Bad Data Injection Attack and Defense in Electricity Market Using Game Theory Study

Mohammad Esmalifalak, Ge Shi, Zhu Han, and Lingyang Song

***Abstract*—Applications of cyber technologies improve the quality of monitoring and decision making in smart grid. These cyber technologies are vulnerable to malicious attacks, and compromising them can have serious technical and economical problems. This paper specifies the effect of compromising each measurement on the price of electricity, so that the attacker is able to change the prices in the desired direction (increasing or decreasing). Attacking and defending all measurements are impossible for the attacker and defender, respectively. This situation is modeled as a zero-sum game between the attacker and defender. The game defines the proportion of times that the attacker and defender like to attack and defend different measurements, respectively. From the simulation results based on the PJM 5-Bus test system, we can show the effectiveness and properties of the studied game.**

I. Introduction

RECENTLY, power systems are becoming more and more sophisticated in the structure and configuration because of the increasing in electricity demand and the limited energy resources. Traditional power grids are commonly used to carry power from a few central generators to a large number of customers. In contrast, the new-generation of electricity grid that is also known as the smart grid uses bidirectional flows of electricity and information to deliver power in more efficient ways responding to wide ranging conditions and events [1] (Fig. 1).

Online monitoring of smart grid is important for control centers in different decision making processes. State estimation (SE) is a key function in building real-time models of electricity networks in Energy Management Centers (EMCs) [2]. State estimators provide precise and efficient observations of operational constraints to identify the current operating state of the system in quantities such as transmission line loadings or bus voltage magnitudes. Accuracy of state estimation can be affected by bad data during the measuring process. Measurements may contain errors due to the various reasons such as random errors, incorrect topology information and injection of bad data by attackers. By integrating more advanced cyber technologies into the energy management system (EMS), cyber-attacks can cause major technical problems such as blackouts in power systems[1][3], [4]. The attacks also can be designed to the attacker's financial benefit at the expense of the general consumer's net cost of electricity [6], [7].

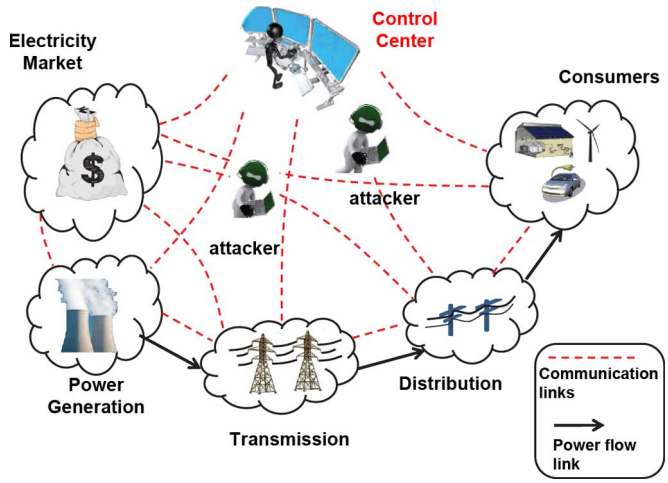


Fig. 1. Flow of energy and data between different parts of smart grids.

In this paper, we consider the case wherein the attacker uses cyber attack against electricity prices. We show that the attacker observes the results of the day-ahead market and changes the estimated transmitted power in order to change the congestion[2] level, resulting in a profit. On the other hand, the defender tries to defend the accuracy of network measurements. Since the attacker and defender are not able to attack and defend all measurements, they will compete to increase and decrease the injected false data, respectively. This behavior is modeled by a two-person zero-sum strategic game where the players try to find the Nash equilibrium and maximize their profits. The results of simulations on the PJM 5-Bus test system show the effectiveness of attack on the prices of electricity on the real-time market.

The remainder of this paper is organized as follows: The literature survey is provided in Section II. The system model is

Manuscript received April 15, 2012; revised September 05, 2012; accepted October 02, 2012. Date of publication January 14, 2013; date of current version February 27, 2013. This work was supported in part by US NSF CNS-0953377, ECCS-1028782, CNS-1117560, Qatar National Research Fund, National Nature Science Foundation of China under Grant 60972009 and 61061130561, as well as the National Science and Technology Major Project of China under Grant 2011ZX03005-002. Paper no. TSG-00212-2012.

M. Esmalifalak and Z. Han are with the ECE Department, University of Houston, Houston, TX 77004 USA (e-mail: esmalifalak.mohammad@gmail.com; zhan2@mail.uh.edu).

G. Shi and L. Song are with the School of Electrical Engineering and Computer Science, Peking University, Beijing, China (e-mail: shigejr@gmail.com; lingyang.song@gmail.com).

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

Digital Object Identifier 10.1109/TSG.2012.2224391

[1]Aurora attack involves a cyber attack against breakers in a generating unit. This experiment shows the abilities of cyber attackers in taking control over breakers and consequently, it reveals the technical problems of this attack for the power grid [5].

[2]Injected power in a specific node of power network, will be transferred to different loads through transmission lines (using Kirchoff's law). In power community we say congestion happens if increasing the power injection, increases (at least one of) transmission lines' power to their (its) thermal limit [8], [9].

given in Section III, and the formulation of an undetectable attack in the electricity market is given in Section IV. Section V models the interactions between the attacker and defender as a zero-sum game. Numerical results are shown in Section VI, and the conclusion closes the paper in Section VII.

II. Literature Review

Due to the importance of the smart grid studies, some surveys have classified the different aspects of smart grids [10]–[12]. In [10] the authors explore three major systems, namely the smart infrastructure system, the smart management system, and the smart protection system and also propose possible future directions in each system. In [11], a survey is designed to define a "smart distribution system" as well as to study the implications of the smart grid initiative on distribution engineering. In [12] relevant approaches are investigated to give concrete recommendations for smart grid standards, which try to identify standardization in the context of smart grids. National Institute of Standards and Technology (NIST) in [13], explains anticipated benefits and requirements of smart grid.

Some researches have been done over cyber security for smart grid [15]–[20]. In [15], an undetectable attack by bad data detectors (BDD) is first introduced, where the attacker knows the state estimation Jacobian matrix (H) and defines an undetectable attack using this matrix. Reference [16] uses independent component analysis (ICA), and inserts an undetectable attack even when this matrix is unknown for attackers. In [17], the authors discuss key security technologies for a smart grid system, including public key infrastructures and trusted computing. Reliable and secure state estimation in smart grid from communication capacity requirement point of view is analyzed in [18]. In [19], a new criterion of reliable strategies for defending power systems is derived and two allocation algorithms have been developed to seek reliable strategies for two types of defense tasks. Reference [20] is a draft from NIST which addresses the cyber security of smart grid extensively. While most of current researches (in bad data injection area) focus on different attack or defend scenarios, our work describes a mutual interaction between both parties. This work shows how the interest of one party (attacker or defender) can influence the other's interest.

Some applications of game theory in smart grids have been studied in [21]–[23], [26]. In [21], the authors present a method for evaluating a fully automated electric grid in real time and finding potential problem areas or weak points within the electric grid by using the game theory. In [22], the authors propose a consumption scheduling mechanism for home and neighborhood area load demand management in smart grid using integer linear programming (ILP) and game theory. Reference [23] is a survey about some of game theory-based applications to solve different problems in smart grid. In [26] the authors model and analyze the interactions between the retailer and electricity customers as a four-stage Stackelberg game.

Demand-side management (DSM), is another topic in smart grid, which is recently considered by researchers. In [24] an intelligent management system is designed based on the objective of orderly consumption and demand-side management, under the circumstances of China's smart grid construction. An Intelligent Metering/Trading/Billing System (ITMBS) with its implementation on DSM is analyzed by [25]. Reference [27] is a research on an autonomous and distributed demand-side energy management system among different users.

III. System Model

In power systems, transmission lines are used to transfer generated power from generating units to consumers. Theoretically, transmitted complex power between bus i and bus j depends on the voltage difference between these two buses, and it is also a function of impedance between these buses. In general, transmission lines have high reactance over resistance (i.e., X/R ratio), and one can approximate the impedance of a transmission line with its reactance. In dc power flow studies, it is assumed that the voltage phase difference between two buses is small and that the amplitudes of voltages in buses are near to unity. Transmitted power is approximated with a linear equation [28]:

$$P_{ij} = \frac{\theta_i - \theta_j}{X_{ij}}, \tag{1}$$

where θ_i is the voltage phase angle in bus i, and X_{ij} is the reactance of transmission line between bus i and bus j. In the state-estimation problem, the control center tries to estimate n phase angles θ_i, by observing m real-time measurements. In power flow studies, the voltage phase angle (θ_i) of the reference bus is fixed and known, and thus only $n-1$ angles need to be estimated. We define the state vector as $\boldsymbol{\theta} = [\theta_1, \ldots, \theta_n]^T$. The control center observes a vector $\mathbf{z}$ for m active power measurements. These measurements can be either transmitted active power P_{ij} from bus i to j, or injected active power to bus i $(P_i = \sum P_{ij})$. The observation can be described as follows:

$$\mathbf{z} = \mathbf{P}(\boldsymbol{\theta}) + \mathbf{e}, \tag{2}$$

where $\mathbf{z} = [z_1, \ldots, z_m]^T$ is the vector of measured active power in transmission lines, $\mathbf{P}(\boldsymbol{\theta})$ is the nonlinear relation between measurement z, state $\boldsymbol{\theta}$ is the vector of n bus phase angles θ_i, and $\mathbf{e} = [e_1, \ldots, e_m]^T$ is the Gaussian measurement noise vector with covariant matrix $\boldsymbol{\Sigma}_e$.

Define the Jacobian matrix $\mathbf{H} \in \mathbb{R}^m$ as

$$\mathbf{H} = \frac{\partial \mathbf{P}(\boldsymbol{\theta})}{\partial \boldsymbol{\theta}} \mid_{\boldsymbol{\theta} = \mathbf{0}} . \tag{3}$$

If the phase difference $(\theta_i - \theta_j)$ in (1) is small, then the linear approximation model of (2) can be described as:

$$\mathbf{z} = \mathbf{H}\boldsymbol{\theta} + \mathbf{e}. \tag{4}$$

The bad data can be injected to $\mathbf{z}$ so as to influence the state estimation of θ. Next, we describe the current bad data injection method used in state estimators of different electricity markets. Given the power flow measurements $\mathbf{z}$, the estimated state vector $\hat{\boldsymbol{\theta}}$ can be computed as:

$$\hat{\boldsymbol{\theta}} = (\mathbf{H}^T \boldsymbol{\Sigma}_e^{-1} \mathbf{H})^{-1} \mathbf{H}^T \boldsymbol{\Sigma}_e^{-1} \mathbf{z} = \mathbf{M}\mathbf{z}, \tag{5}$$

where

$$\mathbf{M} = (\mathbf{H}^T \boldsymbol{\Sigma}_e^{-1} \mathbf{H})^{-1} \mathbf{H}^T \boldsymbol{\Sigma}_e^{-1}. \tag{6}$$

Thus, the residue vector $\mathbf{r}$ can be computed as the difference between measured quantity and the calculated value from the estimated state:

$$\mathbf{r} = \mathbf{z} - \mathbf{H}\hat{\boldsymbol{\theta}}. \tag{7}$$

Therefore, the expected value and the covariance of the residual are:

$$E(\mathbf{r}) = 0 \text{ and } cov(\mathbf{r}) = (\mathbf{I} - \mathbf{M})\boldsymbol{\Sigma}_e, \tag{8}$$

False data detection can be performed using a threshold test [29]. The hypothesis of not being attacked is accepted if

$$\max_i |r_i| \leq \gamma, \tag{9}$$

where γ is the threshold and r_i is the component of $\mathbf{r}$.

IV. Attack in Electricity Market

A power network is a typically large and complicated system, which should be operated without any interruption. Normal operation needs a system wide monitoring of the states of network in specific time intervals. Based on the monitored values, corrective actions need to be taken. Any fault in measurement data (because of measurement failures or cyber attack against them), can change the decisions of control center, which can cause serious technical or economical problems in the network. In this section, we first introduce the electricity market structure, and then from the attacker point of view we will formulate an undetectable attack that can change the prices of electricity.

A. Optimal Power Flow (OPF) and DCOPF

Security and optimality of power network operation are the most important tasks in control centers, which can be achieved by efficient monitoring and decision making. After deregulation of electric industries, different services that can improve security and optimality of network can be traded in different markets. Energy market is one of these markets in which generation companies (GENCOs) and load serving entities (LSEs) compete to generate and consume energy, respectively[3]. Control center knowing the submitted prices and network constraints, tries to maximize social welfare for all participants. A well known program for solving this optimization is Optimal Power Flow (OPF) program. Linear form of optimal power flow is called DCOPF and is used to define the price of electricity (called locational marginal prices or LMPs) in both day-ahead and real-time markets. In the following subsections, the formulation of DCOPF together with the general structure of day-ahead and real-time markets is described.

B. DC Optimal Power Flow (DCOPF)

In general, the LMP can be split into three components including the marginal energy price LMP_i^{Energy}, marginal congestion price LMP_i^{Cong}, and marginal loss price LMP_i^{Loss} [31], [32], [33]. A common model of the LMP simulation is introduced in [31]. It is based on the dc model and Linear Programming (LP), which can easily incorporate both marginal congestion and marginal losses. The generic dispatch model can be written as

$$\min_{\mathbf{G_i}} \sum_{i=1}^{N} C_i \times G_i,$$
$$\text{s.t.} \begin{cases} \sum_{i=1}^{N} G_i - \sum_{i=1}^{N} D_i = 0, \\ \sum_{i=1}^{N} GSF_{k-i} \times (G_i - D_i) \leq F_k^{\max}, \quad k \in \{all\ lines\}, \\ G_i^{\min} \leq G_i \leq G_i^{\max}, \qquad\qquad i \in \{all\ generators\}, \end{cases} \tag{10}$$

where:

N	number of buses;
C_i	generation cost at bus i in ($/MWh);
G_i	generation dispatch at bus i in ($/MWh);
D_i	demand at bus i in (MWh);
GSF_{k-i}	generation shift factor from bus i to line k;
$F_k^{\max}$	transmission limit of line K;
$G_i^{\max}$	upper generation limit for generator i;
$G_i^{\min}$	lower generation limit for generator i.

The general formulation of the LMP at bus i can be written as follows:

$$LMP_i = LMP^{energy} + LMP_i^{cong} + LMP_i^{loss}, \tag{11}$$
$$LMP^{energy} = \lambda, \tag{12}$$
$$LMP_i^{cong} = \sum_{i=1}^{L} GSF_{k-i} \times \mu_k, \tag{13}$$
$$LMP_i^{loss} = \lambda \times (DF_i - 1), \tag{14}$$

where L is the number of lines, λ is the Lagrangian multiplier of the equality constraint, μ_k is the Lagrangian multiplier of the k^{th} transmission constraint, and DF_i is delivery factor at bus i. If the optimization model in (10) ignores losses, we will have $DF_i = 1$ and $LMP_i^{loss} = 0$ in (14). In this work in order to emphasize the main point to be presented, the loss price is ignored.

1) Day-Ahead Market: Based on the submitted bids (from generators and loads) and predicted network condition[4], control center runs the DCOPF program. The output of this market specifies the dispatch schedule for all generators and defines the Locational Marginal Price (LMP) in each bus of power network. Trading electricity in most of electricity markets such as PJM Interconnection, New York, and New England markets is based on the LMP method.

[3]In an electricity (energy) market, GENCOs submit their bids (for generating electricity) to the market. In this case, higher prices will decrease the chance of supplying electricity (selling electricity). Similarly, LSEs submit their bids for consuming energy. In this case, lower bids will decrease the chance of buying electricity. So competition in both entities (GENCOs and LSEs) will increase the efficiency of the electricity market.

[4]Such as the load level for the next day, which can be predicted by the historical load data from the past years.

2) Real-Time Market: In this market the control center conducts the following: 1) Gathers data from the measurements that are installed in the physical layer (power network); 2) Estimates the states of the network (online monitoring of the network); 3) Runs an incremental dispatch model based on the state estimation results. The obtained LMPs will be considered as the real-time price of electricity[5]. The real-time (Ex-Post) model which is used in Midwest ISO, PJM, and ISO-New England, can be written as [34], [35]:

$$\min_{\mathbf{\Delta}G_i} \quad \sum_{i=1}^{N} C_i^{RT} \times \Delta G_i,$$
$$\text{s.t.} \quad \begin{cases} \sum_{i=1}^{N} \Delta G_i - \sum_{i=1}^{N} \Delta D_i = 0, \\ \sum_{i=1}^{N} GSF_{k-i} \times (\Delta G_i - \Delta D_i) \le 0, & k \in \{CL\}, \\ \Delta G_i^{\min} \le \Delta G_i \le \Delta G_i^{\max}, & i \in \{QG\}, \\ \Delta D_i^{\min} \le \Delta D_i \le \Delta D_i^{\max}, & i \in \{PL\}, \end{cases} \tag{15}$$

where C_i^{RT} is the generation cost at bus i in $(\$/MWh)$[6], ΔG_i is the change in the output of generator i, and ΔD_i is the change in the demand of dispatchable load at bus i in (MWh), $\Delta G_i^{\max}$ and $\Delta G_i^{\min}$ are the upper and lower bands for change in the generation of each qualified generator (QG)[7]. Similarly, $\Delta D_i^{\max}$ and $\Delta D_i^{\max}$ are the upper and lower bands for change in the consumption of each dispatchable load (DL). Second constraint shows that any change in the transmitted power in congested lines (CL), should be non-positive value.

Similar to day-ahead market, LMP in bus i (without considering the effect of losses) will be,

$$LMP_i^{RT} = \lambda + \sum_{i=1}^{L} GSF_{k-i} \times \mu_k, \tag{16}$$

where, L is the number of lines, λ is the Lagrangian multiplier of the equality constraint, and μ_k is the Lagrangian multiplier of the k^{th} transmission constraint.

C. Cyber Attack Against Electricity Prices

Real-time market uses the state estimator results that shows the on-line state of the network. In order to transfer data to the state estimator, control center uses different communication channels such as power line communication channel. Using these channels, increases the risk of cyber attack. In other word, if an attacker can change the measurement values[8], the results of state estimation and consequently results of real-time market will be affected. Changing measurements' data without detection by BDD (which can bring financial benefits) is the main goal of the attacker in this paper. In the previous section, we described that the congestion in lines will change the price of electricity in the network. Manipulating prices is a good incentive for the attacker to compromise the measurements. In order to manipulate the congestion level in a specific line, the attacker needs to define the group of measurements that can increase or decrease the congestion, then the attacker can insert false data into the measurements. Equation (1), shows that any change in voltage angle can change the transmitted power through the line. For example, any increase/decrease in $\triangle\hat{\theta} = (\hat{\theta}_i - \hat{\theta}_j)$ will increase/decrease the transmitted power. In online monitoring of power systems, the transmitted power from bus i to bus j can be estimated with $\hat{P_{ij}} = \hat{\theta}_i - \hat{\theta}_j / X_{ij}$, and this equation together with (5) gives the following:

$$\begin{aligned} \hat{P_{ij}} &= \frac{\hat{\theta}_i - \hat{\theta}_j}{X_{ij}} = \frac{(\mathbf{M}_i - \mathbf{M}_j)^T}{X_{ij}}\mathbf{z} \\ &= \mathbf{Q}^T\mathbf{z} = \mathbf{Q}_+^T\mathbf{z}_+ + \mathbf{Q}_-^T\mathbf{z}_-, \end{aligned} \tag{17}$$

where $\mathbf{Q}^T = (\mathbf{M}_i - \mathbf{M}_j)^T / X_{ij}$. The positive and negative arrays of this vector are shown with $\mathbf{Q}_+^T$ and $\mathbf{Q}_-^T$, respectively. These coefficient vectors divide the measurements into two groups $\mathbf{z}_+$ and $\mathbf{z}_-$, in which adding $z^a > 0$ to any array of $\mathbf{z}_+$ and $\mathbf{z}_-$ will increase and decrease the estimated transmitted power flow, respectively. In this paper, the measurements in $\mathbf{z}_+$ and $\mathbf{z}_-$ are considered as group $\mathcal{M}$ and $\mathcal{N}$, respectively[9]. After defining these groups, the attacker tries to insert an undetectable bad data into the measurements. Assume $\mathbf{z} = \mathbf{z}_0$ is the measurement values without corruption (safe mode). From (7) residue for safe mode will be:

$$\mathbf{r}_0 = \mathbf{z} - \mathbf{H}\hat{\boldsymbol{\theta}} = \mathbf{z}_0 - \mathbf{H}(\mathbf{M}\mathbf{z}_0). \tag{18}$$

In the case of attack, $\mathbf{z} = \mathbf{z}_0 + \mathbf{z}^a$ and the residue will be,

$$\begin{aligned} \mathbf{r} &= \mathbf{z} - \mathbf{H}\hat{\boldsymbol{\theta}} = \mathbf{z}_0 + \mathbf{z}^a - \mathbf{H}(\mathbf{M}\mathbf{z}_0 + \mathbf{M}\mathbf{z}^a) \\ &= \mathbf{z}_0 - \mathbf{H}\mathbf{M}\mathbf{z}_0 + \mathbf{z}^a - \mathbf{H}\mathbf{M}\mathbf{z}^a = \mathbf{r}_0 + \mathbf{r}^a, \end{aligned} \tag{19}$$

where $\mathbf{r}^a = (\mathbf{I} - \mathbf{H}\mathbf{M})z^a$. From triangular inequality,

$$\| \mathbf{r} \| \le \| \mathbf{r}_0 \| + \| \mathbf{r}^a \|, \tag{20}$$

this equation shows that if $\| \mathbf{r}^a \| = \| (\mathbf{I} - \mathbf{H}\mathbf{M})z^a \|$ is small, with large probability control center can not distinguish between $\| \mathbf{r} \|$ and $\| \mathbf{r}_0 \|$. So inserted attack will path the bad data detection if, $\|(\mathbf{I} - \mathbf{H}\mathbf{M})\mathbf{z}^a\| \le \boldsymbol{\xi}$. In this constraint ξ is a design parameter for the attacker. Smaller values of ξ will be more likely to be undetected by the control center [7]. However, the ability to manipulate the state estimation, will be limited. we assume ξ is predetermined by the attacker. In order to change congestion, attacker will define the inserted false data using the following optimization,

$$\max_{\mathbf{z^a}} . \quad \sum_{i \in \{\mathcal{M}\}} z^a(i) - \sum_{j \in \{\mathcal{N}\}} z^a(j),$$
$$\text{s.t.} \quad \begin{cases} \|(\mathbf{I} - \mathbf{H}\mathbf{M})\mathbf{z}^a\| \le \boldsymbol{\xi}, \\ z^a(k) = 0 \end{cases} \quad \forall\, k \in \{\mathcal{SM}\}, \tag{21}$$

[5]Dispatch schedule will be similar to the day-ahead market and major changes of load will be covered by the Ancillary Services.

[6]This price can be the same as day-ahead market or can be changed by the generator in a specific time (i.e., 4 P.M.–6 P.M. in PJM market).

[7]All PJM generation units that are following PJM dispatch instructions, are eligible to participate in the real-time market (to set the real-time LMP values), these generation units are called qualified generators.

[8]Attacker can carry out stealth attacks by corrupting the power flow measurements through attacking the Remote Terminal Units (RTUs), tampering with the heterogeneous communication network or breaking into the Supervisory Control and Data Acquisition (SCADA) system through the control center office Local Area Network (LAN) [14], [15].

[9]It is assumed that attacker knows $\mathbf{H}$ (and consequently $\mathbf{M}$). Knowing the location of attack, from (17), attacker can distinguish the measurements in group $\mathcal{M}$ and $\mathcal{N}$.

where $z^a(i)$ is the i^{th} element of attack vector $\mathbf{z}^a$. Group $\mathcal{M}$ and $\mathcal{N}$ consist of measurements that increasing and decreasing their value will increase the congestion. Objective of the above optimization is to increase and decrease measurements value in group $\mathcal{M}$ and $\mathcal{N}$, respectively. First constraint is for avoiding detection of the attack by bad data detector in state estimator. Group $\mathcal{SM}$ shows the safe measurements that can not be compromised (such as those protected by Phasor Measurement Units). With inserting the resulted attack vector z^a to the actual values of measurements ($\mathbf{z} = \mathbf{z}_0 + \mathbf{z}^a$), the attacker will change the estimated transmitted power in the attacked line. From (17), this change will be

$$\Delta \hat{P_{ij}} = \frac{(\mathbf{M}_i - \mathbf{M}_j)^T}{X_{ij}} \mathbf{z}^a. \tag{22}$$

While the attacker tries to increase this change, the defender tries to decrease it by defending the measurements that have high risk of being attacked. Changing the estimated power flow in a specific line will increase the chance of changing prices in both sides of the attacked line[10]. Either increasing or decreasing congestion can bring financial benefits for attacker.

1) Decreasing the Congestion: In day-ahead market the attacker buys at lower price LMP_i^{DA} and sells at higher price LMP_j^{DA} ($LMP_i^{DA} < LMP_j^{DA}$). The difference of two prices should be paid to the transmission company as the congestion prices. In the real-time market, because of decreasing congestion, the congestion price paid by the attacker is less than the supposed congestion price in the day-ahead market so the profit of this trade in \$/MWh will be:

$$\begin{aligned} P_{Cng}^{Dec} &= Congestion_{Price}^{DA} - Congestion_{Price}^{RT} \\ &= (LMP_j^{DA} - LMP_i^{DA}) \\ &\quad - (LMP_j^{RT} - LMP_i^{RT}). \end{aligned} \tag{23}$$

2) Increasing the Congestion: Increasing transmitted power from bus i to bus j, can create congestion in line L_{ij}. This congestion increases/decreases the price of electricity in the receiving/sending end of the transmission line. So the attacker needs to buy a Financial Transmission Right (FTR) from sending bus i to ending bus j. FTR is a financial contract to hedge congestion charges. The FTR holder has access to a specific transmission line in a defined time and location to transmit a specific value of power. In real-time market with creating congestion, FTR can be sold (with higher price) to any Load Serving Entities (LSEs).

In the next section, we will analyze the behavior of both attacker and defender in the real-time market. Limitation in attack (to) and defend (from) different measurements makes a difficult situation for both parties. Mathematical modeling of this behavior in the next section, is an efficient answer to the question of *where should I attack?* and *where should I defend?* for the attacker and the defender, respectively.

[10]The attacker doesn't have access to all data such as the submitted prices, generation limits, etc. So with changing the estimated transmitted power desired direction, the attacker increases the chance of creating or releasing congestion in the attacked line.

V. Gaming Between Attacker and Defender

In order to protect line L, the defender needs to protect group $\mathcal{M}$ and group $\mathcal{N}$. Because the inserted attack will pass the BDD in state estimation [first constraint in (21)], the control center should use some other detection methods. For example, the defender can put some secure measurements into random locations in the network. The main problem in this procedure is that defending all measurements is not possible. On the other hand, it is impossible for the attacker to attack all measurements. Instead it tries to attack measurements that have the most effect on the state estimator without being detected by the control center. This behavior can be modeled with a zero-sum strategic game between the attacker and the defender[11].

A. Two-Person Zero-Sum Game Between Attacker and Defender

Define $A = (\mathcal{N}, (\mathcal{S}_i)_{i\epsilon\mathcal{R}}, (\mathcal{U}_i)_{i\epsilon\mathcal{N}})$ as a game, in which the defender and the attacker compete to increase and decrease the change of the estimated transmitted power ($\Delta \hat{P_{ij}}$), respectively. In this game, $\mathcal{R}$ is the set of players (the defender and the attacker), and the game can be defined as:

- Players set: $\mathcal{R} = \{1, 2\}$ (the defender and the attacker).
- Attacker's strategy: to choose measurements to attack.
- Strategy set $\mathcal{S}_i$: The set of available strategies for player i, $\mathcal{S}_1 = \{{}_\alpha C_{N_a}\}$, $\mathcal{S}_2 = \{{}_\alpha C_{N_d}\}$, where N_a and N_d are the maximum number of measurements that the attacker can attack and the defender can defend and ${}_\alpha C_{N_a}$ is the combination of N_a measurement out of α measurement.
- Utility: $U_1 = \Delta \hat{P_{ij}}$ and $U_2 = -\Delta \hat{P_{ij}}$ for the attacker and the defender, respectively.

B. Noncooperative Finite Games: Two-Person Zero-Sum

A strategic game is a model of interactive decision-making, in which each decision-maker chooses its plan of action once and for all, and these choices are made simultaneously. For a given $(m \times n)$ matrix game $\mathbf{A} = \{a_{ij} : i = 1, \ldots, m;\ j = 1, \ldots, n\}$, let $\{row\ i^*, column\ j^*\}$ be a pair of strategies adopted by the players. Then, if the pair of inequalities

$$a_{i^*j} \leq a_{i^*j^*} \leq a_{ij^*}, \tag{24}$$

is satisfied $\forall i, j$. The two-person zero-sum game is said to have a saddle point in pure strategies. The strategies $\{\text{row } i^*, \text{column } j^*\}$ are said to constitute a saddle-point equilibrium. Or simply, they are said to be the saddle-point strategies. The corresponding outcome $a_{i^*j^*}$ of the game is called the saddle-point value. If a two-person zero-sun game possesses a single saddle point, the value of the game is uniquely given by the value of saddle point. However, the mixed strategies are used to obtain an equilibrium solution in the matrix games that do not possess a saddle point in pure

[11]In the case that there are different non-cooperative attackers, they will have the worst performance. But if the attackers are cooperative, it is the worst case for the defender. In this paper, we consider the worst case by assuming all attackers are together as one party. So we formulate the problem as the two-user zero sum game. If the attackers are non-cooperative, some games such as the Stackelberg game can be employed. These games are interesting topics which needs future investigations.

strategies. A mixed strategy for a player is a probability distribution on the space of its pure strategies. Given an $(m \times n)$ matrix game $\mathbf{A} = \{a_{ij} : i = 1, \ldots, m; j = 1, \ldots, n\}$, the frequencies with which different rows and columns of the matrix are chosen by the defender and the attacker will converge to their respective probability distributions that characterize the strategies. In this way, the average value of the outcome of the game is equal to

$$J(\mathbf{y}, \mathbf{w}) = \sum_{i=1}^{m} \sum_{j=1}^{n} y_i a_{ij} w_j = \mathbf{y}' \mathbf{A} \mathbf{w}, \tag{25}$$

where $\mathbf{y}$ and $\mathbf{w}$ are the probability distribution vectors defined by

$$\begin{aligned} \mathbf{y} &= (y_1, \ldots, y_m)', \\ \mathbf{w} &= (w_1, \ldots, w_n)'. \end{aligned} \tag{26}$$

The defender wants to minimize $J(\mathbf{y}, \mathbf{w})$ by an optimum choice of a probability distribution vector $\mathbf{y} \in Y$, while the attacker wants to maximize the same quantity by choosing an appropriate $\mathbf{w} \in W$. The sets Y and W are

$$Y = \left\{ \mathbf{y} \in R^m : \mathbf{y} \geq \mathbf{0}, \quad \sum_{i=1}^{m} y_i = 1 \right\}, \tag{27}$$

$$W = \left\{ \mathbf{w} \in R^n : \mathbf{w} \geq \mathbf{0}, \quad \sum_{j=1}^{n} w_j = 1 \right\}. \tag{28}$$

Given an $(m \times n)$ matrix game $\mathbf{A}$, a vector $\mathbf{y}^*$ is known as a mixed security strategy for the defender if the following inequality holds $\forall \mathbf{y} \in Y$:

$$\bar{V}_m(\mathbf{A}) \triangleq \max_{\mathbf{w} \in W} \mathbf{y}^{*\prime} \mathbf{A} \mathbf{w} \leq \max_{\mathbf{w} \in W} \mathbf{y}' \mathbf{A} \mathbf{w}, \quad \mathbf{y} \in Y. \tag{29}$$

And the quantity $\bar{V}_m(\mathbf{A})$ is known as the average security level of the defender. We can also define the average security level of the attacker as $\underline{V}_m(\mathbf{A})$ if the following inequality holds for all $\mathbf{w} \in W$:

$$\underline{V}_m(\mathbf{A}) \triangleq \min_{\mathbf{y} \in Y} \mathbf{y}' \mathbf{A} \mathbf{w}^* \geq \min_{\mathbf{y} \in Y} \mathbf{y}' \mathbf{A} \mathbf{w}, \quad \mathbf{w} \in W. \tag{30}$$

The two inequalities can also be given as:

$$\bar{V}_m(\mathbf{A}) = \min_{Y} \max_{W} \mathbf{y}' \mathbf{A} \mathbf{w}, \tag{31}$$

$$\underline{V}_m(\mathbf{A}) = \max_{W} \min_{Y} \mathbf{y}' \mathbf{A} \mathbf{w}. \tag{32}$$

However, it always holds true that $\underline{V}_m(\mathbf{A}) = \bar{V}_m(\mathbf{A})$ for a two-person zero-sum game in the mixed strategies. In this way, for an $(m \times n)$ matrix game $\mathbf{A}$, $\mathbf{A}$ has a saddle point in the mixed strategies, and $V_m(\mathbf{A})$ is uniquely given by

$$\begin{aligned} V_m(\mathbf{A}) &= \bar{V}_m(\mathbf{A}) \\ &= \underline{V}_m(\mathbf{A}). \end{aligned} \tag{33}$$

We can see that if the players are able to use mixed strategies, the matrix games always have a saddle-point solution $V_m(\mathbf{A})$ as the only solution in the zero-sum two-person game.

C. Computation of a Two-Person Zero-Sum Game

One way to get the saddle point in the mixed strategies is to convert the original matrix game into a linear programming (LP) problem. Given $\mathbf{A} = \{a_{ij} : i = 1, \ldots, m; j = 1, \ldots, n\}$ with all entries positive (i.e., $a_{ij} > 0$), the average value of the game in mixed strategies is given by

$$\begin{aligned} V_m(\mathbf{A}) &= \min_{Y} \max_{W} \mathbf{y}' \mathbf{A} \mathbf{w} \\ &= \max_{W} \min_{Y} \mathbf{y}' \mathbf{A} \mathbf{w}. \end{aligned} \tag{34}$$

Obviously, $V_m(\mathbf{A})$ must be a positive quantity on $\mathbf{A}$. Furthermore, the expression can also be written as

$$\min_{\mathbf{y} \in Y} v_1(\mathbf{y}), \tag{35}$$

where $v_1(\mathbf{y})$ is defined as

$$v_1(\mathbf{y}) = \max_{W} \mathbf{y}' \mathbf{A} \mathbf{w} \geq \mathbf{y}' \mathbf{A} \mathbf{w}, \quad \forall \mathbf{w} \in W. \tag{36}$$

In addition, it can also be written as

$$\mathbf{A}' \mathbf{y} \leq \mathbf{1_n} v_1(\mathbf{y}), \quad \mathbf{1_n} \triangleq (1, \ldots, 1)' \in R^n. \tag{37}$$

Now the mixed security strategy for the defender is to

$$\min \ v_1(\mathbf{y}) \quad \text{s.t.} \begin{cases} A' \tilde{\mathbf{y}} \leq \mathbf{1_n}, \\ \tilde{\mathbf{y}}' \mathbf{1_m} = [v_1(\mathbf{y})]^{-1}, \\ \mathbf{y} = \tilde{\mathbf{y}} v_1(\mathbf{y}) \\ \tilde{\mathbf{y}} \geq 0, \end{cases} \tag{38}$$

where $\tilde{\mathbf{y}}$ is defined as $\mathbf{y}/v_1(\mathbf{y})$. This is further equivalent to the maximization problem

$$\max_{\tilde{\mathbf{y}}} \ \tilde{\mathbf{y}}' \mathbf{1_m}, \quad \text{s.t.} \begin{cases} \mathbf{A}' \tilde{\mathbf{y}} \leq \mathbf{1_n}, \\ \tilde{\mathbf{y}} \geq 0 \end{cases}, \tag{39}$$

which is a standard LP problem.

Similarly, we can get the standard LP problem for the attacker

$$\min_{\tilde{\mathbf{w}}} \ \tilde{\mathbf{w}}' \mathbf{1_n}, \quad \text{s.t.} \begin{cases} \mathbf{A} \tilde{\mathbf{w}} \geq \mathbf{1_m}, \\ \tilde{\mathbf{w}} \geq 0, \end{cases} \tag{40}$$

where $\tilde{\mathbf{w}}$ is defined as $\mathbf{w}/v_2(\mathbf{w})$ and

$$v_2 \triangleq \min_{Y} \mathbf{y}' \mathbf{A} \mathbf{w} \leq \mathbf{y}' \mathbf{A} \mathbf{w}, \quad \forall \mathbf{y} \in Y. \tag{41}$$

VI. Numerical Results

In this section, we analyze the effect of attack on the PJM 5-bus test system in [30] with a slightly modifications. Transmission lines' parameters are given in Tables I and II. Generators' and loads' parameters (including $G_i^{\max}$, C_i, and

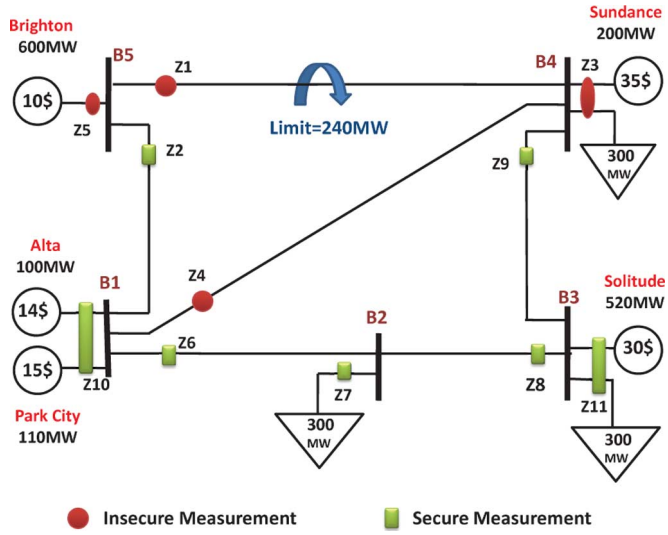


Fig. 2. Measurement configuration in PJM 5-bus test system.

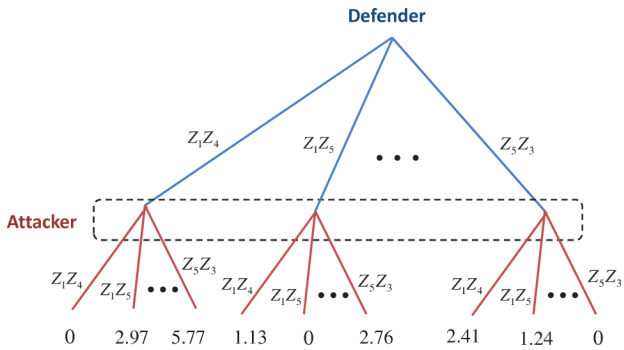


Fig. 3. Extensive form of single-act game.

D_i) together with the location of measurements are shown in Fig. 2. Solving (10) for the day-ahead market shows that L_{54} (line from B_5 to B_4) is congested. Here attacker chooses L_{54} to attack. Knowing H, from (17) the attacker obtains $\mathbf{Q} = [0.2\ 0.05\ 0\ 0.19\ 0.25\ 0.04 - 0.04 - 0.08 - 0.13\ 0.18\ 0.05]$. Positive and negative arrays of this vector correspond to z_+ and z_- vectors, respectively, i.e., $z_+^T = [z_1, z_2, z_4, z_5, z_6, z_{10}]$ and $z_-^T = [z_7, z_8, z_9]$. The greater values of $Q(i)$ correspond to measurements that have more effect on $\hat{P}_{ij}$. Suppose there are 4 insecure measurements $\{z_1, z_4, z_5, z_{10}\}$ and the attacker can compromise 2 of them, also the defender can defend 2 measurements simultaneously. So the attacker should choose 2 measurements among these measurements that have more effect on $\hat{P}_{ij}$ and a sufficiently low probability of detection by the defender. In this example, the attacker can choose from strategy set $\mathcal{S}_1 = \{z_1z_4, z_1z_5, z_1z_3, z_4z_5, z_4z_3, z_5z_3\}$, and the defender can choose from strategy set $\mathcal{S}_2 = \{z_1z_5, z_1z_3, z_4z_5, z_4z_3, z_5z_3\}$. It is assumed that if the attacker for example chooses $\{z_iz_j\}$ (to attack measurement i and j, $i \neq j$) and the defender chooses $\{z_iz_k\}$ (to defend measurement i and k, $i \neq k$), compromising $\{z_j\}$ will be successful, and the change in $\hat{P}_{ij}$ is only because of compromising $\{z_j\}$. If $\boldsymbol{\xi} = [5_{MW}, \ldots, 5_{MW}]'_{(12\times 1)}$, solving (21) and (22) gives $\Delta\hat{P}_{54} = U_1 = -U_2$. As Fig. 3 shows, these payoffs are the results of different attack and defend strategies (which both players take). The attacker and defender in this game are not aware of the sequence of play. Also one player

TABLE I
LINE REACTANCE AND THERMAL LIMIT FOR 5–BUS TEST SYSTEM

Line	L_{12}	L_{14}	L_{15}	L_{23}	L_{34}	L_{45}
X (%)	2.81	3.04	0.64	1.08	2.97	2.97
$F_k^{max}(MW)$	999	999	999	999	999	240

TABLE II
GENERATION SHIFT FACTORS OF LINES IN 5–BUS TEST SYSTEM

Line \ Bus	B_1	B_2	B_3	B_4	B_5
L_{1-2}	0.1939	-0.476	-0.349	0	0.1595
L_{1-4}	0.4376	0.258	0.1895	0	0.36
L_{1-5}	0.3685	0.2176	0.1595	0	-0.5195
L_{2-3}	0.1939	0.5241	-0.349	0	0.1595
L_{3-4}	0.1939	0.5241	0.6510	0	0.1595
L_{5-4}	0.3685	0.2176	0.1595	0	0.4805

TABLE III
ZERO-SUM GAME BETWEEN THE ATTACKER AND THE DEFENDER

		w_1	w_2	w_3	w_4	w_5	w_6
	Att. / Def.	z_1z_4	z_1z_5	z_1z_{10}	z_4z_5	z_4z_{10}	z_5z_{10}
y_1	z_1z_4	0	3.14	2.81	3.14	2.81	4.84
y_2	z_1z_5	1.17	0	2.81	1.17	5	2.81
y_3	z_1z_{10}	1.17	3.14	0	5	1.17	3.14
y_4	z_4z_5	1.28	1.28	4.43	0	2.81	2.81
y_5	z_4z_{10}	1.28	5.35	1.28	3.14	0	3.14
y_6	z_5z_{10}	3.21	1.28	1.28	1.17	1.17	0

has no idea about the other player's action. These situations are described by a normal form zero-sum game in Table III.

Table III shows that $\min(\max_{row}) = 3.21$, which is not equal to $\max(\min_{column}) = 0$. So there is no $a_{i^*j^*}$ that satisfies (24). Therefore, the game doesn't have a single saddle point and the problem shifts to finding the proportion of times that the attacker and the defender, play their own strategies. Solving such a game (which does not have a single saddle point) is a linear programming. From (39) defender defines $\tilde{\mathbf{y}}$, we have

$$\max \quad \tilde{\mathbf{y}}'\mathbf{1_m},$$
$$\text{s.t.} \quad \begin{cases} 1.17\tilde{y}_2 + 1.17\tilde{y}_3 + 1.28\tilde{y}_4 + 1.28\tilde{y}_5 + 3.2\tilde{y}_6 \leq 1, \\ 3.14\tilde{y}_1 + 3.14\tilde{y}_3 + 1.28\tilde{y}_4 + 5.35\tilde{y}_5 + 1.28\tilde{y}_6 \leq 1, \\ 2.81\tilde{y}_1 + 2.81\tilde{y}_2 + 4.43\tilde{y}_4 + 1.28\tilde{y}_5 + 1.28\tilde{y}_6 \leq 1, \\ 3.14\tilde{y}_1 + 1.17\tilde{y}_2 + 5\tilde{y}_3 + 3.14\tilde{y}_5 + 1.17\tilde{y}_6 \leq 1, \\ 2.81\tilde{y}_1 + 5\tilde{y}_2 + 1.17\tilde{y}_3 + 2.81\tilde{y}_4 + 1.17\tilde{y}_6 \leq 1, \\ 4.84\tilde{y}_1 + 2.81\tilde{y}_2 + 3.14\tilde{y}_3 + 2.81\tilde{y}_4 + 3.14\tilde{y}_5 \leq 1, \\ \tilde{y}_1, \tilde{y}_2, \tilde{y}_3, \tilde{y}_4, \tilde{y}_5, \tilde{y}_6 \geq 0, \end{cases} \quad (42)$$

which gives $\tilde{\mathbf{y}} = [0\ 0.049\ 0.134\ 0.136\ 0.018\ 0.183]$. Therefore, $\mathbf{y} = \tilde{\mathbf{y}}v_1(\mathbf{y}) = \tilde{\mathbf{y}}(\tilde{\mathbf{y}}'\mathbf{1_m})^{-1} = [0\ 0.094\ 0.26\ 0.262\ 0.0347\ 0.35]$. Similarly, solving (40) for the attacker gives $\tilde{\mathbf{w}} = [0.29\ 0\ 0.02\ 0.019\ 0.019\ 0.174]$, and therefore, $\mathbf{w} = \tilde{\mathbf{w}}v_1(\mathbf{w}) = \tilde{\mathbf{w}}(\tilde{\mathbf{w}}'\mathbf{1_m})^{-1} = [0.556\ 0\ 0.038\ 0.036\ 0.037\ 0.333]$.

Fig. 4 shows the proportion of times that the defender and the attacker should defend and attack different measurements, respectively. As discussed in Section IV, changing the estimated transmitted power in line L_{54} can change the prices in either bus 5 or bus 4. In real-time market the control center estimates transmitted power and then knowing dispatch schedule (which is defined in day-ahead market) load level in different buses is estimated. This estimated load together with the current state of

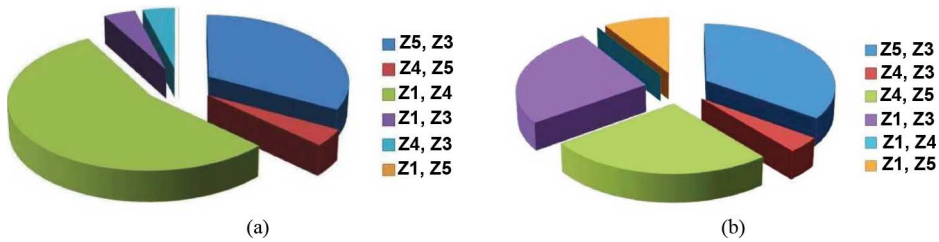


Fig. 4. Proportion of times that attacker and defender, attack and defend to measurements respectively. (a) Probability of attack. (b) Probability of defend.

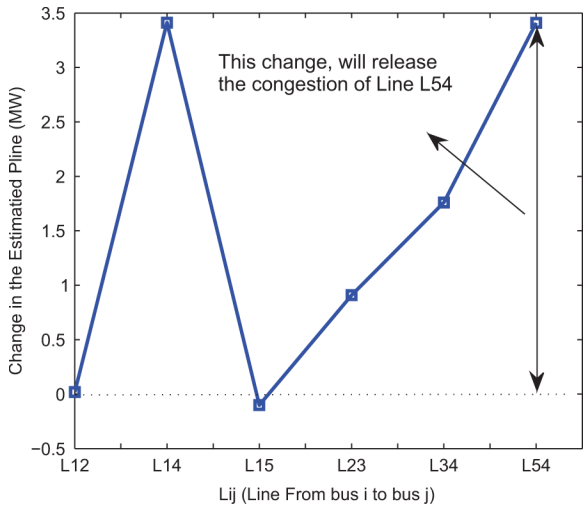


Fig. 5. Change in the estimated transmitted power of lines because of attack to Z_1 and Z_4.

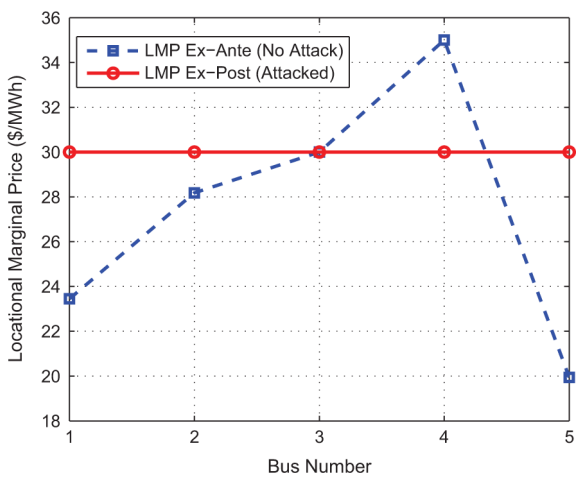


Fig. 6. Locational marginal prices for PJM 5-bus test system for both with attack and without attack.

the network is applied to a DCOPF, and this program defines the real-time prices. If the operating condition (such as the load level) has not changed and there is no error in the measurements, the real-time prices should be the same as the day-ahead prices. Here without loss of generality, we assume that the actual load level doesn't change and any change in the estimated load level is because of bad data injection to the state estimator.

The following example shows how attacker is able to change the prices in real-time market. Suppose attacker compromise $z_1 z_4$ and the defender defends $z_5 z_{10}$ so, attack against $z_1 z_4$ is successful. In this case solving (21) gives $\mathbf{z^a} = [8.21\ 0\ 0\ 8.09\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0]_{(MW)}$. So from (5), estimated states for all buses will be $\hat{\boldsymbol{\theta}} = [50\ 56\ 65\ 01\ 71.6] \times 10^{-3}_{(rad)}$. Using (17), estimated transmitted power can be obtained[12] $\hat{P}_{54} = 236.59_{(MW)}$. This power is less than thermal limit of transmission line that shows, congestion in this line is released. In this case solving (15) and (16) gives the real time prices (here it is assumed that $\Delta G_i^{\max} = -\Delta G_i^{\min} = 0.1_{MW}$ and $\Delta D_i^{\max} = -\Delta D_i^{\min} = 0_{MW}$).

Fig. 6 shows the prices for attacked and without-attack cases. Change of estimated transmitted power in transmission line is shown in Fig. 5. Now, assume that in day-ahead market, the attacker buys 100_{MW} power in bus 5 and sells it in bus 4. From (23), the profit of this contract will be:

$$Profit = [(35 - 20) - (30 - 30)] \times 100 = 1500_{(\$/h)}. \quad (43)$$

VII. Conclusion

In this paper, first we analyzed the effect of compromising each measurement on the state estimator results. Compromising these measurements can change the congestion and consequently the price of electricity, and thus, the attacker has an intensive to change the congestion in the desired direction. Since a typical power system has a huge number of measurements, attacking or defending all of those becomes impossible for attacker and defender, respectively. To this end, this behavior is modeled and analyzed in the framework of game theory. The simulation results on PJM 5–Bus test system indicate that, in the specified load level, how attacker can change the prices in the desired direction (decreasing in this example).

References

[1] T. F. Garrity, "Getting smart," *IEEE Power Energy Mag.*, vol. 6, no. 2, pp. 38–45, Mar./Apr. 2008.
[2] A. Monticelli, "Electric power system state estimation," *Proc. IEEE*, vol. 88, no. 2, pp. 262–282, Feb. 2000.
[3] Y. Yuan, Z. Li, and K. Ren, "Modeling load redistribution attacks in power system," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 382–390, Jun. 2011.
[4] Y. Yuan, Z. Li, and K. Ren, "Quantitative analysis of load redistribution attack in electric grid," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 9, pp. 1731–1738, Sep. 2012.
[5] J. Meserve, "Staged cyber attack reveals vulnerability in power grid," CNN, Sep. 2007 [Online]. Available: http://www.cnn.com/2007/US/09/26/power.at.risk/index.html
[6] M. Esmalifalak, Z. Han, and L. Song, "Effect of stealthy bad data injection on network congestion in market based power system," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Paris, France, Apr. 2012.

[12]This value is considered as the real-time transmitted power in L_{54}.

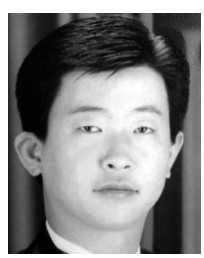
[7] L. Xie, Y. Mo, and B. Sinopoli, "Integrity data attacks in power market operations," *IEEE Trans. Smart Grid*, vol. 2, no. 99, pp. 659–666, Dec. 2011.
[8] G. Chen, Z. Y. Dong, D. J. Hill, and Y. S. Xue, "A zonal congestion management approach using real and reactive power rescheduling," *IEEE Trans. Power Syst.*, vol. 19, no. 1, pp. 554–562, Feb. 2004.
[9] M. E. Falak, M. O. Buygi, and A. Karimpour, "Market oriented reactive power expansion planning using locational marginal price," in *Proc. IEEE 2nd Int. Power Energy Conf. (PECon)*, Johor Baharu, Malaysia, Dec. 2008.
[10] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid—The new and improved power grid: A survey," *Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 944–980, 2012.
[11] H. E. Brown and S. Suryanarayanan, "A survey seeking a defenition of a smart distribution system," in *Proc. North Amer. Power Symp. 2009*, pp. 1–7.
[12] S. Rohjansand, M. Uslar, R. Bleiker, J. González, M. Specht, T. Suding, and T. Weidelt, "Survey of smart grid standardization studies and recommendations," in *Proc. 1st IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, Oldenburg, Germany, Oct. 2010.
[13] Office of the National Coordinator for Smart Grid Interoperability, NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0 Jan. 2010 [Online]. Available: http://www.nist gov/public_affairs/releases/upload/smartgrid-interoperability_final.pdf
[14] A. Teixeira, S. Amin, H. Sandberg, K. H. Johansson, and S. S. Sastry, "Cyber security analysis of state estimators in electric power systems," in *Proc. 49th IEEE Conf. Decision Control (CDC)*, Dec. 2010.
[15] Y. Liu, M. K. Reiter, and P. Ning, "False data injection attacks against state estimation in electric power grids," in *Proc. 16th ACM Conf. Comput. Commun. Security*, Nov. 2009.
[16] M. Esmalifalak, H. Nguyen, R. Zheng, and Z. Han, "Stealth false data injection using independent component analysis in smart grid," in *Proc. IEEE 2nd Conf. Smart Grid Commun.*, Brussels, Belgium, Oct. 2011.
[17] A. R. Metke and R. L. Ekl, "Smart grid security technology," in *Proc. Innov. Smart Grid Technol. (ISGT)*, Schaumburg, IL, Jan. 2010.
[18] H. Li, L. Lai, and R. C. Qiu, "Communication capacity requirement for reliable and secure state estimation in smart grid," in *Proc. 1st IEEE Conf. Smart Grid Commun.*, Oct. 2010, pp. 191–196.
[19] G. Chen, Z. Y. Dong, D. J. Hill, and Y. S. Xue, "Exploring reliable strategies for defending power systems against targeted attacks," *IEEE Trans. Power Syst.*, vol. 26, no. 3, pp. 1000–1009, Aug. 2011.
[20] Smart Grid Interoperability Panel Cyber Security Working Group, Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security Sep. 2010 [Online]. Available: http://www.nist.gov/smartgrid/upload/nistir-7628_total.pdf
[21] M. Swearingen, "Real time evaluation and operation of the smart grid using game theory," in *Proc. IEEE Rural Elect. Power Conf. (REPC)*, Hooker, OK, Apr. 2011.
[22] Z. Zhu, J. Tang, S. Lambotharan, W. H. Chin, and Z. Fan, "An integer linear programming and game theory based optimization for demand-side management in smart grid," in *Proc. IEEE GLOBECOM Workshops (GC Wkshps)*, Loughborough, U.K., Dec. 2011.
[23] Z. M. Fadlullah, Y. Nozaki, A. Takeuchi, and N. Kato, "A survey of game theoretic approaches in smart grid," in *Proc. Int. Conf. Wireless Commun. Signal Process. (WCSP)*, Sendai, Japan, Nov. 2011.
[24] X. Zhang, J. Lu, H. Sun, and X. Ma, "Orderly consumption and intelligent demand-side response management system under smart grid," in *Proc. Asia-Pac. Power Energy Eng. Conf. (APPEEC)*, Beijing, China, Mar. 2010.
[25] P. Wang, J. Y. Huang, Y. Ding, P. Loh, and L. Goel, "Demand side load management of smart grids using intelligent trading/metering/ billing system," in *Proc. IEEE Power Energy Soc. Gen. Meet.*, Singapore, Jul. 2010.
[26] S. Bu, F. R. Yu, and P. X. Liu, "A game-theoretical decision-making scheme for electricity retailers in the smart grid with demand-side management," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, Ottawa, ON, Canada, Oct. 2011.
[27] A. Mohsenian-Rad, V. W. S. Wong, J. Jatskevich, R. Schober, and A. Leon-Garcia, "Autonomous demand-side management based on game-theoretic energy consumption scheduling for the future smart grid," *IEEE Trans. Smart Grid*, vol. 1, no. 3, pp. 320–331, Dec. 2010.
[28] A. J. Wood *et al., Power Generation, Operation, and Control*. New York: Wiley, 1996.
[29] A. Abur and A. G. Exposito, *Power System State Estimation: Theory and Implementation*. New York: Marcel Dekker, 2004.
[30] F. Li and R. Bo, "Small test systems for power system economic studies," in *Proc. Power Energy Soc. Gen. Meet.*, Minneapolis, MN, Jul. 2010.
[31] F. Li and R. Bo, "DCOPF-based LMP simulation: Algorithm, comparison with ACOPF, and sensitivity," *IEEE Trans. Power Syst.*, vol. 22, no. 4, pp. 1475–1485, Nov. 2007.
[32] F. Li, J. Pan, and H. Chao, "Marginal loss calculation in competitive electrical energy markets," in *Proc. 2004 IEEE Int. Conf. Elect. Utility Deregulation, Restructuring Power Technol. (DRPT)*, Apr. 2004, vol. 1, pp. 205–209.
[33] E. Litvinov, T. Zheng, G. Rosenwald, and P. Shamsollahi, "Marginal loss modeling in LMP calculation," *IEEE Trans. Power Syst.*, vol. 19, no. 2, pp. 880–888, May 2004.
[34] A. L. Ott, "Experience with PJM market operation, system design, and implementation," *IEEE Trans. Power Syst.*, vol. 18, no. 2, pp. 528–534, May 2003.
[35] T. Zheng and E. Litvinov, "Ex post pricing in the co-otimized energy and reserve market," *IEEE Trans. Power Syst.*, vol. 21, no. 4, pp. 1528–1538, Nov. 2006.

Mohammad Esmalifalak (S'12) received his M.S. degree in power system engineering from Shahrood University of Technology, Shahrood, Iran, in 2007. He joined the Ph.D. program at the University of Houston (UH), TX, in 2010.

From 2010 to 2012 he was a Research Assistant in the ECE department at UH. He is the author of the paper that won the best paper award in IEEE Wireless Communications and Networking Conference (WCNC 2012), Paris, France. His main research interests include the application of data mining, machine learning, and signal processing in the operation and expansion of smart grids.

Ge Shi is working toward the B.S. degree in electronics engineering from Peking University, Beijing, China.

He is now working on research about intelligent information processing in machine to machine communications (M2M) based on ZigBee protocol under the direction of Prof. Lingyang Song in State Key Laboratory of Advanced Optical Communication Systems & Networks, Peking University. His research interests mainly include smart grids, game theory, and internet of things.



Zhu Han (S'01–M'04–SM'09) received the B.S. degree in electronic engineering from Tsinghua University, China, in 1997, and the M.S. and Ph.D. degrees in electrical engineering from the University of Maryland, College Park, in 1999 and 2003, respectively.

From 2000 to 2002, he was an R&D Engineer of JDSU, Germantown, MD. From 2003 to 2006, he was a Research Associate at the University of Maryland. From 2006 to 2008, he was an Assistant Professor at Boise State University, ID. Currently, he is an Assistant Professor in Electrical and Computer Engineering Department at the University of Houston, TX. His research interests include wireless resource allocation and management, wireless communications and networking, game theory, wireless multimedia, security, and smart grid communication.

Dr. Han is an Associate Editor of IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS since 2010. He is the winner of IEEE Fred W. Ellersick Prize 2011. He is an NSF CAREER award recipient 2010. He is the coauthor for the papers that won the best paper awards in IEEE International Conference on Communications 2009, 7th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt09), and IEEE Wireless Communication and Networking Conference, 2012.

Lingyang Song (S'03–M'06–SM'12) received his Ph.D. degree from the University of York, U.K., in 2007, where he received the K. M. Stott Prize for excellent research.

He worked as a Postdoctoral Research Fellow at the University of Oslo, Norway, and Harvard University, until rejoining Philips Research UK in March 2008. In May 2009, he joined the School of Electronics Engineering and Computer Science, Peking University, China, as a Professor. His main research interests include MIMO, OFDM, cooperative communications, cognitive radio, physical layer security, game theory, and wireless ad hoc/sensor networks. He is co-inventor of a number of patents (standard contributions), and author or co-author of over 100 journal and conference papers.

Dr. Song received the best paper award in IEEE International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM 2007), the best paper award in the First IEEE International Conference on Communications in China (ICCC 2012), the best student paper award in the7th International Conference on Communications and Networking in China (ChinaCom2012), and the best paper award in IEEE Wireless Communication and Networking Conference (WCNC2012). He is currently on the Editorial Board of *IET Communications*, *Journal of Network and Computer Applications*, and *International Journal of Smart Homes*, and a guest editor of *Elsevier Computer Communications* and *EURASIP Journal on Wireless Communications and Networking*. He serves as a member of Technical Program Committee and Co-chair for several international conferences and workshops.