# Financially Motivated FDI on SCED in Real-Time Electricity Markets: Attacks and Mitigation

Chensheng Liu, *Student Member, IEEE*, Min Zhou, *Student Member, IEEE*, Jing Wu, *Member, IEEE*, Chengnian Long, *Member, IEEE*, and Deepa Kundur, *Fellow, IEEE*

***Abstract*—Given the strong cyber-physical coupling that exists in power systems today and of the future, false data injection (FDI) attacks have been shown to be feasible in tampering measurement devices by exploiting cyber vulnerabilities to mislead state estimation and related applications. For example, a corrupt generator owner, motivated by financial gain, may manipulate meter readings associated with short-term load forecasts and *subsequently misguide* the decisions of security constrained economic dispatch (SCED) in *ex-ante* real-time markets. In this paper, we analyze the feasibility of financially motivated FDI attacks in bi-level programming settings where multi-solution uncertainty of SCED is considered. To deter such attacks, a robust *incentive-reduction* strategy is proposed that can prevent financially motivated FDI attacks for all the possible load distributions and solutions of SCED requiring a minimal number of protected meters. Simulations for the IEEE 14-bus and IEEE 30-bus test systems demonstrate attack feasibility and performance of the proposed mitigation strategy for SCED in real-time markets.**

***Index Terms*—Power system security, cyber-physical systems, security constrained economic dispatch.**

## I. Introduction

RECENT advancements in the integration of information systems such as sensing and communication technologies in power systems, are rapidly improving their reliability and efficiency [1] at the expense of increased vulnerabilities to cyberattack. For instance, authentication weaknesses and vulnerabilities in communication protocols [2] enable false data injection (FDI) attacks whereby an opponent can tamper power system meter readings and subsequently mislead state estimation (SE) and related applications without being detected by bad data detection (BDD) methods [3].

A two-settlement electricity market has been widely adopted by regional transmission organizations (RTOs) such as Pennsylvania-New Jersey-Maryland (PJM), which includes day-ahead and (ex-ante and ex-post) real-time markets. To meet the expected load, provided by a very short term load predictor (VSTLP) program [4], while respecting transmission security constraints with minimal cost, security constrained economic dispatch (SCED) is applied in the *ex-ante* real-time markets 10 to 15 min prior to real time [5]. As VSTLP employs real-time telemetry data to generate load forecasts [4], FDI attackers have opportunities to misguide SCED by compromising the meter readings and manipulating the load forecast results. In addition, execution of such an attack by a corrupt generator owner (adversary) can lead to financial gain in real-time markets whereby the adversary sells more energy to the grid than the results of SCED would legitimately compute. Hence, one primary goal of this paper is to explore the feasibility of financially motivated FDI attacks and associated countermeasures in protecting SCED in real-time markets.

FDI attacks have been extensively studied in power systems since it was first proposed by Liu *et al.* in [3]. A significant body of work has focused on FDI for SCED. For example, a special class of FDI attacks called a *load redistribution attack* has been investigated to maximize immediate [6], [7] and delayed operational cost [8], and to overload transmission lines [9]; the primary goal of these proposed attacks is to negatively impact the operation of power systems. Financially motivated FDI attack has also been studied in the context of SCED in ex-post real-time markets, where SCED is conducted in real time to obtain locational marginal price (LMP) for settlement purposes. For example, adversaries, such as generator owners, load serving entities, and third parties, have been shown to fiscally benefit by tampering with congestion patterns [5], [10], topology data [11], and transmission line rates [12] of SCED used in calculating LMP. In contrast to strategies that compromise SCED in the calculation of LMP to benefit, in this paper, we investigate how adversaries can mislead the decisions of SCED in *ex-ante* real-time markets for financial gain. Specifically, previous financially motivated FDI attacks mislead state estimation and SCED in the LMP module as shown in Fig. 1, while the proposed FDI attack manipulates the load forecast of VSTLP to misguide SCED decisions in the unit dispatch system (in *ex-ante* real-time markets), which has the potential to significantly affect the actual generation outputs and potentially benefit adversaries in real-time markets. Hence, our novel approach adds to the existing body of research in FDI for SCED to demonstrate the wide variety of approaches available for financial gain.

Manuscript received March 26, 2017; revised August 8, 2017 and November 6, 2017; accepted December 10, 2017. Date of publication December 18, 2017; date of current version February 18, 2019. This work was supported in part by the National Nature Science Foundation under Grant 61673275 and Grant 61473184, in part by China Scholarship Council, and in part by the National Science and Engineering Research Council of Canada. Paper no. TSG-00420-2017. *(Corresponding authors: Jing Wu; Chengnian Long.)*

C. Liu, M. Zhou, J. Wu, and C. Long are with the Department of Automation, Shanghai Jiao Tong University, and the Key Laboratory of System Control and Information Processing, Ministry of Education of China, Shanghai 200240, China (e-mail: jingwu@sjtu.edu.cn; longcn@sjtu.edu.cn).

D. Kundur is with the Department of Electrical and Computer Engineering, University of Toronto, Toronto, ON M5S 3G4, Canada (e-mail: dkundur@ece.utoronto.ca).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSG.2017.2784366

To deter FDI attacks in power systems, critical-meter protection strategies have been widely investigated in both SE and related applications. For example, a general protection strategy is designed for SE by analyzing the topology [13], [14] or measurement matrix [15] of power systems such that the security of SE can be ensured by protecting a set of basic measurements. In this work, we argue however that even with such protection strategies an adversary can still tamper with the load and generator measurements (without affecting SE) and subsequently misguide SCED when generators and loads connect to the same bus. Moreover, other critical-meter protection strategies have been developed with the goal of exceeding the preset number of attacked meters [16], [17], or minimizing the operational cost [18]. However, such approaches have limited applicability, and we assert do not apply to the scenario considered in this paper wherein the defender's objective (e.g., to minimize the attacker's additional benefit) is affect by multi-solution uncertainty of SCED and the load uncertainty in power systems. Hence, it is important to design a robust protection strategy account for an attacker's specific objective, multi-solution uncertainty and load uncertainty.

Thus, in this paper, we design a robust "incentive-reduction" strategy for protecting critical meters by first analyzing the best adversarial attack strategy. Specifically,

- We define and analyze a financially motivated FDI attack on SCED in *ex-ante* real-time markets, where adversaries can mislead the decision of SCED by manipulating the load forecast of VSTLP.
- We provide a robust mitigation strategy to deter financially motivated FDI attacks taking multi-solution and load uncertainty into consideration, which can prevent such attacks for all the possible load and solutions of SCED with a minimal number of protected meters.
- We design a heuristic "incentive-reduction" algorithm for the tri-level robust defender-attacker-operator programming that can significantly reduce the complexity of finding the minimal set of protected meters for the mitigation of financially motivated FDI attacks.

The remainder of this paper is organized as follows. In Section II, we present SCED model and the threat models. The best FDI attack for adversaries is analyzed in Section III. A robust mitigation strategy for financially motivated FDI attack in SCED is designed in Section IV followed by numerical simulations and conclusions in Sections V and VI, respectively.

## II. SYSTEM MODEL

### A. Notation

We denote the power system under consideration as $(N, A)$ where $N$ is the set of buses and $A$ is the set of transmission lines. Let $N^d \subseteq N$, $N^g \subseteq N$, and $N^a \subseteq N$ be the set of buses connected to load(s), legitimate (i.e., uncorrupt) generator(s) and corrupt generator(s), respectively. Throughout this paper, we assume that attacks start at time $t$ to manipulate the load forecast and subsequently misguide the desired generation output at time $t_+$, where $t$ is 10 to 15 min prior to $t_+$ [5]. Variables with "$\Delta$" denote injected attack data, overline (underline) denotes maximum (minimum) value, hat denotes the legitimate forecast values, and tilde denotes compromised/misguided values. For example, $P^d$ is the real measurement at time $t$, $\hat{P}^d$ is the legitimate load forecast at time $t_+$, and $\tilde{P}^d$ is the misguided load forecast at time $t_+$. Moreover, variables with subscripts, $i$, $j$, $k$, or $\ell$, refer to scalar elements of the corresponding vector variable, typically representing the particular value for a corresponding bus or transmission line. For example, $\Delta P^g$ represents the injected attack vector on overall generator measurements while $\Delta P_i^g$ is specifically the injected attack data in the measurement of the generator at Bus $i$. For ease of reference, nomenclature is provided in Table I.

TABLE I
VARIABLE NOTATION

| Notation | Definition |
|---|---|
| $P^g$ | Generators' measurements at time $t$ or scheduled output at $t_+$. |
| $P^a$ | Corrupt generators' measurements at $t$ or scheduled output at $t_+$. |
| $P^d$ | Load measurements at time $t$. |
| $P^f$ | Transmission lines' power flows. |
| $S_{\ell,i}$ | Shift factor between line $\ell$ and Bus $i$. |
| $c_i^g$ | Bid price or marginal cost of generator at Bus $i$. |
| $c_j^a$ | Bid price or marginal cost of corrupt generator at Bus $j$. |
| $p_j$ | Locational marginal price at Bus $j$. |
| $\delta_i^\times$ | Inductor of attacked meter, $\times$ refers to sensor types. |
| $\sigma_i^\times$ | Inductor of protected meter, $\times$ refers to sensor types. |
| $M$ | Sufficiently large positive constant. |
| $\mathcal{D}$ | All the possible load in SCED. |
| $\mathcal{S}$ | All the possible protected set. |
| $\mathcal{G}(\cdot)$ | Solution set of $P^g$ and $P^a$ in SCED. |
| $\mathcal{A}(\cdot)$ | All the possible attack vector given protected set and load. |
| $\mathscr{C}(\cdot)$ | Generation cost of SCED. |
| $\mathscr{U}(\cdot)$ | Attacker's financial benefit. |
| $\mathscr{U}'(\cdot)$ | Attacker's additional financial benefit. |

### B. SCED Under FDI Attacks

We consider SCED in *ex-ante* real-time electricity markets, where the output of legitimate generators and the corrupt generators are dispatched to meet the load forecast demands. Given the compromised load forecast $\tilde{P}^d$ at time $t_+$, SCED solves the following *SCED problem* (SCEDP) [5]:

$$\text{SCEDP:} \min_{\tilde{P}^g, \tilde{P}^a} \sum_{i \in N^g} c_i^g \cdot \tilde{P}_i^g + \sum_{j \in N^a} c_j^a \cdot \tilde{P}_j^a \tag{1}$$

$$s.t. \sum_{i \in N^g} \tilde{P}_i^g + \sum_{j \in N^a} \tilde{P}_j^a = \sum_{k \in N^d} \tilde{P}_k^d(\lambda) \tag{2}$$

$$\underline{P}_i^g \leq \tilde{P}_i^g \leq \overline{P}_i^g \quad \forall i \in N^g \quad \left(\underline{\omega}_i, \overline{\omega}_i\right) \tag{3}$$

$$\underline{P}_j^a \leq \tilde{P}_j^a \leq \overline{P}_j^a \quad \forall j \in N^a \quad \left(\underline{\mu}_j, \overline{\mu}_j\right) \tag{4}$$

$$-\overline{P}_\ell^f \leq \tilde{P}_\ell^f \leq \overline{P}_\ell^f \quad \forall \ell \in A \left(\underline{\nu}_\ell, \overline{\nu}_\ell\right) \tag{5}$$

$$\tilde{P}_\ell^f = \sum_{i \in N^g} S_{\ell,i} \cdot \tilde{P}_i^g + \sum_{j \in N^a} S_{\ell,j} \cdot \tilde{P}_j^a - \sum_{k \in N^d} S_{\ell,k} \cdot \tilde{P}_k^d \quad \forall \ell \in A, \tag{6}$$

where all the variables $\tilde{P}^g$, $\tilde{P}^a$, and $\tilde{P}^f$ are the desired or scheduled values at time $t_+$, $c_i^g$ and $c_j^a$ are the bid prices [19] or marginal cost,[1] (2) is the necessary power supply-demand balance, (3) and (4) are generation capacity constraints.

[1]Competitive forces of markets are relied upon to "drive" bids in SCED down to their marginal cost under a bid-based regime [21].

Equation (5) represents transmission line thermal constraints, where the power flow on the $\ell$th transmission line, $\tilde{P}^f_\ell$, is determined by (6). $\lambda$, $\underline{\omega}_i$, $\overline{\omega}_i$, $\underline{\mu}_j$, $\overline{\mu}_j$, $\underline{\nu}_\ell$, $\overline{\nu}_\ell$ are Lagrange multipliers corresponding to the constraints above. $S_{\ell,i}$ in (6) is a shift factor representing the increase of power flow in the $\ell$th line, when the output of generator at Bus $i$ increases by 1 p.u. [20]. Since $S_{\ell,i}$ for each bus may be distinct, SCED decisions for distinct load distributions (with a same total load) may be different.

Denote the set of possible load values, satisfying (2)-(6), as $\mathcal{D}$. We assume for any given load measurements $P^d \in \mathcal{D}$, the forecast load $\hat{P}^d$ based on $P^d$ satisfies $\hat{P}^d \in \mathcal{D}$; hence, a solution for SCED exists for any load in $\mathcal{D}$. For a given load $P^d \in \mathcal{D}$, SCED may have multiple solutions, mathematically. To design a robust protection strategy for all possibilities in $\mathcal{D}$ and solutions of SCED, we analyze the best adversarial attack strategy in the following sections.

### *C. Financially Motivated FDI Attacks*

To obtain an unfair advantage in SCED (e.g., sell more energy to the grid than the results of SCED would legitimately compute), corrupt generator owners are motivated to manipulate the load forecast of the VSTLP by tampering meter readings, and subsequently misguide SCED decisions *stealthily*. The reader should note that stealth is an important attack characteristic as it enables long-term financial gain.

Hence, to design a robust protection strategy, we analyze the best adversarial SCED attack strategy and make the following assumptions: 1) Attackers have full information of SCED objectives, constraints [12], the current measurements, and VSTLP. 2) Attackers can only tamper with unprotected measurements. 3) Attackers can only modify at most $n$ sensor measurements (specifically, load, generators, power flow, and corrupt generators' output), and no control command or pricing data. The first assumption is justified because marginal cost, dominated by fuel cost, can be easily estimated. Network parameters, used to calculate shift factor, can be estimated from measurements using independent component analysis [22] or subspace estimation [23]. The lower/upper bound of generation capacity and power flow on transmission lines can be estimated from the minimal/maximal generation output and power flow on transmission lines in history measurements. In addition, the current measurements can be gleaned from plaintext communication or by exploiting cryptographic weaknesses [24]. Moreover, adversaries can glean insight into the method used in VSTLP from disclosed information, e.g., a Kalman estimator-based method applied to power system operated by the Bonneville Power Administration is disclosed in [25]. Assumption 2 is reasonable as we can assume that the electric power utility employs effective mechanisms of protection when applied [16]. The final assumption is consistent with FDI threat models, i.e., *limited resource to compromise meters*, in [3].

Based on the threat model above, an FDI attacker can misguide the SCED decisions via the following steps (see also Fig. 1): 1) To manipulate the load forecast at time $t_+$, adversaries compromise the load measurements at time $t$.

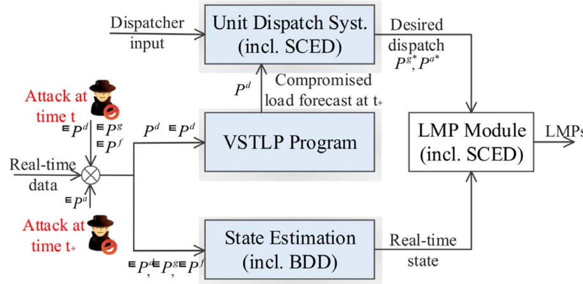



Fig. 1. The steps of financially motivated FDI attacks on SCED.

2) As SE is used to monitor the real-time operation of power systems [20], adversaries must compromise generator measurements, and power flows at time $t$ to camouflage the modification of the load measurements (i.e., to avoid being detected by BDD in SE). The measurements of corrupt generators are not modified at time $t$ to be consistent with the last scheduled output. 3) To accurately match physical supply with the real load forecast at $t_+$, the actual outputs of the corrupt generators may be different from the (compromised) scheduled values. Adversaries must modify the measurements of the corrupt generators at time $t_+$ to mask the actual generation output.

Given that LMP changes only when the estimated states are moved far enough into another congestion pattern region [26], [27], we analyze the financially motivated FDI attack in *ex-ante* real-time markets without considering the effect on LMP in this paper. We assume that LMP at Bus $j$ is $p_j$. We model the relationship between the measurement of load at time $t$ and the load forecast at time $t_+$ as a linear map, e.g., similar day method used in very short term load forecast [28], for simplicity. For a given load measurement $P^d$ at time $t$, i.e., $\hat{P}^d = F \cdot P^d$, adversaries solve the following *financially motivated attack problem*:

$$\max_{a} \sum_{j\in N^a} p_j \cdot \tilde{P}^a_j - \sum_{j\in N^a} c^a_j \cdot \left(\tilde{P}^a_j - \Delta P^a_j\right) - \alpha \cdot \|a\|_0 \tag{7}$$

$$s.t.\ \ \|a\|_0 \le n \tag{8}$$

$$\tilde{P}^d = F \cdot \left(P^d + \Delta P^d\right) = \hat{P}^d + F \cdot \Delta P^d \tag{9}$$

$$\tilde{P}^d \in \mathcal{D} \tag{10}$$

$$-\tau P^d_k \le \Delta P^d_k \le \tau P^d_k \quad \forall k \in N^d \tag{11}$$

$$\Delta P^f_\ell = -\sum_{k\in N^d} S_{\ell,k} \cdot \Delta P^d_k + \sum_{i\in N^g} S_{\ell,i} \cdot \Delta P^g_i \quad \forall \ell \in A \tag{12}$$

$$\sum_{i\in N^g} \Delta P^g_i - \sum_{k\in N^d} \Delta P^d_k = 0 \tag{13}$$

$$\sum_{j\in N^a} \left(\tilde{P}^a_j - \Delta P^a_j\right) + \sum_{i\in N^g} \tilde{P}^g_i = \sum_{k\in N^d} \hat{P}^d_k \tag{14}$$

$$0 \le \Delta P^a_j \le \tilde{P}^a_j \quad \forall j \in N^a \tag{15}$$

$$-\overline{P}^f_\ell \le \tilde{P}'^f_\ell \le \overline{P}^f_\ell \quad \forall \ell \in A \tag{16}$$

$$\tilde{P}'^f_\ell = \sum_{i\in N^g} S_{\ell,i} \cdot \tilde{P}^g_i + \sum_{j\in N^a} S_{\ell,j} \cdot \left(\tilde{P}^a_j - \Delta P^a_j\right) - \sum_{k\in N^d} S_{\ell,k} \cdot \hat{P}^d_k \quad \forall \ell \in A, \tag{17}$$

where $\tilde{P}^g$ and $\tilde{P}^a$ are the misguided decisions in SCED as a response to $\tilde{P}^d$, attack vector $a$ is:

$$a^T = \left[\Delta P^{d^T} \Delta P^{g^T} \Delta P^{f^T} \Delta P^{a^T}\right]. \tag{18}$$

Note that $\Delta P^d$, $\Delta P^g$ and $\Delta P^f$ are injected to the real-time measurements at time $t$ to stealthily misguide the decisions of SCED, while $\Delta P^a$ is injected into the real-time measurements at time $t_+$ to hide the actual generation output.

There are three parts to the utility function (7): the overall benefit to the corrupt generator owners due to the misguided decisions of SCED, the generation cost related to the actual output, and the attack cost ($\alpha > 0$), which is proportional to the number of attacked meters [29]. Equation (9)-(13) are constraints at time $t$, while (14)-(17) are constraints at time $t_+$. Equation (8) denotes a limit on the number of attacked sensors. Equation (9) and (10) ensure that the compromised load is within the feasible region of SCED and hence will not be flagged. As undetectable attack condition in AC state estimation is too complex to be directly used in analysis, we use load shifts limits (11) to model stealthy attacks and use a DC load flow model (12) to characterize the behavior of the network [6], [30].[2] Equation (12) is equivalent to the undetectable FDI constraint $\Delta z = H \cdot \Delta x$ in [3]; see the Appendix. Equation (13) gives the misguided impression that the compromised load and generation are in balance. Equation (14) is used to match the expected load with physical generation at time $t_+$, where $\tilde{P}^a_j - \Delta P^a_j$ is the actual output of the corrupt generators. Equation (15) is the lower and upper bound of $\Delta P^a_j$. Moreover, the actual power flow at time $t_+$ must be within the thermal constraints (16), where the expected power flow at time $t_+$ is determined by (17).

To analyze the best adversarial attack strategy in real-time markets, we assume that opponents coordinate to maximize the total benefit hence acting as one player. This assumption is based on the notion that attackers are motivated to cooperate for stealth (i.e., to achieve (12)), and cooperation is facilitated via smart grid communication network connectivity. To capture the interactions between SCED and attackers, bi-level programming is formulated taking in account the multi-solution uncertainty of SCED.

## III. Financially Motivated FDI Attacks Analysis

To study the best attack strategy for adversaries with multi-solution uncertainty, we formulate the interactions between the attacker and SCED as bi-level programming. By simplifying the bi-level programming problem to single-level mixed integer linear programming (SLMILP), the existence of optimal solutions is proven, and the problem is solved in a straightforward manner.

### A. Bi-Level Programming Formulation

We assert that corrupt generator owners have a first-mover advantage (leader) as they initially manipulate the load forecast to which SCED (follower) responds by making misinformed decisions. We assume that the corrupt generator owners have full disclosure of VSTLP and SCED, including objectives and constraints. Taking the multi-solution uncertainty into consideration, the interactions between attackers and SCED can be formulated as the *attacker-operator problem* (AOP):

$$\begin{aligned}
\text{AOP:}\quad & \max_{a,\tilde{P}^g,\tilde{P}^a} \sum_{j\in N^a} p_j \cdot \tilde{P}^a_j - \sum_{j\in N^a} c^a_j \cdot \left(\tilde{P}^a_j - \Delta P^a_j\right) \\
& \qquad - \alpha \cdot \|a\|_0 \ (7) \\
& s.t.\ \ (8)\text{–}(17) \text{ and } \tilde{P}^g, \tilde{P}^a \in \mathcal{G}\left(\tilde{P}^d\right). \\
& \qquad \mathcal{G}\left(\tilde{P}^d\right) = \arg\left\{\min_{\tilde{P}^g,\tilde{P}^a} \sum_{i\in N^g} c^g_i \cdot \tilde{P}^g_i + \sum_{j\in N^a} c^a_j \cdot \tilde{P}^a_j\right\} \\
& s.t.\ \ (2)\text{–}(6).
\end{aligned}$$

where $\mathcal{G}(\tilde{P}^d)$ is the optimal solutions set of SCED for a given compromised load forecast $\tilde{P}^d$.

Denote $\mathscr{U}(a^*, \tilde{P}^{a*}, \tilde{P}^{g*})$ as the attacker's financial benefit with the optimal solution $a^*$, $\tilde{P}^{a*}$ and $\tilde{P}^{g*}$ in bi-level AOP (similarly, denote $\mathscr{U}(0, P^a, P^g)$ as the attacker's financial benefit when $a = 0$, i.e., there is no FDI attack); the optimal solution satisfies:

$$\begin{aligned}
&\mathscr{U}\left(a^*, \tilde{P}^{a*}, \tilde{P}^{g*}\right) \geq \mathscr{U}\left(a^*, \tilde{P}^a, \tilde{P}^g\right), \forall \tilde{P}^a, \tilde{P}^g \in \mathcal{G}\left(a^*\right) \\
&\mathscr{U}\left(a^*, \tilde{P}^{a*}, \tilde{P}^{g*}\right) \geq \mathscr{U}\left(a, \tilde{P}'^a, \tilde{P}'^g\right), \forall a \in \mathcal{A}\left(0, P^d\right), \tilde{P}'^a, \\
&\qquad \tilde{P}'^g \in \mathcal{G}(a),
\end{aligned}$$

where $\mathcal{A}(0, P^d)$ is the feasible region of attack vector for a given load measurement $P^d$ when no mitigation is applied (see Section IV-A). That is, for a given load measurement $P^d$, $(a^*, \tilde{P}^{a*}, \tilde{P}^{g*})$ is the best attack for adversaries among all the possible attack vector and the optimal solution set $\mathcal{G}(\tilde{P}^d)$.

### B. Existence of the Optimal Solution

We prove the existence of optimal solution in the bi-level AOP. The reader should note that an optimal solution does not always exist in general [32]. We prove the existence of optimal solutions based on an equivalent SLMILP in Section III-C. Even though there exist similar proofs with equilibrium constraints [33], such results are not translatable here because (7) and (8) are discontinuous and the complementary slackness conditions are nonlinear.

*Theorem 1:* There exists at least one optimal solution in the proposed bi-level AOP.

*Proof:* In simplifying the bi-level AOP, we use Karush-Kuhn-Tucker (KKT) optimality conditions and linearization. To ensure the equivalence between AOP and SLMILP, we first prove that KKT conditions are sufficient and necessary conditions for optima in AOP. Since the objective function (1) is convex, the inequality constraints are convex, and the equality constraints are affine, the KKT conditions are sufficient and necessary conditions for optima [34]. Moreover, the nonlinear complementary slackness conditions can be linearized using big-M method, equivalently [35] (see Section III-C for SLMILP).

For an optimal solution to exist in an optimization, we require the objective function be continuous and the feasible region of $a$, $\tilde{P}^g$ and $\tilde{P}^a$ be nonempty and compact [36]. In our case, (7) is not continuous. Moreover, it is hard to analyze the properties of the feasible region in SLMILP, as binary variables exist. However, we can prove the existence

[2]Such formulation can also be generalized by replacing the nonlinear measurement function in AC state estimation with its Jacobian matrix at the current system state [31].

of optimal solution for a given attacked set and any solution of binary variables. First, for a given set of attacked meters $Q$, $|Q| \le n$, we have $\|a\|_0 = |Q|$ in (7) and (8). Hence, (7) is continuous for a given attacked set. Second, for any feasible solution of binary variables, the feasible region of $a$, $\tilde{P}^g$ and $\tilde{P}^a$ is nonempty (at least $a = 0$ satisfies and for any $P^d \in \mathcal{D}$, $\mathcal{G}(\hat{P}^d) \neq \emptyset$) and compact. Therefore, there exists at least an optimal solution for any given attack set $Q$ and feasible solution of binary variables. Thus there exists at least one optimal solution in the bi-level AOP. ■

### C. Single Level Mixed Integer Linear Programming Problem

Attack feasibility is demonstrated through practical computation of $a$, $\tilde{P}^g$ and $\tilde{P}^a$. To solve the bi-level AOP, we simplify the bi-level programming into a single level optimization by replacing the inner optimization, SCEDP, with its KKT optimality conditions, where complementary slackness conditions, utility function (7) and constraint (8) are nonlinear. As slackness conditions are multiplications of a nonnegative Lagrange multiplier and a constrained continuous function, they can be linearized by the big-M method [35]. The number of attacked meters in (7) and (8) can be reformulated as the sum of binary logical variables.

Denote $\delta^d$, $\delta^g$, $\delta^f$ and $\delta^a$, as the attacked sensor indicators of load, generator, power flow, and corrupt generator measurements, respectively. Thus, $\delta_k^d = 1$ when the load measurement at Bus $k$ is attacked, and $\delta_k^d = 0$, otherwise. The number of the attacked meters can be expressed as:

$$\|a\|_0 = \sum_{k\in N^d} \delta_k^d + \sum_{i\in N^g} \delta_i^g + \sum_{\ell\in A} \delta_\ell^f + \sum_{j\in N^a} \delta_j^a. \quad (19)$$

To ensure the equivalence, logical constraints between $\Delta P_k^d$ and $\delta_k^d$ must satisfy: 1) $\Delta P_k^d \neq 0 \Rightarrow \delta_k^d = 1$; 2) $\Delta P_k^d = 0 \Rightarrow \delta_k^d = 0$. Since we maximize the economic utility, the optimization solution will not change when logical constraint 2) is removed. For example, suppose the indictor $\delta_k^d$ can be any element in $\{0, 1\}$ when $\Delta P_k^d = 0$. The indictor converges to $\delta_k^d = 0$ if $\Delta P_k^d = 0$, because $\delta_k^d = 1$ results in a smaller economic utility. Hence, the logical constraints can be relaxed and constraint 1) is sufficient. The logical constraints 1) can be expressed in the following form:

$$\Delta P_k^d \le M \cdot \delta_k^d, \quad \forall k \in N^d, \quad (20)$$
$$\Delta P_k^d \ge -M \cdot \delta_k^d, \quad \forall k \in N^d, \quad (21)$$

where $M$ is a sufficient large positive value.

Similarly, the logical constraints between $(\Delta P_i^g, \delta_i^g)$, $(\Delta P_\ell^f, \delta_\ell^f)$, $(\Delta P_j^a, \delta_j^a)$ can be expressed as:

$$\Delta P_i^g \le M\delta_i^g, \quad \forall i \in N^g \quad (22)$$
$$\Delta P_i^g \ge -M\delta_i^g \quad \forall i \in N^g \quad (23)$$
$$\Delta P_\ell^f \le M\delta_\ell^f, \quad \forall \ell \in A \quad (24)$$
$$\Delta P_\ell^f \ge -M\delta_\ell^f, \quad \forall \ell \in A \quad (25)$$
$$\Delta P_j^a \le M\delta_j^a, \quad \forall j \in N^a \quad (26)$$
$$\Delta P_j^a \ge -M\delta_j^a, \quad \forall j \in N^a, \quad (27)$$

where logical variables satisfy

$$\delta_k^d, \delta_i^g, \delta_\ell^f, \delta_j^a, \in \{0, 1\}, \ \forall i \in N^g, j \in N^a, k \in N^d, \ell \in A. \quad (28)$$

Utilizing KKT optimality conditions, linearization and the reformulation above, the bi-level AOP can be reformulated as the following SLMILP.

$$\max_{a,\tilde{P}^g,\tilde{P}^a} \sum_{j\in N^a} p_j \cdot \tilde{P}_j^a - \sum_{j\in N^a} c_j^a \cdot \left(\tilde{P}_j^a - \Delta P_j^a\right) - \alpha \cdot \|a\|_0 \ (7)$$

$$\begin{aligned}
s.t.\ & (2)\text{–}(6),\ (8),\ (9),\ (11)\text{–}(17),\ (20)\text{–}(28) \\
& c_i^g + \lambda - \underline{\omega}_i + \overline{\omega}_i - \sum_{\ell\in A} S_{\ell,i} \cdot \underline{\nu}_\ell + \sum_{\ell\in A} S_{\ell,i} \cdot \overline{\nu}_\ell = 0, \\
& \quad \forall i \in N^g & (29) \\
& c_j^a + \lambda - \underline{\mu}_j + \overline{\mu}_j - \sum_{\ell\in A} S_{\ell,j} \cdot \underline{\nu}_\ell + \sum_{\ell\in A} S_{\ell,j} \cdot \overline{\nu}_\ell = 0, \\
& \quad \forall j \in N^a & (30) \\
& \underline{\omega}_i \ge 0, \quad \forall i \in N^g & (31) \\
& \overline{\omega}_i \ge 0, \quad \forall i \in N^g & (32) \\
& \underline{\mu}_j \ge 0, \quad \forall j \in N^a & (33) \\
& \overline{\mu}_j \ge 0, \quad \forall j \in N^a & (34) \\
& \underline{\nu}_\ell \ge 0, \quad \forall \ell \in A & (35) \\
& \overline{\nu}_\ell \ge 0, \quad \forall \ell \in A & (36) \\
& \underline{\omega}_i \le M \cdot \gamma_i^{\underline{\omega}}, \quad \forall i \in N^g & (37) \\
& \tilde{P}_i^g - \underline{P}_i^g \le M \cdot \left(1 - \gamma_i^{\underline{\omega}}\right), \quad \forall i \in N^g & (38) \\
& \overline{\omega}_i \le M \cdot \gamma_i^{\overline{\omega}}, \quad \forall i \in N^g & (39) \\
& \overline{P}_i^g - \tilde{P}_i^g \le M \cdot \left(1 - \gamma_i^{\overline{\omega}}\right), \quad \forall i \in N^g & (40) \\
& \underline{\mu}_j \le M \cdot \gamma_j^{\underline{\mu}}, \quad \forall j \in N^a & (41) \\
& \tilde{P}_j^a - \underline{P}_j^a \le M \cdot \left(1 - \gamma_j^{\underline{\mu}}\right), \quad \forall j \in N^a & (42) \\
& \overline{\mu}_j \le M \cdot \gamma_j^{\overline{\mu}}, \quad \forall j \in N^a & (43) \\
& \overline{P}_j^a - \tilde{P}_j^a \le M \cdot \left(1 - \gamma_j^{\overline{\mu}}\right), \quad \forall j \in N^a & (44) \\
& \underline{\nu}_\ell \le M \cdot \gamma_\ell^{\underline{\nu}}, \quad \forall \ell \in A & (45) \\
& \sum_{i\in N^g} S_{\ell,i} \cdot \tilde{P}_i^g + \sum_{j\in N^a} S_{\ell,j} \cdot \tilde{P}_j^a + \overline{P}_\ell^f \\
& \quad - \sum_{k\in N^d} S_{\ell,k} \cdot \tilde{P}_k^d \le M \cdot \left(1 - \gamma_\ell^{\underline{\nu}}\right), \quad \forall \ell \in A & (46) \\
& \overline{\nu}_\ell \le M \cdot \gamma_\ell^{\overline{\nu}}, \quad \forall \ell \in A & (47) \\
& \overline{P}_\ell^f - \sum_{i\in N^g} S_{\ell,i} \cdot \tilde{P}_i^g - \sum_{j\in N^a} S_{\ell,j} \cdot \tilde{P}_j^a \\
& \quad + \sum_{k\in N^d} S_{\ell,k} \cdot \tilde{P}_k^d \le M \cdot \left(1 - \gamma_\ell^{\overline{\nu}}\right), \quad \forall \ell \in A, & (48) \\
& \gamma_i^{\underline{\omega}}, \gamma_i^{\overline{\omega}}, \gamma_j^{\underline{\mu}}, \gamma_j^{\overline{\mu}}, \gamma_\ell^{\underline{\nu}}, \gamma_\ell^{\overline{\nu}} \in \{0, 1\}. & (49)
\end{aligned}$$

Note that $\|a\|_0$ is determined by (19), constraints (8), (9) and (11)–(17) are the attack constraints in the leader's optimization, constraint (10) is omitted due to the existence of follower's primal feasible constraints (2)-(6), (20)-(28) are the constraints of binary logical variables, (29) and (30) are the stationarity conditions in KKT conditions, (31)-(36) are the dual feasible conditions, (37)-(49) are the linearized expression of complementary slackness conditions using big-M method in [35], $\gamma_i^{\underline{\omega}}, \gamma_i^{\overline{\omega}}, \gamma_j^{\underline{\mu}}, \gamma_j^{\overline{\mu}}, \gamma_\ell^{\underline{\nu}}$ and $\gamma_\ell^{\overline{\nu}}$ are new binary variables introduced in the linearization of complementary slackness condition. Binary variables, such as $\delta^d$, $\delta^g$, $\delta^f$ and $\delta^a$ are determined by $\Delta P^d$, $\Delta P^g$, $\Delta P^f$, and $\Delta P^a$ in (18). Moreover, $\Delta P^f$ depends on $\Delta P^d$ and $\Delta P^g$, so the real decision variables are $\Delta P^d$, $\Delta P^g$, $\Delta P^a$, $\tilde{P}^g$, and $\tilde{P}^a$ in this optimization.

Even though, the mixed integer linear programming above is not convex (i.e., the feasible region is not a convex set), such problems can be solved by linear programming relaxations and branch & bound algorithms. In this paper, we use a mixed integer linear programming solver *intlinprog* in the *MATLAB Optimization Toolbox* [37]; see Section V.

## IV. Robust Attack Mitigation Strategy

To mitigate FDI attacks in SE, one general strategy is to protect a *basic measurement set*, which consists of the minimum number of measurements to ensure observability of the states (voltage phase angle at all buses) [13]–[15]. Thus, when protected against tampering (e.g., via effective cryptographic mechanisms and protocols), the integrity of state estimation is guaranteed, i.e., bus injections, determined by voltage phase angle at buses, can't be tampered. However, adversaries can still tamper with the load and generator power measurements (without modifying bus injections) and subsequently misguide SCED when generators and loads connect to the same bus. Hence, it is insufficient to protect a basic measurement set of SE to prevent FDI attacks in SCED. Moreover, defender needs to ensure the security of SCED for all the possible load and multiple solutions of SCED. Thus a robust strategy in protecting critical meters is needed for SCED that we address in this section. We first analyze the interactions amongst defender, attacker and operator (SCED) to design a robust "incentive-reduction" strategy for financially motivated FDI attacks.

### A. Tri-Level Programming Formulation

The interactions amongst defender, attacker and SCED are formulated as a tri-level defender-attacker-operator programming. Compared to the bi-level AOP in Section III-A, there is an additional *player*, the defender, who proactively decides on a security strategy prior to attack. Specifically, defender (tier 1) initially decides on the protected meter set $S$ (*strategy*) from all the possible protected meter sets $\mathcal{S}$ (*strategy set*) to minimize the attacker's *utility*. Subsequently, the attacker, who initiates FDI attack based on knowledge of $S$, is at mid-hierarchy. This leaves SCED at the lowest tier. We assume that the attacker knows the indices of the protected meters [16]. For example, an attacker can easily distinguish ciphertext and plaintext in encryption based protection, as ciphertext characteristics are distinct and unintelligible when observed.

Suppose the protected measurement set is $S$. Let $\sigma_k^d$ be the protection indicator variable, i.e., $\sigma_k^d = 1$ if the meter of load $P_k^d$ is in $S$, and $\sigma_k^d = 0$, otherwise. Similar definitions apply for $\sigma_i^g$, $\sigma_\ell^f$ and $\sigma_j^a$. The possible attack vector for a given protected set $S$ and load $P^d$ can be expressed as $\mathcal{A}(S, P^d)$. The relationship between the protected and attacked measurement sets can be expressed as:

$$\sigma_k^d + \delta_k^d \le 1, \quad \forall k \in N^d, \tag{50}$$

$$\sigma_i^g + \delta_i^g \le 1, \quad \forall i \in N^g, \tag{51}$$

$$\sigma_\ell^f + \delta_\ell^f \le 1, \quad \forall \ell \in A, \tag{52}$$

$$\sigma_j^a + \delta_j^a \le 1, \quad \forall j \in N^a \tag{53}$$

where the indictor variables satisfy

$$\sigma_k^d, \sigma_i^g, \sigma_\ell^f, \sigma_j^a \in \{0, 1\}, \ \forall i \in N^g, j \in N^a, k \in N^d, \ell \in A. \tag{54}$$

As it is costly and time-consuming to protect all the meters, the defender attempts to "force" the attacker's additional benefit (i.e., the attacker's benefit in attack minus the normal benefit) to zero using a minimal number of protected meters. Hence, the defender solves the following problem:

$$\begin{aligned}
\min_{S\in\mathcal{S}} \ & \Bigg\{ \beta \cdot |S| + \max_{P^d\in\mathcal{D}} \Bigg\{ \max_{a,\tilde{P}^a,\tilde{P}^g} \underbrace{\mathscr{U}\left(a, \tilde{P}^a, \tilde{P}^g\right)}_{\mathscr{U}_a} \\
& \qquad - \max_{P^a,P^g} \underbrace{\mathscr{U}\left(0, P^a, P^g\right)}_{\mathscr{U}_0} \Bigg\} \Bigg\} \\
s.t. \ & (8)\text{–}(17), \ (50)\text{–}(54), \\
& \{\tilde{P}^a, \tilde{P}^g\} \in \mathcal{G}(\tilde{P}^d) = \arg \mathrm{SCEDP}(\tilde{P}^d), \\
& \{P^a, P^d\} \in \mathcal{G}(P^d) = \arg \mathrm{SCEDP}(\hat{P}^d),
\end{aligned} \tag{55}$$

There are four programs in (55): 1) The *defender* protects a set of meters $S$ to secure SCED for all the possible load distributions and multi-solution uncertainty with a minimal number of protected meters, where $\mathcal{S}$ denotes all the feasible protection set; 2) The defender maximizes the additional benefit among all the possible load distributions $\mathcal{D}$ to ensure the security of SCED for all the possible loads; 3) The *attacker* maximizes financial benefit in (7) for a given protected set $S$ and load $P^d$, where (8)-(17) and (50)-(53) is the feasible region of $a$, denoted as $\mathcal{A}(S, P^d)$, $\mathcal{G}(\tilde{P}^d)$ is optimal solution set of SCED determined by the compromised load $\tilde{P}^d$; 4) The attacker maximizes financial benefit without attack among the optimal solution set of SCED,[3] $\mathcal{G}(\hat{P}^d)$, determined by real load forecast $\hat{P}^d$. Note that $|S|$ is the number of the protected meters:

$$|S| = \sum_{i\in N^g} \sigma_i^g + \sum_{j\in N^a} \sigma_j^a + \sum_{k\in N^d} \sigma_k^d + \sum_{\ell\in A} \sigma_\ell^f \tag{56}$$

In (55), multiplier $\beta$ is used to coordinate the two objectives, i.e., secure SCED with a minimal protected meters.

For a given load $P^d$, i.e., the real estimated load $\hat{P}^d$, the maximal financial benefit without attack, i.e., the fourth program in (55), $\mathscr{U}(0, P^{a*}, P^{g*})|_{P^d}$, can be obtained by solving the following bi-level optimization:

$$\begin{aligned}
\max_{P^a,P^g} \ & \mathscr{U}\left(0, P^a, P^g\right) \\
& \left\{P^a, P^g\right\} \in \mathcal{G}\left(\hat{P}^d\right) = \arg \mathrm{SCEDP}\left(\hat{P}^d\right)
\end{aligned}$$

Denote the cost function (1) in SCEDP as $\mathscr{C}(P^a, P^g)$. The bi-level optimization above can be reformulated as the following (single-level) *modified dispatch problem* (MDP):

$$\begin{aligned}
\text{MDP:} \ \min_{P^a,P^g} \ & \mathscr{C}\left(P^a, P^g\right) - \eta \cdot \mathscr{U}\left(0, P^a, P^g\right) \\
s.t. \ & (2)\text{–}(6),
\end{aligned} \tag{57}$$

[3] Maximal financial benefit among the optimal solution set of SCED corresponds to the best attack for adversaries, which is used here to ensure there is no additional benefit when there is no attack.

where $\eta \cdot \mathscr{U}(0, P^a, P^g)$ should not be too small compared to $\mathscr{C}(P^a, P^g)$ [9]. By replacing MDP with it's KKT optimality conditions, and denoting the feasible region as $\mathcal{G}'(\hat{P}^d)$, the optimal protected set can be obtained by solving the tri-level robust *defender-attacker-operator problem* (DAOP) below:

$$\min_{S\in\mathcal{S}} \left\{ \beta\cdot|S| + \max_{P^d,a,\tilde{P}^a,\tilde{P}^g} \left\{ \underbrace{\mathscr{U}(a,\tilde{P}^a,\tilde{P}^g) - \mathscr{U}(0,P^{a*},P^{g*})|_{P^d}}_{\mathscr{U}'} \right\} \right\}$$
$$\begin{aligned} s.t.\ & (8)\text{–}(17),\ (50)\text{–}(53), \\ & \left\{\tilde{P}^a,\tilde{P}^g\right\} \in \mathcal{G}(\tilde{P}^d) = \arg\mathrm{SCEDP}\left(\tilde{P}^d\right), \\ & P^d \in \mathcal{D},\ \text{and}\ \left\{P^{a*},P^{g*}\right\} \in \mathcal{G}'\left(\hat{P}^d\right). \end{aligned} \tag{58}$$

In (58), defender make decisions on protected meters $S$ at tier 1. Additional benefit is maximized among all the possible load and multiple solutions of SCED at mid level. Optimal solution set $\mathcal{G}(\tilde{P}^d)$ is determined by SCED at bottom level, as a response to $\tilde{P}^d$. $\mathcal{G}'(\hat{P}^d)$ is the KKT optimality condition of MDP. As $\mathscr{U}(0, P^{a*}, P^{g*})|_{P^d}$ is determined by $P^d$, for a given $P^d$, it is equivalent to maximize the additional benefit $\mathscr{U}'$ in (58) and attacker's utility in (7). That is, attacker's objective is included in the mid level optimization of the tri-level robust DAOP. Since $\mathscr{U}(0, P^{a*}, P^{g*})|_{P^d}$ is not related to the protected set $S$, the robust "incentive-reduction" protection strategy will not affect the corrupt generator owners' financial benefit without attack.

### B. Existence of the Optimal Solution

As discussed in Section III-B, the optimal solution for a tri-level programming does not always exist. Here, we prove the existence of the optimal solution for our tri-level programming, which demonstrates the existence of a protected set $S$ to mitigate financially motivated FDI attacks on SCED.

*Theorem 2:* There exists at least one optimal solution with finite value in the tri-level robust DAOP.

*Proof:* As described in Section III-C, the optimizations in the mid and the bottom levels of the robust DAOP, can be simplified to a SLMILP using KKT optimality conditions. Hence, the tri-level DAOP here can be simplified to a mixed integer bi-level optimization. Define $\mathcal{S}_m = \{S \in \mathcal{S} \big| |S| = m\}$ for a constant $m \geq 1$. For any protected set $S \in \mathcal{S}_m$, $\beta \cdot |S|$ is a constant, and the mixed integer bi-level optimization can be reformulated as a mixed integer bi-level min-max optimization.

As described in [38], bi-level min-max optimization has optimal solutions with finite value for $\mathcal{S}_m$, if the following conditions hold: 1) $\mathcal{S}_m \neq \emptyset$; 2) for all $S \in \mathcal{S}_m$ and $\forall P^d \in \mathcal{D}$, $\mathcal{A}(S, P^d) \neq \emptyset$, $\mathcal{G}(\tilde{P}^d) \neq \emptyset$, and $\mathcal{G}'(\hat{P}^d) \neq \emptyset$; 3) there exists $\exists S \in \mathcal{S}_m$ such that the attacker's additional benefit is bounded.

Since $\mathcal{S}_m$ consists of all possible protected sets satisfying $|\mathcal{S}_m| = m$ and is non-empty, i.e., 1) holds. For any $S \in \mathcal{S}_m$ and $P^d \in \mathcal{D}$, there exists at least $0 \in \mathcal{A}(S, P^d)$, i.e., $\mathcal{A}(S, P^d) \neq \emptyset$, and $\tilde{P}^d = \hat{P}^d \in \mathcal{D}$. As for any load $P^d \in \mathcal{D}$, solution exists in SCED, we have $\mathcal{G}(\tilde{P}^d) \neq \emptyset$, $\mathcal{G}'(\hat{P}^d) \neq \emptyset$, and 2) holds for all possible $\mathcal{S}_m$. Moreover, since $P^g$ and $P^a$ ($\tilde{P}^g$ and $\tilde{P}^a$) are limited by generation capacities, the financial benefit is finite. That is, 3) hold for all possible $\mathcal{S}_m$. Based on the description above, the tri-level robust DAOP has at least one optimal solution with finite value. ■

### C. Solution of the Tri-Level Programming

The solution to the tri-level programming demonstrates the ability to prevent financially motivated FDI attacks in SCED. The first step for solving the robust DAOP is merging the lower-level and the mid-level problems into a single-level problems using KKT optimality conditions, i.e., the tri-level DAOP is reduced to a bi-level problem, where binary variables are in both objectives and constraints, e.g., (50)–(53). Such binary variables prevent directly deriving dual variables to formulate dual cuts [18]. The nonlinear objective, $\beta \cdot |S|$, in (58) invalidate the Benders primal decomposition method [39]. As the defender's decision variables are discrete and finite, we can search all the possible protected set in ascending order of $|S|$ and stop when the maximal additional benefit, under protected set $S$, is small enough. To eliminate attacker's additional benefit, we set the threshold of additional benefit $\varepsilon$ as $10^{-3}$.

For a given protected measurement set $S$, we obtain the maximal additional benefit by solving the subproblem (SP):

$$\begin{aligned} \mathrm{SP}: \max_{P^d,a,\tilde{P}^a,\tilde{P}^g}\ & \mathscr{U}\left(a,\tilde{P}^a,\tilde{P}^g\right) - \mathscr{U}\left(0,P^{a*},p^{g*}\right)|_{P^d} \\ s.t.\ & (8)\text{–}(17),\ (50)\text{–}(53), \\ & \left\{\tilde{P}^a,\tilde{P}^g\right\} \in \mathcal{G}\left(\tilde{P}^d\right) = \arg\mathrm{SCEDP}(\tilde{P}^d), \\ & P^d \in \mathcal{D},\ \text{and}\ \left\{P^{a*},P^{g*}\right\} \in \mathcal{G}'\left(\hat{P}^d\right). \end{aligned} \tag{59}$$

Similar to the method in Section III-C, the subproblem above can be simplified to a SLMILP using KKT optimality conditions. We check the maximal additional benefit with the threshold $\varepsilon$ to verify the performance of the current protected set $S$. We update the protected set when the maximal additional benefit is larger than $\varepsilon$, and stop, otherwise.

Even though the subproblem can be easily solved, it is time-consuming to enumerate all possible protected sets in a large power system. Hence, in this paper, we design a heuristic algorithm for updating the protected meter set by choosing one of the most critical meters from the attacked set to protect in each iteration where the most critical meter is defined as the meter corresponding to the minimal additional benefit when moving one meter from the attacked set to the protected set in each iteration (refer lines 10-16 in Algorithm 1 for details). As SCED makes decisions on the generation output as a response to the load forecast, we have $\tilde{P}^a = P^{a*}$, $\tilde{P}^g = P^{g*}$, and the additional benefit is zero when $\tilde{P}^d = \hat{P}^d$, i.e., $\Delta P^d = 0$. It is sufficient to protect all the load measurements $P^d$ to force additional benefit to zero, which gives another terminal condition that iteration stops when the number of protected meters is larger the number of load $|N^d|$. The detailed algorithm is given in Algorithm 1.

In Algorithm 1, iterations terminate when $|S_i| = |N^d|$ or $\mathscr{U}' \leq \varepsilon$. In lines 10-16, the most critical meter corresponds to that which provides the minimal additional benefit when adding it to the protected set. In each iteration, the most critical meter is added to the protected set (Line 17), and at most

TABLE II
GENERATOR PARAMETERS IN SIMULATIONS

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **14-bus** | gen. bus | 1 | 2 | 3 | 6 | 8 | – |
| | min. cap. (MW) | 0 | 0 | 0 | 0 | 0 | – |
| | max. cap. (MW) | 100 | 100 | 600 | 100 | 600 | – |
| | marg. cost ($/MWh) | 30 | 30 | 20 | 25 | 20 | – |
| **30-bus** | gen. bus | 1 | 2 | 13 | 22 | 23 | 27 |
| | min. cap. (MW) | 0 | 0 | 0 | 0 | 0 | 0 |
| | max. cap. (MW) | 600 | 100 | 110 | 50 | 590 | 50 |
| | marg. cost ($/MWh) | 20 | 30 | 25 | 30 | 20 | 30 |

**Algorithm 1** Heuristic "Incentive-Reduction" Algorithm

1: Initialize $S = \emptyset$, $\varepsilon = 10^{-3}$;
**in the $i$th iteration**
2: **while** $|S| <= |N^d|$
3: $\mathscr{U}_i' = \mathrm{SP}(S)$; % solve SP with a given $S$ for $\mathscr{U}_i'$.
4: **if** $\mathscr{U}_i' \le \varepsilon$
5: break; % algorithm stop when $\mathscr{U}_i' \le \varepsilon$.
6: **else**
7: save $A_i$ as the attacked set;
8: **end**
9: $\mathscr{U}' = \mathscr{U}_i'$;
10: **for** each $e \in A_i$ % $e$ is a possible element in $A_i$.
11: $\mathscr{U}_i' = \mathrm{SP}(S \cup e)$;
12: **if** $\mathscr{U}_i' \le \mathscr{U}'$
13: $s = e$; % $s$ is a temporary critical meter.
14: $\mathscr{U}' = \mathscr{U}_i'$;
15: **end**
16: **end**
17: $S = S \cup s$; % $s$ is the most critical meter.
18: **end**

$n$ attacked meters are checked. As the algorithm stops within $|N^d|$ iterations, the subproblem, *SP*, is executed no more than $(n+1) \cdot |N^d|$ times (once in Line 3 and at most $n$ times in Line 11 for each iteration). Even though the solutions of the heuristic "incentive-reduction" algorithm may not be the globally optimal, the proposed algorithm reduces the complexity of searching the minimal number of protected meters for mitigation of financially motivated FDI attacks.

Mixed integer linear programming is computationally intractable [40], hence acceleration techniques [11], such as reducing the number of binary variables, are used to diminish the computational burden. Similar to the approach in Section III-C, we solve the SLMILP using the mixed integer linear programming solver *intlinprog* in the *MATLAB Optimization Toolbox*.

## V. NUMERICAL SIMULATION

We empirically explore the effects of financially motivated FDI attack and our proposed mitigation strategy in the IEEE 14-bus [41] and IEEE 30-bus test systems [42] with generator parameters (capacity and marginal cost) as shown in Table II. Other configuration data, such as branch reactance, are obtained from MATPOWER packages [43].

As shown in Fig. 2, there are 56 meters in the 14-bus system, including 5 generation meters, 11 load meters, and 40 power flow meters (both "from" and "to"). There are 108 meters in the 30-bus system, including 6 generation meters, 20 load meters, and 82 power flow meters (both "from" and "to"). According to data in MATPOWER package, we take Bus 1 as reference bus in both 14-bus and 30-bus systems. Shift factors are calculated based on DC power flow model and reference bus information [44]. We assume that the owner of generator at Bus 6 in 14-bus system, and generator at Bus 13 in 30-bus system, are corrupt. For simplicity, we assume that $F$ is identity matrix. The locational marginal price at corresponding buses are 30 $/MWh. The number of attacked meters is no larger than 10, i.e., $n = 10$. As forecast error is small in VSTLP [45], we assume that the injected attack data at loads are limited to $\tau = 0.05$. The multiplier of attack cost in (7) is set as $\alpha = 10$. The constant positive value $M$ is set as $M = 5 \times 10^4$. In order to verify thermal constraints' effects on financially motivated FDI attacks and mitigation (see Section V-B), we consider two cases in simulations. In Case 1, we assume that all the transmission lines' capacities are large enough, e.g., all the transmission lines' capacities are 1500MW. In Case 2, we assume that the thermal constraints on transmission line 3-4 in the 14-bus system and transmission line 12-15 in the 30-bus system are 400MW and 200MW, respectively, and other transmission lines' capacities are large enough, e.g., other transmission lines' capacities are 1500MW.

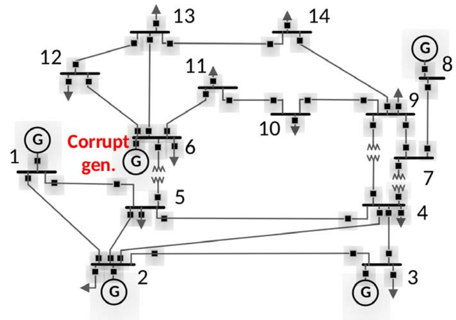
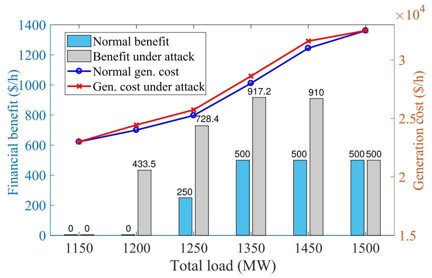



Fig. 2. IEEE 14-bus test system.

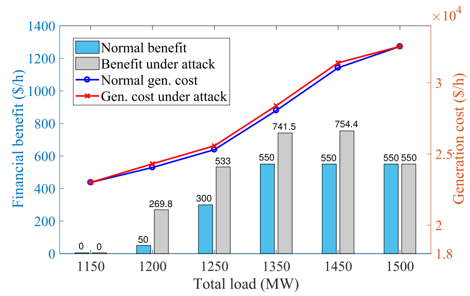
### A. Financially Motivated FDI Attacks

We verify the feasibility of financially motivated FDI attack by analyzing normal benefit, benefit under attack, normal generation cost, and generation cost under attack. Thermal constraints in Case 2 is used in this part. For a given total load, we simulate 100 times for randomly generated individual load values. Average financial benefit and generation cost in the IEEE 14-bus and 30-bus systems are presented in Fig. 3.

Obviously, for a given feasible load in SCED, there exists at least one optimal solution in the bi-level AOP. As shown in Fig. 3(a) and Fig. 3(b), attackers can benefit from SCED by injecting attack data. As evident, the additional benefits are attractive to attackers when the total loads are within 1200 MW $\sim$ 1450 MW for the 14-bus system and the 30-bus system. For example, in the 14-bus system, the additional benefit is more than 400$/h for total load within 1200MW$\sim$ 1450MW, and the financial benefit under attack is about 3 times of the normal benefit when the total load is 1250MW. Moreover, in the 30-bus system, the additional benefit is about 200$/h for the total load within 1200MW $\sim$ 1450MW, and the financial benefit under attack is about twice of the normal benefit




(a) Simulation results in the 14-bus test system.




(b) Simulation results in the 30-bus test system.

Fig. 3. Average benefit and generation cost in the 14-bus and 30-bus systems.

when the total load is 1250MW, which is attractive to attackers. Specifically, attackers can benefit by: 1) changing the total load; For example, in the 14-bus system, attacker can increase the financial benefit from 0 to 1700\$/h, by changing the total load from 1200MW ($P_2^d = 300$MW, $P_3^d = 400$MW and $P_4^d = 500$MW) to 1260MW ($P_2^d = 315$MW, $P_3^d = 420$MW and $P_4^d = 525$MW). 2) redistributing load; For example, in the 14-bus system attacker can increase the financial benefit from 0 to 460\$/h, by redistributing the original load $P_2^d = 108$MW, $P_3^d = 1276$MW and $P_{11}^d = 16$MW to $P_2^d = 103$MW, $P_3^d = 1281$MW and $P_{11}^d = 16$MW without changing the total load. Since the misguided generation outputs are different from the optimal ones, generation cost increase from 24000\$/h to 25500\$/h and from 30000\$/h to 30500\$/h, respectively. In the 14-bus system, the additional benefit is 0 when the total load is no larger than 1150 MW, because the total load is so small that the scheduled output of the corrupt generator is 0 even in the presence of FDI attacks. The additional benefit increases greatly when the total load is 1200 MW in the 14-bus system, because attacker can obtain additional benefit from the difference of scheduled output and real output, i.e, $\Delta P^a > 0$. The additional benefit decreases when the total loads are near to the maximal generation capacity, because attack vectors are limited by power system stability constraints (14) and (15).

### B. Financially Motivated FDI Attacks Mitigation

We study mitigation strategies for financially motivated FDI attacks in the IEEE 14-bus and 30-bus test systems. Thermal constraints assumptions in Case 1 and Case 2 are used in this part. To compare the proposed mitigation strategy with the basic-measurement-set protection strategy in [13]–[15], we

TABLE III
MITIGATION STRATEGY IN THE IEEE 14-BUS AND 30-BUS SYSTEMS

| Items | | Protected meters | $P^d$(MW) | $\mathscr{U}'$(\$/h) | Attacked meters |
|---|---|---|---|---|---|
| **14-bus** | **Case 1** | $P_6^a$ | all | 0 | – |
| | | $S_1$ * | (1238.1,0,0,...,0) | 1827.1 | $P_2^d, P_6^a, P_2^g$ |
| | **Case 2** | $P_6^a$ | (108,1276,0,...,16,0,0,0) | 460 | $P_2^d, P_3^d, P_2^g, P_3^g$ |
| | | $P_6^a, P_2^d, P_2^g$ | all | 0 | – |
| | | $S_1$ | (1238.1,0,0,...,0) | 1827.1 | $P_2^d, P_6^a, P_2^g$ |
| **30-bus** | **Case 1** | $P_{13}^a$ | all | 0 | – |
| | | $S_2$ | (1200,0,0,0,...,0) | 1820 | $P_2^d, P_{13}^a, P_2^g$ |
| | **Case 2** | $P_{13}^a$ | (309,0,0,0,0,0,672,0,0,0, 0,0,0,0,0,309,0,0,0,0) | 12.2 | $P_2^d, P_{23}^d, P_2^g, P_{23}^g$ |
| | | $P_{13}^a, P_{23}^g$ | all | 0 | – |
| | | $S_2$ | (1229.9,0,0,0,0,0,0,0, 8.6,0,0,0,0,0,0,0,0,0,0,0) | 1814.8 | $P_2^d, P_{13}^a, P_2^g$ |

* Note: $S_1 = \{$1-2,1-5,2-3,2-4,4-7,4-9,5-6,6-11,6-12,6-13,7-8,9-10,9-14$\}$, and $S_2 = \{$1-2,1-3,2-4,2-5,2-6,5-7,6-8,6-9,6-10,6-28,9-11,4-12,12-13,12-14, 12-15,12-16,14-15,16-17,18-19,19-20,10-21,10-22,15-23,22-24,24-25, 25-26,25-27,27-29,27-30$\}$, where elements in $S_1$ and $S_2$ are (power flow) meters of the corresponding branches, e.g., 1-2 denotes power flow meter on line 1-2.

calculate attacker's additional benefit when a basic measurement set, denoted as $S_1$ and $S_2$ in the 14-bus and 30-bus systems, is protected. Protected meters and corresponding simulation data in the IEEE 14-bus and 30-bus test systems are presented in Table III.

As the modification of load measurements are limited by (2) and (14), the total load modification is zero when the meter of corrupt generator is protected. That is, attackers can only modify the load distribution without affecting the total load, i.e., load redistribution attack [6]. As discussed in [6], attacker can not misguide the generation outputs when transmission lines' capacities are large enough in load redistribution attack, i.e., it is sufficient to protect the meter of corrupt generator for the IEEE 14-bus and 30-bus system in Case 1. As the capacities of line 3-4 in the 14-bus system and line 12-15 in the 30-bus system are 400MW and 200MW in Case 2, respectively, attacker can exploit such thermal constraints to benefit when the meter of corrupt generator is protected. For example, in the IEEE 14-bus system, attacker can obtain additional benefit 460\$/$h$ by modifying readings of $P_2^d$, $P_3^d$, $P_2^g$, and $P_3^g$, when loads are $P_2^d = 108$MW, and $P_3^d = 1276$MW. The reason is that attacker can redistribute load to change the scheduled generation output utilizing thermal constraints on line 3-4. By protecting $P_6^a$, $P_2^d$ and $P_2^g$, defender can deter financially motivated attack in Case 2 of the IEEE 14-bus system, launched by the owner of generator at Bus 6. Similarly, defender can prevent such attack, launched by the owner of generator at Bus 13, by protected $P_{13}^a$ and $P_{23}^g$ in Case 2 of the IEEE 30-bus system. Basic-measurement-set protection strategy, generally used in securing state estimation, cannot ensure the security of SCED. For example, even though a basic set of meters $S_2$ are protected in the IEEE 30-bus system, attacker can still obtain additional benefit 1814.8\$/$h$ by modifying $P_2^d$, $P_{13}^a$ and $P_2^g$, when loads are $P_2^d = 1229.9$MW and $P_{15}^d = 8.6$MW. Thus, attacker can obtain additional benefit even when a basic measurement set is protected if there are generators and loads connect to the same bus.

In simplifying the bi-level and tri-level programming, a large amount of binary variables are introduced, e.g., there are 255 binary variables in the SLMILP simplified from SP in IEEE 30-bus system. Even though acceleration techniques are used to reduce binary variables, the computational burden is still high in large power systems. As the attack vector $a$ is determined by the current load measurement only in the bi-level programming, we can calculate the attack vector in advance and search the appropriate attack vector based on the current load to timely inject false data. Since the robust attack mitigation strategy in the tri-level programming is not related to the real-time measurements, it can also be calculated in advance. Models of very short term load predictor must be further investigated to make financially motivated FDI attack and mitigation strategy more practical.

## VI. Conclusion

In this paper, we analyze the feasibility of financially motivated FDI attacks on security constrained economic dispatch in real-time markets and further design an incentive-reduction protection strategy by protecting critical meters in security constrained economic dispatch. We demonstrate that for a large class of possible loads, an attacker can simultaneously obtain additional benefit (i.e., increase financial benefit due to attack) and increase the generation cost of security constrained economic dispatch when no mitigation is applied. Our proposed security strategy can prevent the success of such attacks for all the possible load and solutions of security constrained economic dispatch by protecting a minimal number of meters.

## Appendix
## Equivalent Undetectable Attack Constraints

To avoid bad data detection in state estimation, the injected attack vector must satisfy $\Delta z = H \cdot \Delta x$ [3], i.e.,

$$\begin{bmatrix} \Delta P^f \\ \Delta P^b \end{bmatrix} = \begin{bmatrix} H^f \\ H^b \end{bmatrix} \cdot \Delta x,$$

where $\Delta x$ is the state change introduced by FDI (note: state at the reference bus is typically excluded in state estimation [46]), $H^f$ is power flow related measurement matrix, and $H^b$ is the bus injection related measurement matrix. Note that $\Delta P^b$ is the modification of bus injection, and the injection of Bus $i$, $\Delta P_i^b$, is the sum of the load and generators modification at Bus $i$: $\Delta P_i^b = \Delta P_i^g - \Delta P_i^d$. Since $H^b$ is invertible, the relationship between $\Delta P^f$ and $\Delta P^b$ can be expressed as $\Delta P^f = H^f \cdot (H^b)^{-1} \cdot \Delta P^b$, where $H^f \cdot (H^b)^{-1}$ is shift factor matrix. To deter bad data detection in state estimation, the injected attack data must satisfy:

$$\Delta P_\ell^f = -\sum_{k \in N^d} S_{\ell,k} \cdot \Delta P_k^d + \sum_{i \in N^g} S_{\ell,i} \cdot \Delta P_i^g, \quad \forall \ell \in A.$$

Thus, $\Delta P^f$ is determined by $\Delta P^d$ and $\Delta P^g$.

## References

[1] A. Ipakchi and F. Albuyeh, "Grid of the future," *IEEE Power Energy Mag.*, vol. 7, no. 2, pp. 52–62, Mar./Apr. 2009.
[2] C. Liu, J. Wu, C. Long, and Y. Wang, "Dynamic state recovery for cyber-physical systems under switching location attacks," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 1, pp. 14–22, Mar. 2017.
[3] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Security*, vol. 14, no. 1, pp. 1–33, 2011.
[4] Y. V. Makarov, C. Loutan, J. Ma, and P. Mello, "Operational impacts of wind generation on California power systems," *IEEE Trans. Power Syst.*, vol. 24, no. 2, pp. 1039–1050, May 2009.
[5] 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.
[6] 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.
[7] X. Liu, Z. Li, Z. Shuai, and Y. Wen, "Cyber attacks against the economic operation of power systems: A fast solution," *IEEE Trans. Smart Grid*, vol. 8, no. 2, pp. 1023–1025, Mar. 2017.
[8] Y. Yuan, Z. Li, and K. Ren, "Quantitative analysis of load redistribution attacks in power systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 9, pp. 1731–1738, Sep. 2012.
[9] X. Liu and Z. Li, "Trilevel modeling of cyber attacks on transmission lines," *IEEE Trans. Smart Grid*, vol. 8, no. 2, pp. 720–729, Mar. 2017.
[10] L. Jia, R. J. Thomas, and L. Tong, "Impacts of malicious data on real-time price of electricity market operations," in *Proc. HICSS*, 2012, pp. 1907–1914.
[11] D.-H. Choi and L. Xie, "Economic impact assessment of topology data attacks with virtual bids," *IEEE Trans. Smart Grid*, to be published, doi: 10.1109/TSG.2016.2535246.
[12] H. Ye, Y. Ge, X. Liu, and Z. Li, "Transmission line rating attack in two-settlement electricity markets," *IEEE Trans. Smart Grid*, vol. 7, no. 3, pp. 1346–1355, May 2016.
[13] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 645–658, Dec. 2011.
[14] J. Kim and L. Tong, "On topology attack of a smart grid: Undetectable attacks and countermeasures," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 7, pp. 1294–1305, Jul. 2013.
[15] R. B. Bobba, K. M. Rogers, and Q. Wang, "Detecting false data injection attacks on DC state estimation," in *Proc. 1st Workshop Secure Control Syst.*, Stockholm, Sweden, Apr. 2010.
[16] 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, Jun. 2011.
[17] X. Liu, Z. Li, and Z. Li, "Optimal protection strategy against false data injection attacks in power systems," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1802–1810, Jul. 2017.
[18] X. Wu and A. J. Conejo, "An efficient tri-level optimization model for electric grid defense planning," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 2984–2994, Jul. 2017.
[19] X. Zhang, "Restructured electric power systems and electricity markets," in *Restructured Electric Power Systems: Analysis of Electricity Markets With Equilibrium Models*. Hoboken, NJ, USA: Willey, 2010, ch. 2, pp. 53–98.
[20] A. L. Ott, "Experience with PJM market operation, system design, and implementation," *IEEE Trans. Power Syst.*, vol. 18, no. 2, pp. 528–534, May 2003.
[21] "Report on security constrained economic dispatch," Joint Board PJM/MISO Region, Federal Energy Regulatory Commission, Washington, DC, USA, Rep. AD05-13-000, 2006.
[22] M. Esmalifalak, H. Nguyen, R. Zheng, and Z. Han, "Stealth false data injection using independent component analysis in smart grid," in *Proc. IEEE SmartGridComm*, Brussels, Belgium, Oct. 2011, pp. 244–348.
[23] J. Kim, L. Tong, and R. J. Thomas, "Subspace methods for data attack on state estimation: A data driven approach," *IEEE Trans. Signal Process.*, vol. 63, no. 5, pp. 1102–1114, Mar. 2015.
[24] "Common cyber security vulnerabilities observed in control system assessment by the INL NSTB program," U.S. DOE Office Electricity Delivery Energy Rel., Washington, DC, USA, Rep. INL/EXT-08-13979, Nov. 2008, pp. 21–22.
[25] D. J. Trudnowski, W. L. McReynolds, and J. M. Johnson, "Real-time very short-term load prediction for power-system automatic generation control," *IEEE Trans. Control Syst. Technol.*, vol. 9, no. 2, pp. 254–260, Mar. 2001.
[26] L. Jia, R. J. Thomas, and L. Tong, "On the nonlinearity effects on malicious data attack on power system," in *Proc. PESGM*, San Diego, CA, USA, 2012, pp. 1–8.
[27] L. Jia, J. Kim, R. J. Thomas, and L. Tong, "Impact of data quality on real-time locational marginal price," *IEEE Trans. Power Syst.*, vol. 29, no. 2, pp. 627–636, Mar. 2014.
[28] C. Y. Fok and M. I. Vai, "Very short term load forecasting for Macau power system," in *Proc. ICIC*, 2012, pp. 538–546.

[29] G. Dan, K. C. Sou, and H. Sanberg, "Power system state estimation security: Attacks and protection schemes," in *Smart Grid Communications and Networking*. Cambridge, U.K.: Cambridge Univ. Press, 2014, ch. 17, pp. 388–412.
[30] J. Liang, L. Sankar, and O. Kosut, "Vulnerability analysis and consequences of false data injection attack on power system state estimation," *IEEE Trans. Power Syst.*, vol. 31, no. 5, pp. 3864–3872, Sep. 2016.
[31] G. Hug and J. A. Giampapa, "Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1362–1370, Sep. 2012.
[32] G. K. D. Saharidis, A. J. Conejo, and G. Kozanidis, "Exact solution methodologies for linear and (mixed) integer bilevel programming," in *Metaheuristics for Bi-Level Optimization*. Berlin, Germany: Springer, 2013, ch. 8, pp. 221–245.
[33] Z. Luo, J. Pang, and D. Ralph, "Introduction," in *Mathematical Programs With Equilibrium Constraints*. New York, NY, USA: Cambridge Univ. Press, 1996, ch. 1, pp. 1–60.
[34] S. P. Boyd and L. Vandenberghe, "Duality," in *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004, ch. 5, pp. 215–288.
[35] J. Fortuny-Amat and B. McCarl, "A representation and economic interpretation of a two-level programming problem," *J. Oper. Res. Soc.*, vol. 32, no. 9, pp. 783–792, Sep. 1981.
[36] W. Rudin, "Continuity," in *Principles of Mathematical Analysis*, 3rd ed. New York, NY, USA: McGraw-Hill, 1976, ch. 4, pp. 83–102.
[37] *Intlinprog, Mixed-Integer Linear Programming (MILP)*. Accessed: Nov. 6, 2017. [Online]. Available: http://cn.mathworks.com/help/optim/ug/intlinprog.html
[38] Y. Tang, J.-P. Richard, and J. C. Smith, "A class of algorithms for mixed-integer bilevel min–max optimization," *J. Glob. Optim.*, vol. 66, no. 2, pp. 225–262, Oct. 2016.
[39] B. Zeng and L. Zhao, "Solving two-stage robust optimization problems using a column-and-constraint generation method," *Oper. Res. Lett.*, vol. 41, no. 5, pp. 457–461, Sep. 2013.
[40] J. Hu, J. E. Mitchell, J. S. Pang, and B. Yu, "On linear programs with linear complementarity constraints," *J. Glob. Optim.* vol. 53, no. 1, pp. 29–51, 2012.
[41] *14 Bus Power Flow Test Case*. Accessed: Nov. 6, 2017. [Online]. Available: https://www2.ee.washington.edu/research/pstca/pf14/pg_tca14bus.htm
[42] *30 Bus Power Flow Test Case*. Accessed: Nov. 6, 2017. [Online]. Available: https://www2.ee.washington.edu/research/pstca/pf30/pg_tca30bus.htm
[43] *MATPOWER, A MATLAB Power System Simulation Package*. Accessed: Nov. 6, 2017. [Online]. Available: http://www.pserc.cornell.edu/matpower/
[44] I. Dobson *et al.*, "Security of transfer capacity," in *Electric Power Transfer Capability: Concepts, Applications, Sensitivity, Uncertainty*, Power Syst. Eng. Res. Center, University of Wisconsin, 2001, ch. 3, pp. 25–28.
[45] J. W. Taylor, "An evaluation of methods for very short-term load forecasting using minute-by-minute British data," *Int. J. Forecast.*, vol. 24, no. 4, pp. 645–658, 2008.
[46] A. Abur and A. G. Exposito, "Weighted least squares state estimation," in *Power System State Estimation: Theory and Implementation*. New York, NY, USA: Marcel Dekker, 2004, ch. 2.

**Chensheng Liu** (S'12) received the B.Eng. degree in control science and engineering from Shandong University, Jinan, China, in 2012. He is currently pursuing the Ph.D. degree with the School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai, China. He was an international visiting graduate student with the Department of Electrical and Computer Engineering, University of Toronto, Canada, from 2016 to 2017. His current research interests include security of smart grid, electric vehicle navigation, and voltage control in smart grid.

**Min Zhou** (S'15) received the B.Eng. degree in information science and engineering from the East China University of Science and Technology, Shanghai, China, in 2015. She is currently pursuing the Ph.D. degree with the School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai. Her current research interest is cyber-physical security of smart grid.

**Jing Wu** (M'08) received the B.S. degree from Nanchang University in 2000, the M.S. degree from Yanshan University in 2002, and the Ph.D. degree from the University of Alberta in 2008, all in electrical engineering. Since 2011, she has been with Shanghai Jiao Tong University, Shanghai, China, where she is currently an Associate Professor. Her current research interests include robust model predictive control, security control, and stability analysis and estimations for cyber-physical systems. She is a registered Professional Engineer in Alberta, Canada.

**Chengnian Long** (M'07) received the B.S., M.S., and Ph.D. degrees from Yanshan University, China, in 1999, 2001, and 2004, respectively, all in control theory and engineering. He was a Research Associate with the Department of Computer Science and Engineering, Hong Kong University of Science and Technology, and a Killam Post-Doctoral Fellow with the University of Alberta, Canada. He has been with Shanghai Jiao Tong University in 2009, where he has been a Full Professor since 2011. His current research interests include cyber-physical systems security, mobile Internet of Things, and distributed intelligence systems.

**Deepa Kundur** (S'91–M'99–SM'03–F'15) received the B.A.Sc., M.A.Sc., and Ph.D. degrees from the University of Toronto in 1993, 1995, and 1999, respectively, all in electrical and computer engineering. She is a Professor with the Edward S. Rogers Sr. Department of Electrical and Computer Engineering, University of Toronto, and currently serves as the Chair of the Division of Engineering Science, University of Toronto. From 2003 to 2012, she was a Faculty Member of electrical and computer engineering, Texas A&M University, and from 1999 to 2002, she was a Faculty Member of electrical and computer engineering with the University of Toronto.

Her research interests include the interface of cyber security, signal processing, and complex dynamical networks. She has participated on several editorial boards and currently serves on the Advisory Board of *IEEE Spectrum*. She currently serves as a TPC Co-Chair for IEEE SmartGridComm 2018. Recently, she also served as the Symposium Co-Chair for the Communications for the Smart Grid Track of ICC 2017, the General Chair for the Workshop on Communications, Computation, and Control for Resilient Smart Energy Systems at ACM e-Energy 2016, the Workshop on Cyber-Physical Smart Grid Security and Resilience at Globecom 2016, the Symposium on Signal and Information Processing for Smart Grid Infrastructures at GlobalSIP 2016, the 2015 International Conference on Smart Grids for Smart Cities, the 2015 Smart Grid Resilience Workshop at IEEE GLOBECOM 2015, and the IEEE GlobalSIP'15 Symposium on Signal and Information Processing for Optimizing Future Energy Systems.

Prof. Kundur was a recipient of best paper recognitions at numerous venues including the 2015 IEEE Smart Grid Communications Conference, the 2015 IEEE Electrical Power and Energy Conference, the 2012 IEEE Canadian Conference on Electrical and Computer Engineering, the 2011 Cyber Security and Information Intelligence Research Workshop, and the 2008 IEEE INFOCOM Workshop on Mission Critical Networks. She is a fellow of the Canadian Academy of Engineering.