False Data Injection Attacks in Electricity Markets

Le Xie*, Yilin Mo† and Bruno Sinopoli†
*Department of Electrical and Computer Engineering, Texas A&M University, College Station, TX, USA
Email: Lxie@mail.ece.tamu.edu
†Department of Electrical and Computer Engineering, Carnegie Mellon University, Pittsburgh, PA, USA
Email: ymo@andrew.cmu.edu, brunos@ece.cmu.edu

***Abstract*—We present a potential class of cyber attack, named *false data injection attack*, against the state estimation in deregulated electricity markets. With the knowledge of the system configuration, we show that such attacks will circumvent the bad data measurement detection equipped in present SCADA systems, and lead to profitable financial misconduct such as virtual bidding the ex-post locational marginal price (LMP). We demonstrate the potential attacks on an IEEE 14-bus system.**

I. Introduction

The electric power industry is undergoing profound changes as our society increasingly emphasizes the importance of a smarter grid in support of sustainable energy integration and utilization. Enabled by the technological advances in sensing, communication, and actuation, the monitoring and control of future electric power system is likely to involve many more real-time information gathering and processing devices such as Phasor Measurement Units (PMUs). While major research efforts have been conducted in improving the power system operational efficiency and reliability by use of novel cyber technologies, the potential risks of cyber security bleach on electric energy systems also need to be seriously investigated before massively deploying these smart grid technologies. Institutionally, the deregulation of electricity industry has unbundled the generation and transmission. Market participants such as independent power producers (IPPs), load serving entities (LSEs), and virtual market participants could submit their bids and offers in a variety of electricity markets, the operation of which depends on the physical power system status. In this paper we investigate a potential cyber security bleach scenario in the power system state estimators, which could lead to financially profitable misconducts in electricity markets.

The physical and financial operations in electric power system become much more different after the industry deregulation. 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). The market operations are performed in a software engine named Market Management System (MMS). The physical information of the electric power grid is measured, communicated, and estimated in another package named Energy Management System (EMS).

The well functioning of the electricity market relies on faithful characterization of the real-time physical power system information. As more and more advanced cyber technologies are getting integrated into the EMS, potential cyber attack threats are becoming a major security concern for RTOs. One of the key functions in EMS is the state estimation routine, which provides robust estimation of the entire power grid's real-time information according to field measurements. In [6] the scheme of false data injection attack against power grid state estimation was first introduced. By leveraging the knowledge of the power network topology, it was shown that false data injection attack could bypass the bad data detection in today's Supervisory Control and Data Acquisition (SCADA) system. In [7] two possible indices are proposed in order to quantify required efforts to implement such a class of attack. As a function of the system topology, the indices could reveal the least effort needed to achieve attack goals while avoiding bad-data alarms in the control center. In [8] efforts have been made to develop computationally efficient heuristics to detect these false data attacks against state estimators. However, the potential risks and costs of such a class of cyber attack are not well understood yet. In [4] an attempt has been made to systematically model the potential impact of cyber attacks in deregulated electricity market operations.

While most cyber attack study on the SCADA systems for the electric power transmission network primarily focuses on the physical impact of such attacks, this paper presents a novel integrated which shows the potential financial misconduct that may be induced from cyber attack. In addition to the catastrophic electric power system blackout scenarios that cyber attacks can affect, the proposed scheme will be much more often with cumulative significant financial losses to the social welfare. The physical and financial impact of these cyber attacks may lead to more vulnerable testing from entities. The objective of this paper is to reveal such potential risks, and to convey a starting formulation to analyze, and prevent such a class of cyber attacks. An interdisciplinary approach with power, control, and communication aspects would lead to important findings to prevent such cyber attacks from happening in the future. We illustrate in an IEEE standard 14-bus system the possibility of such a class of cyber attack-induced financial misconduct.

We present in this paper a first attempt to convey the potential financial risks that could be induced by these false data injection attacks. In summary, the main contribution of this paper is twofold:

978-1-4244-6511-8/10/$26.00 ©2010 IEEE

- We posed the problem of the data injection attack against state estimation in deregulated electricity markets, which leads to financial misconduct .
- We provided a heuristic for finding profitable attack, which can be formulated as a convex optimization problem.

The rest of this paper is organized as follows. Section II provides basic background of how electricity markets are operated in major RTOs. The possible false data injection attack model is then elaborated in Section III. In Section IV we present from the attacker's perspective how a false virtual bidding could be performed in conjunction with a false data injection attack. Numerical example in an IEEE standard system and discussions are presented in Section V. Concluding remarks and future work are drawn in Section VI.

II. Preliminaries

In deregulated electricity markets, the nodal price of electric energy is determined at the Regional Transmission Organizations (RTOs). The electric energy market consists of several look-ahead forward markets and real-time spot market. In the real-time spot market, the Market Operations will calculate the ex-post locational marginal price (LMP) based on the actual state estimation from the SCADA system, the results of which will be the final settlement price. In this section we will briefly introduce state estimation algorithm in power grid and how it will affect the ex-post market.

A. Notations

We first summarize the notations which will be used throughout this paper in Table I. We will also use superscript to indicate the contexts of 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
$\lambda_i(k)$	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 Market

The Ex-Ante market is used to compute optimal generation power Pg_i^* with minimum total cost for each generator given the predicted load Ld_j^*. Moreover, the optimal solution needs to satisfy certain safety and operation constraints. First, due to the inertia of generator, Pg_i^* cannot deviate too large from the current generation power. Thus, the constraints can be expressed as

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

where Pg_i^{min}, Pg_i^{max} are functions of the current generation power and ramping rate of the generator. Second, the power flow for each transmission line must remain within the capacity, which implies that

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

LMPs are calculated based on the linearized DC- optimal power flow model. Therefore, we can represent the line flow vector as a linear function of nodal injection vector:

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

where H is the distribution factor matrix of the nodal injection vector. For future analysis, we would like to define the jth column of H to be H_j.

By all the previous argument, the Ex-Ante market will try to solve the following optimization problem

Ex-Ante Formulation:

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

The solution of the above minimization problem will be published and sent to each generator.

C. Real-time Market Model and State Estimation

Due to the stochastic nature of demand Ld_j, the real time Pg, Ld, F may be different from the optimal value Pg^*, Ld^*, F^*. Hence, it is necessary to measure the real time system in order to estimate the real-time state variables. To simplify notation, let us denote the state x as the vector consists of net power injection at each bus [1]. Since the real-time states are different from the optimal value, we have the following equations

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

where w is the deviation of run time states from the scheduled optimal states. In this paper we will assume that w is a

[1] Under the assumption of DC power flow, there exists bijective relationship between bus voltage phase angle and net power injection [9].

Gaussian random variable with zero mean and covariance Q. We assume that $I+J+L$ number of 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 which is 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 are linear, one can proof that the solution of the minimum mean square error estimator is given by

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

where $P \triangleq (C'RC)^{-1}C'R$. 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 states Pg, Ld, F is different from the optimal states given by Ex-Ante market, it is reasonable to recalculated the nodal price based on the run time data. In this paper we will use the Ex-Post market model proposed by [3]. Let us first define the positive congestion set to be

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

the negative congestion set to be

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

and the non congestion set to be

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

The Ex-Post Market will try to solve the following optimization problem:

Ex-Post Formulation:

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

where ΔPg_i^{max} and ΔPg_i^{min} is usually chosen to be $0.1MWh$ and $-2MWh$ respectively. The Lagrangian of the above minimization problem is defined as

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

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

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

To simply 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 multiplier $\lambda, \mu_{i,max}, \mu_{i,min}, \eta_l, \zeta_l$, we can define the nodal price at each load bus of the network, which is 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 [1]. 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 a malicious third party want to attack the system by compromising certain number of sensors and sending bogus measurement to the RTO in order to make a profit from the market. The attacker is assumed to have the following capabilities:

1) The attacker knows the underlying system model and price model.
2) The attacker knows the optimal states Pg^*, Ld^*, F^* given by the Ex-Ante market.
3) The attacker compromised several 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 by the attacker. Hence, the corrupted measurements received by the RTO can be written as

$z' = z + z^a$, where $z^a \in span(\Gamma)$ is the bias introduced by the attacker[2].

Based on the above assumptions, we can write the state estimation equations as

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

Therefore, the new residue $r' = r + (I - CP)z^a$. By triangular inequality, we know that

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

Thus, 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:

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

Remarks 1: ε is a design parameter for the attacker. A smaller ε causes more difficulties for the RTO to detect the attack. On the other hand, a smaller ε also limits the magnitude of attacker inputs. In the rest of the paper we will assume ε is pre-determined by the attacker.

Besides being unnoticeable, the attack must also bring profit 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 New England and PJM, virtual bidding activities are legitimate financial instruments in electricity markets. A market participant purchase/sell a certain amount of virtual power P at location i in day-ahead forward market, and will be obligated to sell/purchase the exact same amount in the corresponding real-time market. Therefore, the attacker's action can be summarized as

- In day-ahead forward market, buy and sell virtual power P 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 P at locations j_1 and j_2 at price λ_{j_1}, λ_{j_2}, respectively.

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

$$\begin{aligned} Profit &= (\lambda_{j_1} - \lambda_{j_1}^{DA})P + (\lambda_{j_2}^{DA} - \lambda_{j_2})P \\ &= (\lambda_{j_1} - \lambda_{j_2} + \lambda_{j_2}^{DA} - \lambda_{j_1}^{DA})P \end{aligned}$$

Let us define

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

Combining (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 to make a profit, the attacker would like to enforce that $p(z') > 0$. However, since the system is stochastic and the attacker does not know the whole z' vector, 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 implicit and hence Monte Carlo method may be needed 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. Main Result

In this section, we will develop a heuristic for the attacker, which can be effectively formulated as a convex optimization problem and solved efficiently. First 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

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

Now by the fact that $\eta_l(\zeta_l)$ is non-negative and is 0 if the line is not positive(negative) congested, we know that the following conditions are sufficient for $p(z') > 0$

1) $\lambda_{j_2}^{DA} > \lambda_{j_1}^{DA}$.
2) $\hat{F}_l' < F_l^{max}$ if $l \in L_-$, i.e. the line is not positive congested.
3) $\hat{F}_l' > F_l^{min}$ if $l \in L_+$, i.e. the line is not negative congested.

The first condition can be easily satisfied in the day-ahead market. As a result, the attacker needs to manipulate the measurement z' to make sure that the last two conditions hold. Following such intuition, we give the following definition:

Defnition 2: An attack input z^a is called δ-profitable if the following holds

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

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

Remarks 2: Since the real $\hat{F}'$ is a Gaussian random variable with mean $\mathbb{E}\hat{F}'$, a large margin δ will guarantee that with large probability the last two conditions are not violated.

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

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

[2] $span(\Gamma)$ refers to the vector space containing all the subspaces of Γ.

Remarks 3: It is possible that the above convex optimization problem is infeasible. In other words, with the compromised sensors, the attacker could not guarantee that all the lines in L_- are not positively congested and all the lines in L_+ are not negatively congested. In that case, the attacker could instead seek to decongest as many lines as possible. As a result, the attacker could relax the hard constraints to soft constraints by adding penalties on the congested lines, which leads to the following formulation:

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

where $D > 0$ is the weight of the penalty and β_l is the penalty for line l.

V. Illustrative Examples

In this Section we illustrate examples of financial virtual bidding misconducts, which are direct consequences of false data injection attack against the EMS state estimators. Figure 1 shows the topology of the IEEE 14-bus system. There are a total of five generators in this system. Table II describes two scenarios that are simulated. In both cases, a small subset of transmission line flow sensors are compromised by false data injection attack.

A malicious attacker follows the procedure described in the end of Section III with the purpose of gaining profit from virtual bidding. At the pair of the nodes that are pre-specified in the third column of Table II, an attacker purchases 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 purchases at the lower price node and sells at the higher price node [3]. In real-time market, the attacker then executes false data injection attacks on the selected sensors in order to remove a subset of congested lines. 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.

In Case I, only one transmission line (from bus 1 to bus 2) is congested. The attacker chooses to buy virtual power at bus 4 and sells virtual power at bus 3 in day-ahead market. By compromising two line flow sensors with false data injection, the transmission line congestion gets relieved, leading to a system-wide uniform ex-post market price. Figure 2 shows the LMPs with and without the cyber attacks. Based on (12), the profit of such transaction is about $1/MWh. In Case II, there are three congested lines in the day-ahead market. By compromising three line flow sensors, the desired attack pair of nodes (buses 1 and 2) result in the same LMP in ex-post market. The reason is that the cyber attacks maliciously lower the estimated line flow information, thereby setting the shadow prices of the actual congested lines to be zero. The profit of such transaction is about $8/MWh. In Table III we compare the attack efforts and expected financial profits for both cases. We use the norm infinity of z_a with respect to the norm infinity of z as an indicator of the attack efforts. As the system congestion becomes more complex, the potential of gaining financial profits by maliciously placing false data attack is also higher. Due to the space limitation, here we do not elaborate the numerical stability of the RTOs' market clearing software.

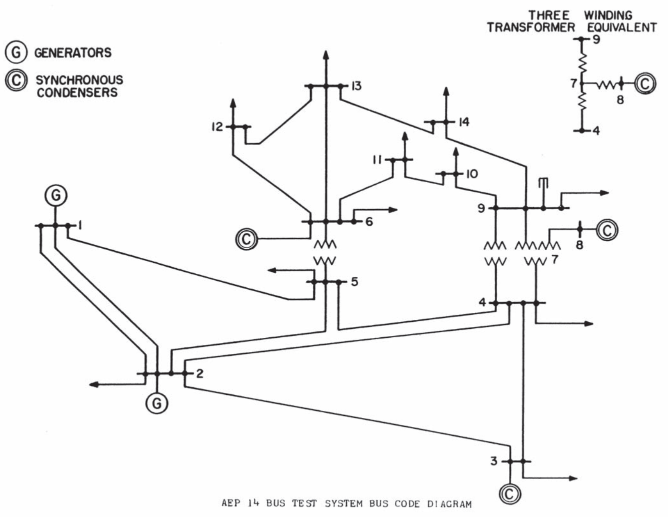
GENERATORS
SYNCHRONOUS CONDENSERS
THREE WINDING TRANSFORMER EQUIVALENT
9
7
8
4
13
12
14
11
10
1
6
9
8
5
7
4
2
3
G
C
AEP 14 BUS TEST SYSTEM BUS CODE DIAGRAM

Fig. 1. IEEE standard 14-bus system

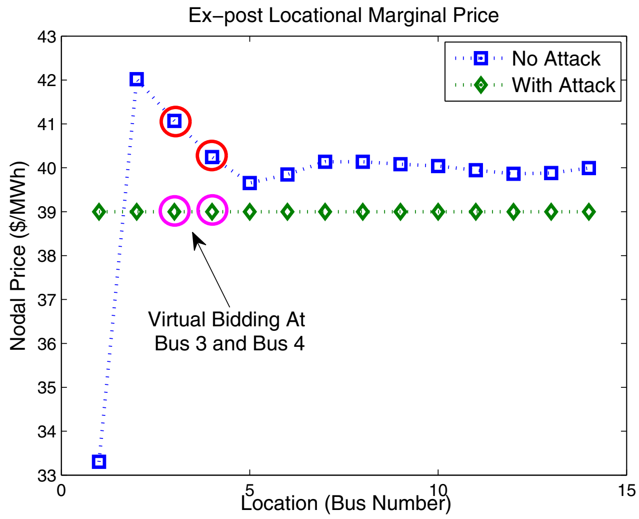

Fig. 2. LMP with and without cyber attacks (only one line congestion)

[3] The choice of pairs of nodes do not necessarily have to be between a congested transmission line [9]. As long as the pair of nodes exhibit consistent sign on nodal price difference, it could be a candidate.

TABLE II
CASE DESCRIPTION

	congested lines in day-ahead (from bus-to bus)	virtual bidding nodes	compromised sensors
Case I	1-2	3 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

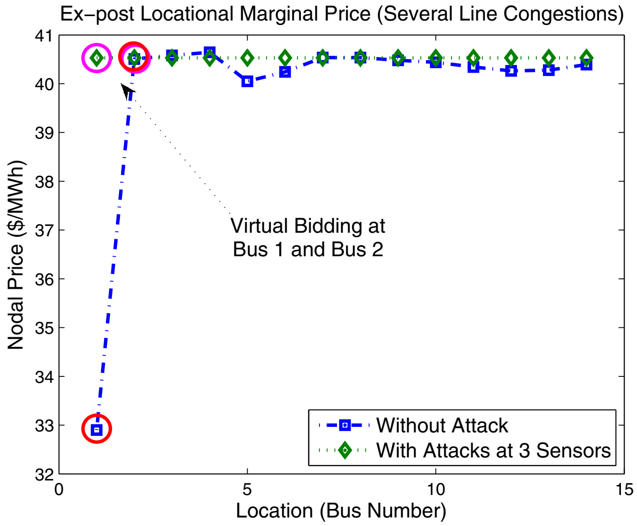

Fig. 3. LMP with and without cyber attacks (three congested lines)

TABLE III
ATTACK EFFORTS AND PROFITS ($\varepsilon = 1$MWH)

	relative efforts ($\frac{\|z_a\|_\infty}{\|z\|_\infty}$)	profits (% of transaction cost)
Case I	1.53%	2.50%
Case II	1.21%	9.76%

Future research could address the possible alternatives to the Lagrangian multiplier-based pricing mechanism in order to prevent such false data injection attacks.

VI. CONCLUSION AND FUTURE WORK

In this paper we examine the effect of false data injection attacks on the electricity market. We show that an attacker could manipulate the nodal price of Ex-Post market while being undetected by the system operator. Combining with virtual bidding, such attack could bring financial profit to the attacker. A heuristic is developed to compute the optimal injection of the attacker, which can be formulated as a convex optimization problem and thus solved efficiently by the attacker. An illustrative example is further provided to show the effect of false data injection attacks on the IEEE 14-bus systems. In the future, we would like to design counter measures to mitigate the financial impact of false data injection attacks.

ACKNOWLEDGMENT

We thank Dr. Feng Zhao of ISO-New England for informative discussion on the electricity market pricing. 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. Foundation. 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, CMU, or the U.S. Government or any of its agencies.

REFERENCES

[1] F. C Schweppe, J. Wildes, and D. B. Rom, "Power system static state estimation, Parts I, II and III," *IEEE Transactions on Power Apparatus and Systems*, Vol. 89, Issue 1, pp. 120-135, Jan 1970.

[2] F. F. Wu, "Power system state estimation: a survey," *International Journal of Electrical Power & Energy Systems*, Vol. 12, Issue 2, pp. 80-87, Apr 1990.

[3] F. Li, Y. Wei, and S. Adhikari, "Improving an unjustified common practice in ex post LMP calculation," *IEEE Transactions on Power Systems*, Vol. 25, Issue 2, pp. 1195-1197, May 2010.

[4] M. Negrete-Pincetic, F. Yoshida, and G. Gross, "Towards quantifying the impacts of cyber attacks in the competitive electricity market environment," *Proceedings of IEEE PowerTech*, Jul 2009.

[5] 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," *Proceedings of IEEE Power and Energy Society General Meeting*, Jul 2008.

[6] Y. Liu, M. K. Reiter, and P. Ning, "False data injection attacks against state estimation in electric power grids," *Proceedings of the 16th ACM Conference on Computer and Communications Security*, 2009.

[7] H. Sandberg, A. Teixeira, and K. H. Johansson, "On security indices for state estimators in power networks," *First Workshop on Secure Control Systems, CPSWEEK 2010*, Apr 2010.

[8] O. Kosut, L. Jia, R. Thomas, and L. Tong, "Limiting false data attacks on power system state estimation," *Proceedings of Conference on Information Sciences and Systems*, Mar 2010.

[9] F. F. Wu, P. Varaiya, P. Spiller, and S. Oren, "Folk theorems on transmission access: proofs and counterexamples," *Journal of Regulatory Economics*, Vol. 10, Issue 1, pp. 5-23, Jul 1996.