Proc. of the Intl. Conf. on Advances In Computing, Communication and Information Technology – CCIT 2014.

ISBN: 978-1-63248-010-1 doi: 10.15224/ 978-1-63248-010-1-16

Jamming Attack in Smart Grid with Dynamic Gaming Theory

[Yuting Liu, Jinghuan Ma, Lingyang Song and Zhu Han]

***Abstract*—As the current power grid system is upgrading to smart grid, it becomes more vulnerable to security attacks such as Denial-of-Service attacks. One type of such attacks is jamming attack. In this paper, we analyze the scenario in which the attacker can jam specific signal channels in order to change the electricity prices to create the opportunity for profit, and the defender protect a limited number of channels. Based on the electricity marketing model, we propose multi-act dynamic game between the attacker and the defender, in which both of them will take the optimal strategy to maximize their own profits. We construct the gaming process and discuss the prosperities of the outcome. Simulation results confirm the optimality and prosperities of the proposed scheme.**

***Keywords*—smart grid, jamming, dynamic games**

I. Introduction

Smart grid is an emerging cyber-physical system integrating power infrastructures with information technologies [1]. To guarantee reliable cooperation in smart grid, online monitoring to offer real-time measurements and state estimation are two key components required [2]. Sensors throughout the power system provide observations to identify the current operating state such as the transmission line loadings and bus voltage, based on which the control center (such as SCADA center) stabilizes the whole power grid. However, attack on the communication system can cause malfunctions of the power market or power grid.

Many researches have been conducted over cyber security for smart grid [3]–[4]. In [3], the authors presented an undetectable attack method based on the Jacobian matrix. In [4], based on the hierarchical information and communication model, the information security risks and information security protection demands of smart grid were studied.

Specifically, the denial-of-service (DoS) attack on the communication infrastructure in smart grid is a severe threat, causing the instability of the power system or even regional blackout. One type of DoS attacks is the jamming in the physical layer of the grid's communication networks [5]. In the attack, a jammer emits undesired signals to the communication channel to interfere the ongoing data transmission. Hence, it is critical to ensure the capability of the robustness against the jamming attack. Until now, many works have been done over attacks in wireless sensor networks [6]. When analyzing attacker's strategy during the attack, the game theory approaches have been applied in smart grid to simulate the optimization of the strategy choices during the attack [7].

The general case is that attacks always last for a long term. Once jamming attack is launched, the detection module equipped with sensor nodes is triggered to inform the control center for countermeasures. However, when the control center responds to take action after the detection, attacker can further changes jamming signals to continue their attack. We divide the whole process to time slots, each of which is defined as an independent level, when both attacker and defender will decide their strategies based on their observation and prediction to attain optimal profit.

In this paper, we study the jamming attack and anti-jamming strategy in smart grid. The jammer can profit from the price gap between the day-ahead market and the real-time market [8]. Due to the limited resources available, it can be modeled by a two-person finite dynamic game. Our contributions are summarized as:

- We study the impact of jamming attack on the electricity market and propose countermeasures to antagonize attacks for security in power grid.
- We adopt the multi-act dynamic games and investigate the strategy equilibrium between the attacker and defender.
- The simulation results confirm the effectiveness of the proposed algorithm over PJM 5-bus test system.

The remainder of the paper is organized as follows. The system model is provided in Section II. The elements of the proposed game are defined in Section III, and the Nash equilibrium is analyzed in Section IV. The numerical results and conclusions are provided in Sections V and VI, respectively.

II. System Model

In this section, we study the power state estimation in transmission system, which provides the real-time information of power demand and generation. Then we investigate the pricing mechanism Optimal Power Flow (OPF) and the Locational Marginal Price (LMP) that has been applied in the electricity market.

A. *Power System State Estimation*

In the state estimation, the control center obtains the observation of m real-time measurements from n sensors among the network with phase angles ϕ_i. Since the voltage phase (ϕ_i) of a reference bus is fixed and known, we only

Yuting Liu/1st Affiliation
Peking University
China

Proc. of the Intl. Conf. on Advances In Computing, Communication and Information Technology – CCIT2014.

ISBN: 978-1-63248-010-1 doi: 10.15224/ 978-1-63248-010-1-16

have to estimate ($n-1$) left unknown. We define the state vector as $\phi=[\phi_1,...,\phi_n]^T$ and the observed vector P for m active power measurements [9], related with the active power, which can be described as follows [10]:

$$P = p(\phi)+\varepsilon, \quad (1)$$

where $P=[P_1,...,P_m]^T$ denotes the vector of measured active power in transmission lines, p(•) is the non-linear relation between measurements, ϕ denotes the vector of n bus phase angles ϕ_i and $\varepsilon=[\varepsilon_1,...,\varepsilon_m]^T$ is the Gaussian measurement noise vector with covariant matrix $\sum e$. The Jacobian matrix $H \in \Re^m$ is defined as:

$$H=\frac{\partial p(\phi)}{\partial \phi}|_{\phi=0}. \quad (2)$$

Since the phase difference ($\phi_i-\phi_j$) is small, equation (1) can be reduced to P the following linear approximation:

$$P = p(\phi)+\varepsilon, \quad (3)$$

The bad data can be injected to P to impact the state estimation of ϕ_i. Given the power flow measurements P, the estimated state vector $\hat{\phi}$ can be computed as:

$$\hat{\phi}=(H^T \sum_e^{-1} H)^{-1} H^T \sum_e^{-1} P = BP, \quad (4)$$

where $B=H(H^T \sum_e^{-1} H)^{-1} H^T \sum_e^{-1}$. □□□□□□□□□□

B. *DC OPF and LMP*

OPF is adopted to provide the constraints of optimization of electricity allocation in power systems [11]. The locational marginal pricing methodology has been the primary approach in electricity markets to set electricity prices and deal with transmission congestion. LMPs are forecasted on the basis of the OPF model. The linear form of DC OPF to predict the electricity price in the market is proved to be effective in generation scheduling [12]. Then, LMP at each bus of the power network is decided by the linear programming solution of the problems described as:

$$\min_{G_i} \sum_{i=1}^{N} C_i \times G_i. \quad (5)$$

$$\text{s.t.} \begin{cases} \sum_{i=1}^{N} G_i - \sum_{i=1}^{N} D_i(z) = 0, \\ \sum_{i=1}^{N} GSF_{k-i} \times (G_i - D_i(p)) \le Limit_k^{\max}, k \in \kappa, \\ G_i^{\min} \le G_i \le G_i^{\max}, i \in \Im, \end{cases}$$

Specifically, we assume that LMP_i can be denoted from this equation set as:

$$LMP_i = \lambda + \sum_{i=1}^{L} GSF_{k-i} \times \mu_k, \quad (6)$$

where N denotes the number of buses, C_i denotes the generation cost at bus i in (\$/MWh), G_i is the generation dispatch at bus i in (MWh), GSF_{k-i} denotes the generation shift factor from bus i to line k, κ is the set of all lines in the grid, $\Im$ is the set of all generators and $Limit_k^{\max}$ denotes the transmission limit for line k. In particular, $D_i(p)$ is the demand for the electricity, which is a one-variable function of the measurement p.

III. Jamming Attack in Electricity Market

In this section, we introduce how attackers change the electricity price by jamming attack on the monitoring system.

A. *Jamming Attack Procedure*

The pricing mechanism is dependent on the state estimation from the sensors. However, when being jammed, the measurements from state estimators are unavailable to the control center [13]. We adopt a discrete-time model of jamming attacks, in which time is divided into time slots. The procedure in each time slot is given below:

- At the beginning, the attacker jams specific channels in the network to cause measurements unavailable.
- The control center uses default values to substitute lost measurements for the DC OPF model.
- The attacker keeps monitoring the power market and jamming the insecure measurements.
- The attacker predicts real-time prices.
- The attacker will buy electricity at lower price and sell at higher price.

B. *Jamming Attack Strategies*

Manipulating prices is one incentive for the attacker to compromise the measurements. With online monitoring of power systems, the transmitted power load on the transmission lines can be depicted in a linear model as:

$$\hat{p}_{ij} = \frac{\phi_i - \phi_j}{X_{ij}} = \frac{(B_i - B_j)^T}{X_{ij}} P = M^T P, \quad (7)$$

From (7), we can ensure the linear relation between $\hat{p}_{ij}$ and P in one time slot.

With no state estimation received from sensors during the jamming attack, the control substitutes the default value P_{def} for sensors jammed by the attacker. LMP_i^{jam} is given as:

Proc. of the Intl. Conf. on Advances In Computing, Communication and Information Technology – CCIT 2014.

ISBN: 978-1-63248-010-1 doi: 10.15224/ 978-1-63248-010-1-16

$$LMP_i^{jam} = \lambda^{jam} + \sum_{i=1}^{L} GSF_{k-i} \times \mu^{jam}. \quad (8)$$

At the end of a time slot, the attacker ceases jamming, so the control center receives the real-time estimation again. DCOPF program decides the real-time price in the same form of (7). Then LMP_i^{AJ} after jammers' ceasing attack, which is altered in the form as:

$$LMP_i^{AJ} = \lambda^{AJ} + \sum_{i=1}^{L} GSF_{k-i} \times \mu^{AJ}. \quad (9)$$

Given the definition of two prices LMP_i^{jam} and LMP_i^{AJ}, we can clearly define the profit that the attacker gains from the attack during one time slot. We assume that the attacker will gain all the difference between two prices ΔL_i at every bus i:

$$\Delta L_i = \left| LMP_i^{jam} - LMP_i^{AJ} \right|. \quad (10)$$

IV. Attacker and Defender Gaming

In this section, we firstly introduce the single-act games solutions in both pure strategy and mixed strategy. Then we turn to dynamic games with multiple stages and specifically introduce the advantages of the recursive algorithm to analyze behaviors in the electricity market.

A. *Single-act Games in Extensive Forms*

To start with, we define a two-person zero sum game A, in which two players compete with each other for more profit given the maintaining zero sum of gains [14]. Extensive form games are compared with the normal form ones where we separately consider the outcomes resulted from two players' strategies.

A two-person zero-sum finite game without chance moves is a finite tree structure. The set of all strategies for Pi is called his strategy set (space), and it is denoted by Γ^i.Let $J(\gamma^1, \gamma^2)$ denote the attacker's profit from the successful attack as the loss to defender's when they employ the strategies in Γ^1 and Γ^2. In this way, a pair of strategies $\{\gamma^{1*} \in \Gamma^1, \gamma^{2*} \in \Gamma^2\}$ is in saddle-point equilibrium if the following set of the inequalities is satisfied for all $\gamma^1 \in \Gamma^1$, $\gamma^2 \in \Gamma^2$:

$$J(\gamma^{1*}, \gamma^2) \le J(\gamma^{1*}, \gamma^{2*}) \le J(\gamma^1, \gamma^{2*}), \quad (11)$$

where $J(\gamma^{1*}, \gamma^{2*})$ is the saddle-point value of the zero-sum game. We briefly introduce the optimal algorithm for stable maximum profit in zero-sum single-act games in Table I.

TABLE I. ALGORITHM FOR OPTIMIZATION IN SINGLE-ACT GAMES

Step	Procedures
1	Define the defender as the 1st-acting P1 and attacker P2
2	Rewrite A into several sub-games g^i in matrix form
3	Determine every solution $(\gamma^{1*}, \gamma^{2*})$ for corresponding g^i

Then we introduce the saddle-point solution $(\gamma^{1*}, \gamma^{2*})$ in two different circumstances.

1) In pure strategy:

As for a given $(s \times t)$ matrix game $g^i = \{a_{mn}\}^i$, (row m^*, column $n^*)^i$ constitutes a saddle-point equilibrium which is satisfied for all $a_{mn}^i \in g^i$:

$$a_{m^*n}^i \le \max_n a_{m^*n}^i, = \bar{V}(g^i) = \underline{V}(g^i) = \min_m a_{mn^*}^i \le a_{mn^*}^i, \quad (12)$$

and corresponding outcome $a_{m^*n^*}^i$ is called the saddle-point value, denoted by $V(A)$.

2) In mixed strategy:

We denote that players can pick probability distribution on space of strategies by Γ^1 and Γ^2. Here, we note the s-dimensional simplex, Y, and t-dimensional simplex, X, as both players' strategy space. Hence, the average value of the outcome of the game is given as:

$$J(y,x)^i = \sum_{m=1}^{s}\sum_{n=1}^{t} y_m a_{mn}^i x_n = y' g^i x, \quad (13)$$

where y and x are probability distribution vectors defined by

$$y = (y_1, ..., y_s)', \; x = (x_1, ..., x_t). \quad (14)$$

In any matrix game, the average security levels of the players in mixed strategies coincide, that is:

$$\bar{V}_B(g^i) = \min_Y \max_X y' g^i x = \max_X \min_Y y' g^i x = \underline{V}_B(g^i), \quad (15)$$

where $\bar{V}_B$ and $\underline{V}_B$ is the upper and lower level of the defender's and attacker's security level. Hence, the mixed–strategy equilibrium is uniquely given by:

$$\bar{V}_B(g^i) = V_B(g^i) = \underline{V}_B(g^i). \quad (16)$$

B. *Dynamic Games*

The attack always lasts for a long term instead of the attacker's single-stage decision. Both attacker and defender should adjust their strategies according to the observation of both players' past choices. Their behavior can be modeled with a multi-act non-cooperative game between the attacker and the defender.

Define $A = (k, (S_i)_{i \in \square}, (U_i)_{i \in N})$ as a game in which, the defender and the attacker compete to compromise and defend the insecure measurements in set N within k levels. Game A in Figure 1 consists of:

- Player set: $R = \{1, 2\}$ (P1 and P2);
- Attacker's strategy: insecure measurements available
- Strategy set S_i: set of available strategies for player i;
- Utility: function to assign profit between players

Proc. of the Intl. Conf. on Advances In Computing, Communication and Information Technology – CCIT 2014.

ISBN: 978-1-63248-010-1 doi: 10.15224/ 978-1-63248-010-1-16

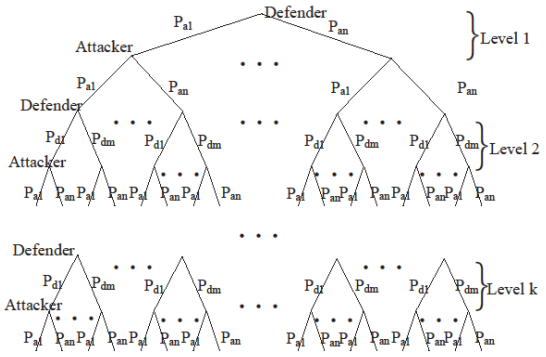

Figure 1. Two–person Zero–sum Game in Extensive Form with K Levels

In this model, we introduce the multi-act games within the discrete-time c model in the electricity market. In a game with K levels, a typical strategy γ^i of defender and attacker can be viewed as composed of K components $(\gamma_1^1,...,\gamma_1^K)$ and $(\gamma_2^1,...,\gamma_2^K)$ .where γ_i^j stands for the corresponding strategy of P_i at his j^{th} level of action. Then we introduce the dynamic algorithm in Table II.

TABLE II. ALGORITHM FOR OPTIMIZATION IN SINGLE-ACT GAMES

Step	Procedures
1	Solve g_K^i assigned by P2's information set at Kth level using the algorithm in Table I
2	Solve every satisfying $(\gamma_K^{1*},\gamma_K^{2*})$ in (11) for all g_K^i.
3	Compute corresponding outcomes $V(g_K^i)$ or $V_B(g_K^i)$.
4	Assign outcomes V at Kth level to each (K-1)-level nodes.
5	Repeat step 2, 3, and 4 until A is simplified into single-act.

1) Optimality of Algorithm:

To illustrate this algorithm in the smart gird more specifically, we need some refinements of the Nash equilibrium concept and then illustrate the optimality

The saddle–point solution of feedback games $(\gamma^{1*},\gamma^{2*})$ satisfies recursively the following set of K pairs of inequalities for all $\gamma_j^i \in \Gamma_j^i$, $i=1,2;\ \ j=1,...,K$:

$$\left.\begin{aligned} &J(\gamma_1^1,...,\gamma_{k-1}^1,\gamma_k^{1*};\gamma_1^2,...,\gamma_K^2) \le J(\gamma_1^1,...,\gamma_K^{1*};\\ &\gamma_1^2,...,\gamma_{k-1}^2,\gamma_k^{2*}) \le J(\gamma_1^1,...,\gamma_K^1;\gamma_1^2,...\gamma_{K-1}^2,\gamma_K^{2*}),\\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\ &J(\gamma_1^{1*},...,\gamma_k^{1*};\gamma_1^2,\gamma_2^{2*}...,\gamma_K^{2*}) \le J(\gamma_1^{1*},...,\gamma_K^{1*};\\ &\gamma_1^{2*},...,\gamma_k^{2*}) \le J(\gamma_1^1,\gamma_2^{1*}...,\gamma_K^{1*};\gamma_1^{2*},...,\gamma_K^{2*}) \end{aligned}\right\} \quad (17)$$

Proof: The outcome $J(\gamma_1^1,...,\gamma_K^1;\gamma_1^2,...,\gamma_K^2)$ in the whole game is independently addictive. Then we add the same $J(\gamma_1^1,...,\gamma_{K-1}^1;\gamma_1^2,...,\gamma_{K-1}^2)$ to (11) can acquire the first inequality in (17). Recursively, we can get all these inequalities one by one.

2) Algorithm Comparison

Multi-act games can be solved with different algorithms, one commonly utilized of which is simply repeated algorithm, Players take simply repeated algorithm repeat their choices during the whole process without any strategy evolution, in which case, the maximization will be processed for one time.

In simply repeated games, two players fix their strategy choices on $(\gamma_1^{1*},\gamma_1^{2*})$. From optimality of dynamic programming, dynamic algorithm performs better in outcomes than simply repeated algorithm for all level $i, i\in\{1,2,...K\}$:

$$J(\gamma_1^{1*},\gamma_1^{2*}) \le J(\gamma_i^{1*},\gamma_i^{2*}). \quad (18)$$

V. Numerical Results

A. Parameters

We analyze the effect of attack on the PJM 5-bus test system in [15] with some slightly modifications. Transmission lines' parameters are given in Table III and Table IV, generators' and loads' parameters in Figure 1. The default values of the measurements are shown in Table V. These default values are utilized to substitute corresponding insecure measurements, when the real-time measurements have been jammed.

B. Two–Person Zero–Sum Dynamic Games

In 5-bus test system shown in Figure 1, we suppose that there are three insecure measurements $\{P_1,P_3,P_5\}$, only one of which can be compromised by the attacker at each level. Once the previous transmitted data is jammed, the system will be aware of it.

Here, we assume a two-level attack, in which the possible outcomes are decided by defender's two choices in order represented in rows and the attacker's two choices in columns. Then we will show how the attacker optimizes his profit in this two-level attack.

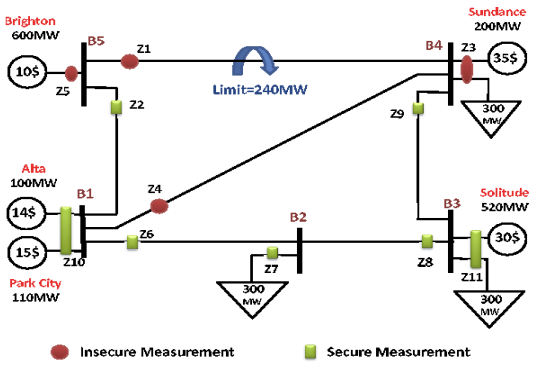

Figure 2. Example of a fig

Proc. of the Intl. Conf. on Advances In Computing, Communication and Information Technology – CCIT2014.

ISBN: 978-1-63248-010-1 doi: 10.15224/ 978-1-63248-010-1-16

TABLE III. GENERATION SHIFT FACTORS OF LINES IN 5-BUS SYSTEM

Bus / Line	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	0.651	0	0.1595
L_{4-5}	0.3685	0.2176	0.1595	0	0.4805

TABLE IV. DEFAULT VALUES OF MEASUREMENTS

Measurements	P_1	P_2	P_3	P_4	P_5	P_6
Vaule (MW)	250	340	-180	170	675	370
Measurements	P_7	P_8	P_9	P_{10}	P_{11}	
Vaule (MW)	300	-80	220	300	-300	

C. *Results of Dynamic Algorithm*

Applying the proposed algorithm, we start from the second level (the last level). The recursive procedure requires 9 single-act saddle-point solutions corresponding to the defender's 9 information sets at this level. After the integration of all mixed strategies $\hat{\gamma}_2^{1*}$ and $\hat{\gamma}_2^{2*}$, which satisfy (11), then with the optimal strategy in the second level given, we can simplify the original game into the single-act one with its terminal points. All value of $\{J_1^*, J_1^*, ..., J_9^*\}$ combined the new matrix game, so we can solve the final value $L = 6.36$. To sum up, the attacker choosing the optimal strategy $(\gamma_1^{1*}, \gamma_1^{2*}; \gamma_2^{1*}, \gamma_2^{2*})$ to jam the bus on which the electricity transmitted will be paid for average \$6.36 per unit to the attacker. Zero–Sum Dynamic Games

Figure. 3 shows how the attacker profits from two different algorithms given the same circumstance. We can find that the difference at different levels between

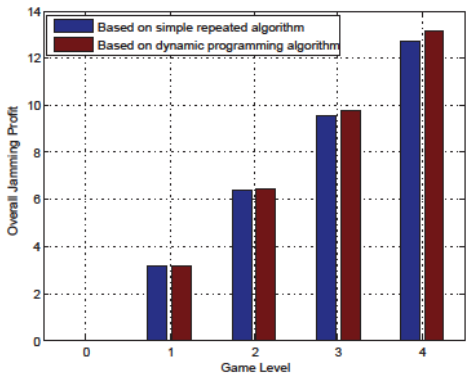

Figure 3. Dynamic Optimality between Two Algorithms.

VI. Conclusion

In this paper, we introduced the pricing mechanism and the method attackers utilize to change the congestion and the electricity price. Then we formulated the optimization problem of maximizing attacker's profit from most effective strategy choices with the context of the theory about multi-act two-person zero-sum game with extensive forms. We introduce the detailed algorithm to solve the problem step by step and give the further demonstration of its optimality. In simulation, we gave the specific example of a PJM 5-bus test system, in which we provide the detailed procedure shown in to find the saddle-point equilibrium of the game at each level, all of which altogether combine to build the final solution in a multi-act game.

References

[1] T. F. Garrity, "Getting smart," IEEE Power and Energy Magazine, vol. 6, no. 2, pp. 38–45, March–April 2008.

[2] A. Monticelli, "Electric power system state estimation," Proceedings of IEEE, vol. 88, no. 2, pp. 262–282, Feb. 2000.

[3] Y. Liu, M. K. Reiter, and P. Ning, "False data injection attacks against state estimation in electric power grids," The 16th ACM Conference on Computer and Communications Security, Chicago, IL, Nov. 2009.

[4] Y. Wang, B. Zhang, W. Lin, and T. Zhang, "Smart grid information security - a research on standards," 2011 International Conference on Advanced Power System Automation and Protection (APAP), pp. 1188–1194, Oct. 2011.

[5] E. Altman, K. Avrachenkov, and A. Garnaev, "Jamming game with incomplete information about the jammer," in Proc. of ICST/ACM International Workshop on Game Theory in Communication Networks, Pisa, Italy, Dec. 2009.

[6] H. M. Sun, S. P. Hsu, and C. M. Chen, "Mobile jamming attack and its countermeasure in wireless sensor networks," 21st International Conference on Advanced Information Networking and Applications Workshops, AINAW '07, vol. 1, pp.4 57–462, Ontario, Canada, May 2007.

[7] Z. M. Fadlullah, Y. Nozaki, A. Takeuchi, and N. Kato, "A survey of game theoretic approaches in smart grid," 2011 International Con9 ference on Wireless Communications and Signal Processing (WCSP), Sendai, Japan, Nov. 2011.

[8] Q. Zhu, Z. Han, and T. Basar, "A differential game approach to distributed demand side management in smart grid," 2012 IEEE International Conference on Communications (ICC), pp. 3345-3350, Ottawa, Canada, Jun. 2012.

[9] A. Abur and A. G. Exposito, Power System State Estimation: Theory and Implementation, Marcel Dekker, Inc., 2004.

[10] A. J. Wood and B. F. Wollenberg, Power Generation, Operation, and Control, Wiley New York et al., 1996.

[11] T. Logenthiran, D. Srinivasan, and T. Z. Shun, "Demand side management in smart grid using heuristic optimization," IEEE Transactions on Smart Grid, vol.22, no.4, pp.1244-1252, Sep. 2012.

[12] 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.

[13] H. Li, L. Lai, and R.C. Qiu, "A denial-of-service jamming game for remote state monitoring in smart grid," 2011 45th Annual Conference on Information Sciences and Systems (CISS), Baltimore, MD, Mar. 2011.

[14] ISO New England Inc., Overview of the Smart Grid: Policies, Initiatives and Needs, Feb. 17, 2009.

[15] F. Li and R. Bo "Small test systems for power system economic studies," Power and Energy Society General Meeting, Minneapolis, MN, Jul. 2010.