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.2017.2695120, IEEE Transactions on Smart Grid

Data Injection Attacks on Electricity Markets by Limited Adversaries: Worst-case Robustness

Mateo R. Mengis, *Member, IEEE* and Ali Tajer, *Senior Member, IEEE*

***Abstract*—Electricity markets consist of multiple *look-ahead* and *real-time* spot markets, across which energy price is generally volatile. Moreover, dispatch and pricing decisions in the *real-time* markets strongly hinge on the quality of the real-time state estimates, which are formed dynamically in order to delineate real-time information about operation state of the grid. Adversaries can leverage price volatility in conjunction with the dependence of the real-time markets on the state estimates in order to carry out profitable financial misconduct, e.g., via virtual bidding on the locational marginal prices. When the adversaries are *omniscient* (i.e., have full and instantaneous access to grid topology and dynamics), the attack strategies for maximizing financial profits are studied extensively in the existing literature. This paper focuses on *limited* adversaries who have only *partial* and *imperfect* information about the grid, and offers a framework for analyzing the attack strategies for limited adversaries and the associated confidence about profitable attacks. Specifically, adversaries' information is considered to be within a measure of bounded error, and attack strategies are designed such that the adversaries are guaranteed a certain level of confidence to gain profit. Designing such attacks is investigated analytically and examined in the IEEE 14- and 118-bus systems.**

***Index Terms*—Deregulated electricity market, false data injection attack, incomplete information, state estimation, robustness.**

I. Introduction

Bulk electric systems are monitored, controlled, and coordinated by the system operators (SOs), which are responsible for balancing demand and supply, while optimizing efficiency, ensuring reliability, and complying with regulatory requirements. To ensure efficient operation, the SOs strongly rely on accurate information about the electricity markets for determining the most cost-effective generating units to commit to throughout dispatch [1, 2]. Electricity markets, on the other hand, have been transitioning from being monopolized to becoming more competitive, and consist of various day-ahead (DA) and real-time (RT) markets [3].

Some SOs (e.g., PJM) use a pricing mechanism called locational marginal pricing, which captures the value of the energy delivered at a specific time and location in order to establish the price of energy in the wholesale electricity markets. Locational marginal prices (LMPs) are subsequently used for determining nodal prices and coping with transmission congestion [3]. In the DA markets, the LMPs are calculated based on the demand forecasts and the optimal power flow (OPF) solution, and do not depend on the real-time system dynamics. In contrast, the LMPs in the RT markets are calculated by leveraging real-time information about the system (e.g., state estimates) and solving incremental OPF problems [3, 4]. Hence, in the RT markets efficient and reliable computation of the LMPs hinges strongly on the fidelity of the real-time information gathered by various measurement units. Such dependency makes the RT markets vulnerable to security threats [5–7], such that any distortion not properly detected by the monitoring modules (e.g., bad data detectors) leads to undesired changes in the LMPs.

M. R. Mengis was with the ECSE Department, Rensselaer Polytechnic Institute, Troy, NY, and is currently with the U. S. Army Corps of Engineers' Hydroelectric Design Center, Portland, OR.

A. Tajer is with the the ECSE Department, Rensselaer Polytechnic Institute, Troy, NY.

This research was supported by the National Priorities Research Program through the Qatar National Research Fund (a member of Qatar Foundation) under Grant 6-149-2-058.

A. False Data Injection Attacks

In this paper, we focus on false data injection attacks (FDIAs), which refer to a class of malicious strategies that target at corrupting the data by physically tampering the measurement units [8]. Such attacks are viable when the meters are not physically protected. In such circumstances, an attacker compromises the meters such that the compromised meters report corrupt data. It is noteworthy that in the FDIAs, the attackers corrupt the meter measurements before the measurements are used for any monitoring (e.g., state estimation and bad data detection) function at the control center. There exist also a number of other critical stages at which the attackers get a chance to corrupt the data. For instance, the attackers can potentially intrude to the control center and replace the data collected at the control center with corrupt data [9]; or in the cases that the data is stored in cloud servers, an attacker can intrude into the cloud server and compromise (delete or replace) the measurements on the server [10].

The primary goal of the FDIAs is to disrupt the operation of the grid, while minimizing the likelihood of being detected by the bad data detectors (BDDs) [11]. While the FDIAs are primarily focused on distorting state estimates, their impact transcends that, and they can affect the LMPs and economic dispatch decisions in the RT markets too. More specifically, a compromised estimate of the system state can lead to non-optimal dispatch, which, in turn, can cause the nodal prices at different system buses to shift away from their optimal values. An adversary can take advantage of such a price shift to carry out financial misconduct. In this paper, we focus on attackers that have *incomplete* information about the network, analyze the worst-case guarantees that attackers can enjoy for distorting the LMPs in the RT markets, and design attack strategies that achieve these guarantees. It is noteworthy that when attacks are launched in isolation and target a very

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.2017.2695120, IEEE Transactions on Smart Grid

small number of measurement units, the impact of the attacks can be marginal, or even negligible. There exist studies that analyze the minimum number of measurements that need to be compromised in order to make an effective attack. Intuitively, it is expected that most network functions remain rather uninterrupted if the attacks take place in isolation, or the number of them is below a critical mass. The dynamics between the number of measurement units protected (or compromised) and the effectiveness of the attacks is studied [12].

Finally, we remark that while the system can be equipped with cryptography to protect the integrity and confidentially if the data it communicates over the communication medium [13], it is widely investigated that cryptography might not properly counter FDIAs launched at the physical level. Specifically, such attacks corrupt the data before the data is being encrypted and transmitted over the communication channel. As a result, the role of cryptography will be limited to protecting the integrity and confidentiality of the data that is already corrupt.

B. Existing Work

A quantitative framework for assessing the impact of cyber attacks on the electricity market was first formalized in [5]. In [14], an FDIA strategy is constructed based on the fact that the attackers can launch FDIAs to manipulate RT power flow estimates in order to shift RT LMPs in a desired direction, and carry out financial misconduct. Specifically, an attacker participates in the market through virtual bidding and designs an attack such that the LMPs on a selected pair of buses between the DA and the RT markets are shifted in a desired direction. The study in [15] presents another FDIA design strategy, which maximizes the generated market revenue with a single measurement attack. Based on the multi-step electricity price (MEP) model introduced in [16], the impact of FDIAs in RT market against MEP is investigated in [17]. In order to incorporate the inter-temporal constraints, [18] proposes an attack strategy to withhold generation capacity for profit by manipulating the ramp constraints of the generators during look-ahead dispatch. In [19], an FDIA strategy based on the geometric characterization of the RT LMPs on the state space of grid is proposed.

Game-theoretic frameworks for modeling the dynamics between the attack and defense strategies are studied in [20] and [21]. Specifically, the study in [20] focuses on strategies based on FDIAs that compromise state estimates, and consequently, manipulate the RT LMPs, while [21] investigates jamming the communication channels that convey the measurement information in order to manipulate the RT LMPs. The idea of directly jamming the pricing signals is studied in [22], where the attackers can make a profit without intruding the power system and changing the reported data. The study in [23] investigates attack strategies by adopting a nonlinear model for power systems and considering nonlinear state estimators, and [24] discusses the RT LMPs under corrupt data.

C. Contributions

Most existing studies, irrespective of their discrepancies in settings or objectives, conform in adopting the common assumption that the attackers are *omniscient* and have complete knowledge of network information, including network topology and branch parameters (e.g., the exact positions of circuit breaker switches, transformer tap changers, and power line admittance values) [25]. In reality, however, network information is too extensive, secured, and temporally volatile to be completely accessible to an attacker. Therefore, such all-encompassing knowledge of the network information is a strong assumption to make for an attacking entity, and considering adversaries with partial (imperfect) knowledge of the network information is a more realistic scenario. FDIAs with incomplete information of the networks are investigated in other contexts (c.f. [26] and [27]). However, the impacts of such limited adversaries with incomplete information on electricity markets are not investigated in the literature.

Motivated by the realistic and practical significance of limited adversaries, in this paper we focus on the settings in which the attackers have imperfect views of the system topology and dynamics. This means that even though the attackers still have some method of accessing the electrical system information, the accessed data is contaminated with bounded errors. The bounded errors are unknown to the attackers, which indicates that the attackers know that the actual system realization belongs to a space of possible realizations. Corresponding to each realization of this space, the attacker can enjoy a certain level of confidence for gaining profit. Nevertheless, since the actual realization is unknown, an attacker is interested in determining the *worst-case* profit confidence over the entire space of possible realizations. We demonstrate that designing such robust FDIAs leads to solving a semi-infinite non-convex problem. While such semi-infinite non-convex problems in their most general forms are NP-hard to solve [28], with the additional structures of the problem at hand we show that this problem can be simplified and posed as an equivalent convex semi-definite programming (SDP) problem, which can be solved efficiently (in polynomial time) via the well-established interior point method [29]. We provide an analytical closed-form solution for the worst-case robust FDIA and quantify the economic impact of such limited attacks. We also provide simulations in the IEEE 14- and 118-bus systems to assess the robustness of the proposed attack approach under different levels of network model uncertainties.

II. System Model

A. Monitoring Model

Consider a power system consisting of M generators and J loads connected by L transmission lines. The power injected by generator $m \in \{1, \ldots, M\}$ is denoted by p_m and the load (demand) power withdrawn from the system by load $j \in \{1, \ldots, J\}$ is denoted by ℓ_j. Accordingly, we denote the power injection vector and load vector by $\boldsymbol{p} \triangleq [p_1, \ldots, p_M]^T$ and $\boldsymbol{\ell} \triangleq [\ell_1, \ldots, \ell_J]^T$, respectively. We consider a linearized DC power flow model, in which there exists a bijective relationship between bus voltage phase angles and the net power injection. Hence, estimates on bus voltage angles can be used to uniquely form estimates for the net power injections [30]. For the convenience in notations in monitoring and

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.2017.2695120, IEEE Transactions on Smart Grid

dispatch processes, we set $N \triangleq J+M$, and denote the vector of net power injections by

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

where positive and negative net injections correspond to generation and load, respectively. Based on the DC power flow model, the line flows denoted by $\boldsymbol{f} \triangleq [f_1, \ldots, f_L]^T$ satisfy

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

where $\boldsymbol{H} \in \mathbb{R}^{L\times N}$ is the distribution factor matrix [14]. Each row of $\boldsymbol{H}$ represents the linear sensitivities linking the amount of line flow change that occurs on a given line due to a change in net injections. The network is equipped with $K \triangleq J + M + L$ measurement units to measure generation, load, and transmission line flows. The measurements, denoted by $\boldsymbol{z} \in \mathbb{R}^{K\times 1}$, are related to $\boldsymbol{x}$ according to

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

where we have defined $\boldsymbol{H}_s \triangleq [\boldsymbol{I}_N \quad \boldsymbol{H}^T]^T$, and $\boldsymbol{w}$ accounts for the measurement noise, which has a zero-mean Gaussian distribution with covariance matrix $\boldsymbol{W}$. Upon collecting measurements $\boldsymbol{z}$, network operators constantly from estimates of $\boldsymbol{x}$ for various monitoring, control, and dispatch purposes. The maximum likelihood (ML) estimate of $\boldsymbol{x}$ based on (3) is

$$\hat{\boldsymbol{x}} = \boldsymbol{K}\boldsymbol{z} \ , \tag{4}$$

where we have defined

$$\boldsymbol{K} \triangleq (\boldsymbol{H}_s^H\boldsymbol{W}^{-1}\boldsymbol{H}_s)^{-1}\boldsymbol{H}_s^H\boldsymbol{W}^{-1}. \tag{5}$$

Hence, the estimate residue used for BDD is

$$\boldsymbol{r} \triangleq \boldsymbol{z} - \boldsymbol{H}_s\hat{\boldsymbol{x}} \overset{(4)}{=} (\boldsymbol{I} - \boldsymbol{H}_s\boldsymbol{K})\boldsymbol{z} \ . \tag{6}$$

Finally, we denote the upper and lower limits of real power flow in line $l \in \{1, \ldots, L\}$ by $f_l^{\max}$ and $f_l^{\min}$, respectively. Similarly, we denote upper and lower limits afforded by generator $m \in \{1, \ldots, M\}$ by $P_m^{\max}$ and $P_m^{\min}$, respectively.

B. Attack Model

In order to launch effective attacks, the attacker monitors network dynamics and compromises the measurement units, and creates an altered measurement vector

$$\boldsymbol{z}' \triangleq \boldsymbol{z} + \boldsymbol{z}_a \ , \tag{7}$$

where $\boldsymbol{z}_a$ is the injected attack vector. In the event of an attack, state estimates are formed based on the compromised measurements, and change to

$$\hat{\boldsymbol{x}}' \overset{(4)}{=} \boldsymbol{K}\boldsymbol{z}' = \hat{\boldsymbol{x}} + \boldsymbol{K}\boldsymbol{z}_a \ . \tag{8}$$

Accordingly, the residue value used for BDD becomes

$$\boldsymbol{r}' \overset{(6)}{=} \boldsymbol{r} + \boldsymbol{r}_a \ , \tag{9}$$

where we have defined $\boldsymbol{r}_a \triangleq (\boldsymbol{I} - \boldsymbol{H}_s\boldsymbol{K})\boldsymbol{z}_a$. When the injected attack vector $\boldsymbol{z}_a$ is perfectly aligned in the null space of $(\boldsymbol{I} - \boldsymbol{H}_s\boldsymbol{K})$, it leads to $\boldsymbol{r}_a = \boldsymbol{0}$, and the attacker remains undetectable by the BDDs. However, when such perfect alignment is infeasible, in order to maintain a high probability of being undetectable, the attacker must keep the ℓ_∞-norm of $\boldsymbol{r}_a$ small, i.e., below a specified threshold ε:

$$\|\boldsymbol{r}_a\|_\infty \ = \ \max\{r_1, r_2, \ldots, r_K\} \ \leq \ \varepsilon \ . \tag{10}$$

This constraint guarantees that the residue corresponding to every state parameter is below ε. Based on this, the individual residue test corresponding to the state parameter $k \in \{1, \ldots, K\}$ is

$$\|\boldsymbol{e}_k(\boldsymbol{I} - \boldsymbol{H}_s\boldsymbol{K})\boldsymbol{z}_a\|_2 \leq \varepsilon, \quad \forall k \in \{1, \ldots, K\} \ , \tag{11}$$

where $\boldsymbol{e}_k \in \mathbb{R}^{1\times K}$ is the standard unit vector satisfying

$$\boldsymbol{e}_k[\, i\,] = \begin{cases} 1, & i = k \\ 0, & i \neq k \end{cases}, \quad \text{for } \ k \in \{1, \ldots, K\} \ . \tag{12}$$

This constrained measures the attacker's detectability risk.

Remark 1: The value of ε depends on the range of the state parameters and it is selected such that the rate of the false alarms is controlled below a desired level [31].

Remark 2: ℓ_2-norm based residue test is also a common test to detect the presence of bad measurements [11, 32, 33]. Controlling the ℓ_2-norm below a desired threshold leads to a less stringent bad data detectability constraint. All the analyses provided in this paper can be readily extended to the ℓ_2-norm based residue test.

Maintaining a small value for $\|\boldsymbol{e}_k(\boldsymbol{I} - \boldsymbol{H}_s\boldsymbol{K})\boldsymbol{z}_a\|_2$ strongly hinges on the perfect and instantaneous knowledge of the attacker about $\boldsymbol{H}_s\boldsymbol{K}$. This implies that effective design of undetectable attacks necessitates that the attacker has perfect access to the network topology and its instantaneous dynamics. In this paper, we assume that there exists a mismatch between the actual network model and the one presumed by the attackers. Specifically, we assume that the attacker has access to only a noisy version of $\boldsymbol{H}_s\boldsymbol{K}$. To formalize this, we define $\boldsymbol{Q} \triangleq \boldsymbol{H}_s\boldsymbol{K}$ to represent the actual realization of $\boldsymbol{H}_s\boldsymbol{K}$, and denote its noisy estimate known to the attacker by $\tilde{\boldsymbol{Q}}$. Furthermore, we define $\Delta\boldsymbol{Q} \triangleq \boldsymbol{Q} - \tilde{\boldsymbol{Q}}$ to describe the attacker's uncertainty about network dynamics. We assume that the uncertainty errors are bounded and confined within an origin-centered hyper-spherical region of radius β, i.e.,

$$\|\Delta\boldsymbol{Q}\|_2 \leq \beta \ . \tag{13}$$

Hence, while the attacker does not know matrix $\boldsymbol{Q}$, it knows that it belongs to the set

$$\mathcal{A}(\beta) \triangleq \{\boldsymbol{Q} \mid \boldsymbol{Q} = \tilde{\boldsymbol{Q}} + \Delta\boldsymbol{Q}, \|\Delta\boldsymbol{Q}\|_2 \leq \beta\} \ . \tag{14}$$

Similarly, the uncertainty matrix $\Delta\boldsymbol{Q}$ belongs to the set

$$\mathcal{C}(\beta) \triangleq \{\Delta\boldsymbol{Q} \mid \|\Delta\boldsymbol{Q}\|_2 \leq \beta\} \ . \tag{15}$$

Due to the uncertainties associated with $\boldsymbol{Q}$, the attacker faces uncertainties about the injection vector $\boldsymbol{z}_a$, since different actual realizations for $\boldsymbol{Q}$ lead to different attack vectors. From the attacker's perspective, the attack is most likely detectable, which we refer to as the *worst-case* attack, when the combination of the attack and the actual system realization leads to the largest value for $\|(\boldsymbol{I} - \boldsymbol{Q})\boldsymbol{z}_a\|_2$. If the attacker designs its

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.2017.2695120, IEEE Transactions on Smart Grid

attack strategy such that even under the worst-case setting it remains undetectable by the BDD, it immediately ensures that any arbitrary system realization enjoys that guarantee as well. Motivated by this, we define the ε-robust attack as follows.

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

$$\|\boldsymbol{e}_k(\boldsymbol{I}-\boldsymbol{Q})\boldsymbol{z}_a\|_2 \leq \varepsilon,\ \forall \boldsymbol{Q} \in \mathcal{A}(\beta),\ \forall k \in \{1,\ldots,K\}\ , \quad (16)$$

which is equivalent to

$$\sup_{\boldsymbol{Q}\in\mathcal{A}(\beta)} \|\boldsymbol{e}_k(\boldsymbol{I}-\boldsymbol{Q})\boldsymbol{z}_a\|_2 \leq \varepsilon,\ \forall k \in \{1,\ldots,K\}\ . \quad (17)$$

C. Electricity Markets

The deregulated market, consisting of the DA and RT markets, is widely used by the SOs to stabilize the power system and calculate LMPs based on the DC optimal power flow (DCOPF) model [3].

1) Day-Ahead Market: In the DA market, the SOs perform optimal dispatch calculations to minimize the aggregate cost given the dispatchable load forecast $\boldsymbol{\ell}$. We denote the cost associated with generator $m \in \{1,\ldots,M\}$ with output p_m by $C_m(p_m)$. Accordingly, we define vectors

$$\boldsymbol{C}(\boldsymbol{p}) = [C_1(p_1),\ldots,C_M(p_M)]^T\ . \quad (18)$$

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

$$\begin{cases} \min\limits_{\boldsymbol{p}} & \mathbf{1}_M \cdot \boldsymbol{C}(\boldsymbol{p}) \\ \text{s.t.} & \mathbf{1}_M \cdot \boldsymbol{p} = \mathbf{1}_J \cdot \boldsymbol{\ell} \\ & p_m^{\min} \leq p_m \leq p_m^{\max},\ \ \forall m \in \{1,\ldots,M\} \\ & f_l^{\min} \leq f_l \leq f_l^{\max},\ \ \forall l \in \{1,\ldots,L\} \end{cases} \quad (19)$$

2) Real-Time Market: In the RT market, due to variations in the actual load, the SOs update dispatch $\boldsymbol{p}^*$ via performing incremental dispatch calculation to achieve real-time optimal system operation. Such updates leverage state estimates $\hat{\boldsymbol{x}}$ and estimate $\hat{p}_m$ as the power generated at bus $m \in \{1,\ldots,M\}$, $\hat{\ell}_j$ as the load of bus $j \in \{1,\ldots,J\}$, and $\hat{f}_l$ as the transmission flow of line $l \in \{1,\ldots,L\}$. In the case the loads are not flexible, the change in load in the real-time $\Delta\ell_j$ can be ignored. By defining Δp_m as the change in power of generator $m \in \{1,\ldots,M\}$, Δf_l as the change in transmission flow $l \in \{1,\ldots,L\}$, and setting the power vector

$$\Delta\boldsymbol{p} \triangleq [\Delta p_1,\ldots,\Delta p_M]^T, \quad (20)$$

the optimal dispatch is the solution to:

$$\begin{cases} \min\limits_{\Delta\boldsymbol{p}} & \mathbf{1}_M \cdot \boldsymbol{C}(\hat{\boldsymbol{p}} + \Delta\boldsymbol{p}) \\ \text{s.t.} & \mathbf{1}_M \cdot \Delta\boldsymbol{p} = 0 \\ & \Delta p_m^{\min} \leq \Delta p_m \leq \Delta p_m^{\max},\ \ \forall m \in \{1,\ldots,M\} \\ & \Delta f_l \leq 0,\ \ \forall l \in \Omega_+ \\ & \Delta f_l \geq 0,\ \ \forall l \in \Omega_- \end{cases} \quad (21)$$

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

$$\Omega_+ \triangleq \{l \in \{1,\ldots,L\} \mid \hat{f}_l \geq f_l^{\max}\}\ , \quad (22)$$

Ω_- is defined as the negative congestion set

$$\Omega_- \triangleq \{l \in \{1,\ldots,L\} \mid \hat{f}_l \leq f_l^{\min}\}\ , \quad (23)$$

and Ω_0 is defined as the non-congestion set

$$\Omega_0 \triangleq \{l \in \{1,\ldots,L\} \mid f_l^{\min} < \hat{f}_l < f_l^{\max}\}\ . \quad (24)$$

Finally, following the discussions in [14], corresponding to each load bus $j \in \{1,\ldots,J\}$ we define an LMP denoted by λ_j. By defining λ_{ref} as the LMP of a reference bus, the LMPs are given by

$$\lambda_j = \lambda_{\text{ref}} + \boldsymbol{H}_j^T \cdot \boldsymbol{\alpha},\ \forall j \in \{1,\ldots,J\}\ , \quad (25)$$

where $\boldsymbol{H}_j$ represents the j^{th} column of $\boldsymbol{H}$ defined in (2), and $\boldsymbol{\alpha} \triangleq [\alpha_1,\ldots,\alpha_L]^T$ is defined such that α_l is called the *shadow* price corresponding to line l, which dependends on the congestion condition of the corresponding power flow [14], and satisfies

$$\begin{cases} \alpha_l \geq 0, & \text{if } l \in \Omega_+ \\ \alpha_l \leq 0, & \text{if } l \in \Omega_- \\ \alpha_l = 0, & \text{if } l \in \Omega_0 \end{cases}\ . \quad (26)$$

Based on (25), for buses j_1 and j_2 we have

$$\lambda_{j_1} - \lambda_{j_2} = (\boldsymbol{H}_{j_1} - \boldsymbol{H}_{j_2})^T \cdot \boldsymbol{\alpha}\ . \quad (27)$$

D. Profit Model

Based on the LMP model given in Section II-C, next we quantify the attacker's profit. In order to increase competition and liquidity in the electricity market, many SOs (e.g., ISO-New England) allow for virtual bidding at electricity market prices [1]. Virtual-bidding entities are participants in the market with no affiliated generation or load. In this paper, we assume that the attacker is a virtual bidder in an electricity market, who has access to the following two categories of information.

1) Attacker has only partial information about the network dynamics with bounded uncertainties.
2) Attacker knows the states of optimal power generations $\boldsymbol{p}^*$, expected loads $\boldsymbol{\ell}^*$, and the optimal power flows $\boldsymbol{f}^*$ reported by the SOs in the DA market.

The attacker is interested in maximizing its probability of making profitable trades. This can be accomplished by constructing a data injection attack vector $\boldsymbol{z}_a$, which can shift a selected pair of nodal prices in the desired direction from the DA market to the RT market. Specifically, in the DA market, the attacker observes the nodal price results of the DA market, then buys and sells equal amounts of energy P at load locations j_1 and j_2 with nodal price $\lambda_{j_1}^{\text{DA}}$ and $\lambda_{j_2}^{\text{DA}}$, respectively. Subsequently,

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.2017.2695120, IEEE Transactions on Smart Grid

the attack vector $\boldsymbol{z}_a$ is injected in order to shift the RT nodal prices at load locations j_1 and j_2 in the desired directions. In the RT market, the attacker sells and buys equal amounts of energy P at nodal prices, $\lambda_{j_1}^{\mathrm{RT}}$ and $\lambda_{j_2}^{\mathrm{RT}}$, on load buses j_1 and j_2, respectively. Based on such virtual trading strategy and by defining the sets

$$\mathcal{L}_+ \triangleq \{l \in \{1,\cdots,L\}:\ H_{l,j_1} > H_{l,j_2}\}\,, \tag{28}$$

$$\mathcal{L}_- \triangleq \{l \in \{1,\cdots,L\}:\ H_{l,j_1} < H_{l,j_2}\}\,, \tag{29}$$

the profit denoted by $g(\boldsymbol{z}')$ can be formulated as

$$\begin{aligned} g(\boldsymbol{z}') &= (\lambda_{j_1}^{\mathrm{RT}} - \lambda_{j_2}^{\mathrm{RT}} + \lambda_{j_2}^{\mathrm{DA}} - \lambda_{j_1}^{\mathrm{DA}}) \cdot P \\ &= P \sum_{l\in\mathcal{L}_+} (H_{l,j_1} - H_{l,j_2}) \cdot \alpha_l \\ &\quad + P \sum_{l\in\mathcal{L}_-} (H_{l,j_2} - H_{l,j_1}) \cdot \alpha_l \qquad (30) \\ &\quad + \lambda_{j_2}^{\mathrm{DA}} - \lambda_{j_1}^{\mathrm{DA}}\,. \qquad (31) \end{aligned}$$

As shown in [14], the following three conditions suffice to ensure that attacker's profit $g(\boldsymbol{z}')$ is positive:

$$\begin{aligned} &1)\ \lambda_{j_2}^{\mathrm{DA}} - \lambda_{j_1}^{\mathrm{DA}} \geq 0\,; \\ &2)\ \forall l \in \mathcal{L}_+ \text{ we have } \hat{f}_l' > f_l^{\min},\ \text{i.e.,}\ l \notin \Omega_-\,;\ \text{and} \\ &3)\ \forall l \in \mathcal{L}_- \text{ we have } \hat{f}_l' < f_l^{\max},\ \text{i.e.,}\ l \notin \Omega_+, \end{aligned} \tag{32}$$

where $\hat{f}_l'$ denotes the compromised (attacked) estimate of f_l. Since $\hat{f}_l'$ values are random, an attacker cannot ensure that these three conditions are always satisfied. Nevertheless, it can design the attack vector $\boldsymbol{z}_a$ such that the likelihood of meeting these requirements is maximized. Motivated by this, and by following the same line of argument as in [14], we define δ-profitable attacks as follows.

Definition 2: An attack $\boldsymbol{z}_a$ is δ-profitable if the following two conditions are satisfied.

$$\begin{aligned} &\mathbb{E}[\hat{f}_l'] \leq f_l^{\max} - \delta, \quad \forall\, l \in \mathcal{L}_-,\ \text{and}\ \forall \boldsymbol{Q} \in \mathcal{A}(\beta) \\ &\mathbb{E}[\hat{f}_l'] \geq f_l^{\min} + \delta, \quad \forall\, l \in \mathcal{L}_+,\ \text{and}\ \forall \boldsymbol{Q} \in \mathcal{A}(\beta) \end{aligned}\,. \tag{33}$$

It is noteworthy that δ, which we define as *profit confidence*, is not the expected profit from the real electricity market, but rather, it can be interpreted as the safety distance between the expected value of the power flow of lines in the ex-post market after an attack and the limit of the transmission lines. Hence, increasing δ leads to an increased probability that the last two conditions in (32) are not violated. From the attacker's perspective, for each individual line $l \in \{1,\ldots,L\}$, $\hat{f}_l'$ is a random variable, for which we have [14]

$$\mathbb{E}[\hat{f}_l'] = f_l^* + \boldsymbol{e}_l \boldsymbol{H} \boldsymbol{K} \boldsymbol{z}_a\,, \tag{34}$$

where f_l^* is the optimal power flow on line $l \in \{1,\ldots,L\}$ obtained in the DA market.

III. Robust Attack Formulation

Based on the notations and definitions provided in Section II, the attacker's strategy is to find an ε-robust attack vector $\boldsymbol{z}_a$ such that the profit confidence δ is maximized. The attack strategy, as a result, can be found as the solution to:

$$\begin{cases} \max\limits_{\boldsymbol{z}_a \in \mathcal{S}} & \delta \\ \text{s.t.} & \|\boldsymbol{e}_k(\boldsymbol{I}-\boldsymbol{Q})\boldsymbol{z}_a\|_2 \leq \varepsilon,\ \forall \boldsymbol{Q} \in \mathcal{A}(\beta),\ \forall k \\ & \mathbb{E}[\hat{f}_l'] \ \leq\ f_l^{\max} - \delta,\ \forall l \in \mathcal{L}_-,\ \text{and}\ \forall \boldsymbol{Q} \in \mathcal{A}(\beta) \\ & \mathbb{E}[\hat{f}_l'] \ \geq\ f_l^{\min} + \delta,\ \forall l \in \mathcal{L}_+,\ \text{and}\ \forall \boldsymbol{Q} \in \mathcal{A}(\beta) \\ & \delta \ >\ 0 \end{cases} \tag{35}$$

where $\mathcal{S}$ represents the attack vector space, which describes the attack pattern with respect to the type and number of compromised sensors. Note that the problem given in (35) instead of optimizing the profit confidence δ toward a single known network model, which is the case when network information is known to the attackers perfectly, it aims to maximize δ by maintaining inequality constraints for a continuum of all possible network models included in $\mathcal{A}(\beta)$. Hence, the constraints in (35) guarantee that the maximized profit confidence δ will be maintained in the worst case. Therefore, such a design ensures the robustness of the δ-profitable strategy against the uncertainties of the network dynamics.

For each choice of $\boldsymbol{Q} \in \mathcal{A}(\beta)$, the ε-robust and δ-profitable constraints in (35) represent *nonlinear* and *non-convex* constraints on $\boldsymbol{z}_a$. Since there exists an infinite number of matrices $\boldsymbol{Q}$ in $\mathcal{A}(\beta)$, there is an infinite number of such constraints. Hence, (35) is a *semi-infinite* non-convex quadratic program. It is known that such semi-infinite non-convex quadratic programming problems are NP-hard in their most general form. However, as we will show next, due to the special structure of the constraints in the problem at hand, the problem (35) can be reformulated as a convex SDP problem, and solved efficiently in polynomial time via the well-established interior point method.

IV. Robust Attack under Limited Information

In this section, through solving (35) we develop an optimal approach for the attacker that is robust against any arbitrary uncertainty superimposed onto the true network dynamic model. For this purpose, we show that the problem (35) can be equivalently cast as a convex SDP problem. Specifically, we show how the ε-robust constraints can be converted to proper semi-definite constraints, and the δ-profitable constraints can be converted to equivalent quadratic ones.

A. δ-profitable Constraints

We first provide the following proposition, which facilitates expressing the dependence of the δ-profitable constraints, defined in (33), on $\boldsymbol{Q}$.

Proposition 1: Matrices $\boldsymbol{H}$ and $\boldsymbol{H}_s$ defined in (2) and (3), respectively, are related according to

$$\boldsymbol{H} = [\boldsymbol{0}_{L\times N} \quad \boldsymbol{I}_L]\boldsymbol{H}_s. \tag{36}$$

Based on Proposition 1, (34) can be expressed as

$$\mathbb{E}[\hat{f}_l'] \overset{(34)}{=} f_l^* + \boldsymbol{e}_l[\boldsymbol{0} \quad \boldsymbol{I}]\boldsymbol{H}_s\boldsymbol{K}\boldsymbol{z}_a\,, \quad \text{for}\ l \in \{1,\ldots,L\}\,. \tag{37}$$

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.2017.2695120, IEEE Transactions on Smart Grid

By recalling that $\boldsymbol{Q} \triangleq \boldsymbol{H}_s\boldsymbol{K}$, we equivalently have

$$\mathbb{E}[\hat{f}_l'] = f_l^* + \boldsymbol{e}_l[\boldsymbol{0} \quad \boldsymbol{I}]\boldsymbol{Q}\boldsymbol{z}_a. \tag{38}$$

Hence, the δ-profitable constraints given in (33) can be rewritten as

$$\begin{matrix} f_l^* + \boldsymbol{e}_l[\boldsymbol{0} \quad \boldsymbol{I}]\boldsymbol{Q}\boldsymbol{z}_a \le f_l^{\max} - \delta, \ \forall l \in \mathcal{L}_-, \text{ and } \forall \boldsymbol{Q} \in \mathcal{A}(\beta) \\ f_l^* + \boldsymbol{e}_l[\boldsymbol{0} \quad \boldsymbol{I}]\boldsymbol{Q}\boldsymbol{z}_a \ge f_l^{\min} + \delta, \ \forall l \in \mathcal{L}_+, \text{ and } \forall \boldsymbol{Q} \in \mathcal{A}(\beta) \end{matrix},$$

which in turn can be equivalently re-stated as

$$\begin{matrix} \sup\limits_{\boldsymbol{Q}\in\mathcal{A}(\beta)} \{\boldsymbol{e}_l[\boldsymbol{0} \quad \boldsymbol{I}]\boldsymbol{Q}\boldsymbol{z}_a\} \le f_l^{\max} - \delta - f_l^*, \ \forall l \in \mathcal{L}_- \\ \inf\limits_{\boldsymbol{Q}\in\mathcal{A}(\beta)} \{\boldsymbol{e}_l[\boldsymbol{0} \quad \boldsymbol{I}]\boldsymbol{Q}\boldsymbol{z}_a\} \ge f_l^{\min} + \delta - f_l^*, \ \forall l \in \mathcal{L}_+ \end{matrix}. \tag{39}$$

The following theorem provides closed-form representations for these two constraint by converting the semi-infinite non-convex δ-profitable constraints to tractable quadratic constraints.

Theorem 1: The δ-profitable constraints in (33) can be equivalently stated as

$$\begin{matrix} \beta\|\boldsymbol{z}_a\|_2 + \tilde{\boldsymbol{q}}_l\boldsymbol{z}_a \le -\delta - f_l^* + f_l^{\max}, \quad \forall l \in \mathcal{L}_- \\ \beta\|\boldsymbol{z}_a\|_2 - \tilde{\boldsymbol{q}}_l\boldsymbol{z}_a \le -\delta + f_l^* - f_l^{\min}, \quad \forall l \in \mathcal{L}_+ \end{matrix}, \tag{40}$$

where we have defined

$$\tilde{\boldsymbol{q}}_l \triangleq \boldsymbol{e}_l[\boldsymbol{0} \quad \boldsymbol{I}]\tilde{\boldsymbol{Q}}\,. \tag{41}$$

Proof: See Appendix A. ∎

Based on this theorem, the δ-profitable constraints are converted to two quadratic constraints depending only on $\boldsymbol{z}_a$.

B. ε-Robust Constraints

Next we show that the semi-infinite non-convex quadratic constraints (17) can be converted to linear matrix inequality (LMI) constraints.

Theorem 2: The constraints

$$\|\boldsymbol{e}_k(\boldsymbol{I} - \boldsymbol{Q})\boldsymbol{z}_a\|_2 \le \varepsilon, \ \forall \boldsymbol{Q} \in \mathcal{A}(\beta), \ \forall k \in \{1, \ldots, K\} \tag{42}$$

can be can be satisfied if and only if there exists a $\gamma \ge 0$ such that for $\forall k \in \{1, \ldots, K\}$

$$\boldsymbol{T}_k \triangleq \begin{bmatrix} \varepsilon^2 & \boldsymbol{z}_a^T(\boldsymbol{I} - \tilde{\boldsymbol{Q}})^T\boldsymbol{e}_k^T & -\beta\boldsymbol{z}_a^T \\ \boldsymbol{e}_k(\boldsymbol{I} - \tilde{\boldsymbol{Q}})\boldsymbol{z}_a & 1 - \gamma & \boldsymbol{0} \\ -\beta\boldsymbol{z}_a & \boldsymbol{0} & \gamma\boldsymbol{I} \end{bmatrix} \succeq 0\,, \tag{43}$$

i.e., $\boldsymbol{T}_k$ is semi-positive definite.

Proof: See Appendix B. ∎

Hence, the semi-infinite non-convex quadratic constraints in (17) are converted to equivalent LMIs in which matrices $\boldsymbol{T}_k$ depends linearly on parameters $\boldsymbol{z}_a$ and γ, which we aim to optimize. As a result, theorems 1 and 2 conclude that the semi-infinite non-convex quadratic programming problem (35) can be equivalently cast an SDP problem as follows.

$$\begin{cases} \max\limits_{\boldsymbol{z}_a\in\mathcal{S},\gamma\ge 0} & \delta \\ \text{s.t.} & \boldsymbol{T}_k \succeq 0, \ \forall k \in \{1, \ldots, K\} \\ & \beta\|\boldsymbol{z}_a\|_2 + \tilde{\boldsymbol{q}}_l\boldsymbol{z}_a \ \le \ -\delta - f_l^* + f_l^{\max}, \ \forall l \in \mathcal{L}_- \\ & \beta\|\boldsymbol{z}_a\|_2 - \tilde{\boldsymbol{q}}_l\boldsymbol{z}_a \ \le \ -\delta + f_l^* - f_l^{\min}, \ \forall l \in \mathcal{L}_+ \\ & \delta \ > \ 0 \end{cases} \tag{44}$$

Hence, in summary, we converted the worst-case robust attack design problem formulized in (35) into a semi-definite convex problem (44). Even though these problems are mathematically equivalent, the original problem (35) is computationally intractable, whereas the semi-definite convex problem (44) can be solved using standard and efficient interior point method software tools, e.g., [34].

V. Numerical Evaluations

In this section we provide numerical evaluations in the IEEE 14 and IEEE 118 bus systems to assess the impacts of the FDIAs on the RT electricity markets, where the attacks are designed by limited adversaries, which face network dynamic uncertainties. In the simulations, we consider both AC and DC power flow models. In all simulations, we set the ε-robust threshold to $\varepsilon = 0.5$, and define $\xi \triangleq \beta/\|\boldsymbol{Q}\|_2$ to capture the relative uncertainty level of the actual network dynamics from the attacker's perspective. All the simulations are conducted using Matlab-based software packages including MATPOWER [35] and convex programming solver CVX [34].

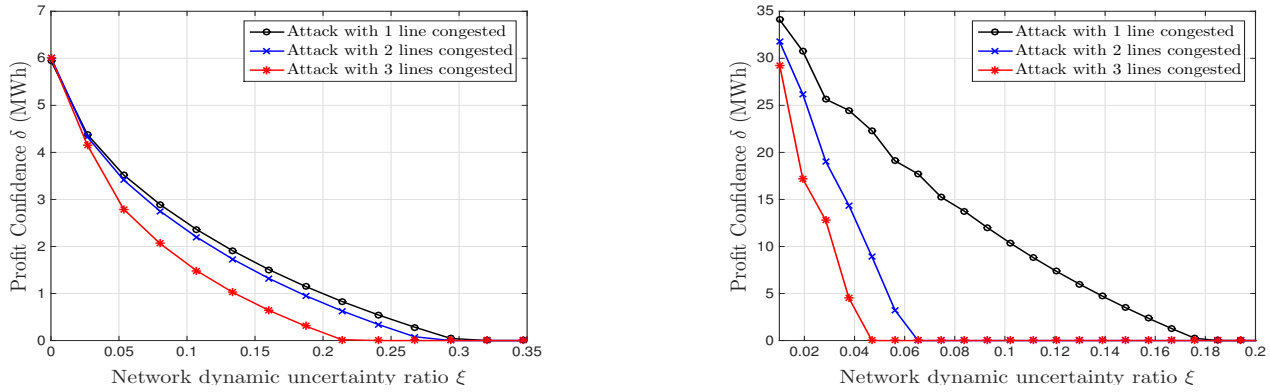
A. Varying Degree of Uncertainties

In order to assess the connection between the profit confidence δ and the network dynamic uncertainty ratio ξ, we first focus on settings in which different numbers of transmission lines are congested. Figures 1(a) and 1(b) demonstrate the variations of profit confidence δ with respect to the network dynamic uncertainty ratio ξ in the IEEE 14- and 118-bus systems, respectively. It is observed that under the perfect knowledge of network dynamics ($\xi = 0$), the profit confidence takes its maximum values. For instance, in the 14-bus system, when the line connecting buses 2 and 4 is congested, we have $\delta = 6$MWh. With the increasing uncertainty ratio ξ, profit confidence δ decreases monotonically and reaches 0MWh when the uncertainty ratio reaches $\xi = 0.3$. The reason underlying this observation is that the attack vector $\boldsymbol{z}_a$ must satisfy the ε-robust constraints

$$\sup_{\boldsymbol{Q}\in\mathcal{A}(\beta)} \|\boldsymbol{e}_k(\boldsymbol{I} - \boldsymbol{Q})\boldsymbol{z}_a\|_2 \le \varepsilon, \ \forall k \in \{1, \ldots, K\}\,, \tag{45}$$

based on which as uncertainty β (or equivalently ξ) increases, the region $\mathcal{A}(\beta)$ defined in (14) expands. As a result, since the attack vector $\boldsymbol{z}_a$ must satisfy the constraint in (45) for $\forall k \in \{1, \ldots, K\}$, the constraint $\|\boldsymbol{e}_k(\boldsymbol{I} - \boldsymbol{Q})\boldsymbol{z}_a\|_2 \le \varepsilon$ for all numbers of $\mathcal{A}(\beta)$, the room for the injected attack vector $\boldsymbol{z}_a$, and subsequently, the attacker's ability to manipulate the state estimates, shrinks rapidly. Hence, beyond a certain uncertainty ratio ξ, the attacks cannot affect the LMPs in the RT markets.

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.2017.2695120, IEEE Transactions on Smart Grid



(a) IEEE 14-bus

(b) IEEE 118-bus

Fig. 1: Profit confidence δ versus network dynamic uncertainty ratio ξ for different number of congested lines.

Furthermore, Fig. 1(a) and Fig. 1(b) depict the variations of δ versus ξ for different settings with 1, 2, and 3 congested transmission lines. It is observed that as the number of congested transmission lines increases, for increasing uncertainty ratio ξ, profit confidence δ declines faster. The underlying reason is that attack vector $\boldsymbol{z}_a$ is also limited by the δ-profitable constraints (33). Therefore, as the number of lines in congestion increases, the attackers have to relieve a larger system congestion pattern, which enforces stricter requirements for the design of the attack vector $\boldsymbol{z}_a$. Consequently, it lowers the potential to make profit by maliciously placing FDIAs in order to relieve the certain congested transmission lines.

B. Attacked Power Flow

In this experiment, we aim to investigate the relationship between the expected attacked power flow $\mathbb{E}[\hat{f}_l']$ and the network dynamic uncertainty ratio ξ. To illustrate this, we select two transmissions lines in the IEEE 14-bus, one connecting buses 2 and 4, and the second one connecting buses 2 and 5. Recall that the mean of the attacked power flow on individual line $l \in \{1, \ldots, L\}$ can be expressed as

$$\mathbb{E}[\hat{f}_l'] = f_l^* + \boldsymbol{e}_l[\boldsymbol{0} \quad \boldsymbol{I}]\boldsymbol{Q}\boldsymbol{z}_a \,. \tag{46}$$

In this experiment, the optimal line flows from bus 2 to bus 4 and from bus 2 to bus 5 are $f_{2-4}^* = 55.04$ MWh and $f_{2-5}^* = 40.82$ MWh, respectively. When an adversary launches profitable attack by injecting attack vector $\boldsymbol{z}_a$, the expected attacked power flows $\mathbb{E}[\hat{f}_l']$ are shifted to lower values to relieve the positive congestion. Table I provides the attacked power flow results and the specific injected attack data on relevant meters when the attacker's uncertainty ratio is $\xi = 0.05$. From Table I, it is observed that with the increasing uncertainty ratio ξ, the expected attacked power flows $\mathbb{E}[\hat{f}_{2-4}']$ and $\mathbb{E}[\hat{f}_{2-5}']$ rise monotonically until coinciding with the optimal power flow f_{2-4}^* and f_{2-5}^* in the DA market, respectively. In other words, the ability for such attack vector to relieve the positive congestion weakens along with the attacker's raising uncertainty about network dynamics. This observation can be explained by noting that due to increasing uncertainty ratio reduces the magnitude of attack inputs $\boldsymbol{z}_a$ based on (45). Accordingly, in (46), the attack effect term $\boldsymbol{e}_l[\boldsymbol{0} \quad \boldsymbol{I}]\boldsymbol{Q}\boldsymbol{z}_a$ shrinks and the expected attacked power flows $\mathbb{E}[\hat{f}_l']$ approach to the optimal power flows f_l^* in the DA market. This table also shows the LMPs before and after attacks.

TABLE I: Power flow in the IEEE 14-bus system

	Attack-free	Attack with $\xi = 0.05$
$\boldsymbol{z}_a(2)$	0	18.21
$\boldsymbol{z}_a(4)$	0	16.88
$\boldsymbol{z}_a(5)$	0	5.53
f_{2-4}^*	55.04 MWh	47.73 MWh
f_{2-5}^*	40.82 MWh	35.43 MWh
λ_2	34.87\$/MWh	36.47\$/MWh
λ_4	32.99\$/MWh	35.28\$/MWh
λ_5	33.14\$/MWh	35.46\$/MWh

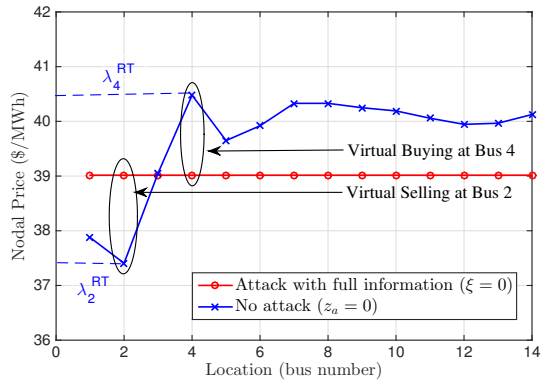
C. Locational Marginal Prices

Next, we evaluate the impact of the FDIAs under uncertainty on the LMPs in the RT market. We assume that in the DA market, a number of transmission lines are congested. If the attacker can distort enough number of state parameters, the congested lines in the system will be relieved completely with confidence, which forces the LMPs at each bus to stay uniform in the RT market. Combining with virtual bidding, such attacks can bring financial profit to the attacker. To illustrate the effect of network dynamic uncertainties on the attacker's potential financial gain, we denote the profit confidence when network dynamics are fully known ($\xi = 0$) by δ_0, which is the profit confidence when congested lines are relieved completely. As uncertainty ratio increases, profit confidence 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.

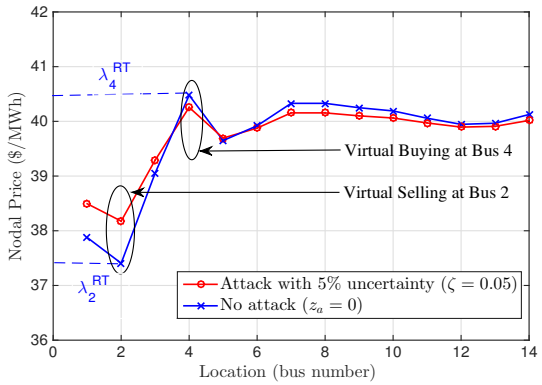
We provide Fig. 2(a) and Fig. 2(b) to demonstrate the virtual bidding profits with and without network dynamic uncertainties, i.e., $\xi = 0.05$ and $\xi = 0$, respectively. In both cases, only one line (connecting buses 2 and 4) is congested. In the DA market, the attacker chooses to buy and sell the same amount of virtual energy at buses 2 and 4, respectively. After launching FDIAs, the attacker chooses to sell and buy the same amount of virtual energy at the corresponding buses, respectively.

Figures 3(a) and 3(b) illustrate the LMPs in the RT with and without attacks under different degrees of uncertainties in the

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.2017.2695120, IEEE Transactions on Smart Grid

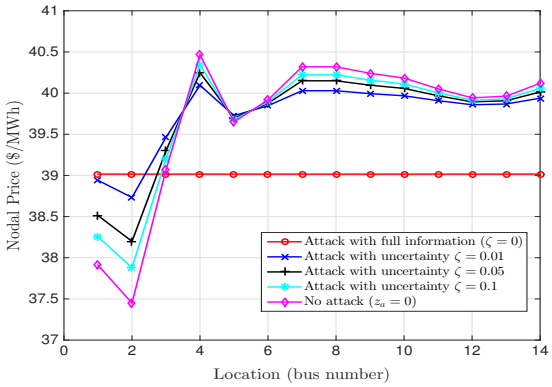


(a) Attack with full information.

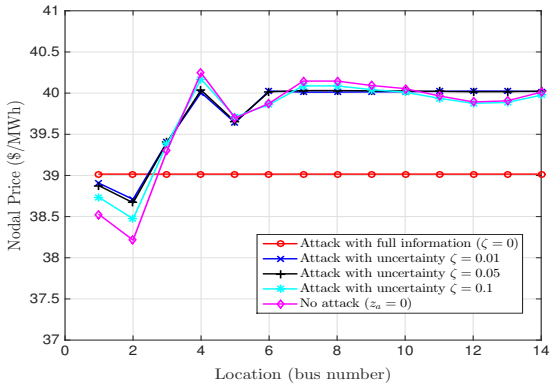


(b) Attack with uncertainty ratio $\xi = 0.05$.

Fig. 2: Real-time LMPs of different buses in attack-free and adversarial settings.



(a) One congested line.



(b) Two congested lines.

Fig. 3: LMPs with and without attack versus varying uncertainty ratios.

IEEE 14-bus system. In Fig. 3(a) only one line is congested, while Fig. 3(b) focuses on a setting in which two lines are congested. In both figures, the "no attack" setting represents the attack-free operation of the grid, i.e., $\boldsymbol{z}_a = 0$, in which case the LMPs on each bus are the same in both markets and there exists no virtual bidding profit. On the other hand, when an attack is launched, the "attack with full information" represents the settings in which the attackers have complete information about the grid, i.e. $\xi = 0$, in which case, the attacker can relieve the congested lines in the RT market. As we can observe in both cases, when uncertainty ratio increases, the LMPs in the RT approach to the ones in the DA market, as increasing uncertainty leads to increasingly incomplete relief of the congested lines. As shown in Fig. 4, if the attacker continues on virtual bidding at buses 2 and 4, its profit reduces with the increasing uncertainty ratio ξ, and reaches $\$0/\text{MWh}$ beyond the uncertainty level $\xi \approx 0.2$.

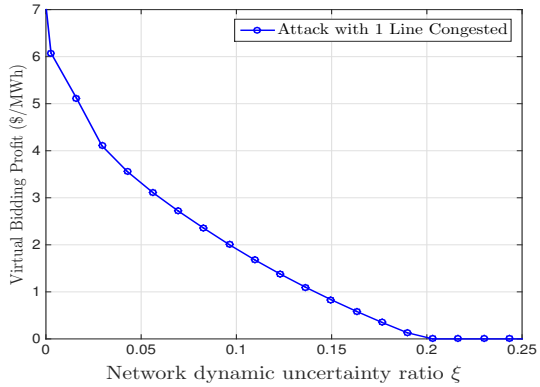


Fig. 4: Virtual bidding profit $g(\boldsymbol{z}')$ versus uncertainty ratio ξ.

D. Limited Access for Compromising the Sensors

In this subsection, we consider the settings in which the attacker can distort only a limited number of measurement units (sensors). This indicates that the 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 meters on the profit confidence. 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. 1(a) we observe that when the attacker can compromise any desired number of sensors, the profit confidence δ decreases as attacker's uncertainty ratio increases. The same trend is valid when a limited number

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.2017.2695120, IEEE Transactions on Smart Grid

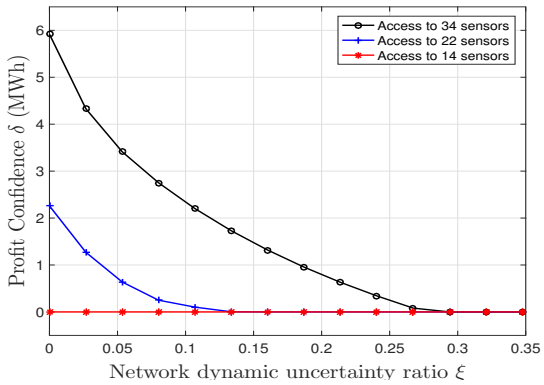


Fig. 5: Different number of sensors compromised.

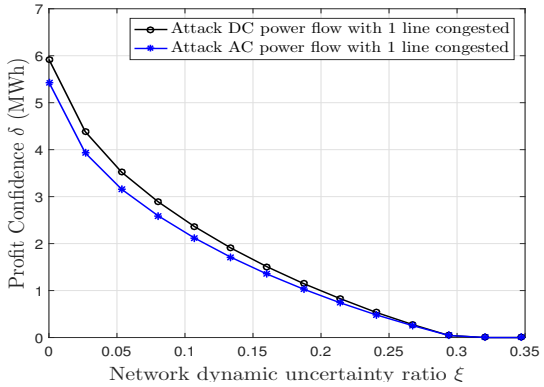


Fig. 6: DC and AC power flow comparison.

of sensors can be compromised due to the same reason that the expanding network dynamic uncertainty shrinks the room to inject the attack vector. Figure 5 depicts variations of δ with respect to ξ when the attacker can compromise a limited number of sensors. It shows that for any given uncertainty ratio ξ, compromising fewer number of sensors leads to smaller profit confidences. It can be explained by that besides the attackers' restriction from ε-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 any uncertainty ratio, when fewer limited sensors are compromised, it is less likely for the attacker to inject attack vector to be both undetectable and profitable in the RT market. Even with perfect knowledge of network information, by compromising fewer sensors the attacker cannot even remain undetectable by the BDDs [11]. Thus, for any given uncertainty ratio, when the compromised sensors are fewer than a critical number, it is impossible for the attacker to launch ε-robust, and thus profitable, attacks in the RT market.

E. DC designed FDIAs with AC Power Flows

In this subsection, we evaluate the validity of the assumption of 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 with both DC and AC power flow models. Fig. 6 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 is only slightly smaller compared to DC model. As the uncertainty level increases, the discrepancy between AC and DC model diminishes and becomes negligible.

VI. Conclusion

In this paper, we have analyzed the impact of false data injection attacks on the locational marginal prices of the real-time market, when the attackers have incomplete information about the grid. Specifically, we have modeled the discrepancy between the actual network dynamics and the one known to the attackers to be confined within a measure of bounded error, and we have introduced an attack strategy in which the attackers are ensured worst-case robustness against uncertainties about grid dynamics. We have shown that even with bounded uncertainty on network dynamics, an attacker can still manipulate nodal prices of the real-time markets without being detected by the bad data detectors. Combining with virtual bidding mechanism, the attackers can still make profit from such attacks. We have shown that designing such worst-case robust attacks involves solving a semi-infinite non-convex problem, which is NP-hard in its most general form. However, we have demonstrated that by leveraging the additional structure of the robust attack design problem, it can be transformed to an equivalent convex semi-definite programming problem. Simulation results have been provided in IEEE 14- and 118-bus systems.

Appendix A
Proof of Theorem 1

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

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

The constraints associated with lines $l \in \mathcal{L}_-$, described in (39), are

$$\sup_{\boldsymbol{Q}\in\mathcal{A}(\beta)} \{\boldsymbol{e}_l[\boldsymbol{0} \quad \boldsymbol{I}]\boldsymbol{Q}\boldsymbol{z}_a\} \leq f_l^{\max} - \delta - f_l^*, \ \forall l \in \mathcal{L}_- \ . \quad (47)$$

By invoking the expansion $\boldsymbol{Q} = \tilde{\boldsymbol{Q}} + \Delta\boldsymbol{Q}$, the left-hand side of this constraint can be equivalently stated as

$$\boldsymbol{e}_l[\boldsymbol{0} \quad \boldsymbol{I}]\tilde{\boldsymbol{Q}}\boldsymbol{z}_a + \sup_{\Delta\boldsymbol{Q}\in\mathcal{C}(\beta)} \{\boldsymbol{e}_l[\boldsymbol{0} \quad \boldsymbol{I}]\Delta\boldsymbol{Q}\boldsymbol{z}_a\} \ . \quad (48)$$

Next, for all $l \in \mathcal{L}_-$ we define

$$\Delta\boldsymbol{q}_l \triangleq \boldsymbol{e}_l[\boldsymbol{0} \quad \boldsymbol{I}]\Delta\boldsymbol{Q} \ , \quad (49)$$

which captures the $(N+l)^{\text{th}}$ row of $\Delta\boldsymbol{Q}$, and as a result, $\Delta\boldsymbol{q}_l \in \mathcal{C}(\beta)$. By leveraging this observation and applying the Cauchy-Schwartz inequality we have

$$\boldsymbol{e}_l[\boldsymbol{0} \quad \boldsymbol{I}]\Delta\boldsymbol{Q}\boldsymbol{z}_a \overset{(49)}{=} \Delta\boldsymbol{q}_l\boldsymbol{z}_a$$

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.2017.2695120, IEEE Transactions on Smart Grid

$$\begin{aligned} &\leq |\Delta \boldsymbol{q}_l \boldsymbol{z}_a| \\ &\overset{(13)}{\leq} \|\Delta \boldsymbol{q}_l\|_2 \cdot \|\boldsymbol{z}_a\|_2 \\ &\leq \beta \|\boldsymbol{z}_a\|_2 \ , \end{aligned} \tag{50}$$

where the inequality holds with equality for realization

$$\Delta \boldsymbol{q}_l = \beta \cdot \frac{\boldsymbol{z}_a}{\|\boldsymbol{z}_a\|_2} \ . \tag{51}$$

Hence, we obtain

$$\sup_{\Delta \boldsymbol{Q} \in \mathcal{C}(\beta)} \{\boldsymbol{e}_l [\boldsymbol{0} \quad \boldsymbol{I}] \Delta \boldsymbol{Q} \boldsymbol{z}_a\} = \beta \|\boldsymbol{z}_a\|_2 \ . \tag{52}$$

The expression in (48) in conjunction with (52) establishes that $l \in \mathcal{L}_-$, the infinite non-convex linear constraint in (39) is equivalent to the following quadratic constraint

$$\sup_{\Delta \boldsymbol{Q} \in \mathcal{C}(\beta)} \{\boldsymbol{e}_l [\boldsymbol{0} \quad \boldsymbol{I}] (\tilde{\boldsymbol{Q}} + \Delta \boldsymbol{Q}) \boldsymbol{z}_a\} = \beta \|\boldsymbol{z}_a\|_2 + \boldsymbol{e}_l [\boldsymbol{0} \quad \boldsymbol{I}] \tilde{\boldsymbol{Q}} \boldsymbol{z}_a \ . \tag{53}$$

and therefore, $\forall l \in \mathcal{L}_-$

$$\beta \|\boldsymbol{z}_a\|_2 + \boldsymbol{e}_l [\boldsymbol{0} \quad \boldsymbol{I}] \tilde{\boldsymbol{Q}} \boldsymbol{z}_a \leq -\delta - f_l^* + f_l^{\max} \ , \tag{54}$$

which is the desired result.

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

By following the same line of arguments, we can show that

$$\begin{aligned} \boldsymbol{e}_l [\boldsymbol{0} \quad \boldsymbol{I}] \Delta \boldsymbol{Q} \boldsymbol{z}_a &= \Delta \boldsymbol{q}_l \boldsymbol{z}_a \\ &\geq -|\Delta \boldsymbol{q}_l \boldsymbol{z}_a| \\ &\geq -\|\Delta \boldsymbol{q}_l\|_2 \cdot \|\boldsymbol{z}_a\|_2 \\ &\geq -\beta \|\boldsymbol{z}_a\|_2 \ , \end{aligned} \tag{55}$$

which establishes that

$$\inf_{\Delta \boldsymbol{Q} \in \mathcal{C}(\beta)} \{\boldsymbol{e}_l [\boldsymbol{0} \quad \boldsymbol{I}] \Delta \boldsymbol{Q} \boldsymbol{z}_a\} = -\beta \|\boldsymbol{z}_a\|_2 \ , \tag{56}$$

and subsequently, $\forall l \in \mathcal{L}_+$

$$\beta \|\boldsymbol{z}_a\|_2 - \boldsymbol{e}_l [\boldsymbol{0} \quad \boldsymbol{I}] \tilde{\boldsymbol{Q}} \boldsymbol{z}_a \leq -\delta + f_l^* - f_l^{\min}, \forall l \in \mathcal{L}_+. \tag{57}$$

APPENDIX B
PROOF OF THEOREM 2

We first provide the following two lemmas by leveraging which we show that the ε-robust constraints

$$\|\boldsymbol{e}_k (\boldsymbol{I} - \boldsymbol{Q}) \boldsymbol{z}_a\|_2 \leq \varepsilon, \ \forall \boldsymbol{Q} \in \mathcal{A}(\beta), \ \forall k \in \{1, \ldots, K\} \tag{58}$$

which are infinite non-convex constraints, can be transformed to equivalent semi-definite constraints.

Lemma 1 (Shur Complement Lemma): Let $\boldsymbol{S}$ be a symmetric matrix partitioned into blocks

$$\boldsymbol{S} = \begin{bmatrix} \boldsymbol{A} & \boldsymbol{B}^T \\ \boldsymbol{B} & \boldsymbol{C} \end{bmatrix} \ , \tag{59}$$

where both $\boldsymbol{A}$ and $\boldsymbol{C}$ are symmetric and square. Then with $\boldsymbol{C} \succ 0$, $\boldsymbol{S} \succeq 0$ if and only if $\Delta \boldsymbol{C} \succeq 0$, where $\Delta \boldsymbol{C}$ is the Schur complement of $\boldsymbol{C}$ in $\boldsymbol{S}$ and is given by

$$\Delta \boldsymbol{C} = \boldsymbol{A} - \boldsymbol{B}^T \boldsymbol{C}^{-1} \boldsymbol{B} \ . \tag{60}$$

Proof: See [36]. ■

Now, by recalling that $\boldsymbol{Q} = \tilde{\boldsymbol{Q}} + \Delta \boldsymbol{Q}$, the constraints in (17) are equivalent to, for $\forall k \in \{1, \ldots, K\}$,

$$\boldsymbol{z}_a^T [\boldsymbol{I} - (\tilde{\boldsymbol{Q}} + \Delta \boldsymbol{Q})]^T \boldsymbol{e}_k^T \boldsymbol{e}_k [\boldsymbol{I} - (\tilde{\boldsymbol{Q}} + \Delta \boldsymbol{Q})] \boldsymbol{z}_a \leq \varepsilon^2, \ \forall \Delta \boldsymbol{Q} \in \mathcal{C}(\beta) \ . \tag{61}$$

By applying the Schur Complement lemma we find that for $\forall k \in \{1, \ldots, K\}$, the constraints

$$\begin{bmatrix} \varepsilon^2 & \boldsymbol{z}_a^T (\boldsymbol{I} - (\tilde{\boldsymbol{Q}} + \Delta \boldsymbol{Q}))^T \boldsymbol{e}_k^T \\ \boldsymbol{e}_k (\boldsymbol{I} - (\tilde{\boldsymbol{Q}} + \Delta \boldsymbol{Q})) \boldsymbol{z}_a & 1 \end{bmatrix} \succeq 0 \tag{62}$$

hold if and only if

$$\boldsymbol{A} \geq \boldsymbol{B}^T \Delta \boldsymbol{Q} \boldsymbol{C} + \boldsymbol{C}^T \Delta \boldsymbol{Q}^T \boldsymbol{B}^T, \ \forall k \in \{1, \ldots, K\} \ , \tag{63}$$

where we have defined

$$\begin{aligned} \boldsymbol{A} &\triangleq \begin{bmatrix} \varepsilon^2 & \boldsymbol{z}_a^T (\boldsymbol{I} - \tilde{\boldsymbol{Q}})^T \boldsymbol{e}_k^T \\ \boldsymbol{e}_k (\boldsymbol{I} - \tilde{\boldsymbol{Q}}) \boldsymbol{z}_a & 1 \end{bmatrix}, \\ \boldsymbol{B} &\triangleq [\boldsymbol{0}_{(L+N) \times 1} \quad \boldsymbol{I}_{L+N}] \ , \\ \text{and } \boldsymbol{C} &\triangleq [\boldsymbol{z}_a \quad \boldsymbol{0}] \ . \end{aligned}$$

The constraints in (63) should be maintained $\forall \Delta \boldsymbol{Q} \in \mathcal{C}(\beta)$. We provide the following lemma to characterize constraints that are equivalent to (63) holding for all $\Delta \boldsymbol{Q} \in \mathcal{C}(\beta)$.

Lemma 2: For any given matrices $\boldsymbol{U}$, $\boldsymbol{V}$, and $\boldsymbol{Y}$ with $\boldsymbol{U} = \boldsymbol{U}^T$, the inequality

$$\boldsymbol{U} \succeq \boldsymbol{V}^T \boldsymbol{Z} \boldsymbol{Y} + \boldsymbol{Y}^T \boldsymbol{Z}^T \boldsymbol{V}, \quad \forall \boldsymbol{Z} : \|\boldsymbol{Z}\|_2 \leq \rho \tag{64}$$

holds if and only if there exists a $\gamma \geq 0$ such that

$$\begin{bmatrix} \boldsymbol{U} - \gamma \boldsymbol{V}^T \boldsymbol{V} & -\rho \boldsymbol{Y}^T \\ -\rho \boldsymbol{Y} & \gamma \boldsymbol{I} \end{bmatrix} \succeq 0 \ . \tag{65}$$

Proof: See [37]. ■

Next, applying Lemma 2 provides that (63) hold if and only if there exists $\gamma \geq 0$ such that for $\forall k \in \{1, \ldots, K\}$,

$$\boldsymbol{T}_k \triangleq \begin{bmatrix} \varepsilon^2 & \boldsymbol{z}_a^T (\boldsymbol{I} - \tilde{\boldsymbol{Q}})^T \boldsymbol{e}_k^T & -\beta \boldsymbol{z}_a^T \\ \boldsymbol{e}_k (\boldsymbol{I} - \tilde{\boldsymbol{Q}}) \boldsymbol{z}_a & 1 - \gamma & \boldsymbol{0} \\ -\beta \boldsymbol{z}_a & \boldsymbol{0} & \gamma \boldsymbol{I} \end{bmatrix} \succeq 0 \ , \tag{66}$$

Equation (62) in conjunction with (66) establish that the ε-robust constraints in (17) can be equivalently cast as $\boldsymbol{T}_k \succeq 0$, for $\forall k \in \{1, \ldots, K\}$, which are SDP constraints.

REFERENCES

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

[2] A. J. Wood and B. F. Wollenberg, *Power generation, operation, and control*. John Wiley and Sons, 2012.

[3] 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.

[4] 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.

[5] M. Negrete-Pincetic, F. Yoshida, and G. Gross, "Towards quantifying the impacts of cyber attacks in the competitive electricity market environment," in *Proc. IEEE PowerTech Conference*, Bucharest, Romania, Jun. 2009, pp. 1–8.

[6] F. Pasqualetti, F. Dorfler, and F. Bullo, "Cyber-physical attacks in power networks: Models, fundamental limitations and moni-

tor design," in *Proc. IEEE Conference on Decision and Control*, Orlando, FL, Dec. 2011, pp. 2195–2201.

[7] 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.

[8] T. B. Smith, "Electricity theft: a comparative analysis," *Energy Policy*, vol. 32, no. 18, pp. 2067–2076, Dec. 2004.

[9] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber–physical system security for the electric power grid," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 210 – 224, Jan. 2012.

[10] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," *Future Generation Computer Systems*, vol. 28, no. 3, pp. 583–592, Mar. 2012.

[11] 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.

[12] T. T. Kim and H. V. Poor, "Strategic Protection Against Data Injection Attacks on Power Grids," *IEEE Transactions on Smart Grid*, vol. 2, no. 2, pp. 326 – 333, June 2011.

[13] F. Borges de Oliveira, *On Privacy-Preserving Protocols for Smart Metering Systems*. Springer International Publishing, 2017.

[14] 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.

[15] 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.

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

[17] 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.

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

[19] 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.

[20] 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.

[21] 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.

[22] H. Li and Z. Han, "Manipulating the electricity power market via jamming the price signaling in smart grid," in *Proc. IEEE Global Communications Conference*, Houston, TX, Dec. 2011, pp. 1168–1172.

[23] L. Jia, R. Thomas, and L. Tong, "On the nonlinearity effects on malicious data attack on power system," in *Proc.IEEE Power and Energy Society General Meeting*, San Diego, CA, Jul. 2012, pp. 1–8.

[24] D.-H. Choi and L. Xie, "Sensitivity Analysis of Real-Time Locational Marginal Price to SCADA Sensor Data Corruption," *IEEE Transactions on Power Systems*, vol. 29, no. 3, pp. 1110–1120, May 2014.

[25] 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.

[26] A. Tajer, S. Kar, H. V. Poor, and S. Cui, "Distributed joint cyber attack detection and state recovery in smart grids," in *Proc. IEEE International Conference on Smart Grid Communications*, Brussels, Belgium, Oct. 2011, pp. 202–207.

[27] A. Anwar, A. N. Mahmood, and M. Pickering, "Data-driven stealthy injection attacks on smart grid with incomplete measurements," in *Proc. Pacific-Asia Workshop on Intelligence and Security Informatics*, Mar. 2016, pp. 180–192.

[28] M. R. Garey and D. S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness*. New York, NY: W. H. Freeman and Co., 1979.

[29] Y. Nesterov and A. Nemirovskii, *Interior-Point Polynomial Algorithms in Convex Programming*. Philadelphia, PA: Society for Industrial and Applied Mathematics, 1994.

[30] F. Wu, P. Varaiya, P. Spiller, and S. Oren, "Folk theorems on transmission access: Proofs and counterexamples," *Journal of Regulatory Economics*, vol. 10, no. 1, pp. 5–23, 1996.

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

[32] 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.

[33] A. Abur, "A bad data identification method for linear programming state estimation," *IEEE Transactions on Power Systems*, vol. 5, no. 3, pp. 894–901, Aug. 1990.

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

[35] 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.

[36] R. A. Horn and C. R. Johnson, *Matrix Analysis*. New York, NY: Cambridge University Press, 1986.

[37] Y. Eldar and N. Merhav, "A competitive minimax approach to robust estimation of random parameters," *IEEE Transactions on Signal Processing*, vol. 52, no. 7, pp. 1931–1946, Jul. 2004.

Mateo R. Mengis (M'11) received the B.S. degree in Electrical Engineering from Oregon State University, Corvallis, OR, USA in 2009 and the M.Eng. degree in Computer & Systems Engineering from Rensselaer Polytechnic Institute, Troy, NY, USA in 2015.

From 2009 to 2014, he was employed as a Control Systems Engineer for the U. S. Army Corps of Engineers' Hydroelectric Design Center in Portland, OR. He has design and installation experience with diesel generators, station service power distribution systems, SCADA systems, and digital governors for hydroelectric powerhouses. He is currently the Chief of the Control Systems Section for the Hydroelectric Design Center.

Mr. Mengis is a Registered Professional Engineer in the State of California.

Ali Tajer (S'05, M'10, SM'15) 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 has previously 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 an NSF CAREER award in 2016.