Impacts of Malicious Data on Real-time Price of Electricity Market Operations

Liyan Jia, Robert J. Thomas, and Lang Tong
School of Electrical and Computer Engineering
Cornell University
Ithaca, NY 14853, USA
Email:{lj92,zy73,lt35}@cornell.edu.

***Abstract*—Impacts of malicious data data attack on the real-time electricity market are studied. It is assumed that an adversary has access to a limitted number of meters and has the ability to construct data attack based on what it observes. Different observation models are considered. A geometric framework is introduced based on which upper and lower bounds on the optimal data attack are obtained and evaluated in simulations.**

***Keywords*-Power system state estimation; false data attack; bad data detection; power network observability; smart grid security;**

I. Introduction

The deregulated electricity market has two interconnected components. The day-ahead market determines the Locational Marginal Prices (LMPs) based on dual variables of the Optimal Power Flow (OPF) solution [1] given bids, demand forecast, constraints on generator capacity and flow limits. The calculation of LMP does not depend on the actual system operation. In the real-time market, on the other hand, an ex-post formulation is often used (*e.g.,* by PJM and ISO-New England [2]) to calculate the real-time LMP by solving an incremental OPF. The prices in the day-ahead and the real-time market are used in the final clearing and settlement process.

Because the real-time price is a function of state estimates, the real-time LMP is a function of data measured from meters. Therefore, anomalies in data will affect prices in the real-time market. If data obtained normal random measurement errors, the bad data detection at the control center will likely filter the outliers out. The net effect of random measurement error is insignificant. The bad data detection also plays the role of removing outliers due to malfunctions of meters, packet drops in communications, and other outliers.

The increasing reliance on networking for wide area situation awareness comes with the threat that an adversary may break into the information network, obtain vital system information, and launch intelligent attacks that can influence covertly the real-time electricity market. While there is no publicized incidents of such attacks, it is of significant value to assess the potential impacts of such attacks. Such analysis may also reveal the vulnerability of the network topology, the inadequacy of meter placement, and potential security enhancement solutions

This work is supported in part by the Intel Fellowship program , the NSF TRUST (The Team for Research in Ubiquitous Secure Technology) center under award CCF-0424422, PSerc, and the DoE supported TCIPG (Trustworthy Cyber Infrastructure for the Power Grid) consortium."

A. Summary of Results and Contributions

In this paper, we study effects of malicious data attack on the real-time electricity market. We consider attacks in the *weak attack regime* where the adversary does not have control of so many meters that its attack is *unobservable* [3], [4]. Consequently, the adversary faces conflicting objectives: (i) evading bad data detection by limiting the perturbation of data sent to the control center; (ii) causing as large economic impact as possible to the real-time market. Here by economic impact we mean the change of real-time prices at different locations.

We focus in this paper attack strategies of an adversary and try to characterize the attack performance measured by the expected price change. A main contribution of this paper over existing work—see Sec I.B for a brief survey—is the adaptive nature of the attack. In particular, the attacker uses the observed data to construct data-dependent attack. This is a significant departure from several related work where time invariant attacks are derived [5], [6].

Our approach is based on a geometric characterization of real-time LMPs on the state space of the power network. By partition the state space into polytope regions where each region is associated with a unique LMP, we formulate the problem of designing malicious data attack as an optimization with the objective of maximizing expected price change subject to flow limits and detection probability constraints.

We consider several observation scenarios that model different levels of intrusion by the adversary. At one extreme, one may assume that the adversary has the full network observation (even though he can only alter data at few locations). In this case, the adversary knows exactly the data that will be received by the control center, which gives the greatest power to the adversary to influence the actual real-

time price. This is the worst case attack that serves as the upper bound on the maximum price deviation.

A more realistic scenario is that the attack can only access a fraction of the meter data. The part of data unobservable to the adversary introduces uncertainties such that the adversary can only estimate what the control center observes and it can only hope to maximize the expected change based on some optimized attack vector as a function of the meter data accessible to him. The optimization formulated in this paper does not have closed-form solution, and we present some suboptimal solutions. As achievable schemes, these suboptimal solutions serve as lower bound on the price deviation caused by the optimal attack.

B. Related Work and Organization

Although the detection of bad data is a classic subject, see [7] and references therein, the problem of malicious data attack and its detection has only attracted attention recently, due in large part by the work of Liu, Reiter and Ning [8]. They have shown that, by compromising enough meters, the adversary can perturb the state estimate arbitrarily in some subspace. Kosut *et al.* found that the condition for the existence of such attacks is equivalent to the network observability condition [9], and a graph theoretic approach is developed to characterize the so-called *security index*—the smallest set of attacked meters that will cause unobservability [3], [4]. When the attacker has only limited access to meters in the weak attack regime, algorithms for detecting malicious attack have been considered [9].

The effect of malicious data attack on real-time market was first considered in [10], [6]. In [6], the authors presented the financial risks induced by the malicious attack and proposed a heuristic technique for finding profitable attacks. While there are similarities between this paper and [6], both consider mechanisms to influence the real-time LMP price based on incremental DC OPF, there some significant differences; most important is that the class of attacks considered in this paper are based on real-time measurement whereas the attacks presented in [6] are data independent.

The structure of this paper is as follows: in Section II, we introduce the problem formulation, making precise definitions of the system model and market model. In Section IV we show the possibility of changing real-time LMP's by alter some meters' values by a simple 5-bus example. Finally, in Section V, we will show the attack problem formulation, under three different scenarios, with full, partial and no observations in real-time.

II. System Models under Normal Conditions

We describe in this section models for the power system, the state estimation, and the day ahead and real-time markets in the absence of malicious attack. We will assume that the control center does not deploy sophisticated intrusion detection schemes; it simply relies on a standard bad data detection based on residue error—the so-called $J(x)$ test [11].

A. Power system model

Consider a lossless power transmission network with n buses. Measurements are collected from the network in a vector $z \in \Re^M$. Our model accommodates various types of measurements including the real line flows of branches, the power generations and loads, and possibly PMU measurements. In real-time market, the calculation of LMP usually involves a DC power flow based on the linearized network model. Since there exists a bijection between nodal power injections and voltage phases [12], we define the states x as the vector of power generation vector P and load vector L, i.e. $x = [P^{\intercal}, L^{\intercal}]^{\intercal}$. The DC model of a power system is given by

$$z = Hx + w, \tag{1}$$

where H is the factor matrix of nodal power injection vector and w is the Gaussian noise of measurements.

B. State estimation and bad data detection

Given the observation of the measurements z, the maximum likelihood (weighted least squares) state estimate is given by

$$\hat{x} = Kz, \quad K \triangleq (H^T R^{-1} H)^{-1} H^T R^{-1}, \tag{2}$$

where R is the covariance matrix of the noise w. By the invariance property of the ML estimator, the maximum likelihood estimation of power generations, loads, and line flows would be

$$\begin{bmatrix} \hat{P} \\ \hat{L} \\ \hat{F} \end{bmatrix} = \begin{bmatrix} \hat{x}_P \\ \hat{x}_L \\ H_F \hat{x} \end{bmatrix} \tag{3}$$

where $\hat{x}_P$ and $\hat{x}_L$ are the parts in x corresponding to P and L, and H_F is the part in H corresponding to the line flows.

To make sure the topology and measurement used in the state estimation is correct, the control center will also conduct the bad data detection procedure. One of the widely used detector in practice is the residue detector [11] (also referred to as the $J(x)$-detector). Define the residual r as

$$r = z - H\hat{x} = Gz, \quad G \triangleq I - H(H^T R^{-1} H)^{-1} H^T R^{-1}. \tag{4}$$

The residue detector δ is a threshold detector of r:

$$\delta(z) = \begin{cases} 1 & \text{if } ||r||^2 > \tau \\ 0 & \text{if } ||r||^2 \leq \tau \end{cases} \tag{5}$$

where τ is the threshold calculated from a certain false alarm probability.

C. Models of day ahead and real-time markets

The deregulated electricity market consists of two components, a day-ahead market and a real-time market. In the day-ahead market, given the load forecast L, the following OPF problem is solved

$$\begin{array}{ll} \text{minimize}_P & \sum_i C_i P_i - \sum_j C_i L_j \\ \text{subject to} & \sum_i P_i - \sum_j L_j = 0 \\ & P_i^{\min} \le P_i \le P_i^{\max} \\ & \sum_i A_{ki} P_i - \sum_j A_{kj} L_j \le T_k^{\max} \end{array},$$

where P_i is the generation at bus i, L_j the forecast load at bus j, $P_i^{\min}$ and $P_i^{\max}$ the lower and upper capacity bounds for generator at bus i, A_{ki} the shift factor of branch k to bus i, and $T_k^{\max}$ the line flow limit for branch k.

The solution P^* of the above optimization is called the *economic dispatch*. The locational marginal price (LMP) is defined as the cost of supplying an additional MW of load at a particular location. From the OPF formulation above, the LMP λ_i^* at bus i is given by

$$\lambda_i^* = \lambda - \sum_k A_{ki}\mu_k, \tag{6}$$

where λ, μ_k are the dual variables corresponding to the equation and line flow constraints, respectively.

As for the real-time market, an ex-post formulation (adopted by PJM, ISO-NE, and etc.) solves the following incremental linear programming problem [13],

$$\begin{array}{ll} \text{minimize} & \sum C_i \Delta P_i - \sum C_j \Delta L_j \\ \text{subjcet to} & \sum \Delta P_i = \sum \Delta L_j \\ & \Delta P_i^{\min} \le \Delta P_i \le \Delta P_i^{\max} \\ & \Delta L_j^{\min} \le \Delta L_j \le \Delta L_i^{\max} \\ & \sum_i A_{ki} \Delta P_i + \sum_j A_{kj} \Delta L_j \le 0, \text{for all } k \in \hat{\mathcal{C}} \end{array}$$

where the set $\hat{\mathcal{C}}$ is the set of estimated congested lines on which the estimated flows are equal or above the flow limits. Since the estimated flows are determined by the state estimate, the estimated congested patter $\hat{\mathcal{C}}$ is also a function of the state estimate. In practice, the upper and lower bound of Δp_i are chosen as 0.1MW and -2MW [14].

The real-time LMP is calculated as

$$\hat{\lambda}_i := \hat{\lambda} - \sum_{j \in \hat{\mathcal{C}}} A_{ji}\hat{\mu}_j \tag{7}$$

where $\hat{\lambda}$ and $\hat{\mu_j}$ are the dual variable corresponding to the linear constraint and line flow constraints, respectively.

In the day-ahead market, the operator calculates the economic dispatch (p^*, λ^*) from the OPF formulation. The generator at bus i receives $P_i^* \lambda_i^*$, and the customer at bus j pays $L_j \lambda_j^*$. In the real time market, the operator does the state estimation, figuring out the network topology and estimated value of generations, loads, and power flow, then calculates the real-time LMP, $\hat{\lambda}$. In real-time market the generator at bus i receives $(\hat{P}_i - P_i^*)\hat{\lambda}_i$ and the customer at bus j pays $(\hat{L}_j - L_j)\hat{\lambda}_j$.

III. Partition of State Space by Real-Time Price

Our approach relies on a geometric characterization of the state space. Let $\mathcal{X} \subset \Re^M$ be the set of possible state vectors. Given a realization of meter data z, the control center obtains the state estimate $\hat{x}(z)$ (we shall drop the dependency of z when no confusion arises). From $\hat{x}$, one obtains the estimated congestion pattern $\hat{\mathcal{C}}$ (also a function of z). From the estimated congestion pattern $\hat{\mathcal{C}}$, a real-time price $\hat{\lambda}$ is obtained.

Since the state estimate $\hat{x}$ is taken as a sufficient statistic, we can drop the original data z. As a result, each $x \in \mathcal{X}$ is associated with a congestion pattern $\mathcal{C}$ thus a real-time price $\lambda(x)$. Define $\pi(\mathcal{C})$ as the region of x's which give the congestion pattern as $\mathcal{C}$. Notice that we have dropped the "hat" on the corresponding variables to indicate that the relation between $x \in \mathcal{X}$ and real-time price λ is not a function of real-time data.

The following Theorem gives a geometric structure of the state space.

Theorem 1 (Price Partition of the State Space): The state space $\mathcal{X}$ is partitioned into polygons (ref. Fig 1) where the interior of each polygon is associated with a unique price λ and the boundaries are defined hyperplanes, each associated with a congestion condition of a single transmission line.

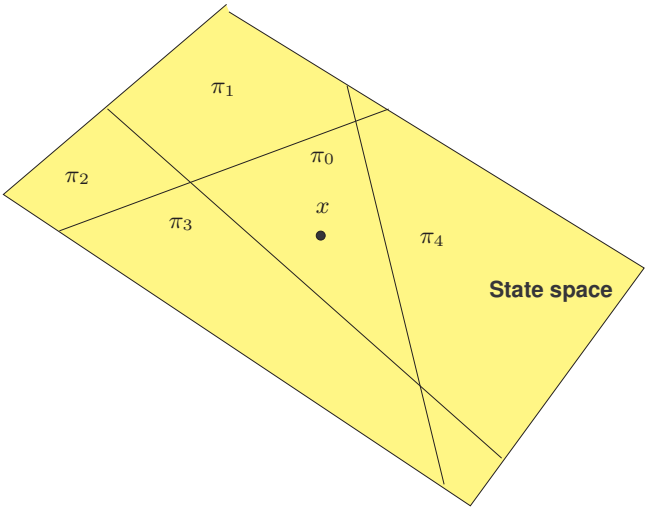


Figure 1: Partition of the state space by real-time price

The significance of Theorem 1 is its succinct characterization of the state space. It is this partition that shows the underlying strategy of attack to be described in later sections. In practice, the operating point of the network—the actual state—is not known precisely. Given observation data from

the networked meters, the state can be estimated. The basic idea of malicious data attack is to create an illusion at the control center that the system is operating at different point from the actual system state. The challenge of creating such illusions is that the estimates of the system operating point by the control center and the adversary, however, can be very different, especially when the adversary has only limited view of the network.

IV. Attack Model and Examples

We now present the attack model along with several simple examples to illustrate some characteristics of the attack. It is perhaps not surprising but nontheless nontrivial, that the price changes due to data attack can be very much decoupled from the location of the attack.

A. Attack scheme

Assume the adversary can manipulate values of a set of meters, which means the adversary can inject a vector a into the DC system model (1). We define the attack pattern, $T(a)$, as the indices set of nonzero values in a. Physically, $T(a)$ means the meters the adversary can manipulate at the same time. Let $\mathcal{T}$ denote the set of all attack patterns available to the adversary, and then $\mathcal{A} = \{a : T(a) \in \mathcal{T}\}$ is the set of all possible attack vectors the adversary can inject. The attack model is then given by

$$z_a = Hx + w + a, a \in \mathcal{A} \tag{8}$$

where z_a is the measurement vector (with attack) and a the attack vector.

Due to the existence of the bad data detector, the adversary cannot inject an arbitrary vector into the system. The adversary needs to design some intelligent attack design method to handle the tradeoff between making profit and avoiding being detected.

B. A simple example

Now we investigate the cases that disturbance of real time measurements will affect the real-time price. Consider the PJM 5-bus system shown below. At bus 2, 3 and 4, there is 300MW load for each. The bidding prices are shown in the circle, standing for the generators. At the operating point, which is the optimal dispatch, branch 1-2 and 4-5 are congested. The real-time LMPs are shown next to the buses.

Next, assume we can alter the meters of generations at bus 1 and 3. By setting different congestion patterns (shown as the bold red line), the real-time LMP's change significantly.

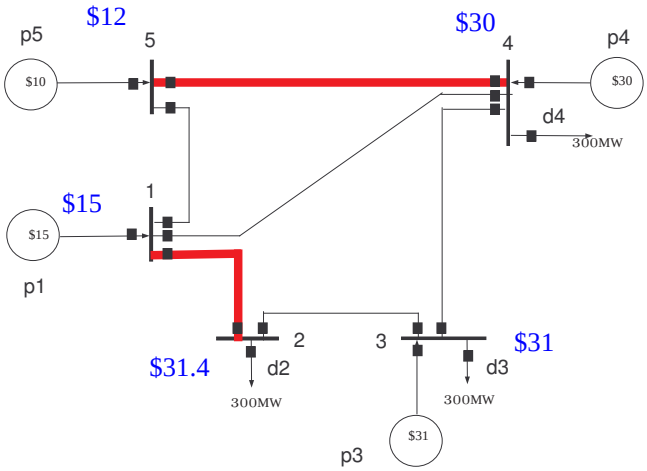


Figure 2: the congestion pattern and real-time LMP without attack

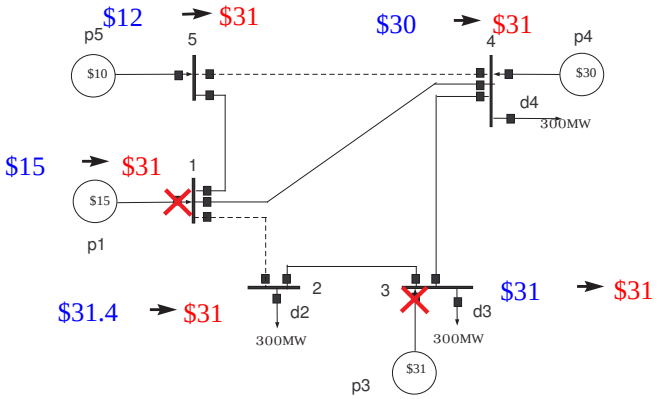


Figure 3: the congestion pattern (no congested lines) and real-time LMP with attack

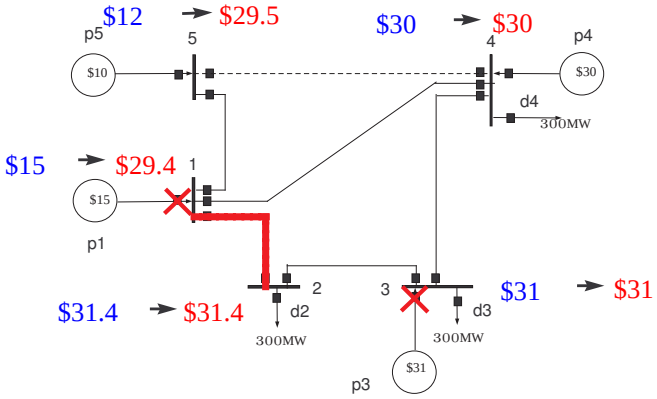


Figure 4: the congestion pattern (line 1-2) and real-time LMP with attack

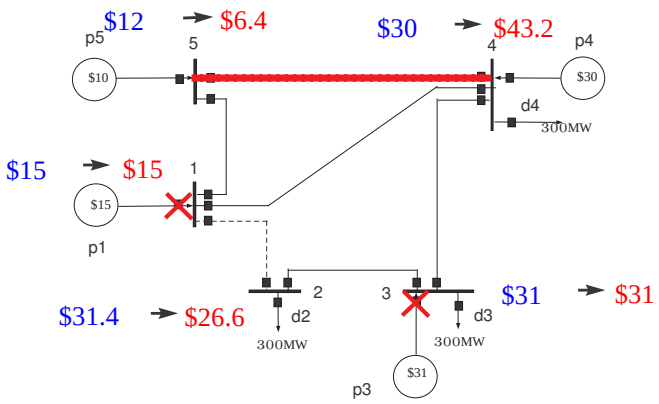


Figure 5: the congestion pattern (line 4-5) and real-time LMP with attack

From the results above, we can get two conclusions. First, changing the congestion pattern, even though slightly, can change the real-time LMP significantly. Second, altering the local meters (generation at bus 1 and 3) may change the LMP far away (LMP at bus 4) significantly.

V. Problem Formulation

A. Objective function

Assume our target is to make profit for generator at bus i in the real-time market. The adversary has the knowledge about some values of the measurement in real-time, and can also inject an attack vector into the system according to the observed result. By changing the real-time congestion pattern, the adversary can alter the corresponding real-time LMPs.

As stated in the previous section, the real-time compensation for the generator at bus i is

$$\hat{\lambda}_i(\hat{p}_i - p_i^*) \tag{9}$$

In practice, $\hat{p}_i$ is given by specific meters, different from those used for state estimation. So here, we only consider the price change caused by the change of measurement values. According to the information known to the adversary, he wants to increase the real-time LMP, $\hat{\lambda}_i$, as much as he can. However, due to the existence of bad data detector, once the measurements result received by the system operator is claimed as bad data, the adversary's attempt to make profit fails. Hence, there is a tradeoff between making more profit and avoiding being detected.

In the following, we consider three different scenarios: the whole set of real-time measurement values is known to the adversary, only part of the real-time measurement values are known to the adversary, and no real-time information is available to the adversary.

We adopt Bayesian formulation in our following analysis. In real-time, we assume the system state follows a Gaussian distribution, $x \sim \mathcal{N}(x_0, \Sigma_x)$, which is known to the adversary ahead of time. This distribution is treated as the prior knowledge of the system states. Based on the observation in real-time, the adversary can make posterior estimation of the states, based on which he makes the attack decision.

B. With full real-time observation

If an attack vector a is injected, according to equation (2) and (8), we can get the WLS estimation of states with attack vector

$$\hat{x}_a = Kz_a = K(z + a) = \hat{x} + Ka \tag{10}$$

As stated in section III, the price is only determined by the congestion pattern. Under the congestion pattern $\hat{\mathcal{C}}$, the real-time price is $\lambda_i = \lambda_i(\hat{\mathcal{C}})$. So the adversary's goal is simply moving the state to the region with highest price without triggering the bad data detector. On the other hand, since the adversary can gather all the real-time measurement values, he can make sure whether a specific attack vector a injected to the system will be detected or not.

Define the available set of congestion pattern under the realization of measurement values is

$$\Gamma(z) = \{\hat{\mathcal{C}} : \exists a, \text{ s.t } \hat{x}_a \in \pi(\hat{\mathcal{C}}), ||Ga||^2 \leq \tau\} \tag{11}$$

The best region is chosen as

$$\hat{\mathcal{C}}^*(z) = \arg \max_{\hat{\mathcal{C}} \in \Gamma(z)} \lambda_i(\hat{\mathcal{C}}) \tag{12}$$

The highest price is

$$\hat{\lambda}^*(z) = \max_{\hat{\mathcal{C}} \in \Gamma(z)} \lambda_i(\hat{\mathcal{C}}) \tag{13}$$

The attack vector is an arbitrary one which makes $\hat{\mathcal{C}}^*(z)$ as the congestion pattern.

C. With partial real-time observation

If only part of the measurement values is known to the adversary, denoted as z_0, the adversary has to make an estimation of the state based on the observation and prior distribution. By Bayesian formulation

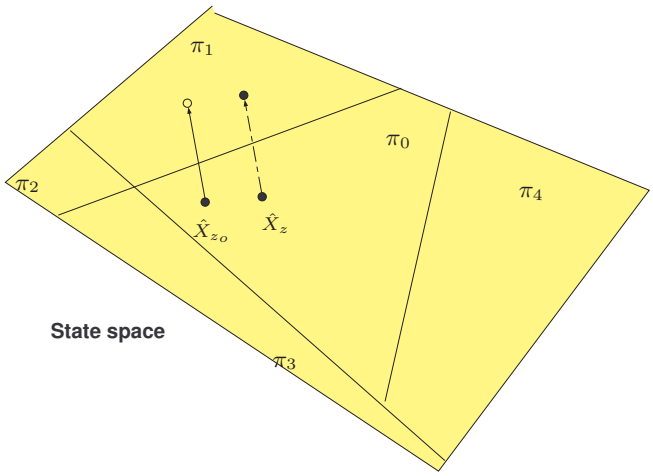
$$\hat{x}_{z_o} = \mathbb{E}(x|z_0) = x_0 + \Sigma_x H_o^T (H_o \Sigma_x H_o^T)^{-1}(z_o - H_o x_0) \tag{14}$$

where H_o is the part of H corresponding to the observed measurements.

The adversary can only move his estimation of state. The best he can do is to move $\hat{x}_{z_o}$ into the region with highest price. In fact, the actual estimated state will also move in parallel as shown in fig. (6)

In order to minimize the effect of the uncertainty, we want to move the estimation of state to the "center" as much as possible.

Figure 6: Move of state estimate with attack vector



Given the attack vector a, the estimate of state under observation z_o is

$$\hat{x}_{a,z_o} = \mathbb{E}(x|z_o; a) = \hat{x}_{z_o} + Ka \tag{15}$$

Since in this scenario, the adversary doesn't have the full map of the measurements. Then, for any attack vector injected, there will be a positive detection probability. So he will need an pre-designed parameter ϵ to control the detection probability. For the congestion pattern $\hat{\mathcal{C}}$, the adversary will solve the following optimization problem. Among all the $\hat{\mathcal{C}}$'s which make the above problem feasible set nonempty, we choose the one with highest price, $\hat{\mathcal{C}}^*$. The solution a is the injected attack vector and the highest desired price is $\lambda_i(\hat{\mathcal{C}}^*)$.

$$\begin{array}{ll} \text{maximize} & \delta \\ \text{subject to} & H_i\hat{x}_{a,z_o} - \delta \geq T_i^{\max}, i \in \hat{\mathcal{C}} \\ & H_j\hat{x}_{a,z_o} + \delta \leq T_j^{\max}, j \notin \hat{\mathcal{C}} \\ & z_o^{\mathrm{T}} G' z_o + a^{\mathrm{T}} G a \leq \epsilon \\ & \delta \geq 0, a \in \mathcal{A} \end{array} \tag{16}$$

where G' is the part of G corresponding to the set of observation.

D. With no real-time observation

If there is no real-time measurement value known to the adversary, he can only inject a constant value into the system according to the prior distribution, no matter what happens in real-time. His best guess of the state is x_0. Also, he wants to move it to the center of the desired region.

Similar to the partial information case, the adversary will solve the following optimization problem, and the attack vector is given by the solution.

$$\begin{array}{ll} \text{maximize} & \delta \\ \text{subject to} & H_i x_0 - \delta \geq T_i^{\max}, i \in \hat{\mathcal{C}} \\ & H_j x_0 + \delta \leq T_j^{\max}, j \notin \hat{\mathcal{C}} \\ & a^{\mathrm{T}} G a \leq \epsilon \\ & \delta \geq 0, a \in \mathcal{A} \end{array} \tag{17}$$

Among all the $\hat{\mathcal{C}}$'s which make the above problem feasible set nonempty, we choose the one with highest price, $\hat{\mathcal{C}}^*$. By solving the problem above, we can get the solution as the injected attack vector. The highest desired price is $\lambda_i(\hat{\mathcal{C}}^*)$

VI. Simulation results

In order to show the effect of malicious data to the real-time market price, we test the three scenarios above on PJM 5-bus system, IEEE 14bus system and IEEE 118-bus system. In fact, the scenario with full real-time observation can be also viewed as the worst case for real-time market price disturbance if bad data exists. Similarly, the scenario with no real-time observation is the lower bound for the real-time price change.

If the number of possible congested lines is not small, the search space grows exponentially with the size of congestion pattern. Then we will start from the estimated state, find the best feasible region in neighborhood until no better neighbor can be found. This strategy will avoid exhaustive search and improve the search efficiency significantly.

In the following simulation, we consider the DC power system, with all the measurements for power injections and power flows(both directions). The redundancy in our simulation is much higher than that used in practice, which makes the attack even harder. However, even in this case, we can still see significant price change in real-time market. Assume the SNR is 10dB, and the measurement noise is i.i.d.. Other data is all from the standard data file. For the partial observation case, we assume half of the meters' values are observable to the adversary.

For PJM 5-bus system, we take 3 meters to attack as shown in Fig VI. The price increase at bus 5 is shown in fig. 8. For the full observation case, the bad data detection is always avoided. So we use dash line to show this scenario as upper bound. For the other two cases, as the detection probability increases, the adversary can make bigger price change.

We also try the three scenarios on IEEE 14bus system (Fig. 9) and 118-bus system (Fig. 10) with 5 meters and 7 meters to attack respectively.

In order to show the adversary's ability under different sizes of attack pattern, we plot the curve of price change under detection probability 0.2 versus the dimension of attack meters. The scenarios with full observation and no observation are served as upper bound and lower bound for real-time price disturbance respectively. See Fig. 11 for IEEE 14-bus system and Fig. 12 for IEEE 118-bus system.

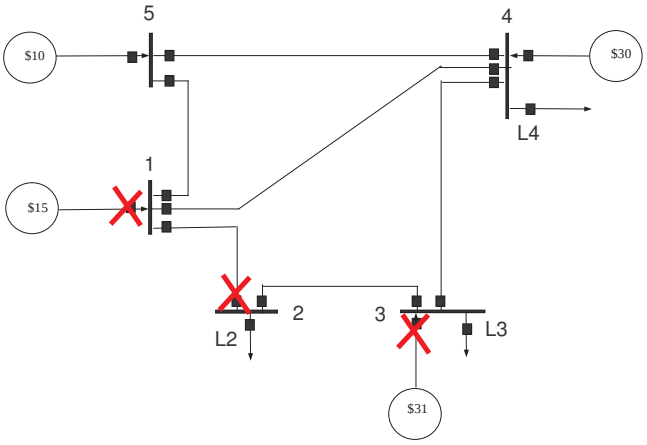


Figure 7: PJM 5 bus system

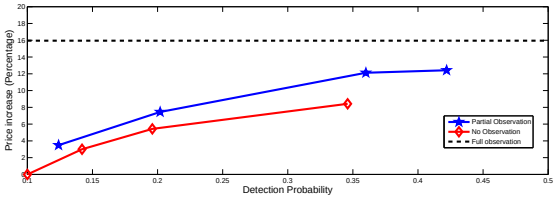


Figure 8: LMP % increase at bus 5 for PJM 5 bus system

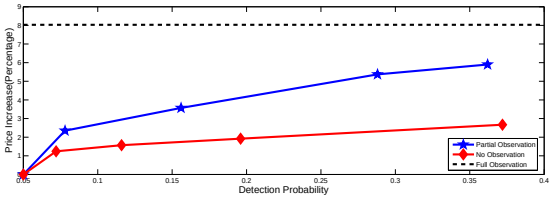


Figure 9: LMP % increase at bus 1 for IEEE 14-bus system

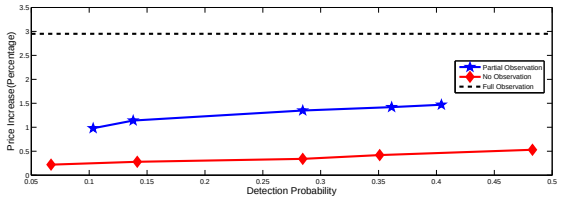


Figure 10: LMP % increase at bus 1 for IEEE 118-bus system

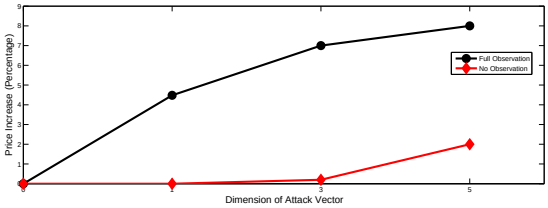


Figure 11: LMP % increase at bus 1 under 0.2 detection probability versus attack vector dimension for IEEE 14-bus system

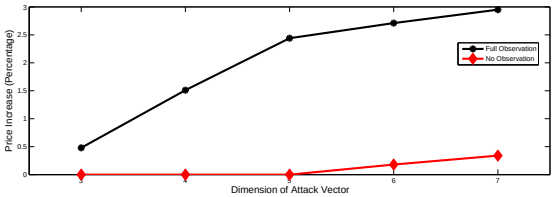


Figure 12: LMP % increase at bus 1 under 0.2 detection probability versus attack vector dimension for IEEE 118-bus system

As the size of system increases, the ability of attacking the system decreases. But since in reality, the ISO uses much less redundancy for state estimation and there may be some isolated part in the system, the price change will still be significant if proper attack vector is injected according to the real-time information.

VII. Conclusion

In this paper, we investigated the effect of malicious attack on real-time electricity market, and showed the chance the adversary can make profit by intelligently manipulating some values of the measurements. Then we formulated the problem under three different scenarios. Finally we showed validity of the proposed strategy by simulation results.

In the future, we are interested in the counterpart of this problem, designing detectors to protect the electricity market from malicious attack. Also, since our solution to the problem is based on the DC model, but in reality, AC model is used for state estimation and bad data detection, we will explore the property of AC model and modify our algorithm to fit the AC model setting.

References

[1] E. Litvinov, T. Zheng, G. Rosenwald, and P. Shamsollahi, "Marginal loss modeling in lmp calculation," *IEEE Transaction on Power System*, vol. 19, no. 2, 2004.

[2] T. Zheng and E. Litvinov, "Ex post pricing in the co-optimized energy and reserve market," *IEEE Transaction on Power System*, vol. 21, no. 4, 2006.

[3] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on smart grid state estimation: attack strategies and countermeasures," in *Proc. IEEE 2010 SmartGridComm*, Gaithersburg, MD, USA, Oct 2010.

[4] O. Kosut, L. Jia, R. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *to appear in IEEE Trans. on Smart Grid*.

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

[6] L. Xie, Y. Mo, and B. Sinopoli, "False data injection attacks in electricity markets," in *Proc. IEEE 2010 SmartGridComm*, Gaithersburg, MD, USA., Oct 2010.

[7] A. Abur and A. G. Expósito, *Power System State Estimation: Theory and Implementation*. CRC, 2000.

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

[9] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "On malicious data attacks on power system state estimation," in *Proc. 45th Intl. Univ. Power Engineering Conf.*, Cardiff, Wales, UK, Aug 2010.

[10] R. J. Thomas, L. Tong, L. Jia, and O. E. Kosut, "Some economic impacts of bad and malicious data," in *PSerc 2010 Workshop*, vol. 1, Portland Maine, July 2010.

[11] E. Handschin, F. C. Schweppe, J. Kohlas, and A. Fiechter, "Bad data analysis for power system state estimation," *IEEE Trans. Power Apparatus and Systems*, vol. PAS-94, no. 2, pp. 329–337, Mar/Apr 1975.

[12] F. Wu, P. Varaiya, P. Spiller, and O. S., "Folk theorems on transimission access: proofs and conterexamples," *Journal of Regulatory Economics*, vol. 10, 1996.

[13] A. L. Ott, "Experience with pjm market operation, system design, and implementation," *IEEE Trans. Power Systems*, vol. 18, no. 2, pp. 528–534, May 2003.

[14] D. Patton and P. Van Schaick, "2007 assessment of the electricity markets in new england," *Potomac Economics*, 2008.