




On Feasibility and Limitations of Detecting False Data Injection Attacks on Power Grid State Estimation Using D-FACTS Devices

Beibei Li, *Member, IEEE*, Gaoxi Xiao , *Senior Member, IEEE*, Rongxing Lu , *Senior Member, IEEE*, Ruilong Deng , *Member, IEEE*, and Haiyong Bao

Abstract—Recent studies have investigated the possibilities of proactively detecting the high-profile false data injection (FDI) attacks on power grid state estimation by using the distributed flexible ac transmission system (D-FACTS) devices, termed as proactive false data detection (PFDD) approach. However, the feasibility and limitations of such an approach have not been systematically studied in the existing literature. In this paper, we explore the feasibility and limitations of adopting the PFDD approach to thwart FDI attacks on power grid state estimation. Specifically, we thoroughly study the feasibility of using PFDD to detect FDI attacks by considering single-bus, uncoordinated multiple-bus, and coordinated multiple-bus FDI attacks, respectively. We prove that PFDD can detect all these three types of FDI attacks targeted on buses or super-buses with degrees

larger than 1, if and only if the deployment of D-FACTS devices covers branches at least containing a spanning tree of the grid graph. The minimum efforts required for activating D-FACTS devices to detect each type of FDI attacks are, respectively, evaluated. In addition, we also discuss the limitations of this approach; it is strictly proved that PFDD is not able to detect FDI attacks targeted on buses or super-buses with degrees equalling 1.

Index Terms—Distributed flexible ac transmission system (D-FACTS) devices, false data injection (FDI) attacks, state estimation, feasibility and limitations, smart grids.

I. INTRODUCTION

EMERGING as the next generation digital information network and modernized power generation, transmission, and distribution systems, smart grids are expected to enable more efficient, reliable, and sustainable power systems that can meet the demands of the 21st century and beyond. However, recent years have witnessed a sharp increase of cyber attacks on energy industry, which are becoming increasingly challenging and threatening [1], [2].

Among the cyber threats on power grids, the high-profile false data injections (FDIs) attacks have drawn extensive research attentions from both energy and security communities [1]–[8]. FDI attackers inject falsified data into the real-time measurements to mislead power system state estimation with an expectation to gain illicit financial gains (e.g., electricity theft) [1], [9] or commit sabotage acts (e.g., power outages) [2], [3]. The success of an FDI attack is based upon attackers' knowledge of power grid connections and configurations. Unfortunately for the defenders, FDI attackers' knowledge harvesting toward power grids has been remarkably facilitated by the rapid integration of information and communications technologies and the global proliferation of powerful hacking tools [10]. Various channels can be exploited by FDI attackers to illegally obtain valuable information of power grids, including the following:

- 1) *Cyber channels*: Eavesdropping, intrusion into the control center, insider theft or accidental leaks, and malicious disclosure by disgruntled employees, etc.
- 2) *Physical channels*: Field measurement/investigation acts with specialized tools in areas with insufficient protection, and physical tampering with the hardware components of field devices.

Manuscript received February 3, 2019; revised April 30, 2019; accepted May 30, 2019. Date of publication June 12, 2019; date of current version January 14, 2020. This work was supported in part by the National Key Research and Development Program of China under Grant 2016YFB08006004 and Grant 2016YFB08006005; in part by the National Natural Science Foundation of China under Grant 61872255, Grant U1736212, and Grant 61572334; in part by the Fundamental Research Funds for the Central Universities, Sichuan University under Grant YJ201933; in part by the Ministry of Education, Singapore under Contract MOE2016-T2-1-119; in part by the Future Resilient System Project at the Singapore-ETH Centre funded by the National Research Foundation of Singapore under its Campus for Research Excellence and Technological Enterprise Program; in part by the Nanyang Technological University (NTU) Internal Funding - SUG - CoE (M4082287) and A*STAR-NTU-SUTD AI Partnership under Grant RGANS1906; in part by the Natural Science Foundation of Zhejiang Province under Grant LY17F020006; and in part by the Key Research and Development Program of Science and Technology Department of Zhejiang Province under Grant 2017C01015. Paper no. TII-19-0385. (Corresponding author: Gaoxi Xiao.)

B. Li is with the College of Cybersecurity, Sichuan University, Chengdu, Sichuan 610065, China and also with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore 639798 (e-mail: bli012@e.ntu.edu.sg).

G. Xiao is with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore 639798 (e-mail: egxxiao@ntu.edu.sg).

R. Lu is with the Faculty of Computer Science, University of New Brunswick, NB E3B 5A3 Fredericton, Canada (e-mail: rlu1@unb.ca).

R. Deng is with the School of Computer Science and Engineering, Nanyang Technological University, Singapore (e-mail: rldeng@ntu.edu.sg).

H. Bao is with the School of Computer Science and Information Engineering, Zhejiang Gongshang University, Hangzhou 310018, China (e-mail: baohy@zjgsu.edu.cn).

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.2019.2922215

3) Cyber-physical channels: Coordinated cyber intrusions and physical measurement/investigation acts.

As is strictly proved that, if armed with valuable information of power grids, the knowledgeable FDI attackers are capable of constructing attack vectors that can easily circumvent the conventional state estimation based false data detection (FDD) defenses [4], [11], [12]. This may make many of existing FDD defenses no longer feasible. We regard such FDD defenses as passive approaches. A few recent studies have demonstrated the possibilities of achieving proactive FDD—termed as PFDD—in power grids by using distributed flexible ac transmission system (D-FACTS) devices [13]–[15]. To the best of our knowledge, Morrow *et al.* pioneered the studies on using D-FACTS devices to achieve topology perturbation for detecting either fault-induced or maliciously injected bad data in the power grid [13]. In early 2018, Tian *et al.* proposed an enhanced hidden moving target defense approach that can not only maintain the power flows after changing the line susceptance but also keep stealthiness even when the attackers are capable of checking the activation of D-FACTS [14]. More recently in late 2018, Liu *et al.* proposed a strategy to enhance detection and identification of FDI attacks using reactance perturbation while maintaining low operational costs [15]. These studies show that, leveraging PFDD approaches to mitigate FDI attacks in smart grids has been considered as a possible option by researchers from both energy and security communities. This is due to the unique capability of D-FACTS devices in generating reactance perturbation that allows producing moving targets against FDI attackers. Another significant reason may lie in the decreasing installation costs and weights of D-FACTS devices [14], [16], which makes it possible to widely deploy D-FACTS devices in the future smart grids.

Despite of these developments, some significant issues regarding PFDD remain largely open, such as the number and locations of D-FACTS devices needed to facilitate the detection of different types of FDI attacks [11]. In this paper, we aim to explore the feasibility and limitations of using PFDD to detect FDI attacks in smart grids. Three types of FDI attacks, namely single-bus, uncoordinated multiple-bus, and coordinated multiple-bus FDI attacks, are considered in our adversary model.

The major contributions of this paper are fourfold.

- 1) We design a framework to detect FDI attacks on power grid state estimation by using the PFDD approach. The rationale behind this framework is also elaborated.
- 2) We explore the feasibility of using the PFDD approach to detect three types of FDI attacks on power grid state estimation. It is proved that PFDD can detect the existence of all these FDI attacks targeted on buses or super-buses with degrees larger than 1, if and only if the deployment of D-FACTS devices covers at least a spanning tree of the power grid graph.
- 3) We obtain the profiles of the minimum *efforts* required for D-FACTS devices to identify FDI attacks with respect to the offsets that attackers desire to inject on the system states, for all three types of FDI attacks, respectively. These profiles are valuable for system defenders to make informed decisions against FDI attacks.

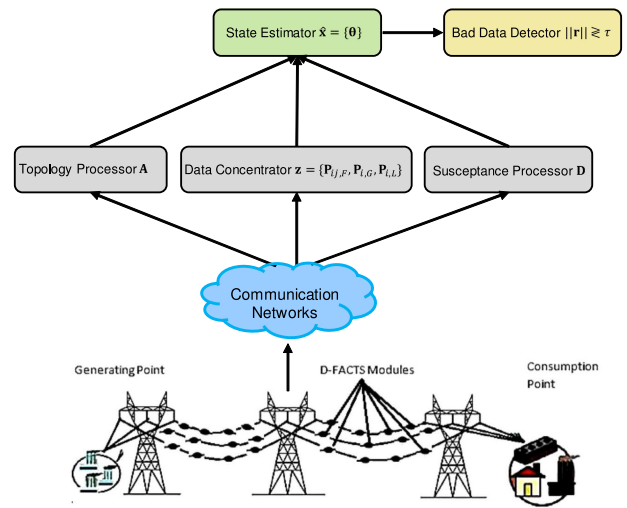


Fig. 1. System model—DC state estimation in smart grids.

- 4) The limitations of using PFDD are also discussed. It is strictly proved that PFDD is unable to detect FDI attacks targeted on buses or super-buses with degrees 1. In addition, we also prove that without knowing the power grid configuration information, specific FDI attacks can remain being undetected by PFDD if launched on buses or super-buses with degrees 1.

The remainder of this paper is organized as follows. In Section II, we present our system model as well as the adversary model. The PFDD framework and its feasibility explorations are elaborated in Section III, followed by discussions on its limitations in Section IV. Section V concludes this paper.

II. SYSTEM AND ADVERSARY MODELS

In this section, we show the system model and adversary model considered in this paper.

A. System Model

In this paper, we consider the power system state estimation involving a bad data detection (BDD) procedure (see Fig. 1) as our system model. Note that although we provide rigorous analyses for both DC and AC power flow based state estimation model, our main focus is on the DC model. Though AC model is more accurate than DC model, it is computationally expensive and highly complicated to be used in real-world applications. DC power flow model, on the other hand, allows much faster and simpler calculations than AC models without sacrificing the accuracy of analysis, especially in high-voltage transmission networks [15], [14], [17].

In a power system, state estimation is used to provide estimates of the internal system states given a collection of measurement data. According to the DC power flow model, the measurement data and system states are related by [18]

$$\mathbf{z} = \mathbf{H}\mathbf{x} + \boldsymbol{\eta} \quad (1)$$

where $\mathbf{z} \in \mathbb{R}^{m \times 1}$ is the measurement vector containing information of nodal power injections (i.e., generations and loads) and power flows, $\mathbf{x} \in \mathbb{R}^{n \times 1}$ is the system state vector including bus voltage phase angles, and $\boldsymbol{\eta} \in \mathbb{R}^{m \times 1}$ is the measurement noise vector with zero mean and covariance $\mathbf{W} \in \mathbb{R}^{m \times m}$, a diagonal matrix. Note that m and n are the numbers of measurements and system states, respectively. $\mathbf{H} \in \mathbb{R}^{m \times n}$ is the measurement Jacobian matrix implying the system connection and configuration information. It can be constructed by [19]

$$\mathbf{H} = \begin{bmatrix} \mathbf{A}^\top \mathbf{D} \mathbf{A} \\ \mathbf{D} \mathbf{A} \\ -\mathbf{D} \mathbf{A} \end{bmatrix} \quad (2)$$

where $\mathbf{A} \in \mathbb{R}^{l \times n}$ denotes the branch-bus connection matrix and $\mathbf{D} \in \mathbb{R}^{l \times l}$ denotes a diagonal matrix, whose diagonal entries are the negative susceptance values of all l branches in a power system.

Using the least squares method, the estimated system state vector $\hat{\mathbf{x}}$, with reference to (1), is given by

$$\hat{\mathbf{x}} = \arg \min_{\mathbf{x}} (\mathbf{z} - \mathbf{H}\mathbf{x})^\top \mathbf{W}^{-1} (\mathbf{z} - \mathbf{H}\mathbf{x}). \quad (3)$$

The solution for this problem is then given by [20]

$$\hat{\mathbf{x}} = (\mathbf{H}^\top \mathbf{W}^{-1} \mathbf{H})^{-1} \mathbf{H}^\top \mathbf{W}^{-1} \mathbf{z} \triangleq \boldsymbol{\Lambda} \mathbf{z} \quad (4)$$

where $\boldsymbol{\Lambda} \triangleq (\mathbf{H}^\top \mathbf{W}^{-1} \mathbf{H})^{-1} \mathbf{H}^\top \mathbf{W}^{-1}$. Then, the estimated measurement data $\hat{\mathbf{z}}$ is given by $\hat{\mathbf{z}} = \mathbf{H}\hat{\mathbf{x}} = \mathbf{H}\boldsymbol{\Lambda}\mathbf{z}$. The measurement residual $\mathbf{r} \in \mathbb{R}^{m \times 1}$ can thus be calculated by $\mathbf{r} = \mathbf{z} - \hat{\mathbf{z}} = (\mathbf{I} - \mathbf{H}\boldsymbol{\Lambda})\mathbf{z}$, where $\mathbf{I} \in \mathbb{R}^{m \times m}$ is an identity matrix.

The BDD procedure is to check the following hypothesis testing:

$$\begin{cases} \text{Null hypothesis } \mathbf{H}_0 : \|\bar{\mathbf{r}}\| > \tau \\ \text{Alternative hypothesis } \mathbf{H}_1 : \|\bar{\mathbf{r}}\| \leq \tau \end{cases} \quad (5)$$

where $\bar{\mathbf{r}} = \sqrt{\mathbf{W}^{-1}}\mathbf{r}$ is the normalized measurement residual vector. This testing is to compare the Frobenius norm of the normalized measurement residual $\|\bar{\mathbf{r}}\|$ with a predefined threshold τ . Specifically, if $\|\bar{\mathbf{r}}\| > \tau$, the null hypothesis is accepted, indicating the existence of anomalous residuals; hence bad measurement data presents in \mathbf{z} . Otherwise (i.e., $\|\bar{\mathbf{r}}\| \leq \tau$), the null hypothesis is rejected, which implies no bad measurement data exists. The value of τ can be determined with reference to [3].

B. Adversary Model

In the adversary model, we consider FDI attacks on smart grids. To construct this attack, the attackers need to design an attack vector $\mathbf{a} \in \mathbb{R}^{m \times 1}$ and fabricate a malicious measurement vector $\mathbf{z}_a = \mathbf{z} + \mathbf{a}$. If there exists a vector $\mathbf{c} \in \mathbb{R}^{n \times 1}$ that can satisfy $\mathbf{a} = \mathbf{H}\mathbf{c}$, a successful FDI is constructed and the original estimated system state vector $\hat{\mathbf{x}}$ is injected with an offset \mathbf{c} by $\hat{\mathbf{x}}_a = \hat{\mathbf{x}} + \mathbf{c}$ [3]. This is because that with such false data being injected, the estimated system states vector $\hat{\mathbf{x}}_a$ with reference to (4) is given by

$$\hat{\mathbf{x}}_a = \boldsymbol{\Lambda} \mathbf{z}_a = \boldsymbol{\Lambda} (\mathbf{z} + \mathbf{a}) = \mathbf{x} + \boldsymbol{\Lambda} \mathbf{H} \mathbf{c} = \mathbf{x} + \mathbf{c} \quad (6)$$

where $\boldsymbol{\Lambda} \mathbf{H} = \mathbf{I}$. The physical meaning of \mathbf{c} is the injected offset on the system states (i.e., voltage phase angles here). Then, the Frobenius norm of the normalized measurement residual with false data injected $\|\bar{\mathbf{r}}_a\|$ is given by [3]

$$\begin{aligned} \|\bar{\mathbf{r}}_a\| &= \|\sqrt{\mathbf{W}^{-1}}(\mathbf{z}_a - \mathbf{H}\hat{\mathbf{x}}_a)\| \\ &= \|\sqrt{\mathbf{W}^{-1}}[\mathbf{z} - \mathbf{H}\hat{\mathbf{x}} + (\mathbf{a} - \mathbf{H}\mathbf{c})]\| \\ &= \|\sqrt{\mathbf{W}^{-1}}(\mathbf{z} - \mathbf{H}\hat{\mathbf{x}})\| \leq \tau. \end{aligned} \quad (7)$$

In this case, no anomaly can be observed; therefore, FDI attacks cannot be detected by the existing BDD approach. However, as we can see and also proved by a line of studies [3], [11], [20], to inject a desired offset \mathbf{c} , the attackers must have full or at least partial useful knowledge of \mathbf{H} , as well as their corresponding attack capabilities. In this paper, to model various behaviors and attack strategies of different attackers with diverse capabilities and knowledge levels of \mathbf{H} in real-world scenarios, we consider three types of FDI attacks, including

- 1) *Single-bus FDI attacks*: This type of FDI attacks can only be planned and carried out on a specific single bus, i.e., $c_i = \theta_a$ for $i \in \mathcal{N} = \{1, 2, \dots, n\}$ and $c_j = 0$ for $\forall j \in \mathcal{N} \setminus i$, where θ_a is a constant value of voltage phase angle. The attackers only need to have relatively weak attack capabilities and basic knowledge levels of \mathbf{H} . Specifically, the attackers are able to launch successful single-bus FDI attacks on a specific bus as long as they have the knowledge of the following: First, this bus's topology information (i.e., connection status to other buses), second, the susceptance information of this bus's all incident branches, as well as third, the capability of manipulating the measurement data of all the line meters and/or phasor measurement unit(s) relevant to this bus and all its incident branches [11].
- 2) *Uncoordinated multiple-bus FDI attacks*: This type of FDI attacks can be simultaneously but independently planned and constructed on multiple buses in an uncoordinated mode, e.g., $\mathbf{c} = (\underbrace{0, \theta_{a1}, 0, 0, \theta_{a2}, \theta_{a3}, 0, \dots}_n)^\top$, where θ_{a1}, θ_{a2} , and θ_{a3} are distinct constant numbers of voltage phase angle. This type of FDI attacks can be regarded as multiple independent single-bus FDI attacks. In this case, the attackers need to have medium-level attack capabilities and advanced knowledge level of \mathbf{H} , i.e., the attack capability and knowledge level of launching multiple independent single-bus FDI attacks (with reference to the single-bus FDI attacks mentioned above).
- 3) *Coordinated multiple-bus FDI attacks (also called super-bus FDI attacks [11])*: This type of FDI attacks can be simultaneously carried out on multiple buses in a coordinated mode, e.g., $\mathbf{c} = (\underbrace{\theta_a, \theta_a, 0, 0, \theta_a, 0, \theta_a, \dots}_n)^\top$.

A super-bus is defined as a union of multiple interconnected buses, where all the united buses can be considered as a merged one. All the internal branches within a super-bus can be considered as being omitted, and all the external branches to other buses are considered as the

Algorithm 1: Framework for PFDD Approach.

```

1: procedure
2:   1). Activate the D-FACTS devices deployed on
      branches of interest;
3:   2). Update  $\mathbf{D}$  matrix by  $\mathbf{D}' = \mathbf{D} + \Delta\mathbf{D}$ ;
4:   3). Update  $\mathbf{H}$  matrix by (8);
5:   4). Conduct state estimation by (4) using updated
       $\mathbf{D}'$  and  $\mathbf{H}'$ ;
6:   5). Execute BDD procedure by (5):
7:   if  $\|\bar{\mathbf{r}}'_a\| > \tau$  then
8:     output: FDI attack is detected.
9:   else
10:    output: No FDI attack is detected.
11:   end if
12: end procedure

```

branches of the super-bus. To launch a successful coordinated multiple-bus FDI attack, the attackers have to be with strong attack capabilities and expertise knowledge level of \mathbf{H} . Likewise, with reference to the single-bus FDI attacks, to mount a super-bus FDI attack, the attackers need to be equipped with the knowledge of the topology and branch susceptance information of this super-bus, as well as the capability of manipulating all the measurement data relevant to this super-bus.

III. FEASIBILITY OF PFDD

In this section, we study the feasibility of using PFDD approach to detect FDI attacks on smart grids. First, we develop a framework for PFDD approach and show the rationale behind it. Then, we evaluate the minimum efforts required for D-FACTS devices to identify FDI attacks with respect to the offsets that attackers desire to inject on the system states. Last, but most important, we formulate and prove a theorem regarding the minimum number of branches deployed with D-FACTS devices required to successfully detect FDI attacks.

A. Framework for PFDD Approach and Its Rationale

As shown in Algorithm 1, we design a framework to describe the PFDD approach. The rationale behind this approach is discussed ahead.

Given that D-FACTS devices are activated, the negative branch susceptance values are altered by $\mathbf{D}' = \mathbf{D} + \Delta\mathbf{D}$, where $\Delta\mathbf{D}$ is a matrix of the negative variations of branch susceptance values. Accordingly, the Jacobian matrix is changed by

$$\mathbf{H}' = \begin{bmatrix} \mathbf{A}^\top \mathbf{D}' \mathbf{A} \\ \mathbf{D}' \mathbf{A} \\ -\mathbf{D}' \mathbf{A} \end{bmatrix} = \mathbf{H} + \begin{bmatrix} \mathbf{A}^\top \Delta\mathbf{D} \mathbf{A} \\ \Delta\mathbf{D} \mathbf{A} \\ -\Delta\mathbf{D} \mathbf{A} \end{bmatrix} = \mathbf{H} + \Delta\mathbf{H} \quad (8)$$

where

$$\Delta\mathbf{H} = \begin{bmatrix} \mathbf{A}^\top \Delta\mathbf{D} \mathbf{A} \\ \Delta\mathbf{D} \mathbf{A} \\ -\Delta\mathbf{D} \mathbf{A} \end{bmatrix}. \quad (9)$$

Note that in most cases, due to limited capabilities, the attackers are incapable of immediately harvesting the knowledge of the updated Jacobian matrix \mathbf{H}' , when D-FACTS devices are activated. Hence, during an FDI attack, the attack vector is still constructed by $\mathbf{a} = \mathbf{H}\mathbf{c}$ with the original knowledge of \mathbf{H} . With the reported measurement data $\mathbf{z}'_a = \mathbf{z}' + \mathbf{H}\mathbf{c}$, the normalized measurement residuals after state estimation is then given by

$$\begin{aligned} \bar{\mathbf{r}}'_a &= \sqrt{\mathbf{W}^{-1}}(\mathbf{z}'_a - \mathbf{H}'\hat{\mathbf{x}}'_a) \\ &= \sqrt{\mathbf{W}^{-1}}(\mathbf{z}' + \mathbf{a} - \mathbf{H}'(\hat{\mathbf{x}}' + \Delta\mathbf{x})) \\ &= \bar{\mathbf{r}}' + \sqrt{\mathbf{W}^{-1}}(\mathbf{a} - \mathbf{H}'\Delta\mathbf{x}) \end{aligned} \quad (10)$$

where \mathbf{z}' , $\hat{\mathbf{x}}'$, $\Delta\mathbf{x}$ are the updated measurement vector, estimated system state vector, and the injected offset on system state vector, respectively. In this case, the injected vector $\sqrt{\mathbf{W}^{-1}}(\mathbf{a} - \mathbf{H}'\Delta\mathbf{x}) = \sqrt{\mathbf{W}^{-1}}(\mathbf{H}\mathbf{c} - \mathbf{H}'\Delta\mathbf{x})$ no longer equals $\mathbf{0}$. It is, therefore, easy to lead to $\|\bar{\mathbf{r}}'_a\| > \tau$ and to trigger the false data alarm. Subsequent sections will provide more details on in what cases, vector $\sqrt{\mathbf{W}^{-1}}(\mathbf{a} - \mathbf{H}'\Delta\mathbf{x})$ shall be equal to $\mathbf{0}$ or not.

B. Evaluation of the Minimum Efforts Required for D-FACTS Devices to Detect Effective FDI Attacks

By introducing the rationale of PFDD approach, we know that it is theoretically feasible to detect FDI attacks using this approach. Then, it is natural and valuable for us to evaluate the minimum efforts needed to detect effective FDI attacks by activating D-FACTS devices. Before starting further evaluations, we make the following definitions:

Definition 1: The efforts when using PFDD approach to detect FDI attacks is defined as the total absolute variations of all branches' susceptance values by tuning D-FACTS devices, which is denoted by $\|\text{diag}(\Delta\mathbf{D})\|$.

Definition 2: An effective FDI attack is the FDI attack that, if not detected and prevented, is capable of injecting falsified measurement data and eventually lead to sufficient impacts/changes on the power flows. In contrast, an ineffective FDI attack is the FDI attack that is capable of injecting falsified measurement data but fail to eventually lead to sufficient impacts/changes on the power flows.

Remark 1: An FDI attack is defined as an ineffective FDI attack, if the entries of \mathbf{c} are within the tolerance threshold of system state errors/faults. Since minor-value false data cannot lead to more significant impacts/changes on the power grid than those caused by measurement noises, and therefore can be tolerated.

Remark 2: A coordinated multiple-bus FDI attack targeted on all buses is defined as an ineffective FDI attack, if $\mathbf{c} = (\underbrace{\theta_a, \theta_a, \dots, \theta_a}_n)^\top$. This FDI attack injects a same value of voltage phase angle θ_a to all buses with no phase difference being created between any two buses; therefore, it cannot cause any impact on the power flows.

Next, we will explore the minimum efforts required for D-FACTS devices to detect effective FDI attacks under both dc and ac power flow models.

1) *Optimization Problem Formulation Under DC Model*: The minimum *efforts* required under dc model, subject to the constraints of D-FACTS capabilities and power flow balance requirements, is formulated by

$$\min_{\Delta \mathbf{D}} \quad \|\text{diag}(\Delta \mathbf{D})\| \quad (11a)$$

$$\text{s.t.} \quad \tau < \|\bar{\mathbf{r}}'_a(\Delta \mathbf{D})\| \quad (11b)$$

$$0 \leq |\Delta d_k| \leq d_k^{\max}, \quad k \in \mathcal{L} \quad (11c)$$

$$P_i = P_{i,G} - P_{i,L} = \sum_{j \in \mathcal{N}_i} P'_{ij}, \quad i, j \in \mathcal{N} \quad (11d)$$

where $\text{diag}(\cdot)$ returns a vector containing the diagonal elements of a square matrix. Δd_k is the k th element of vector $\text{diag}(\Delta \mathbf{D})$. $\bar{\mathbf{r}}'_a(\Delta \mathbf{D})$ denotes the updated normalized estimation residuals with false data injected, which is a function of $\Delta \mathbf{D}$. The set \mathcal{L} is defined by $\mathcal{L} = \{1, 2, \dots, l\}$ and d_k^{\max} serves as the maximum variation of branch susceptance value that D-FACTS devices deployed on the k th branch can achieve. P_i , $P_{i,G}$, and $P_{i,L}$ denote the nodal power injections, nodal power generations, and power loads at bus i , respectively. Further, we denote the neighbor buses of bus i by a set \mathcal{N}_i , and P'_{ij} the updated power flow between buses i and j , when D-FACTS are activated, which in DC model is calculated by

$$P'_{ij} = -b'_{ij}(\theta'_i - \theta'_j) = d'_k(\theta'_i - \theta'_j) \quad (12)$$

where θ'_i and θ'_j are the updated voltage phase angles on buses i and j , respectively, b'_{ij} is the updated susceptance of branch (i, j) (also indexed as the k th branch), and $b'_{ij} = -d'_k = -(d_k + \Delta d_k)$.

With regards to the constraints of this optimization problem, formulas (11c) and (11d) specify the capability constraints of D-FACTS devices and the optimal power flow balance requirements, respectively. More importantly, formula (11b) is specified for the successful identification of FDI attacks via the BDD procedure. The updated estimated system state vector $\hat{\mathbf{x}}'_a$ with false data injected can be expressed as the true updated system states added by the injected offsets: $\hat{\mathbf{x}}'_a = \hat{\mathbf{x}}' + \Delta \mathbf{x}$. Also, according to (4), we have $\hat{\mathbf{x}}'_a = \Lambda' \mathbf{z}'_a = \hat{\mathbf{x}}' + \Lambda' \mathbf{a}$. Thus, $\Delta \mathbf{x}$ can be represented by $\Delta \mathbf{x} = \Lambda' \mathbf{a}$. As a result, constraint (11b) with reference to (10) can be rewritten as

$$\begin{aligned} \tau &< \|\bar{\mathbf{r}}'_a(\Delta \mathbf{D})\| \\ &= \|\bar{\mathbf{r}}' + \sqrt{\mathbf{W}^{-1}}(\mathbf{a} - \mathbf{H}'\Delta \mathbf{x})\| \\ &= \|\bar{\mathbf{r}}' + \sqrt{\mathbf{W}^{-1}}(\mathbf{I} - \mathbf{H}'\Lambda')\mathbf{H}\mathbf{c}\|. \end{aligned} \quad (13)$$

In addition, recall that $\|\bar{\mathbf{r}}'\| < \tau$ holds all the time under normal circumstances with reference to Section II-A, because the entries of vector $\bar{\mathbf{r}}'$ are always sufficiently small (approaching to 0), and thus they can be reasonably neglected. In this way, by (13), we only need to consider

$$\tau < \|\sqrt{\mathbf{W}^{-1}}(\mathbf{I} - \mathbf{H}'\Lambda')\mathbf{H}\mathbf{c}\|. \quad (14)$$

Note that for the sake of simplicity of expressions, we will not substitute \mathbf{H}' and Λ' by $\Delta \mathbf{D}$, but recall that $\Delta \mathbf{D}$ fully reflects the variations of \mathbf{H}' and Λ' .

This optimization problem as formulated in (11) and the inequality as shown in (14) allow us to evaluate the relationship between the minimum $\|\text{diag}(\Delta \mathbf{D})\|$ and \mathbf{c} , and obtain a general profile if given a specific power system with original designs of \mathbf{A} , \mathbf{D} , \mathbf{W} , and τ .

2) *Optimization Problem Formulation Under AC Model*: The objective to minimize the *efforts* subject to constraints of D-FACTS capabilities and power flow balance requirements can also be formulated under ac power flow model, which is given by

$$\min_{\Delta \mathbf{D}} \quad \|\Delta \mathbf{D}\| \quad (15a)$$

$$\text{s.t.} \quad \|\bar{\mathbf{r}}'_a(\Delta \mathbf{D})\| > \tau \quad (15b)$$

$$0 \leq |\Delta d_k| \leq d_k^{\max}, \quad k \in \mathcal{L} \quad (15c)$$

$$P_i = P_{i,G} - P_{i,L} = \sum_{j \in \mathcal{N}_i} P'_{ij}, \quad i, j \in \mathcal{N} \quad (15d)$$

These formulas are seemingly analogous to (11a)–(11d), but it should be noted that the definitions of $\Delta \mathbf{D}$ and $\bar{\mathbf{r}}'_a$ are different under ac power flow model. Specifically, $\mathbf{D} = (d_1, d_2, \dots, d_l)^T \in \mathbb{R}^{l \times 1}$ is defined as the susceptance vector containing the susceptance values of all l branches in a power grid and, correspondingly, $\Delta \mathbf{D}$ is the vector of susceptance variations when D-FACTS devices are activated, which is given by $\Delta \mathbf{D} = (\Delta d_1, \Delta d_2, \dots, \Delta d_l)^T$.

With regard to $\bar{\mathbf{r}}'_a$ under ac power flow model, since the measurement data $\mathbf{z}'_a = \mathbf{z}' + \mathbf{a}$ and system states \mathbf{x}'_a are related by

$$\mathbf{z}'_a = \mathbf{z}' + \mathbf{a} = \mathbf{z}' + \mathbf{h}(\mathbf{c}) = \mathbf{h}'(\mathbf{x}'_a) + \boldsymbol{\eta} \quad (16)$$

based on the ac state estimation model [18], when FDI attacks are in presence and D-FACTS devices are activated, the normalized measurement residual vector $\bar{\mathbf{r}}'_a$ is then given by

$$\bar{\mathbf{r}}'_a = \sqrt{\mathbf{W}^{-1}}(\mathbf{z}'_a - \hat{\mathbf{z}}'_a) = \sqrt{\mathbf{W}^{-1}}[\mathbf{z}'_a - \mathbf{h}'(\hat{\mathbf{x}}'_a)] \quad (17)$$

where vector $\hat{\mathbf{x}}'_a$ is now estimated by

$$\begin{aligned} \hat{\mathbf{x}}'_a &= \min_{\mathbf{x}'_a} [\mathbf{z}'_a - \mathbf{h}'(\mathbf{x}'_a)]^T \mathbf{W}^{-1} [\mathbf{z}'_a - \mathbf{h}'(\mathbf{x}'_a)] \\ &= \sum_{i=1}^m \frac{(z'_i + h_i(\mathbf{c}) - h'_i(\mathbf{x}'_a))^2}{\sigma_i^2}. \end{aligned} \quad (18)$$

Note that σ_i^2 is the i th element in the diagonal of matrix \mathbf{W} , and matrix $\mathbf{h}' = (h'_1, h'_2, \dots, h'_m)$ is the updated Jacobian matrix under ac power flow model containing the information of vector $\Delta \mathbf{D}$. Due to the strong nonlinearity of the relationship between \mathbf{h}' and $\Delta \mathbf{D}$ under ac power flow model, we will not present it here. The above discussions show that the considered optimization problem can also be applied to ac power flow model. However, solving this highly nonlinear optimization problem is computationally expensive and difficult. Our subsequent discussions are, therefore, based on DC power flow model, which can be regarded as a useful simplification of ac model and will not compromise our findings regarding the feasibility and limitations of using PFDD to detect FDI attacks.

3) *Relationship Evaluation Between $\|\text{diag}(\Delta \mathbf{D})\|$ and \mathbf{c}* : We evaluate the relationship by considering all the three types of

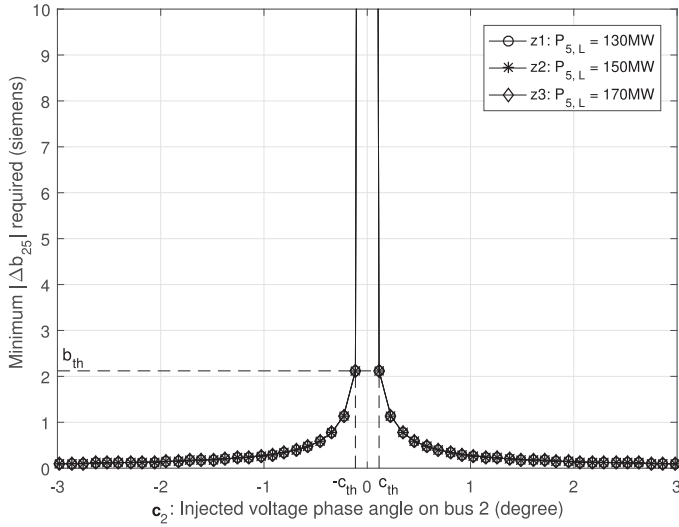


Fig. 2. Relationship between the minimum $|\Delta b_{25}|$ and c_2 .

FDI attacks under DC power flow model. Note that although our numerical results are obtained upon a 7-bus power grid (see Fig. 5), the method adopted to obtain the relationship, as aforementioned, applies to all power grids. Here, we solve the optimization problem by changing the susceptance value (using D-FACTS devices) of only one branch each time, solving the updated power flow analysis, and checking the BDD test. Repeat this procedure until the capability limits of D-FACTS devices are reached. Since the values of Δd_k are discrete, the searching space is rather limited within the range of $[0, d_k^{\max}]$. Hence, it is easy to enumerate all possible values of Δd_k and obtain the minimum *efforts* in a short time.

In the first case, we consider a single-bus FDI attack targeted on bus 2 and D-FACTS devices are deployed on branch (2,5). Fig. 2 shows the relationship between the minimum $|\Delta b_{25}|$ and c_2 under three measurement instants, where $P_{5,L} = 130$ MW, 150 MW, 170 MW, respectively. $|\Delta b_{25}|$ is the absolute susceptance of branch (2,5) and c_2 is the second entry of vector \mathbf{c} . As we can see, the profiles are almost the same for different measurement instants. This justifies the aforementioned finding that this relationship is independent of \mathbf{z} (and \mathbf{x}) because the entries of vector $\bar{\mathbf{r}}$ are always sufficiently small (approaching to 0) under normal circumstances. In addition, we can also see from each profile that the larger the absolute c_2 , the lower minimum *efforts* are required. This indicates that it is easier for system defenders to detect FDI attacks with reckless behaviors injecting large offsets into \mathbf{x} expecting extensive damages or profits. On the other hand, when $|c_2| < c_{th}$, either enormous *efforts* are required or it is not feasible (beyond the adjustment capability of D-FACTS devices) to detect FDI attacks using PFDD. Let $c_{th} > 0$ be the tolerance threshold of voltage phase angle variation, denoting the maximum absolute value of injected voltage phase angle or measurement noises that a power grid can tolerate. The value of c_{th} can be determined by (13) with a given τ , and the solutions $\{c_{th}^1, c_{th}^2, \dots, c_{th}^n\}$ for different buses might be slightly different due to various configurations. For such cases, c_{th} may take the minimum solution, that is $c_{th} = \min\{c_{th}^1, c_{th}^2, \dots, c_{th}^n\}$.

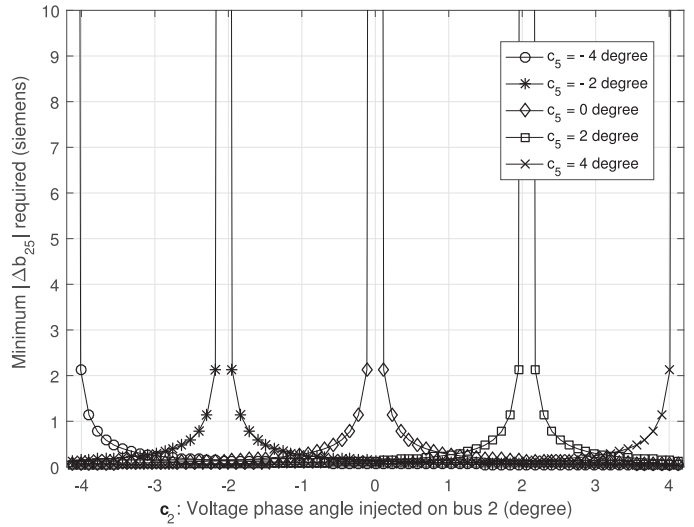


Fig. 3. Relationship between the minimum $|\Delta b_{25}|$ and c_2 under various values of c_5 .

Correspondingly, given c_{th} , a threshold b_{th} for the minimum *efforts* required for D-FACTS devices to detect *effective* FDI attacks can also be determined according to (13).

In the second case, we consider an uncoordinated multiple-bus FDI attack targeted on both buses 2 and 5, and branch (2,5) is deployed with D-FACTS devices. In Fig. 3, we evaluate the relationship between the minimum $|\Delta b_{25}|$ and c_2 under various values of c_5 , the fifth entry of \mathbf{c} . As can be seen from this figure, although with different “central locations,” profiles similar to each other and to that in Fig. 2 are, respectively, obtained under various values of c_5 . That is to say, the profile of the minimum *efforts* required for detecting an uncoordinated multiple-bus FDI attack is similar to that for a single-bus FDI attack, but the exact value is based on the injected phase difference (e.g., $c_2 - c_5$ here) between two targeted buses.

In the third case, a coordinated multiple-bus FDI attack on buses 1, 2, 3, 5, and 7 is simulated, and suppose that D-FACTS devices are deployed on all branches incident to bus 2. As shown in Fig. 4, anomalies (FDI attacks) can only be observed by activating D-FACTS devices on branches (2, 4) and (2, 6). This is because that the coordinated multiple-bus FDI attack injects the same values of voltage phase angle ($|\theta_a| > c_{th}$ by default here) onto all the targeted buses (buses 1, 2, 3, 5, and 7 here). Hence, no injected phase difference among these coordinated buses can be observed. In contrast, sufficient difference can be observed between the untargeted and targeted buses (e.g., between 4 and 2 or 6 and 2 here).

C. Minimum Deployment Requirements of D-FACTS Devices to Detect FDI Attacks

The above discussions have shown that it is feasible to detect *effective* FDI attacks using PFDD approach. To facilitate later discussions, we summarize this finding into Statement 1.

Statement 1: In PFDD approach, D-FACTS devices deployed on a branch is able to detect the existence of effective FDI attacks targeted on either end bus(es) (with degrees both larger

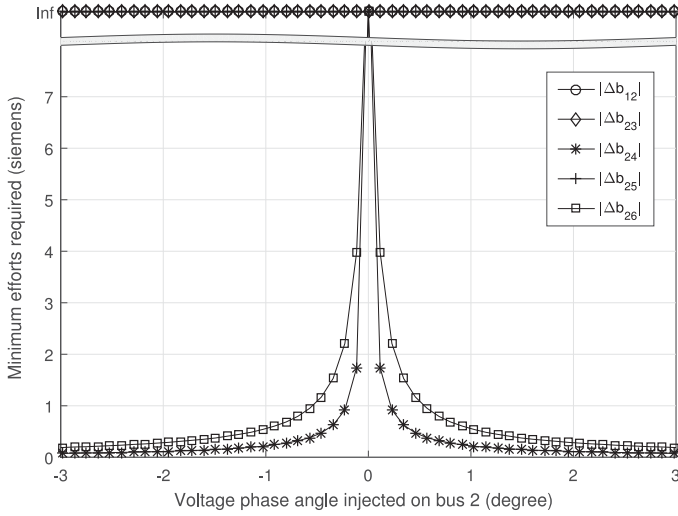


Fig. 4. Relationship between the minimum efforts and the injected voltage phase angle.

than 1) of this branch, if and only if the injected phase angle difference between the two end buses is larger than a tolerance threshold c_{th} .

When talking about the *degree* of a bus or super-bus throughout this paper, it indicates the number of branches (i.e., transmission lines) connecting this bus or super-bus to others. With this statement, we move on to study on the minimum number of branches that need to be deployed with D-FACTS devices to guarantee the detection of all three types of *effective* FDI attacks.

Note that, it is necessary to assume that by activating D-FACTS devices, the states of some branches as well as the buses will be changed, but the power system will still operate normally due to the built-in robustness of the power grid.

Next, we make the following definitions to facilitate our discussions.

Definition 3: A branch is termed as a *known branch* if its susceptance is unalterable and can be known to the attackers; otherwise, it is termed as an *unknown branch*.

Typically, we regard a branch deployed with D-FACTS devices as an *unknown branch* because its susceptance can be altered by activating D-FACTS devices; and a branch without D-FACTS devices is termed as a *known branch*.

Definition 4: A bus is termed as a *protected bus* if it is connected to at least one *unknown branch*; and an *unprotected bus* otherwise.

With these definitions, we can prove the theorem below.

Theorem 1: The PFDD approach is feasible to detect effective FDI attacks targeted on buses or super-buses with degrees larger than 1, if and only if the unknown branches cover at least a *spanning tree* of the power grid graph.

Proof. Sufficiency: Suppose that a set of $n - 1$ branches building a spanning tree \mathcal{T} of the power grid graph $\mathcal{G} = \{\mathcal{V}, \mathcal{E}\}$ are deployed with D-FACTS devices. According to Definitions 3 and 4, these $n - 1$ branches are *unknown branches*, and all buses are *protected buses* as each of them is connected to at least one of these *unknown branches*. In this case, for any form of

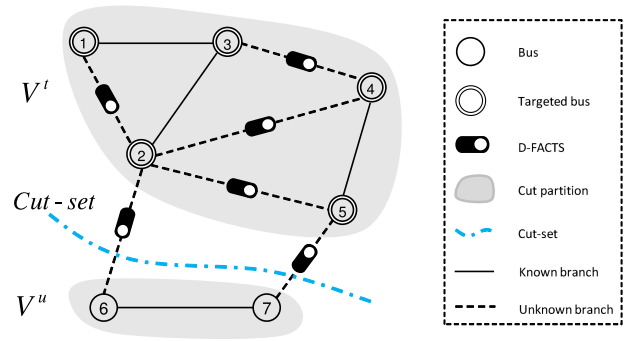


Fig. 5. Illustrative 7-bus power system with D-FACTS deployment covering a spanning tree.

effective single-bus or uncoordinated multiple-bus FDI attacks, there must be at least one *unknown branch* connecting to the targeted bus(es). According to Statement 1, it is feasible to detect these FDI attacks by using PFDD with given *unknown branch(es)*. When it comes to *effective* coordinated multiple-bus FDI attacks, at most $n - 1$ buses are targeted in such an attack, leaving at least one bus untargeted. Thus, there must be a *cut* $\mathcal{C} = \{\mathcal{V}^t, \mathcal{V}^u\}$ that divides the buses in a grid graph into two sets—targeted buses set \mathcal{V}^t and untargeted buses set \mathcal{V}^u , where $\mathcal{V}^t \cup \mathcal{V}^u = \mathcal{V}$. The *cut-set* of \mathcal{C} contains edges that have one endpoint in \mathcal{V}^t and the other in \mathcal{V}^u . Given that the *unknown branches* contain a spanning tree (as an example shown in Fig. 5), the *cut-set* must involve at least one *unknown branch* for any form of *effective* coordinated multiple-bus FDI attacks. Hence, any form of *effective* coordinated multiple-bus FDI attacks can be detected by using PFDD.

Necessity: If *unknown branches* in a power grid do not contain a spanning tree, there must be at least one *cut* $\mathcal{C} = \{\mathcal{V}^1, \mathcal{V}^2\}$ that divides the buses in a grid graph into two sets \mathcal{V}^1 and \mathcal{V}^2 , where its *cut-set* involves no *unknown branch*. Then, a coordinated multiple-bus FDI attack on all buses in either one set (\mathcal{V}^1 or \mathcal{V}^2) but none in the other set can be successfully launched without being detected, because no *unknown branch* is involved in the *cut-set* to detect such an FDI attack using the PFDD approach. Specifically, if there are only $n - 2$ *unknown branches* in a power grid, there must exist one and only one *cut-set* $\mathcal{S} = \{(u, v) \in \mathcal{E} | u \in \mathcal{V}^1, v \in \mathcal{V}^2\}$ dividing \mathcal{V} into \mathcal{V}^1 and \mathcal{V}^2 , where any branch $(u, v) \in \mathcal{S}$ accompanied with the $n - 2$ *unknown branches* can form a spanning tree \mathcal{T} of the grid graph \mathcal{G} . Then, all buses in either \mathcal{V}^1 or \mathcal{V}^2 can be regarded as a super-bus. Since there is no *unknown branch* connecting this super-bus to any other external nodes, *effective* FDI attacks targeted on this super-bus cannot be detected as per Statement 1. Likewise, when there are fewer *unknown branches*, there must exist more than one *cut-sets* covering no *unknown branch*, which makes it unable to detect FDI attacks using the PFDD approach. ■

IV. DISCUSSIONS ON PFDD LIMITATIONS

In this section, we shall discuss on the limitations of using PFDD to detect *effective* FDI attacks targeted on buses or super-buses with degrees 1.

A. Limitations of Detecting FDI Attacks Using PFDD

Our findings of the limitations by using PFDD to detect FDI attacks are summarized in Theorem 2 and Corollary 1.

Theorem 2: Given a power grid hosting buses or super-buses with degrees equalling 1, the PFDD approach is not able to detect effective FDI attacks targeted on these buses or super-buses.

Proof: Let $\epsilon_k \in \{0, 1\}^{l \times 1}$ denote a unit column vector whose k th entry equals 1, and $\delta_i \in \{0, 1\}^{n \times 1}$ a unit column vector whose i th entry equals 1. Define $\mu_{ij} \triangleq \delta_i - \delta_j$. In this way, matrices \mathbf{A} and \mathbf{D} can be written as

$$\mathbf{A} = \sum_{k \in \mathcal{L}} \epsilon_k \mu_{ij}^T, \quad \mathbf{D} = \sum_{k \in \mathcal{L}} -b_{ij} \epsilon_k \epsilon_k^T \quad (19)$$

where $k \sim \{i, j\}$, denoting that branch k connects buses i and j . Let $\rho_S \in \{0, 1\}^{(n+2l) \times 1}$ denote a unit column vector whose i th entry equals 1 for $\forall i \in \mathcal{S}$, where \mathcal{S} is a set of bus indices. Then, \mathbf{H} matrix can be rewritten as

$$\mathbf{H} = \begin{bmatrix} \mathbf{A}^T \mathbf{D} \mathbf{A} \\ \mathbf{D} \mathbf{A} \\ -\mathbf{D} \mathbf{A} \end{bmatrix} = \begin{bmatrix} \sum_{k \in \mathcal{L}} \mu_{ij} \mu_{ij}^T \\ -\sum_{k \in \mathcal{L}} b_{ij} \epsilon_k \mu_{ij}^T \\ \sum_{k \in \mathcal{L}} b_{ij} \epsilon_k \mu_{ij}^T \end{bmatrix} \\ = \sum_{k \in \mathcal{L}} -b_{ij} (\rho_{\{i, n+k\}} - \rho_{\{j, n+l+k\}}) \mu_{ij}^T. \quad (20)$$

For a single bus with degree 1: Suppose that an effective single-bus FDI attack is targeted on bus $\zeta \in \mathcal{N}$ with degree 1, and bus $\gamma \in \mathcal{N}$ is the only neighbor of bus ζ connected by branch $\ell \in \mathcal{L}$. The attacker aims to inject θ_a to bus ζ by designing $\mathbf{c} = (0, 0, \dots, 0, \underbrace{\theta_a}_{\zeta\text{-th}}, 0, \dots, 0)^T$, which can be rewritten as $\mathbf{c} = \theta_a \delta_\zeta$. In this case, the attack vector \mathbf{a} is written as

$$\mathbf{a} = \mathbf{H} \mathbf{c} = -b_{\zeta\gamma} (\rho_{\{\zeta, n+\ell\}} - \rho_{\{\gamma, n+l+\ell\}}) \mu_{\zeta\gamma}^T \theta_a \delta_\zeta \\ = -b_{\zeta\gamma} \theta_a (\rho_{\{\zeta, n+\ell\}} - \rho_{\{\gamma, n+l+\ell\}}). \quad (21)$$

If D-FACTS devices deployed on branch ℓ are activated, the susceptance of this branch is updated to $b'_{\zeta\gamma}$ and \mathbf{H} matrix is updated to \mathbf{H}' . Then, we have the following major finding:

$$\mathbf{a} = \mathbf{H} \mathbf{c} \equiv \mathbf{H}' \mathbf{c}' = -b'_{\zeta\gamma} \theta'_a (\rho_{\{\zeta, n+\ell\}} - \rho_{\{\gamma, n+l+\ell\}}) \quad (22)$$

where $\mathbf{c}' = (0, 0, \dots, 0, \underbrace{\theta'_a}_{\zeta\text{-th}}, 0, \dots, 0)^T$, and $\theta'_a = \frac{b_{\zeta\gamma} \theta_a}{b'_{\zeta\gamma}}$.

Based on (10), $\|\bar{\mathbf{r}}'_a(\Delta \mathbf{D})\|$ can be rewritten as

$$\|\bar{\mathbf{r}}'_a(\Delta \mathbf{D})\| = \|\bar{\mathbf{r}}' + \sqrt{\mathbf{W}^{-1}}(\mathbf{a} - \mathbf{H}' \Delta \mathbf{x})\| \\ = \|\bar{\mathbf{r}}' + \sqrt{\mathbf{W}^{-1}}(\mathbf{H}' \mathbf{c}' - \mathbf{H}' \mathbf{A}' \mathbf{H}' \mathbf{c}')\| \\ = \|\bar{\mathbf{r}}'\| < \tau. \quad (23)$$

It means that no FDI alarm will be triggered if using PFDD to detect effective FDI attacks targeted on single buses with degrees 1.

For a super-bus with degree 1: Suppose that an effective coordinated multiple-bus FDI attack is targeted on buses

$\mathcal{B} = \{\zeta, \zeta + 1, \dots, \zeta + t\}$, where t is a positive integer. These buses form into a super-bus with degree 1, and branch ℓ is the only external branch of this super-bus connecting buses from ζ to γ , i.e., $\ell \sim \{\zeta, \gamma\}$. The attacker aims to inject θ_a to this super-bus by designing $\mathbf{c} = (0, 0, \dots, 0, \underbrace{\theta_a}_{\zeta\text{-th}}, \underbrace{\theta_a}_{(\zeta+1)\text{-th}}, \dots, \underbrace{\theta_a}_{(\zeta+t)\text{-th}}, 0, \dots, 0)^T$, which can be rewritten as $\mathbf{c} = \theta_a \sum_{i=0}^n \delta_{\zeta+i}$. In this case, the attack vector \mathbf{a} is written as

$$\mathbf{a} = \mathbf{H} \mathbf{c} \\ = \sum_{k \in \mathcal{L}^B} -b_{ij} (\rho_{\{i, n+k\}} - \rho_{\{j, n+l+k\}}) \mu_{ij}^T \times \theta_a \sum_{i=0}^t \delta_{\zeta+i} \quad (24)$$

where \mathcal{L}^B denotes the set of branches incident to any of the buses in set \mathcal{B} . It is worth noting that $\forall k \in \mathcal{L}^B \setminus \ell$, there must be both $i, j \in \mathcal{B}$. As for branch ℓ , $\zeta \in \mathcal{B}$, and $\gamma \notin \mathcal{B}$. Then, (24) can be rewritten as

$$\mathbf{a} = \sum_{k \in \{\mathcal{L}^B \setminus \ell\}} \left(-b_{ij} \theta_a (\rho_{\{i, n+k\}} - \rho_{\{j, n+l+k\}}) \mu_{ij}^T (\delta_i + \delta_j) \right) \\ + \sum_{k=\ell} \left(-b_{\zeta\gamma} \theta_a (\rho_{\{\zeta, n+\ell\}} - \rho_{\{\gamma, n+l+\ell\}}) (\delta_\zeta^T - \delta_\gamma^T) \delta_\zeta \right) \\ = \sum_{k \in \{\mathcal{L}^B \setminus \ell\}} \left(-b_{ij} \theta_a (\rho_i - \rho_j + \rho_{n+k} - \rho_{n+l+k}) \times 0 \right) \\ + \left(-b_{\zeta\gamma} \theta_a (\rho_\zeta - \rho_\gamma + \rho_{n+\ell} - \rho_{n+l+\ell}) \times 1 \right) \\ = -b_{\zeta\gamma} \theta_a (\rho_{\{\zeta, n+\ell\}} - \rho_{\{\gamma, n+l+\ell\}}). \quad (25)$$

We have the same finding as that shown in (21). Hence, $\mathbf{H} \mathbf{c} \equiv \mathbf{H}' \mathbf{c}'$ also holds for an effective coordinated multiple-bus FDI attack targeted on a super-bus with degree 1, leading to the failure in detecting such an attack using PFDD approach. Note that similar to the finding as shown in (22), although such an FDI attacks remains undetected, it is eventually transformed to another FDI attack with

$$\mathbf{c}' = (0, 0, \dots, 0, \underbrace{\theta'_a}_{\zeta\text{-th}}, \underbrace{\theta'_a}_{(\zeta+1)\text{-th}}, \dots, \underbrace{\theta'_a}_{(\zeta+t)\text{-th}}, 0, \dots, 0)^T \quad (26)$$

where $\theta'_a = b_{\zeta\gamma} \theta_a / b'_{\zeta\gamma}$.

Corollary 1: Given a single bus or a super-bus ζ with degree 1 (as for a super-bus, ζ represents the bus having the external branch), the external incident bus is denoted by γ , and the branch connecting these two buses is denoted by ℓ . Without knowing the susceptance of branch ℓ , as long as FDI attackers can inject P_a to P_ζ , $-P_a$ to P_γ , and P_a to $P_{\zeta\gamma}$, this FDI attack cannot be detected by using PFDD, where P_ζ , P_γ , $P_{\zeta\gamma}$, and P_a denote the nodal power injections of bus ζ , nodal power injections of bus γ , power flow of branch $\ell \sim \{\zeta, \gamma\}$, and a constant power value, respectively.

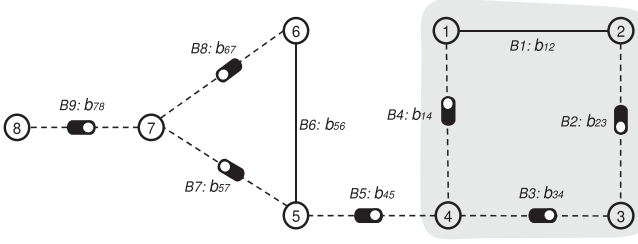


Fig. 6. Illustrative 8-bus power system with D-FACTS deployment covering a spanning tree.

Proof: Recall that \mathbf{z} is an $m \times 1 = (n + 2l) \times 1$ column vector comprising n nodal power injections $\mathbf{P}_I = \{P_1, P_2, \dots, P_n\}$ and $2l$ power flows $\mathbf{P}_F = \{P_{ij} | i, j \in \mathcal{N}, k \sim \{i, j\}, k \in \mathcal{L}\}$ and $-\mathbf{P}_F$. Then, \mathbf{z} can be represented by

$$\mathbf{z} = (\mathbf{P}_I, \mathbf{P}_F, -\mathbf{P}_F)^\top$$

$$= \sum_{i=1}^n P_i \rho_i + \sum_{k \in \mathcal{L}} P_{ij} \rho_{n+k} \sum_{k \in \mathcal{L}} -P_{ij} \rho_{n+l+k}. \quad (27)$$

If FDI attackers can inject P_a to P_ζ , $-P_a$ to P_γ , and P_a to $P_{\zeta+\gamma}$, this means that the attacker can construct an attack vector $\mathbf{a} = P_a(\rho_{\{\zeta, n+l\}} - \rho_{\{\gamma, n+l+l\}})$. Based on (22), we know that when PFDD is employed

$$\mathbf{H}'\mathbf{c}' = P_a(\rho_\zeta - \rho_\gamma + \rho_{n+l} - \rho_{n+l+l}) \quad (28)$$

where

$$\mathbf{c}' = (0, 0, \dots, 0, \underbrace{\theta'_a}_{\zeta\text{-th}}, 0, \dots, 0)^\top, \text{ and } \theta'_a = \frac{P_a}{b'_{\zeta\gamma}} \quad (29)$$

for a single bus ζ with degree 1, and

$$\mathbf{c}' = (0, 0, \dots, 0, \underbrace{\theta'_a}_{\zeta\text{-th}}, \underbrace{\theta'_a}_{(\zeta+1)\text{-th}}, \dots, \underbrace{\theta'_a}_{(\zeta+t)\text{-th}}, 0, \dots, 0)^\top \quad (30)$$

for a super bus ζ with degree 1 comprising buses $\mathcal{B} = \{\zeta, \zeta + 1, \dots, \zeta + t\}$. Such FDI attacks cannot be detected by using PFDD with reference to (23). ■

B. Case Study

In this section, we take an 8-bus power system (see Fig. 6) and an IEEE standard 39-bus system (see Fig. 7) as examples to illustrate *effective* FDI attacks targeted on a single bus and a super-bus with degree 1, respectively. Note that, we have also conducted extensive simulations on IEEE standard 118-bus and 300-bus systems, respectively, both of which verified our findings.

1) *Case 1. An Effective FDI Attack Targeted on Bus 8 in an 8-Bus System:* Suppose that an FDI attacker aims to inject θ_a to bus 8's phase angle θ_8 , he/she constructs

$$\mathbf{c} = \theta_a \delta_8 = (0, 0, 0, 0, 0, 0, 0, \theta_a)^\top \quad (31)$$

and an attack vector \mathbf{a} by

$$\mathbf{a} = \mathbf{H}\mathbf{c} = -b_{78}\theta_a(\rho_{\{7, n+9\}} - \rho_{\{8, n+l+9\}}). \quad (32)$$

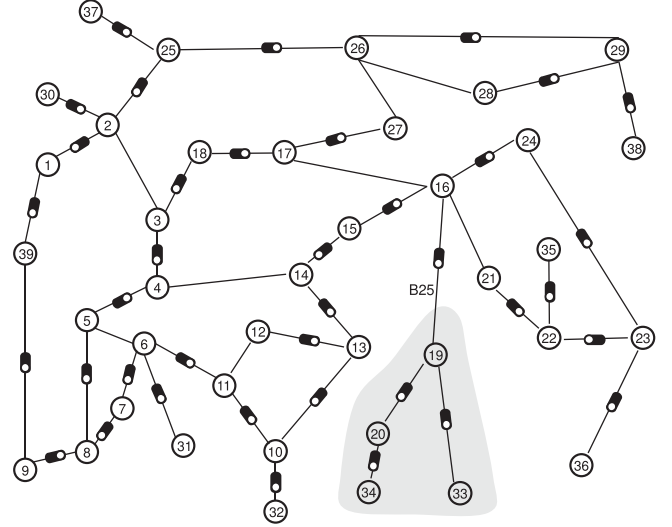


Fig. 7. Illustrative 39-bus power system with D-FACTS deployment covering a spanning tree.

In this case, data falsifications are equivalent to adding $-b_{78}\theta_a$ to P_7 , $b_{78}\theta_a$ to P_8 , $-b_{78}\theta_a$ to P_{78} , and $b_{78}\theta_a$ to P_{87} via compromised meters. When system defenders activate D-FACTS devices deployed on branch B9, b_{78} is changed to b'_{78} . According to (22) and (23), this FDI attack cannot be detected by PFDD, but an offset of $\theta'_a = b_{78}\theta_a/b'_{78}$ other than θ_a is injected to θ_8 . This is equivalent to an FDI attack with $\mathbf{c} = (0, 0, 0, 0, 0, 0, 0, \theta'_a)^\top$.

2) *Case 2. An Effective FDI Attack Targeted on a Super-Bus Composed of Buses 1, 2, 3, and 4 in an 8-Bus System:* Suppose that an FDI attacker aims to inject θ_a to the phase angles of a super-bus composed of buses 1, 2, 3, and 4, he/she constructs

$$\mathbf{c} = \theta_a(\delta_1 + \delta_2 + \delta_3 + \delta_4) = (\theta_a, \theta_a, \theta_a, \theta_a, 0, 0, 0, 0)^\top \quad (33)$$

and an attack vector \mathbf{a} by

$$\mathbf{a} = \mathbf{H}\mathbf{c} = -b_{45}\theta_a(\rho_4 - \rho_5 + \rho_{n+5} - \rho_{n+l+5}). \quad (34)$$

In this case, data falsifications are equivalent to adding $-b_{45}\theta_a$ to P_4 , $b_{45}\theta_a$ to P_5 , $-b_{45}\theta_a$ to P_{45} , and $b_{45}\theta_a$ to P_{54} via compromised meters. When system defenders activate the D-FACTS devices deployed on branch B5, b_{45} is changed to b'_{45} . According to (25) and (23), this FDI attack cannot be detected by PFDD and an offset of $\theta'_a = b_{45}\theta_a/b'_{45}$ is injected to $\theta_1, \theta_2, \theta_3$, and θ_4 , respectively. This is equivalent to an FDI attack with $\mathbf{c} = (\theta'_a, \theta'_a, \theta'_a, \theta'_a, 0, 0, 0, 0)^\top$.

3) *Case 3. An Effective FDI Attack Targeted on A Super-Bus Composed of Buses 19, 20, 33, and 34 in IEEE 39-Bus System:* Suppose that an FDI attacker aims to inject θ_a to the phase angles of a super-bus composed of buses 19, 20, 33, and 34, he/she constructs \mathbf{c} by

$$\mathbf{c} = \theta_a(\delta_{19} + \delta_{20} + \delta_{33} + \delta_{34})$$

$$= (0, 0, \dots, 0, \underbrace{\theta_a}_{19\text{-th}}, \underbrace{\theta_a}_{20\text{-th}}, 0, \dots, 0, \underbrace{\theta_a}_{33\text{-th}}, \underbrace{\theta_a}_{34\text{-th}})^\top \quad (35)$$

and an attack vector \mathbf{a} by

$$\mathbf{a} = \mathbf{H}\mathbf{c} = -b_{16,19}\theta_a(\rho_{19} - \rho_{16} + \rho_{n+25} - \rho_{n+l+25}) \quad (36)$$

where 25 is the index of branch B_{25} that connects buses 16 and 19. Then, the measurement data \mathbf{z} is falsified by $\hat{\mathbf{z}} = \mathbf{z} + \mathbf{a}$. In this case, data falsifications are equivalent to adding $-b_{16,19}\theta_a$ to P_{19} , $b_{16,19}\theta_a$ to P_{16} , $-b_{16,19}\theta_a$ to $P_{19,16}$, and $b_{16,19}\theta_a$ to $P_{19,16}$ via compromised meters. When system defenders activate the D-FACTS devices deployed on branch B_{25} , $b_{16,19}$ is changed to $b'_{16,19}$. According to (25) and (23), this FDI attack cannot be detected by PFDD and an offset of $\theta'_a = b_{16,19}\theta_a/b'_{16,19}$ is injected to θ_{19} , θ_{20} , θ_{33} , and θ_{34} , respectively. This is equivalent to an FDI attack with

$$\mathbf{c} = \underbrace{(0, 0, \dots, 0, \overbrace{\theta'_a}^{19\text{-th}}, \overbrace{\theta'_a}^{20\text{-th}}, 0, \dots, 0, \overbrace{\theta'_a}^{33\text{-th}}, \overbrace{\theta'_a}^{34\text{-th}})}_{39}^T \quad (37)$$

when the susceptance of branch B_{25} is $b'_{16,19}$.

V. CONCLUSION

In this paper, we systemically investigated the feasibility and limitations of using PFDD approach to detect FDI attacks on smart grids. Taking into account three types of FDI attacks namely single-bus, uncoordinated multiple-bus, and coordinated multiple-bus FDI attacks, respectively, we obtained the profiles of the minimum *efforts* required for activating D-FACTS devices to detect FDI attacks. We proved that PFDD can detect all these three types of FDI attacks if and only if the deployment of D-FACTS devices covers branches containing at least a spanning tree of the grid graph. In addition, the limitations of PFDD were also investigated with findings that the PFDD approach is not able to detect effective FDI attacks targeted on buses or super-buses with degrees 1.

This paper solely focused on the *feasibility* and *limitations* of using D-FACTS devices in proactive detection of FDI attacks. It can be imagined that activating D-FACTS devices tuning at random intervals may catch FDI attackers by surprise. Many open issues, such as the potential effects of proactively tuning D-FACTS devices on power system stability, however, still request careful studies before such proactive detection methods could, if ever, be put into real-life applications. Investigating on such open issues shall be of our future research interest.

REFERENCES

- [1] B. Li, R. Lu, W. Wang, and K.-K. R. Choo, "DDOA: A Dirichlet-based detection scheme for opportunistic attacks in smart grid cyber-physical system," *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 11, pp. 2415–2425, Nov. 2016.
- [2] B. Li, R. Lu, W. Wang, and K.-K. R. Choo, "Distributed host-based collaborative detection for false data injection attacks in smart grid cyber-physical system," *J. Parallel Distrib. Comput.*, vol. 103, pp. 32–41, May 2017.
- [3] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inform. Syst. Secur.*, vol. 14, no. 1, May 2011, Art. no. 13.
- [4] M. A. Rahman and H. Mohsenian-Rad, "False data injection attacks with incomplete information against smart power grids," in *IEEE Global Commun. Conf.*, Dec. 2012, pp. 3153–3158.

- [5] R. Deng, G. Xiao, and R. Lu, "Defending against false data injection attacks on power system state estimation," *IEEE Trans. Ind. Inform.*, vol. 13, no. 1, pp. 198–207, Feb. 2017.
- [6] L. Che, X. Liu, and Z. Li, "Fast screening of high-risk lines under false data injection attacks," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 4003–4014, Jul. 2019.
- [7] J. Valenzuela, J. Wang, and N. Bissinger, "Real-time intrusion detection in power system operations," *IEEE Trans. Power Syst.*, vol. 28, no. 2, pp. 1052–1062, May 2013.
- [8] R. Deng, G. Xiao, R. Lu, H. Liang, and A. V. Vasilakos, "False data injection on state estimation in power systems attacks, impacts, and defense: A survey," *IEEE Trans. Ind. Inform.*, vol. 13, no. 2, pp. 411–423, Apr. 2016.
- [9] L. Xie, Y. L. Mo, and B. Sinopoli, "False data injection attacks in electricity markets," in *Proc. IEEE 1st Int. Conf. Smart Grid Commun.*, Oct. 2010, pp. 226–231.
- [10] E. Kovacs, "Wikileaks releases details on CIA hacking tools," *SecurityWeek*, Mar. 2017. [Online]. Available: <http://www.securityweek.com/wikileaks-releases-details-cia-hacking-tool/s>
- [11] R. Deng and H. Liang, "False data injection attacks with limited susceptibility information and new countermeasures in smart grid," *IEEE Trans. Ind. Inform.*, vol. 15, no. 3, pp. 1619–1628, Mar. 2019.
- [12] 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.
- [13] K. L. Morrow, E. Heine, K. M. Rogers, R. B. Bobba, and T. J. Overbye, "Topology perturbation for detecting malicious data injection," in *Proc. 45th Hawaii Int. Conf. System Sci.*, Jan. 2012, pp. 2104–2113.
- [14] J. Tian, R. Tan, X. Guan, and T. Liu, "Enhanced hidden moving target defense in smart grids," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 2208–2223, Mar. 2019.
- [15] C. Liu, J. Wu, C. Long, and D. Kundur, "Reactance perturbation for detecting and identifying FDI attacks in power system state estimation," *IEEE J. Sel. Topics Signal Process.*, vol. 12, no. 4, pp. 763–776, Aug. 2018.
- [16] D. Divan and H. Johal, "Distributed FACTS – A new concept for realizing grid power flow control," *IEEE Trans. Power Electron.*, vol. 22, no. 6, pp. 2253–2260, Nov. 2007.
- [17] K. Purchala, L. Meeus, D. Van Dommelen, and R. Belmans, "Usefulness of DC power flow for active power flow analysis," in *Proc. IEEE Power Eng. Soc. Gen. Meet.*, 2005, pp. 454–459.
- [18] F. C. Schweppe and D. B. Rom, "Power system static-state estimation, Part II: Approximate model," *IEEE Trans. Power App. Syst.*, vol. PAS-89, no. 1, pp. 125–130, Jan. 1970.
- [19] K. C. Sou, H. Sandberg, and K. H. Johansson, "Electric power network security analysis via minimum cut relaxation," in *Proc. 50th Conf. Decis. Control Eur. Control Conf.*, Dec. 2011, pp. 4054–4059.
- [20] A. Monticelli, *State Estimation in Electric Power Systems: A Generalized Approach*. New York, NY, USA: Springer, 2012.



Beibei Li (S'15–M'19) received the B.E. degree in communication engineering from the Beijing University of Posts and Telecommunications, Beijing, China, in 2014, and the Ph.D. degree in cybersecurity from the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, in 2019.

He was invited as a Visiting Researcher at the Faculty of Computer Science, University of New Brunswick, Canada, in 2018 and also a Visiting Researcher with the research group of Networked Sensing and Control, College of Control Science and Engineering, Zhejiang University, Zhejiang, China, in 2019. He is currently an Associate Professor with the College of Cybersecurity, Sichuan University, Chengdu, China. His research interests include span several areas in cyber-physical system security, with a focus on intrusion detection techniques, applied cryptography, and big data security and privacy in smart grids.

Dr. Li served as a Technical Program Committee (TPC) Member for several international conferences, including IEEE Global Communications Conference (GLOBECOM) and International Conference on Wireless Communications and Signal Processing (WCSP), etc.



Gaoxi Xiao (M'99–SM'18) 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, in 1998.

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

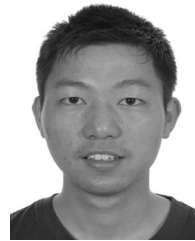
Dr. Xiao serves/served as an Editor or Guest Editor for IEEE TRANSACTIONS ON NETWORK SCIENCE AND ENGINEERING, *PLoS One*, and *Advances in Complex Systems*, etc., and a Technical Program Committee (TPC) Member for numerous conferences including IEEE International Conference on Communications and IEEE Global Communications Conference, etc.



Rongxing Lu (S'09–M'11–SM'15) Ph.D. degree in cryptography from the Department of Electrical and Computer Engineering and in cybersecurity from the Department of Computer Engineering, University of Waterloo, Waterloo, ON, Canada, in 2012.

He has been an Assistant Professor with the Faculty of Computer Science (FCS), University of New Brunswick (UNB), Fredericton, NB, Canada, since 2016. Before that, he worked as an Assistant Professor with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore from 2013 to 2016. He was a Postdoctoral Fellow with the University of Waterloo from 2012 to 2013. He has authored/coauthored extensively in his areas of expertise (with citation 12 300+ and H-index 54 from Google Scholar as of March 2018). His research interests include applied cryptography, privacy enhancing technologies, and Internet of Things (IoT)-Big Data security and privacy.

Dr. Lu was the recipient of the most prestigious Governor Generals Gold Medal, where he received his Ph. D. degree, and won the 8th IEEE Communications Society Asia Pacific Outstanding Young Researcher Award, in 2013. He is currently a senior member of IEEE Communications Society, he was also the recipient of the eight Best (Student) Paper Awards from some reputable journals and conferences. He currently serves as the Vice-Chair (Publication) of IEEE Communications and Information Security Technical Committee (ComSoc CIS-TC). He is the Winner of 2016-17 Excellence in Teaching Award, FCS, UNB.



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

He was a Research Fellow with Nanyang Technological University, Singapore, from 2014 to 2015; and an Alberta Innovates Technology Futures (AITF) Postdoctoral Fellow with the University of Alberta, Edmonton, AB, Canada, from 2015 to 2018. He is currently an Assistant Professor with the School of Electrical and Electronic Engineering, Nanyang Technological University. His research interests include smart grid, cyber security, and wireless networking.

Dr. Deng serves/served as an Editor for IEEE ACCESS and *Journal of Communications and Networks*, and a Guest Editor for IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTING and *IET Cyber-Physical Systems: Theory & Applications*. He also serves/served as a Symposium Chair for IEEE SmartGridComm and a Publication Chair for IEEE Vehicular Technology Society Asia Pacific Wireless Communications Symposium (VTS APWCS) in 2019.



Haiyong Bao received the Ph.D. degree in computer science from Shanghai Jiao Tong University, Shanghai, China, in 2006.

Since 2011, he has been an Associate Professor with the School of Computer Science and Information Engineering, Zhejiang Gongshang University, China. From 2014 to 2015, he was a Postdoctoral Fellow with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore. His research interests include secure data aggregation, insider attack detection, and applied cryptography.