackers can have only limited access to it [19]. This is primarily due to the attackers' lack of real-time information about various grid parameters and attributes, such as the position of circuit breaker switches and transformer tap changers, and also because of the attackers' limited physical access to most grid facilities. To bypass such intractable issues, the most recent work in [20] proposes an online attack strategy by leveraging only the real-time data streams of meter measurements without knowing network topology and branch parameters. Nevertheless, a more realistic FDIA against real-time electricity market is one with *incomplete information*. While there are some efforts to study FDIAs by limited adversaries with incomplete knowledge about power grids against smart grid [19], the impacts of such realistic attack against real-time electricity markets are not studied. In this paper, we study the impacts of the FDIAs on the electricity markets, where the attackers have access to only partial information about the state of the grid.

Specifically, we consider an adversarial setting in which the attackers' knowledge of the state of the grid bears uncertainties. In particular, we assume that the attackers know the parameters characterizing the grid with uncertainty, and adopt a stochastic model to capture such parameter uncertainties. Based on such an uncertainty model, we design an optimal profitable and undetectable attack strategy, which can be formulated as the solution to a chance-constrained optimization problem. We show that the proposed formulation is non-convex and intractable, and provide an efficient convex conservative formulation that guarantees sustaining the constraints of the stochastically optimal design. Simulation results in the IEEE 14-bus and 118-bus systems are also provided to assess the robustness of the proposed attack approach.

C. Assumptions

The analytical statements made in this paper are valid for the following set of assumptions.

- Least squares state estimators and residue-based bad data detectors (BDDs) are used for system state recovery.
- Network model is known to the attacker imperfectly, and the attacker's uncertainty is assumed to follow a Gaussian model.
- The attacker performs virtual bidding, and uses false data injection to manipulate the prices in the electricity market.
- The probability that the attackers bypass the bad data detector is controlled to exceed a pre-specified threshold.
- The probability that the designed attacks can gain profit is controlled to exceed pre-specified thresholds.

II. System Model

A. Monitoring Model

Consider a lossless power transmission network including M generators and J loads connected by L transmission lines. We define $\boldsymbol{p} \triangleq [p_1, \ldots, p_M]^T$ as the power generation vector, where p_m denotes the power injected by generator $m \in \{1, \ldots, M\}$, $\boldsymbol{\ell} \triangleq [\ell_1, \ldots, \ell_J]^T$ as the load vector, where ℓ_j denotes the load power consumed at load bus $j \in \{1, \ldots, J\}$, and $\boldsymbol{f} \triangleq [f_1, \ldots, f_L]^T$ as the power flow vector where f_l denotes the power flow at transmission line $l \in \{1, \ldots, L\}$. Accordingly, we define the state vector $\boldsymbol{x}$ as the nodal injections combining the load vector $\boldsymbol{\ell}$ and the power generation vector $\boldsymbol{p}$, i.e.,

$$\boldsymbol{x} \triangleq [x_1, \ldots, x_N]^T = [\boldsymbol{\ell}^T \ , \ \boldsymbol{p}^T]^T, \tag{1}$$

where $N \triangleq J + M$ and x_n denotes the net power injection at bus $n \in \{1, \ldots, N\}$. In the real-time market, computing the LMPs often leverages the DC power flow model, based on which, the line flows vector $\boldsymbol{f}$ is related to the nodal injection vector $\boldsymbol{x}$ according to

$$\boldsymbol{f} = \boldsymbol{H}\boldsymbol{x} \ , \tag{2}$$

where $\boldsymbol{H} \in \mathbb{R}^{L \times N}$ is the distribution factor matrix [21]. By defining $K \triangleq J + M + L$, we denote the vector of measurements collected throughout the network by $\boldsymbol{z}$, which contains K measurements corresponding to M generation, J load, and L power flow values. These measurements are related to the nodal injection vector $\boldsymbol{x}$ via

$$\boldsymbol{z} = \boldsymbol{H}_s\boldsymbol{x} + \boldsymbol{w} \ , \tag{3}$$

where we have defined

$$\boldsymbol{H}_s \triangleq [\boldsymbol{I}_N \quad \boldsymbol{H}^T]^T \ , \tag{4}$$

in which $\boldsymbol{H}_s \in \mathbb{R}^{K \times L}$, and $\boldsymbol{w}$ accounts for the Gaussian measurement noise with zero mean and covariance matrix $\boldsymbol{\Sigma_w}$. Given measurements $\boldsymbol{z}$, the weighted least squares estimate of $\boldsymbol{x}$ is given by [6]:

$$\hat{\boldsymbol{x}} = \boldsymbol{W}\boldsymbol{z} \ , \ \text{ where } \ \boldsymbol{W} \triangleq (\boldsymbol{H}_s^T\boldsymbol{\Sigma_w^{-1}}\boldsymbol{H}_s)^{-1}\boldsymbol{H}_s^T\boldsymbol{\Sigma_w^{-1}} \ . \tag{5}$$

We also adopt the widely-used residue test for bad data detection to detect the anomalies in the measurements. The residue is defined as

$$\boldsymbol{r} \triangleq \boldsymbol{z} - \boldsymbol{H}_s\hat{\boldsymbol{x}} \overset{(5)}{=} (\boldsymbol{I} - \boldsymbol{H}_s\boldsymbol{W})\boldsymbol{z} = (\boldsymbol{I} - \boldsymbol{Q})\boldsymbol{z} \ , \tag{6}$$

where we have defined $\boldsymbol{Q} \triangleq \boldsymbol{H}_s\boldsymbol{W}$. Anomalies are deemed to exist when the ℓ_2-norm $\|\boldsymbol{r}\|_2$ exceeds a pre-specified threshold, i.e.,

$$\|\boldsymbol{r}\|_2 = \|(\boldsymbol{I} - \boldsymbol{Q})\boldsymbol{z}\|_2 > \tau \ . \tag{7}$$

The value of τ is selected such that the rate of the false alarms is controlled below a desired level [22].

B. Attack Model

Assume that an adversary aims to launch an attack by compromising measurements for the ultimate goal of carrying

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2017.2733346, IEEE Transactions on Smart Grid

out financial misconduct in the electricity market. We define $\boldsymbol{z}'$ as the tampered measurements given by

$$\boldsymbol{z}' \triangleq \boldsymbol{z} + \boldsymbol{z}_a \ , \tag{8}$$

where $\boldsymbol{z}_a$ represents the FDIA vector. Based on (5), the compromised state estimate $\hat{\boldsymbol{x}}'$ based on tampered measurements $\boldsymbol{z}'$ is

$$\hat{\boldsymbol{x}}' \overset{(5)}{=} \boldsymbol{W}\boldsymbol{z}' = \hat{\boldsymbol{x}} + \boldsymbol{W}\boldsymbol{z}_a \ . \tag{9}$$

Accordingly, the residue value defined in (6) becomes

$$\boldsymbol{r}' \overset{(6)}{=} \boldsymbol{r} + \boldsymbol{r}_a \ , \tag{10}$$

where we have defined $\boldsymbol{r}_a \triangleq (\boldsymbol{I} - \boldsymbol{Q})\boldsymbol{z}_a$. When the adversary has *perfect* information about grid dynamics and faces no limitation accessing to all the sensors, it can select the injected attack vector $\boldsymbol{z}_a$ to be perfectly aligned in the null space of $(\boldsymbol{I} - \boldsymbol{Q})$. This leads to $(\boldsymbol{I} - \boldsymbol{Q})\boldsymbol{z}_a = \boldsymbol{0}$, in which case the residue test cannot detect the attack. Hence with perfect information an attacker can accurately construct matrix $\boldsymbol{Q}$, design an FDIA that is undetectable by the BDD, and thus incur arbitrary error to the state estimate $\hat{\boldsymbol{x}}$. However, when the attacker lacks perfect information, perfect alignment is infeasible. In such circumstances, in order to maintain a high probability of being undetectable, the attacker must keep the ℓ_2-norm of $\boldsymbol{r}_a$ small, and below some threshold ε, i.e.,

$$\|\boldsymbol{r}_a\|_2 \leq \varepsilon \ . \tag{11}$$

Controlling ε balances a tradeoff between the detectability and effectiveness of $\boldsymbol{z}_a$. Increasing ε, on the one hand, allows for a broader choices of $\boldsymbol{z}_a$ and increases the chance of more effective attacks, and on the other hand, makes the attacks more likely to be detected.

C. Limited Adversary

In reality, the grid information is too extensive, secured, and temporally volatile to be completely accessible by the attackers. Therefore, such all-encompassing knowledge of the grid information is unrealistic. In this paper, we assume that there exists a mismatch between the actual grid dynamic model and the one presumed by the attacker. More specifically, the actual model is embedded in $\boldsymbol{Q} = \boldsymbol{H}_s\boldsymbol{W}$, and the attacker's estimate of $\boldsymbol{Q}$ is denoted by $\tilde{\boldsymbol{Q}}$. Furthermore, we define $\Delta\boldsymbol{Q} \triangleq (\boldsymbol{Q} - \tilde{\boldsymbol{Q}})$ as an error matrix describing the attacker's grid dynamic uncertainty. In this uncertainty model, we assume that the elements of $\Delta\boldsymbol{Q}$ are independent (but not necessarily identical) Gaussian random variables with zero mean and possibly different variance values, i.e.

$$\Delta Q_{ij} \sim \mathcal{N}(0, \sigma_{ij}^2), \ \forall i, j \in \{1, \ldots, N\} \ . \tag{12}$$

Hence, the actual matrix $\boldsymbol{Q}$, which is unknown to the attacker, belongs to the set

$$\mathcal{A} \triangleq \{\boldsymbol{Q} \mid \boldsymbol{Q} = \tilde{\boldsymbol{Q}} + \Delta\boldsymbol{Q} : \Delta Q_{ij} \sim \mathcal{N}(0, \sigma_{ij}^2)\} \ , \tag{13}$$

and the random error matrix $\Delta\boldsymbol{Q}$ belongs to the set

$$\mathcal{B} \triangleq \{\Delta\boldsymbol{Q} \mid \Delta Q_{ij} \sim \mathcal{N}(0, \sigma_{ij}^2)\} \ . \tag{14}$$

For the simplicity in notations, throughout the analysis we assume that all the variance values are equal, i.e., for all $i, j \in \{1, \ldots, N\}$ we have $\sigma_{ij} = \sigma$, and we provide remarks on generalizing the results to the case of non-identical variance values.

Due to such uncertainties, an attacker cannot guarantee that the attack vector $\boldsymbol{z}_a$ is aligned in the null space of $(\boldsymbol{I} - \boldsymbol{Q})$, since $\boldsymbol{Q}$ is unknown. Consequently, there is no guarantee that the attack can pass the residue detection test (7). Furthermore, due to the stochastic errors associated with $\boldsymbol{Q}$, the attacker faces uncertainties about the effectiveness of the attack since random uncertainties about $\boldsymbol{Q}$ lead to random disruptions in state estimates. Hence, the attacker's strategy should change such that instead of ensuring that it remains undetectable, it aims to design $\boldsymbol{z}_a$ such that the likelihood that it is detected is minimized. Thus, from the attacker's perspective, it is desirable to design an attack strategy that violates the detectability constraint in (11) with minimal probability. Motivated by this, we define the stochastic (ε, η)-robust attack as follows.

Definition 1: An attack vector $\boldsymbol{z}_a$ is called (ε, η)-robust if it satisfies

$$\mathbb{P}\left\{\|(\boldsymbol{I} - \boldsymbol{Q})\boldsymbol{z}_a\|_2 \ \leq \ \varepsilon\right\} \geq \eta, \quad \forall \boldsymbol{Q} \in \mathcal{A} \ , \tag{15}$$

where $\eta \in (0, 1)$ denotes the likelihood that the attack vector $\boldsymbol{z}_a$ remains undetectable.

D. Electricity Markets

In order to establish the impact of the attacks on the electricity market, next we discuss the pricing mechanisms, and present the pricing models adopted in DA and RT markets, which rely on the DC-OPF analysis. In these models, locational marginal pricing is adopted to set the nodal electricity prices.

1) DA Market: In the DA market, the SOs perform optimal dispatch calculations to minimize the aggregate cost given the dispatchable load forecast, the energy balance constraint, power dispatch constraints, and transmission line constraints. In order to formalize the connection between the DC-OPF and LMPs, we define $C_m(p_m)$ as the cost associated with generator $m \in \{1, \ldots, M\}$ when its output power is p_m. Accordingly, we define

$$\boldsymbol{C}(\boldsymbol{p}) \triangleq [C_1(p_1), \ldots, C_M(p_M)]^T \ . \tag{16}$$

By defining $\boldsymbol{1}_d$ as the $1 \times d$ vector of all ones, the optimal dispatch, denoted by $\boldsymbol{p}^*$ is the solution to:

$$\begin{aligned} \min_{\boldsymbol{p}^*} \quad & \boldsymbol{1}_M \cdot \boldsymbol{C}(\boldsymbol{p}) \\ \text{s.t.} \quad & \boldsymbol{1}_M \cdot \boldsymbol{p} = \boldsymbol{1}_J \cdot \boldsymbol{\ell} \\ & p_m^{\min} \leq p_m \leq p_m^{\max}, \ \forall m \in \{1, \ldots, M\} \\ & f_l^{\min} \leq f_l \leq f_l^{\max}, \ \forall l \in \{1, \ldots, L\} \end{aligned} \ , \tag{17}$$

where $p_m^{\min}$ and $p_m^{\max}$ denote the minimum and maximum generation limits for generator $m \in \{1, \ldots, M\}$, respectively, and $f_l^{\min}$ and $f_l^{\max}$ denote the minimum and maximum flow limits for transmission line $l \in \{1, \ldots, L\}$, respectively.

2) RT Market: In the RT market, due to the variations in the actual load or generation, the SOs update dispatch $\boldsymbol{p}^*$ via performing incremental dispatch calculation to achieve real-time

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2017.2733346, IEEE Transactions on Smart Grid

optimal system operation. Such updates leverage estimates $\hat{\boldsymbol{x}}$ and $\hat{p}_m$ as the power generated at bus $m \in \{1,\dots,M\}$, $\hat{\ell}_j$ as the load of bus $j \in \{1,\dots,J\}$, and $\hat{f}_l$ as the transmission flow at line $l \in \{1,\dots,L\}$. By defining Δp_m as the change in the power output by generator $m \in \{1,\dots,M\}$, $\Delta \ell_j$ as the change in the load at bus $j \in \{1,\dots,J\}$, and Δf_l as the change in transmission flow $l \in \{1,\dots,L\}$, and accordingly defining the power vector

$$\Delta \boldsymbol{p} \triangleq [\Delta p_1, \dots, \Delta p_M]^T, \tag{18}$$

the optimal incremental dispatch is the solution to:

$$\begin{aligned} \min_{\Delta \boldsymbol{p}} \quad & \mathbf{1}_M \cdot \boldsymbol{C}(\hat{\boldsymbol{p}} + \Delta \boldsymbol{p}) \\ \text{s.t.} \quad & \mathbf{1}_M \cdot \Delta \boldsymbol{p} = \mathbf{1}_J \cdot \Delta \boldsymbol{\ell} \\ & \Delta p_m^{\min} \le \Delta p_m \le \Delta p_m^{\max}, \quad \forall m \in \{1,\dots,M\} \\ & \Delta f_l \le 0, \qquad\qquad \forall l \in \Omega_+ \\ & \Delta f_l \ge 0, \qquad\qquad \forall l \in \Omega_- \end{aligned} \quad , \tag{19}$$

where $\Delta p_m^{\max}$ and $\Delta p_m^{\min}$ are upper and lower limits of the change in power generated at bus $m \in \{1,\dots,M\}$, and Ω_+ and Ω_- are the sets of estimated congested lines on which the estimated flows are equal to or outside the flow limits. Specifically, Ω_+ is defined as the positive congestion set

$$\Omega_+ \triangleq \{l \in \{1,\dots,L\} \mid \hat{f}_l \ge f_l^{\max}\} , \tag{20}$$

and Ω_- is defined as the negative congestion set

$$\Omega_- \triangleq \{l \in \{1,\dots,L\} \mid \hat{f}_l \le f_l^{\min}\} , \tag{21}$$

and Ω_0 is defined as the non-congestion set

$$\Omega_0 \triangleq \{l \in \{1,\dots,L\} \mid f_l^{\min} < \hat{f}_l < f_l^{\max}\} . \tag{22}$$

Finally, following the discussions in [16], [21], and [23], corresponding to each load bus $j \in \{1,\dots,J\}$ we define an LMP denoted by ζ_j. By defining ζ_{ref} as the LMP of a reference load bus (the system price), we have

$$\zeta_j = \zeta_{\text{ref}} + \boldsymbol{H}_j^T \cdot \boldsymbol{\pi} , \tag{23}$$

where $\boldsymbol{H}_j \in \mathbb{R}^{L\times 1}$ represents the j^{th} column of $\boldsymbol{H}$ defined in (2) and $\boldsymbol{\pi} \triangleq [\pi_1,\dots,\pi_L]^T$ is defined such that π_l is the *shadow price* corresponding to line l, which depends on the congestion condition of the corresponding power flow [10], and it satisfies

$$\begin{cases} \pi_l \ge 0, & \text{if } l \in \Omega_+ \\ \pi_l \le 0, & \text{if } l \in \Omega_- \\ \pi_l = 0, & \text{if } l \in \Omega_0 \end{cases} . \tag{24}$$

Based on (23), the LMP difference between two load buses i and j is given by

$$\zeta_i - \zeta_j = (\boldsymbol{H}_i - \boldsymbol{H}_j)^T \cdot \boldsymbol{\pi} . \tag{25}$$

E. Profit Model

Based on the LMP model given in Section II-D, next we formalize the attacker's profit model. In order to increase competition and liquidity in the electricity market, many SOs (e.g., ISO-New England) allow for virtual bidding in the electricity markets [24]. Virtual-bidding entities are participants in the market with no affiliated generation or load. The attackers are interested in making profit in the electricity market by designing an FDIA vector $\boldsymbol{z}_a$ that creates a certain discrepancy between the LMPs in the DA and RT markets. Specifically, facilitated by virtual bidding, in the DA market the attacker purchases and sells a certain amount of virtual power P at load buses j and i with price ζ_j^{DA} and ζ_i^{DA}, respectively, and then in the RT market, it sells and purchases the same amount of virtual power at the same buses with price ζ_j^{RT} and ζ_i^{RT}, respectively. Hence the profit based on such virtual bidding mechanism can be expressed by

$$\begin{aligned} g(\boldsymbol{z}') &= (\zeta_j^{\text{RT}} - \zeta_i^{\text{RT}} + \zeta_i^{\text{DA}} - \zeta_j^{\text{DA}}) \cdot P \\ &\overset{(23)}{=} P \cdot \sum_{l\in\mathcal{L}_+} (H_{l,j} - H_{l,i}) \cdot \pi_l \\ &\quad + P \cdot \sum_{l\in\mathcal{L}_-} (H_{l,j} - H_{l,i}) \cdot \pi_l + P(\zeta_i^{\text{DA}} - \zeta_j^{\text{DA}}) . \end{aligned} \tag{26}$$

As shown in [21], the following three conditions suffice to ensure that profit $g(\boldsymbol{z}')$ is positive:

1) $\zeta_i^{\text{DA}} - \zeta_j^{\text{DA}} \ge 0$;
2) $\forall l \in \mathcal{L}_+$ we have $\hat{f}_l' \ge f_l^{\min}$, i.e., $l \notin \Omega_-$;
3) $\forall l \in \mathcal{L}_-$ we have $\hat{f}_l' \le f_l^{\max}$, i.e., $l \notin \Omega_+$;

where we have defined

$$\mathcal{L}_+ \triangleq \{l \in \{1,\cdots,L\} :\ H_{l,j} > H_{l,i}\} , \tag{27}$$

$$\text{and} \quad \mathcal{L}_- \triangleq \{l \in \{1,\cdots,L\} :\ H_{l,j} < H_{l,i}\} , \tag{28}$$

and $\hat{f}_l'$ denotes the compromised estimate of f_l. The first condition can be easily satisfied in the DA market by properly selecting locations i and j. However, since from the attacker's point of view, $\hat{f}_l'$ can be regarded as a Gaussian random variable with mean $\mathbb{E}[\hat{f}_l']$, it cannot guarantee that the other two conditions are always satisfied. Nevertheless, it can design the attack vector $\boldsymbol{z}_a$ such that the likelihood that these two conditions are satisfied is maximized. Motivated by this, we introduce δ as the *profit confidence* to represent the minimum safety distance between $\mathbb{E}[\hat{f}_l']$ and line constraints $f_l^{\max}$ and $f_l^{\min}$ for the lines in $\mathcal{L}_+$ and $\mathcal{L}_-$, respectively. Hence, we define the *profit-confidence* constraints:

$$\begin{aligned} \mathbb{E}[\hat{f}_l'] &\le f_l^{\max} - \delta, \ \forall\, l \in \mathcal{L}_- \\ \mathbb{E}[\hat{f}_l'] &\ge f_l^{\min} + \delta, \ \forall\, l \in \mathcal{L}_+ \end{aligned} , \tag{29}$$

where we have

$$\mathbb{E}[\hat{f}'] = f_l^* + \boldsymbol{e}_l^T \boldsymbol{H}\boldsymbol{W}\boldsymbol{z}_a , \tag{30}$$

in which f_l^* denotes the optimal power flow of line l in the DA market, and $\boldsymbol{e}_l \in \mathbb{R}^{L\times 1}$ is a standard unit column vector with 1 at row l.

Remark 1: The value of δ on each line ℓ measures the distance between the power flow f_ℓ and its associated constraint, which depending on whether ℓ belongs to the set $\mathcal{L}+$ or the set $\mathcal{L}_-$, the constraint involves the minimum power flow limit ($f_\ell^{\min}$) or the maximum power flow limit ($f_\ell^{\max}$), respectively. The physical significance of δ is that it captures

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2017.2733346, IEEE Transactions on Smart Grid

how much room the attacker has for shifting the estimates of the power flows such that false estimates still remain within the valid limits (as otherwise they will be easily detectable by the system operator).

Based on (4), it can be readily shown that

$$\boldsymbol{H} = [\mathbf{0}_{L\times N} \quad \boldsymbol{I}_L]\boldsymbol{H}_s. \tag{31}$$

Hence, by recalling $\boldsymbol{Q} = \boldsymbol{H}_s\boldsymbol{W}$, (30) can be reformulated as

$$\mathbb{E}[\hat{f}_l'] = f_l^* + \boldsymbol{q}_l\boldsymbol{z}_a \ , \tag{32}$$

where we have defined $\boldsymbol{q}_l$ as the l^{th} row of $[\mathbf{0} \quad \boldsymbol{I}]\boldsymbol{Q}$, i.e., $\boldsymbol{q}_l \triangleq \boldsymbol{e}_l^T[\mathbf{0} \quad \boldsymbol{I}]\boldsymbol{Q}$. Based on the constraints in (29) and the identity in (32), we define the stochastic δ-profitable attacks as follows.

Definition 2: An attack $\boldsymbol{z}_a$ is δ-profitable with tolerance parameters $\eta_{\max}$ and $\eta_{\min}$ if for $\forall \boldsymbol{Q} \in \mathcal{A}$ the following two conditions are satisfied.

$$\begin{aligned} &\mathbb{P}\{f_l^* + \boldsymbol{q}_l\boldsymbol{z}_a \ \le \ f_l^{\max} - \delta\} \geq \eta_{\max}, \ \forall l \in \mathcal{L}_- \\ &\mathbb{P}\{f_l^* + \boldsymbol{q}_l\boldsymbol{z}_a \ \ge \ f_l^{\min} + \delta\} \geq \eta_{\min}, \ \forall l \in \mathcal{L}_+ \end{aligned} \ , \tag{33}$$

where $\eta_{\max}$, $\eta_{\min} \in (0,1)$, denote the minimum probabilities that profit confidence constraints in (29) are satisfied.

III. Robust Attack Formulation

Based on the notations and definitions provided in Section II, the attacker's objective is to design the attack vector $\boldsymbol{z}_a$, such that the profit confidence δ is maximized, while the (ε,η)-robustness constraint defined in (15) and the profit constraints in (33) are satisfied. Hence, designing the attack strategy can be found as the solution to the following chance-constrained problem:

$$\begin{aligned} \max_{\boldsymbol{z}_a\in\mathcal{S}} \quad & \delta \\ \text{s.t.} \quad & \mathbb{P}\{\|(\boldsymbol{I}-\boldsymbol{Q})\boldsymbol{z}_a\|_2 \ \le \ \varepsilon\} \ \ge \ \eta \\ & \mathbb{P}\{f_l^* + \boldsymbol{q}_l\boldsymbol{z}_a \ \le \ f_l^{\max} - \delta\} \ \ge \ \eta_{\max}, \ \forall l \in \mathcal{L}_-, \\ & \mathbb{P}\{f_l^* + \boldsymbol{q}_l\boldsymbol{z}_a \ \ge \ f_l^{\min} + \delta\} \ \ge \ \eta_{\min}, \ \forall l \in \mathcal{L}_+ \\ & \delta \ > \ 0 \end{aligned} \tag{34}$$

where $\mathcal{S}$ represents the attack vector space, which is the attack pattern including the type and number of compromised sensors. The stochastic (ε,η)-robust and δ-profitable constraints are stochastic, and are non-convex, which make the problem intractable in general. In the next section, we provide a conservative approximation of this problem, which yields a design for $\boldsymbol{z}_a$ that ensures satisfying all the constraints of (34), and results in a profit confidence value δ that is a provable lower bound for the optimal δ. We show that this conservative approximation of (34) is a convex problem that can be solved efficiently.

IV. Robust Attack under Stochastic Uncertainty

Solving (34) involves satisfying stochastic constraints. In this section we provide non-stochastic alternatives to these constraints, which serve as conservative approximations for them, and show that problem in (34) can be solved conservatively through a deterministic semi-definite programming (SDP) optimization problem.

A. (ε,η)-Robust Constraints

We first convert the semi-infinite non-convex stochastic (ε,η)-robust constraint given in (15) to a deterministic one by leveraging a Bernstein-type inequality [25]. By recalling the expansion $\boldsymbol{Q} = \tilde{\boldsymbol{Q}} + \Delta\boldsymbol{Q}$, and defining $\boldsymbol{v} \triangleq \Delta\boldsymbol{Q}\cdot\boldsymbol{z}_a$, (15) can be equivalently stated as

$$\mathbb{P}\left\{\|(\boldsymbol{I}-\tilde{\boldsymbol{Q}})\boldsymbol{z}_a - \boldsymbol{v}\|_2^2 \leq \varepsilon^2\right\} \geq \eta, \quad \forall \boldsymbol{Q} \in \mathcal{A} \ . \tag{35}$$

It can be readily verified that $\boldsymbol{v}$ is distributed according to

$$\boldsymbol{v} \ \sim \ \mathcal{N}(\mathbf{0}, \boldsymbol{R}) \ , \quad \text{where} \quad \boldsymbol{R} \triangleq \sigma^2\|\boldsymbol{z}_a\|^2\cdot\boldsymbol{I}_K. \tag{36}$$

Furthermore, for the vector $\boldsymbol{u}$ defined as $\boldsymbol{u} \triangleq \boldsymbol{R}^{-\frac{1}{2}}\boldsymbol{v}$ we have

$$\boldsymbol{u} \sim \mathcal{N}(\mathbf{0}, \boldsymbol{I}_K) \ . \tag{37}$$

Remark 2: We remark that when the variance values $\{\sigma_{ij}\}$ defined in (12) are not identical, the covariance matrix $\boldsymbol{R}$ will take a slightly different from such that it depends on all $\{\sigma_{ij}\}$. Nevertheless, given $\boldsymbol{R}$, the rest of the analyses follows similar footsteps, albeit with proper adjustments.

By expanding (35), it can be equivalently stated that $\forall \boldsymbol{Q} \in \mathcal{A}$

$$\mathbb{P}\left\{\boldsymbol{u}^T\boldsymbol{R}\boldsymbol{u} + 2\boldsymbol{u}^T\boldsymbol{R}^{\frac{1}{2}}(\tilde{\boldsymbol{Q}}-\boldsymbol{I})\boldsymbol{z}_a \leq \varepsilon^2 - \|(\tilde{\boldsymbol{Q}}-\boldsymbol{I})\boldsymbol{z}_a\|_2^2\right\} \geq \eta \ . \tag{38}$$

Note that (38) is a stochastic inequality involving quadratic form of Gaussian random variables. In the following lemma, we provide an inequality that facilitates converting the stochastic constraint in (38) to a deterministic one.

Lemma 1: ([25]) Let $\boldsymbol{T} \triangleq \boldsymbol{u}^T\boldsymbol{G}\boldsymbol{u} + 2\boldsymbol{u}^T\boldsymbol{r}$, where $\boldsymbol{u} \sim \mathcal{N}(\mathbf{0}, \boldsymbol{I}_K)$, $\boldsymbol{r} \in \mathbb{R}^{K\times 1}$, and $\boldsymbol{G} \in \mathbb{S}^K$ is a real symmetric matrix. Then, for any $\beta > 0$, we have

$$\mathbb{P}\{T \leq \Psi(\beta)\} \geq 1 - e^{-\beta} \ , \tag{39}$$

where $\Psi : \mathbb{R}_+ \to \mathbb{R}$ is defined as

$$\Psi(\beta) \triangleq \text{tr}(\boldsymbol{G}) + 2\sqrt{\beta}\cdot\sqrt{\|\boldsymbol{G}\|_F^2 + 2\|\boldsymbol{r}\|_2^2} + 2\beta\lambda_{\boldsymbol{G}}^+ \ , \tag{40}$$

and we have defined $\lambda_{\boldsymbol{G}}^+ \triangleq \max\{\lambda_{\max}(\boldsymbol{G}), 0\}$ in which $\lambda_{\max}(\boldsymbol{G})$ denotes the maximum eigenvalue of matrix $\boldsymbol{G}$, $\text{tr}(\boldsymbol{G})$ denotes the trace of $\boldsymbol{G}$, and $\|\cdot\|_F$ denotes the Frobenius norm.

The inequality in (39) provides a bound on the probability that the quadratic form of a Gaussian random vector deviates from its mean $\text{tr}(\boldsymbol{G})$. Next, we provide a deterministic constraint, and prove that satisfying such a deterministic constraint is sufficient to guarantee that (38) is also satisfied. The following theorem is instrumental to characterizing the desired deterministic constraint.

Theorem 1 ((ε,β)-robustness constraints): Decompose the matrix $\boldsymbol{I} + \boldsymbol{S}^T\boldsymbol{S} \in \mathbb{R}^{K\times K}$, where $\boldsymbol{S} \triangleq \sqrt{\frac{2}{K\sigma}}(\tilde{\boldsymbol{Q}}-\boldsymbol{I})$, into its triangular Cholesky factors, i.e.,

$$\boldsymbol{I} + \boldsymbol{S}^T\boldsymbol{S} = \boldsymbol{L}^T\boldsymbol{L} \ . \tag{41}$$

Given $\boldsymbol{L}$, for an attack vector with $\boldsymbol{z}_a$ and for any $\beta > 0$, the stochastic (ε,η)-robust constraint in (35) is satisfied if

$$\Psi(\beta) \leq \varepsilon^2 - \|(\tilde{\boldsymbol{Q}}-\boldsymbol{I})\boldsymbol{z}_a\|_2^2 \ , \tag{42}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2017.2733346, IEEE Transactions on Smart Grid

TABLE I: Attack description

congestion	congested line(s) in DA market	virtual bidding nodes	compromised sensors
1 line	4	② and ④	4 and ② and ④
2 lines	4 and 6	② and ③ and ④	4 and 6 and ② and ③ and ④
3 lines	4 and 6 and 7	② and ③ and ④ and ⑤	4 and 6 and 7 and ② and ③ and ④ and ⑤

where $\Psi : \mathbb{R}_+ \to \mathbb{R}$ is defined as

$$\Psi(\beta) = \sigma^2\rho^2(K + 2\beta) + 2\sigma^2\sqrt{\beta K}\rho\|\boldsymbol{L}\boldsymbol{z}_a\|_2 \ , \qquad (43)$$

and $\rho \triangleq \|\boldsymbol{z}_a\|_2^2$.

Proof: See Appendix A. ■

Clearly, the constraint in (42) is a deterministic one, and according to Theorem 1, satisfying this deterministic constraint suffices ensuring the stochastic (ε, η)-robustness constraints.

B. δ-profitable Constraints

In this subsection, we show that the stochastic δ-profitable constraints in (33) can be converted into deterministic second-order cone (SOC) constraints.

Theorem 2 (δ-profitable constraints): The stochastic δ-profitable constraints in (33) can be equivalently expressed as the following deterministic constraints:

$$\begin{aligned} &f_l^* + \tilde{\boldsymbol{q}}_l\boldsymbol{z}_a + \sigma\|\boldsymbol{z}_a\|_2\phi^{-1}(\eta_{\max}) \le f_l^{\max} - \delta, \ \forall l \in \mathcal{L}_- \\ &f_l^* + \tilde{\boldsymbol{q}}_l\boldsymbol{z}_a + \sigma\|\boldsymbol{z}_a\|_2\phi^{-1}(1-\eta_{\min}) \ge f_l^{\min} + \delta, \ \forall l \in \mathcal{L}_+ \end{aligned} \ , \qquad (44)$$

where we have defined $\tilde{\boldsymbol{q}}_l \triangleq \boldsymbol{e}_l^T[\boldsymbol{0} \quad \boldsymbol{I}]\tilde{\boldsymbol{Q}}$, $\phi(\cdot)$ is the inverse of the cumulative probability distribution of the standard Gaussian random variable, and $\eta_{\min}$ and $\eta_{\max}$ satisfy $\eta_{\max} \ge \frac{1}{2}$ and $\eta_{\min} \ge \frac{1}{2}$.

Proof: See Appendix B. ■

Clearly, the constraints in (44) are deterministic SOC constraints, and according to Theorem 2, satisfying these deterministic SOC constraints suffices to satisfy the stochastic δ-profitable constraints in (33).

C. Conservative Robust Attack Formulation

By leveraging Theorem 1 and Theorem 2, the intractable chance-constrained non-convex problem (34) can be conservatively approximated by a deterministically-constrained convex problem as follows.

$$\begin{aligned} \max_{\boldsymbol{z}_a \in \mathcal{S}} \quad & \delta \\ \text{s.t.} \quad & \Upsilon(\beta) \le \varepsilon^2 - \|(\tilde{\boldsymbol{Q}} - \boldsymbol{I})\boldsymbol{z}_a\|_2^2 \\ & f_l^* + \tilde{\boldsymbol{q}}_l\boldsymbol{z}_a + \sigma\|\boldsymbol{z}_a\|_2\phi^{-1}(\eta_{\max}) \le f_l^{\max} - \delta, \ \forall l \in \mathcal{L}_- \\ & f_l^* + \tilde{\boldsymbol{q}}_l\boldsymbol{z}_a + \sigma\|\boldsymbol{z}_a\|_2\phi^{-1}(1-\eta_{\min}) \ge f_l^{\min} + \delta, \forall l \in \mathcal{L}_+ \\ & \|\boldsymbol{z}_a\|_2 \ \le \ \rho \\ & \delta \ > \ 0 \end{aligned} \ , \qquad (45)$$

where $\Upsilon(\beta)$ is defined in (43). The problem in (45) is convex, and specifically, it is a second-order cone programing (SOCP) problem. SOCP problems are convex optimization problems in which a linear function is minimized over the intersection of an affine linear manifold with the Cartesian product of second-order (Lorentz) cones, and are considered special cases of semi-definite programming problems. Such problems, are discussed in details in [26], where it is shown that they can be solved efficiently using the standard and highly efficient interior point method software tools, e.g., CVX [27]. The solution to (45) serves as a conservative approximation to the original problem in (34).

V. Case Study

In this section, we provide simulation results in the IEEE 14-bus system to illustrate the impacts of the FDIAs launched by the limited adversaries on the electricity market. Throughout the simulations, we assume that elements of the uncertainty matrix $\Delta\boldsymbol{Q}$, as defined in (12), are distributed according to $\mathcal{N}(0, \sigma^2)$, and we set $\sigma = 0.1$, unless specified otherwise. The constraint probabilities are also set to $\eta \triangleq \eta_{\max} = \eta_{\min} = 0.9$, unless specified. Accordingly, we have $\beta = -\ln(1-\eta)$. All the simulations are implemented using Matlab-based software packages including MATPOWER [28] and convex programming solver CVX [27].

In all the simulations, we assume that 1, 2, or 3 lines are congested. The list of congested lines, the associated buses, and all the related measurement units are marked in the IEEE 14-bus model depicted in Fig. 1, and they and listed in Table I.

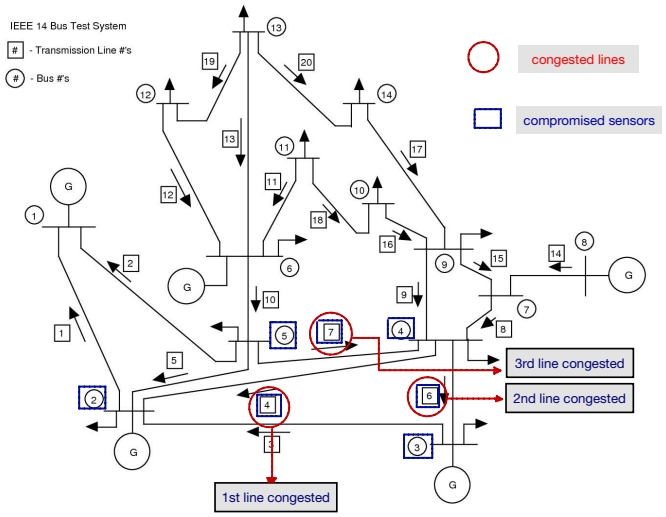


Fig. 1: IEEE standard 14-bus system with the congested lines, the affected buses, and the compromised buses and measurements marked.

A. Effect of the Grid Uncertainty Level

In order to assess the connection between the conservative profit confidence δ and the variance σ, we first focus on

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2017.2733346, IEEE Transactions on Smart Grid

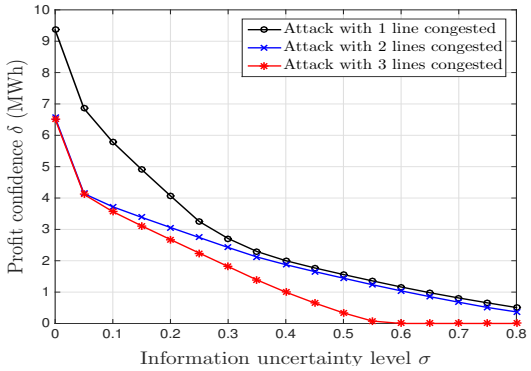


Fig. 2: Profit confidence δ versus model uncertainty σ.

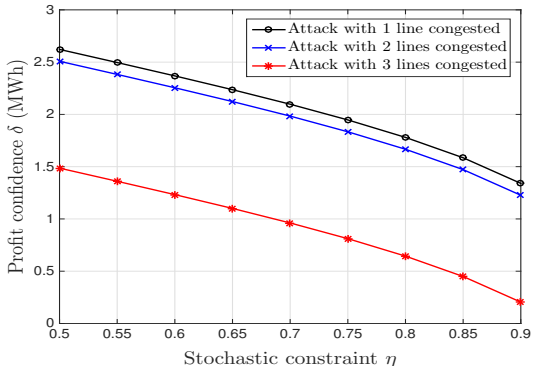


Fig. 3: Profit confidence δ versus attack undetectability η.

the settings in which different numbers of transmission lines are congested. Figure 2 demonstrates the variations of δ versus σ in the IEEE 14-bus system. It is observed that when the attacker has access to perfect information about the grid ($\sigma = 0$), δ takes its maximum values. With the increasing uncertainty level σ, profit confidence δ decreases monotonically and reaches 0 MWh when the uncertainty reaches a certain level. The reason underlying this observation is that the attack vector $\boldsymbol{z}_a$ must satisfy

$$\Upsilon(\beta) \leq \varepsilon^2 - \|(\tilde{\boldsymbol{Q}} - \boldsymbol{I})\boldsymbol{z}_a\|_2^2 \,, \tag{46}$$

based on which when β, the bad data detection threshold ε, and the attack vector norm ρ are fixed, as σ increases the room for the injected attack vector $\boldsymbol{z}_a$, and subsequently, the attacker's ability to manipulate the state estimates, shrinks rapidly. Furthermore, once σ keeps increasing such that we have

$$K\sigma^2\rho^2 + 2\sigma^2\rho^2\beta \geq \varepsilon^2 \,, \tag{47}$$

the constraint in (46) is violated and the problem in (45) becomes infeasible. Therefore, launching an effective attack in the RT market is feasible only if the uncertainty level σ is below a certain level.

Figure 2 also depicts the variations of δ versus σ for different settings with 1, 2, and 3 congested transmission lines. It is observed that along with the increase in the uncertainty level σ, the more transmission lines are congested, the more sharply the profit confidence δ declines. The underlying reason is that the attack vector $\boldsymbol{z}_a$ is limited by the δ-profitable constraints (44). Therefore, as the number of lines in congestion increases, a larger system congestion pattern the attackers have to relieve, which enforces stricter requirements for the design of the attack vector $\boldsymbol{z}_a$.

B. Effect of Stochastic Guarantees

In this subsection, we investigate the variations of δ with respect to the variations of η. In Fig. 3, it is observed that by increasing η, the profit confidence δ decreases monotonically. The reason underlying this observation is that increasing η raises the η-related parameter β and $\phi^{-1}(\eta)$, and decreases $\phi^{-1}(1-\eta)$ in the corresponding constraints in (45). Accordingly, these variations of parameters lead to stricter constraints on the attack vector $\boldsymbol{z}_a$.

C. Effects on the LMPs

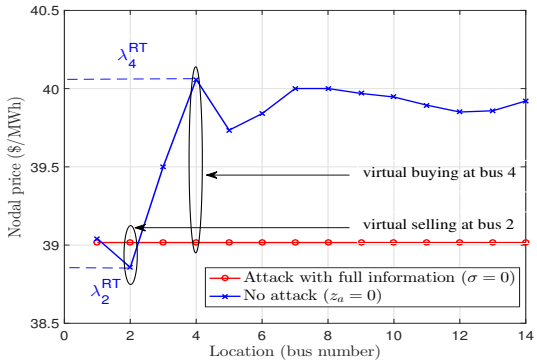
In this subsection, we analyze the effects of the attacker's uncertainty on the manipulated LMPs in the RT electricity market. We assume that in the DA market certain transmission lines are congested. With enough knowledge of network dynamics and a number of comprised sensors, the congested lines in the system can be relieved completely with confidence, which leads to uniform LMPs in the RT market. Combining with virtual bidding, such attacks can bring financial profit to the attacker. To illustrate the effect of model uncertainty on the attacker's potential financial gain, we denote the profit confidence when network dynamics are fully known (i.e., $\sigma = 0$) by δ_0, which is the profit confidence when congested lines are relieved completely. As uncertainty level increases, δ decreases, where $(\delta_0 - \delta)$ represents the relative congestion degree in the RT market, and is reflected by the fluctuations of LMPs at each bus in the RT market.

Figures 4(a) and 4(b) demonstrate LMPs under attack with and without model uncertainty, i.e., $\sigma = 0.8$ and $\sigma = 0$, respectively. In this case, only one line (connecting buses 2 and 3) is congested. In the DA market, the attacker chooses to buy and sell the same amount of virtual power at buses 2 and 3, respectively. After launching an FDIA, the attacker chooses to sell and buy the same amount of virtual power at the corresponding buses, respectively.

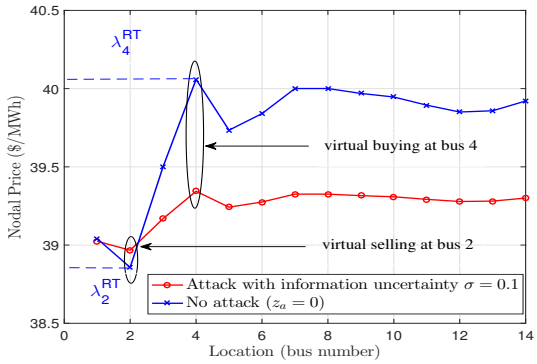
D. Effects of Attack Strength

In this subsection, we discuss the impacts of the attack vector energy ρ on the profit confidence δ. Figure 5 shows that when we enforce $\rho = 0$, which represents the attack-free setting, i.e., $\boldsymbol{z}_a = \boldsymbol{0}$, the corresponding profit confidence is 0. The profit confidence δ increases as we increase the attack energy ρ. This is due to the fact that increased ρ enhances the attacker's ability to manipulate the state estimates in order to relieve certain congested lines in the DA market. Therefore, an increase in ρ will enable the attacker to launch more effective attacks leading to a higher value for the profit confidence δ.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2017.2733346, IEEE Transactions on Smart Grid



(a) Attack with full information.



(b) Attack with uncertainty level $\sigma = 0.8$.

Fig. 4: Real-time LMPs at each load bus under attack with full information ($\sigma = 0$) and with certain uncertainty ($\sigma = 0.8$).

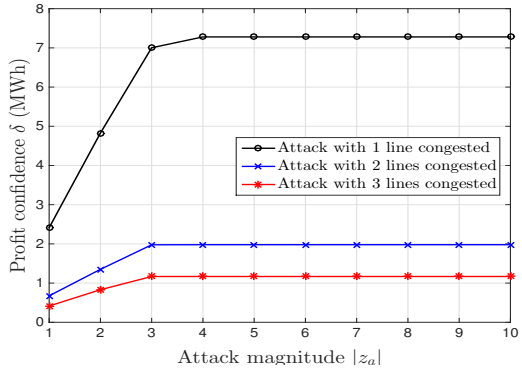


Fig. 5: Profit confidence δ versus attack norm ρ.

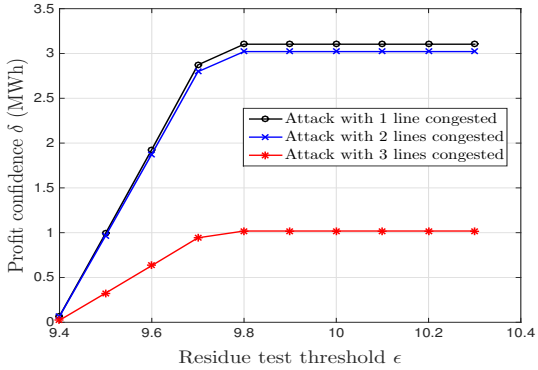


Fig. 6: Profit confidence δ versus residue test threshold ε.

E. Effect of Residue Test Threshold

In this subsection, we evaluate the profit confidence along with the varying threshold of the residue test ε defined in (11). In Fig. 6, it is observed that only when ε is beyond a certain value the attacker can launch feasible attacks. As ε increases, the profit confidence rises monotonically and eventually saturates. The saturation effect can be explained by noting that for any set of given σ, ρ, and η, the attack deign problem is feasible if vector $\boldsymbol{z}_a$ satisfies both of the following two conditions, where the second one holds according to (46):

$$\|\boldsymbol{z}_a\| \leq \rho \qquad \text{and} \qquad \Upsilon(\beta) + \|(\tilde{\boldsymbol{Q}} - \boldsymbol{I})\boldsymbol{z}_a\|_2^2 \leq \varepsilon^2 \ . \quad (48)$$

For smaller values of ε, the second condition on $\boldsymbol{z}_a$ is the dominant one, and as a result, increasing ε allows for increasing the space of $\boldsymbol{z}_a$, and as a resulting designing more effective attacks. When ε is large enough, however, the first condition starts to be the dominant one, and that is the point beyond which increasing ε does not yield in a higher profit, and as a result δ saturates.

F. Limited Compromised Sensors

In this subsection, we consider the settings in which an attacker can distort only a limited number of measurement units (sensors). This indicates that elements of $\boldsymbol{z}_a$ corresponding to the measurement units that cannot be compromised are forced to be 0. In such settings, we evaluate the impacts of the limited number of compromised sensors on the profit confidence δ. For this purpose, we consider the IEEE-14 bus system with one line congested. Such a system consists of 14 buses and 20 branches, and as a result, the number of measurements is $K = 34$ with $N = 14$. In Fig. 2, we observed that when the attacker can compromise any desired number of sensors, the profit confidence δ decreases as the attacker's uncertainty level increases. We observe the same trend when a limited number of sensors can be compromised due to the same reason that the increasing uncertainty shrinks the room for injecting the attack vector. Figure 7 depicts the variations of δ with respect to σ when the attacker can compromise a limited number of sensors. It shows that for any given uncertainty level σ, compromising fewer number of sensors leads to lower profit confidence values. It can be explained by that besides the attackers' restriction from (ε, η)-robust and δ-profitable constraints, they have to face their own restriction with limited non-zero elements in $\boldsymbol{z}_a \in \mathcal{S}$ due to their limited access to measurement meters. For certain uncertainty level, when fewer limited sensors are compromised, it is less likely for the attacker to inject an attack vector that is both undetectable and profitable in the RT market. Even with perfect knowledge of network information, by compromising fewer sensors the attacker cannot even be undetectable by the BDDs [6]. Thus, for any given uncertainty level, when the compromised sensors are fewer than a critical number, it is impossible for the attacker to launch (ε, η)-robust, and thus profitable, attacks in the RT market.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2017.2733346, IEEE Transactions on Smart Grid

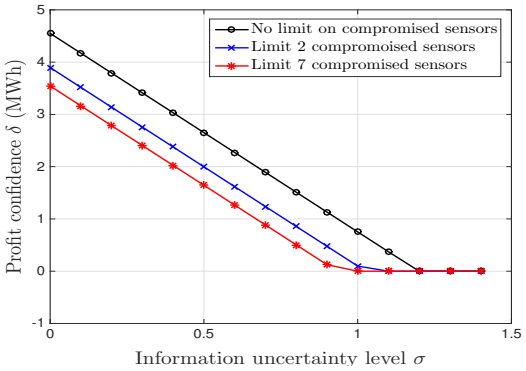


Fig. 7: δ for different number of sensors compromised.

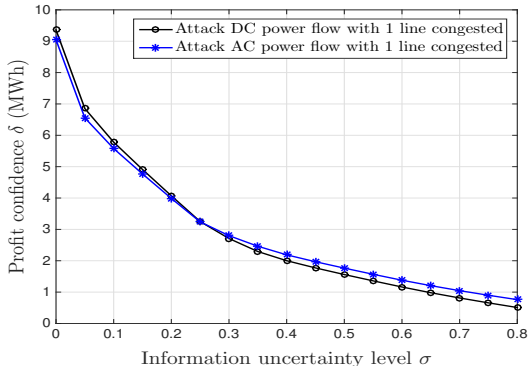


Fig. 8: DC and AC power flow comparison.

These observations raise a natural question pertinent to the necessary protections that ensure minimizing the effectiveness of the attacks. There exists studies (c.f. [29]) that delineate the fraction of measurement units to be protected in order to guarantee detecting the attacks even when the attacker has full and perfect information about the grid. Once the number of protected measurement units is determined, next a system operator should identify the *best* set of measurement units to be protected. To address this, we remark that the attacks are, in principle, most effective when they target manipulating the measurements associated with the lines in which the actual power flow is furthest from their flow constraints. Specifically, as the power flow of line $\ell \in \mathcal{L}_+$ becomes closer to its minimum power flow limit ($f_\ell^{\min}$) or the power flow of line $\ell \in \mathcal{L}_-$ becomes closer to its maximum power flow limit ($f_\ell^{\max}$), it leaves less room for the attacker to manipulate the reported flows. Based on this observations, the most vulnerable lines are those with power flows far from their minimum and maximum limits, depending on whether they belong to set the power flow of line $\ell \in \mathcal{L}_+$ or the power flow of line $\ell \in \mathcal{L}_-$. Hence, the system operator should protect the lines in which the power flows have higher chances of being far from their corresponding limits. Once these lines are identified, based on the linear connection $\boldsymbol{f} = \boldsymbol{H}\boldsymbol{x}$, one can also identify the corresponding elements of the nodal injection vector $\boldsymbol{x}$ that should be protected. It is noteworthy that due to sparsity of the distribution factor matrix $\boldsymbol{H}$, each power flow will be affected by a small number of the elements of $\boldsymbol{x}$. Finally, once these elements are identified, based on the measurement model $\boldsymbol{z} = \boldsymbol{H_s}\boldsymbol{x} + \boldsymbol{w}$, the list of sensors that should be protected can be identified.

G. DC designed FDIAs with AC Power Flows

In this subsection, we evaluate the effectiveness of adopting the DC linearized power flow model. Since the state estimates in this paper are nodal power injections, we compare the performance of the attack strategy in both DC and AC power flow models. Figure 8 illustrates the variations of profit confidence δ with respect to the uncertainty ratio under both AC and DC models with one line congested (connecting buses 2 and 4) in the IEEE 14-bus system. This figure demonstrates that with nonlinear power flow, the profit confidence in both models follows the same trend and the gap between them is negligible.

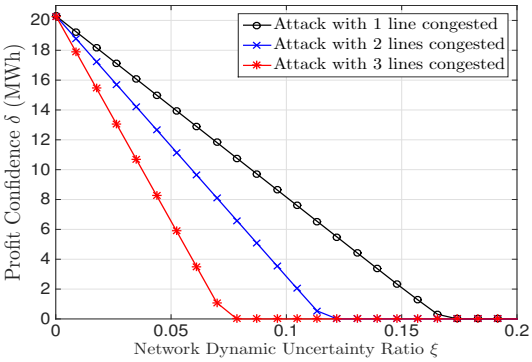


Fig. 9: IEEE 118-bus system.

H. Scalability

The simulation results in the previous subsections are focused on the IEEE 14-bus system. Nevertheless, the same trends in all the simulations can be observed in the larger scale systems as well. The underlying reason is that constructing attack vectors that can mislead the power flow estimates even in a subnetwork is sufficient to manipulate the LMPs and gain profit. Hence, irrespectively of the size of the network, the attacker can always select a subnetwork and compromise its measurement units, and, consequently, its power flow estimates and LMPs. As discussed earlier, there exist studies that establish the interplay between the fraction of the protected sensors and the effectiveness of the attacks. Similar interplay holds valid in our setting as well. Specifically, the simulation results in Fig. 9 show the variations of δ with respect to σ in the IEEE 118-bus system.

I. Stochastic Model

In this paper we have assumed that the uncertainties in the elements of $\boldsymbol{Q}$ are modeled as Gaussian random variables. In order to assess the sensitivity of the results to the specific model adopted, we consider a system with the setting specified for the simulations in Fig. 2, and in this system we compare the profit confidence level δ for two separate models for $\Delta\boldsymbol{Q}$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2017.2733346, IEEE Transactions on Smart Grid

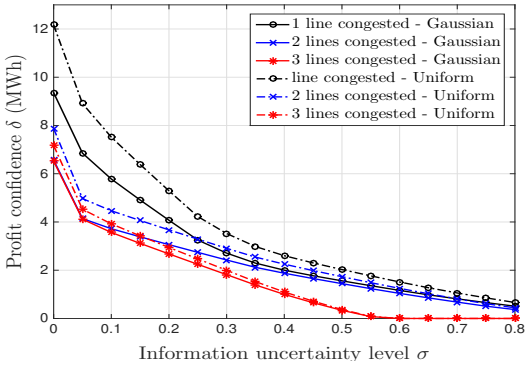


Fig. 10: Profit for Gaussian versus uniform uncertainties.

where in one model the elements of $\Delta \boldsymbol{Q}$ follow Gaussian distributions, and the other one they follow uniform distributions such that $\Delta Q_{ij} \sim \text{Uniform}[-\sqrt{3}\sigma, \sqrt{3}\sigma]$. The range $2\sqrt{3}\sigma$ is selected such that the uniform distribution admits the same variance σ^2 as the Gaussian random valuable. The results are provided in Fig. 10, where it is observed that the profit confidence levels in the setting with a uniform distributions uniformly exceed those of the setting with Gaussian distributions.

VI. Conclusion

In this paper we have considered false data injection attack (FDIA) strategies for adversaries who have imperfect information about grid dynamics. We have analyzed the effects of such adversaries on the electricity market. By adopting a stochastic model for the grid dynamic uncertainties, we have developed a chance-constrained approach to design a stochastically robust FDIA strategy that seeks to maximize the profit confidence while satisfying the stochastic constraints on being detected. We have shown that such a chance-constrained problem is non-convex and is intractable, and we have proposed a conservative approximation of the problem, which guarantees a lower bound on the profit confidence, and can be posed as a convex and computationally-efficient deterministic optimization problem. We have also provided simulation results in the standard IEEE 14-bus and 118-bus systems to evaluate the attack designs found analytically.

Appendix A
Proof of Theorem 1

In order to apply Lemma 1 to constraint (38), let we set

$$\boldsymbol{G} = \boldsymbol{R} \,, \tag{49}$$

$$\boldsymbol{r} = \boldsymbol{R}^{\frac{1}{2}} \cdot (\tilde{\boldsymbol{Q}} - \boldsymbol{I}) \cdot \boldsymbol{z}_a = \sigma \|\boldsymbol{z}_a\| \cdot (\tilde{\boldsymbol{Q}} - \boldsymbol{I}) \cdot \boldsymbol{z}_a \,, \tag{50}$$

$$\text{and} \quad \beta = -\ln(1-\eta) \,. \tag{51}$$

Based on these, we obtain that

$$\text{tr}(\boldsymbol{G}) = K\sigma^2 \|\boldsymbol{z}_a\|^2 \,, \tag{52}$$

$$\|\boldsymbol{G}\|_F^2 = K\sigma^4 \|\boldsymbol{z}_a\|^4 \,, \tag{53}$$

$$\text{and} \qquad \lambda_{\boldsymbol{G}}^{+} = \sigma^2 \|\boldsymbol{z}_a\|^2 \,. \tag{54}$$

According to Lemma 1, we find that for any $\eta \in (0,1)$,

$$\mathbb{P}\{T \le \Psi(\beta)\} \ge 1 - e^{-\beta} \,, \tag{55}$$

Then comparing (38) and (55) establishes that the inequality in (38) holds valid when

$$\Psi(\beta) \le \varepsilon^2 - \|(\tilde{\boldsymbol{Q}} - \boldsymbol{I})\boldsymbol{z}_a\|_2^2 \,. \tag{56}$$

Hence, satisfying (56) is sufficient to ensure that (38), and subsequently, the (ε, η)-robustness constraint in (15) are satisfied. Based on the definitions of $\boldsymbol{G}$ and $\|$, $\Psi(\beta)$ simplifies to: where

$$\begin{aligned}\Psi(\beta) &= K\sigma^2\|\boldsymbol{z}_a\|^2 + 2\beta\sigma^2\|\boldsymbol{z}_a\|^2 \\ &\quad + 2\sqrt{\beta}\cdot\sqrt{K\sigma^4\|\boldsymbol{z}_a\|^4 + 2\sigma^2\|\boldsymbol{z}_a\|^2\|(\tilde{\boldsymbol{Q}}-\boldsymbol{I})\boldsymbol{z}_a\|^2} \\ &= \sigma^2\|\boldsymbol{z}_a\|_2^2(K+2\beta) \\ &\quad + 2\sigma^2\|\boldsymbol{z}_a\|_2\sqrt{\beta K(\|\boldsymbol{z}_a\|_2^2 + \|\boldsymbol{S}\boldsymbol{z}_a\|_2^2)} \,. \end{aligned} \tag{57}$$

Moreover, note that

$$\|\boldsymbol{z}_a\|_2^2 + \|\boldsymbol{S}\boldsymbol{z}_a\|_2^2 = \boldsymbol{z}_a^T(\boldsymbol{I} + \boldsymbol{S}^T\boldsymbol{S})\boldsymbol{z}_a \,. \tag{58}$$

For the positive-definite matrix $(\boldsymbol{I} + \boldsymbol{S}^T\boldsymbol{S})$, we have the Cholesky decomposition

$$\boldsymbol{I} + \boldsymbol{S}^T\boldsymbol{S} = \boldsymbol{L}^T\boldsymbol{L} \,, \tag{59}$$

where $\boldsymbol{L}$ is triangle Cholesky factor. Hence,

$$\|\boldsymbol{z}_a\|_2^2 + \|\boldsymbol{S}\boldsymbol{z}_a\|_2^2 = \|\boldsymbol{L}\boldsymbol{z}_a\|_2^2 \,. \tag{60}$$

Therefore, (57) and (60) establish

$$\Psi(\beta) = \sigma^2\|\boldsymbol{z}_a\|_2^2(K+2\beta) + 2\sigma^2\sqrt{\beta K}\|\boldsymbol{z}_a\|_2\|\boldsymbol{L}\boldsymbol{z}_a\|_2 \,. \tag{61}$$

Hence, for attack vector with norm $\|\boldsymbol{z}_a\|_2 = \rho$ we have

$$\Psi(\beta) = \sigma^2\rho^2(K+2\beta) + 2\sigma^2\sqrt{\beta K}\rho\|\boldsymbol{L}\boldsymbol{z}_a\|_2 \,. \tag{62}$$

Hence, the constraint in (56) can be written as

$$\rho^2(K+2\beta) + 2\sqrt{\beta K}\rho\|\boldsymbol{L}\boldsymbol{z}_a\|_2 + \frac{K}{2\sigma}\|\boldsymbol{S}\boldsymbol{z}_a\|_2^2 \le 1 \,, \tag{63}$$

which is a second-order cone constraint and serves as a conservative formulation for the stochastic (ε, η)-robust constraint in (15).

Appendix B
Proof of Theorem 2

We treat the constraints in (33) associated with lines contained in sets $\mathcal{L}_+$ and $\mathcal{L}_-$ independently.

A. Lines contained in set $\mathcal{L}_-$

By recalling $\boldsymbol{Q} = \tilde{\boldsymbol{Q}} + \Delta\boldsymbol{Q}$, the stochastic δ-profitable constraints contained in $\mathcal{L}_-$ can be rewritten as follows. For any $\Delta\boldsymbol{Q} \in \mathcal{B}$, we have

$$\mathbb{P}\{f_l^* + \tilde{\boldsymbol{q}}_l\boldsymbol{z}_a + \Delta\boldsymbol{q}_l\boldsymbol{z}_a \le f_l^{\max} - \delta\} \ge \eta_{\max} \,, \forall l \in \mathcal{L}_- \,, \tag{64}$$

where we have defined $\Delta\boldsymbol{q}_l \triangleq \boldsymbol{e}_l^T[\boldsymbol{0} \quad \boldsymbol{I}]\Delta\boldsymbol{Q}$. Then it is readily verified that

$$\Delta\boldsymbol{q}_l\boldsymbol{z}_a \sim \mathcal{N}(0, \sigma^2\cdot\|\boldsymbol{z}_a\|_2^2) \,. \tag{65}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2017.2733346, IEEE Transactions on Smart Grid

Hence, the constraints in (64) can be equivalently written as

$$f_l^* + \tilde{\boldsymbol{q}}_l \boldsymbol{z}_a + \sigma \|\boldsymbol{z}_a\|_2 \phi^{-1}(\eta_{\max}) \leq f_l^{\max} - \delta, \ \forall l \in \mathcal{L}_- \ , \quad (66)$$

which is the desired result.

B. Lines contained in set $\mathcal{L}_+$

By following the same line of arguments, we can show that for any $\Delta \boldsymbol{Q} \in \mathcal{B}$, we have

$$\mathbb{P}\left\{ f_l^* + \tilde{\boldsymbol{q}}_l \boldsymbol{z}_a + \Delta \boldsymbol{q}_l \boldsymbol{z}_a \geq f_l^{\min} + \delta \right\} \geq \eta_{\min} \ , \forall l \in \mathcal{L}_+ \ , \quad (67)$$

and subsequently,

$$f_l^* + \tilde{\boldsymbol{q}}_l \boldsymbol{z}_a + \sigma \|\boldsymbol{z}_a\|_2 \phi^{-1}(1 - \eta_{\min}) \geq f_l^{\min} + \delta, \ \forall l \in \mathcal{L}_+ \ , \quad (68)$$

which is the desired result.

REFERENCES

[1] S. M. Amin and B. F. Wollenberg, "Toward a smart grid: power delivery for the 21st century," *IEEE Power and Energy Magazine*, vol. 3, no. 5, pp. 34–41, Sept. 2005.

[2] E. Santacana, G. Rackliffe, L. Tang, and X. Feng, "Getting smart," *IEEE Power and Energy Magazine*, vol. 8, no. 2, pp. 41–48, Mar. 2010.

[3] A. Ipakchi and F. Albuyeh, "Grid of the future," *IEEE Power and Energy Magazine*, vol. 7, no. 2, pp. 52–62, Mar. 2009.

[4] 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 Processing Magazine*, vol. 29, no. 5, pp. 106–115, Sep. 2012.

[5] A. Monticelli, "Electric power system state estimation," *Proceedings of the IEEE*, vol. 88, no. 2, pp. 262–282, Feb 2000.

[6] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proc. ACM Conference on Computer and Communications Security*, Chicago, IL, Nov. 2009, pp. 21–32.

[7] A. Ott, "Experience with PJM market operation, system design, and implementation," *IEEE Transactions on Power Systems*, vol. 18, no. 2, pp. 528–534, May 2003.

[8] E. Litvinov, T. Zheng, G. Rosenwald, and P. Shamsollahi, "Marginal loss modeling in lmp calculation," *IEEE Transactions on Power Systems*, vol. 19, no. 2, pp. 880–888, May 2004.

[9] T. Zheng and E. Litvinov, "Ex post pricing in the co-optimized energy and reserve market," *IEEE Transactions on Power Systems*, vol. 21, no. 4, pp. 1528–1538, Nov. 2006.

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

[11] L. Jia, R. Thomas, and L. Tong, "Malicious data attack on real-time electricity market," in *Proc IEEE International Conference on Acoustics, Speech and Signal Processing*, Prague, May 2011, pp. 5952–5955.

[12] X. Lei, D. Yu, and X. Bai, "Research on multistep electricity price model with bidirectional regulation for large consumers," in *Proc. International Conference on Electrical and Control Engineering*, June 2010, pp. 4114–4117.

[13] J. Lin, W. Yu, and X. Yang, "On false data injection attack against multistep electricity price in electricity market in smart grid," in *Proc. IEEE Global Communications Conference*, Dec. 2013, pp. 760–765.

[14] L. Jia, R. Thomas, and L. Tong, "Impacts of malicious data on real-time price of electricity market operations," in *Proc. Hawaii International Conference on System Science*, Maui, HI, Jan. 2012, pp. 1907–1914.

[15] M. Esmalifalak, G. Shi, Z. Han, and L. Song, "Bad data injection attack and defense in electricity market using game theory study," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 160–169, Mar. 2013.

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

[17] X. Liu and Z. Li, "Local load redistribution attacks in power systems with incomplete network information," *IEEE Transactions on Smart Grid*, vol. 5, no. 4, pp. 1665–1676, July 2015.

[18] ——, "False data attacks against AC state estimation with incomplete network information," *IEEE Transactions on Smart Grid*, vol. Early Access, 2016.

[19] M. Rahman and H. Mohsenian-Rad, "False data injection attacks with incomplete information against smart power grids," in *Proc. IEEE Global Communications Conference*, Anaheim, CA, Dec. 2012, pp. 3153–3158.

[20] 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 Transactions on Smart Grid*, vol. PP, no. 99, pp. 1–1, April 2016.

[21] L. Xie, Y. Mo, and B. Sinopoli, "False data injection attacks in electricity markets," in *Proc. IEEE International Conference on Smart Grid Communications*, Gaithersburg, MD, Oct. 2010, pp. 226–231.

[22] A. Abur and A. G. Exposito, *Power system state estimation: theory and implementation*. CRC press, 2004.

[23] F. Schweppe, "Power system static-state estimation, parts I, II and III," *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-89, no. 1, pp. 120–135, Jan. 1970.

[24] S. Hunt, *Making competition work in electricity*. John Wiley and Sons, 2002, vol. 146.

[25] I. Bechar, "A Bernstein-type inequality for stochastic processes of quadratic forms of Gaussian variables," arXiv:0909.3595, 2009.

[26] F. Alizadeh and D. Goldfarb, "Second-order cone programming," *Mathematical Program- ming*, vol. 95, pp. 3–51, 2003.

[27] M. Grant and S. Boyd, "CVX: Matlab software for disciplined convex programming, version 2.1," http://cvxr.com/cvx, Mar. 2014.

[28] R. D. Zimmerman, C. E. Murillo-Sanchez, and R. J. Thomas, "Matpower: Steady-state operations, planning, and analysis tools for power systems research and education," *IEEE Transactions on Power Systems*, vol. 26, no. 1, pp. 12–19, Feb. 2011.

[29] T. T. Kim and H. V. Poor, "Strategic protection against data injection attacks on power grids," *IEEE Transactions on Smart Grids*, vol. 2, no. 2, pp. 326–333, June 2011.

Ali Tajer (S05, M10, SM15) is an Assistant Professor of Electrical, Computer, and Systems Engineering at Rensselaer Polytechnic Institute. During 2007-2010 he was with Columbia University where he received the M.A degree in Statistics and Ph.D. degree in Electrical Engineering, and during 2010-2012 he was with Princeton University as a Postdoctoral Research Associate. His research interests include mathematical statistics and network information theory, with applications in wireless communications and power grids. Dr. Tajer Serves as an Editor for the IEEE Transactions on Communications, an Editor for the IEEE Transactions on Smart Grid, and in the past has served as the Guest Editor-in-Chief for the IEEE Transactions on Smart Grid Special Issue on Theory of Complex Systems with Applications to Smart Grid Operations. He is a senior member of the IEEE and received the NSF CAREER award in 2016.