Defending Against False Data Injection Attacks on Power System State Estimation

Ruilong Deng, *Member, IEEE*, Gaoxi Xiao, *Member, IEEE*, and Rongxing Lu, *Senior Member, IEEE*

***Abstract*—This paper investigates the problem of defending against false data injection (FDI) attacks on power system state estimation. Although many research works have been previously reported on addressing the same problem, most of them made a very strong assumption that some meter measurements can be absolutely protected. To address the problem practically, a reasonable approach is to assume whether or not a meter measurement could be compromised by an adversary does depend on the defense budget deployed by the defender on the meter. From this perspective, our contributions focus on designing the least-budget defense strategy to protect power systems against FDI attacks. In addition, we also extend to investigate choosing which meters to be protected and determining how much defense budget to be deployed on each of these meters. We further formulate the meter selection problem as a mixed integer nonlinear programming problem, which can be efficiently tackled by Benders' decomposition. Finally, extensive simulations are conducted on IEEE test power systems to demonstrate the advantages of the proposed approach in terms of computing time and solution quality, especially for large-scale power systems.**

***Index Terms*—Cyber attack, false data injection (FDI), power system, state estimation.**

I. Introduction

THE POWER system is a large, sophisticated and interconnected infrastructure that delivers electricity from power plants to end users. Current power systems are continuously monitored and controlled by energy management system/supervisory control and data acquisition (EMS/SCADA) systems to maintain the operating condition in a normal and secure state. Precisely, power system state estimation is to estimate state variables based on meter measurements, and then the estimated state will be used to control electrical grids [1]–[3].

As electricity infrastructures are gradually transformed toward smart grids with integration of information and communications technology (ICT) and cyber components, power systems become more open to and cyberly accessible from outside networks, such as Internet-based office networks and smart meters with two-way communication between supplier and consumer [4]–[6]. Despite the advances, this integration also leads to new vulnerabilities of cyber security, which has been reported as one of the main threats to the reliable operation of power systems [7]–[11]. Concretely, with new entry points being introduced into power systems, potential complex and cooperative cyber attacks are also brought in. For example, recent research shows that the carefully synthesized false data injection (FDI) attacks could bypass bad data detection (BDD) in today's EMS/SCADA systems and introduce arbitrary errors to power system state estimation without being detected [12]. By injecting biased state estimates, FDI attacks could manipulate electricity price in power market to arbitrage financial profit, or worse still, mislead system operator and result in harmful commands to cause regional blackout [13].

Up to now, many studies have come up with several countermeasures to defend against FDI attacks. For example, some existing works proposed to secure some meter measurements and/or some state variables to make FDI attacks unable to stealthily launch [14]–[16]. Other works investigated how FDI attacks could impact electricity market operations by manipulating real-time locational marginal price [17]–[19]. However, none of them has considered the behavior of the attacker and the interaction between the defender and attacker. In addition, the assumption that some meter measurements can be absolutely protected would be too strong for real applications. A more practical assumption is that whether or not a meter measurement could be compromised by an adversary dose depend on the defense budget deployed by the defender on the meter. Following this research line, in this paper, we formulate the behavior of a rational attacker, and investigate how the defender and attacker with different objectives could compete and interact with each other. In particular, we intend to provide insightful guidance on how to deploy the least defense budget to guarantee that the attacker cannot modify any set of state variables. Our main contributions focus on the least-budget defense strategy design and the efficient solution to the meter selection problem, which can be summarized as follows.

1) We formulate the behavior of a rational attacker, investigate the interaction between the defender and attacker, and then design the least-budget defense strategy to make power systems immune to FDI attacks.
2) We formulate the meter selection problem as a mixed integer nonlinear programming (MINLP) problem, and efficiently solve it using Benders' decomposition, achieving satisfactory performance in terms of computing time and solution quality, especially for the large-scale power systems.

This paper is organized as follows. The preliminaries and related works are presented in Section II, and the system

Manuscript received February 14, 2015; revised July 01, 2015; accepted August 11, 2015. Date of publication August 19, 2015; date of current version February 06, 2017. This work was supported by School of Electrical and Electronic Engineering (EEE) Cybersecurity Research Program, Nanyang Technological University, under Nanyang Technological University Start-Up Grant (NTU-SUG) M4081196. Paper no. TII-15-0265. *(Corresponding author: Gaoxi Xiao.)*

The authors are with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore 639798 (e-mail: rldeng@ntu.edu.sg; egxxiao@ntu.edu.sg; rxlu@ntu.edu.sg).

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/TII.2015.2470218

TABLE I
SUMMARY OF NOTATIONS

Symbol[a]	Definition	Unit[b]
i, m, $\mathcal{M}$	Index, number, set of meter measurements	n/a
j, n, $\mathcal{N}$	Index, number, set of state variables	n/a
z_i	ith meter measurement	p.u.
x_j	jth state variable	p.u.
e_i	ith measurement error (noise)	p.u.
$\boldsymbol{H}$	Measurement Jacobian matrix	n/a
$\boldsymbol{H}^*$	Reconstructed $\boldsymbol{H}$ matrix	n/a
θ_j	Bus j voltage angle	rad
F_{ij}	Branch (i, j) active power flow	MW
P_j	Bus j active power injection	MW
b_{ij}	Susceptance of transmission line (i, j)	℧
$\boldsymbol{r}$	Measurement residual vector	n/a
$\boldsymbol{a}$	Attack vector on meter measurements	n/a
$\boldsymbol{c}$	False data injection vector on state variables	n/a
b_i	Defense budget to protect meter measurement z_i	p.u.
k_i	Attack cost to compromise meter measurement z_i	p.u.
$r(j)$	Attack cost to modify state variable x_j	p.u.
B	Defender's limited budget	p.u.
R	Attacker's limited resource	p.u.
$f_i(\cdot)$	Attack cost function	n/a
ψ_i	Binary variable to protect meter measurement z_i	n/a

[a] The bold symbol $\boldsymbol{x}$ denotes the vector of x, and the hat symbol $\hat{x}$ denotes the estimate of x.
[b] The unit of a quantity may be omitted in the rest of the paper if it is specified here.

model is built in Section III. In Section IV, we formulate the least-budget defense problem, whose solution is provided in Section V. In Section VI, we extend to investigate the meter selection problem with efficient solution. Simulation results are given in Section VII, and concluding remarks are drawn in Section VIII with future work.

II. Preliminaries and Related Works

Some important notations used in this paper are summarized in Table I. In the rest of this work, we also use the following mathematical notations from linear algebra: $\boldsymbol{A}^T$ denotes the transpose of $\boldsymbol{A}$; $\boldsymbol{A}^{-1}$ denotes the inverse of $\boldsymbol{A}$; $\operatorname{rank}(\boldsymbol{A})$ denotes the rank of $\boldsymbol{A}$; $\boldsymbol{I}$ denotes the identity (unit) matrix; $\boldsymbol{1}$ denotes the all-ones vector; $\boldsymbol{0}$ denotes the all-zeros vector; and $\|\boldsymbol{x}\|_2$ denotes the $\mathcal{L}_2$ (Euclidean) norm of $\boldsymbol{x}$.

A. Power System State Estimation

Consider a steady-state power system with $n+1$[1] buses and m meters. The state estimation problem is to estimate state variables $\boldsymbol{x} = [x_1, x_2, \ldots, x_n]^T$ based on meter measurements $\boldsymbol{z} = [z_1, z_2, \ldots, z_m]^T$, under independent random measurement errors (noises) $\boldsymbol{e} = [e_1, e_2, \ldots, e_m]^T$, assumed to be following Gaussian distribution with zero mean and diagonal covariance matrix $\boldsymbol{\Sigma}$ [i.e., $\boldsymbol{e} \sim N(\boldsymbol{0}, \boldsymbol{\Sigma})$]. The n state variables are n bus voltage angles; the m meter measurements are branch active power flows and bus active power injections (generation minus load). The meter measurements $\boldsymbol{z}$ are related to the state variables $\boldsymbol{x}$ as: $\boldsymbol{z} = \boldsymbol{h}(\boldsymbol{x}) + \boldsymbol{e}$,

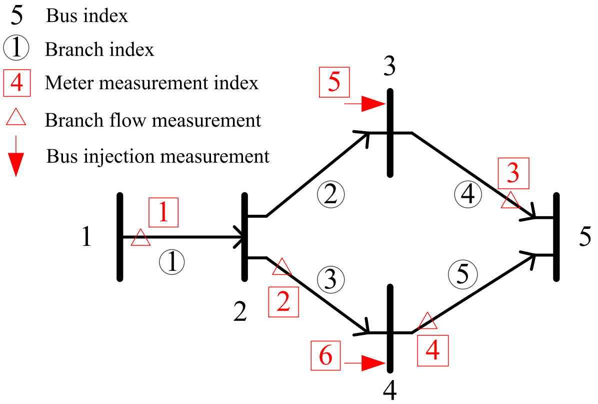


Fig. 1. Example of a partially measured 5-bus power system.

where $\boldsymbol{h}(\boldsymbol{x}) = [h_1(\boldsymbol{x}), h_2(\boldsymbol{x}), \ldots, h_m(\boldsymbol{x})]^T$ and $h_i(\boldsymbol{x})$ is a nonlinear function of $\boldsymbol{x}$. In dc (linearized) power flow model [20], the linear approximation to the nonlinear relationship is expressed as

$$\boldsymbol{z} = \boldsymbol{H}\boldsymbol{x} + \boldsymbol{e} \tag{1}$$

where $\boldsymbol{H} = [h_{ij}]_{m \times n}$ is the measurement Jacobian matrix (which is of full column rank when $m > n$, as is the typical case), defined as

$$\boldsymbol{H} = \left.\frac{\partial \boldsymbol{h}(\boldsymbol{x})}{\partial \boldsymbol{x}^T}\right|_{\boldsymbol{x}=\boldsymbol{0}} = \left[\left.\frac{\partial h_i(\boldsymbol{x})}{\partial x_j}\right|_{x_j=0}\right]_{m \times n}.$$

Take the partially measured 5-bus power system in Fig. 1 as an example. If bus 1 is chosen as the reference bus (i.e., $\theta_1 = 0$), then the state variables are $\boldsymbol{x} = [\theta_2, \theta_3, \theta_4, \theta_5]^T$, and the meter measurements are $\boldsymbol{z} = [F_{12}, F_{24}, F_{35}, F_{45}, P_3, P_4]^T$ (partially measured) [16, Fig. 1]. Based on the dc power flow model, the measurement Jacobian matrix is

$$\boldsymbol{H} = \begin{pmatrix} b_{12} & 0 & 0 & 0 \\ -b_{24} & 0 & b_{24} & 0 \\ 0 & -b_{35} & 0 & b_{35} \\ 0 & 0 & -b_{45} & b_{45} \\ b_{23} & -b_{23} - b_{35} & 0 & b_{35} \\ b_{24} & 0 & -b_{24} - b_{45} & b_{45} \end{pmatrix}$$

where b_{ij} denotes the susceptance of transmission line (i, j).

The state estimation problem is to find an estimate $\hat{\boldsymbol{x}}$ of state variables $\boldsymbol{x}$ that is the best fit of the meter measurements $\boldsymbol{z}$ according to (1) (which is an over determined linear system). The measurement residual is $\boldsymbol{r} = \boldsymbol{z} - \hat{\boldsymbol{z}} = \boldsymbol{z} - \boldsymbol{H}\hat{\boldsymbol{x}}$ (i.e., the difference between the observed measurements $\boldsymbol{z}$ and the estimated measurements $\hat{\boldsymbol{z}}$). The weighted least-squares (WLS) criterion problem is to find an estimate $\hat{\boldsymbol{x}}$ that minimizes the performance index $J(\hat{\boldsymbol{x}})$, defined as $\min_{\hat{\boldsymbol{x}}} J(\hat{\boldsymbol{x}}) \triangleq (\boldsymbol{z} - \boldsymbol{H}\hat{\boldsymbol{x}})^T \boldsymbol{W} (\boldsymbol{z} - \boldsymbol{H}\hat{\boldsymbol{x}})$, where the weight matrix $\boldsymbol{W} \triangleq \boldsymbol{\Sigma}^{-1}$ (i.e., a diagonal matrix whose entries are reciprocals of the variances of measurement errors $\boldsymbol{e}$). Then, $J(\hat{\boldsymbol{x}})$ is differentiated to obtain the first-order optimal condition [21, Ch. 3]

$$\hat{\boldsymbol{x}} = \left(\boldsymbol{H}^T \boldsymbol{W} \boldsymbol{H}\right)^{-1} \boldsymbol{H}^T \boldsymbol{W} \boldsymbol{z} \triangleq \boldsymbol{E}\boldsymbol{z} \tag{2}$$

[1] We choose an arbitrary bus as the reference (slack) bus with zero voltage angle (i.e., $\theta = 0$). The column corresponding to this bus will not be included in the measurement Jacobian matrix.

where $\boldsymbol{E}$ is known as the "pseudo-inverse" of $\boldsymbol{H}$ since $\boldsymbol{E}\boldsymbol{H} = \boldsymbol{I}$. Besides WLS criterion, some other statistical estimation criteria, such as maximum likelihood criterion and minimum variance criterion, are commonly used in state estimation [22, Ch. 12]. When the measurement errors are assumed to be normally distributed with zero mean, these criteria lead to the identical optimal state estimator $\boldsymbol{E}$ [12]. Since $\operatorname{rank}(\boldsymbol{E}) = \operatorname{rank}(\boldsymbol{H}) = n < m$, at least n meters are needed to derive a unique state estimation. The minimum set of measurements required to estimate n state variables is referred to as basic/essential measurements. The other $m - n$ redundant measurements provide redundancy to resist random noises for BDD.

B. FDI Attacks

Errors could be introduced into the meter measurements due to various reasons, such as meter failures and malicious attacks. The current power systems use the following technique for BDD to protect state estimation [21, Ch. 8]: calculate the measurement residual $\boldsymbol{r}$ and compare its $\mathcal{L}_2$ (Euclidean) norm $\|\boldsymbol{r}\|_2$ (gross errors or bias) against a prescribed threshold τ to detect bad measurements (outliers). Specifically, the existence of bad measurements is assumed if $\|\boldsymbol{r}\|_2 > \tau$, otherwise $\boldsymbol{z}$ is considered as normal measurements.

Assume that the independent random measurement errors follow normal distribution with zero mean. It can be mathematically derived that $\|\boldsymbol{r}\|_2^2$ follows χ^2_{m-n} distribution, i.e., chi-square distribution with $m - n$ degrees of freedom (since state estimation is constrained by n independent equations). According to [21, Ch. 8], τ is determined by a hypothesis test with a significance level (false alarm probability) α, i.e., $\Pr\left\{\|\boldsymbol{r}\|_2^2 \geq \tau^2\right\} = \alpha$. This means that $\|\boldsymbol{r}\|_2 > \tau$ identifies bad measurements with a false alarm probability α.

Let $\boldsymbol{z}_a$ denote the malicious measurements that contain malicious data $\boldsymbol{a}$, i.e., $\boldsymbol{z}_a = \boldsymbol{z} + \boldsymbol{a}$, where $\boldsymbol{a} = [a_1, a_2, \ldots, a_m]^T$ is referred to as an attack vector. In general, $\boldsymbol{a}$ is likely to be identified by BDD if it is unstructured. However, it has been found in [12] that some well-structured attack vectors, e.g., $\boldsymbol{a} = \boldsymbol{H}\boldsymbol{c}$, where $\boldsymbol{c} = [c_1, c_2, \ldots, c_n]^T$ is an arbitrary nonzero vector, can systematically bypass BDD.

Theorem 1 [12]. Suppose the original measurements $\boldsymbol{z}$ can pass BDD. The malicious measurements $\boldsymbol{z}_a$ can also pass it if the attack vector

$$\boldsymbol{a} = \boldsymbol{H}\boldsymbol{c}. \tag{3}$$

The attacks with the attack vector $\boldsymbol{a} = \boldsymbol{H}\boldsymbol{c}$ are referred to as FDI attacks (also known as "unobservable" attacks since the system operator cannot distinguish $\hat{\boldsymbol{x}}_a$ from $\hat{\boldsymbol{x}}$). In such a case, the system operator would mistake $\hat{\boldsymbol{x}}_a$ for the valid estimate of state variables $\boldsymbol{x}$, and thus arbitrary errors $\boldsymbol{c}$ can be injected into state estimation $\hat{\boldsymbol{x}}$ without being detected. By modifying state variables, FDI attacks could manipulate electricity price in power market to make financial profit, or, worse still, could mislead the system operator and result in harmful control commands to cause regional blackout.

C. Related Works

A common countermeasure to defend against FDI attacks on power system state estimation can be achieved by either securing a number of meter measurements physically or monitoring a number of state variables directly by phasor measurement units (PMUs). For example, Bobba *et al.* [14] proposed to detect FDI attacks by protecting a strategically selected set of meter measurements and state variables. When there is no verifiable state variable, it is necessary and sufficient to secure a set of basic measurements to detect attacks. Kim and Poor [15] proposed a fast greedy algorithm to select a subset of meter measurements to protect against FDI attacks. They also developed another greedy algorithm to facilitate the strategic placement of secure PMUs for defense. Jia *et al.* [19] studied the impacts of malicious data attacks on real-time price of electrical market operations. They analyzed the chance that the adversary can make profit by intelligently manipulating values of meter measurements.

In summary, the aforementioned works proposed to secure some meter measurements and/or some state variables to make FDI attacks unable to be stealthily launched. They have assumed that some meter measurements can be absolutely protected, i.e., the adversary cannot compromise them no matter how powerful he is. This assumption would be too strong for real applications. A more practical approach is to assume that whether or not a meter measurement could be compromised by an adversary depends on the defense budget deployed by the defender on the meter. From this perspective, our contributions focus on designing the least-budget defense strategy to guarantee that the adversary cannot modify any set of state variables. Furthermore, we extend to investigate choosing which meters for protecting and determining how much defense budget to be deployed on each of these meters, such that the power system can be immune to FDI attacks. In this context, our work will provide insightful guidance on protecting power systems from cyber attacks in real practice.

III. System Model

A. Attack Model

To launch FDI attacks without being detected, the attacker needs to compromise a set of meter measurements simultaneously. Take the 5-bus power system in Fig. 1 as an example. If the attacker wants to modify the state variable x_1, he needs to compromise the set $[z_1, z_2, z_5, z_6]$ of meter measurements at the same time to bypass BDD. This is because that for $\boldsymbol{c} = [c_1, 0, 0, 0]^T$, $\boldsymbol{a} = \boldsymbol{H}\boldsymbol{c} = [b_{12}c_1, -b_{24}c_1, 0, 0, b_{23}c_1, b_{24}c_1]^T$. This scenario corresponds to the constrained case of targeted FDI attacks as that in [12]. Obviously if the attacker wants to modify more state variables, he needs to compromise more meter measurements. Note that in this paper, we define an "attack" as introducing "arbitrary" errors, rather than "specific" errors, into state variables. Although leveraging possible cancellations in the $\boldsymbol{H}$ matrix by inserting specific errors into multiple state variables may construct potentially less expensive attacks, single-state variable attacks associated with arbitrary errors can give the adversary full freedom to achieve his attack goal. Under such case, it is easier for the adversary to launch a constrained targeted FDI attacks than an unconstrained one.

Assume that a rational attacker will choose the easiest target of state variable (with the least cost) to attack. A successful attack is to modify (introduce arbitrary errors into)[2] at least one-state variable without being detected. The attacker's objective is to launch an attack with the least cost. His capabilities include:

1) the knowledge of the power network topology and configuration of the power system, i.e., the $\boldsymbol{H}$ matrix;
2) the ability to access any set of meter measurements simultaneously, which may or may not be compromised depending on the defender's protection budget.

B. Defense Model

Consider a power system with a set $\mathcal{N} = \{1, 2, \ldots, n\}$ of state variables and a set $\mathcal{M} = \{1, 2, \ldots, m\}$ of meter measurements. A common countermeasure to defend against FDI attacks is to physically secure meter measurements by, for instance, guards, video monitoring, tamper-proof communication systems, etc. The defender needs to decide the allocation of the defense budget for the protection of m meter measurements. Let $\boldsymbol{b} = [b_1, b_2, \ldots, b_m]^T$ denote the defender's budget allocation vector, where b_i is the allocated budget for protecting the meter measurement z_i. For example, if $b_i = 0$, there is no defense deployed on z_i.

Under the defender's strategy $\boldsymbol{b}$, the attack cost k_i for an attacker to successfully compromise the meter measurement z_i is assumed to be a function of the deployed budget b_i

$$k_i = f_i\left(b_i\right) \quad \forall i \in \mathcal{M}. \tag{4}$$

When b_i increases, the corresponding k_i should also rise, i.e., it will be more difficult to compromise z_i. Accordingly, the cost function $f_i\left(\cdot\right)$ should be formulated as a monotonic function, and $\boldsymbol{k} = [k_1, k_2, \ldots, k_m]^T$ denotes the attacker's attack cost vector.

IV. Problem Formulation

A. Attack Formulation

For ease of illustration, we construct an $\boldsymbol{H}^*$ matrix from the $\boldsymbol{H}$ matrix. The reconstruction rule is defined as follows:

$$h^*_{ij} = \begin{cases} 0, \text{if } h_{ij} = 0 \\ 1, \text{otherwise} \end{cases} \quad \forall i \in \mathcal{M}, \forall j \in \mathcal{N}. \tag{5}$$

Taking the 5-bus power system in Fig. 1 as an example

$$\boldsymbol{H}^* = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$$

and the jth column of $\boldsymbol{H}^*$ is denoted by $\boldsymbol{h}^*_j \in \mathbb{R}^{m \times 1}$. For instance, $\boldsymbol{h}^*_1 = [1, 1, 0, 0, 1, 1]^T$.

With the $\boldsymbol{H}^*$ matrix, the attack cost for an attacker to successfully modify the state variable x_j without being detected can be expressed as

$$r\left(j\right) = \boldsymbol{h}^{*T}_j \boldsymbol{k} = \sum_{i=1}^{m} h^*_{ij} k_i \quad \forall j \in \mathcal{N}. \tag{6}$$

For the 5-bus power system in Fig. 1, $r\left(1\right) = k_1 + k_2 + k_5 + k_6$. That is to say, if the attacker wants to modify the state variable x_1, the total attack cost is the sum of costs to compromise the meter measurements z_1, z_2, z_5, and z_6. A reasonable assumption is that a rational attacker will choose the easiest target of state variable (with the least cost) to attack. Thus, the attacker's strategy can be formulated as

$$\begin{aligned} &\min_{j \in \mathcal{N}} \quad r\left(j\right) \\ &\text{s.t.} \quad (4)\text{–}(6). \end{aligned} \tag{7}$$

B. Defense Formulation

The interaction between the defender and attacker can be viewed as a two-player zero-sum (strictly competitive) game. The defender plays first, by deploying the protection strategy $\boldsymbol{b}$, while the attacker plays next, by launching an attack on the easiest target x_j (with the least cost) without being detected. It is reasonable to assume that the defender does not know the attacker's strategy beforehand, but the attacker may have zero, partial, or full knowledge of the defender's strategy. In real situation, the attacker will try his best to acquire such information. With more information being collected, the risk (probability) of launching a successful attack goes up. According to risk management theory, for any strategy played by the defender, the easiest target (with the least attack cost) under the strategy always exists [23]. This is the worst-case situation, which corresponds to that the attacker fully knows the defender's strategy. That is, given $\boldsymbol{b}$, the worst case can be achieved by solving (7). The worst-case solution provides a benchmark for risk assessment.

With more information, the attacker can only increase the risk (probability) of launching a successful attack, but cannot further cut down the least attack cost. Thus, the defender's best (versatile) strategy against any attacker's strategy is to raise up the least attack cost as much as possible, under the constraint of the total defense budget B. We have a *primal problem*

$$\begin{aligned} &\max_{\boldsymbol{b} \geq \boldsymbol{0}} \quad \min_{j \in \mathcal{N}} r\left(j\right) \\ &\text{s.t.} \quad \begin{cases} \sum\limits_{i=1}^{m} b_i \leq B \\ (4)-(6). \end{cases} \end{aligned} \tag{8}$$

V. Solution

The maximin problem (8) of the defender is to maximize the attack cost of the attacker for the worst-case scenario. Previous

[2] Throughout the following text, the terms "modify" and "attack" will be interchangeably used, with the same meaning of introducing arbitrary errors into state variables without being detected.

attempts to solve the maximin problem mostly focused on a special case—the saddle point solution, which is relatively easier to be characterized, but requests the following condition to hold [23]:

$$\max_{\boldsymbol{b}\geq\boldsymbol{0}}\ \min_{j\in\mathcal{N}}\ r\left(j\right)=\min_{j\in\mathcal{N}}\ \max_{\boldsymbol{b}\geq\boldsymbol{0}}\ r\left(j\right). \tag{9}$$

However, the saddle point condition (9) requires two players to satisfy some strict restrictions such as simultaneousness. In real situation, such a condition cannot always hold. To tackle the problem, we transform the primal problem into an equivalent one, regardless of whether (9) holds or not.

A. Transformation

Assume that the adversary has the limited attack resource R due to the limited attack duration (within the system maintenance period). The defender intends to deploy the defense budget as low as possible while guaranteeing that the attacker cannot modify any set of state variables (i.e., even the least attack cost needed is still greater than the attacker's limited resource R). In this context, the primal problem (8) can be transformed into an *equivalent problem*

$$\min_{\boldsymbol{b}\geq\boldsymbol{0}}\quad \sum_{i=1}^{m} b_i \tag{10}$$

$$\text{s.t.}\quad \begin{cases}\min\limits_{j\in\mathcal{N}} r\left(j\right)\geq R\\ (4){-}(6)\end{cases}. \tag{10a}$$

Through the equivalent transformation, the minimization operation on the variable j has been moved from the objective function (8) into the constraint (10a), which becomes easier to tackle. The detailed transformation process is elaborated in Appendix A to show the equivalence between (8) and (10).

For (10), the constraint (10a) can be rewritten into the equivalent form of: $r\left(j\right)\geq R\quad \forall j\in\mathcal{N}$. Note that if denote $\boldsymbol{r}=\left[r\left(1\right),r\left(2\right),\ldots,r\left(n\right)\right]^T$ and $\boldsymbol{R}=R\times\boldsymbol{1}$, the constraint (10a) is equivalent to: $\boldsymbol{r}\geq\boldsymbol{R}$. Recall the constraint (4), where $f_i\left(b_i\right)$ is a linear or nonlinear function of b_i. Regardless of which type of function it is, the linear approximation to the cost function (4) is: $\boldsymbol{k}=\boldsymbol{f}\cdot\boldsymbol{b}$, where $\boldsymbol{f}$ is the cost function Jacobian vector defined as

$$\boldsymbol{f}=\left[\left.\frac{\partial f_i\left(b_i\right)}{\partial b_i}\right|_{b_i=0}\right]_{m\times 1}.$$

Besides, recall the constraint (6), and thus we have: $\boldsymbol{r}=\left[\boldsymbol{h}_1^*,\boldsymbol{h}_2^*,\ldots,\boldsymbol{h}_n^*\right]^T\boldsymbol{k}=\boldsymbol{H}^{*T}\boldsymbol{k}=\boldsymbol{H}^{*T}\left(\boldsymbol{f}\cdot\boldsymbol{b}\right)$.

From the above, (10) can be rewritten into the equivalent form of a linear programming (LP) problem

$$\begin{aligned}\min_{\boldsymbol{b}\geq\boldsymbol{0}}\quad & \boldsymbol{1}^T\boldsymbol{b}\\ \text{s.t.}\quad & \boldsymbol{H}^{*T}\left(\boldsymbol{f}\cdot\boldsymbol{b}\right)\geq\boldsymbol{R}.\end{aligned} \tag{11}$$

The problem can be efficiently solved with the computational complexity generally bounded by a polynomial function of the size of the problem m.

TABLE II
COMPARISON OF NUMERICAL SOLUTIONS

#	Metric		
	Defense strategy $\boldsymbol{b}$	Least defense budget $\sum_{i=1}^{m} b_i$	Total attack cost $\sum_{j=1}^{n} r\left(j\right)$
Solution 1	[0 0.2 0.4 0 0.6 0.8]	2	5.4
Solution 2	[0 1 1 0 0 0]	2	4
Solution 3	[0 0 0 0 1 1]	2	6

B. Simplest Case

Take the 5-bus power system in Fig. 1 as an example. For ease of illustration, consider the simplest case where $\boldsymbol{f}=\boldsymbol{R}=\boldsymbol{1}$. By means of LP, we may obtain the solution 1 as shown in Table II. The least defense budget needed is 2, which means that if the defender strategically deploys $[0.2\tilde{}0.4\tilde{}0.6\tilde{}0.8]$ on the set $[z_2,z_3,z_5,z_6]$ of meter measurements, it is guaranteed that the attacker cannot modify any set of state variables.

Although LP can efficiently get a solution for (11), however, since $\boldsymbol{H}^{*T}$ is the $n\times m$ matrix and $n<m$ is the typical case, (11) is an under determined linear system, and theoretically has infinitely many solutions. For example, the solution 2 shown in Table II is also a solution. Nevertheless, from the practical point of view, we may consider that the solution 1 would be better than the solution 2 since the total attack cost that the attacker could modify all state variables, i.e., $\sum_{j=1}^{n} r\left(j\right)$, under the former defense strategy is larger. From the above observation, we may consider additional practical constraints or objectives to let the solution make more sense in real-life applications.

C. Multiobjective Optimization

Inspired by the discussion in Section V-B, we consider another objective, namely maximizing the total attack cost $\sum_{j=1}^{n} r\left(j\right)$. We need a tuning parameter to balance the two objectives, and in choosing the tuning parameter, we should consider the former objective of minimizing the total defense budget as the primary objective. How to theoretically determine the appropriate tuning parameter is out of scope of this paper. For engineering applications, the tuning parameter may be easily determined by samples of trials. Let $\eta\geq 0$ denote the tuning parameter, then the multiobjective optimization problem can be formulated as

$$\begin{aligned}\min_{\boldsymbol{b}\geq\boldsymbol{0}}\quad & \sum_{i=1}^{m} b_i-\eta\times\sum_{j=1}^{n} r\left(j\right)\\ \text{s.t.}\quad & \begin{cases}\min\limits_{j\in\mathcal{N}} r\left(j\right)\geq R\\ (4){-}(6).\end{cases}\end{aligned} \tag{12}$$

Similar to (11), (12) can be rewritten into the equivalent form of an LP problem

$$\begin{aligned}\min_{\boldsymbol{b}\geq\boldsymbol{0}}\quad & \boldsymbol{1}^T\boldsymbol{b}-\eta\times\boldsymbol{1}^T\boldsymbol{H}^{*T}\left(\boldsymbol{f}\cdot\boldsymbol{b}\right)\\ \text{s.t.}\quad & \boldsymbol{H}^{*T}\left(\boldsymbol{f}\cdot\boldsymbol{b}\right)\geq\boldsymbol{R}.\end{aligned} \tag{13}$$

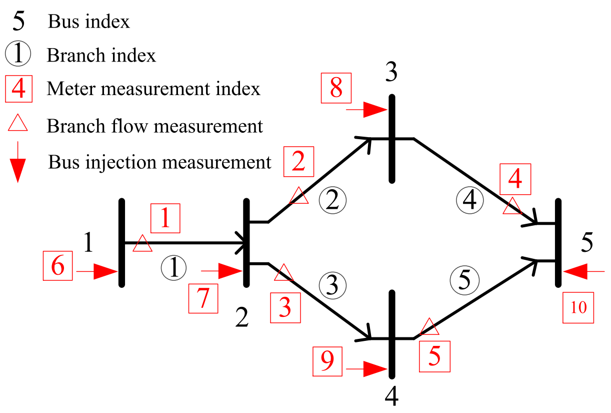


Fig. 2. Example of a fully measured 5-bus power system.

With the appropriately determined tuning parameter ($\eta = 0.1$, defined by samples of trials), LP can achieve a more senseful solution for (13) for practical applications, which is the solution 3 as shown in Table II. Such a solution has the maximum total attack cost among all feasible solutions with the same least defense budget.

VI. Extension to Case With Limited Number of Protected Meters

A. Problem Formulation

In this section, we consider an extension to the proposed problem where the number of protected meters is limited. Assume that meters are deployed at all buses and branches (fully measured). Intuitively, the more meters are protected, the more difficult an FDI attack can be launched without being detected, and thus the total required defense budget can be reduced. On the other hand, the high cost of defense infrastructure is a major hindrance for large-scale deployment. The extension therefore is essentially to find the best selection of a limited number of protected meters, which may be of importance in real-life applications.

For example, taking the fully measured 5-bus power system in Fig. 2, the number of meters is 10, and the meter measurements are $\boldsymbol{z} = [F_{12}, F_{23}, F_{24}, F_{35}, F_{45}, P_1, P_2, P_3, P_4, P_5]^T$. Thus, the measurement Jacobian matrix is

$$\boldsymbol{H} = \begin{pmatrix} b_{12} & 0 & 0 & 0 \\ -b_{23} & b_{23} & 0 & 0 \\ -b_{24} & 0 & b_{24} & 0 \\ 0 & -b_{35} & 0 & b_{35} \\ 0 & 0 & -b_{45} & b_{45} \\ b_{12} & 0 & 0 & 0 \\ -b_{12}-b_{23}-b_{24} & b_{23} & b_{24} & 0 \\ b_{23} & -b_{23}-b_{35} & 0 & b_{35} \\ b_{24} & 0 & -b_{24}-b_{45} & b_{45} \\ 0 & -b_{35} & -b_{45} & b_{35}+b_{45} \end{pmatrix}.$$

According to (5)

$$\boldsymbol{H}^* = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}.$$

Let a binary variable $\psi_i \in \{0, 1\}$ denote whether to protect meter measurement z_i or not, and $\boldsymbol{\psi} = [\psi_1, \psi_2, \ldots, \psi_m]^T$ for the meter selection vector. When $\psi_i = 1$, it means that meter measurement z_i is protected, and otherwise no defense is deployed there. With the $\boldsymbol{H}^*$ matrix and the meter protection strategy $\boldsymbol{\psi}$, (6) is rewritten as

$$r(j) = \sum_{i=1}^{m} h_{ij}^* k_i \psi_i \quad \forall j \in \mathcal{N}. \tag{14}$$

Given the maximum number of protected meters, denoted by M, the meter selection problem is to choose which meters to protect and determine how much defense budget to deploy on each of these meters, such that the total required defense budget is minimized. Thus, (10) is rewritten as

$$\min_{\boldsymbol{\psi} \in \{0,1\}, \boldsymbol{b} \geq \boldsymbol{0}} \quad \sum_{i=1}^{m} b_i \tag{15}$$

$$\text{s.t.} \begin{cases} \sum\limits_{i=1}^{m} \psi_i \leq M \\ \min\limits_{j \in \mathcal{N}} r(j) \geq R \\ (4), (5), (14) \end{cases}. \tag{15a}$$

Note that the only difference between (10) and (15) is the existence of the additional constraint (15a) showing that the number of protected meters is limited. Such an integer constraint, however, makes the problem more difficult to tackle.

Similar to that of (11), (15) can be rewritten into the equivalent form of an MINLP problem

$$\min_{\boldsymbol{\psi} \in \{0,1\}, \boldsymbol{b} \geq \boldsymbol{0}} \quad \boldsymbol{1}^T \boldsymbol{b} \tag{16}$$

$$\text{s.t.} = \begin{cases} \boldsymbol{1}^T \boldsymbol{\psi} - M \leq 0 & \text{(16a)} \\ \boldsymbol{R} - \boldsymbol{H}^{*T} (\boldsymbol{f} \cdot \boldsymbol{\psi} \cdot \boldsymbol{b}) \leq 0. & \text{(16b)} \end{cases}$$

B. Solution by Benders' Decomposition

The meter selection problem is an MINLP problem, which is generally difficult to tackle. Since Benders' decomposition is an effective method to solve this problem with guaranteed optimality, we design the algorithm using Benders' decomposition [24, Ch. 13]. For MINLP (16), $\boldsymbol{\psi}$ is an integer, $\boldsymbol{b}$ is continuous. Let

$\boldsymbol{\psi}^*$ and $\boldsymbol{b}^*$ denote the optimal solution. Two types of constraints appear in MINLP: (16a) contains only integer variables; while (16b) contains both integer and continuous variables. Clearly, finding the optimal integer $\boldsymbol{\psi}^*$ is the critical part of MINLP. When the integer variables are determined, MINLP reduces to LP (11), which can be readily solved as shown in Section V-B. In other words, once $\boldsymbol{\psi}^*$ is obtained, $\boldsymbol{b}^*$ can be easily solved.

Benders' decomposition is an iterative approach to solve MINLP and the underlying intuition is described as follows. First, MINLP is decomposed into a master problem (MP) and a subproblem (SP). MP is an integer programming problem, which aims to obtain the integer variables by considering only the integer constraints (with lower bound solution LB). When the integer variables are determined, SP reduces to an LP to obtain the continuous variables (with upper bound solution UB). In general cases, the integer variables are not optimal, but they can be improved by adding new integer constraints into MP, such that the search/feasible space shrinks and the new integer variables gradually approach the optimum. For example, when SP has the feasible solution but UB>LB (i.e., $\boldsymbol{\psi}$ is not optimal), in order to improve $\boldsymbol{\psi}$, the new LB should be larger than the previous LBs, by adding the feasibility constraint (17a) into MP. When SP is infeasible, in order to avoid obtaining this improper $\boldsymbol{\psi}$ again, the infeasibility constraint (17b) is added into MP. The optimal solution is converged when $|\mathrm{UB} - \mathrm{LB}| \leq \epsilon$, where ϵ is error tolerance (stopping criterion). The iterative approach is summarized in Algorithm 1, which involves the following definitions.

Algorithm 1. Benders' decomposition for solving (16)

```
    /* Initialization                                                  */
Set $k \leftarrow 1, \mathcal{I}^1 \leftarrow \emptyset, \mathcal{J}^1 \leftarrow \emptyset, UB^0 \leftarrow +\infty$;
while do
    Solve $MP^k$ by, e.g., branch and bound;
    if feasible solution then
        Obtain solution $(\boldsymbol{\psi}^k, LB^k)$;
    else if unbounded solution then
        Choose arbitrary $\boldsymbol{\psi}^k \in \{0,1\}$;
        Set $LB^k \leftarrow -\infty$;
    end if
    Solve $SP(\boldsymbol{\psi}^k)$ by, e.g., dual decomposition;
    if feasible solution then
        Obtain solution $\boldsymbol{b}^k$ and Lagrangian multiplier $\boldsymbol{\lambda}^k$;
        Set $UB^k \leftarrow \min\{UB^{k-1}, \mathcal{F}(\boldsymbol{b}^k)\}$;
        if $|UB^k - LB^k| \leq \epsilon$ then /* Converged                    */
            return $(\boldsymbol{\psi}^k, \boldsymbol{b}^k)$;
        else /* Add feasible constraint                                 */
            Set $\mathcal{I}^{k+1} \leftarrow \mathcal{I}^k \cup \{k\}, \mathcal{J}^{k+1} \leftarrow \mathcal{J}^k$;
        end if
    else if infeasible solution then
        Solve $SPF(\boldsymbol{\psi}^k)$ by, e.g., dual decomposition;
        Obtain solution $\boldsymbol{b}^k$ and Lagrangian multiplier $\boldsymbol{\mu}^k$;
        Set $UB^k \leftarrow UB^{k-1}$;
         /* Add infeasible constraint                                  */
        Set $\mathcal{I}^{k+1} \leftarrow \mathcal{I}^k, \mathcal{J}^{k+1} \leftarrow \mathcal{J}^k \cup \{k\}$;
    end if
    Set $k \leftarrow k + 1$;
end while
```

TABLE III

COMPARISON OF NUMERICAL SOLUTIONS

#	Metric		
	Meter selection $\boldsymbol{\psi}$	Defense strategy $\boldsymbol{b}$	Least defense budget $\sum_{i=1}^m b_i$
$M = 1$	n/a	n/a	n/a
$M = 2$	0000000011	[1 1]	2
$M = 3$	0000001011	[0.5 0.5 0.5]	1.5
$M \geq 4$	0000001111	$[\frac{1}{3}\ \frac{1}{3}\ \frac{1}{3}\ \frac{1}{3}]$	$\frac{4}{3}$

TABLE IV

STATISTICS OF POWER SYSTEM TEST CASES

Case	Metric		
	# of branches	# of state variables	# of meter measurements
IEEE 9-bus	9	8	18
IEEE 14-bus	20	13	34
IEEE 30-bus	41	29	71
IEEE 118-bus	186	117	304
IEEE 300-bus	411	299	711

Definition 1: Objective function $\mathcal{F}(\boldsymbol{b})$ and constraint functions $\mathcal{G}(\boldsymbol{\psi})$, $\mathcal{H}(\boldsymbol{\psi}, \boldsymbol{b})$

$$\begin{cases} \mathcal{F}(\boldsymbol{b}) \triangleq \mathbf{1}^T \boldsymbol{b} \\ \mathcal{G}(\boldsymbol{\psi}) \triangleq \mathbf{1}^T \boldsymbol{\psi} - M \\ \mathcal{H}(\boldsymbol{\psi}, \boldsymbol{b}) \triangleq \boldsymbol{R} - \boldsymbol{H}^{*T}(\boldsymbol{f} \cdot \boldsymbol{\psi} \cdot \boldsymbol{b}). \end{cases}$$

Definition 2: Master problem MP^k

$$\min_{\boldsymbol{\psi} \in \{0,1\}, LB} \quad LB \tag{17}$$

$$\text{s.t.} \begin{cases} \mathcal{G}(\boldsymbol{\psi}) \leq 0 \\ LB \geq \mathcal{F}(\boldsymbol{b}^i) + (\boldsymbol{\lambda}^i)^T \mathcal{H}(\boldsymbol{\psi}, \boldsymbol{b}^i) \quad \forall i \in \mathcal{I}^k & \text{(17a)} \\ 0 \geq (\boldsymbol{\mu}^j)^T \mathcal{H}(\boldsymbol{\psi}, \boldsymbol{b}^j) \quad \forall j \in \mathcal{J}^k. & \text{(17b)} \end{cases}$$

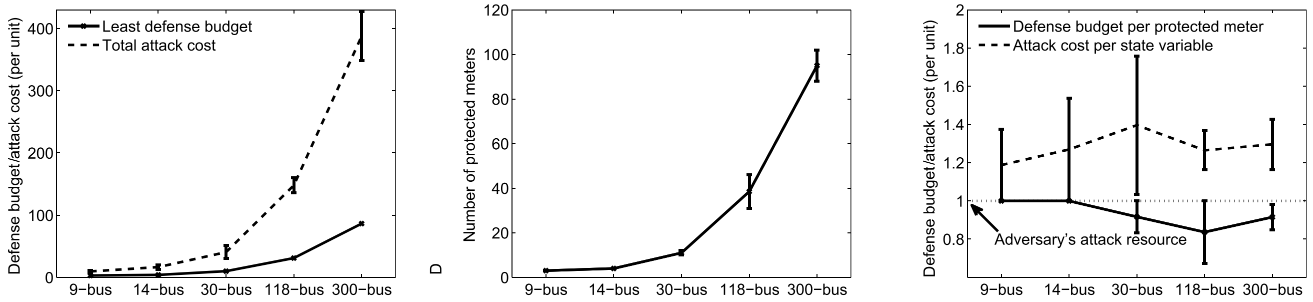
Definition 3: Subproblem $\mathrm{SP}(\boldsymbol{\psi}^k)$

$$\begin{aligned} \min_{\boldsymbol{b} \geq \mathbf{0}} \quad & \mathcal{F}(\boldsymbol{b}) \\ \text{s.t.} \quad & \mathcal{H}(\boldsymbol{\psi}^k, \boldsymbol{b}) \leq 0. \end{aligned} \tag{18}$$

Definition 4: SP feasibility-check $\mathrm{SPF}(\boldsymbol{\psi}^k)$

$$\begin{aligned} \min_{\boldsymbol{b} \geq \mathbf{0}, \boldsymbol{s}} \quad & \mathbf{1}^T \boldsymbol{s} \\ \text{s.t.} \quad & \boldsymbol{I}\boldsymbol{s} \geq \mathcal{H}(\boldsymbol{\psi}^k, \boldsymbol{b}). \end{aligned} \tag{19}$$

Taking the fully measured 5-bus power system in Fig. 2 as an example, by means of Benders' decomposition, we can obtain the solution as shown in Table III. It is observed that, if the number of protected meters is no more than one, we cannot guarantee that the attacker cannot modify any set of state variables, regardless of which meter is protected and how much defense budget is deployed on this meter. This matches the aforementioned intuition: the more meters are protected, the less total defense budget is needed. The reason is that, with an increased number of protected meters, to modify a state variable requests compromising more protected meters, and thus



(a) (b) (c)

Fig. 3. (a) Least defense budget and total attack cost. (b) Number of protected meters. (c) Average defense budget and attack cost of power system test cases.

the more difficult an FDI attack can be launched without being detected. When the number of protected meters reaches four and more, the total required defense budget reaches the least and keeps unchanged.

VII. Simulation Results

In this section, we evaluate the proposed defense strategy against FDI attacks through extensive simulations using IEEE test power systems, including the IEEE 9-bus, 14-bus, 30-bus, 118-bus, and 300-bus systems. The topology and configuration of these test power systems (particularly the $\boldsymbol{H}^*$ matrix) are extracted from MATPOWER, a MATLAB package for solving power flow problems [25]. The names of these source files are case9.m, case14.m, case30.m, case118.m, and case300.m, respectively. All these power system test cases are assumed to be fully measured. For each test system, the state variables are voltage angles of all buses, and the meter measurements are active power flows of all branches and active power injections of all buses. The statistics of these power system test cases are summarized in Table IV. Due to space limitation, we omit the $\boldsymbol{H}^*$ matrix for these test power systems.

In experiments, we simulate FDI attacks on power system state estimation using the dc power flow model. All the experiments are simulated and computed by MATLAB R2011a running on a laptop PC with Intel Core i5-3320 CPU at 2.6 GHz, 4-GB RAM memory, and 32-bit Windows 7 OS. In particular, the LP problem (11) and (13), SP (18), and SPF (19) are solved by "linprog" function, and MP (17) is solved by YALMIP [26]. The maximum number of iterations is 300.

First, we simulate on deploying the defense budget as low as possible while guaranteeing that the attacker cannot modify any set of state variables, i.e., by computing the LP problem (11). We also simulate on obtaining the optimal solution that has the maximum total attack cost among all feasible solutions with the same least defense budget, i.e., by adjusting the tuning parameter in the LP problem (13). The least defense budget and total attack cost, the number of protected meters, and the average defense budget and attack cost with lower and upper bounds are shown in Fig. 3, covering simulation results of five IEEE test power systems. It is observed that, in larger power systems, the least required defense budget for protecting the power system from FDI attacks increases, and the number of protected meters increases as well. Since theoretically there are infinitely many solutions, the number of protected meters may vary. Under the least defense budget, the total attack cost that the attacker could modify all state variables increases as the number of buses (state variables) increases. The average attack cost per state variable is greater than 1 p.u. (which is assumed to be the adversary's limited attack resource), so that the attacker cannot modify any state variable. The average defense budget per protected meter is less than 1 p.u., and this deployment strategy can guarantee that the total required defense budget is the least. The lower and upper bounds in these subfigures are obtained by adjusting the tuning parameter. The appropriate tuning parameter that maximizes the total attack cost while guaranteeing the least defense budget can be easily determined by samples of trials.

TABLE V
Number of Protected Meters Impacts Least Defense Budget

IEEE 9-bus	Maximum # of protected meters	$M \le 2$	$M \ge 3$	
	Least defense budget $\sum_{i=1}^m b_i$	n/a	3	
IEEE 14-bus	Maximum # of protected meters	$M \le 3$	$M \ge 4$	
	Least defense budget $\sum_{i=1}^m b_i$	n/a	4	
IEEE 30-bus	Maximum # of protected meters	$M \le 9$	$M \ge 10$	
	Least defense budget $\sum_{i=1}^m b_i$	n/a	10	
IEEE 118-bus	Maximum # of protected meters	$M \le 30$	$M \ge 31$	
	Least defense budget $\sum_{i=1}^m b_i$	n/a	31	
IEEE 300-bus	Maximum # of protected meters	$M \le 86$	$M = 87$	$M \ge 88$
	Least defense budget $\sum_{i=1}^m b_i$	n/a	87	86.5

Second, we simulate on choosing which meters to protect and determining how much defense budget to be deployed on each of these meters, such that the total required defense budget is minimized, given the maximum number of protection meters. We tackle the MINLP problem (16) using Benders' decomposition. How the maximum number of protected meters impacts the least defense budget is shown in Table V, covering simulation results of five IEEE test power systems. It is observed that, if the number of protected meters is too small, we cannot

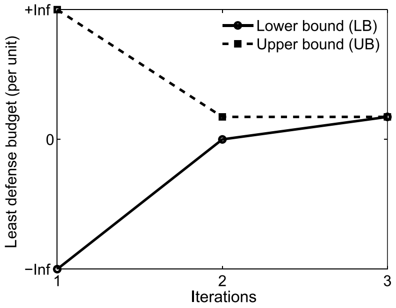


Fig. 4. Convergency of Benders' decomposition on IEEE 300-bus system.

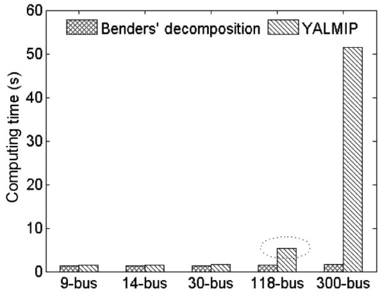


Fig. 5. Comparison between Benders' decomposition and YALMIP.

guarantee that the attacker cannot modify any set of state variables, regardless of which meters are protected and how much defense budget is deployed on these meters. The more meters are protected, the less the total required defense budget is. The reason is that, when the number of protected meters increases, it needs to compromise more protected meters to modify a state variable, and thus the more difficult an FDI attack can be launched without being detected. When the number of protected meters becomes large enough, the total required defense budget reaches the least and keeps unchanged.

Finally, we evaluate the convergence of the Benders' decomposition algorithm to solve the MINLP problem (16). Since the MINLP problem can also be computed by YALMIP, we compare the performance of these two approaches. The convergence of the Benders' decomposition algorithm on the IEEE 300-bus system is shown in Fig. 4. With a total of 1422 integer and continuous variables, the algorithm efficiently computes the solution in three iterations. It is observed that, with feasibility and infeasibility constraints being added to MP (17), the lower and upper bounds of the problem quickly converges to the optimal value. The performance comparison between Benders' decomposition and YALMIP is shown in Fig. 5, covering the computing time of five IEEE test power systems. It is obvious that the computational complexity of YALMIP increases exponentially with the power system scale, while that of Benders' decomposition keeps almost unchanged with great scalability. The reason is that this algorithm decouples integer and continuous variables into independent small-scale SPs, which are easier to be tackled than the original one. Even for the IEEE 300-bus system, the required computing time is less than 2 s. On the other hand, as we circle out in the figure, for the IEEE 118-bus system, YALMIP cannot obtain the feasible solution when $M \leq 32$, and thus the circled computing time is for $M \geq 33$. That is, the proposed Benders' decomposition algorithm outperforms YALMIP in terms of both the computing time and solution quality, especially for large-scale power systems.

VIII. Conclusion and Future Work

In this paper, we have studied the problem of defending against FDI attacks on power system state estimation. We formulated the behavior of a rational attacker, investigated the interaction between the defender and attacker, and designed the least-budget defense strategy to protect power systems against FDI attacks. We then extended to investigate choosing meters to be protected and determining algorithm for defense budget to be deployed on each of these meters. The meter selection problem was formulated as an MINLP problem, which was efficiently tackled by Benders' decomposition. We performed extensive simulations on IEEE test power systems to verify the performance of the proposed approach, showing its satisfactory performance in terms of computing time and quality of solution, especially for large-scale power systems.

Note that the attack/defense scheme considered in this paper is built on the measurement residual-based estimator. The measurement residual will not be affected when FDI attacks are launched. Some other estimators have been adopted in literatures, including minimum-mean-square error (MMSE) and largest normalized residue (LNR) [17], etc. The attack/defense scheme may affect the estimation performance in such cases. The effects of estimation performance when other estimators are deployed will be studied in our future work.

Appendix
Transform From (8) Into (10)

Problem (8) is difficult to solve in its current form due to the "maxmin" term in the objective function. This can be tackled by introducing an auxiliary variable, say R, and rewriting (8) into the equivalent form of

$$\max_{\boldsymbol{b}\geq\boldsymbol{0},R} \quad R$$
$$\text{s.t.} \quad \begin{cases} R \leq \min\limits_{j\in\mathcal{N}} r(j) \\ \sum\limits_{i=1}^{m} b_i \leq B \\ (4)\text{–}(6). \end{cases}$$

The above problem is to maximize the variable R under the constraint of the fixed B, which, from the primal-dual view, is conceptually equivalent to the following problem of minimizing the variable B under the constraint of the fixed R:

$$\min_{\boldsymbol{b}\geq\boldsymbol{0},B} \quad B$$
$$\text{s.t.} \quad \begin{cases} B \geq \sum\limits_{i=1}^{m} b_i \\ \min\limits_{j\in\mathcal{N}} r(j) \geq R \\ (4)\text{–}(6). \end{cases}$$

Obviously, the above problem is equivalent to the one in (10) if we eliminate the auxiliary variable B. The value of R should be chosen to be smaller than that of $\tilde{f}B$ such that (8) and (10) are equivalent, where $\tilde{f} \triangleq \max_{i\in\mathcal{M}} \tilde{f}_i$ and

$\tilde{f}_i = \left[\partial f_i\left(b_i\right)/\partial b_i\right]\big|_{b_i=0}$. The underlying reason is that according to (10a), (6), and (4), we have $R \le \min_{i\in\mathcal{N}} r\left(j\right) \le r\left(j\right) = \sum_{i=1}^{m} h_{ij}^{*} f_i\left(b_i\right)$. Since $h_{ij}^{*} \in \{0,1\}$, we have $R \le \sum_{i=1}^{m} h_{ij}^{*} f_i\left(b_i\right) \le \sum_{i=1}^{m} f_i\left(b_i\right)$. The linear approximation to the function $f_i\left(b_i\right)$ is $\tilde{f}_i b_i$; thus, we have $R \le \sum_{i=1}^{m} f_i\left(b_i\right) \approx \sum_{i=1}^{m} \tilde{f}_i b_i \le \tilde{f} \sum_{i=1}^{m} b_i \le \tilde{f} B$. The accurate value of R can be obtained simply by solving the problem multiple times and tuning.

References

[1] T. Facchinetti and M. L. Della Vedova, "Real-time modeling for direct load control in cyber-physical power systems," *IEEE Trans. Ind. Informat.*, vol. 7, no. 4, pp. 689–698, Nov. 2011.

[2] P. Siano, C. Cecati, H. Yu, and J. Kolbusz, "Real time operation of smart grids via FCN networks and optimal power flow," *IEEE Trans. Ind. Informat.*, vol. 8, no. 4, pp. 944–952, Nov. 2012.

[3] N. Ding, Y. Besanger, F. Wurtz, and G. Antoine, "Individual nonparametric load estimation model for power distribution network planning," *IEEE Trans. Ind. Informat.*, vol. 9, no. 3, pp. 1578–1587, Aug. 2013.

[4] V. C. Gungor *et al.*, "Smart grid technologies: communication technologies and standards," *IEEE Trans. Ind. Informat.*, vol. 7, no. 4, pp. 529–539, Nov. 2011.

[5] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid—The new and improved power grid: A survey," *IEEE Commun. Surv. Tuts.*, vol. 14, no. 4, pp. 944–980, Oct. 2012.

[6] R. Deng, Z. Yang, M.-Y. Chow, and J. Chen, "A survey on demand response in smart grids: Mathematical models and approaches," *IEEE Trans. Ind. Informat.*, vol. 11, no. 3, pp. 570–582, Jun. 2015.

[7] Y. Mo *et al.*, "Cyber–physical security of a smart grid infrastructure," *Proc. IEEE*, vol. 100, no. 1, pp. 195–209, Jan. 2012.

[8] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," *IEEE Commun. Surv. Tuts.*, vol. 14, no. 4, pp. 998–1010, Oct. 2012.

[9] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," *Comput. Netw.*, vol. 57, no. 5, pp. 1344–1371, 2013.

[10] R. Jiang, R. Lu, Y. Wang, J. Luo, C. Shen, and X. S. Shen, "Energy-theft detection issues for advanced metering infrastructure in smart grid," *Tsinghua Sci. Technol.*, vol. 19, no. 2, pp. 105–120, 2014.

[11] H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal denial-of-service attack scheduling with energy constraint," *IEEE Trans. Automat. Control*, doi: 10.1109/TAC.2015.2409905, to be published.

[12] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proc. ACM Comput. Commun. Soc. (CCS)*, 2009, pp. 21–32.

[13] 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.

[14] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. J. Overbye, "Detecting false data injection attacks on DC state estimation," in *Proc. Preprints 1st Workshop Secure Control Syst. (CPSWEEK)*, 2010, pp. 1–9.

[15] 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.

[16] S. Bi and Y. J. Zhang, "Graphical methods for defense against false-data injection attacks on power system state estimation," *IEEE Trans. Smart Grid*, vol. 5, no. 3, pp. 1216–1227, May 2014.

[17] 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.

[18] 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.

[19] L. Jia, R. J. Thomas, and L. Tong, "Impacts of malicious data on real-time price of electricity market operations," in *Proc. IEEE Hawaii Int. Conf. Syst. Sci. (HICSS)*, 2012, pp. 1907–1914.

[20] N. C. Ekneligoda and W. W. Weaver, "A game theoretic bus selection method for loads in multibus dc power systems," *IEEE Trans. Ind. Electron.*, vol. 61, no. 4, pp. 1669–1678, Apr. 2014.

[21] A. Monticelli, State Estimation in Electric Power Systems: A Generalized Approach. New York, NY, USA: Springer, 1999.

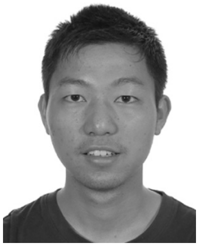
[22] A. J. Wood and B. F. Wollenberg, *Power Generation, Operation and Control*. Hoboken, NJ, USA: Wiley, 1996.

[23] G. Chen, Z. Y. Dong, D. J. Hill, and Y. S. Xue, "Exploring reliable strategies for defending power systems against targeted attacks," *IEEE Trans. Power Syst.*, vol. 26, no. 3, pp. 1000–1009, Aug. 2011.

[24] D. Li and X. Sun, *Nonlinear Integer Programming*. New York, NY, USA: Springer, 2006.

[25] R. D. Zimmerman, C. E. Murillo-Sánchez, and R. J. Thomas, "MATPOWER: Steady-state operations, planning, and analysis tools for power systems research and education," *IEEE Trans. Power Syst.*, vol. 26, no. 1, pp. 12–19, Feb. 2011.

[26] J. Löfberg, "YALMIP: A toolbox for modeling and optimization in MATLAB," in *Proc. IEEE Int. Symp. Comput. Aided Control Syst. Des. (CACSD)*, 2004, pp. 284–289.



Ruilong Deng (S'11–M'14) received the B.Sc. and Ph.D. degrees in control science and engineering from Zhejiang University, Hangzhou, China, in 2009 and 2014, respectively.

He visited Simula Research Laboratory, Fornebu, Norway, in 2011, and the University of Waterloo, Waterloo, ON, Canada, from 2012 to 2013. Currently, he is a Research Fellow with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore. His research interests include smart grid, cognitive radio, and wireless sensor network.

Dr. Deng currently serves as an Editor for the *IEEE/KICS Journal of Communications and Networks*. He also serves/served as a Technical Program Committee Member for IEEE Global Communications Conference (Globecom'15), the IEEE International Conference on Communications (ICC'15–16), IEEE International Conference on Computing, Networking and Communication (ICNC'15–16), the IEEE Consumer Communications and Networking Conference (CCNC'15–16), the IEEE International Conference on Smart Grid Communications (SmartGridComm'13), etc.

Gaoxi Xiao (M'99) received the B.S. and M.S. degrees in applied mathematics from Xidian University, Xi'an, China, in 1991 and 1994, respectively, and the Ph.D. degree in computing from Hong Kong Polytechnic University, Hung Hom, Hong Kong, in 1998.

He was an Assistant Lecturer with Xidian University, from 1994 to 1995. He was a Postdoctoral Research Fellow with Polytechnic University, Brooklyn, NY, USA, in 1999, and a Visiting Scientist at the University of Texas at Dallas, Richardson, TX, USA, from 1999 to 2001. He joined the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, in 2001, where he is now an Associate Professor. His research interests include complex systems and networks, communication networks, cyber security, and system resilience and robustness.

Rongxing Lu (S'09–M'11–SM'15) received the Ph.D. degree in computer science and engineering from Shanghai Jiao Tong University, Shanghai, China, in 2006, and the Ph.D. degree in electrical and computer engineering from the University of Waterloo, Waterloo, ON, Canada, in 2012.

He is currently an Assistant Professor with the Division of Communication Engineering, School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore. His research interests include wireless network security, applied cryptography, and system security and data forensics.

Dr. Lu was the recipient of Governor General's Gold Medal of Canada (2012), the IEEE Communications Society Asia Pacific Outstanding Young Researcher Award (2013), and the Best Paper Award of IEEE Wireless Communications and Networking Conference (WCNC) 2013, International Conference on Body Area Networks (BodyNets) 2010, IEEE International Conference on Computer Communications and Networks (ICCCN) 2009, and International Conference on Communications and Networking in China (Chinacom) 2008.