MALICIOUS DATA ATTACK ON REAL-TIME ELECTRICITY MARKET

Liyan Jia, Robert J. Thomas, and Lang Tong

School of Electrical and Computer Engineering
Cornell University, Ithaca, NY 14850

ABSTRACT

Malicious data attacks to the real-time electricity market are studied. In particular, an adversary launches an attack by manipulating data from a set of meters with the goal of influencing revenues of a real-time market. The adversary must deal with the tradeoff between avoiding being detected by the control center and making maximum profit from the real time market. Optimal attacking strategy is obtained through an optimization of a quasi-concave objective function. It is shown that the probability of detection of optimal attack will always be less than 0.5. Attack performance is evaluated using simulations on the IEEE 14-bus system.

***Index Terms*—** Smart grid, electricity market, location marginal price, cyber-physical systems, cyber security, data attack.

1. INTRODUCTION

During the last decade, nationwide deregulation has changed the electricity market in the United States from a traditional monopolized market to a competitive one. Locational Marginal Prices (LMP) are commonly used as a means to determine day-ahead and real-time price [1, 2] by various regional transmission organizations.

In the day-ahead market, by matching the generation offers and demand bids, the LMP is calculated from the Optimal Power Flow (OPF) solution [3]. In the real-time market, on the other hand, an ex-post formulation is often used (*e.g.*, by PJM and ISO-New England [1]) 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.

An adversary can affect the real-time market in two ways. It can manipulate the meter readings that affect directly the quantity of electricity usage. Indirectly, and often more effectively, is to manipulate meter readings that will affect the LMP calculation. This latter approach, as shown in Section 3, can cause significant changes in LMPs throughout the network, sometimes at locations remote from the attack.

The power grid is monitored and controlled by its energy management system (EMS) at the control center. One of the key functions of EMS is bad data detection where the EMS determines whether a particular piece of data is unreliable due to meter malfunction or perhaps simply an outlier that needs to be excluded. Thus anomalies from data may be detected by a sophisticated EMS design. The adversary therefore faces a tradeoff between acting aggressively to cause large changes in profit/loss and acting covertly to avoid being detected. This tradeoff, referred to as the *attacker operating characteristic*, is fundamental for both the adversary and grid EMS.

1.1. 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* [4, 5].

For a fixed detection scheme, the EMS at the control center operates at a particular operating point, typically at the 0.1 false alarm probability of the receiver operating characteristic (ROC) curve. Given the network configuration, we formulate the problem of optimal attack as finding the attacking meters and the corresponding attacking data to maximize the overall profit at a particular location.

For a fixed congestion pattern, we show that the maximum profit gain by a single meter attack is a quasi-concave function of the attacking data vector, and the resulting optimal attack is a solution of an optimization of the quasi-concave function under linear constraints. We also show that, for the single meter attack, the probability of detection of optimal attack is always below 0.5.

1.2. Related Work

Although the detection of bad data has been studied for a long time, see [6] 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 [7]. They have shown that, by compromising enough meters, the adversary can perturb the state estimate arbitrarily

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."

in some subspace. Kosut *et al.* found that the condition for the existence of such attacks is equivalent to the network observability condition [8], and a graph theoretic approach is developed to characterize the so-called *security index*—the smallest set of attacked meters that will cause unobservability [4, 5]. When the attacker has only limited access to meters in the weak attack regime, algorithms for detecting malicious attack have been considered [9, 8].

The effect of malicious data attack on real-time market was first considered in [10, 11]. In [11], the authors presented the financial risks induced by the malicious attack and proposed a heuristic for finding profitable attacks. However, it only considered the situation that the malicious attack pushes the estimated line flows all below the limits. The formulation and strategies presented here leads to optimal attack and applies to more general situations.

The structure of this paper is as follows: in Section 2, we introduce the problem formulation, making precise definitions of the system model, market model and attack model. In Section 3 we propose an strategy to find the optimal single attack vector, which is exact and efficient. Finally, in Section 4, we will show some numerical results on IEEE 14 bus system by using the proposed strategy.

2. PROBLEM FORMULATION

2.1. 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 combination of power generation vector P and demand vectir L, i.e. $x = [P^{\mathrm{T}}, L^{\mathrm{T}}]^{\mathrm{T}}$. 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 the Gaussian noise of measurements.

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

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

where R is the covariance matrix of the noise w. Accordingly, 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.

2.2. Attack and detection models

Now we present the attack model. Assume the adversary can manipulate values of a set of meters. Let $\mathcal{T}$ be the set of possible attack patterns. For example, if the adversary can only attack one meter at a time, $\mathcal{T}$ contains only singletons, each is an index of a vulnerable meter. The attack model is then given by

$$z_a = Hx + w + a, \tag{4}$$

where z_a is the measurement vector (with attack) and a the attack vector constrained by $\mathcal{T}$. Specifically, there exists $T \subset \mathcal{T}$ that gives the indices of nonzero entries of a.

One of the widely used detector in practice is the residue detector [13] (also referred to as the $J(x)$-detector). Define the residual r as

$$r = z - H\hat{x} = Gz, \;\; G \triangleq I - H(H^T R^{-1} H)^{-1} H^T R^{-1}. \tag{5}$$

The residue detector δ is a threshold detector of r:

$$\delta(z) = \begin{cases} 1 & \text{if } ||r||^2 \geq \tau \\ 0 & \text{if } ||r||^2 \leq \tau \end{cases} \tag{6}$$

where τ is the threshold for a certain false alarm probability.

2.3. Electricity market model

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

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

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, S_{ki} the shift factor of branch k to bus i, and $T_k^{\max}$ the line flow limit for branch k.

The solution P^* is called *economic dispatch*, and the locational marginal price (LMP) at bus i is given by

$$\lambda_i^* = \lambda - \sum_k S_{ki} \mu_k, \tag{7}$$

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 solves the following incremental linear programming problem[2],

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

where the set $\hat{C}$ is the set of congested lines, which we refer to as *congested pattern*. $\hat{C}$ is determined by the state estimation. 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

$$\hat{\lambda}_i := \hat{\lambda} - \sum_{j \in \hat{C}} S_{ji} \hat{\mu}_j \tag{8}$$

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^*). 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 and calculates the real-time LMP, $\hat{\lambda}$, then the generator at bus i receives $(\hat{P}_i - P_i^*)\hat{\lambda}_i$ and the customer at bus j pays $(\hat{L}_j - L_j)\hat{\lambda}_j$.

3. OPTIMAL ATTACK STRATEGY

Assume our objective is to make maximum profit for the generator at bus i in the real-time market. We call i the *target location*. Let P^*, L and F^* denote the value of generations, loads and line flows in the day-ahead economic dispatch.

If the attack vector is detected by the bad data detection, the adversary's attempt for making profit fails. So we focus on the expected profit and the objective of our problem should be

$$\text{maximize}_a \ \hat{\lambda}_i (\hat{P}_i - P_i^*)(1 - P_D) \tag{9}$$

where P_D is the detection probability, which is a function of the attack vector.

Now we consider a simple scenario, in which every participant in market follows the day-ahead dispatch. Then the real-time price will only be determined by the congestion pattern. For each congestion pattern $\hat{C}$, if it is achieved by the state estimation with attack, a set of linear constraints should be satisfied for the attack vector a

$$\begin{array}{ll} F_k^* + \sum_i S_{ki} a_i \geq T_k^{\max} & \text{for every } k \in \hat{C} \\ F_k^* + \sum_i S_{ki} a_i < T_k^{\max} & \text{for every } k \notin \hat{C} \end{array}$$

Actually, for a specific economic dispatch, only the lines with flows close to the limit can be made into the congestion set by attack vector under relatively low detection probability. So we define the *vulnerable set* of lines, V, as

$$V \triangleq \{k : T_k^{\max} - F_k^* \leq \delta\} \tag{10}$$

where δ is a arbitrary threshold.

According to equation (2), the expectation of the difference between estimated generation and economic dispatch is given by,

$$\mathbb{E}(\hat{P}_i - P_i^*) = \mathbb{E}((K_{P_i}(Hx + w + a)) - P_i^* = K_{P_i} a \tag{11}$$

where K_{P_i} is the part of K corresponding to the measurement of generation at bus i.

Under the attack vector a introduced by the adversary, the residual's 2-norm will be

$$\begin{aligned} ||r_a||^2 &= ||G(Hx + w + a)||^2 \\ &= w^T G w + 2a^T G w + a^T G a. \end{aligned} \tag{12}$$

Assuming $w \sim \mathcal{N}(0, \sigma^2 I)$, we then have[13]

$$E(||r_a||^2) = (n - m)\sigma^2 + a^T G a \tag{13}$$

$$\text{Var}(||r_a||^2) = 2(n - m)\sigma^4 + 4\sigma^2 a^T D a \tag{14}$$

where n and m are the number of H's rows and columns respectively, and $D = \text{diag}(G_{11}, G_{22}, ..., G_{nn})$.

When the size of the system is large, the distribution of $||r_a||^2$ can be approximated by [13]

$$||r_a||^2 \sim \mathcal{N}(E(||r_a||^2), \text{Var}(||r_a||^2)). \tag{15}$$

So given an attack vector a and the threshold for the detector, the detection probability is

$$P_D = Q\left(\frac{\tau - ((n - m)\sigma^2 + a^T G a)}{\sqrt{2 * (n - m)\sigma^4 + 4\sigma^2 * a^T D a}}\right) \tag{16}$$

where $Q(\cdot)$ is the function of the tail probability of standard normal distribution.

Now we only consider the single attack problem, *i.e.*, $a = \alpha e_j$. For a fixed congestion pattern $\hat{C}$, the real-time LMP $\hat{\lambda}_i$ is fixed. Then, the objective function is

$$F(\alpha) = \hat{\lambda}_i K_{p_i,j} \alpha \left(1 - Q\left(\frac{\tau - ((n - m)\sigma^2 + G_{jj}\alpha^2)}{\sqrt{2(n - m)\sigma^4 + 4\sigma^2 G_{jj}\alpha^2}}\right)\right). \tag{17}$$

We have the following two theorems, the proofs of which are quite straightforward by taking the derivative. They're omitted due to the page limit.

Theorem 1 *The objective function for single attack, $F(\alpha)$, is quasi-concave on $[0, \infty)$ when $K_{p_i,j} > 0$, and quasi-concave on $(\infty, 0]$ when $K_{p_i,j} < 0$.*

Theorem 2 *At the optimal point of the objective function, $F(\alpha)$, the detection probability is less than 0.5.*

These two theorems show that the objective function is unimodal. Therefore the unique zero point of $F'(\alpha)$, α_0, is the maximal point for the unconstrained problem. Then, our problem can be converted into the following one

$$\begin{array}{lll} \min & |\alpha - \alpha_0| & \\ \text{s.t.} & F_k^* + \sum_i S_{ki} a_i \geq T_k^{\max} & \text{for every } k \in \hat{C} \\ & F_k^* + \sum_i S_{ki} a_i < T_k^{\max} & \text{for every } k \notin \hat{C} \\ & K_{p_i,j} \alpha \geq 0 & \end{array} \tag{18}$$

Then we can test every congestion pattern $\hat{C} \subset V$ and every possible meter for single meter attack, getting the one with maximal objective value as the optimal attack.

4. NUMERICAL RESULTS

We test our proposed strategy on the IEEE-14 bus system to show its validity. Assume all of the generations at bus 1, 2, 3, 6 and 8 can generate real power, with cost 15, 31, 30, 10 and 20 respectively.

In Fig. 1, we show the attacker operating characteristic, which is the tradeoff between detection probability and the expected profit made in real-time market, with generation at bus 1 as target. We see that the objective function is unimodal, and achieves its maximum below P_D 0.5.

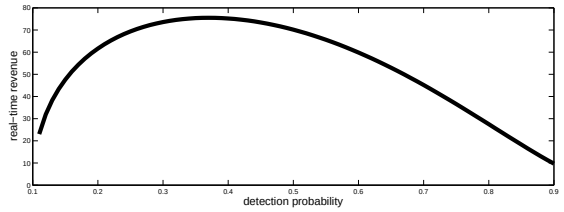

Fig. 1: the attacker operating characteristic curve

To compare with our proposed strategy, we use another two possible strategies for the market attack, random attack, choosing a random attack vector within detection probability $[0, 0.5]$, and 0.5 detection probability attack, choosing the attack vector with exactly 0.5 detection probability. In fig. 2, we show the numerical result for single attack to market under these three attack strategies, at different target locations. Still, the Y-axis is the expected profit in real-time market.

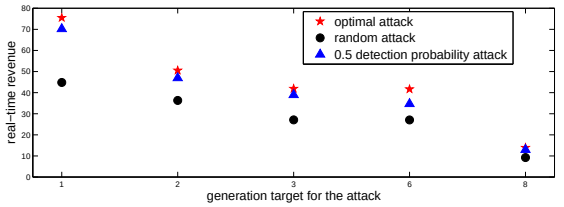

Fig. 2: Real-time profit at different target locations for 3 attack strategies

5. 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 proposed an strategy to find the optimal single attack vector. Finally we showed validity of the proposed strategy simulation results.

In the future, we may consider how to find the optimal multiple attack vector or the sub-optimal one. Also we are interested in the counterpart of this problem, designing detectors to protect the electricity market from malicious attack.

6. REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] 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.

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

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

[7] Y. Liu, M.K. 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.

[8] 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.

[9] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Limiting false data attacks on power system state estimation," in *Proc. 2010 Conference on Information Sciences and Systems*, Mar 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*, Portland Maine, July 2010, vol. 1.

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

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

[13] 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.

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