Ramp-Induced Data Attacks on Look-Ahead Dispatch in Real-Time Power Markets

Dae-Hyun Choi, *Student Member, IEEE*, and Le Xie, *Member, IEEE*

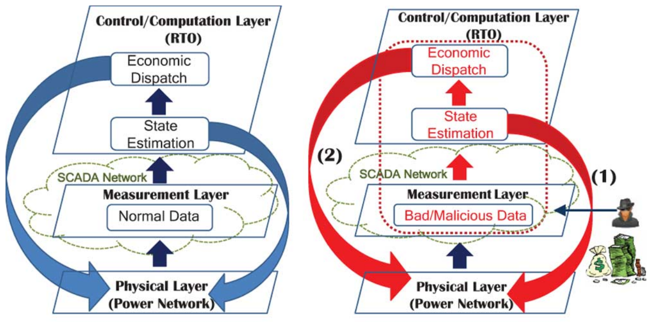
***Abstract*—This paper presents a new class of false data injection attacks on state estimation, which may lead to financial arbitrage in real-time power markets with an emerging *look-ahead* dispatch model. In comparison with prior work of cyber attack on static dispatch where no inter-temporal ramping constraint is considered, we propose a novel attack strategy with which the attacker can manipulate, in look-ahead dispatch, the limits of ramp constraints of generators. It is demonstrated that the proposed attack may lead to financial profits via malicious capacity withholding of selected generators, while being undetected by the existing bad data detection algorithm embedded in the state estimator. The feasibility of such cyber attacks and their economic impact on real-time electricity market operations are illustrated in the IEEE 14-bus system.**

***Index Terms*—Cyber security, economic dispatch, power system state estimation, ramp-induced data attack.**

I. Introduction

Critical infrastructure (e.g., the electricity grid) has been facing an increasing number of potential cyber attacks. Given the much stronger coupling between cyber and physical layers of smart grid, development of cyber security technology tailored for smart grid is of paramount importance.

The main objective of this paper is to study the impact of cyber attacks on state estimation, which subsequently influence the result of the newly emerging *look-ahead dispatch model* in the real-time electricity market. Fig. 1(a), 1(b) illustrate the information flow in a three-layered framework (with physical, measurement, and control/computation layer) without and with such cyber attacks, respectively. The information includes the physical state such as the nodal power injection and flow and the dispatch instruction such as the optimal generation output and nodal price. Compared to Fig. 1(a), 1(b) describes that bad/malicious data injected into the measurement layer can lead to corrupted estimation of the states of the physical layer. Consequently, the attacker could distort the feedback information from control/communication layer back to the physical layer in two ways, leading to 1) physical insecurity in the power grid operations, and/or 2) financial misconduct in the power markets as shown in Fig. 1(b). This paper contributes to topic 2) using a more realistic dispatch model in power markets.



(a) (b)

Fig. 1. A three-layered framework illustrating cyber data attack. (a) Without cyber data attack. (b) With cyber data attack.

A large body of literature has been accumulated recently on the subject of cyber security in power grids, ranging from risk mitigation [1], generation control security (e.g., automatic generation control (AGC) attack [2], [3]), control security in distribution system [4], and privacy protection [5]–[8]. A concise summary paper is presented in [9], including risk assessment methodology, power system control application and cyber infrastructure security. Meanwhile, many researchers have been studying false data injection attacks, which malfunction the state estimator by injecting false data into sensors. For the subject of false data injection attacks, two major categories of work have been presented:

- *Vulnerability analysis of state estimation*: a false data injection attack was formulated and analyzed in [10], [11]. Efficient algorithm to find sparse attacks and phasor measurement units (PMUs) placement algorithm to prevent sparse attacks were developed in [12], [13]. A distributed joint detection-estimation approach to malicious data attack was presented in [14]. In [15], it was shown that the attacker can hack the power grid without the knowledge of the power network topology, which can be estimated using linear independent component analysis (ICA).
- *Financial risk analysis in electricity market operations*: this area examined the economic impact of false data injection attacks on electricity market operations. Undetectable and profitable attack strategies, which exploit virtual bidding mechanism, were proposed in [16]. In [17], a more general malicious data attack problem was formulated in the real-time electricity market.

However, in [16], [17], the proposed attacks were characterized in *static* economic dispatch without modeling inter-temporal constraints.

In this paper we present a new type of potential cyber attacks in more realistic economic dispatch model, i.e., *look-ahead* dispatch. Motivated by the increasing penetration of variable

Manuscript received June 20, 2012; revised September 09, 2012; accepted October 31, 2012. Date of publication May 31, 2013; date of current version August 21, 2013. This work was supported in part by the Power Systems Engineering Research Center, and in part by National Science Foundation ECCS Grant 1029873. Paper no. TSG-00380-2012.

The authors are with the Department of Electrical and Computer Engineering, Texas A&M University, College Station, TX 77840 USA (e-mail: cdh8954@neo.tamu.edu; Lxie@ece.tamu.edu).

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

Digital Object Identifier 10.1109/TSG.2012.2228508

resources such as wind and solar [18], look-ahead dispatch has been implemented by major Independent System Operators (ISOs)/Regional Transmission Organizations (RTOs) in the past few years in order to improve the market dispatch efficiency [19]–[21]. Look-ahead dispatch is different from conventional static dispatch in that it calculates the optimal dispatch in an extended period of time, taking into account inter-temporal ramp rates of generators of different technologies. In this paper, an attack strategy is demonstrated, in which the attacker could withhold generation capacity for financial gain by stealthily manipulating the ramp constraint limits of generators in look ahead dispatch. It should be noted that the proposed attack strategy is different from the capacity withholding methods used for a generation company to report capacity noticeably lower than its maximum capacity based on learning algorithm (e.g., SA-Q-Learning algorithm) [22], [23]. In contrast, the proposed method is to inject *undetectable* malicious data in order to withhold capacity for financial misconduct in real-time markets. The main contributions of this paper are two-fold:

1) We formulate a malicious ramp-induced data (RID) attack problem in look-ahead dispatch. The attacker could stealthily change the ramp constraint limits of generators through manipulating sensors' data, aiming at increasing the nodal price by withholding capacity of generator.
2) We propose a RID attack strategy with which the attacker could make a profit without being detected by RTOs in the real-time electricity market. Numerical examples are illustrated in the IEEE-14 bus system.

The rest of this paper is structured as follows. Section II provides the brief overview of state estimation and real-time power market with look-ahead dispatch model. Section III states the cyber attack problem. The proposed attack formulation including required conditions, attack procedure and strategy, and attack performance metrics is elaborated in more detail in Section IV, which is followed by illustrative examples based on the IEEE 14-bus test system in Section V. Section VI presents the conclusions and future work.

II. Background

The notations used in this paper are summarized in Table I.

A. State Estimation Model

We consider the linearized dc state estimation model:

$$\mathbf{z} = \mathbf{H}\mathbf{x} + \mathbf{e} = \begin{bmatrix} \mathbf{I} \\ \mathbf{H_d} \end{bmatrix} \mathbf{x} + \mathbf{e}, \tag{1}$$

where

$\mathbf{x}$ State vector (nodal power injections).

$\mathbf{z}$ Measurement vector (power injection and flow measurements).

$\mathbf{e}$ Independent identically distributed (i.i.d.) Gaussian measurement error vector following $\mathcal{N}(0, \mathbf{R})$.

$\mathbf{H}$ The system factor matrix specifying the relationship between $\mathbf{x}$ and $\mathbf{z}$.

TABLE I
NOTATIONS

i	Index for generators i
n	Index for buses n
l	Index for transmission line l
K	Total number of sampling period
N	Total number of buses
L	Total number of transmission lines
M	Total number of measurements
G	Set of generation units
G_M	Set of marginal units
$\underline{G}_M^c$	Set of binding units with lower marginal cost than marginal unit
$\overline{G}_M^c$	Set of binding units with higher marginal cost than marginal unit
D	Set of demands
$P_{g_i}[k]$	Scheduled ith generator power at time k
$\hat{D}_n[k]$	nth bus fixed demand at time k
$F_l[k]$	Transmission flow at line l at time k
R_i	Ramp rate of generator i
ΔT	Dispatch interval
$P_{g_i}^{\min}$, $P_{g_i}^{\max}$	Min/max generation limits for generator i
$F_l^{\min}$, $F_l^{\max}$	Min/max flow limits at line l

Here the matrix $\mathbf{H}$ is concatenated with two submatrices, $\mathbf{H_d}$ and $\mathbf{I}$, which denote the distribution factor matrix and the identity matrix, respectively. The state estimation problem is to find the optimal estimate of $\mathbf{x}$ to minimize the weighted least square of measurement error:

$$\text{minimize} \quad J(\mathbf{x}) = \mathbf{r}^T \mathbf{R}^{-1} \mathbf{r} \tag{2}$$

$$\text{s.t.} \quad \mathbf{r} = \mathbf{z} - \mathbf{H}\mathbf{x}, \tag{3}$$

where $\mathbf{r}$ is the estimated residual vector. If the system is observable (i.e., the system factor matrix $\mathbf{H}$ is full rank), the unique weighted least squares estimate of $\mathbf{x}$ is given by

$$\hat{\mathbf{x}}(z) = (\mathbf{H}^T \mathbf{R}^{-1} \mathbf{H})^{-1} \mathbf{H}^T \mathbf{R}^{-1} \mathbf{z} = \mathbf{B}\mathbf{z}. \tag{4}$$

B. Real-Time Power Market With Look-Ahead Dispatch Model

The electric power market consists of two-settlement system, day-ahead, and real-time spot markets. Recently, due to limited predictability in day-ahead and high inter-temporal variability of renewable resources (e.g., wind and solar), RTOs are upgrading real-time market clearing engine from static dispatch to look-ahead dispatch models for more flexible operations in support of high penetration of variable resources [19]. For the system operator, look-ahead dispatch is formulated as follows:

$$\min_{P_{g_i}[k]} \sum_{k=1}^{K} \sum_{i \in G} C_i(P_{g_i}[k]) \tag{5}$$

s.t.

$$\sum_{i \in G} P_{g_i}[k] = \sum_{n=1}^{N} \hat{D}_n[k] \quad \forall k = 1, \ldots, K \tag{6}$$

$$|P_{g_i}[k] - P_{g_i}[k-1]| \le R_i \Delta T \quad \forall k = 1, \ldots, K \tag{7}$$

$$P_{g_i}^{\min} \le P_{g_i}[k] \le P_{g_i}^{\max} \quad \forall k = 1, \ldots, K \tag{8}$$

$$F_l^{\min} \le F_l[k] \le F_l^{\max} \quad \forall k = 1, \ldots, K. \tag{9}$$

In this formulation, the objective function is to minimize the total generation costs in (5). Equation (6) is the system-wide energy balance equations. Equations (7) and (8) are the ramp constraints and the physical capacity constraints of each generator, respectively. Equation (9) is the transmission line constraints. In this paper, we define one-step look-ahead dispatch with $K = 1$ as static dispatch. The Lagrangian function of the aforementioned look-ahead dispatch is written as

$$\begin{aligned}
\mathcal{L} = &\sum_{k=1}^{K}\sum_{i\in G} C_i(P_{g_i}[k]) \\
&- \sum_{k=1}^{K} \lambda[k]\left[\sum_{i\in G} P_{g_i}[k] - \sum_{n=1}^{N} \hat{D}_n[k]\right] \\
&+ \sum_{k=1}^{K}\sum_{i\in G} [\omega_{i,\max}[k](P_{g_i}[k] - P_{g_i}[k-1] - R_i\Delta T)] \\
&+ \sum_{k=1}^{K}\sum_{i\in G} [\omega_{i,\min}[k](P_{g_i}[k-1] - P_{g_i}[k] - R_i\Delta T)] \\
&+ \sum_{k=1}^{K}\sum_{i\in G} \left[\tau_{i,\max}[k](P_{g_i}[k] - P_{g_i}^{\max})\right] \\
&+ \sum_{k=1}^{K}\sum_{i\in G} \left[\tau_{i,\min}[k](P_{g_i}^{\min} - P_{g_i}[k])\right] \\
&+ \sum_{k=1}^{K}\sum_{l=1}^{L} [\mu_{l,\max}[k](F_l[k] - F_l^{\max})] \\
&+ \sum_{k=1}^{K}\sum_{l=1}^{L} \left[\mu_{l,\min}[k](F_l^{\min} - F_l[k])\right],
\end{aligned}$$

where all the Lagrangian multipliers at time k ($\lambda[k]$, $\omega_{i,\max}[k]$, $\omega_{i,\min}[k]$, $\tau_{i,\max}[k]$, $\tau_{i,\min}[k]$, $\mu_{l,\max}[k]$, and $\mu_{l,\min}[k]$) are positive. According to the definition of the nodal price [24], and assuming that bus 1 is the slack bus, the locational marginal price (LMP) for each bus n ($n = 2, \ldots, N$) at time k is given by

$$\lambda_n[k] = \lambda[k] - \mathbf{H_{d_n}}^T(\mu_{\max}[k] - \mu_{\min}[k]), \tag{10}$$

where $\lambda[k]$ is the LMP for the slack bus 1 at time k, $\mathbf{H_{d_n}} = [\partial F_1/\partial\hat{D}_n, \ldots, \partial F_L/\partial\hat{D}_n]^T$, $\mu_{\max}[k] = [\mu_{1,\max}[k], \ldots, \mu_{L,\max}[k]]^T$, and $\mu_{\min}[k] = [\mu_{1,\min}[k], \ldots, \mu_{L,\min}[k]]^T$.

Alternatively, by the first-order KKT condition of look-ahead dispatch formulation, the LMP for each generator i connected to bus n is written as

$$\begin{aligned}
\lambda_i[k] = &\frac{\partial C_i(P_{g_i}[k])}{\partial P_{g_i}[k]} - \mathbf{H_{d_n}}^T(\mu_{\max}[k] - \mu_{\min}[k]) \\
&+ (\tau_{i,\max}[k] - \tau_{i,\min}[k]) \\
&+ (\omega_{i,\max}[k] - \omega_{i,\max}[k+1]\mathbb{1}_A[k]) \\
&+ (\omega_{i,\min}[k+1]\mathbb{1}_A[k] - \omega_{i,\min}[k]),
\end{aligned} \tag{11}$$

where $\mathbb{1}_A[k]$ is the indicator function based on the set $A = \{1 \leq k \leq K-1\}$. In other words, $\mathbb{1}_A[k] = 1$ when $k \in A$, otherwise (i.e., $k \in A^c = \{k = K\}$) $\mathbb{1}_A[k] = 0$. We can observe from (11) that the Lagrangian multipliers, $\omega_{i,\max}[k+1]$ and $\omega_{i,\min}[k+1]$, corresponding to the ramp constraints at the future time $k+1$ influence the LMPs calculation at the current time k. However, the LMP formulation in static dispatch (one-step look-ahead) does not capture future constraints.

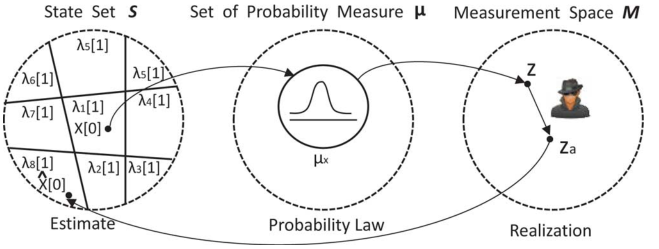


Fig. 2. Statistical signal processing framework illustrating the relationship among sensor data, state estimation, and economic dispatch.

III. Statement of the Cyber Attack Problem

A general problem of cyber attack against state estimation in economic dispatch can be illustrated in statistical signal processing framework in Fig. 2. It provides a graphical interpretation for the relationship among sensor's measurement, state estimation, and economic dispatch. The state set $\boldsymbol{\mathcal{S}}$ is partitioned into a finite number of nodal price subsets $\lambda_i[1]$. The operation of economic dispatch is implicitly included in the state set $\boldsymbol{\mathcal{S}}$. The measurement space $\boldsymbol{\mathcal{M}}$ is the collection of all realizable sensor's measurements $\mathbf{z}$. The set of probability measure $\boldsymbol{\mu}$ provides a mathematical basis for describing the randomness of measurements. In the power system state estimation literature, the probability measure normally follows the Gaussian distribution. These random measurement errors can be filtered by the existing bad data processing algorithm. The objective of the attacker is to move the estimate from a certain nodal price subset to a desired nodal price subset by corrupting original measurements $\mathbf{z}$ into $\mathbf{z_a}$ while avoiding the bad data detection. Detailed attack model and formulation are described in Section IV.

In the above framework, a potential cyber attack in look-ahead dispatch is described as follows. The ith unit's initial generation power $P_{g_i}[0]$ embedded in (7) is replaced, at every dispatch interval, by its corresponding estimate $\hat{P}_{g_i}(\mathbf{z})$, which is processed and delivered by the state estimator. Therefore, in static dispatch the generation power of unit i at $k = 1$ becomes bounded by

$$P_{g_i}^{\max}[1] = \min\{P_{g_i}^{\max}, P_{g_{i,\mathrm{R}}}^{\max}(\mathbf{z})\} \tag{12}$$

$$P_{g_i}^{\min}[1] = \max\{P_{g_i}^{\min}, P_{g_{i,\mathrm{R}}}^{\min}(\mathbf{z})\}, \tag{13}$$

where the maximum and minimum limits of the ramp constraints, $P_{g_{i,\mathrm{R}}}^{\max}(\mathbf{z})$ and $P_{g_{i,\mathrm{R}}}^{\min}(\mathbf{z})$, are

$$\begin{aligned}
P_{g_{i,\mathrm{R}}}^{\max}(\mathbf{z}) &= \hat{P}_{g_i}(\mathbf{z}) + R_i\Delta T, \\
P_{g_{i,\mathrm{R}}}^{\min}(\mathbf{z}) &= \hat{P}_{g_i}(\mathbf{z}) - R_i\Delta T.
\end{aligned} \tag{14}$$

If the attacker manipulates the estimate $\hat{P}_{g_i}(\mathbf{z})$ by injecting false data into $\mathbf{z}$ so that the capacity limits of unit i at $k = 1$ are binding to stealthily changed ramp constraint limits, the optimal generation dispatch and nodal price might be miscalculated by RTOs. In this paper we define this type of attack as a ramp-

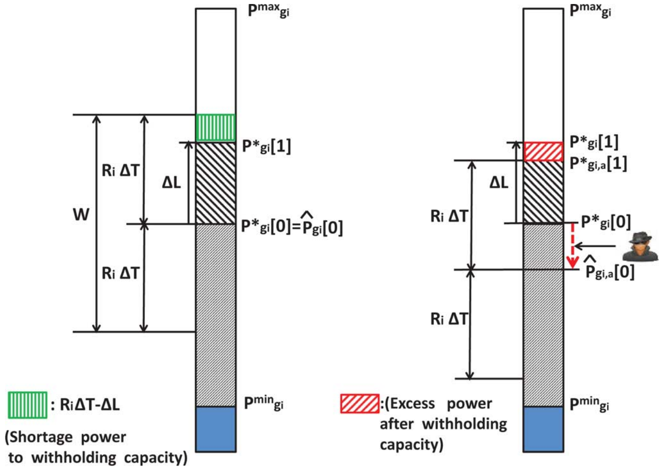


Fig. 3. Conceptual diagrams illustrating a ramp-induced data attack.

induced data (RID) attack in a potential class of malicious inter-temporal data attacks.

Fig. 3 illustrates the RID attack, which withholds capacity of a marginal unit (a part-loaded generator). Left and right diagrams describe the generation characteristics of the marginal unit without and with the attack, respectively. W is the feasible range of generation limited by the ramp rate of the marginal unit, and ΔL is an incremental (in this figure) or decremental system load from $k=0$ to $k=1$. We note that as $\hat{P}_{g_i}[0]$ (for simplicity, we omit $\mathbf{z}$, instead emphasize the time) is manipulated by the attacker, ΔL can deviate, upwards or downwards, from the range of W, leading to capacity withholding or capacity withdrawing, respectively. The right diagram in Fig. 3 shows that if $\hat{P}_{g_i}[0]$ is decreased to $\hat{P}_{g_i,\mathbf{a}}[0]$ by the attacker at $k=0$ so that ΔL deviates upwards from the range of W, the attacker succeeds in withholding capacity, resulting in a new dispatch output $\hat{P}^*_{g_i,\mathbf{a}}[1]$ at $k=1$. As a result, the infra-marginal unit (the unit with the next higher marginal cost) is dispatched to supply the excess demand, consequently leading to a uniformly higher market price.

Remark 1: Define $\hat{P}_{g_i,\mathbf{a}}[0] - P^*_{g_i}[0]$ as the contribution of the attacker to changing the nodal price. The RID attack fails (i.e., the nodal price remains unchanged) if the value of this contribution belongs to the following interval:

$$\Delta L - R_i\Delta T \leq \hat{P}_{g_i,\mathbf{a}}[0] - P^*_{g_i}[0] \leq \Delta L + R_i\Delta T. \qquad (15)$$

The feasible region of $\hat{P}_{g_i}[0]$ based on constraint (15) is defined as the price-invulnerable region.

IV. Formulation of the Ramp-Induced Data Attack

A. Attack Model and Undetectability

We consider the additive attack measurement model:

$$\mathbf{z_a} = \mathbf{Hx} + \mathbf{e} + \mathbf{a}, \qquad (16)$$

where $\mathbf{a}$ is the attack vector, which leads to the corrupted measurement vector $\mathbf{z_a}$. The new residual vector $\mathbf{r_a}$ can be decomposed into two terms, corresponding to without and with attack, respectively:

$$\mathbf{r_a} = \mathbf{r} + (\mathbf{I} - \mathbf{HB})\mathbf{a}, \qquad (17)$$

and by triangular inequality of the L_2-norm $\|\cdot\|_2$,

$$\begin{aligned} \|\mathbf{r_a}\|_2 &= \|\mathbf{r} + (\mathbf{I} - \mathbf{HB})\mathbf{a}\|_2 \\ &\leq \|\mathbf{r}\|_2 + \|(\mathbf{I} - \mathbf{HB})\mathbf{a}\|_2 < \eta, \end{aligned} \qquad (18)$$

where η is the bad data detection threshold. For bypassing the bad data detection algorithm, the attacker aims at constructing the attack vector $\mathbf{a}$ so that the value of $\|(\mathbf{I} - \mathbf{HB})\mathbf{a}\|_2$ added to $\|\mathbf{r}\|_2$ still makes the above undetectable condition hold true.

B. Requirements and Procedure for a Successful RID Attack

From the analysis above, in order to implement a RID attack with profits, the attacker is required to have the knowledge of:

R1) the system topology (e.g., distribution factor matrix), which remains constant at every dispatch interval;

R2) the ramp rates of the targeted generators;

R3) the amount of changing system load between two consecutive dispatch intervals.

The system topology for the targeted power system in Requirement R1) can be simply obtained off-line by an internal intruder in a control center or estimated by linear independent component analysis (ICA) technique proposed in [15]. For Requirement R2), typical ramp rates are estimable for typical generators. Requirement R3) is feasible since the attacker can estimate an amount of changing system load from RTOs' website. With these assumptions, the procedure of the proposed RID attack is summarized as follows:

Step 1): The attacker synchronizes the attack time with the start time at every dispatch interval. This step is necessary for injected false data to mislead economic dispatch via the state estimator.

Step 2): The attacker determines sensors to compromise and computes the attack vector using the proposed attack strategy formulated in the next subsection.

Step 3): The attacker injects the attack vector into sensors' measurements at the attack time set in Step 1). Then, these corrupted measurements are transmitted to the state estimator via SCADA network.

Step 4): The state estimator based on received false measurements may lead to distorted generation output estimates. They are utilized for setting the ramp constraints in look-ahead dispatch.

Step 5): Consequently, the manipulated ramp constraints result in the attacker's desired dispatch instruction. Then, it is sent to the dispatchable generators.

Step 6): For the continuous attack, the procedure goes back to Step 2).

C. Proposed Attack Strategy

In this subsection we formulate a ramp-induced data attack strategy. The power system is assumed to have sufficient transmission capacity. As the first step toward understanding the impact of cyber attack on *temporal* ramp-constrained economic dispatch, we exclude the impact of *spatial* transmission congestion on the market clearning prices. In practice, temporal ramp constraints are coexisting with spatial transmission flow constraints. Therefore, for a successful RID attack in congested networks the attacker should know the targeted power system very well and as much as the system operator knows, however this scenario is unrealistic. Developing a feasible RID attack strategy in congested networks is beyond the scope of this paper and referred to as a future work.

The proposed attacks are classified into the following three types:

- *Marginal unit attack*: a injection measurement sensor associated with the marginal unit is compromised.
- *Binding unit attack*: injection measurement sensors associated with the binding units are compromised.
- *Coordinated attack*: injection measurement sensors associated with the binding units as well as the marginal unit are compromised.

Here a binding unit represents two types of units: an intra-marginal unit with the lower marginal cost or an infra-marginal unit with the higher marginal cost than a marginal unit. The following proposed attack strategy and simulation results focus on intra-marginal unit attack belonging to binding unit attack.

Remark 2: When there is no network transmission congestion, it is well acknowledged that static dispatch involves a single marginal unit and multiple binding units that produce their minimum or maximum outputs. On the other hand, look-ahead dispatch may involve multiple marginal units even if there is no congestion in the the transmission network. In this paper the marginal unit attack is associated with the marginal unit in static dispatch.

For achieving undetectability and profitability, the attacker computes the attack vector $\mathbf{a}$ by compromising sensors $i \in G_M$ or $j \in \underline{G}_M^c$, which is the solution of the following optimization problem:

$$\max_{\mathbf{a} \in \mathrm{span}(\mathcal{A})} \delta \tag{19}$$

s.t.

$$\|(\mathbf{I} - \mathbf{H}\mathbf{B})\mathbf{a}\|_2 \leq \epsilon \tag{20}$$

$$\alpha \mathcal{C}_M(\mathbf{a}) + \beta \mathcal{C}_B(\mathbf{a}) \leq \Delta L - R_i \Delta T - \delta \tag{21}$$

$$\delta > 0 \tag{22}$$

where

$$\mathcal{C}_M(\mathbf{a}) = \mathbf{B}_i \mathbf{a}, \quad \mathcal{C}_B(\mathbf{a}) = \sum_{j \in \underline{G}_M^c} [\mathbf{B}_j \mathbf{a} + R_j \Delta T].$$

TABLE II
COMPARISON BETWEEN RID ATTACK AND SPATIAL ATTACK

	RID Attack	Spatial Attack
Potential Attacker	Generation Company	Third Party
Bidding Method	Generation Bidding	Virtual Bidding
Market Structure	RT (Time-coupled only)	DA/RT
RT Pricing Model	Ex-ante	Ex-post
Line Congestion	No	Yes
Vulnerability Index	$\Delta L - R_i \Delta T$	$F_l^{\max} - F_l^{\mathrm{ante}}$
Target Sensors	Injection Sensors	Flow Sensors

* RT: Real-time, DA: Day-ahead

$\mathcal{C}_M(\mathbf{a})$ and $\mathcal{C}_B(\mathbf{a})$ are the contributions of the attacker to changing the nodal price, corresponding to the marginal unit and binding unit attacks, respectively. The derivations of these contribution terms are referred to in Appendix A. The set $\mathcal{A}$ represents the attack vector space, which describes the attack pattern related to the type and number of compromised sensors. $\Delta L - R_i \Delta T$ is the minimum amount of power which the attacker should reduce at $k = 0$ in order to withhold the capacity of unit i at $k = 1$. Constraint (20) assures undetectability as the parameter ϵ is tuned with an appropriate value. Constraint (21) assures profitability since it enables unit i to bind at the limit of the up-ramp constraint, leading to the increasing nodal price. Therefore, the attacker aims to maximize the margin δ in order to make a financial gain via capacity withholding with a high probability. The binary values of α and β in (21) determine the following three types of attacks:

1) $\alpha = 1, \beta = 0$: Marginal unit attack
2) $\alpha = 0, \beta = 1$: Binding unit attack
3) $\alpha = 1, \beta = 1$: Coordinated attack.

Remark 3: Compared to the capacity withholding mentioned above, capacity withdrawing can benefit a load serving entity (LSE) by manipulating the down-ramp constraint limit. This type of the attack is feasible when constraint (21) is replaced with

$$\alpha \mathcal{C}_M(\mathbf{a}) + \beta \mathcal{C}_B(\mathbf{a}) \geq \Delta L + R_i \Delta T + \delta \tag{23}$$

where

$$\mathcal{C}_M(\mathbf{a}) = \mathbf{B}_i \mathbf{a}, \quad \mathcal{C}_B(\mathbf{a}) = \sum_{j \in \bar{G}_M^c} [\mathbf{B}_j \mathbf{a} - R_j \Delta T].$$

Remark 4: Table II summarizes the characteristics of the RID attack, as well as the spatial attack proposed in [16]. Specifically, we note the vulnerability index. This quantifies the vulnerability of the targeted power system subject to each type of attack. If variables ΔL and F_l^{ante} (power flow at the Ex-ante market) become closer to constants $R_i \Delta T$ and $F_l^{\max}$, respectively, the power system becomes more and more vulnerable to both attacks.

D. Attack Performance Metrics

The performance of the proposed RID attack is evaluated using the following performance metrics:

1) Attack Profitability: Assuming that the power injection measurement sensor at generator i is compromised, we define the attack profit efficiency (PE) of generator i as the ratio of the profit with attack to without attack:

$$\mathrm{PE}(i) = \frac{P_{g_i,\mathbf{a}}^*[1](\lambda_i^{(a)} - c_i)}{P_{g_i}^*[1](\lambda_i^{(b)} - c_i)} \times 100\ (\%). \tag{24}$$

Here, $\left(\lambda_i^{(a)}, P_{g_i,\mathbf{a}}^*[1]\right)$ and $\left(\lambda_i^{(b)}, P_{g_i}^*[1]\right)$ are two pairs of the nodal price and optimal generation dispatch with and without attack, respectively. c_i is the marginal cost for generator i.

2) Attack Undetectability: The system operator normally performs the Chi-squares test [25] for detecting bad data in the measurements. Bad (or malicious) data will bypass if

$$J(\hat{\mathbf{x}}) \leq \chi^2_{(m-s),p} := \eta_\chi, \tag{25}$$

where p is the detection confidence probability, and m and s represent the number of measurements and state variables, respectively.

3) Attack Vulnerability: Since the measurement noise follows a Gaussian distribution, the manipulated estimate of the state at generator i is also a Gaussian random variable

$$\hat{\mathbf{x}}_i(z_a) \sim \mathcal{N}(\mathbf{P}_{\mathbf{i}}^*[\mathbf{0}] + \mathbf{B}_i\mathbf{a}, \mathbf{B}_i\mathbf{R}\mathbf{B}_i^T). \tag{26}$$

The probability of the distorted estimate $\hat{\mathbf{x}}_i(z_a)$ being within the price-invulnerable region defined in Remark 1 is expressed as in terms of $Q(\cdot)$ functions

$$\begin{aligned}\mathbb{P}_i(\mathbf{a}) &= \mathbb{P}(\mathbf{l}(i) \leq \hat{\mathbf{x}}_i(z_a) \leq \mathbf{u}(i)) \\ &= Q(\mathbf{l}(i)) - Q(\mathbf{u}(i)),\end{aligned} \tag{27}$$

where the complementary Gaussian cumulative distribution function $Q(x)$ is defined as

$$Q(x) = \int_x^\infty \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{\xi^2}{2}\right) d\xi \tag{28}$$

and

$$\mathbf{l}(i) = \frac{\Delta L - R_i\Delta T - \mathbf{B}_i\mathbf{a}}{\sqrt{\mathbf{B}_i\mathbf{R}\mathbf{B}_i^T}} \tag{29}$$

$$\mathbf{u}(i) = \frac{\Delta L + R_i\Delta T - \mathbf{B}_i\mathbf{a}}{\sqrt{\mathbf{B}_i\mathbf{R}\mathbf{B}_i^T}}. \tag{30}$$

We define $\mathbb{P}_i(\mathbf{a})$ as the price-invulnerable probability (PIP) with respect to generator i. From (27), (28), (29), and (30), we specify the relationship among the ramp rate $R_i\Delta T$, the diagonal measurement covariance matrix $\mathbf{R}$, and the PIP as follows:

1) The increase of the $R_i\Delta T$ leads to the increase of the PIP.
2) The decrease of the values of the diagonal elements in $\mathbf{R}$ leads to the increase of the PIP.

In other words, the deployment of more accurate sensors and generators with a faster ramp rate enables the power system to become more robust to the RID attack.

V. Numerical Example

In this section the economic impact of the proposed RID attack on the real-time electricity market operation is illustrated in the IEEE 14-bus system as shown in Fig. 4. Measurement configuration includes nodal power injection measurements at all generation and load buses, and power flow measurements at one end of each transmission line. This system has a total of 34 measurements including 14 power injection and 20 power flow measurements, which assure the system observability. Table III shows the five generators' operating characteristics, including unit type (generation bus number), physical capacity limit, ramp rate, and marginal cost (MC).

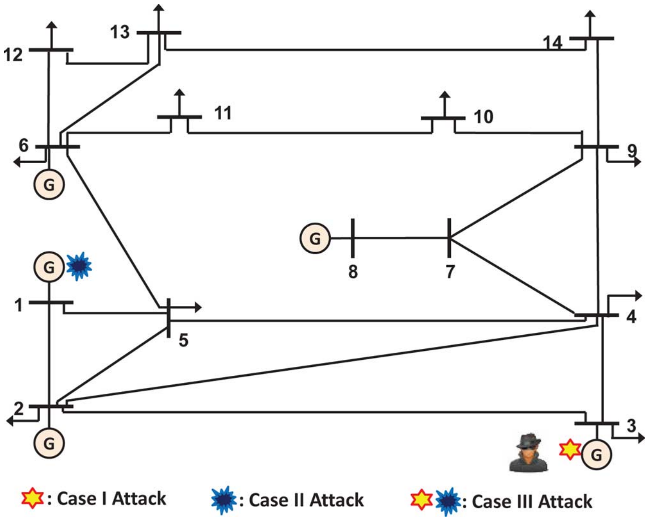


Fig. 4. IEEE 14-bus Test system.

TABLE III
Generator Parameters of the IEEE 14-Bus Test System

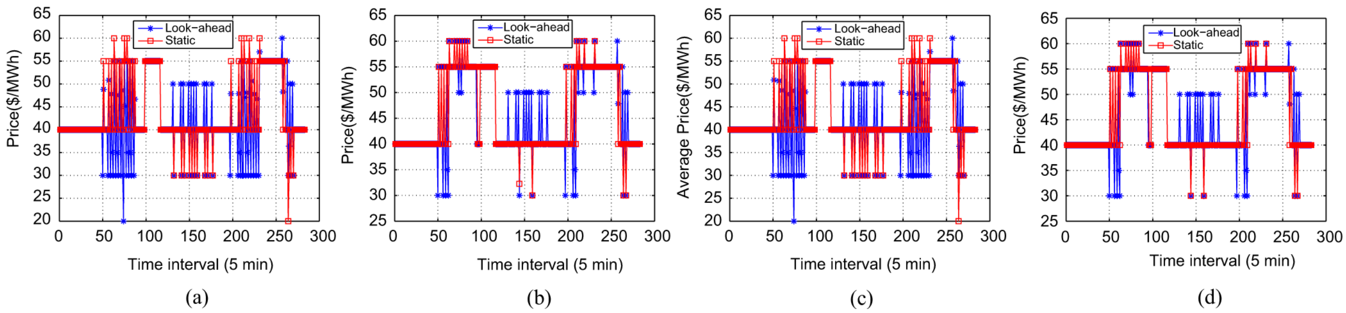
Unit Type	$P_{\min}$	$P_{\max}$	Ramp Rate	MC
Coal(1)	0MW	200MW	10MW/5min	30$/MWh
Wind(2)	0MW	300MW	150MW/5min	20$/MWh
Nuclear(3)	0MW	300MW	8MW/5min	40$/MWh
Coal(6)	50MW	250MW	15 MW/5min	55$/MWh
Oil(8)	60MW	150MW	60 MW/5min	60$/MWh

In this section, three cases are simulated in the IEEE-14 bus system:

- Case I: Marginal unit attack.
- Case II: Binding unit attack.
- Case III: Coordinated attack.

The performance of the proposed RID attack is evaluated based on the one day load profile with a 5-min resolution. This load profile is obtained by interpolating a 15-min daily data in the ERCOT website. The load is scaled down to be consistent with the IEEE 14-bus test system's peak load data. The common goal of all three cases is to withhold the capacity of generator 3 for the purpose of making a profit. A power injection sensor at generation bus 3 is compromised in Case I whereas a power injection sensor at generation 1 is compromised in Case II. Case III represents the coordinated attack, which compromises both sensors targeted in Case I and Case II.

Fig. 5 show the comparison of the LMPs between static ($K = 1$) and look-ahead dispatch ($K = 6$) without attack and with attack in Cases I, II, and III. Due to no network transmission congestion, the prices in these figures denote the uniform LMPs for all the buses at every dispatch interval. In Fig. 5(a), the LMPs in look-ahead dispatch are oscillating around 40 $/MWh more than the ones in static dispatch. This phenomenon is due to the fact that the binding of generator 3 at the up- or down-ramp constraints at time $k+1$ makes its corresponding Lagrangian multiplier, $\omega_{3,\max}[k+1]$ or $\omega_{3,\min}[k+1]$, become positive. As shown in (11), this leads to different LMPs at time k than the ones from static dispatch. We observe from Fig. 5(b), 5(c), 5(d) that the LMPs in both dispatch models tend to increase with attack. This observation implies that the attacker successfully withholds the



(a) (b) (c) (d)

Fig. 5. LMP of static and look-ahead dispatch without attack and with Case I, II, and III attacks. (a) Without attack. (b) Case I attack. (c) Case II attack. (d) Case III attack.

capacity of generator 3 by lowering its up-ramp constraint limit through the reduction of the initial estimate $\hat{P}_{g_3,\mathbf{a}}[0]$. Consequently, this leads to the shift of the marginal unit to another one with a more expensive marginal cost.

Table IV shows the attack performance of Cases I, II, and III in both static and look-ahead dispatch. The second and third columns of this table indicate the attack profit efficiency at generation bus 3. We can observe from the comparison of these two columns several facts. First, the PE values in all three cases of both dispatch models are larger than 100. It indicates that the attacker makes an additional profit using the proposed attack strategy. Second, for all three cases, the PE in look-ahead dispatch is higher than in static dispatch. This observation might result from the fact that the attack leads to more increase of the nodal price in look-ahead dispatch than in static dispatch. Lastly, among three cases, Case I and Case II attacks yield the largest and smallest PE, respectively. The PE in Case III is between Case I and Case II. This result is natural since Case II and Case III attacks require an extra effort for withholding the binding unit's capacity as well as the marginal unit's capacity so that both attacks fail with a higher probability than Case I attack. Fig. 6 shows the amount of generator 3's capacity which all three attacks withhold between 80 and 90 time intervals. As expected, it is verified that Case I, Case III, and Case II attacks withhold capacity the most in a descending order. This fact also justifies the third observation mentioned above. The values of the estimated objective functions for all three cases are shown in the last column of Table IV. Based on the measurement configuration with $m = 34$ and $s = 14$, the threshold (η_χ) of the Chi-squares test with a 99% confidence level is set to 37.6. For undetectability, the parameter ϵ in (20) is set to 3. Therefore, all three attacks in both dispatch models succeed in avoiding the Chi-squares bad data detection.

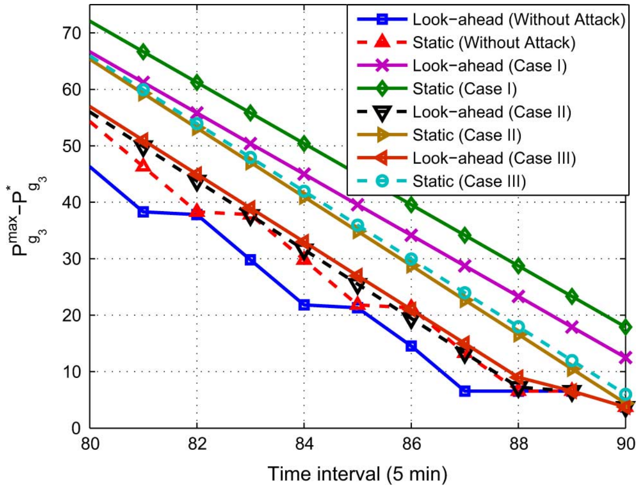


Fig. 6. $P_{g_3}^{\max} - P_{g_3}^{*}$ of static and look-ahead dispatch without attack and with Case I, II, and III attacks.

TABLE IV
ATTACK PERFORMANCE IN STATIC AND LOOK-AHEAD DISPATCH

Case	Static (PE(3))	Look-ahead (PE(3))	$J(\eta_\chi = 37.6)$
I	131.9	148.9	28.2
II	101.2	102.6	35.5
III	108.9	113.8	31.5

Table VI shows the sensitivity of Case I attack performance with respect to the attack magnitude. In this table, the attack relative magnitude (ARM) is defined as $\|\mathbf{a}\|_\infty/\|\mathbf{z}\|_\infty \times 100$ where $\|\cdot\|_\infty$ denotes an infinity norm. We observe from this table that the increase of the ARM leads to more profit (the third and fourth rows) in both dispatch models. However, the estimated objective function J (the fifth row) used for the Chi-squares bad data test increases and the PIP (the last row) decreases. This implies that as the ARM increases the attack becomes more vulnerable to the bad data detection and fails with an increasing probability. Table V shows Case I attack performance with the varying ramp rate of generator 3 and measurement variance of sensors. We first observe from this table that as the ramp rate of generator 3 increases the PE in both dispatch models decreases. Another observation is that the decrease of measurement variance leads to the decrease of the attack profit. These observations imply that the nodal prices become less manipulable, which is verified with the increasing PIP in Table V.

VI. CONCLUSIONS

This paper is concerned about cyber data attacks on state estimation and their effects on time-coupled look-ahead dispatch. With the assumption of no network transmission congestion, we propose an undetectable ramp-induced data attack method with which the attacker could manipulate the ramp constraint limits of generators for withholding generation capacity, subsequently leading to making a profit in the real-time power market. Numerical examples simulated in the IEEE 14-bus system demonstrate the undetectability and profitability of the proposed cyber data attack.

In future work, a system-theoretical framework to analyze the effect of various types of spatial and temporal data attacks

TABLE V
IMPACT OF RAMP RATE AND MEASUREMENT VARIANCE ON THE ATTACK PERFORMANCE IN CASE I

	Ramp Rate (MW/5min)				Measurement Variance (σ^2)			
	8	10	12	14	0.0005	0.005	0.05	0.5
Static (PE(3))	131.9	119.7	106.4	100.5	123.2	129.1	130.3	136.9
Look-ahead (PE(3))	148.9	123.5	108.5	103.1	143.5	144.75	146.1	152.8
PIP	0.017	0.021	0.037	0.044	0.056	0.041	0.034	0.021

TABLE VI
ATTACK PERFORMANCE WITH VARYING ATTACK MAGNITUDE IN CASE I

	Attack Relative Magnitude (ARM %)			
	0.25	0.5	0.75	1
Static (PE(3))	111.8	120.8	126.4	126.9
Look-ahead (PE(3))	112.2	125.8	127.6	137.7
J	21.1	25.4	29.2	33.1
PIP	0.433	0.344	0.259	0.188

on real-time electricity market operations will be developed. The key challenge lies in how to analytically quantify the impact of manipulated sensor's measurement on the nodal price in space-time coupled optimization problem. Another important future direction is to design the robust real-time pricing model as countermeasures to mitigate the financial risks of a variety of cyber data attacks.

APPENDIX
DERIVATION OF ATTACK CONTRIBUTION

In this appendix, we derive the two types of the attack contribution terms in the second inequality constraint of the attack formulation described in Section IV-C. We define the contributions of the marginal unit and binding unit attacks in the expected sense as

$$\mathcal{C}_M(\mathbf{a}) = E[d_i^M(\mathbf{a})] \tag{31}$$

$$\mathcal{C}_B(\mathbf{a}) = E[d^B(\mathbf{a})] \tag{32}$$

where

$$d_i^{(M)}(\mathbf{a}) = \hat{P}_{g_{i,\mathbf{a}}}[0] - P_{g_i}^*[0] \tag{33}$$

$$d^{(B)}(\mathbf{a}) = \sum_{j\in\underline{G}_M^c} (\hat{P}_{g_{j,\mathbf{a}}}[0] + R_j\Delta T - P_{g_j}^{\max}[0]). \tag{34}$$

Here, $\hat{P}_{g_{i,\mathbf{a}}}[0]$ is the manipulated estimate of generation power at generation bus i. Then,

$$\begin{aligned}\mathcal{C}_M(\mathbf{a}) &= E[d_i^{(M)}(\mathbf{a})]\\ &= E[\hat{P}_{g_i,\mathbf{a}}[0]] - P_{g_i}^*[0]\\ &\overset{(a)}{=} E[\mathbf{B}_i(\mathbf{H}\mathbf{x}+\mathbf{e}+\mathbf{a})] - P_{g_i}^*[0]\\ &\overset{(b)}{=} \mathbf{B}_i\mathbf{a}\end{aligned} \tag{35}$$

where $\mathbf{B}_i$ is the row vector of matrix $\mathbf{B}$, which corresponds to the injection measurement sensor of generator i. (a) follows from $\hat{P}_{g_i,\mathbf{a}}[0] = \mathbf{B}_i\mathbf{z}$. (b) follows from $\mathbf{B}_i\mathbf{H} = [0\ldots 0\,1\,0\ldots 0]$ where 1 is the ith element of vector $\mathbf{B}_i\mathbf{H}$ and $E[\mathbf{x}_i] \approx P_{g_i}^*[0]$ together with $E[\mathbf{e}] = 0$. Similarly,

$$\begin{aligned}\mathcal{C}_B(\mathbf{a}) &= E[d^{(B)}(\mathbf{a})]\\ &= \sum_{j\in\underline{G}_M^c} [E[\hat{P}_{g_{j,\mathbf{a}}}[0]] + R_j\Delta T - P_{g_j}^{\max}[0]]\\ &= \sum_{j\in\underline{G}_M^c} [\mathbf{B}_j\mathbf{a} + P_{g_j}^*[0] + R_j\Delta T - P_{g_j}^{\max}[0]]\\ &\overset{(c)}{=} \sum_{j\in\underline{G}_M^c} [\mathbf{B}_j\mathbf{a} + R_j\Delta T]\end{aligned} \tag{36}$$

where (c) follows from $P_{g_j}^*[0] = P_{g_j}^{\max}[0]$.

REFERENCES

[1] D. Kundur, X. Feng, S. Liu, T. ZourntosK, and K. Butler-Purry, "Towards a framework for cyber attack impact analysis of the electric smart grid," in *Proc. 1st IEEE Smart Grid Commun. Conf.*, Oct. 2010.

[2] P. M. Esfahani, M. Vrakopoulou, K. Margellos, J. Lygeros, and G. Andersson, "Cyber attack in a two-area powr system: Impact identification using reachability," in *Proc. Amer. Control Conf.*, Jun. 2010, pp. 962–967.

[3] S. Sridhar and G. Manimaran, "Data integrity attacks and their impacts on SCADA control system," in *Proc. IEEE Power Energy Soc. Gen. Meet.*, Jul. 2010, pp. 1–6.

[4] R. Anderson and S. Fuloria, "Who controls the off switch?," in *Proc. 1st IEEE Smart Grid Commun. Conf.*, Oct. 2010.

[5] Y. E. Kim, C.-H. Ngai, and M. B. Srivastava, "Cooperative state estimation for preserving privacy of user behaviors in smart grid," in *Proc. 2nd IEEE Smart Grid Commun. Conf.*, Oct. 2011.

[6] L. Sankar, S. Kar, R. Tandon, and H. V. Poor, "Competitive privacy in the smart grid: An information-theoretic approach," in *Proc. 2nd IEEE Smart Grid Commun. Conf.*, Oct. 2011.

[7] S. R. Rajagopalan, L. Sankar, S. Mohajer, and H. V. Poor, "Smart meter privacy: A utility-privacy framework," in *Proc. 2nd IEEE Smart Grid Commun. Conf.*, Oct. 2011.

[8] S. Wang, L. Cui, J. Que, D.-H. Choi, X. Jiang, S. Cheng, and L. Xie, "A randomized response model for privacy preserving smart metering," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1317–1324, Sep. 2012.

[9] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-physical system security for the electric power grid," *Proc. IEEE*, vol. 99, no. 1, pp. 1–15, 2012.

[10] Y. Liu, M. K. Reiter, and P. Ning, "False data injection attacks against state estimation in electric power grids," in *Proc. 16th ACM Conf. Comput. Commun. Security*, Nov. 2009.

[11] O. Kosut, L. Jia, R. Thomas, and L. Tong, "Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures," in *Proc. 1st IEEE Smart Grid Commun. Conf.*, Oct. 2010.

[12] T. T. Kim and H. V. Poor, "Strategic protection against data injection attacks on power grids," *IEEE Trans. Smart Grid*, vol. 3, no. 2, pp. 326–333, Jun. 2011.

[13] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla, "Smart grid data integrity attacks: Characterizations and countermeasures," in *Proc. 2nd IEEE Smart Grid Commun. Conf.*, Oct. 2011.

[14] A. Tajer, S. Kar, H. V. Poor, and S. Cui, "Distributed joint cyber attack detection and state recovery in smart grids," in *Proc. 2nd IEEE Smart Grid Commun. Conf.*, Oct. 2011.

[15] M. Esmalifalak, H. A. Nguyen, R. Zheng, and Z. Han, "Stealth false data injection using independent component analysis in smart grid," in *Proc. 2nd IEEE Smart Grid Commun. Conf.*, Oct. 2011.

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

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

[18] L. Xie, P. M. S. Carvalho, L. A. F. M. Ferreira, J. Liu, B. H. Krogh, N. Popli, and D. Ilic, "Wind integration in power systems: Operational challenges and possible solutions," *Proc. IEEE*, vol. 99, no. 1, pp. 1890–1908, Jan. 2011.

[19] A. Ott, "Unit commitment in the PJM day-ahead and real-time markets," in *Proc. FERC Tech. Conf. Increasing Market Planning Efficiency Through Improved Software Hardware*, Washington, DC, Jun. 2010.

[20] ERCOT, "Functional description of core market management system (MMS) applications for look-ahead SCED," White Paper, 2011.

[21] CAISO, *Business Practice Manuals (BPM) Library: Market Operations, Version 11* Aug. 2010 [Online]. Available: http://bpm.caiso.com/bpm/bpm/version/000000000000096

[22] H. Li and L. Tesfatsion, "Capacity withholding in restructured wholesale power markets: An agent-based test bed study," in *Proc. Power Syst. Conf. Expo.*, Mar. 2009.

[23] A. Tellidou and A. Bakirtzis, "Agent-based analysis of capacity withholding and tacit collusion in electricity markets," *IEEE Trans. Power Syst.*, vol. 22, no. 4, pp. 1735–1742, Nov. 2007.

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

[25] A. Abur and A. G. Expósito*, Power System State Estimation. Theory and Implementation*. New York: Marcel Dekker, 2004.

Dae-Hyun Choi (S'10) received the B.S. in electrical engineering from Korea University, Seoul, Korea in 2002, and the M.Sc. in Electrical and Computer Engineering from Texas A&M University, College Station, in 2008. He is working toward the Ph.D degree in the Department of Electrical and Computer Engineering at Texas A&M University.

From 2002 to 2006, he was a Researcher with Korea Telecom (KT), Seoul, Korea where he worked on designing and implementing home network systems. His research interest includes power system state estimation, electricity markets, cyber-physical security of smart grid, and theory and application of cyber-physical energy systems.

Le Xie (S'05–M'10) received the B.E. degree in electrical engineering from Tsinghua University, Beijing, China, in 2004, the M.Sc. degree in engineering sciences from Harvard University, Cambridge, MA, in 2005, and the Ph.D. degree from Electric Energy Systems Group (EESG) in the Department of Electrical and Computer Engineering at Carnegie Mellon University, Pittsburgh, PA, in 2009.

He is an Assistant Professor in the Department of Electrical and Computer Engineering at Texas A&M University, College Station, where he is affiliated with the Electric Power and Power Electronics Group. His industry experience includes an internship in 2006 at ISO-New England and an internship at Edison Mission Energy Marketing and Trading in 2007. His research interest includes modeling, estimation and control of large-scale power systems, and electricity markets.