Integrity Data Attacks in Power Market Operations

Le Xie, *Member, IEEE*, Yilin Mo, *Student Member, IEEE*, and Bruno Sinopoli, *Member, IEEE*

***Abstract*—We study the economic impact of a potential class of integrity cyber attacks, named *false data injection attacks*, on electric power market operations. In particular, we show that with the knowledge of the transmission system topology, attackers may circumvent the bad data detection algorithms equipped in today's state estimator. This, in turn, may be leveraged by attackers for consistent financial arbitrage such as virtual bidding at selected pairs of nodes. This paper is a first attempt to formalize the economic impact of malicious data attacks on real-time market operations. We show how an attack could systematically construct a profitable attacking strategy, in the meantime being undetected by the system operator. Such a result is also valuable for the system operators to examine the potential economic loss due to such cyber attack. The potential impact of the false data injection attacks is illustrated on real-time market operations of the IEEE 14-bus system.**

***Index Terms*—Cyber security, economic dispatch, electricity markets, false data injection attack, locational marginal price, state estimation.**

I. Introduction

THE ELECTRIC power industry is undergoing profound changes as our society increasingly emphasizes the importance of a smarter grid for sustainable energy utilization [1]. Technically, enabled by the advances in sensing, communication, and actuation, power system operations are likely to involve more real-time information gathering and processing devices such as phasor measurement units (PMUs) [2]. Institutionally, the increasing presence of distributed generation resources and flexible demand programs may lead to more integrated SCADA and end-user networks [3].

Financially, the deregulation of electricity industry has unbundled the generation, transmission and distribution. In most regions, the operation of the wholesale level electricity markets and the underlying physical power systems are organized in regional transmission organizations (RTOs) such as independent system operators (ISO) New England, Pennsylvania-New Jersey-Maryland (PJM) and California Independent System Operator (CAISO). Market operations have become an important part of RTOs' responsibilities in addition to ensuring physically secure electricity transmission services. Given the stronger coupling among cyber components (sensors and communication networks, in particular), physical, and financial operations in electric power systems, smart grid of the future must cope with a variety of anomalies in this cyber-physical energy system.

The primary goal of this paper is to establish an analytical framework to investigate the impact of cyber security violations on the physical and financial operations in electric power systems. As more and more advanced cyber components become integrated in RTOs' software support systems, potential cyber-security threats also raise increasing concerns. The measurement sensors equipped in today's Supervisory Control and Data Acquisition (SCADA) systems are subject to local and remote attacks. Insider attacks to control centers software systems are also likely to happen. Two major software systems, called energy management systems (EMS) and market management systems (MMS), used employed to support RTOs' physical and market operations respectively. One of the key functions of EMS is to perform state estimation [4], which converts field sensor measurements and other available information into an estimate of the state of the electric power system [4]. The estimated physical states in the system are then processed by higher level tools in both EMS and MMS to make operational and pricing decisions respectively. Given the key role of state estimation in coupling the cyber layer (field sensor measurements and communication networks) with physical and market operations, the physical and financial risks associated with an attack on state estimation require utmost attention.

Recent literature has begun to assess the impact of cyber attacks on state estimation on power system operations. In [8] the possibility of false data injection attacks against power grid state estimation was first conceived. By leveraging the knowledge of the power system topology, it was shown that false data injection attack can circumvent the bad data detection routine equipped in today's SCADA systems, therefore resulting in a manipulated snapshot of system operating states. In [9] and [12] two possible indices are proposed for quantifying the required efforts to implement such a class of malicious data attack. The proposed indices can be represented as functions of the system topology, and they could reveal the least effort attack while avoiding bad data alarms in SCADA system. In [10] and [11] computationally efficient strategies have been developed to detect these malicious data attacks against state estimators. In [6] a four-layer conceptual framework is proposed to assess potential impact of cyber attacks in deregulated electricity markets.

While most literature focus on the physical impact of cyber attacks to the power system, the potential financial risks of such a class of cyber attack are not well understood yet [13]. In this paper, we present a novel integrated framework which analyzes the economic impact of malicious data attacks against state estimators. In particular, we demonstrate how malicious attackers

Manuscript received October 16, 2010; revised April 14, 2011; accepted June 05, 2011. Date of publication November 09, 2011; date of current version November 23, 2011. This work was supported in part by Texas Engineering Experiment Station, and in part by CyLab at Carnegie Mellon under Grant DAAD19-02-1-0389 from the Army Research Office. Paper no. TSG-00186-2010.

L. Xie is with the Departments of Electrical and Computer Engineering, Texas A&M University, College Station, TX 77843 USA (e-mail: lxie@mail.ece.tamu.edu).

Y. Mo and B. Sinopoli are with the Department of Electrical and Computer Engineering, Carnegie Mellon University, Pittsburgh, PA 15213 USA (e-mail: ymo@andrew.cmu.edu; brunos@ece.cmu.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.2011.2161892

could make profitable market transactions by compromising several line flow sensors using false data injection attacks while going undetected. Such a class of malicious attacks may lead to consistent financial losses to the social welfare. By revealing such potential risks, the central message of this paper is that besides the catastrophic physical consequences cyber attacks may provoke, it is equally important to prevent economic loss due to malicious attacks in future smart grid market operations. An interdisciplinary approach based on power engineering, control systems, and communication can lead to the development of effective techniques to prevent this grim scenario from becoming reality in the near future. The main contributions of this paper can be summarized as threefold:

- We formulate the problem of malicious data injection attack against state estimation, which leads to financial misconducts in electric power market operations.
- We provide strategies for finding undetectable and profitable attacks, which can be formulated as a convex optimization problem.
- We quantify the economic impact of such malicious data attacks on electricity market operations using day-ahead and ex-post real-time pricing models in today's RTOs.

The rest of this paper is organized as follows. Section II provides the basic overview of how deregulated electric power markets are operated in major RTOs. The malicious data injection attacks against state estimation is then formulated in Section III. In Section IV we describe the attacker's strategy to leverage the malicious data attacks for virtual bidding transactions, leading to consistent financial arbitrage between day-ahead and ex-post real-time prices at selected pairs of nodes. In Section V we analyze the optimal attack strategy under the assumption that only a limited number of measurement sensors could be compromised. In Section VII numerical examples and an economic assessment of malicious data attacks on market operations are provided using the standard IEEE 14-bus system as a testbed.

II. Preliminaries

In deregulated electricity markets in the U.S. (and in many other countries), the nodal prices are determined at the regional transmission organizations (RTOs). The electric power market consists of several forward and real-time spot markets. In real-time spot markets, MMS calculates the ex-post locational marginal price (LMP) based on the actual state estimation from the SCADA system. The ex-post LMP is the settlement price for all the market participants. In this section we briefly introduce state estimation algorithm in power system operations and describe the effect of state estimation on ex-post pricing.

A. Notations

We first summarize the notations used throughout this paper in Table I. For consistency we use superscript to indicate the context of the used variables. For example Pg_i^* denotes the optimal generation power at bus i given by the ex-ante solution. Pg_i denotes the real-time generation power and $\hat{P}g_i$ is the estimated real-time generation power.

TABLE I
Notations

i	Index for generators i
j	Index for load buses j
l	Index for transmission line l
k	Time k
I	Total number of generators
J	Total number of load buses
L	Total number of transmission lines
Ld_j	Load at bus j during run time
Pg_i	Generation at i during run time
x	A vector consists of all Pg_i and Ld_j
z	Collection of sensor measurements
$C_i(Pg_i)$	Generation cost of producing Pg_i
$Pg_i^{min(max)}$	Minimum (maximum) available power from generator i
λ_i	Electricity price at bus i
F_l	Transmission flow at line l
F_l^{max}	Maximum allowed transmission flow at line l
F_l^{min}	Minimum allowed Transmission flow at line l

B. Ex-Ante Real-Time Market

The ex-ante real-time market, which usually takes place every 10 to 15 min prior to real time, conducts security-constrained economic dispatch (SCED) to determine the optimal power generation Pg_i^* given the expected load Ld_j^*. The optimal power flow solution needs to satisfy physical security constraints. Firstly, due to the inertia of generator, Pg_i^* cannot deviate generation capacity limits

$$Pg_i^{\min} \le Pg_i^* \le Pg_i^{\max}, \quad \forall i = 1, \ldots, I.$$

Secondly, power flow on each transmission line cannot exceed the transmission capacity, which implies that

$$F_l^{\min} \le F_l^* \le F_l^{\max}, \quad \forall l = 1, \ldots, L.$$

Based on the linearized dc-power flow model, the line flow vector is a linear function of the nodal injection vector

$$F = H \begin{bmatrix} Ld \\ Pg \end{bmatrix}, \tag{1}$$

where H is the distribution factor matrix of the nodal power injection vector [14]. For future analysis, we define the jth column of H to be H_j.

Therefore, the SCED problem solved in ex-ante market can be expressed as follows, the result of which will be the dispatch order given to each market participant (generator, load serving entities, etc). **Ex-ante Formulation**:

$$\begin{aligned} \underset{Pg_i^*}{\text{minimize}} \quad & \sum_{i=1}^{I} C_i\left(Pg_i^*\right) \\ \text{subject to} \quad & \sum_{i=1}^{I} Pg_i^* = \sum_{j=1}^{J} Ld_j^* \\ & Pg_i^{\min} \le Pg_i^* \le Pg_i^{\max} \quad \forall i = 1, \ldots, I \\ & F_l^{\min} \le F_l^* \le F_l^{\max} \quad \forall l = 1, \ldots, L. \end{aligned}$$

C. State Estimation in Real-Time Operations

Due to the stochastic nature of demand Ld_j, the real-time values of Pg, Ld, F may differ from the optimal Pg^*, Ld^*, F^*

calculated in the ex-ante market clearing. Hence, measurements are necessary to estimate the real-time state variables. For dc linearized power flow modes, the states are typically the bus voltage phase angle $\boldsymbol{\theta}$. Given a fixed topology and choice of slack bus, there exists a bijective relationship between bus voltage phase angle $\boldsymbol{\theta}$ and the vector of nodal power injection x [14]. Since the LMPs are explicitly calculated from nodal power injections, we define the states in this paper as the vector of nodal power injection x. Because the real-time states are typically not exactly the same as the optimal value, we have the following equations:

$$x = x^* + w, \quad F = H(x^* + w),$$

where w is the deviation of run time states from the scheduled optimal states. In this paper we will assume that w is a Gaussian random variable with zero mean and covariance Q. We assume that $I + J + L$ sensors are deployed to measure Pg_i, Ld_j, F_l respectively. As a result, the observation equation can be written in the matrix form as follows:

$$z = \begin{bmatrix} I \\ H \end{bmatrix} x + e = Cx + e, \tag{2}$$

where e is the measurement error, also assumed to be Gaussian with zero mean and covariance R.

Given z, a minimum mean square error estimator is used to estimate the state x based on the following criterion:

$$\hat{x} = argmin_{\hat{x}} \mathbb{E}\|x - \hat{x}\|_2^2. \tag{3}$$

Since we assume the observation equations and flow model to be linear, one can prove that the solution of the minimum mean square error estimator is given by

$$\hat{x} = (C'R^{-1}C)^{-1}C'R^{-1}z = Pz. \tag{4}$$

We also assume that a detector is used to detect abnormality in the measurements. Let us define the residue r to be

$$r \triangleq z - C\hat{x}. \tag{5}$$

We will assume the detector triggers an alarm based by comparing the norm of r with certain threshold, i.e. an alarm is triggered if the following event happens:

$$\|r\|_2 = \|z - C\hat{x}\|_2 > threshold. \tag{6}$$

D. Ex-Post Market

Since the run time state variables Pg, Ld, F are different from the dispatch level in ex-ante market, RTOs will calculate the vector of LMPs based on the run-time data for settlement purposes. In this paper we use the ex-post pricing model described in detail in [5]. Let us first define the positive congestion set to be

$$cl_+ = \left\{ l : \hat{F}_l \geq F_l^{\max} \right\},$$

the negative congestion set to be

$$cl_- = \left\{ l : \hat{F}_l \leq F_l^{\min} \right\},$$

and the noncongestion set to be

$$cl_0 = \{ l : l \notin cl_+, l \notin cl_- \}.$$

The ex-post market clearing solves the SCED in a small range around the actual system state in order to obtain the LMPs for settlement purposes:

Ex-post Formulation:

$$\begin{aligned} \underset{\Delta Pg_i}{\text{minimize}} \quad & \sum_{i=1}^{I} C_i(\Delta Pg_i + \hat{P}g_i) \\ \text{subject to} \quad & \sum_{i=1}^{I} \Delta Pg_i = 0 \\ & \Delta Pg_i^{\min} \leq \Delta Pg_i \leq \Delta Pg_i^{\max} \quad \forall i = 1, \ldots, I \\ & \Delta F_l \leq 0 \qquad \forall l \in cl_+ \\ & \Delta F_l \geq 0 \qquad \forall l \in cl_-, \end{aligned}$$

where $\Delta Pg_i^{\max}$ and $\Delta Pg_i^{\min}$ is usually chosen to be 0.1 MWh and -2 MWh respectively. $\hat{P}g_i$ is the estimated power generation by generator i. The Lagrangian of the above minimization problem is defined as

$$\begin{aligned} \mathcal{L} = & \sum_{i=1}^{I} C_i(\Delta Pg_i + \hat{P}g_i) - \lambda \sum_{i=1}^{I} \Delta Pg_i \\ & + \sum_{i=1}^{I} \mu_{i,max} \left(\Delta Pg_i - \Delta Pg_i^{\max} \right) \\ & + \sum_{i=1}^{I} \mu_{i,min} \left(\Delta Pg_i^{\min} - \Delta Pg_i \right) \\ & + \sum_{l \in cl_+} \eta_l \Delta F_l + \sum_{l \in cl_-} \zeta_l (-\Delta F_l). \end{aligned}$$

It is well known that the optimal solution of the optimization problem must satisfy the KKT conditions. In particular, we know that the following holds:

$$\eta_l \geq 0, \quad \zeta_l \geq 0. \tag{7}$$

To simplify the notation, we define $\eta_l = 0$ if $l \notin cl_+$, $\zeta_l = 0$ if $l \notin cl_-$. After solving the above optimization problem and computing the Lagrangian multipliers $\lambda, \mu_{i,max}, \mu_{i,min}, \eta_l, \zeta_l$, we can define the nodal price at each load bus of the network, given by

$$\lambda_j = \lambda + \sum_{l=1}^{L} (\eta_l - \zeta_l) \frac{\partial F_l}{\partial Ld_j}. \tag{8}$$

More details of the derivation of nodal price can be found in [4]. Now let us write (8) in a more compact matrix form. Let us define $\eta = [\eta_1, \ldots, \eta_L]' \in \mathbb{R}^L$ to be a vector of all η_l and $\zeta = [\zeta_1, \ldots, \zeta_L]'$. By (1), we know that $\partial F_l / \partial Ld_j = H_{lj}$, where H_{lj} is the element on the lth row and jth column of H. Hence, (8) can be simplified as

$$\lambda_j = \lambda + H_j^T(\eta - \zeta), \tag{9}$$

where H_j is the jth column of H matrix. The difference of price at two nodes j_1 and j_2 is given by

$$\lambda_{j_1} - \lambda_{j_2} = (H_{j_1} - H_{j_2})^T (\eta - \zeta). \tag{10}$$

III. Attack Model

In this section we assume that a malicious third party wants to attack the system and make a profit from the market, by compromising a number of sensors and sending bogus measurements to the RTO. We assume the attacker has the following capabilities:

1) The attacker has full knowledge the underlying system topology.
2) The attacker knows the optimal states Pg^*, Ld^*, F^* published by the RTO from the ex-ante market.
3) The attacker compromised several sensors and can manipulate their readings arbitrarily. We consider two possible scenarios:
   a) The attacker has already compromised a fixed subset of sensors. Let us define matrix $\Gamma = diag(\gamma_1, \ldots, \gamma_{I+J+L})$, where γ_i is a binary variable and $\gamma_i = 1$ if and only if sensor i is compromised. Hence, the corrupted measurements received by the RTO can be written as $z' = z + z^a$, where z^a, which lie in the column space of Γ, is the bias introduced by the attacker.
   b) The attacker can choose which sensor to compromise, however due to limited resources, he can only compromise no more than N sensors. In that case, we can still write the corrupted measurement as $z' = z + z^a$. However, instead of requiring z^a to lies in certain subspace, we now require z^a to have no more than N nonzero elements.

Based on the above assumptions, the state estimation equations can be written as

$$\hat{x}' = Pz' = \hat{x} + Pz^a. \tag{11}$$

Thus, the new residue becomes $r' = r + (I - CP)z^a$. By triangular inequality,

$$\|r'\|_2 \leq \|r\|_2 + \|(I - CP)z^a\|_2 .$$

As a result, if $\|(I-CP)\Delta z^a\|_2$ is small, then with a large probability the detector cannot distinguish r' and r. In the limit case, if $(I - CP)\Delta z = 0$, then r' will pass the detector whenever r passes the detector. Based on these arguments, we give the following definition:

Definition 1: The attacker's input z^a is called ε-feasible if $\|(I - CP)z^a\|_2 \leq \varepsilon$.

Remark 1: ε is a design parameter for the attacker depending on how subtle he wants the attack to be. An attack with smaller ε will be more likely to be undetected by the RTO. However, the magnitude of attacker inputs, and hence the attacker's ability to manipulate the state estimation, will be limited. In the rest of the paper we will assume ε is predetermined by the attacker.

Besides being unnoticeable, the attack must also be profitable to the attacker. In this paper, we assume that the attacker will exploit the virtual bidding mechanism to make a profit. In many RTOs such as ISO-New England, virtual bidding activities are legitimate financial instruments in electricity markets. A market participant purchase/sell a certain amount of virtual power Po at location i in day-ahead forward market, and will be obliged to sell/purchase the exact same amount in the subsequent real-time market. Therefore, the attacker's action can be summarized as:

- In day-ahead forward market, buy and sell virtual power Po at locations j_1 and j_2 at price $\lambda_{j_1}^{DA}, \lambda_{j_2}^{DA}$, respectively.
- Inject z^a to manipulate the nodal price of ex-post market.
- In ex-post market, sell and buy virtual power Po at locations j_1 and j_2 at price $\lambda_{j_1}, \lambda_{j_2}$, respectively.

The profit that the attacker could obtain from this combination of virtual trading is

$$\begin{aligned} Profit &= \left(\lambda_{j_1} - \lambda_{j_1}^{DA}\right) Po + \left(\lambda_{j_2}^{DA} - \lambda_{j_2}\right) Po \\ &= \left(\lambda_{j_1} - \lambda_{j_2} + \lambda_{j_2}^{DA} - \lambda_{j_1}^{DA}\right) Po. \end{aligned}$$

Let us define

$$p = \lambda_{j_1} - \lambda_{j_2} + \lambda_{j_2}^{DA} - \lambda_{j_1}^{DA}. \tag{12}$$

Combined with (10), (12) can be written as

$$p(z') = (H_{j_1} - H_{j_2})^T (\eta(z') - \zeta(z')) + \lambda_{j_2}^{DA} - \lambda_{j_1}^{DA}.$$

Ideally, the attacker would like to enforce that $p(z') > 0$. However, since the system is stochastic and the z' vector is partially unknown to the attacker, it can only try to guarantee that $\mathbb{E}p(z') > 0$, i.e., the attack is profitable in the expected sense. Such a problem is still quite hard since the relationship between η, ζ and z' is given by the Lagrangian multiplier and hence implicit. As a result, Monte Carlo method may be used in order to compute $\mathbb{E}p(z')$. In the next section, we will exploit the structure of the ex-post formulation and develop a heuristic for the attacker.

IV. Scenario I: Predetermined Subset of Compromised Sensors

In this section, we develop a heuristic for the attacker to find a profitable input z^a when the subset of compromised sensors is fixed. We will show that such a problem can be effectively formulated as a convex optimization problem and solved efficiently. Let us define the set

$$L_+ = \{l : H_{l,j_1} > H_{l,j_2}\},$$

and

$$L_- = \{l : H_{l,j_1} < H_{l,j_2}\}.$$

As a result, $p(z')$ can be written as

$$\begin{aligned} p(z') = &\sum_{l \in L+} (H_{l,j_1} - H_{l,j_2}) (\eta_l(z') - \zeta_l(z')) \\ &+ \sum_{l \in L-} (H_{l,j_2} - H_{l,j_1}) (\zeta_l(z') - \eta_l(z')) + \lambda_{j_2}^{DA} - \lambda_{j_1}^{DA}. \end{aligned} \tag{13}$$

By the fact that $\eta_l(\zeta_l)$ is nonnegative and it is 0 if the line is not positive (or negative) congested, we can see that the following conditions are sufficient for $p(z') > 0$

(A1) $\lambda_{j_2}^{DA} > \lambda_{j_1}^{DA}$.

(A2) $F_l' < F_l^{\max}$ if $l \in L_-$, i.e., the line is not positive congested.

(A3) $\hat{F}'_l > F_l^{\min}$ if $l \in L_+$, i.e., the line is not negative congested.

(A1) can be easily satisfied in the day-ahead market. Hence, the attacker needs to manipulate the measurement z' to make sure that (A2) and (A3) hold or at least hold with a large probability. Following such intuition, we give the following definition:

Definition 2: An attack input z^a is called δ-profitable if the following inequalities hold

$$\begin{aligned} &\mathbb{E}\hat{F}'_l \le F_l^{\max} - \delta, \quad \forall l \in L_-, \\ &\mathbb{E}\hat{F}'_l \ge F_l^{\min} + \delta, \quad \forall l \in L_+, \end{aligned}$$

where $\mathbb{E}\hat{F}' = F^* + HPz^a$.

Remark 2: It is worth mentioning that δ does not directly relate to the profit (or expected profit). However, it is related to the probability that (A2) and (A3) hold. Recall that from the attacker's perspective, $\hat{F}'$ is a Gaussian random variable with mean $\mathbb{E}\hat{F}'$. As a result, a large margin δ will guarantee that with large probability (A2) and (A3) are not violated.

Therefore, the attacker's strategy during the run time is to find an ε feasible z^a such that the margin δ is maximized. The problem can be formulated as

$$\begin{aligned} \underset{z^a \in span(\Gamma)}{\text{maximize}} \quad & \delta \\ \text{subject to} \quad & \|(I - CP)z^a\|_2 \le \varepsilon \\ & \mathbb{E}\hat{F}'_l \le F_l^{\max} - \delta \qquad \forall l \in L_- \\ & \mathbb{E}\hat{F}'_l \ge F_l^{\min} + \delta \qquad \forall l \in L_+ \\ & \delta > 0. \end{aligned}$$

It is easy to verify that the objective function and all the constraints are convex. Therefore, the problem itself is a convex programming problem and can be solved efficiently [16].

Remark 3: It may happen that the above convex optimization problem is infeasible. In other words, the sensors compromised by the attacker are not sufficient to decongest all the lines in L_- and L_+. In that case, we can relax the above optimization problem by adding a penalty on those lines that are congested in the undesirable directions. The new formulation is as follows:

$$\begin{aligned} \underset{z^a \in span(\Gamma)}{\text{maximize}} \quad & \delta - D\sum_{l=1}^{l} \beta_l \\ \text{subject to} \quad & \|(I - CP)z^a\|_2 \le \varepsilon \\ & \mathbb{E}\hat{F}'_l \le F_l^{\max} - \delta + \beta_l \qquad \forall l \in L_- \\ & \mathbb{E}\hat{F}'_l \ge F_l^{\min} + \delta - \beta_l \qquad \forall l \in L_+ \\ & \delta > 0 \\ & \beta_l > 0 \qquad \forall l = 1, \ldots, l, \end{aligned}$$

where $D > 0$ is the weight of the penalty and β_l is the relaxation variable.

V. Scenario II: Limited Resources to Compromise Sensors

In this section, we consider a scenario in which the attacker can select the set of sensors to compromise. However, due to limited resources, the total number of compromised sensor cannot exceed certain threshold N. As a result, not only does the attacker need to design an optimal input to system, but also it need to choose the optimal set of sensors to compromise.

Following the previous argument, we can write the optimization problem as

$$\begin{aligned} \underset{z^a}{\text{maximize}} \quad & \delta \\ \text{subject to} \quad & \|(I - CP)z^a\|_2 \le \varepsilon \\ & \mathbb{E}\hat{F}'_l \le F_l^{\max} - \delta \qquad \forall l \in L_- \\ & \mathbb{E}\hat{F}'_l \ge F_l^{\min} + \delta \qquad \forall l \in L_+ \\ & \delta > 0 \\ & \|z^a\|_0 \le N, \end{aligned}$$

where $\|\cdot\|_0$ is the zero norm, which is defined as the number of nonzero elements in a vector. Note that in this formulation we do not require that z^a lies in the span of Γ, but instead we require z^a to have no more than N nonzero elements. The nonzero elements of z^a correspond to the sensors the attacker needs to compromise.

However, the above formulation is a hard combinatorial problem, since it involves a constraint involving the zero norm of a vector, which is not convex. To render the problem solvable, we resort to a convex relaxation of the original optimization problem, using the method developed in [15]. According to this method, the L_0 norm is substituted with a weighted L_1 norm, where the weights are chosen to avoid the penalization, given by the L_1 norm, of the bigger coefficients. In that paper, the authors propose an iterative algorithm that alternates between an estimation phase and a redefinition the weights, based on the empiric consideration that the weights should relate inversely to the true signal magnitudes. The resulting algorithm is composed of the following four steps:

1) Set the iteration count c to zero and set the weights vector to $w_i^0 = 1$ for $i = 1, \ldots, I + J + L$.
2) Solve the weighted L_1 minimization problem

$$\begin{aligned} \underset{z^a}{\text{maximize}} \quad & \delta \\ \text{subject to} \quad & \|(I - CP)z^a\|_2 \le \varepsilon \\ & \mathbb{E}\hat{F}'_l \le F_l^{\max} - \delta \qquad \forall l \in L_- \\ & \mathbb{E}\hat{F}'_l \ge F_l^{\min} + \delta \qquad \forall l \in L_+ \\ & \delta > 0 \\ & \sum_i |z_i^a w_i^c| \le N, \end{aligned}$$

   Let the solution be $z_1^{a,c}, \ldots, z_{I+J+L}^{a,c}$.
3) Update the weights

$$w_i^{c+1} = \frac{1}{|z_i^{a,c}| + \zeta}, \quad i = 1, \ldots, I + J + L,$$

   where ζ is a small positive constant.
4) Terminate on convergence or when c reaches a specified maximum number of iterations $c_{\max}$. Otherwise, increment c and go to step 2.

Remark 4: Similarly to [15], here we introduce the parameter $\zeta > 0$ in step 3 in order to avoid inversion of zero-valued component in z^a.

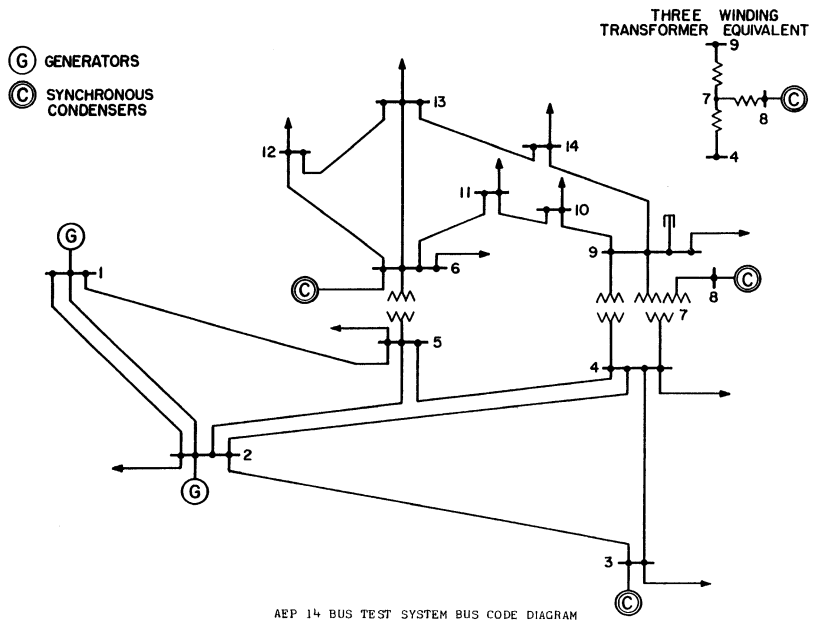

Fig. 1. IEEE standard 14-bus system.

TABLE II
CASE DESCRIPTION

	congested lines in day-ahead (from bus-to bus)	virtual bidding nodes	compromised sensors
Case I	1-2	2 and 4	line flow sensors 1-2, 3-4
Case II	1-2, 2-4, 2-5	1 and 2	line flow sensors 1-2, 2-3, 2-4
Case III	1-2, 2-4, 2-5	1 and 2	line flow sensors 1-2, 2-3

The economic impact on power market operations due to such a class of false data injection attacks is illustrated in the next section.

VI. ILLUSTRATIVE EXAMPLES

In this section we consider the standard IEEE 14-bus system in Fig. 1 to discuss the economic impact of malicious data attacks against state estimation. The system comprises a total of five generators. Three cases, summarized in Table II, are analyzed. In Case I, only one transmission line is congested and two line flow sensors are assumed to be compromised using false data injection attack. In Cases II and III, we assume there are multiple congested transmission lines. Compared with Case II, Case III only allows a limited number of sensors which can be compromised. As a result, the attacker needs to both pick a subset of sensors and its input.

In Cases I and II, an attacker follows the procedure described in the end of Section III with the purpose of gaining profit from virtual bidding. In Case III, the attacker follows the limited sensor attack algorithm described in Section V. At the pair of the nodes that are prespecified in the third column of Table II, the attacker buys and sells the same amount of virtual power in day-ahead market at nodes j_1 and j_2, respectively. Based on historical trends, the attacker buys at the lower priced node and sell at the higher priced node.[1] In real-time market operations, the attacker compromises the selected line flow sensors by injecting false data without being detected. By doing so, the congested transmission lines in day-ahead operations appear no longer congested from the system state estimation. This, in turn, will result different real-time ex-post LMPs with controllable bias compared to the day-ahead LMPs.[2]

In Case I, only one transmission line (from bus 1 to bus 2) is congested. The attacker chooses to buy same amount of virtual power at bus 4 (lower price) and sells virtual power at bus 2 (higher price) in day-ahead market. By compromising two line flow measurement sensors with false data injection, the transmission line congestion appears to be relieved in real-time EMS. This manipulated system state is then passed to real-time market clearing procedure, which computes a uniform ex-post LMP across the system. Fig. 2 shows the LMPs with and without the cyber attacks. Based on (12), the profit of such transaction is about \$2/MWh. In Case II, day-ahead market clearing shows that there are three congested lines, bus 1 and bus 2 have LMP difference of about \$8/MWh. By compromising three line flow sensors indicated in the third column of Table II, the designated pair of nodes (buses 1 and 2) has the same LMP in ex-post real-time market. The reason is that malicious data injection attacks to these three sensors lower the estimated line flow, thereby setting the shadow prices of the actual congested lines to be zero. The profit of such transaction is approximately \$8.2/MWh. In Case III, we assume that an attacker can compromise at most two sensors. By applying the algorithm described in Section V, the attacker chooses to compromise line flow sensors between nodes 1–2, and nodes 2–3. Compromising only

[1]The choice of pairs of nodes does not necessarily have to be between a congested transmission line [14]. As long as the pair of nodes exhibit consistent nodal price differences, this pair of nodes could be a candidate.

[2]To illustrate the effect of the attacks on ex-post market clearing prices, we assume that the load forecast at day-ahead is perfect. In other words, if there were no cyber attacks, the day-ahead LMP will be the same as the ex-post LMP.

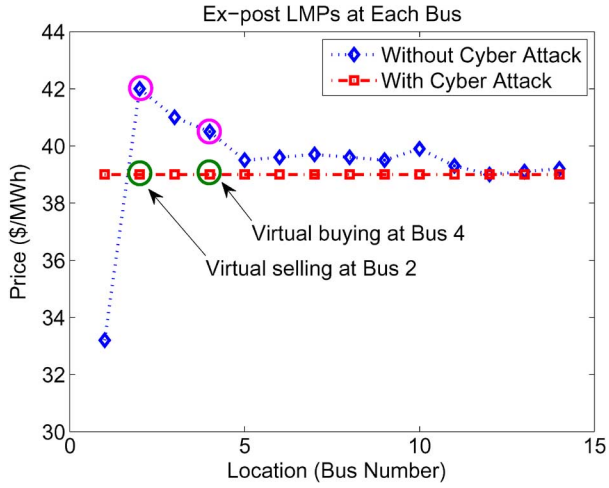

Fig. 2. LMP with and without cyber attacks (only one line congestion).

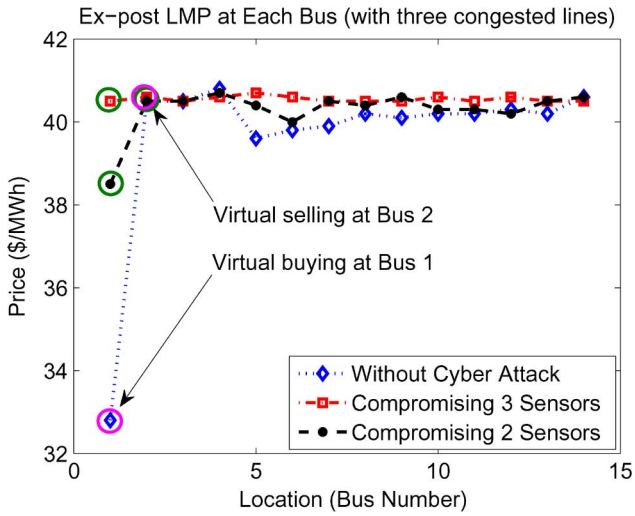

Fig. 3. LMP with and without cyber attacks (three congested lines).

these two sensors cannot make all the congested lines appear uncongested in real-time operations. However, as shown in Fig. 3, compromising just two sensors can still generate $6.0/MWh of profit for the attacker.

In Table III we compare the attack efforts and the associated expected financial profits for all the three cases. We use the infinity norm of z_a normalized by the infinity norm of z as an indicator of the attacker's effort. As the system congestion becomes more complex, the potential of financial gain by maliciously placing false data attacks is also higher. One can observe from the comparison between Case II and Case III that if the attacker can only compromise a limited number of sensors, then the expected profits decrease. However, even compromising a very small number of sensors (e.g. two sensors in the Case III) can lead to profits, showing how the economic losses due to even small false data injection attacks can be significant in the long run.

VII. Conclusions and Future Work

In this paper we examine the possible economic impact of false data injection attacks against state estimation in electric power market operations. We show how an attacker can manipulate the nodal price of ex-post real-time market without being detected by the state estimators. In conjunction with virtual bidding, these integrity attacks can lead to consistent financial profit for the attacker. A heuristic is developed to compute the optimal injection of false data from the attacker's perspective. False data injection attacks with a limited number of sensors are formulated as a convex optimization problem and thus solved efficiently by the attacker. Illustrative examples in IEEE 14-bus system show that the potential economic gain for the attackers are significant even with small number of sensors being compromised by the attackers.

TABLE III
Attack Efforts and Profits ($\varepsilon = 1$ MWh)

	relative efforts ($\frac{\|z_a\|_\infty}{\|z\|_\infty}$)	profits (% of transaction cost)
Case I	1.23%	2.40%
Case II	1.41%	9.46%
Case III	1.31%	7.54%

In future work, the development of countermeasures to mitigate the financial risks of malicious data injection attacks will be investigated. We also plan to study the sensitivity of different ex-post LMP pricing models subject to such a class of malicious data injection attacks [17]. Another important future direction of research is to conduct more realistic case studies, and investigate the accumulate profit of such attacks. Finally, we believe that future robust state estimation algorithms which could detect these false/malicious data injections need to be developed.

Acknowledgment

The authors would like to thank Dr. Feng Zhao of ISO-New England for informative discussion on the electricity market pricing models. The views and conclusions contained here are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either express or implied, of ARO, Texas A&M, Carnegie Mellon, or the U.S. Government or any of its agencies.

References

[1] S. M. Amin and B. F. Wollenberg, "Toward a smart grid," *IEEE Power Energy Mag.*, vol. 3, no. 5, pp. 34–41, Sep./Oct. 2005.
[2] M. D. Ilić, L. Xie, U. A. Khan, and J. M. F. Moura, "Modeling of future cyber-physical energy systems for distributed sensing and control," *IEEE Trans. Systems, Man, Cybern. A, Syst. Hum.*, vol. 40, no. 4, pp. 825–838, Jul. 2010.
[3] F. F. Wu, K. Moslehi, and A. Bose, "Power system control centers: Past, present, and future," *Proc. IEEE*, vol. 93, no. 11, pp. 1890–1908, Nov. 2005.
[4] F. C. Schweppe, J. Wildes, and D. B. Rom, "Power system static state estimation, Parts I, II and III," *IEEE Trans. Power App. Syst.*, vol. PAS-89, no. 1, pp. 120–135, Jan. 1970.
[5] F. Li, Y. Wei, and S. Adhikari, "Improving an unjustified common practice in ex post LMP calculation," *IEEE Trans. Power Syst.*, vol. 25, no. 2, pp. 1195–1197, May 2010.
[6] M. Negrete-Pincetic, F. Yoshida, and G. Gross, "Towards quantifying the impacts of cyber attacks in the competitive electricity market environment," *Proc. IEEE PowerTech*, Jul. 2009.
[7] D. Salem-Natarajan, L. Zhao, W. Shao, M. Varghese, S. Ghosh, M. Subramanian, G. Lin, H. Chiang, and H. Li, "State estimator for CA ISO market and security applications-relevance and readiness," in *Proc. IEEE Power Energy Soc. Gen. Meet.*, Jul. 2008.
[8] 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*, 2009.
[9] H. Sandberg, A. Teixeira, and K. H. Johansson, "On security indices for state estimators in power networks," in *Proc. 1st Workshop Secure Control Syst. (CPSWEEK)*, Apr. 2010.

[10] O. Kosut, L. Jia, R. Thomas, and L. Tong, "Limiting false data attacks on power system state estimation," in *Proc. Conf. Inf. Sci. Syst.*, Mar. 2010.
[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] G. Dan and H. Sandberg, "Stealth attacks and protection schemes for state estimators in power systems," in *Proc. 1st IEEE Smart Grid Commun. Conf.*, Oct. 2010.
[13] L. Xie, Y. Mo, and B. Sinopoli, "False data injection attacks in electricity markets," in *Proc. 1st IEEE Smart Grid Commun. Conf.*, Oct. 2010.
[14] F. F. Wu, P. Varaiya, P. Spiller, and S. Oren, "Folk theorems on transmission access: Proofs and counterexamples," *J. Regul. Econ.*, vol. 10, no. 1, pp. 5–23, Jul. 1996.
[15] E. J. Candes, M. B. Wakin, and S. Boyd, "Enhancing sparsity by reweighted l1 minimization," *J. Fourier Anal. Appl.*, vol. 14, no. 5, pp. 877–905, Dec. 2008.
[16] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.
[17] T. Zheng and E. Litvinov, "On ex post pricing in the real-time electricity market," *IEEE Trans. Power Syst.*, vol. 26, no. 1, pp. 153–164, Feb. 2011.

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 the Department of Electrical and Computer Engineering, 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. His industry experience includes an internship at ISO-New England and an internship at Edison Mission Energy Marketing and Trading. His research interest is the modeling and control of large-scale power systems with renewable energy resources, smart grids, and electricity markets.

Yilin Mo received the B.Eng. degree from the Department of Automation, Tsinghua University, Beijing, China, in 2007. He is currently working toward the Ph.D. Degree in electrical and computer engineering from Carnegie Mellon University, Pittsburgh, PA.

His research interests include secure control systems and networked control systems, with applications in sensor networks.

Bruno Sinopoli received the Dr. Eng. degree from the University of Padova in 1998 and the M.S. and Ph.D. degrees in electrical engineering from the University of California at Berkeley (UC Berkeley) in 2003 and 2005 respectively.

After a postdoctoral position at Stanford University, he joined the faculty at Carnegie Mellon University, Pittsburgh, PA, where he is an Assistant Professor in the Department of Electrical and Computer Engineering with courtesy appointments in Mechanical Engineering and in the Robotics Institute. His research interests include networked embedded control systems, distributed estimation, and control with applications to wireless sensor-actuator networks and system security.

Dr. Sinopoli was awarded the 2006 Eli Jury Award for outstanding research achievement in the areas of systems, communications, control and signal processing at UC Berkeley and the NSF Career award in 2010.