Transmission Line Rating Attack in Two-Settlement Electricity Markets

Hongxing Ye, *Student Member, IEEE,* Yinyin Ge, *Student Member, IEEE,* Xuan Liu, *Student Member, IEEE,*
and Zuyi Li, *Senior Member, IEEE*

***Abstract*—The potential economic impact of transmission line rating (TLR) attacks in two-settlement electricity markets is studied in this paper. We show that nodal prices in real-time markets can be manipulated via a TLR attack, which can be modeled as a bi-level optimization problem. Several acceleration techniques are developed to reduce the computational burden of solving the bi-level problem. A heuristic strategy is proposed to deal with the issue of multiplicity in pricing. The uncertainties in load are also considered in the proposed TLR model. Numerical simulations demonstrate that well-designed TLR attacks can manipulate the profits of market participants in the two-settlement markets. Benchmark testing shows that the proposed acceleration techniques can reduce computation time tremendously and the proposed heuristic strategy can mitigate the issue of multiplicity in pricing.**

***Index Terms*—False Data Injection Attack, Transmission Line Rating Attack, Pricing Multiplicity, Two-settlement Electricity Market.**

NOMENCLATURE

Indices

i, l, n	index for generator, line and bus

Constants

N_g, N_l	numbers of generators and lines
N_w	number of pieces to approximate the cost curves
$\boldsymbol{c}$	cost coefficient vector
$\boldsymbol{v}, v_n$	virtual transactions vector, the n^{th} entry in $\boldsymbol{v}$
$\boldsymbol{\phi_{DA}}, \boldsymbol{p_{DA}}$	day-ahead market LMP vector, generation
$\boldsymbol{d}, d_n$	load vector, load at bus n
$\boldsymbol{K_p}$	bus-generator incidence matrix
$\boldsymbol{K_d}$	bus-load incidence matrix
$\boldsymbol{\Gamma}, \boldsymbol{\Gamma}_{l\bullet}$	shift factor matrix, shift factor row for line l
$\Gamma^g_{l,i}$	generation shift factor for generator i and line l
$\hat{\boldsymbol{r}}, \underline{\boldsymbol{r}}, \bar{\boldsymbol{r}},$	initial, lower/upper limit vectors for TLR
$\hat{r}_l, \underline{r}_l, \bar{r}_l$	initial, lower/upper limit for TLRs of line l
S	number of lines allowed to be compromised
M, ϵ	Big-M and small perturbation

Variables

φ	profit due to TLR attack
$\boldsymbol{\phi_{RT}}$	Real-time market LMP vector
z	total system operation cost
$\boldsymbol{p}$	generation vector
$\boldsymbol{r}, r_l$	TLR vector, TLR of line l
λ	Lagrangian multipliers for (10)
$\boldsymbol{\mu^+}, \boldsymbol{\mu^-}$	Lagrangian multipliers for (11)
μ_l^+, μ_l^-	Lagrangian multiplier entries in vector $\boldsymbol{\mu^+}, \boldsymbol{\mu^-}$
$\boldsymbol{\beta^+}, \boldsymbol{\beta^-}$	Lagrangian multipliers for (12)
β_i^+, β_i^-	Lagrangian multipliers entries in vector $\boldsymbol{\beta^+}, \boldsymbol{\beta^-}$
f_l	DC power flow of line l
b_l^-, b_l^+	indicators of line l flow binding in negative or positive direction
g_i^-, g_i^+	indicators of unit i generation reaching its lower or upper limit
y_l	indicator of TLR of line l being changed

Sets and functions

J, Θ	possible binding lines and uncertain load buses set
$(\bullet)^\top$	transpose of vector or matrix

I. INTRODUCTION

WITH the development of smart grids, both the physical power grid and electricity markets are undergoing intense evolution [1]–[3]. New sensors and instruments are being deployed in power systems to collect data, which are then sent to control centers. Sending, receiving, and processing these data require more Information Technologies (IT) infrastructures be applied [4], [5]. While the IT technologies provide system operators more capabilities of monitoring and controlling the operating states of the system, they also pose new challenges to maintain the cyber-security of the system.

Security in power systems include information security, infrastructure security, and control security. Besides the IT network, generations and other equipments are also connected to the grid, and most of them are centrally controlled. Supervisory Control and Data Acquisition (SCADA), and Energy Management System (EMS), and Generation Management System (GMS) are used in the electricity industry to supervise, control, optimize, and manage the generation and transmission systems [6]. Software tools are used by Regional Transmission Organizations (RTOs) and Independent System Operators (ISOs) in electricity markets to optimally commit and dispatch generation resources to meet demands.

Two-settlement market model dominates the electricity markets in the U.S. It includes day-ahead market (DAM) and real-time market (RTM) [7]. Settlements are performed at each market seperately. In DAM, RTOs/ISOs run Security-Constrained Unit Commitment (SCUC) to determine the optimal generation schedule for the next day based on the data in the SCADA/EMS/GMS [8]. The solution respects system constraints, such as load balance constraints, reserve requirement and transmission capacity limits, as well as unit-wise

This work is supported in part by DOE grants DE-FC26-08NT02875 and DE-OE-0000449. The authors are with the Robert W. Galvin Center for Electricity Innovation at Illinois Institute of Technology, Chicago, IL 60616, USA. (e-mail: hye9@hawk.iit.edu; yge9@hawk.iit.edu; xliu108@hawk.iit.edu; lizu@iit.edu).

constraints such as generation capacity constraints, minimum on/off time requirement, ramping up/down rate limits. In RTM, which is also called balance market, energy imbalance is managed by solving rolling SCUC and Security-Constrained Economic Dispatch (SCED). The majority of the market is cleared in DAM based on Locational Marginal Price (LMP), and deviations between DAM and RTM are settled according to ex-post real-time LMPs [9], [10].

Transmission network in DAM is not always the same as that in RTM. The difference could be status change due to the unforeseen line outages in the grid although transmission owners usually inform RTOs/ISOs the scheduled outages in advance. The difference could also be transmission line rating (TLR) change due to weather or other operating conditions. For example, the effective TLRs for lines within a system, especially those near the geographical border of the system, may vary due to the changes of external power flows. As stated in [11], [12], the changes of TLRs are not rare in the PJM market as well as in other markets. So, attackers can manipulate the effective TLRs via false external power flow information. Attackers may also compromise sensors and send false TLRs to the SCADA/EMS. It is also possible that attackers may change the TLRs in the SCADA/EMS database directly.

In this paper, we demonstrate that attackers are able to gain economic benefits by attacking a limited number of TLRs in the two-settlement markets. The contributions of this paper are:

1) The TLR attack is formulated as a bi-level optimization model, in which the objective of the attacker is to maximize the profit of arbitrage between the two-settlement electricity market.
2) The bi-level model is converted into a single-level mixed integer linear programming (MILP) problem using KKT-based approach and Big-M method in [13]. However, the Big-M method is computationally expensive [14]–[16]. Although sophisticated general cutting planes are employed in modern MILP solvers [17]–[19], the performance is generally poor due to the Big-M coefficient of binary variables when the problem size is large. To achieve better computation performance, tight bound is used in [16]. An effective techique to tighten the coefficients for a class of formulation is presented in [20]. In this paper, we have explored the special structure of the problem, and developed several high performance cutting planes. We have also proposed a technique to reduce the number of binary variables, which helps the solver to exclude non-optimal binary combinations in advance. Simulation results show that these techniques can reduce computational burden tremendously.
3) To our best knowledge, we are the first to analyze the multiplicity issue of LMPs due to cyber attacks. We also address the issue via a heuristic method that effectively mitigates the degeneration cases of linear programming.
4) The uncertainties of loads is modeled into the TLR attack problem. Stochastic approach is employed to obtain the maximum expected profit from an attacker's point of view.

A. Related Work

The issue of cyber attack in power system has attracted a lot of attentions in recent years [15], [21]–[25]. Researchers have proposed false data injection attack models against state estimation in [21]. By acknowledging the grid information, the attacker may manipulate system operating point obtained by state estimation software. [21] shows that traditional state estimation in power system is vulnerable. Protection strategies against the false data attacks are proposed in [26] under some circumstances.

Authors in [15], [24] proposed load redistribution attack against state estimation. The false load injection attack respecting power flow equations is difficult to detect. In [27], the authors analyzed economic impacts of injecting false load data. Studies in [15], [24], [27] focus on the false load injections. Recently, [23] studied the impacts by real-time price signal attack in electricity market with price-sensitive loads, and authors in [25] reported the attack of introducing the ramping data in the SCADA database.

The rest of paper is organized as follows. In Section II, the TLR attack model is formulated. The acceleration techniques of solving the resulting MILP problem are presented in Section III. The multiplicity of LMP is discussed in Section IV. The model considering load uncertainties is discussed in Section V. In Section VI, the case study is presented. We conclude the paper in Section VII.

II. Model of Transmission Line Rating Attack

It is assumed in this paper that the attacker has the full knowledge of the system including system load, generation cost information, unit output limits, and network information and can manipulate a limited number of TLRs.

A. Objective and Constraints of TLR Attack

As DAM is a forward market, the energy consumed and produced is not necessarily the same as that in RTM. It is inevitable that generations and loads in RTM will deviate from those in DAM. The deviations lead to LMP differences between DAM and RTM as well as profit uncertainties, which pose financial risk for market participants. Virtual transactions are introduced as financial instruments to hedge these risks. They include virtual Increment offers (INC) and Decrement bids (DEC). INC behaves like dispatchable generation and DEC behaves like price-sensitive demand in the market. Market participants submit the INCs (DECs) in DAM, and collect (pay) money based on day-ahead LMP ϕ_{DA} according to the cleared amount. The exact amount of cleared INCs and DECs must be purchased (sold) back later based on real-time LMP ϕ_{RT} in RTM. INCs and DECs are included in the LMP calculation in DAM, but not in RTM. Virtual transactions are used to improve the convergences between DAM and RTM, and promote the market liquidity as pure finical products. More details can also be found in [9], [28], [29].

Different from generation and price-sensitive load, the amount of virtual transaction is not impacted by the changes of energy pricing in RTM. The profit of a market participant from virtual transaction is

$$\left(\boldsymbol{\phi_{RT}} - \boldsymbol{\phi_{DA}}\right)^\top \boldsymbol{v}, \tag{1}$$

where day-ahead LMP $\boldsymbol{\phi_{DA}}$ is determined in DAM. $\boldsymbol{v}$ is the virtual transaction vector, and its dimension is the number of buses. The real time LMP $\boldsymbol{\phi_{RT}}$ is a function of generation, transmission, and load data. Once the TLR data is compromised, the energy pricing can be manipulated. Let $\boldsymbol{\phi_{RT}}(\hat{\boldsymbol{r}})$ and $\boldsymbol{\phi_{RT}}(\boldsymbol{r})$ denote the LMPs before and after the TLR attack, respectively. $\hat{\boldsymbol{r}}$ is the true TLR vector while $\boldsymbol{r}$ is the compromised one. The change of profit due to the TLR attack is

$$\Big(\boldsymbol{\phi_{RT}}(\boldsymbol{r}) - \boldsymbol{\phi_{RT}}(\hat{\boldsymbol{r}})\Big)^\top \boldsymbol{v}. \tag{2}$$

Note that $\boldsymbol{\phi_{RT}}(\boldsymbol{r})$ is the only variable in (2) and is a step function of $\boldsymbol{r}$ based on the sensitivity analysis theory [30]. Also if a generator owner launches the attack, the change of its profit can be formulated as

$$\boldsymbol{\phi}_{\boldsymbol{RT}}^\top(\boldsymbol{r})\Big(\boldsymbol{p}(\boldsymbol{r}) - \boldsymbol{p_{DA}}\Big) - \boldsymbol{\phi}_{\boldsymbol{RT}}^\top(\hat{\boldsymbol{r}})\Big(\boldsymbol{p}(\hat{\boldsymbol{r}}) - \boldsymbol{p_{DA}}\Big),$$

where $\boldsymbol{\phi}_{\boldsymbol{RT}}^\top(\boldsymbol{r})\boldsymbol{p}(\boldsymbol{r})$ is a quadratic term, and the awarded $\boldsymbol{p}$ is also a function of $\boldsymbol{r}$. In this case, the problem becomes more complicated. For simplicity, we only consider attacks from entities engaging in virtual transactions in this paper to illustrate the market impacts of TLR attacks.

For practical reasons, we assume that the changes of TLRs are within given limits to avoid being detected and the attacker has limited resources to change TLRs. Particularly, if the protective device, such as relay, is not compromised for line, the upper bound of TLR must be limited below the pickup level of the relay. Otherwise, the response of the protection system to line overloading, such as line tripping, can increase the risk of the attack being detected. In this paper, the resource constraints of TLR attack is modeled as

$$\begin{cases} \hat{r}_l - (\hat{r}_l - \underline{r}_l)y_l \leq r_l \leq \hat{r} + (\bar{r}_l - \hat{r}_l)y_l, \forall l & (3) \\ \displaystyle\sum_l y_l \leq S, & (4) \end{cases}$$

where y_l is the indicator of TLR of line l being changed. $\underline{r}_l$ and $\bar{r}_l$ represent the lower and upper bounds of changed TLR r_l for line l. Constraint (3) indicates whether the TLR of a line is compromised, and (4) means the attack is constrained by the limited resources. The number of compromised lines must be less than S. Coefficients can be added in (4) to represent other types of constraints, such as cost constraint.

B. Bi-level and MILP Formulations for TLR Attack

The TLR attack problem can be formulated as a bi-level optimization problem

$$\begin{aligned} &\max_{\boldsymbol{r}} \varphi && (5) \\ &\text{s.t. } \varphi \leq \left(\boldsymbol{\phi_{RT}} - \boldsymbol{\phi_{DA}}\right)^\top \boldsymbol{v} && (6) \\ &\qquad \boldsymbol{\phi_{RT}} = \lambda \boldsymbol{1} + \boldsymbol{\Gamma}^\top \left(-\boldsymbol{\mu}^+ + \boldsymbol{\mu}^-\right) && (7) \\ &\qquad (3-4) && \\ &\text{and } (\lambda, \boldsymbol{\mu}^+, \boldsymbol{\mu}^-) \in \operatorname*{argmin}_{\boldsymbol{p}} z && (8) \\ &\qquad \text{s.t. } z \geq \boldsymbol{c}^\top \boldsymbol{p} && (9) \\ &\qquad \boldsymbol{1}^\top \boldsymbol{p} = \boldsymbol{1}^\top \boldsymbol{d} \qquad \lambda && (10) \\ &\qquad -\boldsymbol{r} \leq \boldsymbol{\Gamma}\left(\boldsymbol{K_p p} - \boldsymbol{K_d d}\right) \leq \boldsymbol{r} \qquad \boldsymbol{\mu}^-, \boldsymbol{\mu}^+ && (11) \\ &\qquad \underline{\boldsymbol{p}} \leq \boldsymbol{p} \leq \overline{\boldsymbol{p}} \qquad \boldsymbol{\beta}^-, \boldsymbol{\beta}^+. && (12) \end{aligned}$$

The upper-level problem (3-7) is to maximize the profit where TLR vector $\boldsymbol{r}$ is the decision variable. The price $\boldsymbol{\phi_{RT}}$ is obtained based on the dual solution to the lower-level problem, which is the SCED performed by ISOs/RTOs when the TLR is changed. Equation (6) represents the attacker's profit of arbitraging between RTM and DAM via virtual transaction vector $\boldsymbol{v}$. The term $\boldsymbol{\phi}_{\boldsymbol{DA}}^\top \boldsymbol{v}$ is constant and determined in DAM. LMPs formulation is presented in (7) where λ, $\boldsymbol{\mu}^+$ and $\boldsymbol{\mu}^-$ are the Lagrangian multipliers for constraints (10) and (11) and $\boldsymbol{\Gamma}$ is the shift factor matrix. The attack resource limits are (3-4). In the lower-level problem, the ISO/RTO minimizes the total operation cost (8), respecting generation/load balance constraint (10), line flow limits (11), and generation limits (12). $\boldsymbol{d}$ is the load vector and $\boldsymbol{p}$ is the generation vector.

The lower-level problem is a linear programming (LP) problem, which is convex. Hence, the Karush-Kuhn-Tucker (KKT) conditions are the sufficient and necessary conditions of the optimality. This bi-level problem is then converted into a single-level linear problem with linear complementary constraints (LPCC) [14], [31].

$$\begin{aligned} &\max_{\boldsymbol{r}} \varphi && (13) \\ &\text{s.t. } (6-7), (3-4), (10-12) && \\ &\qquad \boldsymbol{c} + \boldsymbol{K}_{\boldsymbol{p}}^\top \boldsymbol{\Gamma}^\top (\boldsymbol{\mu}^+ - \boldsymbol{\mu}^-) + \boldsymbol{\beta}^+ - \boldsymbol{\beta}^- + \lambda \boldsymbol{1} = \boldsymbol{0} && (14) \\ &\qquad \mu_l^+ \left(\boldsymbol{\Gamma}\left(\boldsymbol{K_p p} - \boldsymbol{K_d d}\right) - \boldsymbol{r}\right)_l = 0, \forall l && (15) \\ &\qquad \mu_l^- \left(-\boldsymbol{\Gamma}\left(\boldsymbol{K_p p} - \boldsymbol{K_d d}\right) - \boldsymbol{r}\right)_l = 0, \forall l && (16) \\ &\qquad \beta_i^+ \left(p_i - \bar{p}_i\right) = 0, \forall i && (17) \\ &\qquad \beta_i^- \left(-p_i + \underline{p}_i\right) = 0, \forall i && (18) \\ &\qquad \boldsymbol{\mu}^+, \boldsymbol{\mu}^-, \boldsymbol{\beta}^+, \boldsymbol{\beta}^- \geq \boldsymbol{0}, && (19) \end{aligned}$$

where $\mu_l^+, \mu_l^-, \beta_i^+$ and β_i^- are entries in vector $\boldsymbol{\mu}^+, \boldsymbol{\mu}^-, \boldsymbol{\beta}^+$ and $\boldsymbol{\beta}^-$. The complementary slackness constraints (15)-(18) are nonlinear. Due to the nonconvexity, a problem with this type of constraints is normally hard to solve. Big-M method is employed to linearize these complementary constraints exactly [13], [16]. By choosing a proper M, modern MILP solver can be used to solve the problem. For example, constraint (17) is converted into a linear form as

$$\begin{cases} -M(1 - g_i^+) \leq p_i - \bar{p}_i, \forall i, \\ 0 \leq \beta_i^+ \leq M g_i^+, \forall i, \\ g_i^+ \in \{0, 1\}, \forall i, \end{cases}$$

where M is a big enough constant and g_i^+ is the indicator of $p_i = \bar{p}_i$. If $g_i^+ = 1$, then it can be observed that $\beta_i^+ \leq Mg^+$ is redundant, and the first constraint is equivalent to $p_i - \bar{p}_i = 0$ since $p_i - \bar{p}_i \leq 0$. Similarly, it can be shown that the above constraints are equivalent to $\beta_i^+ = 0$ if $g_i^+ = 0$. As the big constant M is introduced, it is called Big-M method in literatures. We can tighten M for constraints (11) and (12) in this paper to improve the solution performance. By using Big-M method, the constraints (11-12) (15-19) are reformulated as

$$-2r_l\left(1-b_l^+\right) \le f_l - r_l \le 0, \forall l \tag{20}$$

$$-2r_l\left(1-b_l^-\right) \le -f_l - r_l \le 0, \forall l \tag{21}$$

$$(\underline{p}_i - \bar{p}_i)(1-g_i^+) \le p_i - \bar{p}_i \le 0, \forall i \tag{22}$$

$$(\underline{p}_i - \bar{p}_i)(1-g_i^-) \le -p_i + \underline{p}_i \le 0, \forall i \tag{23}$$

$$0 \le \mu_l^+ \le Mb_l^+, 0 \le \mu_l^- \le Mb_l^-, \forall l \tag{24}$$

$$0 \le \beta_i^+ \le Mg_i^+, 0 \le \beta_i^- \le Mg_i^-, \forall i \tag{25}$$

$$b_l^+ + b_l^- \le 1, g_i^+ + g_i^- \le 1, \forall l, i \tag{26}$$

$$b_l^+, b_l^-, g_i^+, g_i^- \in \{0,1\}, \forall i, l, \tag{27}$$

where $f_l = \boldsymbol{\Gamma}_{l\bullet}(\boldsymbol{K_p p} - \boldsymbol{K_d d})$ and $\boldsymbol{\Gamma}_{l\bullet}$ is shift factor row for line l. b_l^+, b_l^- and g_i^- are indicators of f_l reaching r_l, $-r_l$ and p_i reaching $\underline{p}_i$ respectively.

So far, we can formulate the TLR attack model as a single-level MILP problem (OP) by substituting constraints (11-12)(15-19) with constraints (20-27).

$$\begin{aligned} \text{(OP)} \quad & \max_{\boldsymbol{r}} \quad \varphi \\ & \text{s.t.} \quad (6-7), (10), (3-4), \\ & \qquad\; (14), (20-27). \end{aligned}$$

III. Acceleration Techniques for TLR Attack Model

The MILP problem formulated in section II is computationally intractable [14]. In order to reduce the computational burden, we propose several acceleration techniques in this section. The first technique is to generate strong valid cuts, or called cutting planes, that fully take advantage of the special structure of the MILP problem. The second technique is to reduce the number of binary variables as the computational burden increases in a non-polynomial fashion with the number of binary variables and with the introduction of Big-M in the MILP problem.

A. Addition of Strong Valid Cuts

Modern MILP solvers such as CPLEX and GUROBI employ sophisticated branch and cutting method to solve the MILP problem. However, cutting planes such as Gomory and Cover cuts used in those solvers are for general MILP problems, and do not consider the special structure of the problem (OP). In this section, we develop special strong valid cuts exploring the structure of the MILP-based TLR attack problem in order to accelerate the solution process. The basic idea of applying the cutting plane is illustrated in Fig. 1. The black dots are the feasible integer points and the gray dot is the optimal point. By adding an effective cutting plane, the upper left area is excluded. Strong cutting plane can shrink the feasible region without losing the optimal point [18]. The major challenge of cutting plane methods is how to construct effective cutting planes for a specific problem [18], [19].

In problem (OP), the strong duality condition (i.e. the objective values of primal and dual problems are the same) is not explicitly listed. Here we develop four sets of necessary optimality conditions that explore the strong duality condition, which can accelerate the computation. The values of the primal and dual objective functions are restricted within an interval by these necessary conditions, therefore the gap between them never exceeds that interval.

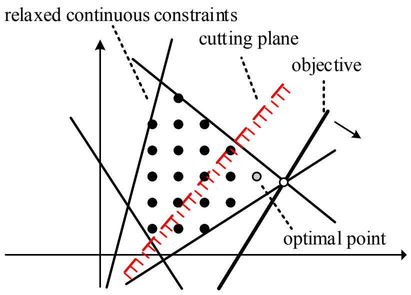


Fig. 1. Illustration of Cutting Plane

Theorem 1. *Let $z(\boldsymbol{r})$, $\underline{\boldsymbol{r}}$ and $\bar{\boldsymbol{r}}$ denote the optimal value of the lower-level SCED problem, lower and upper bounds of $\boldsymbol{r}$ respectively. Assume SCED is feasible at $\boldsymbol{r} = \underline{\boldsymbol{r}}$ and $\boldsymbol{r} = \bar{\boldsymbol{r}}$. Then the following inequalities*

$$z(\bar{\boldsymbol{r}}) \le z(\boldsymbol{r}) \le z(\underline{\boldsymbol{r}}), \tag{28}$$

always hold.

Proof is presented in Appendix A. The lower bound $z(\bar{\boldsymbol{r}})$ and upper bound $z(\underline{\boldsymbol{r}})$ of the operation cost can be obtained with little efforts by solving two LP problems. According to (28), the optimal point to the primal SCED problem must respect

$$\begin{cases} -\boldsymbol{c}^\top \boldsymbol{p} + z(\bar{\boldsymbol{r}}) \le 0 & (29) \\ \boldsymbol{c}^\top \boldsymbol{p} - z(\underline{\boldsymbol{r}}) \le 0. & (30) \end{cases}$$

Inequalities (29-30) constrain the generation $\boldsymbol{p}$ in the set near the optimal points. They are two strong valid cuts for problem (OP).

The optimal point to the dual problem of the lower-level SCED also respects

$$\begin{aligned} & z(\bar{\boldsymbol{r}}) \\ \le & -\lambda \boldsymbol{1^T d} + (-\boldsymbol{\mu}^+ + \boldsymbol{\mu}^-)^\top \boldsymbol{\Gamma K_d d} \\ & - (\boldsymbol{\mu}^+ + \boldsymbol{\mu}^-)^\top \boldsymbol{r} + \underline{\boldsymbol{p}}^\top \boldsymbol{\beta}^- - \bar{\boldsymbol{p}}^\top \boldsymbol{\beta}^+ \\ \le & \; z(\underline{\boldsymbol{r}}), \end{aligned} \tag{31}$$

where $\lambda, \boldsymbol{\mu}^+, \boldsymbol{\mu}^-, \boldsymbol{\beta}^+$ and $\boldsymbol{\beta}^-$ are Lagrangian multipliers when TLR is $\boldsymbol{r}$. Equation (31) holds for $\forall \boldsymbol{r} \in [\underline{\boldsymbol{r}}, \bar{\boldsymbol{r}}]$ and the associated Lagrangian multipliers. With (29), (30), and (31), the gap between dual and primal objective function values is limited below $z(\underline{\boldsymbol{r}}) - z(\bar{\boldsymbol{r}})$. However, the term $(\boldsymbol{\mu}^+ + \boldsymbol{\mu}^-)^\top \boldsymbol{r}$ is nonlinear and cannot be added into a MILP solver directly.

Theorem 2. *Equations*

$$\begin{cases} z(\bar{\boldsymbol{r}}) \le -\lambda \boldsymbol{1}^\top \boldsymbol{d} + (-\boldsymbol{\mu}^+ + \boldsymbol{\mu}^-)^\top \boldsymbol{\Gamma K_d d} & \\ \qquad - (\boldsymbol{\mu}^+ + \boldsymbol{\mu}^-)^\top \underline{\boldsymbol{r}} + \underline{\boldsymbol{p}}^\top \boldsymbol{\beta}^- - \bar{\boldsymbol{p}}^\top \boldsymbol{\beta}^+ & (32) \\ z(\underline{\boldsymbol{r}}) \ge -\lambda \boldsymbol{1}^\top \boldsymbol{d} + (-\boldsymbol{\mu}^+ + \boldsymbol{\mu}^-)^\top \boldsymbol{\Gamma K_d d} & \\ \qquad - (\boldsymbol{\mu}^+ + \boldsymbol{\mu}^-)^\top \bar{\boldsymbol{r}} + \underline{\boldsymbol{p}}^\top \boldsymbol{\beta}^- - \bar{\boldsymbol{p}}^\top \boldsymbol{\beta}^+ & (33) \end{cases}$$

are necessary conditions of (31) .

Proof is presented in Appendix B. Theorem 2 provides another two strong valid cuts for problem (OP). These two inequalities regarding the dual problem constrain the Lagrangian multipliers near the optimal points. If the SCED problem is infeasible at $\boldsymbol{r} = \underline{\boldsymbol{r}}$, then $z(\underline{\boldsymbol{r}}) = \infty$. In fact, $z(\underline{\boldsymbol{r}})$ and $z(\bar{\boldsymbol{r}})$ can be replaced with any tighter bounds according to the available resources to the attacker.

Another two cutting planes can be derived for the binding indicators of the generation limit constraints. It is easy to show that there exists an integer $1 \le k_1 \le N_g$, such that

$$\begin{cases} \sum_{m=1}^{k_1-1} \bar{p}_{i_m} \le \mathbf{1}^\top \boldsymbol{d} \le \sum_{m=1}^{k_1} \bar{p}_{i_m} \\ \bar{p}_{i_1} \le \bar{p}_{i_2} \cdots \le \bar{p}_{i_{N_g}}. \end{cases} \tag{34}$$

Based on equation (34), the following cutting plane

$$\sum_i g_i^+ \le k_1. \tag{35}$$

is obtained. k_1 is an upper bound for the summation of g_i^+.

We can also get the upper bound for the summation of g_i^-. Let $q_i = \bar{p}_i - \underline{p}_i$, the following inequality constraints

$$\begin{cases} \sum_{m=1}^{k_2-1} q_{i_m} \le \mathbf{1}^\top \boldsymbol{d} - \sum_{i=1}^{N_g} \underline{p}_i < \sum_{m=1}^{k_2} q_{i_m} \\ q_{i_1} \le q_{i_2} \cdots \le q_{i_{k_2}} \cdots \le q_{i_{N_g}} \end{cases} \tag{36}$$

must hold for integer k_2, where $1 \le k_2 \le N_g$. Then, a cutting plane for the lower bound indicators of generation limits

$$\sum_{i=1}^{N_g} g_i^- \le k_2 - 1 \tag{37}$$

holds. The computational burden to get integer k_1 in (35) and integer k_2 in (36) is very small.

In this section, we developed cutting planes (29-30), (32-33), (35), (37).

B. Reduction of Binary Variables

In order to linearize the complementary constraints (15-18), the auxiliary binary variables b_l^+, b_l^-, g_i^+, and g_i^- are introduced in (20-27). These variables indicate whether the original constraints are binding for the SCED problem at the optimal point. In practice, many of the these constraints are always inactive. As shown in [32], a large number of those inactive security constraints can be identified easily. For convinience, the conclusion in [32] is presented as follows. If

$$\begin{cases} \sum_{m=1}^{k-1} \bar{p}_{i_m} \le \mathbf{1}^\top \boldsymbol{d} < \sum_{m=1}^{k} \bar{p}_{i_m} \\ \sum_{m=1}^{k-1} (\Gamma_{l,i_m}^g - \Gamma_{l,i_k}^g)\bar{p}_{i_m} + \Gamma_{l,i_k}^g \mathbf{1}^\top \boldsymbol{d} < r_l - \boldsymbol{\Gamma}_{\boldsymbol{l\cdot}} \boldsymbol{K_d d} \\ \Gamma_{l,i_1}^g \ge \Gamma_{l,i_2}^g \ge \cdots \ge \Gamma_{l,i_{N_g}}^g \end{cases} \tag{38}$$

holds for integer k, then the forward direction constraint for line l is inactive. Γ_{l,i_m}^g is the coefficient for generator i_m and line l in $\boldsymbol{\Gamma}$, also called generation shift factor sometimes.

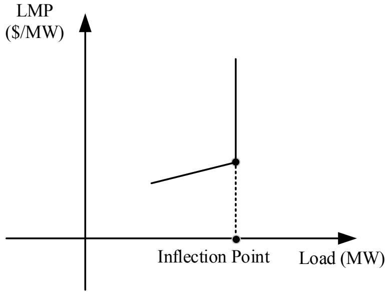


Fig. 2. Multiplicity of LMP

In this paper, the TLR r_l is not a constant anymore. Hence, we substitute r_l with the lower bound $\underline{r}_l$ in (38), and get a necessary condition

$$\begin{cases} \sum_{m=1}^{k-1} \bar{p}_{i_m} \le \mathbf{1}^\top \boldsymbol{d} < \sum_{m=1}^{k} \bar{p}_{i_m} \\ \sum_{m=1}^{k-1} (\Gamma_{l,i_m}^g - \Gamma_{l,i_k}^g)\bar{p}_{i_m} + \Gamma_{l,i_k}^g \mathbf{1}^\top \boldsymbol{d} < \underline{r}_l - \boldsymbol{\Gamma}_{\boldsymbol{l\cdot}} \boldsymbol{K_d d} \\ \Gamma_{l,i_1}^g \ge \Gamma_{l,i_2}^g \ge \cdots \ge \Gamma_{l,i_{N_g}}^g \end{cases} \tag{39}$$

to identify the inactive constraints. If the network constraint for line l is always inactive, the corresponding binary variable b_l^+ is fixed to 0. Similarly, the binary variable b_l^- can also be preprocessed. In the following sections, we denote the possible binding line set as J. Those inactive network constraints can be eliminated from the lower-level SCED problem without affecting the optimal point.

IV. Multiplicity Issue of LMP

Besides the intractable computational burden, the issue of multiplicity in pricing is another difficulty in the TLR attack model. The LMP is a natural byproduct of the SCED problem, and it is a closed form function of the dual solution. Most modern solvers also provide the dual solution while the primal problem is solved. Under the normal circumstances, ISOs/RTOs can get a unique price at each node. Multiplicity of LMP occurs when the degenerated basic solution exists [33]. In the degenerated case, there are multiple dual solutions even if the primal optimal point is unique. In fact, the degenerated cases are not uncommon in LP problem. Shadow prices (i.e. dual variables) under these circumstances are not unique.

Fig. 2 illustrates an example of the LMP multiplicity at some node. Once the load reaches the inflection point, multiple optimal points to the dual problem of SCED exist. Then the uniqueness of LMP is lost at the specific load level as shown in Fig. 2. The LMP multiplicity may be very rare if electricity bids, offers, network parameters, and ancillary services requirement are given. However, the chances of multiplicity increase once any of those information is to be determined. Different ISOs/RTOs may have different strategies of selecting a fair shadow price in the optimal dual solution pool when there are multiple prices. It is not easy for an attacker to model the strategies in the TLR attack problem.

Another critical drawback in model (5-12) is that the dual solution in the optimal point pool that results in larger profit is always picked up. In practice, the chance of the attacker gaining that profit is very small. This is because the likelihood of ISOs/RTOs calculating LMPs based on the same dual solutions as the attacker is extremely low when multiple dual solutions are available. In a special case, if there exists TLR $\boldsymbol{r}$ which leads to unbounded profit φ in (5), then that particular $\boldsymbol{r}$ is always a good solution candidate to problem (OP). It is noted that problem (OP) becomes bounded with large φ when the artificial upper bound "Big-M" for the dual variables is set, and some dual solutions reach "Big-M". Although the unreasonable large profit φ is an optimal value to (OP), the attacker would never gain that profit.

In this section, a heuristic way to address the LMP multiplicity issue is proposed. When a degenerated solution exists, it means that the number of binding constraints of the optimization problem at the optimal point is larger than the number of variables [30]. In this case, we establish necessary conditions for non-degeneracy as

$$\begin{cases} \sum_{l} (b_l^+ + b_l^-) + \sum_{i} \left(g_i^+ + g_i^-\right) \leq N_g - 1, & (40) \\ -r_l + \epsilon(1 - b_l^-) \leq f_l \leq r_l - \epsilon(1 - b_l^+), l \in J, & (41) \end{cases}$$

where (40) guarantees no more than N_g constraints in (10-12) are active at the optimal points, and forces the original free dual variables to be zero due to constraint (24). And $r_l - |f_l|$ is larger than a small constant ϵ when $b_l^+ = 0$ or $b_l^- = 0$ in (41) . The above condition, although not a sufficient condition, excludes most of the degenerated solutions in our simulations.

V. Uncertainty of Load and Generation

In practical system, the load and generation in RTM may deviate from those in DAM, especially with the renewable energy and price-sensitive load. Forecasting errors are inevitable even if the state-of-art technology is employed. Hence, both the ISOs/RTOs and attackers cannot predict exactly the level of load and generation. So far, stochastic and robust optimization techniques have been applied successfully in the SCUC problem to address the uncertainty issue [34]–[36].

As shown in [36], generation variation can be modeled as negative load in the SCED problem from a mathematic point of view. In this paper, we assume that the probability distribution function (PDF) of the uncertain load is available to both ISOs/RTOs and attackers. The scenario-based stochastic optimization approach is employed to solve the SCED problem considering uncertainties. The uncertain load is modeled as

$$\underline{d}_n \leq d_n \leq \bar{d}_n, n \in \Theta, \tag{42}$$

where Θ is the index set of uncertain loads.

The objective of the attacker is to maximize the profit of the virtual transactions by manipulating LMPs in RTM. However, the loads at some nodes are not determined at the moment of designing the attack vector. Based on the PDF information, several scenarios are generated with the probability of scenario j being π_j [34]. Then the objective of the attacker is to maximize the profit expectation of the virtual transactions based on these scenarios.

The new MILP problem is expressed as

$$\begin{aligned}
\text{(STP)} \max_{\boldsymbol{r}} \quad & z & (43)\\
\text{s.t.} \quad & z \leq \sum_j \pi_j (\boldsymbol{\phi_{RT,j}} - \boldsymbol{\phi_{DA}})^\top \boldsymbol{v} & (44)\\
& \boldsymbol{\phi_{RT,j}} = \lambda_j \mathbf{1} + \boldsymbol{\Gamma}^\top \left(-\boldsymbol{\mu_j^+} + \boldsymbol{\mu_j^-}\right), \forall j & (45)\\
& \mathbf{1}^\top \boldsymbol{p_j} = \mathbf{1}^\top \boldsymbol{d_j}, \forall j & (46)\\
& \boldsymbol{f_j} = \boldsymbol{\Gamma} \left(\boldsymbol{K_p p_j} - \boldsymbol{K_d d_j}\right), \forall j & (47)\\
& \mu_{l,j}^+ \left(f_{l,j} - r_l\right) = 0, \forall l, j & (48)\\
& \mu_{l,j}^- \left(f_{l,j} + r_l\right) = 0, \forall l, j & (49)\\
& \beta_{i,j}^+ \left(p_{i,j} - \bar{p}_i\right) = 0, \forall i, j & (50)\\
& \beta_{i,j}^- \left(-p_{i,j} + \underline{p}_i\right) = 0, \forall i, j & (51)\\
\boldsymbol{c} + \boldsymbol{K_p}^\top \boldsymbol{\Gamma}^\top & (\boldsymbol{\mu_j^+} - \boldsymbol{\mu_j^-}) + \boldsymbol{\beta_j^+} - \boldsymbol{\beta_j^-} + \lambda_j \mathbf{1} = \mathbf{0}, \forall j & (52)\\
& \underline{\boldsymbol{p}} \leq \boldsymbol{p_j} \leq \overline{\boldsymbol{p}}, \forall j & (53)\\
& \underline{\boldsymbol{r}} \leq \boldsymbol{r} \leq \bar{\boldsymbol{r}} & (54)\\
& \lambda_j, \boldsymbol{\mu_j^+}, \boldsymbol{\mu_j^-}, \boldsymbol{\beta_j^+}, \boldsymbol{\beta_j^-} \geq \mathbf{0}, \boldsymbol{\forall j}, & (55)
\end{aligned}$$

where subscript j represents the variable(s) in scenario j. Problem STP is a large-scale LPCC problem with a computational burden much larger than that of problem (OP). Note that the techniques developed in III are still applicable.

VI. Case Study

The TLR attacks are simulated in this section using the modified IEEE 14-Bus and IEEE 118-Bus testing systems. Simulations on the IEEE 14-Bus system illustrate the basic ideas presented in this paper. And the IEEE 118-Bus system is employed to show the effectiveness of the proposed acceleration techniques. It is performed on Intel Xeon E7340@2.40GHz 64GB RAM using GUROBI 5.6.3 [17].

A. Modified IEEE 14-Bus Testing System

The one-line diagram of the modified IEEE 14-Bus system is shown in Fig 3. There are 5 generators and 11 loads in the system. All the 14 nodes are connected by 20 transmission lines. The original data can be found at [37], and a modified version is used in this paper. The transmission line data are presented in Table I. And Table II lists other data including lower/upper limits of generator outputs, fuel cost, load, and virtual transactions. The positive and negative values for virtual transaction refer to sale and purchase, respectively. It is assumed that unit commitment is determined in advance, and all the units in the system are committed. Generation and load information is assumed accurate. Three cases are tested:

1) Case 1: Single incremental costs of generators are used.
2) Case 2: Stepwise incremental costs of generators are used.
3) Case 3: Several lines are protected and cannot be compromised.

1) Case 1: The TLR vector is constrained by $\boldsymbol{r} \in [\hat{\boldsymbol{r}} - 0.15\hat{\boldsymbol{r}}, \hat{\boldsymbol{r}} + 0.15\hat{\boldsymbol{r}}]$. The simulation results are presented in Table III. In the base case, no TLR attack vector is injected (i.e. $S = 0$). The LMPs reflect the true value of the power at each node. Line 1 and line 4 are binding in this case,

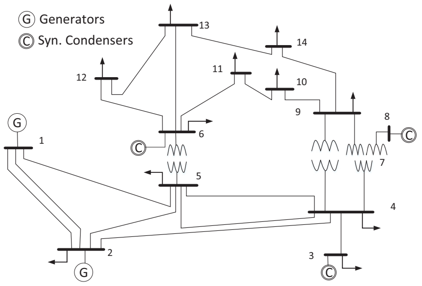


Fig. 3. IEEE 14-Bus Testing System.

TABLE I
TRANSMISSION LINE DATA FOR IEEE 14-BUS SYSTEM

from	to	reactance	rating (MW)
1	2	0.05917	120
1	5	0.22304	45
2	3	0.19797	70
2	4	0.17632	30
2	5	0.17388	80
3	4	0.17103	60
4	5	0.04211	55
4	7	0.20912	30
4	9	0.55618	50
5	6	0.25202	90
6	11	0.1989	50
6	12	0.25581	30
6	13	0.13027	60
7	8	0.17615	50
7	9	0.11001	50
9	10	0.0845	100
9	14	0.27038	20
10	11	0.19207	60
12	13	0.19988	50
13	14	0.34802	20

TABLE II
GENERATION AND LOAD DATA FOR IEEE 14-BUS SYSTEM

bus	$\underline{p}$ (MW)	$\bar{p}$(MW)	I.C.*	$\boldsymbol{d}$(MW)	$\boldsymbol{v}$(MW)	a **	b **	c **
1	40	200	30.327	0	0	0.043	20	0
2	30	140	62.5	52.87	0	0.25	20	0
3	15	90	41.05	177.6	25	0.01	40	0
4	0	0	0	38.85	0	0	0	0
5	0	0	0	19.98	0	0	0	0
6	20	120	31.4	17.45	0	0.01	30	0
7	0	0	0	0	0	0	0	0
8	20	110	36.3	0	0	0.01	35	0
9	0	0	0	27.75	-30	0	0	0
10	0	0	0	21.65	10	0	0	0
11	0	0	0	8.33	0	0	0	0
12	0	0	0	14.99	0	0	0	0
13	0	0	0	33.3	0	0	0	0
14	0	0	0	36.63	0	0	0	0

* \$/MW ** \$/MW^2, \$/MW, \$. Cost at level p is $ap^2 + bp + c$.

and the market participant collects \$231.87 for the virtual transactions. Lagrangian multipliers for the binding lines are small. Hence, the LMP differences of the three nodes where the virtual transactions occur are also small. The largest LMP is \$41.05 at bus 3, and the smallest LMP is \$39.63 at bus 10.

TABLE III
CASE 1 RESULT FOR 14-BUS SYSTEM*

S	profits(\$)	comp. line	binding line	ϕ_{RT3}**	ϕ_{RT9}**	ϕ_{RT10}**
0	231.87	-	1, 4	41.05	39.69	39.63
1	2146.90	17	2, 17	77.30	8.00	45.48
2	5804.10	7, 17	7, 17	153.80	-67.00	-5.07
3	5804.10	3, 7, 17	7, 17	153.80	-67.00	-5.07
10	5804.10	7, 17, others	7, 17	153.80	-67.00	-5.07

* $\Delta r = 0.15\hat{r}$; ** \$/MW

The second row in Table III shows that the attacker can gain much more profit by compromising just one TLR. The profit is increased from \$231.87 to \$2146.9. The TLR attack occurs on line 17, whose TLR is decreased by 2.982 MW. The SCED problem is performed again according to the false TLR. At the optimal point, line 2 and line 17 become binding, and line 1 and line 4 are no longer binding. It demonstrates that it is not necessary to change the TLR of one line directly if the attacker wants to alter the binding status of that line. Instead, it can be achieved by TLR changes of other line(s) due to loop flow and the optimality of the dispatch. Almost half of the profits gained by the attack comes from bus 3 and bus 10. The LMP drops to \$8.00/MWh from \$39.69/MWh at bus 9, where energy is to be purchased back in RTM. In comparison, LMP at bus 3 soars to \$77.3/MWh from \$41.05/MWh, where energy is to be sold. It indicates that the small change of critical TLRs can manipulate the LMPs a lot. Consequently, the attacker may have enough incentives to launch a TLR attack.

The third row in Table III lists the attack results of $S = 2$. By decreasing the TLRs of line 7 and line 17 by 7.6248 MW and 2.3289 MW, respectively, the attacker can gain \$5804 in RTM, which is almost 25 times of the original profit. In this case, the LMPs at bus 9 and bus 10 are negative. It means the attacker pays money for the energy "sold" at bus 10 and collects money for the energy "purchased" at bus 9. An interesting point is that the attacker is trying to maximize the total profit although it loses money at bus 10. The profits remain the same when S increases from 3 to 7 as shown in Table III. The attacker's profit increases monotonically with its available resources. But after a threshold (i.e. $S = 2$), the attacker does not have extra benefits by using more resources.

2) Case 2: In this case, the piecewise linear cost model is used to approximate generators' quadratic cost curves. Accordingly, the incremental cost curves are stepwise. The single incremental cost model in Case 1 is a special case of the stepwise incremental cost model where $N_w = 1$. In Case 2, the incremental costs are different at various generation levels for the same unit. As a result, the LMPs vary more in comparison with the single incremental cost model. Table IV presents the profits the attacker gain when different stepwise incremental cost models are used. It shows that the maximum profits are attained when $S = 2$ and line 7 and line 17 are attacked no matter how many pieces are used to approximate the cost curves. The largest profit is \$5804 when $N_w = 1$ and $S \geq 2$. The second largest profit \$4389 is achieved when $N_w = 7$ and $S \geq 2$. Hence, it is observed that the profits do not increase monotonically with N_w.

In Case 2, the degeneracy issues are observed and effectively addressed by adding (40-41) to the model. And a

TABLE IV
CASE 2 RESULT FOR 14-BUS SYSTEM ($)

S	$N_w = 1$	$N_w = 3$	$N_w = 5$	$N_w = 7$	$N_w = 9$
0	231.87	224.22	189.53	155.74	159.63
1	2,146.9	779.99	575.13	471.07	480.47
2	5,804.15	2,480.52	3,809.97	4,389.15	3,372.85
3	5,804.15	2,480.52	3,809.97	4,389.15	3,372.85
4	5,804.15	2,480.52	3,809.97	4,389.15	3,372.85
5	5,804.15	2,480.52	3,809.97	4,389.15	3,372.85

TABLE V
CASE 3 RESULT FOR 14-BUS SYSTEM ($)

S	$N_w = 1$	$N_w = 3$	$N_w = 5$	$N_w = 7$	$N_w = 9$
0	231.87	224.22	189.53	155.74	159.63
1	366.09	236.24	252.5	261.18	159.63
2	366.09	243.88	288.18	261.18	269.21
3	366.09	243.88	288.18	265.3	274.96
4	366.09	243.88	288.18	265.3	274.96

good choice of ϵ also helps to avoid the numerical challenge. It is set to 1×10^{-5} in this paper. Consider the scenario with $N_w = 5$ and $S = 3$. Without constraints (40-41), the profit calculated is $246,159 when $M = 1 \times 10^5$. The profit increases to $24,543,398 with $M = 1 \times 10^7$. Obviously, this is impossible in practice. These profits are obtained with degenerated solutions, and multiplicity of pricing occurs. In fact, the profit is unbounded in two directions. It could be any number from $-\infty$ to ∞. As an attacker, a possible strategy is to avoid the degeneracy since the profits are unknown and the abnormal LMP increases the risk of the attack being detected. The profits listed in Table IV are obtained using the strategy in section IV. It should be noted that multiple optimal TLRs to problem (OP) may exist. For example, if the line flow constraint for l is supposed to be inactive and $r_l \neq \hat{r}_l$ at the optimal point, then any r'_l satisfying $\bar{r}_l \geq r'_l > r_l$ is also optimal as it doesn't change LMPs and the optimal value.

3) Case 3: From the results in Case 2, it is observed that line 7 and line 17 are favorable to the attacker. The largest profits are obtained by attacking these two lines. In this case, line 7 and line 17 are protected, so the attacker cannot manipulate their TLRs. Table V shows that the maximum profit that can be achieved is only $366 when $S = 2$ and $N_w = 1$. In other situations, the profits are less than $300. The minimal value of the profit is $243.88, which means the attacker only gains $20 more by changing the TLRs. Thus, the system operator can effectively mitigate the impact of the TLR attack by protecting line 7 and line 17.

4) Acceleration Techniques: Computational burden for the IEEE 14-Bus system is small, and the corresponding problems can be solved in 1s. As the improvement is neglectable, the main purpose of using this system here is to illustrate the basic idea. Detailed benchmark testing is presented in the next section. The necessary conditions of optimality related to generation levels are formulated as

$$15,655.5 \leq \sum_{i=1}^{5} c_i p_i \leq 19,872.2,$$

where 19,872.2 is a tighter upper bound than $z(\underline{\boldsymbol{r}}) = \infty$. It is obtained by dispatching the most expensive generations meeting the load demand, which is an upper bound to the optimal point. The other two necessary optimality conditions in (32-33) can be obtained as

$$\begin{aligned} & 15,655.5 + \sum_{l=1}^{20} \underline{r}_l(\mu_l^+ + \mu_l^-) \\ \leq \quad & -449.38\lambda + \sum_{l=1}^{20} \tau_l(-\mu_l^+ + \mu_l^-) + \sum_{i=1}^{5} \underline{p}_i \beta_i^- - \bar{p}_i \beta_i^+ \\ \leq \quad & 19,872.2 + \sum_{l=1}^{20} \bar{r}_l(\mu_l^+ + \mu_l^-), \end{aligned}$$

where $\tau_l = (\boldsymbol{\Gamma K_d d})_l$ is the l^{th} entry in $\boldsymbol{\Gamma K_d d}$. The cutting plane corresponding to (35) is

$$g_1^+ + g_2^+ + g_3^+ + g_4^+ + g_5^+ \leq 3.$$

According to the data in Table II, we have

$$q_1 = 160, q_2 = 110, q_3 = 75, q_4 = 100, q_5 = 90.$$

Then the following sequence

$$q_3 < q_5 < q_4 < q_2 < q_1$$

is obtained, and $k_2 = 3$. Hence, we can generate a cutting plane

$$g_1^- + g_2^- + g_3^- + g_4^- + g_5^- \leq 2$$

corresponding to (37). From the two cutting planes generated above, it can be seen that at most three upper generation limits can be reached simultaneously, and no more than two generators will reach their lower generation limits at the same time.

As discussed in Section III, the line flow binding binary variables for lines whose flow limit constraints will not be binding can be eliminated. Based on the inactive condition shown in (39), we can reduce the number of line flow binding binary variables from 40 to 14. The remaining ones are $b_1^+, b_2^+, b_3^+, b_4^+, b_5^+, b_8^+, b_{10}^+, b_{13}^+, b_{15}^+, b_{17}^+, b_6^-, b_7^-, b_8^-$ and b_{14}^-. The number of binary combinations decreases to 2^{14} from 2^{40} by eliminating the binary variables that can be fixed at zero.

B. IEEE 118-Bus Testing System

The IEEE 118-Bus testing system consists of 54 generators, 186 transmission lines, and 91 loads. The detailed data including generator capacities and cost curves, line reactances and ratings, and load profiles can be found at http://motor.ece.iit.edu/Data/.

In this section, we mainly focus on evaluating the computational performance of the acceleration techniques introduced in Section III, especially for the scenario-based stochastic model considering load uncertainties. The set of uncertain loads are $\Theta = \{1, 5, 7, 10, 12, 13, 15, 16, 50, 60, 80\}$. The confidence interval of load is $[0.8d_n, 1.2d_n]$. Simulations are performed with different number of scenarios from 1 to 6 using the MILP solver GUROBI. The original MILP problem has 2080 constraints and 1272 variables for one scenario. The numbers

TABLE VI
COMPUTATION BENCHMARK FOR IEEE 118-BUS SYSTEM

#	Origi.		W/ Eli.		W/ Cut.		W/ E.&C.	
	time(s)	gap(%)	time(s)	gap(%)	time(s)	gap(%)	time(s)	gap(%)
1	0.95	4.46	0.33	3.23	0.25	2.34	0.17	0.33
2	8.42	3.91	2.98	1.78	0.83	0.99	0.45	4.61
3	65.03	1.21	27.31	2.41	1.52	3.52	0.63	2.04
4	657.47	4.43	51.48	2.83	16.7	3.69	3.52	1.7
5	4628.63	2.49	836.73	2.04	21.09	1.58	6.89	4.92
6	7200.08	12.36	1931.94	2.18	11.48	4.07	14.39	3.15

of constraints and variables increase to 10615 and 5772 respectively if 6 scenarios are included.

Table VI presents the computation time and solution quality when different approaches are used. The time limit for the MILP solver is set to 2 hours, and the gap is set to 5%. The parameter "NumericFocus" is set to 3 to avoid numerical issues. The first column lists the number of scenarios conisdered. The second and third columns show the results obtained based on the original approach without applying any acceleration techniques. The 4th and 5th columns list the performance of the approach with binary variables and inactive constraints elimination. The approach including strong cutting planes are presented in the 6th and 7th columns. The last two columns present results for the approach with both binary variables elimination and cutting planes.

It is observed that the computation time increases extremely nonlinearly with the number of scenarios. The original approach is interrupted due to the 2-hour limit, and the relative gap of the solution obtained is 12.36% with 6 scenarios. It is observed that the binary variables elimination technique can effectively reduce the computation time when the number of scenarios is large. The time is reduced to less than half when the number of scenarios is 3, and the advantages are more obvious with larger number of scenarios. Data in the 6th and 7th columns show that cutting planes further reduce the computation time tremendously. When the number of scenarios is 5, the approach using cutting planes reduces the computation time to 21s from 836s and with smaller gap. By adding cutting planes, the third and fourth approaches have overwhelming advantages over the original approach and the binary variables elimination only approach. For example, the computation time is less than 15 seconds in the case with 6 scenarios, which is only 0.725% that of the second approach. The advantages are due largely to the cuts (29-30) and (32-33). These cuts dramatically reduce the computational burden of the MILP by providing a good search area in advance.

VII. CONCLUSION

An attacker can gain more profit from virtual transactions in the two-settlement markets by solving a bi-level optimization problem, where the LMPs in RTM are manipulated via false TLR vector injection. Simulation results show that the profit gain could be very large, so the attacker may have enough incentives to launch a TLR attack. In order to accelerate the computation, several techniques are developed. The benchmark testing results on the modified IEEE 118-Bus system validate their effectiveness. A heuristic strategy to address the multiplicity of pricing is proposed in this paper. We are working on an exact approach that can resolve the multiplicity issue. The research on how to protect the transmission network against TLR attack is also ongoing. The market impact of transmission line status attack is another interesting topic being investigated.

APPENDIX A

Let $\chi(\boldsymbol{r})$ denote the feasible set of generation vector $\boldsymbol{p}$ when the TLR vector is $\boldsymbol{r}$ in the SCED problem (8-12). $\chi(\underline{\boldsymbol{r}}) \subseteq \chi(\boldsymbol{r}) \subseteq \chi(\bar{\boldsymbol{r}})$ follows as $\underline{\boldsymbol{r}} \leq \boldsymbol{r} \leq \bar{\boldsymbol{r}}$ holds for any $\boldsymbol{r}$ in (11). The minimal objective value corresponding to a feasible set is always not greater than that to its subset, so (28) holds.

APPENDIX B

Let $\eta(\boldsymbol{\mu}^+, \boldsymbol{\mu}^-, \boldsymbol{\beta}^+, \boldsymbol{\beta}^-)$ denote

$$(-\boldsymbol{\mu}^+ + \boldsymbol{\mu}^-)^\top \boldsymbol{\Gamma} \boldsymbol{K_d d} + \underline{\boldsymbol{p}}^\top \beta^- - \bar{\boldsymbol{p}}^\top \beta^+ - \lambda \boldsymbol{1^T d},$$

then equation (31) can be rewritten into

$$z(\bar{\boldsymbol{r}}) \leq \eta(\boldsymbol{\mu}^+, \boldsymbol{\mu}^-, \boldsymbol{\beta}^+, \boldsymbol{\beta}^-) - (\boldsymbol{\mu}^+ + \boldsymbol{\mu}^-)^\top \boldsymbol{r} \leq z(\underline{\boldsymbol{r}}). \quad (56)$$

Equations (32-33) in Theorem 2 can also be rewritten as

$$\begin{cases} z(\bar{\boldsymbol{r}}) \leq \eta(\boldsymbol{\mu}^+, \boldsymbol{\mu}^-, \boldsymbol{\beta}^+, \boldsymbol{\beta}^-) - (\boldsymbol{\mu}^+ + \boldsymbol{\mu}^-)^\top \underline{\boldsymbol{r}} & (57) \\ z(\underline{\boldsymbol{r}}) \geq \eta(\boldsymbol{\mu}^+, \boldsymbol{\mu}^-, \boldsymbol{\beta}^+, \boldsymbol{\beta}^-) - (\boldsymbol{\mu}^+ + \boldsymbol{\mu}^-)^\top \bar{\boldsymbol{r}} & (58) \end{cases}$$

Comparing equations (56-58), Theorem 2 is proved as long as

$$(\boldsymbol{\mu}^+ + \boldsymbol{\mu}^-)^\top \underline{\boldsymbol{r}} \leq (\boldsymbol{\mu}^+ + \boldsymbol{\mu}^-)^\top \boldsymbol{r} \leq (\boldsymbol{\mu}^+ + \boldsymbol{\mu}^-)^\top \bar{\boldsymbol{r}}. \quad (59)$$

holds. We have

$$\mu_l^+ + \mu_l^- \geq 0, \bar{r}_l - r_l \geq 0, \forall l \quad (60)$$

so the product of two left hand sides in (60) is still non-negative

$$(\mu_l^+ + \mu_l^-)(\bar{r}_l - r_l) \geq 0, \forall l. \quad (61)$$

Hence

$$(\mu_l^+ + \mu_l^-)\bar{r}_l \geq (\mu_l^+ + \mu_l^-) r_l, \forall l. \quad (62)$$

Therefore, the second inequality in (59)

$$\begin{aligned} (\boldsymbol{\mu}^+ + \boldsymbol{\mu}^-)^\top \bar{\boldsymbol{r}} &= \sum_l (\mu_l^+ + \mu_l^-)\bar{r}_l \\ \geq \quad & \sum_l (\mu_l^+ + \mu_l^-) r_l = (\boldsymbol{\mu}^+ + \boldsymbol{\mu}^-)^\top \boldsymbol{r} \end{aligned}$$

is valid. The first inequality in (59) can also be proved similarly. Hence, Theorem 2 is proved.

REFERENCES

[1] H. Farhangi, "The path of the smart grid," *IEEE Power Energy Mag.*, vol. 8, no. 1, pp. 18–28, 2010.

[2] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart gridthe new and improved power grid: A survey," *Communications Surveys & Tutorials, IEEE*, vol. 14, no. 4, pp. 944–980, 2012.

[3] S. M. Amin and B. F. Wollenberg, "Toward a smart grid: power delivery for the 21st century," *IEEE Power Energy Mag.*, vol. 3, no. 5, pp. 34–41, 2005.

[4] F. M. Cleveland, "Cyber security issues for advanced metering infrastructure (ami)," in *Power and Energy Society, General Meeting IEEE*, 2008, pp. 1–5.

[5] G. N. Ericsson, "Cyber security and power system communicationessential parts of a smart grid infrastructure," *IEEE Trans. Power Del.*, vol. 25, no. 3, pp. 1501–1507, 2010.

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

[7] M. Shahidehpour, H. Yamin, and Z. Li, *Market Operations in Electric Power Systems-Forecasting, Scheduling and Risk Management*. John Wiley & Sons, 2002.

[8] H. Wu, X. Guan, Q. Zhai, and H. Ye, "A systematic method for constructing feasible solution to SCUC problem with analytical feasibility conditions," *IEEE Trans. Power Syst.*, vol. 27, no. 1, pp. 526–534, 2012.

[9] A. L. Ott, "Experience with PJM market operation, system design, and implementation," *IEEE Trans. Power Syst.*, vol. 18, no. 2, pp. 528–534, 2003.

[10] T. Zheng and E. Litvinov, "On ex post pricing in the real-time electricity market," *IEEE Trans. Power Syst.*, vol. 26, no. 1, pp. 153–164, 2011.

[11] "PJM options to address FTR underfunding," PJM, Tech. Rep., 2012.

[12] "FTR revenue stakeholder report," PJM, Tech. Rep., Apr. 2012.

[13] J. Fortuny-Amat and B. McCarl, "A representation and economic interpretation of a two-level programming problem," *Journal of the operational Research Society*, pp. 783–792, 1981.

[14] J. Hu, J. E. Mitchell, J.-S. Pang, and B. Yu, "On linear programs with linear complementarity constraints," *Journal of Global Optimization*, vol. 53, no. 1, pp. 29–51, 2012.

[15] Y. Yuan, Z. Li, and K. Ren, "Modeling load redistribution attacks in power systems," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 382–390, Jun. 2011.

[16] V. Gabrel, M. Lacroix, C. Murat, and N. Remli, "Robust location transportation problems under uncertain demands," *Discrete Applied Mathematics*, 2011.

[17] I. Gurobi Optimization, *Gurobi Optimizer Reference Manual*, 2014. [Online]. Available: http://www.gurobi.com

[18] G. L. Nemhauser and L. A. Wolsey, *Integer and combinatorial optimization*. Wiley New York, 1988, vol. 18.

[19] H. Marchand, A. Martin, R. Weismantel, and L. Wolsey, "Cutting planes in integer and mixed integer programming," *Discrete Applied Mathematics*, vol. 123, no. 1, pp. 397–446, 2002.

[20] F. Qiu, S. Ahmed, S. S. Dey, and L. A. Wolsey, "Covering linear programming with violations," *INFORMS Journal on Computing*, vol. 26, no. 3, pp. 531–546, Aug. 2014.

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

[22] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious Data Attacks on Smart Grid State Estimation: Attack Strategies and Countermeasures," in *IEEE International Conference on Smart Grid Communications*, 2010.

[23] R. Tan, V. Badrinath Krishna, D. K. Yau, and Z. Kalbarczyk, "Impact of integrity attacks on real-time pricing in smart grids," in *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*. New York, NY, USA: ACM, 2013, pp. 439–450.

[24] Y. Yuan, Z. Li, and K. Ren, "Quantitative analysis of load redistribution attacks in power systems," *IEEE Trans. Parallel and Distrib. Syst.*, vol. 23, no. 9, pp. 1731–1738, 2012.

[25] D.-H. Choi and L. Xie, "Ramp-induced data attacks on look-ahead dispatch in real-time power markets," *IEEE Trans. Smart Grid*, vol. 4, no. 3, pp. 1235–1243, 2013.

[26] T. Kim and H. Poor, "Strategic protection against data injection attacks on power grids," *Smart Grid, IEEE Transactions on*, vol. 2, no. 2, pp. 326–333, June 2011.

[27] L. Xie, Y. Mo, and B. Sinopoli, "Integrity data attacks in power market operations," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 659–666, Dec. 2011.

[28] "Virtual transactions in the midwest ISO markets," accessed: 2014-10-01. [Online]. Available: http://www.misostates.org/files/WorkGroups/VirtualPrimerOMS041709_1.pdf

[29] "California ISO - convergence bidding," accessed: 2014-10-01. [Online]. Available: http://www.caiso.com/1807/1807996f7020.html

[30] D. Bertsimas and J. Tsitsiklis, *Introduction to Linear Optimization*, 1st ed. Athena Scientific, 1997.

[31] U.-P. Wen and S.-T. Hsu, "Linear bi-level programming problems – a review," *The Journal of the Operational Research Society*, vol. 42, no. 2, pp. 125–133, Feb. 1991.

[32] Q. Zhai, X. Guan, J. Cheng, and H. Wu, "Fast identification of inactive security constraints in SCUC problems," *IEEE Trans. Power Syst.*, vol. 25, no. 4, pp. 1946–1954, 2010.

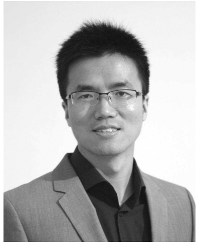
[33] W. W. Hogan, "Multiple market-clearing prices, electricity market design and price manipulation," *The Electricity Journal*, vol. 25, no. 4, pp. 18–32, 2012.

[34] L. Wu, M. Shahidehpour, and Z. Li, "Comparison of scenario-based and interval optimization approaches to stochastic scuc," *IEEE Trans. Power Syst.*, vol. 27, no. 2, pp. 913–921, May 2012.

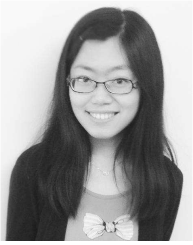
[35] D. Bertsimas, E. Litvinov, X. Sun, J. Zhao, and T. Zheng, "Adaptive robust optimization for the security constrained unit commitment problem," *IEEE Trans. Power Syst.*, vol. 28, no. 1, pp. 52–63, Feb 2013.

[36] R. Jiang, M. Zhang, G. Li, and Y. Guan, "Two-stage network constrained robust unit commitment problem," *European Journal of Operational Research*, 234 (3), 751-762, 2014.

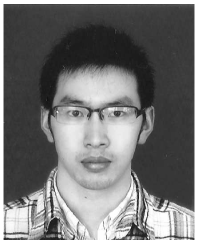
[37] "IEEE 14-Bus test case," http://www.ee.washington.edu/research/pstca, accessed: 2014-08-28.



Hongxing Ye (S'14) received his B.S. degree and M.S. degree from Xi'an Jiaotong University, China in 2007 and 2011, both in electrical engineering. He is currently working toward the Ph.D. degree at the Illinois Institute of Technology, Chicago. His research interests include optimization, economic operation and security analysis of power system.



Yinyin Ge (S'14) received her B.S. degree and M.S. degree from Xi'an Jiaotong University, China in 2008 and 2011, both in electrical engineering. She is currently a Ph.D. candidate of Electrical Engineering at Illinois Institute of Technology in Chicago. Her research interests are power system optimization and modeling, Smart Grid and power system stability and control.



Xuan Liu (S'14) received the B.S. and M.S degrees from Sichuan University, China, in 2008 and 2011, respectively. He is currently working toward the Ph.D. degree in the Electrical and Computer Engineering Department, Illinois Institute of Technology. His research interests include smart grid security, operation and economics of power systems.

Zuyi Li (SM'09) received the B.S. degree from Shanghai Jiaotong University, Shanghai, China, in 1995, the M.S. degree from Tsinghua University, Beijing, China, in 1998, and the Ph.D. degree from the Illinois Institute of Technology (IIT), Chicago, in 2002, all in electrical engineering. Presently, he is a Professor in the Electrical and Computer Engineering Department at IIT. His research interests include economic and secure operation of electric power systems, cyber security in smart grid, renewable energy integration, electric demand management of data centers, and power system protection.