Quantitative Analysis of Load Redistribution Attacks in Power Systems

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

Abstract—Cyber security is becoming an area of growing concern in the electric power industry with the development of smart grid. False data injection attack, which is against state estimation through SCADA network, has recently attracted wide research interests. This paper further develops the concept of load redistribution (LR) attack, a special type of false data injection attack. The damage of LR attacks to power system operations can manifest in an immediate or a delayed fashion. For the immediate attacking goal, we show in this paper that the most damaging attack can be identified through a max-min attacker-defender model. Benders decomposition within a restart framework is used to solve the bilevel immediate LR attack problem with a moderate computational effort. Its effectiveness has been validated by the Karush-Kuhn-Tucker (KKT)-based method solution in our previous work. For the delayed attacking goal, we propose a trilevel model to identify the most damaging attack and transform the model into an equivalent single-level mixed-integer problem for final solution. In summary, this paper enables quantitative analysis of the damage of LR attacks to power system operations and security, and hence provides an in-depth insight on effective attack prevention when resource budgets are limited. A 14-bus system is used to test the correctness of the proposed model and algorithm.

Index Terms—Benders decomposition, delayed LR attack, false data injection attack, immediate LR attack, load redistribution attack, restart framework, state estimation.

1 Introduction

Electric power systems have evolved over the past century to the largest and most complex cyber-physical systems. Their secure and reliable operation is critical to any country's economy and security. The well functioning of state estimation, which provides faithful estimation of the real-time physical system information based on a large number of distributed meter measurements, is of paramount importance for maintaining stable and secure system operation. Unfortunately, state estimation can be vulnerable to cyber attacks since its functioning relies deeply on measurement sensing and communication technologies. False data injection attack [1] can manipulate the outcome of state estimation in an arbitrary and predicted way without being detected through cooperatively modifying measurements. The attacker could corrupt the measurement data by tampering remote terminal units (RTUs), heterogeneous communication networks and control center office LANs [2]. False state estimation will further mislead the operation and control function of Energy Management System (EMS), possibly resulting in catastrophic consequences. With the development of smart grid which features greater dependence on communication and network technologies, it becomes very important to analyze the damage of such cyber-security attack and establish effective attack prevention.

In recent years, false data injection attack has attracted increasing research interests. Some work has been done to limit the effect of false data attacks on power system state estimation based on a Bayesian framework [3]. Kosut et al. [4] develop a heuristic to obtain the attack that minimizes the probability of being detected with the assumption of underlying states, while increasing the error of state estimation. Sandberg et al. [2] introduce two security indices for each power flow measurement: attack vector sparsity and attack vector magnitude, and intends to protect the measurements with low security indices. Kim and Poor [5] propose a greedy algorithm to select a subset of measurements, the protection of which significantly increases the number of measurements the attacker has to manipulate in order to realize a false data injection attack. Xie et al. [6] study the potential financial misconduct that may be induced from false data injection attacks in real-time spot market.

Our previous work [7] thoroughly studies the damaging effect of load redistribution (LR) attack on power system operation and control. LR attack is a special type of false data attack in which only load bus power injection and line power flow measurements are attackable. LR attack is more realistic than general false data injection attack in electric grid. Security-constrained economic dispatch (SCED), which minimizes the total system operation cost through the redispatch of generation output, relies on state estimation solution. Once the estimated state is manipulated by an LR attack, 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

- *The authors are with the Department of Electrical and Computer Engineering, Illinois Institute of Technology, 3301 Dearborn St, Siegel Hall, Chicago, IL 60616.*
  E-mail: yyuan7@hawk.iit.edu, lizu@iit.edu, kren@ece.iit.edu.

Manuscript received 18 Aug. 2011; revised 29 Dec. 2011; accepted 30 Jan. 2012; published online 2 Feb. 2012.
Recommended for acceptance by S. Papavassiliou, N. Kato, Y. Liu, C.-Z. Xu, and X. Wang.
For information on obtaining reprints of this article, please send e-mail to: tpds@computer.org, and reference IEEECS Log Number TPDSSI-2011-08-0546.
Digital Object Identifier no. 10.1109/TPDS.2012.58.

operating state that may cause wider load shedding in a delayed time without immediate corrective actions. The immediate and delayed damaging effects of LR attacks are clearly illustrated in a simple 2-bus system example in [7]. For immediate attacking goal, the attacker aims to maximize the operation cost immediately after the attack; for delayed attacking goal, the attacker aims to maximize the total operation cost after the tripping of overloaded lines, which is a delayed effect of LR attack. Yuan et al. [7] focus on the modeling of immediate LR attack problem and identify the most damaging LR attack by solving a max-min attacker-defender problem. This paper further develops the theory on LR attack based on our previous work.

For the immediate LR attack problem, KKT-based method is employed in [7] to solve the bilevel immediate LR attack problem. This paper makes a great improvement on computational efficiency by using Benders decomposition within a restart framework. Recent researches on vulnerability analysis of electric grid under physical terrorist attacks provide abundant approaches for solving max-min attacker-defender model, such as KKT-based method [8], duality-based method [9], and decomposition-based heuristic method [10]. Unfortunately, not all these methods are suitable in solving the LR attack problem. This is due to the distinct characteristics of the LR attack problem: an LR attack is represented by both the location of the measurements to be attacked and the attack quantity. The attack vectors in the upper level attacker problem are continuous variables. Thus, the duality-based method is not viable since multiplication of these continuous variables and dual variables would appear in the strong duality equality, which cannot be modeled in a mixed-integer linear form. Although KKT-based method can be employed to solve the LR attack problem, it is computationally inefficient due to the handling of the nonlinear complementary slackness conditions proposed by Fortuny-Amat and McCarl [11]. Despite its computational inefficiency, KKT-based method does guarantee a global optimal solution. So, its result can be used to check the correctness of any new algorithms. Artificial intelligence methods, such as particle swarm optimization [12], generic algorithm, and co-evolutionary algorithm [13] can be also employed to solve bilevel problems. However, those methods are not suitable for large systems due to their deficiency in search strategy and convergence. Salmeron et al. [10] introduce a decomposition-based heuristic that solves a series of Optimal Power Flow (OPF) models. The solutions to each OPF subproblem are used to construct estimates of the attractiveness or "value" of components for further interdiction. However, this method lacks the foundation of a formal algorithm that guarantees convergence, except through complete enumeration [14]. Salmeron et al. [14] propose a global Benders decomposition method for solving Interdict Power Flow (IPF) problem based on empirically validated assumptions. This decomposition relies on a sequence of upper bounding (i.e., optimistic) piecewise-linear functions for the interdictor's objective. However, for LR attack problem, cut generation lacks an accepted theoretical principle as in the physical terrorist attack problem. In this paper, Benders decomposition within a restart framework [15], [16] is used to solve the LR attack problem. Benders decomposition is a method initially introduced for solving large-scale mixed-integer problems (MIPs). The basic idea is to reform the original one-level larger optimization problem into a bilevel program via decomposition in order to accelerate the calculation speed. Therefore, Benders decomposition is an attractive technique when the original problem is itself a bilevel programming problem [15]. However, in order to guarantee convergence to the optimum, Benders decomposition requires that the objective function of the considered problem, projected on the subspace of the complicating variables, have a convex hull [16] (for a minimization problem). Unfortunately, this requirement is not met in the case of LR attack problem. Resembling the illustration in [14], the objective of LR attack problem is a nonconcave function of attack vectors, which cannot be maximized via Benders decomposition. This drawback can be overcome by restarting Benders decomposition with points that cover most of the solution space. The restarting framework avoids local optima and could eventually reach the global optimum. Thus, this technique is particularly appropriate for the LR attack problem. In [16], the Benders decomposition technique within a restart framework is used to solve a mixed-integer nonconvex problem. In [15], this technique successfully solves the physical terrorist threat problem in which line switching is considered as one of the operator's corrective actions. In this paper, the Benders decomposition in a restart framework is employed to solve the immediate LR attack problem in an efficient manner. The correctness of this algorithm is verified against the result of KKT-based method.

The delayed LR attack problem and its alike have not been studied before. This paper proposes a trilevel model for the first time representing attacker and two steps of SCED implementation. Using KKT-based method and duality-based method, this trilevel model can be transformed into a single-level mixed-integer problem. The most damaging delayed LR attack maximizes the total system operation cost after the tripping of overloaded lines, which is a delayed effect of LR attack.

The contributions of this paper are summarized as follows:

1. This paper applies Benders decomposition within a restart framework to solve the immediate LR attack problem.
2. This paper models the delayed LR attack problem and solves it using KKT-based method and duality-based method.
3. With the most damaging attack known, control center can then deploy specific protection strategy in order to avoid the most damaging effect. Such strategy can protect the system from LR attacks more practically and effectively.

The remainder of this paper is organized as follows: Section 2 presents the main concept of LR attack and describes the damage effect of LR attacks to system operation and control. Section 3 presents the modeling of the immediate LR attack problem and the proposed Benders decomposition solution algorithm. Section 4 proposes the modeling of the delayed LR attack problem and its solution methodology. Section 5 provides case studies. Section 6 draws relevant conclusions and future work.

2 Load Redistribution Attacks

False data injection attack [1], which cooperatively modifies selected measurement data transmitted through supervisory control and data acquisition (SCADA) system, can manipulate the state estimation outcome in an arbitrary and predicted way without being identified. The construction of false data injection attacks relies on the information of the Jacobin matrix **H**. It is assumed that every measurement is attackable. However, in power systems, the attack on some measurements will easily expose itself and the attacked measurements will be denied as effective data for state estimation. For example, the attack on generator output measurements can be detected and corrected through the direct communication between control center and power plant control room.

LR attack is a more realistic form of false data injection attack against state estimation in power systems. Only load bus power injection and line power flow measurements are attackable. Load measurements can be modified in a specified range of their true value so as not to be suspected. An LR attack can be modeled as

$$\sum_{d} \Delta D_d = 0 \tag{1}$$

$$\mathbf{\Delta PL} = -\mathbf{SF} \cdot \mathbf{KD} \cdot \Delta\mathbf{D} \tag{2}$$

$$-\tau D_d \leq \Delta D_d \leq \tau D_d \qquad \forall\, d. \tag{3}$$

Since the generation output measurements cannot be attacked, LR attack artificially increases load at some buses and reduces load at some other buses while maintaining the total load unchanged (1). Line power flow measurements need to be cooperatively modified in order to hide the attack from bad data detection. The construction of LR attack relies on the information of shifting factor matrix **SF** and bus-load incidence matrix **KD** as in (2), both of which are topological information of the network and can be derived from the Jacobin matrix **H**. LR attack can be essentially viewed as a disturbance that follows the power flow equation (2), where $\mathbf{\Delta PL}$ is the attack on the power flow measurements. Constraint (3) limits the attack magnitude of load ΔD_d to a percentage (τ) of the original load measurement D_d.

Based on the manipulated state estimation outcome, 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 occur in the worst case. This damaging effect is realized immediately after the enforcement of SCED. It can be quantified by the operation cost from the SCED implementation. Second, the false SCED may lead the system into an insecure operating state, i.e., power flow on some transmission lines actually exceed their transmission capacity. Operators in the control center will assume that all transmission lines operate within their security ranges based on the false SCED. Without immediate corrective actions, the overloaded lines will trip and could cause more load shedding in a delayed time. This damaging effect is equivalent to an indirect physical terrorist attack to transmission lines; the difference is that this damaging effect is realized in a delayed time after the enforcement of the false SCED. The damaging effect of delayed LR attacks can be quantified based on the first SCED immediately after the attack and the second SCED implementation triggered by the tripping of overloaded lines. In conclusion, LR attacks may mislead the normal functioning of SCED and result in economic and security risk. Since the introduction of deregulation [17], increased levels of consumption and lack of investment on transmission system upgrade are driving the operation of power systems closer to their static and dynamic limits, so power systems are becoming increasingly vulnerable to LR attacks. In particular, power systems are extremely vulnerable to LR attacks when multiple transmission lines are operating near their capacity limits.

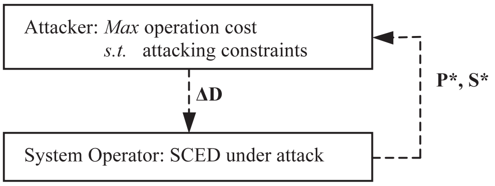
Attacker: *Max* operation cost
s.t. attacking constraints
ΔD
P*, S*
System Operator: SCED under attack

Fig. 1. Bilevel model for immediate LR attack problem.

3 The Immediate LR Attack Problem

To wisely protect the system from LR attacks under limited protection resources, control centers have to first identify the most damaging attack and then deploy protection measures to avoid its happening. This section presents the bilevel attacker-defender model for the immediate LR attack problem and its solution methodology.

3.1 Model of Immediate LR Attack

The goal of the most damaging immediate LR attack 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. 1 is designed in [7] to identify the most damaging attack given posited attacking resources. The upper level represents the attacker and determines the attack vector $\mathbf{\Delta D}$ to be injected into the original meter measurements in order to maximize the operation cost of the system. The system operator in the lower level optimally reacts to the false state estimation that has been successfully manipulated by the attack vector determined in the upper level. The operation cost is determined by the generation output $\mathbf{P}^*$ and load shedding $\mathbf{S}^*$ based on the false SCED solution.

The mathematical model of the immediate LR attack problem is shown as

$$\underset{\mathbf{\Delta D}}{Max} \sum_{g} c_g P_g^* + \sum_{d} cs_d S_d^* \tag{4}$$

$$\text{s.t.} \sum_{d} \Delta D_d = 0 \tag{5}$$

$$\mathbf{\Delta PL} = -\mathbf{SF} \cdot \mathbf{KD} \cdot \mathbf{\Delta D} \tag{6}$$

$$-\tau D_d \leq \Delta D_d \leq \tau D_d \qquad \forall\, d \tag{7}$$

$$\Delta D_d = 0 \Leftrightarrow \delta_{D,d} = 0 \qquad \forall\, d \tag{8}$$

$$\Delta PL_l = 0 \Leftrightarrow \delta_{PL,l} = 0 \qquad \forall\, l \tag{9}$$

$$\sum_d \delta_{D,d} + 2\sum_l \delta_{PL,l} \leq R \tag{10}$$

$$\delta_{D,d}, \delta_{PL,l} \in \{0,1\} \qquad \forall\, d, l \tag{11}$$

$$\{\mathbf{P}^*, \mathbf{S}^*\} = \arg\left\{ \underset{\mathbf{P},\mathbf{S}}{Min} \sum_g c_g P_g + \sum_d cs_d S_d \right\} \tag{12}$$

$$\text{s.t.} \sum_g P_g = \sum_d (D_d - S_d) \tag{13}$$

$$\mathbf{PL} = \mathbf{SF}\cdot\mathbf{KP}\cdot\mathbf{P} - \mathbf{SF}\cdot\mathbf{KD}\cdot(\mathbf{D}+\boldsymbol{\Delta}\mathbf{D}-\mathbf{S}) \tag{14}$$

$$-PL_l^{\max} \leq PL_l \leq PL_l^{\max} \qquad \forall\, l \tag{15}$$

$$P_g^{\min} \leq P_g \leq P_g^{\max} \qquad \forall\, g \tag{16}$$

$$0 \leq S_d \leq D_d + \Delta D_d \qquad \forall\, d, \tag{17}$$

where c_g and P_g are the generation cost (\$/MWh) and generation outputs (MW) of generator g, respectively; cs_d and S_d are the load shedding cost (\$/MWh) and load shedding amount (MW) of load d, respectively; PL_l is the flow (MW) of transmission line l; and $\mathbf{KP}$ is the bus-generator incidence matrix. $\delta_{D,d}$ indicates whether the measurement of load d is attacked. $\delta_{PL,l}$ indicates whether the power flow measurement of line l is attacked.

The attacker model is represented by the upper level problem (4)-(11). The attacker maximizes the system operation cost, which includes generation cost and load shedding cost as shown in (4), considering a set of attack constraints (5)-(11). Constraints (5)-(7) ensure a legitimate LR attack. Constraints (8) and (9) model the logic relationships between the attack vector and the resource it uses for each attackable measurements. For a fully measured system, the attacker needs to modify two meters in order to attack a power flow measurement. Constraint (10) guarantees that the attack satisfies attack resource limitation R. The system operator model is represented by an SCED model in the lower level problem (12)-(17), which is parameterized in terms of the upper level attack variables $\boldsymbol{\Delta}\mathbf{D}$. It minimizes system operation cost in (12), considering the SCED constraints (13)-(17). Constraint (13) represents system balance equation. Constraint (14) represents line flow equations. Constraint (15) enforces corresponding line flow capacity limits. Constraints (16) and (17) set the limits of generation and load shedding, respectively. Note that the upper limit of load shedding considers the influence of attack on load measurement $\boldsymbol{\Delta}\mathbf{D}$. As is commonly assumed, a dc model of the transmission system is used and only constraints under base case are considered.

The most damaging LR attack can be identified by solving the above bilevel attacker-defender problem. Benders decomposition within a restart framework is employed to solve this problem, which is computationally more efficient than the KKT-based method. First, we present the compact mathematical formulation of the master problem and subproblem of the immediate LR attack problem. Then, we provide the process of multistart Benders decomposition and introduce a new technique to create tighter cuts.

3.2 Compact Formulation

The immediate LR attack problems can be reformulated in a compact manner as

$$\underset{\mathbf{y}}{Min} - f(\mathbf{x}^*) \tag{18}$$

$$\text{s.t. } h(\mathbf{u},\mathbf{y}) \leq \mathbf{0} \tag{19}$$

$$\mathbf{x}^* = \arg\left\{ \underset{x}{Min}\, f(\mathbf{x}) \right\} \tag{20}$$

$$\text{s.t. } g(\mathbf{x},\mathbf{y}) \leq \mathbf{0}, \tag{21}$$

where variables $\mathbf{y}$ in the upper level problem refer to attack vector $\boldsymbol{\Delta}\mathbf{D}$; variables $\mathbf{u}$ in the upper level problem include $\boldsymbol{\Delta}\mathbf{PL}$, δ_D, and δ_{PL}; variables $\mathbf{x}$ in the lower level problem include dispatch variables $\mathbf{P}$, $\mathbf{S}$; the objective function is the system operation cost.

According to [15], at iteration k, Benders decomposition transforms problem (18)-(21) into a master problem

$$\underset{\mathbf{y}}{Min}\ \alpha \tag{22}$$

$$\text{s.t. } h(\mathbf{u},\mathbf{y}) \leq 0 \tag{23}$$

$$\alpha \geq -f(\mathbf{x}^{(v)}) - \boldsymbol{\eta}^{(v)^T}(\mathbf{y}-\mathbf{y}^{(v)}) \quad v = 1, \mathrm{K}\ldots, k-1 \tag{24}$$

and a subproblem

$$\underset{\mathbf{x}}{Min}\, w = f(\mathbf{x}) \tag{25}$$

$$\text{s.t. } g(\mathbf{x},\mathbf{y}) \leq \mathbf{0} \tag{26}$$

$$\mathbf{y} = \mathbf{y}^{(k)} : \boldsymbol{\eta}^{(k)} \tag{27}$$

$$g(\mathbf{x},\mathbf{y}) \leq \mathbf{0}, \tag{28}$$

where $\boldsymbol{\eta}^{(k)}$ is the dual variables associated with (27) in the kth iteration of Benders loop.

3.3 Restarting Framework

Due to the nonconcave nature of the objective as a function of attack variables, the maximization process may falsely terminate at local optima. To overcome this drawback, a multistart Benders decomposition framework is adopted in this paper to avoid local optima and could eventually reach the global optimum. The procedure of multistart Benders decomposition is shown in Fig. 2 and discussed as follows:

1. Restarting initialization. Set the restarting counter $j = 1$, and the global optimum of the problem (18)-(21) $z_{opt} = \infty$.
2. Benders initialization. Set the Benders iteration counter $k = 1$.
3. Master problem solution. Solve the master problem (22)-(24) and get the upper level variables $\mathbf{y}^{(k)}$, with a lower bound for objective function $z_{lo}^{(k)} = \alpha^{(k)}$.
4. Subproblem solution. Solve the subproblem (25)-(28) and get the optimal operation cost $w^{(k)}$, optimal dispatch variables $\mathbf{x}^{(k)}$ and dual variables $\boldsymbol{\eta}^{(k)}$ and the upper bound for objective function $z_{up}^{(k)} = \min(z_{up}^{(k-1)}, -w^{(k)})$.
5. Update duals. This step yields tighter cut coefficients, resulting in a tighter master-problem bound and a more efficient decomposition algorithm. The updating is based on the following two rules:

$$\begin{cases} \text{if } \Delta D_d^{(k)} = \tau D_d, \text{ and } \eta_d^{(k)} > 0, \text{then set } \eta_d^{(k)} = 0 \\ \text{if } \Delta D_d^{(k)} = -\tau D_d, \text{ and } \eta_d^{(k)} < 0, \text{then set } \eta_d^{(k)} = 0 \end{cases}.$$

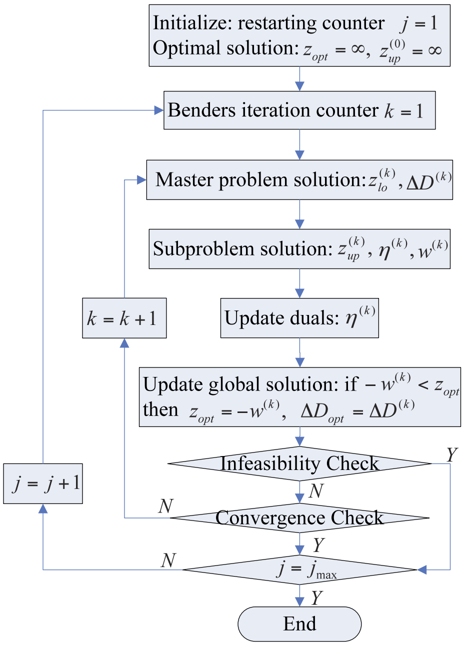
Initialize: restarting counter $j = 1$
Optimal solution: $z_{opt} = \infty$, $z_{up}^{(0)} = \infty$
Benders iteration counter $k = 1$
Master problem solution: $z_{lo}^{(k)}, \Delta D^{(k)}$
Subproblem solution: $z_{up}^{(k)}, \eta^{(k)}, w^{(k)}$
$k = k+1$
Update duals: $\eta^{(k)}$
Update global solution: if $-w^{(k)} < z_{opt}$ then $z_{opt} = -w^{(k)}$, $\Delta D_{opt} = \Delta D^{(k)}$
Infeasibility Check
Y
$j = j+1$
N
N
Convergence Check
Y
N
$j = j_{\max}$
Y
End

Fig. 2. Flowchart of the multistart Benders decomposition.

The above updating rules are valid since there are no possibilities of cost increase for both situations.

6. Update global solution. If $-w^{(k)} < z_{opt}$, update the global solution, $z_{opt} = -w^{(k)}$, $\mathbf{y}_{opt} = \mathbf{y}^{(k)}$.
7. Infeasibility check. If $z_{up}^{(k)} < z_{lo}^{(k)}$, which means that a nonconvex region is constructed and no solution can be identified, go to step 9. Otherwise, go to step 8.
8. Convergence check. If $|z_{up}^{(k)} - z_{lo}^{(k)}| \le \varepsilon$ or $k = k_{\max}$, a solution with a level of accuracy ε is found or the Benders iteration counter reaches its maximum value, go to step 9. Otherwise, Benders iteration continues and $k = k + 1$, and go to step 3.
9. Restart stop criterion. If $j = j_{\max}$, the restart iteration counter reaches its maximum value, the algorithm stops. Otherwise, the Benders decomposition is restarted and $j = j + 1$, and go to step 2. When the Benders decompositions is restarted, Benders cuts of the previous Benders loops are discarded except for the last one.

Note that $-z_{opt}$ is the operation cost of the most damaging immediate LR attack. $z_{up}^{(k)}$ and $z_{lo}^{(k)}$ are the upper bound and lower bound of z_{opt}, respectively.

4 The Delayed LR Attack Problem

The most damaging delayed LR attack is identified by the delayed LR attack problem, the modeling and solution of which are introduced in this section.

4.1 Modeling of Delayed LR Attack

The most damaging delayed LR attack aims to maximize the total operation cost after the tripping of overloaded lines, which is a delayed effect of LR attack. The delayed attack includes three steps: 1) attacker decides an attack vector; 2) control center performs the first SCED function based on the false state estimation and line overloading occurs; 3) control center performs the second SCED after the tripping of the overloaded lines. This paper assumes: 1) Multiple overloaded lines, if any, will trip together; 2) Load demand does not change between the first SCED and second SCED. A trilevel model for identifying the most damaging LR attack in a delayed timeframe is shown in Fig. 3. The upper level represents the attacker and determines the attack vector $\mathbf{\Delta D}$ to be injected into the original meter measurements in order to maximize the total operation cost of the system. In the middle level, the system operator implements the first SCED reacting to the false state estimation that has been successfully manipulated by the attack vector $\mathbf{\Delta D}$. After the first SCED, control center presumes load demand is $\mathbf{D} + \mathbf{\Delta D}$ and line power flow is $\mathbf{PL_1}$ under optimal dispatch $\mathbf{P_1}$ and load shedding $\mathbf{S_1}$. However, the actual power flow should be

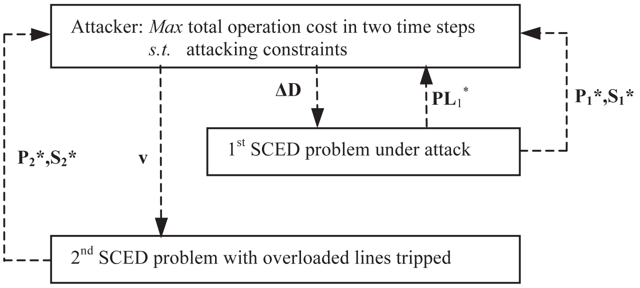
Attacker: Max total operation cost in two time steps
s.t. attacking constraints
ΔD
PL1*
P1*,S1*
P2*,S2*
v
1st SCED problem under attack
2nd SCED problem with overloaded lines tripped

Fig. 3. Trilevel model for delayed attacking goal.

$$\begin{aligned}
&\mathbf{SF} \cdot \mathbf{KP} \cdot \mathbf{P_1} - \mathbf{SF} \cdot \mathbf{KD} \cdot (\mathbf{D} - \mathbf{S}_1) \\
&= \mathbf{SF} \cdot \mathbf{KP} \cdot \mathbf{P_1} - \mathbf{SF} \cdot \mathbf{KD} \cdot (\mathbf{D} + \mathbf{\Delta D} - \mathbf{S}_1) \\
&\quad + \mathbf{SF} \cdot \mathbf{KD} \cdot \mathbf{\Delta D} \\
&= \mathbf{PL_1} + \mathbf{SF} \cdot \mathbf{KD} \cdot \mathbf{\Delta D} = \mathbf{PL_1} - \mathbf{\Delta PL}.
\end{aligned} \tag{29}$$

Based on the actual power flow after the first SCED implementation, the overloaded transmission lines can then be determined, which are indicated by binary variable $\mathbf{v}$. The second SCED in the lower level is implemented after the tripping of all overloaded lines. The total operation cost is determined by the solution of the first SCED and the second SCED.

The mathematical model of the delayed LR attack problem is shown as (30)-(50), where $\mathbf{KL}$ is the bus-branch incidence matrix; B_{MVA} is the system MVA base; x_l is the reactance (p.u.) of line l; θ_l^{FR} and θ_l^{TO} are the phase angles (rad) at the "from" bus and "to" bus of line l, respectively, in (30)-(50). Subscript "1" refers to the first SCED solution and subscript "2" refers to the second SCED solution. $v_l = 0$ indicates that line l is actually overloaded after the implementation of the first SCED and will trip in a delayed time.

The upper level problem (30)-(38) represents the attacker with the delayed attacking goal. Constraints (31)-(36) are the constraints for LR attacks. Constraints (37)-(38) determine the overloaded lines based on attack vector $\mathbf{\Delta PL}$ and the power flow solution $\mathbf{PL_1}$ of the first SCED. According to constraint (37), if the actual power flow of line l after the first SCED is overloaded, the indicator v_l is set to 0. Middle-level optimization problem (39)-(44) models the control center's first SCED under the given attack. Lower level optimization problem (45)-(50) models the control center's second SCED after the tripping of overloaded lines. Constraint (46) expresses the line flow in terms of nodal phase angles and indicator v_l. If line l is actually overloaded after the implementation of the first SCED, this line will be tripped and its power flow is set to 0 by (46). Note that constraint (46) is nonlinear due to the products of binary variables and continuous variables $v_l\theta_l^{FR}$ and $v_l\theta_l^{TO}$. Both the nonlinearities can be replaced with equivalent linear expressions by introducing new binary variables and continuous variables. Constraint (47) represents the nodal power balance equations. Constraint (48) enforces the corresponding line flow capacity limits. Finally, constraints (49) and (50) set the limits of generation and load shedding, respectively.

$$\underset{\mathbf{\Delta D}}{Max} \sum_g c_g\left(P^*_{1,g} + P^*_{2,g}\right) + \sum_d cs_d\left(S^*_{1,d} + S^*_{2,d}\right) \tag{30}$$

$$\text{s.t.} \sum_d \Delta D_d = 0 \tag{31}$$

$$-\tau D_d \le \Delta D_d \le \tau D_d \qquad \forall\, d \tag{32}$$

$$\Delta D_d = 0 \Leftrightarrow \delta_{D,d} = 0 \qquad \forall\, d \tag{33}$$

$$\Delta PL_l = 0 \Leftrightarrow \delta_{PL,l} = 0 \qquad \forall\, l \tag{34}$$

$$\sum_d \delta_{D,d} + 2\sum_l \delta_{PL,l} \le R \tag{35}$$

$$\delta_{D,d}, \delta_{PL,l} \in \{0,1\} \qquad \forall\, d,l \tag{36}$$

$$-PL_l^{\max} \le PL^*_{1,l} - \Delta PL_l \le PL_l^{\max} \Leftrightarrow v_l = 1 \qquad \forall\, l \tag{37}$$

$$v_l \in \{0,1\} \qquad \forall\, l \tag{38}$$

$$\{\mathbf{P}_1^*, \mathbf{S}_1^*, \mathbf{PL}_1^*\} = \arg\left\{\underset{\mathbf{P}_1,\mathbf{S}_1}{Min} \sum_g c_g P_{1,g} + \sum_d cs_d S_{1,d}\right\} \tag{39}$$

$$\text{s.t.} \sum_g P_{1,g} = \sum_d (D_d - S_{1,d}) \tag{40}$$

$$\mathbf{PL}_1 = \mathbf{SF}\cdot\mathbf{KP}\cdot\mathbf{P}_1 - \mathbf{SF}\cdot\mathbf{KD}\cdot(\mathbf{D} + \mathbf{\Delta D} - \mathbf{S}_1) \tag{41}$$

$$-PL_l^{\max} \le PL_{1,l} \le PL_l^{\max} \qquad \forall\, l \tag{42}$$

$$P_g^{\min} \le P_{1,g} \le P_g^{\max} \qquad \forall\, g \tag{43}$$

$$0 \le S_{1,d} \le D_d + \Delta D_d \qquad \forall\, d \tag{44}$$

$$\{\mathbf{P}_2^*, \mathbf{S}_2^*\} = \arg\left\{\underset{\mathbf{P}_2,\mathbf{S}_2}{Min} \sum_g c_g P_{2,g} + \sum_d cs_d S_{2,d}\right\} \tag{45}$$

$$\text{s.t. } PL_{2,l} = B_{MVA}\cdot x_l^{-1} v_l\left(\theta_l^{FR} - \theta_l^{TO}\right) \qquad \forall\, l \tag{46}$$

$$\mathbf{KL}\cdot\mathbf{PL}_2 = \mathbf{KP}\cdot\mathbf{P}_2 - \mathbf{KD}\cdot(\mathbf{D} - \mathbf{S}_2) \tag{47}$$

$$-PL_l^{\max} \le PL_{2,l} \le PL_l^{\max} \qquad \forall\, l \tag{48}$$

$$P_g^{\min} \le P_{2,g} \le P_g^{\max} \qquad \forall\, g \tag{49}$$

$$0 \le S_{2,d} \le D_d \qquad \forall\, d. \tag{50}$$

4.2 Solution Methodology

Given the continuous upper level attack vector $\mathbf{\Delta D}$, the first SCED problem in the middle-level problem is linear and convex. Given the integer upper level variable $\mathbf{v}$, the second SCED problem in the lower level problem is linear and convex. Thus, this trilevel problem can be transformed into a single-level mixed-integer problem by replacing the middle-level problem with its KKT optimality condition and then the lower level problem with its duality equivalent form.

5 Numerical Results

This section presents a case study based on a modified IEEE 14-bus system with generator parameters shown in Table 1. Other configuration data of the test system are obtained from [18]. 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 value. Attack resource is limited to 20 meters. Suppose that the cost of unmet demand is $cs = 100$ \$/MWh. For illustration purposes, the transmission capacities are modified to simulate the condition under which the system is operating close to its capacity limit. Transmission capacity of line 1 is 160 MW, and capacities of all other lines are 60 MW.

TABLE 1
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

5.1 The Most Damaging Immediate LR Attack

In this paper, the immediate LR attack problem is solved using the Benders decomposition in a restart framework. For the immediate attack goal, 16 meters will be attacked in the most damaging LR attack, as shown in Table 2. The most damaging attack "transfers" load at bus 2, 4, and 5 to bus 3, which originally has the heaviest load in the system. The load distributions of the system according to the original load measurements and the measurements after attack are shown in Fig 4. Six line power flow measurements have to be cooperatively modified in order to realize an undetectable attack. By simulating the most damaging attack, we observe that false SCED leads to a load shedding of 12.9243 MW at bus 3. However, there is no load shedding in the original SCED results without attack. The comparison of the false SCED and the original SCED is shown in Table 3.

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 $7{,}113.9 - 6{,}203.3 = 910.6$ \$/h. Note that in this case, after the implementation of the false SCED, the actual power flows on transmission lines are all within capacity limits. That is, the most damaging immediate LR attack will not cause line tripping in a delayed time.

Using the multistart Benders decomposition, the immediate LR attack problem converges to the optimal solution in four restarting rounds as shown in Table 4. Fig. 5 demonstrates the convergence of the multistart Benders decomposition. Whenever $z_{up}^{(k)} < z_{lo}^{(k)}$, which means a nonconvex region is constructed, the Benders decomposition is restarted by setting the iteration counter $k = 1$. The multistart Benders decomposition framework reaches the global optimum after four restarts and eight Benders iterations.

The correctness of this solution has been validated by the KKT-based method solution in [7]. While it takes up to hundreds of seconds to solve the same problem using KKT-based method, it only takes several seconds using the multistart Benders decomposition. The advantage in computational efficiency makes this multistart Benders decomposition suitable for solving LR attack problems in large-scale systems.

TABLE 2
The Most Damaging Immediate LR Attack

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
43	P_3^{inj}	-38.4047
44	P_4^{inj}	23.9000
45	P_5^{inj}	3.6547

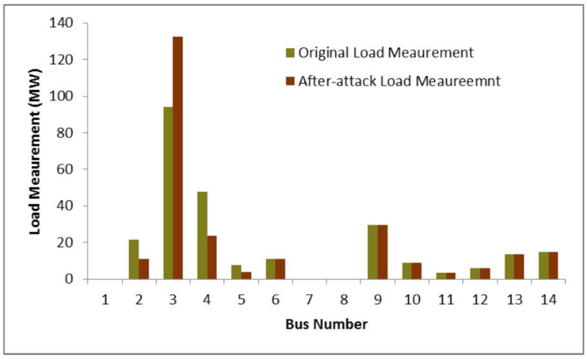

Fig. 4. Load distribution before and after attack.

TABLE 3
Comparison of False and Original SCED

		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

TABLE 4
The Solution Details of Immediate LR Attack Problem

j	*k*	z_{lo}	*w*	z_{up}	z_{opt}
1	1	$-\infty$	6203.3	-6203.3	-6203.3
	2	-6366.7	6426.6	-6426.6	-6426.6
2	1	-7415.9	6203.3	-6426.6	-6426.6
	2	-6657.7	6203.3	-6426.6	-6426.6
	3	-6517.3	6333.7	-6426.6	-6426.6
	4	-6413.2	6727.0	-6727.0	-6727.0
3	1	-7055.2	7113.9	-7113.9	-7113.9
4	1	-7113.9	7113.9	-7113.9	-7113.9

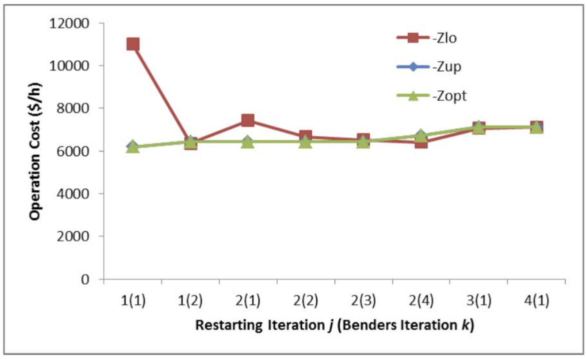

Fig. 5. Convergence of multistart Benders decomposition.

TABLE 5
The Most Damaging Delayed LR Attack

Meas. *p*	Meas.	Attack quantity (*MW*)
1 & 21	PL_{12}& PL_{21}	0.0100 &-0.0100
2 & 22	PL_{15}& PL_{51}	-0.0100 &0.0100
3 & 23	PL_{23}& PL_{32}	-0.0100 &0.0100
5 & 25	PL_{25}& PL_{52}	-0.0162 & 0.0162
6 & 26	PL_{34}& PL_{43}	0.0116 & -0.0116
7 & 27	PL_{45}& PL_{54}	-0.0670 & 0.0670
10 & 30	PL_{56}& PL_{65}	0.0112 & -0.0112
42	P_2^{inj}	-0.0362
43	P_3^{inj}	0.0216
44	P_4^{inj}	-0.0786
45	P_5^{inj}	0.1044
46	P_6^{inj}	-0.0112

TABLE 6
Comparison of False and Original SCED

		False SCED		Original SCED	
		1st	2nd	1st	2nd
Generation dispatch on bus (MW)	1	180.4952	132.9809	180.4449	180.4449
	2	44.7537	0	44.7837	44.7837
	3	13.7511	30	13.7714	13.7714
	6	0	50	0	0
	8	20	20	20	20
Total gen. (MW)		259	232.9809	259	259
Oper. cost ($/h)		6202.6	9661.5	6203.3	6203.3
Total cost ($/h)		15864		12407	

5.2 The Most Damaging Delayed LR Attack

In the most damaging delayed LR attack, 19 meters will be attacked cooperatively, as shown in Table 5. By simulating the most damaging delayed LR attack, transmission lines 1-5 and 2-3 are actually overloaded. After the tripping of the two lines, the second SCED leads to a load shedding of 4.2 MW at bus 3 and 21.8191 MW at bus 4. The comparison of the false SCED and the original SCED is shown in Table 6. The most damaging LR attack causes a total economic loss of $15{,}864 - 12{,}407 = 3{,}457$ $/h.

It is worth mentioning that the attack quantities of the most damaging delayed LR attack are very small since 1) in the model of legitimate LR attacks, we set 0.01MW as the minimum quantity that can be injected; 2) Lines 1-5 and 2-3 are originally running close to their transmission capacities, so a small attack injection is enough to cause their overloading; 3) The objective of the attacker is to maximize the total operation cost of the first SCED and the second SCED. For LR attacks with delayed damaging effect, the operation cost of the false first SCED is lower than what it should be originally if there is no load shedding in the false 1st SCED. A small injection of LR attack helps to keep the generation cost of the false first SCED very close to its upper limit 6,203.3, as shown in Table 6.

All tests in this paper are carried out on a 2.93 GHz computer with 1.98 GB of RAM. The model and algorithm are implemented in Matlab. The optimization problems are solved with CPLEX.

6 Conclusion and Future Work

This paper further develops the concept of load redistribution attack in our previous research. For the immediate LR problem, a multistart Benders decomposition method is used to find the most damaging immediate attack from the attacker's perspective. Its advantage in computational efficiency makes it suitable for solving LR attack problem in large-scale power systems. This paper also improves our previous research by modeling the trilevel delayed LR attack problem. KKT optimality condition and duality theory are used to transform the trilevel problem into a single-level optimization problem. The identification of the most damaging LR attacks for both immediate and delayed attacking goal provides an in-depth insight on effective attack prevention strategy with limited protection resource budget.

In the future work, we will study the influence of LR attacks on power market operation and the construction of LR attacks against AC state estimation.

Acknowledgments

The authors would like to thank the referees for their helpful comments and suggestions. This research was supported in part by the US Department of Energy under Grant DE-FC26-08NT02875 and the US National Science Foundation (NSF) under Grant CNS-1117811.

References

[1] Y. Liu, P. Ning, and M. Reiter, "False Data Injection Attacks against State Estimation in Electric Power Grids," *Proc. 16th ACM Conf. Computer Comm. Security,* pp. 21-32, Nov. 2009.

[2] H. Sandberg, A. Teixeira, and K.H. Johansson, "On Security Indices for State Estimators in Power Networks," *Proc. First Workshop Secure Control Systems (CPSWEEK),* Apr. 2010.

[3] O. Kosut, L. Jia, R. Thomas, and L. Tong, "Limiting False Data Attacks on Power System State Estimation," *Proc. Ann. Conf. Information Sciences and Systems,* pp. 1-7, Mar. 2010.

[4] O. Kosut, L. Jia, R. Thomas, and L. Tong, "Malicious Data Attacks on Smart Grid State Estimation: Attack Strategies and Countermeasures," *Proc. IEEE Conf. Smart Grid Comm.,* pp. 220-225, Oct. 2010.

[5] T.T. Kim and H.V. Poor, "Strategic Protection against Data Injection Attacks on Power Grids," *IEEE Trans. Smart Grid,* vol. 2, no. 2, pp. 326-333, June 2011.

[6] L. Xie, Y. Mo, and B. Sinopoli, "False Data Injection Attacks in Electricity Markets," *Proc. IEEE Conf. Smart Grid Comm.,* pp. 226-231, Oct. 2010.

[7] Y. Yuan, Z. Li, and K. Ren, "Modeling Load Redistribution Attacks in Power Systems," *IEEE Trans. Smart Grid,* vol. 2, no. 2, pp. 326-333, June 2011.

[8] J.M. Arroyo and F.D. Galiana, "On the Solution of the Bilevel Programming Formulation of the Terrorist Threat Problem," *IEEE Trans. Power Systems,* vol. 20, no. 2, pp. 789-797, May 2005.

[9] A.L. Motto, J.M. Arroyo, and F.D. Galiana, "A Mixed-Integer LP Procedure for the Analysis of Electric Grid Security under Disruptive Threat," *IEEE Trans. Power Systems,* vol. 20, no. 3, pp. 1357-1365, Aug. 2005.

[10] J. Salmeron, K. Wood, and R. Baldick, "Analysis of Electric Grid Security under Terrorist Threat," *IEEE Trans. Power Systems,* vol. 19, no. 2, pp. 905-912, May 2004.

[11] J. Fortuny-Amat and B. McCarl, "A Representation and Economic Interpretation of a Two-Level Programming Problem," *J. Operational Research Soc.,* vol. 32, pp. 783-792, Sept. 1981.

[12] 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'l Conf. Systems, Man, Cybernetics,* pp. 611-616, Oct. 2009.

[13] J. Wang, M. Shahidehpour, Z. Li, and A. Botterud, "Strategic Generation Capacity Expansion Planning with Incomplete Information," *IEEE Trans. Power Systems,* vol. 24, no. 2, pp. 1002-1010, May 2009.

[14] J. Salmeron, K. Wood, and R. Baldick, "Worst-Case Interdiction Analysis of Large-Scale Electric Power Grids," *IEEE Trans. Power Systems,* vol. 24, no. 1, pp. 96-104, Feb. 2009.

[15] A. Delgadillo, J.M. Arroyo, and N. Alguacil, "Analysis of Electric Grid Interdiction with Line Switching," *IEEE Trans. Power Systems,* vol. 25, no. 2, pp. 633-641, May 2010.

[16] R. Minguez and F. Milano, R. Zarate-Minano, and A.J. Conejo, "Optimal Network Placement of SVC Devices," *IEEE Trans. Power Systems,* vol. 22, no. 4, pp. 1851-1860, Nov. 2007.

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

[18] MATPOWER, "A MATLAB Power System Simulation Package," http://www.pserc.cornell.edu/matpower/, 2012.

Yanling Yuan received the BS degree from Wuhan University of Hydraulic and Electrical Engineering, Yichang, China, in 2001, the MS degree from Wuhan University, China, in 2004, both in electrical engineering. She is currently working toward the PhD degree from the Electrical and Computer Engineering (ECE) Department, Illinois Institute of Technology (IIT), Chicago. She is a student member of the IEEE.

Zuyi Li (SM'09) received the BS degree in electrical engineering from Shanghai Jiaotong University, China, in 1995, the MS degree in electrical engineering from Tsinghua University, Beijing, China, in 1998, and the PhD degree in electrical engineering from Illinois Institute of Technology, Chicago, in 2002. Presently, he is an associate professor in the ECE Department at IIT. He is a senior member of the IEEE.

Kui Ren (SM'11) received the BS and MS degrees from Zhejiang University and the PhD degree from Worcester Polytechnic Institute. He is currently an assistant professor of the ECE Department at IIT. His research interests include smart grid security, security and privacy in cloud computing, wireless security, and sensor and mesh network security. He was a guest editor for the *IEEE Transactions on Smart Grid, Special Issue on Cyber, Physical and System Security for Smart Grid*. He serves as an associate editor for *IEEE Wireless Communications* and *IEEE Transactions on Smart Grid*. His research is supported by the US National Science Foundation (NSF), US Department of Energy (DOE), Air Force Research Laboratory, and Amazon Web Services. He received the NSF CAREER Award in 2011. He is a senior member of the IEEE.