Modeling Load Redistribution Attacks in Power Systems

Yanling Yuan, Zuyi Li, *Senior Member, IEEE*, and Kui Ren, *Senior Member, IEEE*

***Abstract*—State estimation is a key element in today's power systems for reliable system operation and control. State estimation collects information from a large number of meter measurements and analyzes it in a centralized manner at the control center. Existing state estimation approaches were traditionally assumed to be able to tolerate and detect random bad measurements. They were, however, recently shown to be vulnerable to intentional false data injection attacks. This paper fully develops the concept of load redistribution (LR) attacks, a special type of false data injection attacks, and analyzes their damage to power system operation in different time steps with different attacking resource limitations. Based on damaging effect analysis, we differentiate two attacking goals from the adversary's perspective, i.e., immediate attacking goal and delayed attacking goal. For the immediate attacking goal, this paper identifies the most damaging LR attack through a max-min attacker-defender model. Then, the criterion of determining effective protection strategies is explained. The effectiveness of the proposed model is tested on a 14-bus system. To the author's best knowledge, this is the first work of its kind, which quantitatively analyzes the damage of the false data injection attacks to power system operation and security. Our analysis hence provides an in-depth insight on effective attack prevention with limited protection resource budget.**

***Index Terms*—Delayed LR attacks, effective protection strategies, false data injection attacks, immediate LR attacks, load redistribution attacks, state estimation.**

NOMENCLATURE

Indices

d	Load index.
g	Generator index.
l	Transmission line index.

Constants

c_g	Generation cost (in \$/MWh) of generator g.
cs_d	Load shedding cost (in \$/MWh) of load d.
D_d	Actual value of load d (in MW).
$\mathbf{KD}$	Bus-load incidence matrix. $\mathbf{KD}_{.d}$ is the d^{th} column of matrix $\mathbf{KD}$.
$\mathbf{KP}$	Bus-generator incidence matrix. $\mathbf{KP}_{.g}$ is the g^{th} column of matrix $\mathbf{KP}$.
M	Sufficiently large positive constant.
N_d	Number of loads.
N_g	Number of generators.
N_l	Number of transmission lines.
$P_g^{\max}, P_g^{\min}$	Maximum and minimum generation outputs (in MW) of generator g.
$PL_l^{\max}$	Capacity (in MW) of transmission line l.
R	Attacking resources.
$\mathbf{SF}$	Shifting factor matrix.
ε	Sufficiently small positive constant.
τ	Upper bound of $\Delta D_d/D_d$ for each load d.

Variables

ΔD_d	Attack on the measurement (in MW) of load d.
P_g	Generation output (in MW) of generator g.
PL_l	Power flow (in MW) of transmission line l.
ΔPL_l	Attack on the power flow measurement (in MW) of transmission line l.
S_d	Load shedding (in MW) of load d.
$\underline{\alpha}_l, \overline{\alpha}_l$	Lagrange multipliers associated with the lower and upper bounds for the power flow of line l.
$\underline{\beta}_g, \overline{\beta}_g$	Lagrange multipliers associated with the lower and upper bounds for the MW output of generator g.
$\delta_{D,d}, \delta_{D+,d}, \delta_{D-,d}$	Indicators. $\delta_{D,d} = 1$ if the measurement of load d is attacked, i.e., $\Delta D_d \neq 0$; $\delta_{D+,d} = 1$ indicating $\Delta D_d > 0$; $\delta_{D-,d} = 1$ indicating $\Delta D_d < 0$. $\delta_{D,d} = 0$ if $\Delta D_d = 0$.

Manuscript received October 15, 2010; accepted October 29, 2010. Date of publication April 21, 2011; date of current version May 25, 2011. This work was supported in part by the U.S. Department of Energy under Grant DE-FC26-08NT02875. Paper no. TSG-00175-2010.

The authors are with the Electrical and Computer Engineering Department, Illinois Institute of Technology, Chicago, IL 60616 USA (e-mail: yyuan7@iit.edu; lizu@iit.edu; kren2@iit.edu).

Digital Object Identifier 10.1109/TSG.2011.2123925

$\delta_{PL,l}, \delta_{PL+,l}, \delta_{PL-,l}$	Indicators. $\delta_{PL,l} = 1$ if the power flow measurement of line l is attacked, i.e., $\Delta PL_l \neq 0$; $\delta_{PL+,l} = 1$ indicating $\Delta PL_l > 0$; $\delta_{PL-,l} = 1$ indicating $\Delta PL_l < 0$. $\delta_{PL,l} = 0$ if $\Delta PL_l = 0$.
$\underline{\gamma}_d, \overline{\gamma}_d$	Lagrange multipliers associated with the lower and upper bounds for the load shedding of load d.
λ	Lagrange multiplier associated with the power balance equation for the system.
μ_l	Lagrange multiplier associated with the power flow equation for line l.
$\omega_{\underline{\alpha},l}, \omega_{\overline{\alpha},l}$	Additional binary variables to represent the complementary slackness conditions for the power flow constraints of line l.
$\omega_{\underline{\beta},g}, \omega_{\overline{\beta},g}$	Additional binary variables to represent the complementary slackness conditions for the generation output constraints of generator g.
$\omega_{\underline{\gamma},d}, \omega_{\overline{\gamma},d}$	Additional binary variables to represent the complementary slackness conditions for the load shedding constraints of load d.

Note that a variable in bold without index represents the vector form of that variable.

I. Introduction

ELECTRIC power systems, as the driving force of the modern society, are critical to any country's economy and security. The physical vulnerability of electric power systems to natural disasters and sabotage has long been recognized [1]. Recent works have addressed the vulnerability analysis of the power systems under physical terrorist attacks [2]–[8]. Effective defense or protective measures are determined by identifying the critical components in power systems whose outages may cause the maximum disruption to the systems.

The development of smart grid has brought in tremendous economic benefits and advanced communication and control capabilities to the electricity industry. In the meantime, the so-called cyber-vulnerability has caused more and more concerns. Supervisory Control and Data Acquisition (SCADA) systems, which transmit measurements, status information, and circuit-breaker signals to and from remote terminal units (RTUs), are susceptible to cyber-security attacks due to their reliance on communication and network technologies. It was shown recently that an attacker could corrupt the measurement data that SCADA systems collect through RTUs, heterogeneous communication networks, or control center office LANs [9]. As the information source of the control center, SCADA systems, once being attacked, may affect the outcome of state estimation and further mislead the operation and control functions of energy management system (EMS), possibly resulting in catastrophic consequences. False data injection attacks [10], one type of cyber attacks against state estimation through SCADA systems, are getting more attention as the smart grid develops. They cooperatively manipulate the measurements taken at several meters, and thus distort the outcome of the state estimation. A key observation in [10] is that a false data injection attack vector $\boldsymbol{a}$ is totally undetectable if it is a linear combination of the column vectors of the Jacobin matrix $\mathbf{H}$, which is determined by the power network configuration. This injected attack can successfully bypass bad data detection since it does not affect the measurement residual $\mathbf{r}$ while the existing bad data detection techniques are all based on the measurement residual. False data injection attacks can be easily constructed if an attacker gains access to the $\mathbf{H}$ matrix. Furthermore, they can manipulate the state estimation outcome in an arbitrary and predicted way, and potentially cause serious consequences. It is thus critical to protect the power systems from false data injection attacks.

In fact, it has long been known in the power systems community that certain errors are undetectable by residual analysis [11], [12]. This can be viewed as a fundamental limitation on the ability of the state estimation to handle cooperative attacks. Some work has been done to limit the effect of false data injection attacks on power system state estimation. Reference [13] introduced a Bayesian framework, which was based on the belief that power system state usually changes from one to the next gradually unless a contingency has occurred. With some prior information on the actual state, the damage of false data injection attacks was effectively limited from infinity to some finite range. A new L_∞ norm detector was then introduced instead of the more standard L_2 norm based detectors by taking advantage of the inherent sparsity of the attack vector. However, the actual state of the system is usually hard to predict since a power system could undergo rapid load changes even without the occurrence of a contingency. Also, as shown in [13], under the most damaging false data injection attack, the error of state estimation can still jump to a level that may be high enough to endanger the reliable operation of power systems. Some other work focused on the protection strategy to false data injection attacks. Reference [9] introduced two security indices for each measurement: attack vector sparsity and attack vector magnitude. The security indices of a measurement evaluate how many and by how much other measurements need to be corrupted in coordination with this measurement to avoid the triggering of alarms. It was shown that larger measurement redundancy seems to give higher security in terms of attack vector magnitude. Unfortunately, no relationship exists between redundancy and security in terms of attack vector sparsity. Moreover, [9] intended to establish protection strategy on measurements with low security indices. However, this strategy can only protect the system from those attacks that need less effort to implement.

It is well known that state estimation is used to make the best estimate on the state of the power systems in system monitoring. Based on the estimated state, security-constrained economic dispatch (SCED) then intends to minimize the total system operation cost through the redispatch of generation output. If the estimated state is contaminated by false data injection attacks, a false SCED solution may lead the system to an uneconomic operating state that could be accompanied with

immediate load shedding, or even to an insecure operating state that could cause wider load shedding in a delayed time without immediate corrective actions. This paper thoroughly studies the damaging effect of load redistribution attacks on power system operation and control, which is economically quantified based on the system operation cost from the result of a false SCED. For simplicity, SCED in this paper only considers base case power network constraints, and the operation cost only includes generation cost and load shedding cost. In this paper, the most damaging attack is identified under posited attacking resources. Effective protection strategies are designed and deployed to mitigate the damaging effect of load redistribution attacks.

The contributions of this paper are summarized as follows.

1) This paper defines a special type of false data injection attacks—load redistribution attacks (LR attacks), in which only load bus injection measurements and line power flow measurements are attackable. LR attacks are realistic false data injection attacks with limited access to specific meters.
2) This paper analyzes the damaging effects of LR attacks. Since LR attacks can successfully bypass bad data detection and manipulate the state estimation outcome, SCED based on the false estimated state would lead the system into a false secure and optimal operating state. The damage of LR attacks is described in two time steps. Accordingly, this paper differentiates two different attacking goals from the adversary's perspective, i.e., immediate attacking goal and delayed attacking goal.
3) This paper proposes a bilevel model in order to identify the most damaging LR attack with immediate attacking goal. The goal of the attack is to maximize the system operation cost under the logical assumption that the control center will implement feasible corrective actions to minimize the operation cost based on the false state estimation.
4) This paper describes the theory and criterion of protecting the system from the damage of a specific LR attack considering the existence of stochastic measurement error. With this protection criterion, effective protection strategies can then be designed to defeat the attacker's attempt.

The remainder of this paper is organized as follows. Section II introduces LR attacks and analyzes their damages to power system operation through a simple 2-bus system example. Section III presents the bilevel formulation for LR attacks with immediate attacking goal and describes the proposed solution algorithm. Section IV introduces the criterion of effective protection strategies for a specific LR attack. Section V presents and analyzes the numerical results from two case studies. Section VI draws relevant conclusions and presents future work. In the Appendix, the derivation of the effective protection criterion is explained in detail.

II. Load Redistribution Attacks

In practical power systems, the attack on some measurements will easily expose itself and the attacked measurements will be denied as effective data for state estimation. Considering the practical situations in power system state estimation, we make a few assumptions in this paper: 1) Generator output measurements cannot be attacked, since the attack can be easily detected and corrected through the direct communication between control center and power plant control room. 2) The bus injection measurement of zero injection buses in the network cannot be attacked. Zero injection buses are those having neither generation nor load connected. In state estimation, zero injection may be interpreted as an exact measurement of the bus injection power. 3) Load measurements are attackable. In power systems, loads are constantly changing and load meters are widely distributed. However, since short-term load forecasting provides an approximate estimation of the load, attack that causes load measurements to deviate far from their true values will be under suspicion. In this paper, we suppose that the attack magnitude for a load measurement does not exceed $\tau = 50\%$ of its true load value. Note that τ value is a constant preset by the control center based on historical data. In smart grid environment, τ may be varying for different types of load. 4) Power flow measurement for transmission lines can be attacked without being suspected. With the above assumptions, the effect of false data injection attacks is actually load redistribution, i.e., increasing load at some buses and reducing loads at other buses while maintaining the total load unchanged. Only load bus power injection measurements and line power flow measurements are attackable in LR attacks.

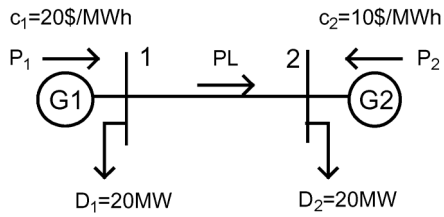

Fig. 1. Two-bus system.

As a special case of false data injection attacks, LR attacks can mislead the state estimation process without being detected by any of the existing techniques for bad data detection. False SCED solution may harm power system operation in two time steps. First, it may lead the system into a nonoptimal generation dispatch; load shedding, which is originally unnecessary, may happen at the worst case. Second, it may lead the system into an insecure operating state, i.e., power flows on some transmission lines may actually exceed their capacities. Without immediate corrective actions, the outage of these overloaded lines will cause wider load shedding in a delayed time.

The damaging effect of LR attacks can be clearly seen from a simple 2-bus system example shown in Fig. 1. Bus 1 is chosen as the reference bus. Generator output limits are: $0 \leq P_1 \leq 18$ MW, $0 \leq P_2 \leq 30$ MW. Transmission line capacity limit is $|PL| \leq 5$ MW. Load-shedding cost is $cs = 40\$/\text{MWh}$. Assume that the original system state is: $P_1 = 18$ MW, $P_2 = 22$ MW, $PL = -2$ MW. Without attack, SCED should originally lead the system to the optimal state: $P_1' = 15$ MW, $P_2' = 25$ MW, $PL' = -5$ MW. There should be no load shedding in the system and the total generation cost is $C' = 550\$/\text{h}$.

In LR attacks, line power flow measurements should be manipulated cooperatively with load measurements according to

$$\Delta\mathbf{PL} = -\mathbf{SF} \cdot \mathbf{KD} \cdot \Delta\mathbf{D}. \tag{1}$$

TABLE I
IMMEDIATE DAMAGING EFFECT TO A 2-BUS SYSTEM
(POWER QUANTITIES IN MW, COST QUANTITIES IN $/h)

attack case		1	2	3	4	5	6
LR attack	ΔD_1	2	4	6	8	10	-10
	ΔD_2	-2	-4	-6	-8	-10	10
	ΔPL	-2	-4	-6	-8	-10	10
false state estimation	$D_{f,1}$	22	24	26	28	30	10
	$D_{f,2}$	18	16	14	12	10	30
	PL_f	-4	-6	-8	-10	-12	8
false SCED results	$P'_{f,1}$	17	18	18	18	18	10
	$P'_{f,2}$	23	21	19	17	15	30
	PL'_f	-5	-5	-5	-5	-5	0
	$S'_{f,1}$	0	1	3	5	7	0
	$S'_{f,2}$	0	0	0	0	0	0
	C'_f	570	610	670	730	790	500
actual	PL'_t	-3	-1	1	3	5	-10

In this 2-bus system,

$$\mathbf{SF} = [0 \quad -1],\ \mathbf{KD} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},\ \Delta PL = -[0 \quad -1] \cdot \begin{bmatrix} \Delta D_1 \\ \Delta D_2 \end{bmatrix}.$$

Assume that an LR attack with ΔD_1, ΔD_2, and ΔPL manipulates the estimation of the system state to $D_{f,1}$, $D_{f,2}$, and PL_f. The control center implements SCED based on the false state estimation and directs the system into a false optimal state $P'_{f,1}$, $P'_{f,2}$, and PL'_f, with possible load shedding $S'_{f,1}$ and $S'_{f,2}$ and total operation cost C'_f (generation cost + load shedding cost). However, the actual power flow is PL'_t instead PL'_f. The immediate damaging effect of six different LR attacks is shown in Table I.

In attack case 1, the false SCED leads the system into a nonoptimal generation dispatch with an operation cost of 570$/h, which is 20$/h higher than that of the original case. In this case, there is no load shedding after the implementation of SCED solution. The false state estimation for line power flow ($PL_f = -4$ MW) is well within the line capacity limit. For attack case 2, the attack magnitude increases to 20% of the original load. The falsely estimated line power flow ($PL_f = -6$ MW) exceeds its capacity limit. In order to maintain a secure operation, SCED based on the false state estimation ($D_{f,1} = 24$ MW, $D_{f,2} = 16$ MW) leads the system to a false optimal operating state with a total operation cost of 610$/h and 1 MW load shedding on bus 1. As the attack magnitude increases gradually up to 50% of the original load in cases 3–5, load shedding and operation cost increase accordingly. For the above cases, we observe that in order to mislead the control center to shed load immediately, two conditions must be satisfied for an LR attack: 1) attack magnitude is big enough; 2) the falsely estimated power flow exceeds its corresponding transmission capacity limit. Note that even if load shedding does not happen after the attack, the false SCED may still result in a nonoptimal dispatch and a false power flow, as shown in case 1. The damaging effect is realized immediately after the enforcement of SCED decision for attack cases 1–5.

For attack case 6, false state estimation ($D_{f,1} = 10$ MW, $D_{f,2} = 30$ MW) leads to a false generation dispatch ($P'_{f,1} = 10$ MW, $P'_{f,2} = 30$ MW). The control center presumes that the line power flow is $PL'_f = 0$ after the implementation of the false generation dispatch. However, since the actual system load is $D_1 = 20$ MW, $D_2 = 20$ MW, the false generation dispatch actually leads the power flow to $PL'_t = -10$ MW, which is overloaded. However, control center will not be aware of this security problem until the next measurement collection. Without timely corrective actions, the overloaded line will trip in a delayed time. A new cycle of measurement collection, state estimation, and SCED processes will be initiated by this system topology change, and this 2-bus system will be operated in a steady state $P''_1 = 18$ MW, $P''_2 = 20$ MW with 2 MW load shedding on bus 1. This attack case illustrates the potential threat of LR attacks to system operation security. In practical power systems, line outages may lead to wide load shedding. This effect is equivalent to an indirect physical terrorist attack to transmission lines; the difference is that the damage of LR attacks is exposed in a delayed time after the enforcement of the false SCED results. It is worth mentioning that for the attack case in which the operation cost of the false SCED is lower than that of the original SCED, there must be line/lines operating out of its/their security range, since only relaxation on the transmission line capacity could render a lower operation cost. As shown in Table I, attack case 6 indeed has a lower operation cost 500$/h as a false SCED solution. Note that if the system has enough transmission capacity, there may be no overload in the actual line power flow.

From the above example, we observe that LR attacks may destroy the functioning of SCED and leave the system out of control, even result in security risk. Since the introduction of deregulation [14], increased levels of consumption and lack of investment on transmission system upgrade are driving the operation of power systems close to their static and dynamic limits, so power systems are becoming increasingly vulnerable to LR attacks.

To protect the system from the LR attacks under limited protection resources, the control center has to first identify the most damaging attack. Since the damaging effects can be achieved in two time steps, this paper differentiates two attacking goals, i.e., immediate attacking goal and delayed attacking goal. Immediate LR attacks aim to maximize the operation cost immediately after the attacks; delayed LR attacks aim to maximize the total operation cost after the outage of overloaded lines, which is a delayed effect of LR attacks. This paper focuses on the modeling of the immediate LR attack problem.

III. BILEVEL MODEL OF THE LOAD REDISTRIBUTION ATTACK

The goal of immediate LR attacks is to maximize the system operation cost subject to attacking resource limitation, under the logical assumption that the control center will implement effective corrective actions to minimize the operation cost based on the false state estimation outcome. A bilevel model shown in Fig. 2 is proposed to identify the most damaging attack given posited attacking resources. The upper level represents the attacker and determines the attack vector to be injected into original meter measurements in order to maximize the operation cost of the system. The system operator in the lower level problem optimally reacts to the false state estimation that has been successfully manipulated by the attack vector determined

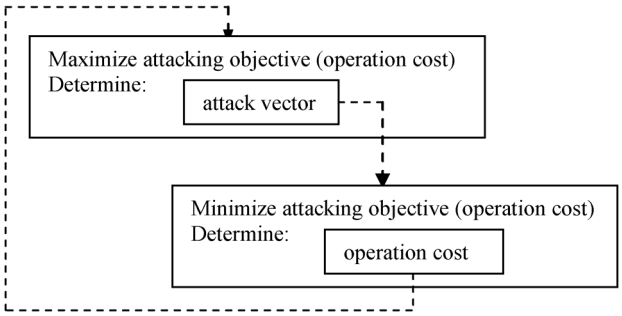

Fig. 2. Bilevel model for immediate attacking goal.

in the upper level. In this paper, this reaction only includes generation redispatch and load shedding, although the start-up of fast-response generators or the switching of transmission lines could also be effective corrective actions.

As in most vulnerability analysis of the power systems under physical terrorist attacks, we use dc load flow model to characterize the behavior of the network. The mathematical modeling of immediate LR attacks is shown below. The attacker is represented by the upper-level problem (2)–(8). The attacker maximizes the system operation cost, which includes generation cost and load shedding cost as shown in (2), considering a set of attack constraints (3)–(8). Constraints (3)–(5) ensure that the attack is an LR attack and the attack magnitude for a load measurement does not exceed a limit defined by τ and its true value in order not to be suspected. Constraints (6) and (7) model the logic relationships between the attack vector and the resource it uses for each attackable measurements. Constraint (8) guarantees that the attack satisfies attack resource limitation. Suppose that the system is fully measured, i.e., the power injections at all buses and the power flows of all lines on both directions are measured. Accordingly, to attack the power flow measurement of one line, the attacker needs to manipulate two meters. The system operator is represented by an SCED model in the lower-level problem (9)–(14), which is parameterized in terms of the upper-level decision variables $\Delta\mathbf{D}$. The system operator minimizes system operation cost (9), considering the SCED constraints (10)–(14). Note that only constraints under base case are considered.

$$\max_{\Delta\mathbf{D}} \sum_{g=1}^{N_g} c_g P_g^* + \sum_{d=1}^{N_d} cs_d S_d^* \tag{2}$$

$$\text{s.t.} \quad \sum_{d=1}^{N_d} \Delta D_d = 0 \tag{3}$$

$$\Delta\mathbf{PL} = -\mathbf{SF}\cdot\mathbf{KD}\cdot\Delta\mathbf{D} \tag{4}$$

$$-\tau D_d \le \Delta D_d \le \tau D_d \qquad \forall d \tag{5}$$

$$\Delta D_d = 0 \Leftrightarrow \delta_{D,d} = 0 \qquad \forall d \tag{6}$$

$$\Delta PL_l = 0 \Leftrightarrow \delta_{PL,l} = 0 \qquad \forall l \tag{7}$$

$$\sum_{d=1}^{N_d} \delta_{D,d} + 2\sum_{l=1}^{N_l} \delta_{PL,l} \le R \tag{8}$$

$$\{\mathbf{P}^*, \mathbf{S}^*\} = \arg\left\{ \min_{\mathbf{P},\mathbf{S}} \sum_{g=1}^{N_g} c_g P_g + \sum_{d=1}^{N_d} cs_d S_d \right\} \tag{9}$$

$$\text{s.t.} \quad \sum_{g=1}^{N_g} P_g = \sum_{d=1}^{N_d} (D_d - S_d) \qquad (\lambda) \tag{10}$$

$$\mathbf{PL} = \mathbf{SF}\cdot\mathbf{KP}\cdot\mathbf{P} - \mathbf{SF}\cdot\mathbf{KD} \cdot(\mathbf{D} + \Delta\mathbf{D} - \mathbf{S}) \qquad (\boldsymbol{\mu}) \tag{11}$$

$$-PL_l^{\max} \le PL_l \le PL_l^{\max} \qquad \forall l \quad (\underline{\alpha}_l, \overline{\alpha}_l) \tag{12}$$

$$P_g^{\min} \le P_g \le P_g^{\max} \qquad \forall g \quad (\underline{\beta}_g, \overline{\beta}_g) \tag{13}$$

$$0 \le S_d \le D_d + \Delta D_d \qquad \forall d \quad (\underline{\gamma}_d, \overline{\gamma}_d). \tag{14}$$

The logical constraints (6) can be modeled in mixed integer linear form (6a) by introducing additional binary variables. Constraint (7) can be similarly transformed to (7a).

$$\begin{cases} \Delta D_d + \tau D_d \delta_{D,d} \ge 0 \\ \Delta D_d - \tau D_d \delta_{D,d} \le 0 \\ \delta_{D+,d} + \delta_{D-,d} - 2\delta_{D,d} \le 0 \\ \Delta D_d + (-\tau D_d - \varepsilon)\delta_{D+,d} \ge -\tau D_d \\ \Delta D_d + (\tau D_d + \varepsilon)\delta_{D-,d} \le \tau D_d \\ \delta_{D+,d} + \delta_{D-,d} + \delta_{D,d} \le 2 \\ \delta_{D+,d} + \delta_{D-,d} - \delta_{D,d} \ge 0 \\ \delta_{D+,d}, \delta_{D-,d}, \delta_{D,d} \in \{0,1\} \end{cases} \qquad \forall d \tag{6a}$$

$$\begin{cases} \Delta PL_l + M\delta_{PL,l} \ge 0 \\ \Delta PL_l - M\delta_{PL,l} \le 0 \\ \delta_{PL+,l} + \delta_{PL-,l} - 2\delta_{PL,l} \le 0 \\ \Delta PL_l + (-M - \varepsilon)\delta_{PL+,l} \ge -M \\ \Delta PL_l + (M + \varepsilon)\delta_{PL-,l} \le M \\ \delta_{PL+,l} + \delta_{PL-,l} + \delta_{PL,l} \le 2 \\ \delta_{PL+,l} + \delta_{PL-,l} - \delta_{PL,l} \ge 0 \\ \delta_{PL+,l}, \delta_{PL-,l}, \delta_{PL,l} \in \{0,1\} \end{cases} \qquad \forall l. \tag{7a}$$

Given the upper-level attack vector, which is determined by $\Delta\mathbf{D}$, the lower-level optimization problem (9)–(14) is linear and convex. Similar to [3] and [15], this bilevel model can be transformed into an equivalent single-level mixed-integer program by replacing the lower-level optimization problem with its Karush-Kuhn-Tucker (KKT) optimality conditions. KKT optimality conditions were used in [16] and [17] to deduce the sensitivity functions in order to solve the bilevel bidding problems for FTR and GENCOs in power market. As illustrated in [8], KKT-based method is computationally inefficient due to the handling of the linearization expressions of the nonlinear complementary slackness conditions proposed by Fortuny-Amat and McCarl [18]. A duality-based approach proposed in [4] proved to be more efficient in vulnerability analysis of the power system under physical terrorist attacks. However, it is not suitable in our model of LR attacks. Since the lower-level problem is based on the value of the upper-level continuous variables $\Delta\mathbf{D}$, a multiplication of these continuous variables and dual variables will appear in the strong duality equality, which cannot be modeled in mixed-integer linear form. Artificial intelligence methods, such as particle swarm optimization [19], generic algorithm and coevolutionary algorithm [20] were also employed to solve bilevel problems. However, those methods are not suitable for large systems due to their deficiency in search efficiency and convergence. So, in this paper, we adopt the KKT-based method despite its computational complexity. Other methods like Benders Decomposition are under study in order to solve large-scale real-world problems.

Using KKT-based method, the original bilevel problem (2)–(14) can be transformed into an equivalent single-level MILP model as follows. (3)–(5), (6a), (7a), and (8) are the

constraints of upper-level optimization problem. Constraints (10)–(22) are equivalent to the lower-level optimization problem. (10)–(14) are primal feasibility constraints. (15)–(22) represent the KKT necessary optimality feasibility constraints, in which constraints (19)–(22) are the linearized expression of complementary slackness conditions [18].

$$\max_{\Delta \mathbf{D}} \sum_{g=1}^{N_g} c_g P_g^* + \sum_{d=1}^{N_d} cs_d S_d^* \tag{2a}$$

$$\text{s.t.} \quad (3),(4),(5),(6a),(7a),(8)$$

$$(10)-(14)$$

$$c_g - \lambda + (\mathbf{SF}\cdot\mathbf{KP}_{\cdot g})^T\cdot\boldsymbol{\mu} - \underline{\beta}_g + \overline{\beta}_g = 0 \quad \forall g \tag{15}$$

$$-\mu_l - \underline{\alpha}_l + \overline{\alpha}_l = 0 \quad \forall l \tag{16}$$

$$cs_d - \lambda + (\mathbf{SF}\cdot\mathbf{KD}_{\cdot d})^T\cdot\boldsymbol{\mu} - \underline{\gamma}_d + \overline{\gamma}_d = 0 \quad \forall d \tag{17}$$

$$\underline{\alpha}_l, \overline{\alpha}_l, \underline{\beta}_g, \overline{\beta}_g, \underline{\gamma}_d, \overline{\gamma}_d \geq 0 \quad \forall g, \forall l, \forall d \tag{18}$$

$$\begin{cases} \underline{\alpha}_l \leq M\omega_{\underline{\alpha},l} \\ PL_l + PL_l^{\max} \leq M(1-\omega_{\underline{\alpha},l}) \\ \overline{\alpha}_l \leq M\omega_{\overline{\alpha},l} \\ PL_l^{\max} - PL_l \leq M(1-\omega_{\overline{\alpha},l}) \\ \omega_{\underline{\alpha},l} + \omega_{\overline{\alpha},l} \leq 1 \end{cases} \quad \forall l \tag{19}$$

$$\begin{cases} \underline{\beta}_g \leq M\omega_{\underline{\beta},g} \\ P_g - P_g^{\min} \leq M(1-\omega_{\underline{\beta},g}) \\ \overline{\beta}_g \leq M\omega_{\overline{\beta},g} \\ P_g^{\max} - P_g \leq M(1-\omega_{\overline{\beta},g}) \\ \omega_{\underline{\beta},g} + \omega_{\overline{\beta},g} \leq 1 \end{cases} \quad \forall g \tag{20}$$

$$\begin{cases} \underline{\gamma}_d \leq M\omega_{\underline{\gamma},d} \\ S_d \leq M(1-\omega_{\underline{\gamma},d}) \\ \overline{\gamma}_d \leq M\omega_{\overline{\gamma},d} \\ D_d + \Delta D_d - S_d \leq M(1-\omega_{\overline{\gamma},d}) \\ \omega_{\underline{\gamma},d} + \omega_{\overline{\gamma},d} \leq 1 \end{cases} \quad \forall d \tag{21}$$

$$\omega_{\underline{\alpha},l}, \omega_{\overline{\alpha},l}, \omega_{\underline{\beta},g}, \omega_{\overline{\beta},g}, \omega_{\underline{\gamma},d}, \omega_{\overline{\gamma},d} \in \{0,1\}. \tag{22}$$

IV. Effective Protection Strategy

For a specific false data injection attack, an efficient protection strategy has to first guarantee that the state estimator can detect the existence of the attack. As mentioned before, bad data injection attacks cannot be detected since they do not affect measurement residuals. Actually, a bad data injection attack can be viewed as a set of multiple interacting and conforming bad data. The reason for its success is that such a multiple interacting and conforming bad data set is complete. So, for a specific LR attack, an effective protection strategy has to satisfy two requirements:

1) Break the completeness of the multiple interacting and conforming bad data set so that measurement residuals are different from those of the original measurements. This can be achieved by protecting at least one measurement meter that is supposed to be manipulated in this LR attack.
2) With the incomplete LR attacks, the weighted sum of squared measurement residuals of the system should exceed the detection threshold so that the state estimator can detect the presence of bad data. This is a problem of which measurement meters should be protected, or which measurement meters are effective protection choices.

Considering that the protection resources are usually limited, the control center tends to protect as few meters as possible, as long as this protection strategy can effectively expose the existence of the attack.

Suppose that the measurement errors conform to normal distribution and the original measurement data can pass bad data detection. Since the errors are stochastic, whether protecting a measurement meter can expose the existence of the attack is not certain. For a specific attack vector $\boldsymbol{a}$, if its manipulation on measurement p fails, the distribution of weighted sum of squared measurement residuals $J_{a,p}$ can be studied. If the lower bound of $J_{a,p}$ under specific significance level and confidence degree exceeds the detection threshold, the attack can be detected with large probability. Protecting measurement p is then called an "effective" protection strategy. Its effectiveness is not influenced by the stochastic measurement error in the original measurement data. The theory and criterion of determining "effective" protection strategies are explained in the Appendix.

For a specific attack, once an effective protection strategy is implemented, the bad data detection will alarm the existence of this attack. Subsequently, bad data identification process can successfully identify the incomplete attack using the Combinatorial Optimization Identification (COI) method [21]. This method is based on the theory that the Euclidean norm of the multiple normalized residual corresponding to the bad data is the maximum. In the identification process, the measurement of the protected device is assumed to be a good measurement.

To sum up, an effective protection strategy can avoid the damage of a specific attack.

V. Numerical Results

This section presents two case studies based on a modified IEEE 14-bus system with generator parameters shown in Table II. Other configuration data of the test system is obtained from the MATPOWER package [22]. The system is fully measured, with $m = 54$ measurements. Measurements 1–20 are for the power flows at the "from" bus; measurements 21–40 are for the power flows at the "to" bus; measurements 41–54 are for bus power injections. $n = 13$ state variables need to be estimated. The attack magnitude for a load measurement is limited at $\tau = \pm 50\%$ of its true load value and attack resource is limited to 20 meters. Suppose that the cost of unmet demand is $cs = 100\$/\text{MWh}$.

In case 1, we assume that there are no transmission capacity constraints. For this case, SCED based on the original measurements yields an operation cost of 5180$/h with generator 1 supplying all 259 MW loads. Under any LR attack, false SCED yields the same operation cost and generation dispatch as in original SCED solution. It implies that the LR attacks in this case have no immediate damaging effect to the system. The only difference between original SCED solution and false SCED solution is line power flow. However, since transmission line capacities are assumed unlimited, the LR attacks have no delayed damaging effect on the system.

In case 2, transmission capacities are modified to simulate the scenarios in which the system is operating close to its capacity limit. Transmission capacities of line 1 is 160 MW, capacity of all other lines are 60 MW. In this case, 16 meters will be attacked in the most damaging LR attack as shown in Table III. It

TABLE II
GENERATOR PARAMETERS

Gen. bus	1	2	3	6	8
$P^{\min}$ (MW)	0	0	0	0	0
$P^{\max}$ (MW)	300	50	30	50	20
c ($/MWh)	20	30	40	50	35

TABLE III
THE MOST DAMAGING IMMEDIATE LR ATTACK FOR CASE 2

Meas. p	Meas.	Attack quantity (MW)
1 & 21	PL_{12}& PL_{21}	1.3993 & -1.3993
2 & 22	PL_{15}& PL_{51}	-1.3993 & 1.3993
3 & 23	PL_{23}& PL_{32}	16.7348 & -16.7348
4 & 24	PL_{24}& PL_{42}	-2.2301 & 2.2301
5 & 25	PL_{25}& PL_{52}	-2.2614 & 2.2614
6 & 26	PL_{34}& PL_{43}	-21.6699 & 21.6699
42	P_2^{inj}	10.8500 (50%)
43	P_3^{inj}	-38.4047 (-40.77%)
44	P_4^{inj}	23.9000 (50%)
45	P_5^{inj}	3.6547 (48.09%)

TABLE IV
COMPARISON OF FALSE AND ORIGINAL SCED FOR CASE 2

		False SCED	Original SCED
Generation dispatch on gen. bus (MW)	1	196.0757	180.4449
	2	0	44.7837
	3	30	13.7714
	6	0	0
	8	20	20
Total generation (MW)		246.0757	259
Operation cost ($/h)		7113.9	6203.3

can be seen that this attack tries to transfer load on bus 2, 4, and 5 to bus 3, which originally has the heaviest load in the system. The attack tries to create a situation in which 1) the load distribution is more focused on bus 3 than it originally is; 2) at least one transmission line is overloaded in the false state estimation, so that load shedding may be necessary to bring the flow on the overloaded line back to its secure range. It is observed that the identification of the most damaging attack depends on the original load distribution as well as the transmission capacity in each line.

Note that attacking resources have not been used up for the most damaging LR attack in this case. However, any attack on an additional load measurement or any additional attack quantity on a load measurement needs cooperative manipulations on several other line power flow measurements. For example, if an attacker tries to further worsen the load distribution by increasing attack quantity on the injection power measurement of bus 5 from 3.6547 MW (48.09%) to 3.8 MW (50%) and adjust the manipulation on bus 3 injection power measurement from -38.4047 MW (-40.77%) to -38.55 MW (-40.92%) accordingly, the attacker must manipulate almost all the line power flow meters cooperatively, which is not possible due to the attacking resource limitation.

By simulating the most damaging attack, we observe that the false SCED leads to a load shedding of 12.9243 MW on bus 3. However, there is no load shedding in the original SCED results. The comparison of the false SCED and the original SCED is shown in Table IV.

TABLE V
EFFECTIVENESS CHECK OF PROTECTION STRATEGIES UNDER THE MOST DAMAGING ATTACK

p	$J_{a,p}^{true}$	$J_{a,p}^{lower}$
1 & 21	0.7474	18.4659
2 & 22	0.8318	18.2653
3 & 23	116.6135	74.7265
4 & 24	2.1193	16.2902
5 & 25	2.1842	16.2224
6 & 26	189.8589	130.0910
42	34.1290	21.9826
43	590.0887	467.2439
44	150.0439	99.4541
45	4.0000	14.9056

TABLE VI
THE MOST DAMAGING IMMEDIATE LR ATTACKS UNDER DIFFERENT ATTACKING RESOURCE LIMITATIONS

Attacking Resources R	20	15	10	6
Attacked meas.	1,2,3,4,5,6, 21,22,23,24, 25,26,42, 43,44,45	3,4,6,7,10,23, 24,26,27, 30, 42,43, 44,45,46	3,6,23, 26, 42,43,44	--
No. of attacked meas.	16	15	7	--
Operation cost ($/h)	7113.9	6434.3	6333.7	--
Load shedding (MW)	12.9243 (on bus 3)	1.6768 (on bus 3)	0	--
Effective protection choices	3,6,23,26, 43,44	43	43	--

Apparently, the attack leads the system to a nonoptimal generation dispatch with unnecessary load shedding. The most damaging LR attack causes an immediate economic loss of $7113.9 - 6203.3 = 910.6\$/\mathrm{h}$. Note that in this case, after the implementation of the false SCED decision, the actual power flows on lines are all within capacity limits. That is, the most damaging immediate LR attack will not cause line outage in a delayed time in this case. The modeling of delayed damaging attacks is beyond the scope of this paper.

For a strategy that protects measurement p, the value of $J_{a,p}^{\mathrm{true}}$ and $J_{a,p}^{\mathrm{lower}}$ are listed in Table V. Significance level α is chosen to be 0.01 in this paper, so the detection threshold is $\chi^2_{41,0.99} = 64.9501$. Checking the effective protection criterion for each protection choice p, we conclude that the effective protection strategy of the most damaging attack is to protect one of the measurements 3,6,23,26,43,44. That is, if any one of these measurements is protected, the most damaging immediate LR attack will be detected.

Table VI shows the most damaging immediate LR attacks under different attacking resource limitations. We can see from Table VI that the immediate damage of LR attacks decreases as attacking resources decreases. We also observe that protecting measurement 43 is always an effective choice for a wide range of attacking resources. Moreover, for case 2, the least number of measurements to be attacked for a complete LR attack is 7, as shown in the fourth column of Table VI. Its attack vector actually corresponds to the third column of the matrix $\mathbf{H}$ of the IEEE 14-bus system provided in [10]. As can be seen from the matrix $\mathbf{H}$, column 8 has only 4 nonzero elements. However, the

attacks based on this column need to manipulate the meter on bus 7 (a zero-injection bus) and meter on bus 8 (a generation bus), and thus they are not legitimate LR attacks by definition.

VI. Conclusions and Future Work

This paper first defines a special type of false data injection attacks—load redistribution (LR) attacks with realistic assumptions on power system state estimation. For a specific LR attack, its damage to system operation can be quantitatively analyzed through the increased operation cost that a false SCED leads to. From the damaging effect analysis, we differentiate two attacking goals, i.e., immediate attacking goal and delayed attacking goal. Immediate LR attacks aim to maximize the total operation cost immediately after the attack; delayed LR attacks aim to maximize the total operation cost after the tripping of actually overloaded lines, which is the delayed effect of LR attacks. For the immediate attacking goal, a bilevel model is established and a KKT-based method is used to identify the most damaging attack from an attacker's perspective. Effective protection strategies are then determined so that a control center can always effectively avoid the damage of the most damaging attack.

The solution to the bilevel model may also heuristically guide the defender to prevent more than just a single most damaging attack plan. A trilevel model as [6] can be designed in the future to actively deploy limited protection resources in anticipation of an LR attack. Unlike physical attack in [6], not all the to-be-attacked measurement devices are effective protection choices for a specific attack, so the criterion of determining the effectiveness of protection choices should be incorporated in the model.

The modeling for delayed LR attacks will be more complex than that for the immediate LR attacks. It includes three steps: 1) the attacker decides an attack vector; 2) the control center performs SCED function based on the false state estimation and actually overloaded lines are identified; 3) the control center performs SCED again after the outage of the overloaded lines. A trilevel model will be needed to identify the most damaging attack for the delayed attacking goal. The solution methodology of solving this trilevel problem is now under study.

Appendix

The dc state estimation problem relates measurement vector $\mathbf{z} = (z_1, z_2, \ldots, z_m)^T$ to state vector $\mathbf{x} = (x_1, x_2, \ldots, x_n)^T$, i.e.,

$$\mathbf{z} = \mathbf{H}\mathbf{x} + \mathbf{e} \tag{A.1}$$

where m is the number of measurements and n is the number of state variables. $\mathbf{H}$ is the Jacobian matrix.

Assume that random measurement errors $\mathbf{e} = (e_1, e_2, \ldots, e_m)^T$ are normally distributed and independent with $e_i \sim N(0, \sigma_i^2)$. Then measurement residuals can be expressed as

$$\mathbf{r} = \mathbf{S}\mathbf{e} \tag{A.2}$$

where matrix $\mathbf{S}$ is called residual sensitivity matrix, representing the sensitivity of measurement residuals to the measurement errors [23]. Matrix $\mathbf{S}$ has the property $\mathbf{SH} = \mathbf{0}$. The weighted sum of squared measurement residuals based on original measurements $\mathbf{z}$ is

$$J = (\mathbf{S}\mathbf{e})^T \mathbf{W} (\mathbf{S}\mathbf{e}) \tag{A.3}$$

where matrix $\mathbf{W}$ is the inverse of the covariance matrix of the measurement errors, $\mathbf{R}_\mathbf{z}$.

Let $\mathbf{z}_a$ represent the observed measurements that has been attacked by a complete LR attack $\mathbf{a}$, i.e., $\mathbf{z}_a = \mathbf{z} + \mathbf{a}$. As a special false data injection attack, the attack can be expressed as $\mathbf{a} = \mathbf{H}\mathbf{c}$, where $\mathbf{c}$ is a nonzero $n \times 1$ vector. Thus, the measurement residuals based on $\mathbf{z}_a$ is

$$\mathbf{r}_a = \mathbf{S}(\mathbf{e} + \mathbf{a}) = \mathbf{S}\mathbf{e} + \mathbf{S}\mathbf{H}\mathbf{c} = \mathbf{S}\mathbf{e} \tag{A.4}$$

From (A.2) and (A.4), we can see that a complete LR attack will not change the measurement residuals. The weighted sum of squared measurement residuals based on $\mathbf{z}_a$ is $J_a = J$. Since the widely used bad data detection methods are all based on measurement residuals, $\mathbf{z}_a$ will bypass bad data detection as long as no bad data is detected in $\mathbf{z}$.

Suppose a nonzero element a_p in attack vector $\mathbf{a}$ cannot be successfully injected since measurement p is protected. Let $\mathbf{a}'$ denote the incomplete attack vector, which is equal to $\mathbf{a}$ except that its element p is zero. The measurement residuals based on $\mathbf{z}'_a = \mathbf{z} + \mathbf{a}'$ is

$$\mathbf{r}'_a = \mathbf{S}(\mathbf{e} + \mathbf{a}') = \mathbf{S}(\mathbf{e} + \mathbf{a} - \mathbf{a}_p) = \mathbf{S}\mathbf{e} - \mathbf{S}\mathbf{a}_p \tag{A.5}$$

where $\mathbf{a}_p$ is $m \times 1$ vector, $\mathbf{a}_p = \mathbf{a} - \mathbf{a}'$.

Assume that there is no measurement error in $\mathbf{z}$, i.e., $\mathbf{e} = \mathbf{0}$, then the weighted sum of squared measurement residuals based on $\mathbf{z}'_a$ is

$$J^{\text{true}}_{a,p} = (-\mathbf{S}\mathbf{a}_p)^T \mathbf{W} (-\mathbf{S}\mathbf{a}_p) = (\mathbf{S}\mathbf{a}_p)^T \mathbf{W} (\mathbf{S}\mathbf{a}_p). \tag{A.6}$$

If error $\mathbf{e} \neq \mathbf{0}$, the weighted sum of squared measurement residuals based on $\mathbf{z}'_a$ is

$$\begin{aligned} J_{a,p} &= {\mathbf{r}'_a}^T \mathbf{W} \mathbf{r}'_a = (\mathbf{S}\mathbf{e} - \mathbf{S}\mathbf{a}_p)^T \mathbf{W} (\mathbf{S}\mathbf{e} - \mathbf{S}\mathbf{a}_p) \\ &= J - 2(\mathbf{S}\mathbf{a}_p)^T \mathbf{W} (\mathbf{S}\mathbf{e}) + J^{\text{true}}_{a,p}. \end{aligned} \tag{A.7}$$

Since $\mathbf{e} \sim N(\mathbf{0}, \mathbf{R}_\mathbf{z})$, $(\mathbf{S}\mathbf{a}_p)^T \mathbf{W} (\mathbf{S}\mathbf{e})$ is normally distributed with

$$E\left\{ (\mathbf{S}\mathbf{a}_p)^T \mathbf{W} (\mathbf{S}\mathbf{e}) \right\} = 0 \tag{A.8}$$

$$D\left\{ (\mathbf{S}\mathbf{a}_p)^T \mathbf{W} (\mathbf{S}\mathbf{e}) \right\} = (\mathbf{S}\mathbf{a}_p)^T \mathbf{W} \mathbf{S} \mathbf{R}_\mathbf{z} \mathbf{S}^T \mathbf{W} (\mathbf{S}\mathbf{a}_p). \tag{A.9}$$

Let

$$\sigma^2_{a,p} = (\mathbf{S}\mathbf{a}_p)^T \mathbf{W} \mathbf{S} \mathbf{R}_\mathbf{z} \mathbf{S}^T \mathbf{W} (\mathbf{S}\mathbf{a}_p) \tag{A.10}$$

we have $0.5(J_{a,p} - J^{\text{true}}_{a,p} - J) \sim N(0, \sigma^2_{a,p})$. The probability that the following relation holds is 99.7%:

$$-3\sigma_{a,p} \leq 0.5\left(J_{a,p} - J^{\text{true}}_{a,p} - J\right) \leq 3\sigma_{a,p} \tag{A.11}$$

which yields

$$-6\sigma_{a,p} + J^{\text{true}}_{a,p} + J \leq J_{a,p} \leq 6\sigma_{a,p} + J^{\text{true}}_{a,p} + J. \tag{A.12}$$

Suppose measurement $\mathbf{z}$ can pass the bad data detection test under significance level α, then the probability that J lies in the following range is $1-2\alpha$

$$\chi^2_{K,\alpha} \leq J \leq \chi^2_{K,1-\alpha} \tag{A.13}$$

where $K = m - n$ is the degree of freedom for the chi-square distribution of J.

So, the lower bound of $J_{a,p}$ is

$$J^{\text{lower}}_{a,p} = -6\sigma_{a,p} + J^{\text{true}}_{a,p} + \chi^2_{K,\alpha}. \tag{A.14}$$

If this lower bound exceeds the detection threshold, i.e.,

$$J^{\text{lower}}_{a,p} > \chi^2_{K,1-\alpha} \tag{A.15}$$

it is safe to say that the existence of attack can be detected. Then protecting measurement p is an effective strategy. (A.15) is called effective protection criterion.

For a specific attack vector $\mathbf{a}$ and a measurement p, $J^{\text{true}}_{a,p}$ and $\sigma_{a,p}$ can be calculated through (A.6) and (A.10) respectively. If (A.15) is satisfied, then protecting measurement p is an effective strategy, and its effectiveness is insensitive to the measurement error in the original measurements. Note that (A.15) is easy to implement and no original measurements $\mathbf{z}$ is needed.

REFERENCES

[1] Physical vulnerability of electric systems to natural disasters and sabotage, OTA-E-453, 1990.

[2] J. Salmeron, K. Wood, and R. Baldick, "Analysis of electric grid security under terrorist threat," *IEEE Trans. Power Syst.*, vol. 19, no. 2, pp. 905–912, May 2004.

[3] J. M. Arroyo and F. D. Galiana, "On the solution of the bilevel programming formulation of the terrorist threat problem," *IEEE Trans. Power Syst.*, vol. 20, no. 2, pp. 789–797, May 2005.

[4] A. L. Motto, J. M. Arroyo, and F. D. Galiana, "A mixed-integer LP programming formulation of the terrorist threat problem," *IEEE Trans. Power Syst.*, vol. 20, no. 3, pp. 1357–1365, Aug. 2005.

[5] J. Salmeron, K. Wood, and R. Baldick, "Worst-case interdiction analysis of large-scale electric power grids," *IEEE Trans. Power Syst.*, vol. 24, no. 1, pp. 96–104, Feb. 2009.

[6] Y. Yao, T. Edmunds, D. Papageorgiou, and R. Alvarez, "Trilevel optimization in power network defense," *IEEE Trans. Syst., Man, Cybern. C, Appl. Rev.*, vol. 37, no. 4, pp. 712–718, Jul. 2007.

[7] A. Delgadillo, J. M. Arroyo, and N. Alguacil, "Analysis of electric grid interdiction with line switching," *IEEE Trans. Power Syst.*, vol. 25, no. 2, pp. 633–641, May 2010.

[8] J. M. Arroyo, "Bilevel programming applied to power system vulnerability analysis under multiple contingencies," *IET Gener., Transm. Distrib.*, vol. 4, no. 2, pp. 178–190, Feb. 2010.

[9] H. Sandberg, A. Teixeira, and K. H. Johansson, "On security indices for state estimators in power networks," presented at the 1st Workshop Secure Control Syst. (CPSWEEK), Stockholm, Sweden, Apr. 2010.

[10] Y. Liu, P. Ning, and M. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proc. 16th ACM Conf. Comput. Commun. Security*, Nov. 2009, pp. 21–32.

[11] L. Mili, T. Cutsem, and M. Ribbens-Pavella, "Bad data identification methods in power system state estimation—A comparative study," *IEEE Trans. Power App. Syst.*, vol. PAS-104, no. 11, pp. 3037–3049, Nov. 1985.

[12] F. F. Wu and W.-H. E. Liu, "Detection of topology errors by state estimation," *IEEE Trans. Power Syst.*, vol. 4, no. 1, pp. 176–183, Feb. 1989.

[13] O. Kosut, L. Jia, R. Thomas, and L. Tong, "Limiting false data attacks on power system state estimation," in *Proc. Conf. Inf. Sci. Syst.*, Mar. 2010, pp. 1–7.

[14] M. Shahidehpour, H. Yamin, and Z. Li, *Market Operations in Electric Power Systems*. New York: Wiley, 2002.

[15] H. Li, Y. Li, and Z. Li, "A multiperiod energy acquisition model for a distribution company with distributed generation and interruptible load," *IEEE Trans. Power Syst.*, vol. 22, no. 2, pp. 588–596, May 2007.

[16] T. Li and M. Shahidehpour, "Risk-constrained FTR bidding strategy in transmission markets," *IEEE Trans. Power Syst.*, vol. 20, no. 2, pp. 1014–1021, May 2005.

[17] T. Li and M. Shahidehpour, "Strategic bidding of transmission-constrained GENCOS with incomplete information," *IEEE Trans. Power Syst.*, vol. 20, no. 1, pp. 437–447, Feb. 2005.

[18] J. Fortuny-Amat and B. McCarl, "A representation and economic interpretation of a two-level programming problem," *J. Oper. Res. Soc.*, vol. 32, pp. 783–792, Sep. 1981.

[19] G. Zhang, G. Zhang, Y. Gao, and J. Lu, "A bilevel optimization model and a PSO-based algorithm in day-ahead electricity markets," *Proc. IEEE Int. Conf. Syst., Man, Cybern.*, pp. 611–616, Oct. 2009.

[20] J. Wang, M. Shahidehpour, Z. Li, and A. Botterud, "Strategic generation capacity expansion planning with incomplete information," *IEEE Trans. Power Syst.*, vol. 24, no. 2, pp. 1002–1010, May 2009.

[21] A. Monticelli, *State Estimation in Electric Power Systems: A Generalized Approach*. Norwell, MA: Kluwer, 1999.

[22] MATPOWER, A MATLAB Power System Simulation Package [Online]. Available: http://www.pserc.cornell.edu/matpower/

[23] A. Abur and A. G. Exposito, *Power System State Estimation: Theory and Implementation*. New York: Marcel Dekker, 2004.

Yanling Yuan is working toward the Ph.D. degree in the Electrical and Computer Engineering (ECE) Department at Illinois Institute of Technology (IIT), Chicago.

Zuyi Li (SM'09) is an Associate Professor in the Electrical and Computer Engineering (ECE) Department at Illinois Institute of Technology (IIT), Chicago.

Kui Ren (SM'11) is an Assistant Professor in the Electrical and Computer Engineering (ECE) Department at Illinois Institute of Technology (IIT), Chicago.