Bid Modification Attack in Smart Grid for Monetary Benefits

Kush Khanna, Bijaya Ketan Panigrahi
Department of Electrical Engineering
Indian Institute of Technology Delhi
New Delhi, India
kushkhanna06@gmail.com, bkpanigrahi@ee.iitd.ac.in

Anupam Joshi
Computer Science and Electrical Engineering Department
University of Maryland Baltimore County
Baltimore MD 21250, USA
joshi@umbc.edu

***Abstract*—In the quest for reliability and automation, the entire smart grid operation and control depends on the communication infrastructure. This reliance on the information and communication technologies has also opened up possibilities of cyber-intrusions. In this paper, a bid modification attack on the power exchange server is presented with the aim of gaining monetary benefits in the real-time power market. The attack is modelled for PJM 5 bus and IEEE 14 bus test system. The minimum number of load bids required to be changed for launching the attack is obtained and impacts on real time locational marginal prices (LMPs) are presented.**

***Index Terms*—Cyber security, false data injection, power systems, smart grids, state estimation.**

NOMENCLATURE

$\boldsymbol{\delta}$	Load angle vector.
$\boldsymbol{f}$	From bus vector ($n_{line} \times 1$).
$\boldsymbol{P_d}$	Load demand vector.
$\boldsymbol{P_g^*}$	Day-ahead generator dispatch vector after attack.
$\boldsymbol{P_g^+}$	Day-ahead generator dispatch vector.
$\boldsymbol{P_{ij}}$	Line flow vector ($n_{line} \times 1$).
$\boldsymbol{P_{loss}}$	Line loss vector ($n_{line} \times 1$).
$\boldsymbol{t}$	To bus vector ($n_{line} \times 1$).
ΔP_{dm}	Change in the load measurement of m^{th} bus.
$\lambda, \upsilon^+, \upsilon^+, \mu^-, \mu^+$	Lagrange multipliers.
$C_{gi}(P_{gi})$	Cost of generator on i^{th} bus.
L_m	$L_m = 1$ indicating $\Delta P_{dm} \neq 0$.
n_{line}	Number of lines in the network.
NB	Set of all the buses in the network.
ND	Set of all the buses where load is connected.
NG	Set of generator buses.
$P_{gi}^{min}/P_{gi}^{max}$	Min/Max generation limit of the generator at ith bus.
P_{max}^l	Line flow limit of lth line.
r_l	Resistance of lth line.
x_l	Reactance of lth line.

I. INTRODUCTION

For quick decision making and increased automation, power grid rely heavily on communication links between Remote Terminal Units (RTUs), Intelligent Electronic Devices (IEDs) and Supervisory Control And Data Acquisition Systems/Energy Management Systems (SCADA/EMS). The communication link which carries the critical power grid information like voltage, current, load and generation data, status of circuit breaker and relays, is susceptible to cyber intrusions. Recent research in this area has exposed various vulnerabilities of the power system in the event of cyber-attack. Error injected in the meters causes incorrect estimation of power system state at control centre which further affect the operation of entire power system [1]–[3].

Major research in recent past is primarily focused on the impacts of false data injection attacks against state estimation, a tool for system operator to obtain the current snapshot of power system operation [4], [5]. The intruder on gaining supervisory access to SCADA system can launch malicious actions which may cause system wide catastrophe [6], [7]. Researchers have proposed defence techniques against false data injection attacks by protecting the critical set of measurement sensors [8]–[11]. However, an attack aiming for financial misconduct can still be launched by changing the load dispatch schedule by hacking in the power exchange server. This is presented in this paper.

In power system, transmission lines are power highways through which all the power transactions takes place. These power highways have transmission limits. System operator must ensure that power injection and withdrawal should be such that none of the operating limits get violated. Violations on transmission limit could lead to uneconomic power system operation or in worst case blackout. As the transmission lines get more congested, the constraints for scheduling the cheapest generator increases and therefore, the price difference between the congested line increases [12]. Therefore, in deregulated power system, the most challenging issue is to manage transmission line congestion.

In the competitive market environment, attacker can exploit the above mentioned vulnerabilities in the power system to create the congestion in the transmission network, thereby, increasing the price difference between the buses of the congested line. Moreover, it is worth noting that, the attacker if succeeds in creating the congestion can possibly allow the higher priced generator to be scheduled in the real-time market and thus setting up the opportunity for financial benefit to the

costlier generator.

In this paper, we present a bid modification attack by which an adversary modifies the critical day ahead seller/buyer bid information to create congestion in the transmission network. We present with case studies on PJM 5 bus and IEEE 14 bus test system, how adversary a private player in a competitive electricity market can make monetary gains in real-time market by this attack.

The rest of the paper is organised as follows, section II presents the brief overview on power flow and false data injection attacks. Attack model is explained in section III. Results and discussion are given in section IV and section V concludes the paper with future outlook.

II. Brief Overview

A. Power Flow

For analysing steady state power system operation, load flow or power flow serves as a crucial tool. The main purpose of power flow is to determine the complex voltage and complex power flow for each bus and line of the power system. The buses are classified into three categories; 1) *slack bus* or *swing bus* or *reference bus*, 2) *generator bus* or *PV bus* and 3) *load bus* or *PQ bus*. Newton-Raphson method (Newtons point form) is most widely used method of solving AC power flow problems. However, as Jacobian must be calculated for each iteration, therefore, for larger networks approximate methods like decoupled and fast-decoupled methods are used. Furthermore, more simplification can be achieved by neglecting the Q-V equations from the AC power flow to get a linear or 'DC' power flow solution [13]. Most system operators uses this approximation to obtain the generator dispatch schedule.

As resistance of the transmission line is neglected in DC power flow, the solution becomes lossless, therefore, the actual dispatch are different from those obtained from DC power flow. To overcome, this drawback, Loss Compensated DC Optimal Power Flow (LC-DCOPF) is generally used by system operator for calculating the generator dispatch [14]. The formulation of LC-DCOPF is explained in section III of the paper.

B. Electricity Market

The structure of deregulated power system is shown in the Fig. 1. The deregulation has brought many benefits to the end users as the competitive environment offers cheaper electricity, choices to the customers and better customer service. The independent system operator is responsible for security, control and operation of power system. For secure and reliable operation of grid, the system operator determines day-ahead and real-time generator and load dispatch schedules from the bids obtained from the market operator or retailer [15].

In a decentralised market, generators and loads submit bids to buy or sell electricity to market operator. Market operator matches the seller and buyer bids to obtain the dispatch schedules which are confirmed by the system operator, who runs security analysis. Once confirmed by the system operator, market operator sends the schedules to market participants (sellers and buyers).

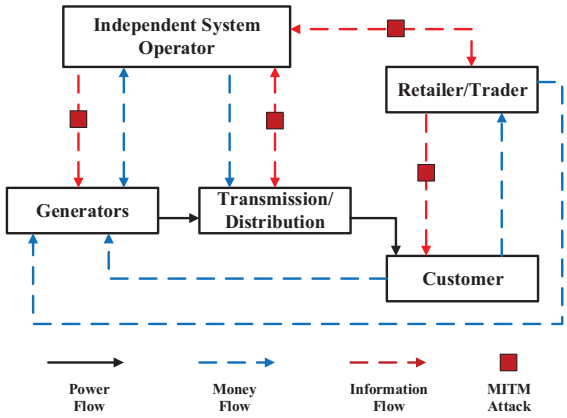

Fig. 1. Structure of deregulated power system.

An adversary can launch a man in the middle (MITM) attack by hacking the communication medium carrying critical bid information of seller and buyer as shown in Fig. 1. Once this information is obtained, the attacker can model an attack by modifying the day-ahead load schedules to gain economic benefit in real time which will be explained in section III.

III. Attack Model

Loss compensated DC optimal power flow equations are considered to model the attack as LC-DCOPF gives the generator dispatch very close to AC optimal power flow (ACOPF) with lesser computational complexity.

The LC-DCOPF is modelled as an optimization problem given in (1), subjected to (2)-(8).

$$\{\boldsymbol{P_g^+}, \boldsymbol{\delta}\} = arg\{\min_{\boldsymbol{P_g}, \boldsymbol{\delta}}\{\sum_{i=1}^{NG} C_{gi}(P_{gi})\}\} \tag{1}$$

The objective function minimizes the total cost of the generation as given in (1). $\boldsymbol{P_g}$ and $\boldsymbol{\delta}$ are variables of the problem.

$$[\lambda_i]: \quad P_{gi} - P_{di} = \sum_{\forall f(l)=i} P_{ij}^l - \sum_{\forall t(l)=i} P_{ij}^l + \sum_{\forall f(l)=i} P_{loss}^l \quad \forall i \in NB \tag{2}$$

$$[\mu_l^+]: \quad P_{ij}^l + P_{loss}^l \leq P_{max}^l \quad \forall P_{ij}^l > 0 \tag{3}$$

$$[\mu_l^-]: \quad -P_{max}^l \leq P_{ij}^l - P_{loss}^l \quad \forall P_{ij}^l < 0 \tag{4}$$

$$[\upsilon_i^-, \upsilon_i^+]: \quad P_{gi}^{min} \leq P_{gi} \leq P_{gi}^{max} \quad \forall i \in NG \tag{5}$$

$$-\pi \leq \delta_i \leq \pi \quad \forall i \in NB \tag{6}$$

Equation (2) represents the nodal power balance equation. Lagrange multiplier (λ_i) corresponding to the nodal power balance equation gives the LMP of the bus i. Transmission line limits are modelled using (3) and (4). Unlike DC-OPF, here line losses are added to the line flows obtained from (7). Line losses are calculated from (8).

$$P_{ij}^{l} = (\delta_{f(l)} - \delta_{t(l)})/x_l \tag{7}$$

$$P_{loss}^{l} = r_l * (P_{ij}^{l})^2 \tag{8}$$

The day-ahead dispatch are obtained after solving the problem (1). To create congestion in kth line, the minimum number of changed load schedules are obtained by solving the bi-level optimization problem (9). Here **P1** is the outer level problem subjected to (10)-(13).

$$\textbf{P1} \quad \{\boldsymbol{\Delta P_d}\} = arg \min_{\boldsymbol{\Delta P_d}} \{\sum_{m=1}^{ND} L_m\} \tag{9}$$

$$L_m = \begin{cases} 1 & \Delta P_{dm} \neq 0, \\ 0 & \Delta P_{dm} = 0 \end{cases} \quad \forall m \in ND \tag{10}$$

$$-\epsilon P_{di} \leq \Delta P_{di} \leq \epsilon P_{di} \quad \forall i \in ND \tag{11}$$

$$\boldsymbol{P_g^*} = \boldsymbol{P_g^+} \tag{12}$$

$$|(\delta_{f(l)}^{*} - \delta_{t(l)}^{*})/x_l| = P_{max}^{k} \tag{13}$$

The changes in the day-ahead load schedule is limited by ϵ in (11). Equation (12) ensures day-ahead generator dispatch and dispach after attack remains same. Constraint (13) ensures that the targeted kth line is congested.

The inner level problem is denoted by **P2**, subjected to (3)-(8) and (15).

$$\textbf{P2} \quad \{\boldsymbol{P_g^*}, \boldsymbol{\delta^*}\} = arg\{\min_{\boldsymbol{P_g}, \boldsymbol{\delta}} \{\sum_{i=1}^{NG} C_{gi}(P_{gi})\}\} \tag{14}$$

$$P_{gi} - P_{di} - \Delta P_{di} = \sum_{\forall f(l)=i} P_{ij}^{l} - \sum_{\forall t(l)=i} P_{ij}^{l} + \sum_{\forall f(l)=i} P_{loss}^{l} \quad \forall i \in NB \tag{15}$$

Once $\boldsymbol{\Delta P_d}$ (change in the day-ahead load schedule) is obtained the real-time generator dispatch can be calculated by considering real-time load schedules (5% increase in the load for certain specified buses in this study) for solving the problem (1). The real-time LMP is again given by Lagrange multiplier λ_i for the nodal power balance equation by considering real-time load schedule.

IV. Results and Discussion

The attack is modelled as an optimization problem and is tested for PJM 5-bus and IEEE 14-bus system. The minimum load required to be changed for launching the attack are obtained for bot test systems. The line data and generator cost data for both PJM and IEEE test system is given in Appendix. Maximum change in the day-ahead load ϵ is limited to 15% for this study. Generator real time prices and day-ahead prices are assumed to be same.

A. PJM 5-Bus System

PJM 5 bus system is shown in Fig. 2. The day-ahead generator dispatch schedule is shown in Table IV-A. The minimum day-ahead load changes required to create congestion in line 2-3 are three. The attacked day-ahead load schedules are shown in Table II. Five percent increase in the load of bus 3 and bus

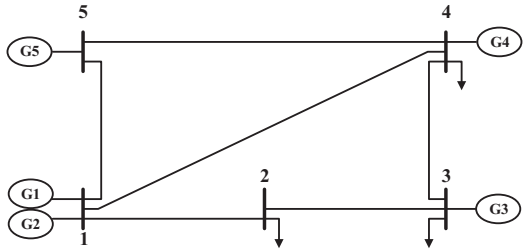

Fig. 2. PJM 5 bus system

4 is considered in the real-time. Locational marginal prices for PJM 5-bus system is shown in Fig. 3. LMPs after attack is significantly higher when compared to day-ahead LMP without attack and real-time LMP considering five increase in above mentioned loads. Table III shows real-time line flows

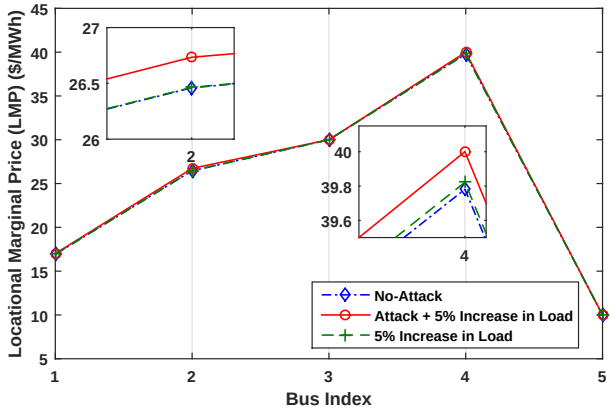

Fig. 3. Locational Marginal Price for PJM 5 bus system

for five percent increase in the load at bus 3 and bus 4 with and without attack. The real time generator dispatch with and without the attack is also given in Table IV-A. Without attack, generator at bus 4 is not scheduled in the real-time market, however, if the attack on the day ahead bidding information is

considered then the generator is scheduled for 20 MW is real-time. The results reveals that for carrying out such attack, the adversary must be able to modify the day-ahead load schedule for loads at buses 2,3 and 4.

TABLE I
DISPATCH SCHEDULE FOR PJM 5 BUS SYSTEM

Gen. Bus	Day-Ahead Schedule (MW)	Real-Time Schedule (MW)	Real-Time Schedule (Attack) (MW)
1	40	40	40
1	170	170	170
3	332.38	377.27	347.39
4	0	0	20
5	462.41	452.36	462.41

TABLE II
DAY-AHEAD LOADS FOR PJM 5 BUS SYSTEM

Bus	Day-Ahead Load (MW)	Day-Ahead Load (Attack) (MW)	Change (MW)
1	0	0	0
2	300	315.28	15.28
3	300	279.14	-20.86
4	400	405.56	5.56
5	0	0	0

TABLE III
LINE FLOWS FOR PJM 5 BUS SYSTEM

Line	Day-Ahead Flows (MW)	Day-Ahead Flows (Attack) (MW)	Real-Time Flows (MW)	Real-Time Flows (Attack) (MW)
1-2	247.08	247.08	234.92	247.08
1-4	186.70	186.70	188.83	186.70
1-5	-224.42	-224.42	-214.34	-224.42
2-3	-54.68	-70	-66.71	-70
3-4	-22.29	-16.72	-4.39	-16.72
4-5	-240	-240	-240	-240

B. IEEE 14-Bus System

IEEE 14-bus system is shown in Fig. 4. The minimum number of changes in day-ahead load schedule required to launch the attack by congesting line 9-10 are three, i.e., at 9th, 10th and 11th bus as shown in Table IV. Day-ahead and real-time LMPs for IEEE 14 bus system with and without considering day-ahead load modification attack is shown in Fig. 5.

For calculating the real-time dispatch, loads at the buses 10, 11, 12, 13 and 14 are assumed to be increased by five percent. Congestion in the line 9-10 causes significant change in real-time LMPs for buses 10, 11 and 12 as shown in Fig 5. Line flows before and after the attack is shown in Table V. The results reveals that congestion in line 9-10 causes the change in the real-time generator dispatch before and after the attack.

As shown in Table IV, generator connected at bus 6 can get financial benefit from the attack as the real-time dispatch after modified day-ahead loading schedule at bus 6 is higher as compared to the dispatch schedule without considering attack.

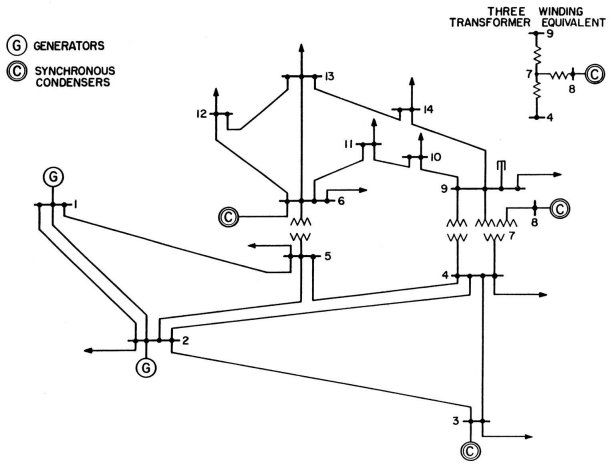

Fig. 4. IEEE 14 bus system

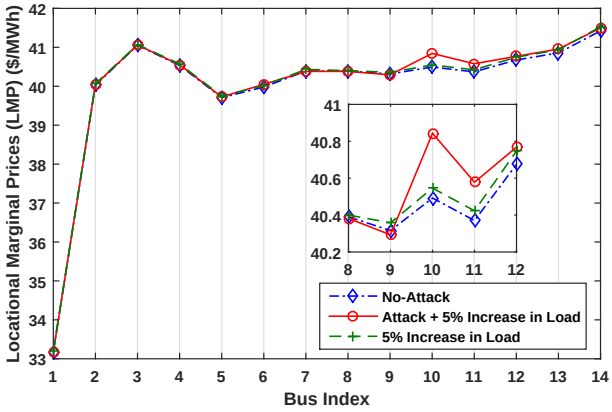

Fig. 5. Locational Marginal Price for IEEE 14 bus system

TABLE IV
GENERATOR AND LOAD DISPATCH FOR IEEE 14 BUS SYSTEM

Bus	No-Attack			Attack	
	Day-Ahead Dispatch (MW)	Day-Ahead Load (MW)	Real-Time Dispatch (MW)	Day-Ahead Load (MW)	Real-Time Dispatch (MW)
1	153.14	0	153.32	0	153.17
2	40.06	21.70	40.13	21.70	40.09
3	52.61	94.20	53.46	94.20	53.00
4	-	47.80	-	47.80	-
5	-	7.60	-	7.60	-
6	0	11.20	0.844	11.20	2.40
7	-	0	-	0	-
8	19.53	0	20.00	0	19.08
9	-	29.50	-	28.63	-
10	-	9.00	-	10.24	-
11	-	3.50	-	3.12	-
12	-	6.10	-	6.10	-
13	-	13.50	-	13.50	-
14	-	14.90	-	14.90	-

TABLE V
LINE FLOWS FOR IEEE 14 BUS SYSTEM

Line	Day-Ahead Flows (MW)	Day-Ahead Flows (Attack) (MW)	Real-Time Flows (MW)	Real-Time Flows (Attack) (MW)
1-2	100.00	100.00	100.00	100.00
1-5	53.14	53.14	53.32	53.17
2-3	40.03	40.02	39.70	39.90
2-4	42.92	42.92	43.10	43.05
2-5	33.54	33.53	33.76	33.58
3-4	-2.30	-2.29	-1.75	-2.03
4-5	-39.72	-39.72	-39.57	-40.09
4-7	17.32	17.31	17.61	17.85
4-9	13.80	13.80	14.06	14.02
5-6	37.50	37.50	38.03	37.21
6-11	3.40	3.40	3.61	4.04
6-12	7.18	7.18	7.55	7.62
6-13	15.71	15.71	16.52	16.75
7-8	-19.53	-19.53	-20.00	-19.09
7-9	36.85	36.85	37.61	36.94
9-10	9.13	10.00	9.56	10.00
9-14	12.02	12.02	12.62	12.32
10-11	0.10	0.27	0.08	0.73
12-13	1.02	1.02	1.08	1.14
13-14	3.07	3.07	3.24	3.53

V. CONCLUSION AND FUTURE SCOPE

In the smart grid environment, security against the cyber-threats is of utmost priority. The economy of the entire nation depends on the electric grid. A well-coordinated cyber-attack can cause system wide failure. In this paper we have presented an attack on power exchange server, by modifying day-ahead load schedules intelligently, an adversary, also a competitive player in power market can make financial profit by getting a costlier generator scheduled in real time market. The attack model is simulated for PJM 5 bus and IEEE 14 bus test system. The paper reveals the importance of securing the smart grid against the malicious cyber-activities not only to protect grid from system wide collapse but also to alleviate financial misconducts.

APPENDIX

A. Line data

The line data for IEEE 14-bus and PJM 5-bus test system is given in Table VI and Table VII respectively. All the resistances and reactances of the lines are given in pu. The line limits are given in MW.

TABLE VI
LINE DATA FOR IEEE 14 BUS SYSTEM

Line	Resistance (pu)	Reactance (pu)	Line Limit (MW)
1-2	0.01938	0.05917	100
1-5	0.05403	0.22304	60
2-3	0.04699	0.19797	50
2-4	0.05811	0.17632	50
2-5	0.05695	0.17388	40
3-4	0.06701	0.17103	20
4-5	0.01335	0.04211	50
4-7	0	0.20912	20
4-9	0	0.55618	20
5-6	0	0.25202	40
6-11	0.09498	0.19890	10
6-12	0.12291	0.25581	10
6-13	0.06615	0.13027	20
7-8	0	0.17615	20
7-9	0	0.11001	40
9-10	0.03181	0.08450	10
9-14	0.12711	0.27038	20
10-11	0.08205	0.19207	10
12-13	0.22092	0.19988	10
13-14	0.17093	0.34802	10

TABLE VII
LINE DATA FOR PJM 5 BUS SYSTEM

Line	Resistance (pu)	Reactance (pu)	Line Limit (MW)
1-2	0.00281	0.0281	400
1-5	0.00304	0.0304	999
2-3	0.00064	0.0064	999
2-4	0.00108	0.0108	70
2-5	0.00297	0.0297	999
3-4	0.00297	0.0297	240

B. Generator Cost Data

The generator cost data for IEEE 14-bus and PJM 5-bus is given in Table VIII and Table IX respectively. a_i, b_i and c_i are quadratic linear and constant cost coefficients of ith generator respectively.

TABLE VIII
GENERATOR COST DATA FOR IEEE 14 BUS SYSTEM

Gen. Bus	a_i	b_i	c_i	PG_{min} (MW)	PG_{max} (MW)
1	0.043	20	0	0	200
2	0.25	20	0	0	140
3	0.01	40	0	0	100
6	0.01	40	0	0	100
8	0.01	40	0	0	100

TABLE IX
GENERATOR COST DATA FOR PJM 5 BUS SYSTEM

Gen. Bus	a_i	b_i	c_i	PG_{min} (MW)	PG_{max} (MW)
1	0	14	0	0	40
1	0	15	0	0	170
3	0	30	0	0	520
4	0	40	0	0	200
5	0	10	0	0	600

REFERENCES

[1] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, p. 13, 2011.

[2] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *Smart Grid, IEEE Transactions on*, vol. 2, no. 4, pp. 645–658, 2011.

[3] Z. Qin, Q. Li, and M.-C. Chuah, "Unidentifiable attacks in electric power systems," in *Proceedings of the 2012 IEEE/ACM Third International Conference on Cyber-Physical Systems*. IEEE Computer Society, 2012, pp. 193–202.

[4] A. Abur and A. G. Exposito, *Power system state estimation: theory and implementation*. CRC Press, 2004.

[5] F. C. Schweppe, "Power system static-state estimation, part i,ii,iii," *Power Apparatus and Systems, IEEE Transactions on*, no. 1, pp. 120–135, 1970.

[6] C. W. Ten, C. C. Liu, and G. Manimaran, "Vulnerability assessment of cybersecurity for scada systems," *IEEE Trans. Power Syst.*, vol. 23, no. 4, pp. 1836–1846, Nov 2008.

[7] C. C. Liu, A. Stefanov, J. Hong, and P. Panciatici, "Intruders in the grid," *IEEE Power Energy Mag.*, vol. 10, no. 1, pp. 58–66, Jan 2012.

[8] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. J. Overbye, "Detecting false data injection attacks on dc state estimation," in *Preprints of the First Workshop on Secure Control Systems, CPSWEEK*, vol. 2010, 2010.

[9] M. Talebi, C. Li, and Z. Qu, "Enhanced protection against false data injection by dynamically changing information structure of microgrids," in *Proc. IEEE 7th Sensor Array Multichannel Signal Process. Workshop (SAM)*. IEEE, 2012, pp. 393–396.

[10] S. Bi and Y. J. Zhang, "Defending mechanisms against false-data injection attacks in the power system state estimation," in *Proc. IEEE GLOBECOM Workshops (GC Wkshps)*. IEEE, 2011, pp. 1162–1167.

[11] L. Liu, M. Esmalifalak, Q. Ding, V. A. Emesih, and Z. Han, "Detecting false data injection attacks on power grid by sparse optimization," *IEEE Trans. Smart Grid*, vol. 5, no. 2, pp. 612–621, 2014.

[12] M. O. Buygi, G. Balzer, H. M. Shanechi, and M. Shahidehpour, "Market based transmission expansion planning: fuzzy risk assessment," in *Electric Utility Deregulation, Restructuring and Power Technologies, 2004. (DRPT 2004). Proceedings of the 2004 IEEE International Conference on*, vol. 2, April 2004, pp. 427–432 Vol.2.

[13] A. J. Wood and B. F. Wollenberg, *Power generation, operation, and control*. John Wiley & Sons, 2012.

[14] E. Litvinov, T. Zheng, G. Rosenwald, and P. Shamsollahi, "Marginal loss modeling in lmp calculation," *IEEE Transactions on Power Systems*, vol. 19, no. 2, pp. 880–888, May 2004.

[15] "Congestion management," indian Energy Exchange. [Online]. Available: http://www.iexindia.com/pdf/dam_appendix2.pdf