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

R ECENT 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.
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 affected by multi-solution uncertainty of SCED and the load uncertainty in power systems. Hence, it is important to design a robust multi-solution uncertainty and load uncertainty protection strategy account for an attacker’s specific objective, in power systems. Hence, it is important to design a robust multi-solution uncertainty and load uncertainty mitigation strategy that can significantly reduce the complexity of finding the minimal set of protected meters for the mitigation of financially motivated FDI attacks.

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 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, \(P^{\text{d}}\) is the real measurement at time \(t\), \(\hat{P}^{\text{d}}\) is the legitimate load forecast at time \(t_+\), and \(\tilde{P}^{\text{d}}\) 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, \(\Delta P_{\ell}\) represents the injected attack vector on overall generator measurements while \(\Delta P_{\ell}^i\) 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.

### 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 \(\tilde{P}^{\text{d}}\) at time \(t_+\), SCED solves the following SCED problem (SCEDP) [5]:

\[
\begin{align*}
\text{SCEDP:} & \min_{P, \tilde{P}} \sum_{i \in N^d} c^d_i \cdot \tilde{P}^d_i + \sum_{j \in N^g} c^g_j \cdot \hat{P}^g_j \\
\text{s.t.} & \sum_{i \in N^d} \tilde{P}^d_i + \sum_{j \in N^g} \hat{P}^g_j = \sum_{k \in N^a} \hat{P}^a_k (\lambda) \\
& \tilde{P}^d_i \leq \tilde{P}^d_i \leq \tilde{P}^d_i \forall i \in N^g (\omega, \bar{\omega}) \\
& \hat{P}^g_i \leq \hat{P}^g_i \leq \hat{P}^g_i \forall j \in N^g (\mu, \bar{\mu}) \\
& -\bar{P}_\ell \leq \tilde{P}^d_\ell \leq \tilde{P}^d_\ell \forall \ell \in A (\nu, \bar{\nu}) \\
& \hat{P}^\ell_\ell = \sum_{i \in N^d} S_{\ell, i} \cdot \tilde{P}^d_i + \sum_{j \in N^g} S_{\ell, j} \cdot \hat{P}^g_j \\
& -\sum_{k \in N^a} S_{\ell, k} \cdot \hat{P}^a_k \forall \ell \in A, 
\end{align*}
\]

where all the variables \(\tilde{P}^d, \tilde{P}^g,\) and \(\hat{P}^\ell\) are the desired or scheduled values at time \(t_+\), \(c^d\) and \(c^g\) 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, $P^d_\ell$, is determined by (6). $\lambda$, $\omega$, $\mu$, $\nu$, $\mu_f$, $\nu_f$, $\mu_i$, and $\nu_i$ are Lagrange multipliers corresponding to the constraints above. $S_{t,i}$ in (6) is a shift factor representing the increase in power flow in the $\ell$th line, when the output of generator at Bus $i$ increases by 1 p.u. [20]. Since $S_{t,i}$ 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 $D$. We assume for any given load measurements $P^d \in D$, the forecast load $P^f$ based on $P^d$ satisfies $P^f \in D$; hence, a solution for SCED exists for any load in $D$. For a given load $P^d \in D$, SCED may have multiple solutions, mathematically. To design a robust protection strategy for all possibilities in $D$ 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 at time $t$ to misguide the SCED decisions via the following steps (see also Fig. 1): 1) To manipulate the load forecast at time $t$, attackers compromise meters and subsequently misguide SCED decisions (with a same total load) may be different.

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 $t_s$, 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 $t_s$ 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 the load at time $t$ and the load forecast at time $t_s$ 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., $P^d = F \cdot P^f$, adversaries solve the following financial motivated attack problem:

$$\max_a \sum_{j \in N^a} p_j \cdot \tilde{P}_j^a - \sum_{j \in N^a} c_{j}^a \cdot \left( \tilde{P}_j^a - \Delta P^d_j \right) - \alpha \cdot \| a \|_0$$

$$s.t. \quad \| a \|_0 \leq n$$

$$\tilde{P}_j^a = F \cdot \left( P^d + \Delta P^d \right) = \tilde{P}_j^d + F \cdot \Delta P^d$$

$$\tilde{P}_j^d \in D$$

$$-\tau P^d_k \leq \Delta P^d_k \leq \tau P^d_k \quad \forall k \in N^d$$

$$\Delta P^d_\ell = - \sum_{k \in N^d} S_{t,k} \cdot \Delta P^d_k = \sum_{k \in N^d} S_{t,k} \cdot \Delta P^d_k \quad \forall \ell \in A$$

$$\sum_{k \in N^d} \Delta P^d_k = \sum_{k \in N^d} \Delta P^d_k$$

$$\sum_{j \in N^a} \left( \tilde{P}_j^a - \Delta P^d_j \right) + \sum_{k \in N^d} \tilde{P}^g_k = \sum_{k \in N^d} \tilde{P}^d_k$$

$$0 \leq \Delta P^d_j \leq P^d_j \quad \forall j \in N^a$$

$$-P^d_\ell \leq \tilde{P}^d_\ell \leq P^d_\ell \quad \forall \ell \in A$$

$$\tilde{P}^d_\ell = \sum_{j \in N^a} S_{t,j} \cdot \tilde{P}^g_j + \sum_{j \in N^a} S_{t,j} \cdot \left( \tilde{P}_j^a - \Delta P^d_j \right) - \sum_{k \in N^d} S_{t,k} \cdot \tilde{P}^d_k \quad \forall \ell \in A.$$
where \( \tilde{P}_d \) and \( \tilde{P}_a \) are the misguided decisions in SCED as a response to \( \tilde{P}_d \), attack vector \( \tilde{a} \):
\[
\tilde{a}^T = \left[ \Delta P_d^T \Delta P_a^T \Delta P_f^T \Delta P_o^T \right].
\] (18)

Note that \( \Delta P_d^t \), \( \Delta P_s^t \) and \( \Delta P_f^t \) are injected to the real-time measurements at time \( t \) to stealthily misguide the decisions of SCED, while \( \Delta P_o^t \) is injected into the real-time measurements at time \( t_\alpha \) 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 \( (\alpha \geq 0) \), 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 \( t_\alpha \). 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].

Equation (12) is equivalent to the undetectable FDI constraint \( \Delta \zeta = H \cdot \Delta x \) 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 \( t_\alpha \), where \( \tilde{P}_d^t - \Delta P_s^t \) is the actual output of the corrupt generators. Equation (15) is the lower and upper bound of \( \Delta P_f^t \). Moreover, the actual power flow at time \( t_\alpha \) must be within the thermal constraints (16), where the expected power flow at time \( t_\alpha \) 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):

\[
\text{AOP:} \quad \max_{a, \tilde{P}_d, \tilde{P}_a} \sum_{j \in N_d^a} p_j \cdot (\tilde{P}_j^d - \sum_{j \in N_d^a} c_j^a (\tilde{P}_j^d - \Delta P_j^d)) - \alpha \cdot ||a|| \quad (7)
\]

\[
\text{s.t.} \quad (8)-(17) \quad \text{and} \quad \tilde{P}_d^t, \tilde{P}_a^t \in G(\tilde{P}_d^t).
\]

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

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

\[
\mathcal{U}(a^*, \tilde{P}_d^*, \tilde{P}_a^*) \geq \mathcal{U}(a, \tilde{P}_d^*, \tilde{P}_a^*), \forall \tilde{P}_d^t, \tilde{P}_a^t \in G(a^*)
\]

\[
\mathcal{U}(a^*, \tilde{P}_d^*, \tilde{P}_a^*) \quad \text{satisfies} \quad \forall a \in A(0, \tilde{P}_d^t), \tilde{P}_d^t, \tilde{P}_a^t \in G(a),
\]

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

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 equivalence 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 \( a, \tilde{P}_d^* \) 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...
of optimal solution for a given attacked set and any solution of binary variables. First, for a given set of attacked meters \( Q, |Q| \leq n \), 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 \( a, P^s \) and \( P^d \) is nonempty (at least \( a = 0 \) satisfies and for any \( P^d \in \mathcal{D} \), \( G(P^d) \neq \emptyset \)) 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 \( a, P^s \) and \( P^d \). 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 \( \delta^d, \delta^s, \delta^f \) and \( \delta^q \), as the attacked sensor indicators of load, generator, power flow, and corrupt generator measurements, respectively. Thus, \( \delta^d_k = 1 \) when the load measurement at Bus \( k \) is attacked, and \( \delta^d_k = 0 \). Otherwise, the number of the attacked meters can be expressed as:

\[
\|a\|_0 = \sum_{k \in N^d} \delta^d_k + \sum_{i \in N^g} \delta^s_i + \sum_{\ell \in \mathcal{A}} \delta^f_\ell + \sum_{j \in N^a} \delta^q_j.
\]

To ensure the equivalence, logical constraints between \( \Delta P^d_k \) and \( \delta^d_k \) must satisfy: 1) \( \Delta P^d_k \neq 0 \Rightarrow \delta^d_k = 1; 2) \( \Delta P^d_k = 0 \Rightarrow \delta^d_k = 0 \). Since we maximize the economic utility, the optimization solution will not change when logical constraint 2) is removed. For example, suppose the indicator \( \delta^d_k \) can be any element in \([0, 1]\) when \( \Delta P^d_k = 0 \). The indicator converges to \( \delta^d_k = 0 \) if \( \Delta P^d_k = 0 \), because \( \delta^d_k = 1 \) 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:

\[
\begin{align*}
\Delta P^d_k &\leq M \cdot \delta^d_k, \quad \forall k \in N^d, \\
\Delta P^d_k &\geq -M \cdot \delta^d_k, \quad \forall k \in N^d,
\end{align*}
\]

where \( M \) is a sufficient large positive value.

Similarly, the logical constraints between \( (\Delta P^g, \delta^s_i), (\Delta P^f, \delta^f_\ell), (\Delta P^a, \delta^q_j) \) can be expressed as:

\[
\begin{align*}
\Delta P^g_i &\leq M \delta^s_i, \quad \forall i \in N^g, \\
\Delta P^g_i &\geq -M \delta^s_i, \quad \forall i \in N^g, \\
\Delta P^f_\ell &\leq M \delta^f_\ell, \quad \forall \ell \in \mathcal{A}, \\
\Delta P^f_\ell &\geq -M \delta^f_\ell, \quad \forall \ell \in \mathcal{A}, \\
\Delta P^a_j &\leq M \delta^q_j, \quad \forall j \in N^a, \\
\Delta P^a_j &\geq -M \delta^q_j, \quad \forall j \in N^a,
\end{align*}
\]

where logical variables satisfy

\[
\delta^d_k, \delta^s_i, \delta^f_\ell, \delta^q_j, \in \{0, 1\}, \quad \forall i \in N^g, j \in N^a, k \in N^d, \ell \in \mathcal{A}. \tag{28}
\]

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

\[
\begin{align*}
\max_{a^*, P^s^*, P^d^*} & \sum_{j \in N^a} p_j \cdot P^s_j - \sum_{j \in N^a} c^a_j \cdot \left( P^d_j - \Delta P^d_j \right) - \alpha \cdot \|a\|_0 \\
\text{s.t.} & \quad (2)-(6), (8), (9), (11)-(17), (20)-(28) \\
& \quad c^d_j + \lambda - \omega_j + \bar{\omega}_j - \sum_{\ell \in A} S_{\ell,i} \cdot \nu_\ell + \sum_{\ell \in A} S_{\ell,i} \cdot \bar{\nu}_\ell = 0, \\
& \quad \forall i \in N^g \\
& \quad c^d_j + \lambda - \mu_j + \bar{\mu}_j - \sum_{\ell \in A} S_{\ell,j} \cdot \nu_\ell + \sum_{\ell \in A} S_{\ell,j} \cdot \bar{\nu}_\ell = 0, \\
& \quad \forall j \in N^a \\
& \quad \omega_j \geq 0, \quad \forall i \in N^g \\
& \quad \bar{\omega}_j \geq 0, \quad \forall i \in N^g \\
& \quad \mu_j \geq 0, \quad \forall j \in N^a \\
& \quad \bar{\mu}_j \geq 0, \quad \forall j \in N^a \\
& \quad \nu_\ell \geq 0, \quad \forall \ell \in A \\
& \quad \bar{\nu}_\ell \geq 0, \quad \forall \ell \in A \\
& \quad \omega_i \leq M \cdot \gamma^\omega, \quad \forall i \in N^g \\
& \quad \bar{o}_i \leq M \cdot \gamma^\bar{o}, \quad \forall i \in N^g \\
& \quad \mu_j \leq M \cdot \gamma^\mu, \quad \forall j \in N^a \\
& \quad \bar{\mu}_j \leq M \cdot \gamma^\bar{\mu}, \quad \forall j \in N^a \\
& \quad \nu_\ell \leq M \cdot \gamma^\nu, \quad \forall \ell \in A \\
& \quad \bar{\nu}_\ell \leq M \cdot \gamma^\bar{\nu}, \quad \forall \ell \in A \\
& \quad \sum_{i \in N^g} S_{\ell,i} \cdot \tilde{P}^s_i + \sum_{j \in N^a} S_{\ell,j} \cdot \tilde{P}^f_j + \tilde{P}^f_\ell - \sum_{k \in N^d} \tilde{P}^d_k \leq M \cdot (1 - \gamma^\ell), \quad \forall \ell \in A \\
& \quad \forall i \in N^g \\
& \quad \forall j \in N^a \\
& \quad \forall \ell \in A \\
& \quad \gamma^\omega_i, \gamma^\bar{o}, \gamma^\mu_j, \gamma^\bar{\mu}_j, \gamma^\nu_\ell, \gamma^\bar{\nu}_\ell \in [0, 1]. \tag{49}
\end{align*}
\]

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], \( \gamma^\omega_i, \gamma^\bar{o}, \gamma^\mu_j, \gamma^\bar{\mu}_j, \gamma^\nu_\ell, \gamma^\bar{\nu}_\ell \) and \( \gamma^\ell \) are new binary variables introduced in the linearization of complementary slackness condition. Binary variables, such as \( \delta^d, \delta^s, \delta^f \) and \( \delta^q \) are determined by \( \Delta P^d, \Delta P^g, \Delta P^a, \Delta P^f \) and \( \Delta P^2 \) in (18). Moreover, \( \Delta P^2 \) depends on \( \Delta P^d, \Delta P^g, \Delta P^a, \Delta P^f, \) and \( \Delta P^2 \) 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 \( S \) (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 \( \sigma^d_k \) be the protection indicator variable, i.e., \( \sigma^d_k = 1 \) if the meter of load \( P^d_k \) is in \( S \), and \( \sigma^d_k = 0 \) otherwise. Similar definitions apply for \( \sigma^r_j \), \( \sigma^l_\ell \) and \( \sigma^f_j \). The possible attack vector for a given protected set \( S \) and load \( P^d \) can be expressed as \( A(S, P^d) \). The relationship between the protected and attacked measurement sets can be expressed as:

\[
\sigma^d_k + \delta^d_k \leq 1, \quad \forall k \in N^d, \\
\sigma^r_j + \delta^r_j \leq 1, \quad \forall j \in N^r, \\
\sigma^l_\ell + \delta^l_\ell \leq 1, \quad \forall \ell \in A, \\
\sigma^f_j + \delta^f_j \leq 1, \quad \forall j \in N^f, \\
\]

where the indicator variables satisfy

\[
\sigma^d_k, \sigma^r_j, \sigma^l_\ell, \sigma^f_j \in \{0, 1\}, \quad \forall i \in N^g, \quad j \in N^a, \quad k \in N^d, \quad \ell \in A. \quad (54)
\]

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:

\[
\min_{S \in \mathcal{S}} \left\{ \beta \cdot |S| + \max_{P^d \in \mathcal{D}} \left\{ \max_{\lambda, \tilde{P}^a, \tilde{P}^e} \frac{\mathcal{U}(\lambda, \tilde{P}^a, \tilde{P}^e)}{\mathcal{U}^0} \right\} \right\}
\]

\[
- \max_{P^a, P^e} \mathcal{U}(0, P^a, P^e)
\]

s.t. (8)–(17), (50)–(54),

\[
(P^a, P^e) \in \mathcal{G}(\tilde{P}^d) = \arg \text{SCEDP}(\tilde{P}^d),
\]

\[
(P^a, P^e) \in \mathcal{G}(P^d) = \arg \text{SCEDP}(\hat{P}^d),
\]

(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 \( S \) denotes all the feasible protection set; 2) The defender maximizes the additional benefit among all the possible load distributions \( D \) 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 \( A(S, P^d), \mathcal{G}(\tilde{P}^d) \) 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:

\[
|S| = \sum_{i \in N^g} \sigma^r_i + \sum_{j \in N^a} \sigma^l_j + \sum_{k \in N^d} \sigma^f_k + \sum_{\ell \in A} \sigma^l_\ell
\]

(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), \( \mathcal{U}(0, P^a, P^e)|_{P_{\text{ext}}} \), can be obtained by solving the following bi-level optimization:

\[
\max_{P^a, P^e} \mathcal{U}(0, P^a, P^e)
\]

\[
(P^a, P^e) \in \mathcal{G}(\hat{P}^d) = \arg \text{SCEDP}(\hat{P}^d)
\]

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

\[
\text{MDP: } \min_{P^a, P^e} \mathcal{C}(P^a, P^e) - \eta \cdot \mathcal{U}(0, P^a, P^e)
\]

s.t. (2)–(6),

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

$$\min_{S \in \mathcal{S}} \left\{ \beta \cdot |S| + \max_{P^d, a, P^s, P^e} \left\{ \mathcal{U}(a, P^a, P^s) - \mathcal{U}(0, P^a, P^e) \right\} \right\}$$

s.t. (8)–(17), (50)–(53),

$$\left\{ P^d, \hat{P} \right\} \in \mathcal{G}(\hat{P}^d),$$

$$P^d \in \mathcal{D}, \quad \text{and} \quad \left\{ P^a, P^e \right\} \in \mathcal{G}'(\hat{P}^d).$$

(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 $\mathcal{G}(\hat{P}^d)$ is determined by SCED at bottom level, as a response to $\hat{P}^d$. $\mathcal{G}'(\hat{P}^d)$ is the KKT optimality condition of MDP. As $\mathcal{U}(a, 0, P^a, P^e)$ is determined by $P^d$ for a given $P^d$, it is equivalent to maximize the additional benefit $\mathcal{U}'$ 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 $\mathcal{U}(0, P^a, P^e)$ 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 SLMLIP using KKT optimality conditions. Hence, the tri-level DAOP here can be simplified to a mixed integer bi-level optimization. Define $S_m = \{ S \in \mathcal{S} | |S| = m \}$ for a constant $m \geq 1$. For any protected set $S \in S_m$, $\beta \cdot |S|$ 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 $S_m$, if the following conditions hold: 1) $S_m \neq \emptyset$; 2) for all $S \in S_m$ and $P^d \in \mathcal{D}$, $\mathcal{A}(S, P^d) \neq \emptyset$, $\mathcal{G}(P^d) \neq \emptyset$, and $\mathcal{G}'(P^d) \neq \emptyset$; 3) there exists $S \in S_m$ such that the attacker’s additional benefit is bounded.

Since $S_m$ consists of all possible protected sets satisfying $|S_m| = m$ and is non-empty, i.e., 1) holds. For any $S \in S_m$ 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 $\mathcal{G}(P^d) \neq \emptyset$. As for any load $P^d \in \mathcal{D}$, solution exists in SCED, we have $\mathcal{G}'(P^d) \neq \emptyset$, $\mathcal{G}'(P^d) \neq \emptyset$, and 2) holds for all possible $S_m$. Moreover, since $P^s$ and $P^a$ ($P^x$ and $P^e$) are limited by generation capacities, the financial benefit is finite.

That is, 3) hold for all possible $S_m$. 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):

$$\text{SP :} \quad \max_{P^d, a, P^a, P^e} \mathcal{U}(a, P^a, P^e) - \mathcal{U}(0, P^a, P^e)$$

s.t. (8)–(17), (50)–(53),

$$\left\{ P^d, \hat{P} \right\} \in \mathcal{G}(\hat{P}^d),$$

$$P^d \in \mathcal{D}, \quad \text{and} \quad \left\{ P^a, P^e \right\} \in \mathcal{G}'(\hat{P}^d).$$

(59)

Similar to the method in Section III-C, the subproblem above can be simplified to a SLMLIP 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 $P^s = P^{sx}, P^e = P^{xe}$, and the additional benefit is zero when $P^d = P^d, i.e., \Delta P^d = 0$. 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 than the number of load $|N^d|$. The detailed algorithm is given in Algorithm 1.

In Algorithm 1, iterations terminate when $|S| = |N^d|$ or $\mathcal{U}' \leq \varepsilon$. 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

<table>
<thead>
<tr>
<th></th>
<th>gen. bus</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>6</th>
<th>8</th>
<th>–</th>
</tr>
</thead>
<tbody>
<tr>
<td>14-bus</td>
<td>min. cap (MW)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>100</td>
<td>600</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>max. cap (MW)</td>
<td>100</td>
<td>100</td>
<td>600</td>
<td>100</td>
<td>600</td>
<td>–</td>
</tr>
<tr>
<td></td>
<td>marg. cost ($/MWh)</td>
<td>30</td>
<td>30</td>
<td>20</td>
<td>25</td>
<td>20</td>
<td>–</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>gen. bus</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>6</th>
<th>8</th>
<th>–</th>
</tr>
</thead>
<tbody>
<tr>
<td>30-bus</td>
<td>min. cap (MW)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>max. cap (MW)</td>
<td>600</td>
<td>100</td>
<td>110</td>
<td>30</td>
<td>590</td>
<td>50</td>
</tr>
<tr>
<td></td>
<td>marg. cost ($/MWh)</td>
<td>20</td>
<td>30</td>
<td>25</td>
<td>30</td>
<td>20</td>
<td>30</td>
</tr>
</tbody>
</table>

Algorithm 1 Heuristic "Incentive-Reduction" Algorithm

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

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.

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 are 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 ~ 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$/h for total load within 1200MW ~ 1450MW, and the financial benefit under attack is about 3 times of the normal benefit when the total load is 1250MW. Moreover, in the 30-bus system, the additional benefit is about 200$/h for the total load within 1200MW ~ 1450MW, and the financial benefit under attack is about twice of the normal benefit.
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 $P_{d_2}^1$, $P_{d_3}^1$, $P_{d_4}^1$, and $P_{d_5}^1$, when loads are $P_{g_1}^1 = 108MW$, and $P_{g_2}^1 = 1276MW$. The reason is that attacker can redistribute load to change the scheduled generation output utilizing thermal constraints on line 3-4. By protecting $P_{d_1}^1$, $P_{d_2}^3$, and $P_{d_3}^3$, 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 $P_{d_1}^{13}$ and $P_{d_2}^{13}$ 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 readings of $P_{d_2}^{13}$, $P_{d_3}^{13}$, and $P_{d_5}^{13}$, when loads are $P_{g_1}^{13} = 1276MW$ and $P_{g_2}^{13} = 1229.9MW$. 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

### Table III

<table>
<thead>
<tr>
<th>Items</th>
<th>Protected meters</th>
<th>$F^P$(MW)</th>
<th>$W^P$($/h)$</th>
<th>Attacked meters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Case 1</td>
<td>$P_{d_1}$</td>
<td>(1238.1,0.0,...,0)</td>
<td>1827.1</td>
<td>$P_{d_2}^{13}$, $P_{d_3}^{13}$, $P_{d_5}^{13}$</td>
</tr>
<tr>
<td>Case 2</td>
<td>$P_{d_1}$</td>
<td>(108,1276.0,...,16.0,0.0)</td>
<td>460</td>
<td>$P_{d_2}^{13}$, $P_{d_3}^{13}$, $P_{d_5}^{13}$</td>
</tr>
</tbody>
</table>

Note: $S_1 = \{1,2,1,2,3,2,4,2,4,7,4,9,5,6,11,6,12,6,13,7,8,9,10,9,14\}$, and $S_2 = \{1,2,1,3,3,2,4,2,5,2,6,7,6,8,9,6,10,6,28,9,11,4,12,13,14,12,15,12,16,14,15,16,17,18,19,19,20,10,21,10,22,15,23,24,25,25,26,25,27,27,29,27,30\}$, 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.

### 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 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 $P_{d_2}^1$, $P_{d_3}^1$, $P_{d_4}^1$, and $P_{d_5}^1$, when loads are $P_{g_1}^1 = 108MW$, and $P_{g_2}^1 = 1276MW$. The reason is that attacker can redistribute load to change the scheduled generation output utilizing thermal constraints on line 3-4. By protecting $P_{d_1}^1$, $P_{d_2}^3$, and $P_{d_3}^3$, 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 $P_{d_1}^{13}$ and $P_{d_2}^{13}$ 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 readings of $P_{d_2}^{13}$, $P_{d_3}^{13}$, and $P_{d_5}^{13}$, when loads are $P_{g_1}^{13} = 1276MW$ and $P_{g_2}^{13} = 1229.9MW$. 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

### Table III

<table>
<thead>
<tr>
<th>Items</th>
<th>Protected meters</th>
<th>$F^P$(MW)</th>
<th>$W^P$($/h)$</th>
<th>Attacked meters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Case 1</td>
<td>$P_{d_1}$</td>
<td>(1238.1,0.0,...,0)</td>
<td>1827.1</td>
<td>$P_{d_2}^{13}$, $P_{d_3}^{13}$, $P_{d_5}^{13}$</td>
</tr>
<tr>
<td>Case 2</td>
<td>$P_{d_1}$</td>
<td>(108,1276.0,...,16.0,0.0)</td>
<td>460</td>
<td>$P_{d_2}^{13}$, $P_{d_3}^{13}$, $P_{d_5}^{13}$</td>
</tr>
</tbody>
</table>

Note: $S_1 = \{1,2,1,2,3,2,4,2,4,7,4,9,5,6,11,6,12,6,13,7,8,9,10,9,14\}$, and $S_2 = \{1,2,1,3,3,2,4,2,5,2,6,7,6,8,9,6,10,6,28,9,11,4,12,13,14,12,15,12,16,14,15,16,17,18,19,19,20,10,21,10,22,15,23,24,25,25,26,25,27,27,29,27,30\}$, 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.
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 strategy to protect a minimal number of meters. Since the robust attack vector must satisfy $H f \Delta x = H b \Delta x$ [3], i.e.,

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

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 $\Delta P b^i$ is the modification of bus injection, and the injection of Bus $i$, $\Delta P f^i = \Delta P f^i - \Delta P b^i$. Since $H b$ is invertible, the relationship between $\Delta P f^i$ and $\Delta P b^i$ can be expressed as $\Delta P f^i = H f \cdot (H b)^{-1} \cdot \Delta P b^i$, where $H f \cdot (H b)^{-1}$ is shift factor matrix. To deter bad data detection in state estimation, the injected attack vector must satisfy:

$$
\Delta P f^i = - \sum_{k \in N^i} S_{k,i} \cdot \Delta P f^k + \sum_{i \in A} S_{i,i} \cdot \Delta P b^i, \quad \forall \ell \in A.
$$

Thus, $\Delta P f^i$ is determined by $\Delta P f^k$ and $\Delta P b^i$.

REFERENCES


