Enhanced Hidden Moving Target Defense in Smart Grids

Jue Tian, Rui Tan, *Member, IEEE*, Xiaohong Guan, *Fellow, IEEE*, and Ting Liu, *Member, IEEE*

***Abstract*—Recent research has proposed a moving target defense (MTD) approach that actively changes transmission line susceptance to preclude stealthy false data injection (FDI) attacks against the state estimation of a smart grid. However, existing studies were often conducted under a weak adversarial setting, in that they ignore the possibility that alert attackers can also try to detect the activation of MTD before they launch the FDI attacks. We call this new threat as parameter confirming-first (PCF) FDI. To improve the stealthiness of MTD, we propose a hidden MTD approach that cannot be detected by the attackers and prove its equivalence to an MTD that maintains the power flows of the whole grid. Moreover, we analyze the completeness of MTD and show that any hidden MTD is incomplete in that FDI attacks may bypass the hidden MTD opportunistically. This result suggests that the stealthiness and completeness are two conflicting goals in MTD design. Finally, we propose an approach to enhancing the hidden MTD against a class of highly structured FDI attacks. We also discuss the MTD's operational costs under the dc and ac models. We conduct simulations to show the effectiveness of the hidden MTD against PCF-FDI attacks under realistic settings.**

***Index Terms*—False data injection attack, moving target defense, smart grid, state estimation.**

I. Introduction

As CRITICAL infrastructures, power grids must remain stable, safe, and secure. However, recent security incidents such as Stuxnet have alerted us to a general class of data integrity attacks called *false data injection* (FDI). The Stuxnet worm [1] injected malicious control commands to induce the centrifuges in Iranian nuclear facilities out of control, and meanwhile corrupted the system state readings to cover the ongoing faults. Similar FDI attacks can also be launched against the state estimation (SE) of power grids while keeping stealthy to the SE's bad data detection (BDD) mechanism [2], if the attackers know the details of the BDD and can compromise the sensor measurements through hardware intrusion or data tampering during network transmission. The wrong grid state estimates caused by the stealthy FDI attacks can result in erroneous controls that endanger grid safety.

Aiming at precluding the FDI attacks, existing studies have resorted to securing the sensor measurements and adding more data integrity check mechanisms. In [3] and [4], a minimum subset of sensors and their data links are identified such that securing them can preclude the FDI attacks. Secure data collection protocols based on in-network data aggregation [5] and en-route filtering [6] have also been developed. The bus voltage phases measured by phasor measurement units (PMUs) can be used to verify the integrity of the state estimation based on power flow measurements only [7]. However, a high security level of the sensors' and PMUs' data is often very costly.

Alternatively, we can invalidate the attackers' knowledge about the power system to preclude or reveal stealthy FDI attacks. To this end, recent studies [8]–[10] proposed a moving target defense (MTD) approach that actively changes the power system configuration. In the past decade, adjusting system configuration to maintain desirable power flows has been studied. The emerging distributed flexible ac transmission system (D-FACTS) devices, which can change the transmission line impedance, are promising for wide deployment due to their decreasing cost and thus enhancing the system operator's capability in adjusting the power system configuration. This increasing capability can foster the adoption of the proposed MTD approach.

However, existing MTD studies [8]–[10] were conducted under a weak adversary setting, in that they ignore the possibility that alert attackers can also try to detect the activation of MTD before they launch an FDI attack. In this paper, we show that the attackers can detect the activation of MTD easily and immediately, by applying the BDD based on the original power system configuration to the eavesdropped sensor measurements. The detection will drive the attackers to stop FDI and invest more resources to launch data exfiltration attacks that can always obtain the latest system configuration. In this

Manuscript received April 29, 2017; revised July 12, 2017, September 14, 2017, and December 7, 2017; accepted December 28, 2017. Date of publication January 9, 2018; date of current version February 18, 2019. This work was supported in part by the Start-Up Grant at Nanyang Technological University, in part by the National Key Research and Development Program of China under Grant 2016YFB0800202, in part by the National Natural Science Foundation of China under Grant 61472318, Grant 61632015, Grant 61772408, Grant U1766215, and Grant U1736205, in part by the Fok Ying-Tong Education Foundation under Grant 151067, and in part by the Fundamental Research Funds for the Central Universities. Paper no. TSG-00572-2017. *(Corresponding author: Jue Tian.)*

J. Tian was with the School of Computer Science and Engineering, Nanyang Technological University, Singapore. He is now with the Systems Engineering Institute, MOE KLINNS Laboratory, Xi'an Jiaotong University, Xi'an 710049, China (e-mail: juetian@sei.xjtu.edu.cn).

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

X. Guan is with the Systems Engineering Institute, MOE KLINNS Laboratory, Xi'an Jiaotong University, Xi'an 710049, China, and also with the Center for Intelligent and Networked Systems, Department of Automation, Tsinghua University, Beijing 100084, China (e-mail: xhguan@sei.xjtu.edu.cn).

T. Liu is with the Systems Engineering Institute, MOE KLINNS Laboratory, Xi'an Jiaotong University, Xi'an 710049, China (e-mail: tliu@sei.xjtu.edu.cn).

This paper has supplementary downloadable material available at http://ieeexplore.ieee.org, provided by the author.

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

Digital Object Identifier 10.1109/TSG.2018.2791512

sense, existing MTD approaches may not decrease the risk faced by the system substantially. We call this new threat as *Parameter Confirming-First False Data Injection* (PCF-FDI).

To improve the stealthiness of MTD, in this paper, we propose a *hidden MTD* approach that cannot be detected by the attackers. Specifically, on the activation of the hidden MTD, the attackers' BDD based on the original system configuration will not raise an alarm. The FDI attacks, crafted based on the original system configuration, will be mostly caught by the system's BDD after MTD, and then discarded or redirected to a honeypot for further forensic analysis that can help expose the details of the attackers. Hence, this hidden MTD approach can induce the attackers to launch futile attacks and increase their chance of getting exposed. In contrast, with the existing MTD approach, the forensic analysis is impossible and the system faces heightened threats since the persistent attackers will try to defeat the MTD. Thus, under a highly adversary setting, making the defense stealthy to the attackers is generally beneficial to the defenders in the attack-defense race, just like the attackers also try to make their attacks stealthy to the defenders.

In addition to stealthiness, we also analyze the completeness of MTD to show that the attackers may construct an FDI attack to bypass the BDD after the MTD without the new system configuration. Though this bypassing is opportunistic, it is important to study a desirable *complete MTD* approach that can preclude any possible bypassing and understand the relationship between stealthiness and completeness. For instance, an interesting question to ask is: Can we design an MTD approach that is hidden and complete simultaneously?

In this paper, we make the following contributions to understand the stealthiness and completeness of MTD:

- We study PCF-FDI and propose hidden MTD to address PCF-FDI. We prove that a necessary and sufficient condition for hidden MTD is that the power flows of the whole grid are maintained after MTD. Based on this result, we develop algorithms to compute the needed parameter perturbations to the D-FACTS-equipped transmission lines under both the dc and ac power flow models. Under the dc model, we analyze a basic feasibility condition for hidden MTD when a subset of lines are D-FACTS-equipped. With this condition, we can assess whether the hidden MTD can be implemented for a power grid. Thus, it can guide the grid design and enhancement.
- We define the completeness of MTD and enhance the hidden MTD to address a class of highly structured FDI attacks. Specifically, our analysis shows that real-world power grids generally do not provide sufficient transmission lines needed for realizing complete MTD. We further show that any hidden MTD must be incomplete, suggesting that the stealthiness and completeness are two conflicting goals in MTD design. Moreover, we analyze a class of FDI attacks against incomplete MTD and propose an *enhanced MTD* approach that precludes these attacks by strategically deploying D-FACTS devices. Since the complete MTD is generally not realizable, the enhanced hidden MTD is desired in practice.
- Since the MTD may change the total generation and the generation dispatch, we analyze MTD's operational costs in terms of the generation cost change both under the dc and ac models.
- We conduct simulations based on the IEEE 14-bus system to compare the stealthiness and completeness of hidden MTD with existing MTD approaches.

The rest of this paper is organized as follows. Section II discusses the background by reviewing existing failure scenarios and overviews the proposed approach. Section III presents preliminaries and related work. Section IV states our research problems. Section V presents the hidden MTD approach. Section VI analyzes the MTD's completeness. Section VII analyzes MTD's operational cost. Section VIII presents simulation results. Section IX discusses the system settings, attack identification and mitigation. Section X concludes.

II. Background

In this section, we review the U.S. *National Electric Sector Cybersecurity Organization Resource* (NESCOR) failure scenarios and recent security incidents to motivate the threats considered in this paper. Then, we overview the proposed approach and its effects on a networked power system.

A. Failure Scenarios in Smart Grids

To foster energy sector cybersecurity research, the NESCOR Team 1 has summarized the cybersecurity failure scenarios based on more than 100 cybersecurity incidents in 9 domains of the smart grids that have generated negative impacts [11]. The NESCOR failure scenarios show the security risks of the smart devices (e.g., phasor measurement unit (PMU) and smart meters) in the wide area. Here are several relevant instances from NESCOR:

- The control signals to the smart devices may be altered or injected into malicious messages through a spoofing attack (from WAMPAC.2 in [11]);
- The sensor measurements may be modified or stolen due to a backdoor or malware (from WAMPAC.4 and WAMPAC.8);
- The historical measurement data in the database may be stolen, corrupted or deleted (from WAMPAC.7).

These security risks are derived from and have been repeatedly alerted by the cybersecurity incidents in cyber-physical systems. The cyber-attacks against supervisory control and data acquisition (SCADA) systems have doubled since 2013 and mostly target the power plants, factories, or refineries [12]. The Stuxnet worm (2011) [1] and BlackEnergy trojan (2016) [13] injected malicious control commands and/or sensor data into industrial control systems and caused physical damages to the nuclear facilities and a power plant, respectively. Similar attacks also subverted the safe operations of Polish trains and city tram system (2008) [14], and Illinois water utility (2011) [15], etc. In addition, various malwares (e.g., the Night Dragon (2011) [16], Duqu (2011) [17], Flame (2012) [18], Dragonfly (2014) [19]) started the attacks by

first obtaining privileged accesses into the industrial control systems and then exfiltrated or gathered the sensitive information about the systems.

The FDI threat considered in this paper is aligned with the NESCOR security risks. The FDI attack injects false sensor measurements that are crafted based on a measurement matrix used in power grid state estimation. First, the false sensor measurement injection is an important security risk considered by NESCOR/WAMPAC.4 and WAMPAC.8. Second, recent studies showed that the measurement matrix can be estimated by a blind FDI approach [20] or topology leaking attacks [21] based on a certain amount of historical sensor data. Moreover, as the measurement matrix is a static information in the traditional power grids, from NESCOR/WAMPAC.2, WAMPAC.4, WAMPAC.8 and WAMPAC.7, the attackers may obtain the measurement matrix and launch the stealthy FDI attacks. Thus, the stealthy FDI attack is an important security concern.

B. Overview of the Enhanced Hidden MTD Approach

This paper proposes an enhanced hidden MTD approach for enhancing smart grid cybersecurity. We now overview how the proposed approach can be deployed in real systems and the relevant requirements. First, the system operators will need to deploy D-FACTS devices on the appropriately selected lines. The selection of the lines will be discussed in detail in Section VI-B. Then, a software program implementing our proposed algorithm will run in the control center to compute the parameter settings of all the D-FACTS devices based on the deployment, the parameter boundaries of D-FACTS devices, and the current sensor measurements to achieve the enhanced hidden MTD. Once the proposed approach is implemented, the power system can defend against the attackers who can launch the FDI attacks to bypass the BDD as studied in [2] and also try to detect the activation of the arbitrary MTD approach proposed in [10]. As a result, the implementation of our approach will provide enhanced protection for the smart grid.

III. Preliminaries and Related Work

A. FDI Attacks Against SE

Table I summarizes the notations used in this paper. We use a boldface letter (e.g., $\mathbf{H}$) to denote a matrix or a vector.

This paper mainly considers the dc power flow model that ignores transmission line resistance and assumes identical bus voltage magnitude. We note that, under the ac model, the system state consists of the voltage phasors (i.e., voltage magnitude and voltage phase) of all the buses. Under the dc model, due to the simplification of assuming identical bus voltage magnitude, the system state consists of all buses' voltage phases only. Although the dc model is less accurate than the ac model, the dc power flow analysis is faster and more robust than the ac power flow analysis. Section V-C extends our analysis to address the ac model. The SE is executed periodically, e.g., every five minutes. In this paper, this time period is referred to as *SE period*. Under the dc model, in the tth SE period, the system state, denoted by $\mathbf{x}_t \in \mathbb{R}^n$ (n is the number of buses), contains the voltage phases of all the buses. It is determined by the bus power injections and bus susceptance matrix. Specifically, $\mathbf{p}_t = \mathbf{B}\mathbf{x}_t$, where $\mathbf{p}_t \in \mathbb{R}^n$ is the vector of bus power injections, and $\mathbf{B} \in \mathbb{R}^{n\times n}$ is the bus susceptance matrix that encompasses both the system topology and the susceptances of all lines. For a connected power system, the $\mathbf{B}$ is non-singular. Thus, $\mathbf{x}_t = \mathbf{B}^{-1}\mathbf{p}_t$. Moreover, $\mathbf{z}_t = \mathbf{H}\mathbf{x}_t + \mathbf{e}_t$, where $\mathbf{z}_t \in \mathbb{R}^m$ denotes the vector of the active power flow measurements through a total of m monitored lines and $m \geq n$; $\mathbf{e}_t \in \mathbb{R}^m$ is the vector of measurement noises; $\mathbf{H} \in \mathbb{R}^{m\times n}$ is the *measurement matrix* with full column rank, i.e., rank($\mathbf{H}$) $= n$. Denote by $z_{t,ij}$ the measurement of the power flow through the line (i, j) that connects bus i and j, by $e_{t,ij}$ the measurement noise contained in $z_{t,ij}$, and by $x_{t,i}$ the element in $\mathbf{x}_t$ that corresponds to bus i. We have $z_{t,ij} = -b_{ij}(x_{t,i} - x_{t,j}) + e_{t,ij}$, where b_{ij} is the line susceptance. Thus, the corresponding row vector of $\mathbf{H}$, denoted by $\mathbf{H}_{ij}$, is given by [4]

$$\mathbf{H}_{ij} = \Big[0 \ \cdots \ 0 \quad \underbrace{-b_{ij}}_{i\text{th column}} \quad 0 \ \cdots \ 0 \quad \underbrace{b_{ij}}_{j\text{th column}} \quad 0 \ \cdots \ 0\Big].$$

If the measurement noises are independent and identically distributed Gaussians, the estimated system state $\hat{\mathbf{x}}_t = (\mathbf{H}^T\mathbf{H})^{-1}\mathbf{H}^T\mathbf{z}_t$ gives the minimum mean squared error. The BDD of SE detects existence of corrupted measurements by comparing the 2-norm estimation residual $r_t = \|\mathbf{z}_t - \mathbf{H}\hat{\mathbf{x}}_t\|_2$ with a threshold η. Specifically, if $r_t > \eta$, BDD yields a positive detection result. If the measurement noises follow the normal distribution $\mathcal{N}(0, \sigma^2)$, the threshold η can be set to be $\sigma\sqrt{\chi^2_{(m-n),\alpha}}$ to ensure a false alarm rate of $(1-\alpha)$, where $\chi^2_{(m-n),\alpha}$ represents the $100\alpha\%$-percentile of the $\chi^2_{(m-n)}$ distribution, since the $(r/\sigma)^2$ follows a $\chi^2_{(m-n)}$ distribution. In this paper, we set $\alpha = 0.95$. The study [2] showed that, in a stealthy FDI attack, the compromised measurement vector $(\mathbf{z}_t + \mathbf{a}_t)$ will not trigger the BDD if the attack vector $\mathbf{a}_t$ satisfies $\mathbf{a}_t = \mathbf{H}\mathbf{c}$, where $\mathbf{c} \in \mathbb{R}^n$ is an arbitrary vector. In other words, $\mathbf{a}_t \in$ col($\mathbf{H}$), where col($\cdot$) represents the column space of a matrix.

TABLE I
Summary of Notations

Symbol	Definition	Symbol	Definition
n	system state dimension	m	number of lines
$\mathbf{x}$	system state vector	$\hat{\mathbf{x}}$	estimated system state vector
$\mathbf{z}$	measurement vector	$\mathbf{H}$	measurement matrix
$\mathbf{H}_{ij}$	$\mathbf{H}$'s row about line (i, j)	$\tilde{\mathbf{H}}$	immutable part of $\mathbf{H}$
$\mathbf{B}$	bus susceptance matrix	$\mathbf{p}$	bus power injection vector
$\mathbf{a}$	FDI attack vector	$\mathbf{K}$	set of lines
$\mathbf{K}_D$	set of D-FACTS-equipped lines	$\mathbf{K}_A$	set of compromised lines
$\mathbf{K}_C$	critical set	b_{ij}	susceptance of line (i, j)
b'_{ij}	line susceptance after MTD	Δb_{ij}	variation of line susceptance
q_m	MTD's perturbation magnitude	q_d	load's variation magnitude
σ	system noise deviation	d	magnitude of attack
$\{\cdot\}'$	quantity after MTD $\mathbf{H}'$	$\{\cdot\}'^*$	SCOPF point after MTD
T	MTD's execution cycle	T_a	model learning time
η	threshold of BDD	C_0	generation cost under SCOPF
C_1	generation cost after MTD and convergence of frequency controls	C_2	generation cost after MTD and generation redispatch
b^{min}_{ij}	lower bound of susceptance modification	b^{max}_{ij}	upper bound of susceptance modification

To simplify the discussions, in the analysis of this paper, we assume that the sensor measurements are noiseless (i.e., $\mathbf{e} = \mathbf{0}$ and $\mathbf{z}$ consists of the actual power flows). In this case, the threshold η can be set to be 0, which ensures a zero false alarm rate. We will discuss the impact of the measurement noises on our analysis when applicable. Moreover, our simulations in Section VIII will evaluate the impact of the measurement noises on the effectiveness of our MTD approach.

B. MTD Model

In general, MTD actively introduces controlled changes to a system to increase uncertainty and complexity for attackers. In this paper, the defender actively perturbs the reactance of D-FACTS-equipped transmission lines, aiming at precluding FDI attacks. For simplicity of exposition, we adopt the line susceptance instead of reactance. We note that the product of a line's susceptance and reactance is -1 under the dc model. Specifically, if a transmission line (i, j) is equipped with a D-FACTS device, the defender can actively modify its susceptance to a target value $b_{t,ij}$, where $b_{ij}^{min} \leq b_{t,ij} \leq b_{ij}^{max}$, b_{ij}^{min} and b_{ij}^{max} denote the susceptance limits that the D-FACTS device can achieve. As a result, the measurement matrix $\mathbf{H}$ becomes time-varying. We re-denote it by $\mathbf{H}_t$. We assume that the attackers need at least T_a SE periods to obtain the susceptance values through data exfiltration attacks. Specifically, in the tth SE period, the attackers can obtain $\mathbf{H}_\nu$ only, where $\nu \leq t - T_a$. To ensure that the attackers always lack timely knowledge of the current system, the defender should execute MTD every T SE periods, where $T \leq T_a$. As a result, the MTD operates in an ex-ante mode, i.e., there are no ongoing FDI attacks on the time of MTD. If the attacker injects an attack vector that is crafted based on $\mathbf{H}_\nu$ as $\mathbf{a}_t = \mathbf{H}_\nu \mathbf{c}$, the defender's estimation residual is

$$r_t = \left\| (\mathbf{z}_t + \mathbf{H}_\nu \mathbf{c}) - \mathbf{H}_t \left(\mathbf{H}_t^T \mathbf{H}_t\right)^{-1} \mathbf{H}_t^T (\mathbf{z}_t + \mathbf{H}_\nu \mathbf{c}) \right\|_2.$$

When $m = n$, $\mathbf{H}_t(\mathbf{H}_t^T\mathbf{H}_t)^{-1}\mathbf{H}_t^T = \mathbf{I}_m$ and the above residual is zero, where $\mathbf{I}_m \in \mathbb{R}^{m \times m}$ denotes the identity matrix. When $m > n$, $\mathbf{H}_t(\mathbf{H}_t^T\mathbf{H}_t)^{-1}\mathbf{H}_t^T$ is generally not $\mathbf{I}_m$, and according to [2, Th. 3.2], $\left(\mathbf{I}_m - \mathbf{H}_t(\mathbf{H}_t^T\mathbf{H}_t)^{-1}\mathbf{H}_t^T\right)\mathbf{a}_t = \mathbf{0}$ if and only if $\mathbf{a}_t \in \text{col}(\mathbf{H}_t)$. As $m > n$ in actual power grids and $\mathbf{H}_\nu \neq \mathbf{H}_t$, the above residual is mostly non-zero and the attack will be detected.

In the analysis of this paper, we assume that the loads do not change in a time duration around the activation of the MTD. This assumption is referred to as *steady loads*. We will discuss and evaluate through simulations the impact of this simplification on the effectiveness of our MTD approach.

C. Related Work

Recent research has studied the FDI attacks against the SE of power grids. Liu *et al.* [2] analyzed the condition for bypassing the BDD of SE to mislead the control center into an incorrect system state estimation. In consideration of several practical constraints, Yuan *et al.* [22] considered an FDI-based load redistribution (LR) attack. Both the general FDI attack and the LR attack can be launched based on complete or incomplete information obtained by the attackers [23], [24]. In addition, FDI attacks for different malicious objectives have been studied, including maximizing the system operational cost [22], obtaining profits from financial misconducts in electricity markets [25], [26], and inducing economic dispatch into an infeasible region [27]. Hug and Giampapa [28] introduced a physical-property-based analytical technique to assess the vulnerability of ac SE under the FDI attacks at the remote terminal unit (RTU) level. Wang *et al.* [29] analyzed the feasibility of launching the alter-and-hide (AaH) attack, which is a stealthy hybrid attack consisting of behavioral and cyber attacks, from the attackers' capabilities and the attack execution plan in the substations. Ginter [30] thoroughly discussed the security, cyber attacks and the defense failures in SCADA, and used Stuxnet as a case study to illustrate these issues.

To detect the stealthy FDI attacks, Bobba *et al.* [3] proposed to protect a set of strategically selected sensor measurements such that no FDI attack vectors satisfying the stealthy condition analyzed in [2] can be found. Better attack detection algorithms have also been developed. For instance, Huang *et al.* [31] used adaptive CUSUM test to improve detection performance. Liu *et al.* [32] designed a new detector based on the separation of nominal and abnormal power grid states. Liu *et al.* [33] used a colored Petri net describing the information flows in smart meters to detect FDI attacks in advanced metering infrastructures. An alternate approach to the FDI attack detection is to leverage out-of-band information that is assumed to be intact. For instance, the analysis in [7] shows that $(p + 1)$ PMUs deployed at carefully chosen locations in a grid can neutralize a collection of p irreducible FDI attacks. Besides, several detection methods are derived from the data correlation between multiple SE periods. Gu *et al.* [34] used history data to track the dynamics of measurement variations. Ashok *et al.* [35] used the predicted data for FDI attack detection.

MTD approaches of mutating hosts' IP addresses can enhance network security [36]. The MTD concept has been recently applied to increase the barrier for the attackers to launch stealthy FDI attacks against power grids. Morrow *et al.* [8] and Davis *et al.* [9] proposed an ex-post MTD approach to detect ongoing FDI attacks. Specifically, if an attack is present, after applying known perturbations to the system configuration, the observed power flow changes will be different from the predicted changes. Rahman *et al.* [10] proposed an ex-ante MTD approach that randomly selects a subset of transmission lines and randomly perturbs their susceptance, as well as randomly select a subset of sensor measurements for SE, such that the attackers lack the knowledge of the system to launch FDI attacks. However, as discussed in Section I, the activation of this ex-ante MTD approach can be detected by the attackers. In contrast, as an ex-ante MTD approach, our hidden MTD is stealthy to the attackers due to the unchanged power flows.

Our preliminary work [37] has described the hidden MTD under the dc model and its construction algorithm. Based on [37], we make four new contributions in this paper. First, we extend the hidden MTD construction algorithm to address the ac model. Second, we study and evaluate the completeness of MTD in terms of attack space. Third, we analyze a class of

structured FDI attacks against incomplete MTD and enhance hidden MTD by strategically deploying the D-FACTS devices. Fourth, we analyze MTD's operational cost both under the dc and ac models.

In addition to the FDI attacks against SE, various intelligent attacks against power systems have been studied. For instance, Kim and Tong [4] proposed the topology attacks against the generalized SE to mislead the control center into an incorrect network topology understanding. Wang *et al.* [29] proposed the AaH attack, which executes disruptive switching actions and tampers with the actual measurements to cover the malicious switching actions. Liu *et al.* [38] developed the coordinated switching attacks to cause frequency and voltage instabilities in the transmission systems. The MTD can be applied to enhance the system resilience against these attacks, if the stealthiness of the attacks is based on the assumption of unchanged system parameters. For example, for the AaH attack implemented based on the replay attack against the distributed network protocol (DNP) [29], the replayed measurements may be diagnosed as normal when the measurement matrix is fixed, but can be detected by MTD, since the replayed measurements are inconsistent with the new measurement matrix.

IV. Problem Statement

In this section, we introduce the threat model and state the problems addressed in this paper with a motivating example.

A. Threat Model

We assume that the attackers have the following capabilities:

- Capability 1: The attackers can eavesdrop on the measurements of the sensors on all the lines.
- Capability 2: As discussed in Section II-A and III-B, the attackers may obtain the susceptance values of all the lines through data exfiltration attacks. The minimum required time to obtain the susceptances is T_a SE periods. Thus, if the MTD's execution cycle $T \leq T_a$, the attackers always lack timely knowledge of the current system.
- Capability 3: The attackers can tamper with a subset of or all the sensor measurements.

Moreover, we assume that the attackers adopt the following strategy. The attackers verify their information about the target power system before they inject false data. They launch the FDI attack only when the verification succeeds; otherwise, they should cancel any FDI attack. Thus, we name the threat considered in this paper as Parameter Confirming-First False Data Injection (PCF-FDI). Specifically, the attackers test the eavesdropped sensor measurements using the BDD based on the possibly out-of-date measurement matrix $\mathbf{H}_v$. The 2-norm estimation residual computed by the attackers using the sensor measurements in the tth time period, denoted by $\bar{r}_t$, is

$$\bar{r}_t = \left\| \mathbf{z}_t - \mathbf{H}_v \left(\mathbf{H}_v^T \mathbf{H}_v \right)^{-1} \mathbf{H}_v^T \mathbf{z}_t \right\|_2.$$

Similar to the BDD described in Section III-A, when $m > n$ and $\mathbf{z}_t \notin \text{col}(\mathbf{H}_v)$, the above residual is mostly non-zero. The attackers would detect the activation of MTD if the residual exceeds a predefined threshold.

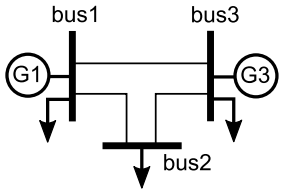


Fig. 1. 3-bus system.

We now discuss the Capability 1 and 3 of the attackers. All traditional power systems adopt a centralized control theme. Specifically, all the sensor measurements are transmitted to a control center for system monitoring. If the attackers can eavesdrop on the data flows through several critical routers close to the control center or directly eavesdrop on the data flows in the control center (which is not impossible as evidenced in the recent high-profile intrusions such as Stuxnet), they can get read access to all the power flow measurements. We note that with this assumption, as shown in Section IV-B, the attackers can detect the activation of the arbitrary MTD. As the focus of this paper is to develop a defense approach, it is beneficial to assume a strong adversary model (i.e., assume the attackers can have read access to all measurements). The defense based on this strong adversary model will be also effective to the weaker attackers who can obtain a subset of the measurements only. With Capability 3, the attackers can launch the FDI attacks. We note that the Capability 1 and 3 are aligned with NESCOR/WAMPAC.2, WAMPAC.4 and WAMPAC.8.

We now discuss the Capability 2 of the attackers. The analysis in the rest of this paper focuses on the SE period when MTD is activated. For conciseness, we use $\mathbf{H}$ to denote the original measurement matrix before the MTD, and $\mathbf{H}'$ to denote the new measurement matrix after the MTD. From the discussions in Section II-A on NESCOR/WAMPAC.7 and recent studies [20], [21], it is possible for the attackers to obtain the measurement matrix $\mathbf{H}$. However, obtaining the matrix takes time. In this paper, we assume that the minimum time for obtaining the matrix is T_a SE periods. The typical values of T_a will be discussed in detail in Section IX-A. Thus, if MTD's execution cycle is smaller than T_a, the attackers cannot obtain the $\mathbf{H}'$ that is in use in the current MTD cycle. In this paper, we also use the prime symbol ($'$) to modify the quantities after the MTD.

B. Problem Statement

Existing studies [8]–[10] mainly focus on an *arbitrary MTD* approach, i.e., the setpoints of the D-FACTS devices are arbitrarily chosen for MTD. The activation of such an arbitrary MTD would be easily detected by PCF-FDI attackers.

We illustrate PCF-FDI with an example based on a 3-bus system shown in Fig. 1. Bus 1 is chosen as the reference bus. Each bus is connected with a load. Two generators are connected to bus 1 and bus 3, respectively. The original load and generation profile is $p_{d1} = 50\,\text{MW}$, $p_{d2} = 170\,\text{MW}$, $p_{d3} = 280\,\text{MW}$, $p_{g1} = 182\,\text{MW}$, $p_{g3} = 318\,\text{MW}$, where p_{di}

TABLE II
RESULTS OF SEVERAL MTD APPROACHES ON THE 3-BUS SYSTEM

Case	$\mathbf{K}_D$	Δb_{12}	Δb_{13}	Δb_{23}	z'_{12}	z'_{13}	z'_{23}	x'_2	x'_3	$\bar{r}$
Original					-107.26	-24.74	62.74	-3.10	-0.81	0
Case 1	$\{(1,2)\}$	-1.98	0	0	-110.21	-21.79	59.79	-2.89	-0.71	5.1
Case 2	$\{(1,2),(1,3),(2,3)\}$	-1.04	0.83	-1.47	-107.26	-24.74	62.74	-2.94	-0.85	0
Case 3	$\{(1,2),(2,3)\}$	-1.04	0	-1.14	-107.26	-24.74	62.74	-2.94	-0.81	0

*Power quantifies in MW; line susceptance quantifies in p.u.; phase quantifies in deg.

denotes the active load on bus i, and p_{gj} denotes the generator's power output on bus j. The line susceptance values are $b_{12} = -19.84$, $b_{13} = -17.48$, and $b_{23} = -15.72$. Thus, $\mathbf{H} = \begin{bmatrix} -19.84 & 0 \\ 0 & -17.48 \\ 15.72 & -15.72 \end{bmatrix}$. The system state can be derived as $\mathbf{x} = [-3.10 \ -0.81]^T$. The first row of Table II shows the original system state and the power flow measurements. In the table, Δb_{ij} denotes the line susceptance perturbations in an MTD; $\mathbf{K}_D$ represents the set of lines equipped with D-FACTS devices. The result of an arbitrary MTD approach is given in Case 1 of the table, where only the susceptance of the line $(1, 2)$ is changed by $\Delta b_{12} = -1.98$. After the MTD, the estimation residual computed by the attackers, i.e., $\bar{r}$, is 5.1. Thus, the MTD is not stealthy to PCF-FDI attackers.

To push the state of the art in MTD design, we study the following two problems in this paper:

Stealthiness of MTD: How to schedule the new setpoints of D-FACTS devices such that the activation of the MTD cannot be detected by PCF-FDI attackers? Such MTD is called *hidden MTD* and is studied in Section V.

Completeness of MTD: Whether hidden MTD can detect all possible FDI attacks? If not, how to enhance the hidden MTD to detect certain types of highly structured attacks that bypass hidden MTD? This is the subject of Section VI.

V. HIDDEN MTD

In this section, we propose the hidden MTD to defend against PCF-FDI, and present the properties and construction algorithm of hidden MTD under the dc model. Moreover, the construction algorithm is extended to address the ac model.

A. Hidden MTD and Its Properties

This section defines the hidden MTD and shows its equivalence to a *power flow invariant* MTD (PFI-MTD) approach.

Definition 1: A hidden MTD ensures zero BDD residual computed by the attackers, i.e., $\bar{r} = \|\mathbf{z}' - \mathbf{H}(\mathbf{H}^T\mathbf{H})^{-1}\mathbf{H}^T\mathbf{z}'\|_2 = 0$.

Definition 2: A PFI-MTD approach maintains the power flows unchanged after the prescribed changes to the electrical characteristics of transmission lines are applied.

Lemma 1: An MTD $\mathbf{H}'$ is a PFI-MTD if and only if there exists $\mathbf{x}'' \in \mathbb{R}^n$, such that $\mathbf{H}\mathbf{x} = \mathbf{H}'\mathbf{x}''$.

Proof (Sufficiency): Let $\mathbf{x}'$, $\mathbf{z}'$ and $\mathbf{B}'$ denote the system state, the actual line flows, and the susceptance matrix after MTD that gives a new measurement matrix $\mathbf{H}'$, respectively. Note that the $\mathbf{x}''$ is defined as an arbitrary vector that satisfies $\mathbf{H}\mathbf{x} = \mathbf{H}'\mathbf{x}''$. Thus, its definition is different from that of $\mathbf{x}'$. Now, we prove $\mathbf{x}'' = \mathbf{x}'$.

As loads do not change in a time duration around the activation of the MTD (see Section III-B), the generators' power outputs do not change as well given the already established balance between generation and load. (A more detailed explanation from a perspective of frequency control is given in Remark 1 after this proof.) Thus, the power injection of each bus, which is the difference between the load's power draw and the generator's output at the bus, remains unchanged. Hence, we have $\mathbf{p} = \mathbf{B}'\mathbf{x}'$. By denoting p_i and $\mathbf{B}_i$ the ith elements of $\mathbf{p}$ and $\mathbf{B}$, respectively, we have $p_i = \mathbf{B}_i\mathbf{x}$. Note that the bus power injection is the sum of power flows through all the outgoing lines, i.e., $\mathbf{B}_i = \sum_{\forall j,(i,j)\in\mathbf{K}} \mathbf{H}_{ij}$, where $\mathbf{K}$ is the set of all the transmission lines. From $\mathbf{H}\mathbf{x} = \mathbf{H}'\mathbf{x}''$, we have $\mathbf{B}_i\mathbf{x} = \sum_{\forall j,(i,j)\in\mathbf{K}} \mathbf{H}_{ij}\mathbf{x} = \sum_{\forall j,(i,j)\in\mathbf{K}} \mathbf{H}'_{ij}\mathbf{x}'' = \mathbf{B}'_i\mathbf{x}''$. Thus, $\mathbf{p} = \mathbf{B}'\mathbf{x}'' = \mathbf{B}'\mathbf{x}'$. As $\mathbf{B}'$ is non-singular, we have $\mathbf{x}'' = \mathbf{x}'$. Thus, $\mathbf{z}' = \mathbf{H}'\mathbf{x}' = \mathbf{H}'\mathbf{x}'' = \mathbf{H}\mathbf{x} = \mathbf{z}$, i.e., the line flows remain unchanged. Hence, $\mathbf{H}'$ is a PFI-MTD.

Necessity: Since $\mathbf{H}'$ is a PFI-MTD, we obtain $\mathbf{z} = \mathbf{z}'$. From $\mathbf{z} = \mathbf{H}\mathbf{x}$ and $\mathbf{z}' = \mathbf{H}'\mathbf{x}'$, $\mathbf{x}'$ satisfies $\mathbf{H}\mathbf{x} = \mathbf{H}'\mathbf{x}'$. ■

Remark 1: As assumed in Section III-B, the loads are steady around the activation of MTD. Each generator's output is automatically adjusted by the primary and secondary frequency controls. Since the loads are steady, the total generation is equal to the total load and the frequency is at the nominal value. Under the dc model, the line loss is always zero. Therefore, after MTD, the balance between generation and load remains and the frequency is still at the nominal value. Thus, each generator's output will not be adjusted and the bus power injections remain unchanged.

As $\mathbf{H}'$ is non-singular, if there exists $\mathbf{x}''$ satisfying $\mathbf{H}\mathbf{x} = \mathbf{H}'\mathbf{x}''$, the $\mathbf{x}''$ is unique and must be the system state after executing MTD $\mathbf{H}'$. As an example, in Case 2 of Table II, the MTD is $\mathbf{H}' = \begin{bmatrix} -20.89 & 0 \\ 0 & -16.65 \\ 17.19 & -17.19 \end{bmatrix}$. There exists $\mathbf{x}'' = \begin{bmatrix} -2.94 \\ -0.85 \end{bmatrix}$, such that $\mathbf{H}\mathbf{x} = \mathbf{H}'\mathbf{x}''$. Thus, $\mathbf{H}'$ is a PFI-MTD and the system state becomes $\mathbf{x}''$ after MTD. In addition, this MTD is stealthy to the attackers because $\bar{r} = 0$ as shown in the table.

Now, we show that PFI-MTD is equivalent to hidden MTD.

Proposition 1: An MTD is a hidden MTD if and only if it is a PFI-MTD.

Proof (Sufficiency): For a PFI-MTD $\mathbf{H}'$, $\mathbf{z} = \mathbf{z}'$. From $\mathbf{z} = \mathbf{H}\mathbf{x}$, the estimation residual computed by the attackers, i.e., $\bar{r} = \|\mathbf{z}' - \mathbf{H}(\mathbf{H}^T\mathbf{H})^{-1}\mathbf{H}^T\mathbf{z}'\|_2 = \|\mathbf{z} - \mathbf{H}(\mathbf{H}^T\mathbf{H})^{-1}\mathbf{H}^T\mathbf{z}\|_2 = \|\mathbf{z} - \mathbf{H}\mathbf{x}\|_2 = 0$. Thus, $\mathbf{H}'$ is a hidden MTD.

Necessity: For a hidden MTD $\mathbf{H}'$, $\bar{r} = \|\mathbf{z}' - \mathbf{H}(\mathbf{H}^T\mathbf{H})^{-1}\mathbf{H}^T\mathbf{z}'\|_2 = 0$. Thus, we have $\mathbf{z}' = \mathbf{H}\mathbf{x}''$, where

$\mathbf{x}'' \in \mathbb{R}^n$. Moreover, from $\mathbf{z}' = \mathbf{H}'\mathbf{x}'$, we have $\mathbf{H}'\mathbf{x}' = \mathbf{H}\mathbf{x}''$. Since the bus power injections remain unchanged right after the MTD, we have $\mathbf{p} = \mathbf{B}\mathbf{x} = \mathbf{B}'\mathbf{x}'$. From $\mathbf{H}'\mathbf{x}' = \mathbf{H}\mathbf{x}''$, we have $p_i = \mathbf{B}_i'\mathbf{x}' = \sum_{\forall j,(i,j)\in\mathbf{K}} \mathbf{H}_{ij}'\mathbf{x}' = \sum_{\forall j,(i,j)\in\mathbf{K}} \mathbf{H}_{ij}\mathbf{x}'' = \mathbf{B}_i\mathbf{x}''$. Thus, $\mathbf{p} = \mathbf{B}\mathbf{x}'' = \mathbf{B}\mathbf{x}$. As $\mathbf{B}$ is non-singular, we have $\mathbf{x}'' = \mathbf{x}$. Thus, $\mathbf{z}' = \mathbf{H}'\mathbf{x}' = \mathbf{H}\mathbf{x}'' = \mathbf{H}\mathbf{x} = \mathbf{z}$, i.e., $\mathbf{H}'$ is a PFI-MTD. ■

B. Construction of Hidden MTD

From Lemma 1 and Proposition 1, the construction of hidden MTD is to find an $\mathbf{H}'$ that satisfies $\mathbf{H}\mathbf{x} = \mathbf{H}'\mathbf{x}''$. This section presents an approach to constructing such an $\mathbf{H}'$ and analyzes a basic feasibility condition of hidden MTD when a subset of lines are D-FACTS-equipped.

Our approach firstly defines the system state after MTD (i.e., $\mathbf{x}''$) and then computes the new line susceptance b_{ij}' using $z_{ij} = -b_{ij}(x_i - x_j) = -b_{ij}'(x_i'' - x_j'')$ since the power flow should remain unchanged. In addition, b_{ij}' must be within the susceptance limits, i.e., $b_{ij}^{min} \le b_{ij}' \le b_{ij}^{max}$. We now consider two cases. For a line (i,j), if its power flow is zero (i.e., $-b_{ij}(x_i - x_j) = 0$), $x_i - x_j = x_i'' - x_j'' = 0$ and the new susceptance b_{ij}' can be arbitrarily chosen from $[b_{ij}^{min}, b_{ij}^{max}]$. If its power flow is non-zero, $(x_i'' - x_j'')$ needs to be non-zero. Thus, $b_{ij}' = b_{ij}\frac{x_i - x_j}{x_i'' - x_j''}$. To ensure $b_{ij}^{min} \le b_{ij}' \le b_{ij}^{max}$, x_i'' and x_j'' must meet $\frac{b_{ij}}{b_{ij}^{min}} \le \frac{x_i'' - x_j''}{x_i - x_j} \le \frac{b_{ij}}{b_{ij}^{max}}$. We now summarize the constraints that $\mathbf{x}''$ and b_{ij}' need to satisfy as follows:

$$\begin{cases} \frac{b_{ij}}{b_{ij}^{min}} \le \frac{x_i'' - x_j''}{x_i - x_j} \le \frac{b_{ij}}{b_{ij}^{max}}, & \text{if } x_i \ne x_j, (i,j) \in \mathbf{K}; \\ x_i'' = x_j'', & \text{if } x_i = x_j, (i,j) \in \mathbf{K}. \end{cases} \tag{1}$$

$$\begin{cases} b_{ij}' = b_{ij}\frac{x_i - x_j}{x_i'' - x_j''}, & \text{if } x_i \ne x_j, (i,j) \in \mathbf{K}; \\ b_{ij}^{min} \le b_{ij}' \le b_{ij}^{max}, & \text{if } x_i = x_j, (i,j) \in \mathbf{K}. \end{cases} \tag{2}$$

If some transmission lines are not equipped with D-FACTS devices, the above two constraints may not be satisfied, i.e., a PFI-MTD may not exist. The condition for the existence of PFI-MTD is given by the following proposition.

Proposition 2: Denote by $\widetilde{\mathbf{H}}$ the immutable part of $\mathbf{H}$, i.e., $\widetilde{\mathbf{H}}$ consists of the $\mathbf{H}$'s rows corresponding to all the lines with no D-FACTS devices. If each element of $\mathbf{z}$ is non-zero, a PFI-MTD exists if and only if $\text{rank}(\widetilde{\mathbf{H}}) < \text{rank}(\mathbf{H})$.

Proof (Sufficiency): Suppose $\widetilde{\mathbf{z}} = \widetilde{\mathbf{H}}\widetilde{\mathbf{x}}$, where $\widetilde{\mathbf{z}}$ consists of the $\mathbf{z}$'s elements corresponding to the rows in $\widetilde{\mathbf{H}}$, and $\widetilde{\mathbf{x}} \in \mathbb{R}^n$. By denoting $s = \text{rank}(\mathbf{H}) - \text{rank}(\widetilde{\mathbf{H}})$, we have $\widetilde{\mathbf{x}} = \mathbf{x} + \sum_{1\le l\le s} w_l \cdot \mathbf{u}_l$, where the vectors $\mathbf{u}_l \in \mathbb{R}^n$, $1 \le l \le s$, are a basis of the kernel of $\widetilde{\mathbf{H}}$ and $w_l \in \mathbb{R}$ is arbitrary. Thus, when each element of $\mathbf{z}$ is non-zero, there always exists a group of w_l, $1 \le l \le s$, such that $\widetilde{\mathbf{x}} \ne \mathbf{x}$, and $\widetilde{\mathbf{x}}$ is subject to the constraint in (1). Thus, we find a PFI-MTD $\mathbf{H}'$ different from original measurement matrix $\mathbf{H}$.

Necessity: Suppose $\text{rank}(\widetilde{\mathbf{H}}) = \text{rank}(\mathbf{H})$, i.e., $\widetilde{\mathbf{H}}$ has full column rank, then $\mathbf{x} = (\widetilde{\mathbf{H}}^T\widetilde{\mathbf{H}})^{-1}\widetilde{\mathbf{H}}^T\widetilde{\mathbf{z}}$. If there exists a PFI-MTD $\mathbf{H}'$, we have $\mathbf{z}' = \mathbf{z}$. Then, $\widetilde{\mathbf{z}}' = \widetilde{\mathbf{z}}$, where $\widetilde{\mathbf{z}}'$ consists of $\mathbf{z}'$'s elements corresponding to the elements in $\widetilde{\mathbf{z}}$. Note that $\widetilde{\mathbf{H}}$ is the immutable part of $\mathbf{H}$, i.e., the corresponding part in $\mathbf{H}'$ is also $\widetilde{\mathbf{H}}$. Then, $\mathbf{x}' = (\widetilde{\mathbf{H}}^T\widetilde{\mathbf{H}})^{-1}\widetilde{\mathbf{H}}^T\widetilde{\mathbf{z}}'$. Thus, we have $\mathbf{x}' = \mathbf{x}$. From (2) and each element of $\mathbf{z}$ is non-zero, we have $b_{ij} = b_{ij}'$, $\forall (i,j) \in \mathbf{K}$, i.e., $\mathbf{H}' = \mathbf{H}$. In other words, the power flow is invariant unless without MTD, which contradicts the assumption that a PFI-MTD exists. ■

Algorithm 1 Method to Compute a PFI-MTD

Input: $\mathbf{z}$, $\mathbf{H}$, $\mathbf{K}_D$, b_{ij}^{min}, b_{ij}^{max}, for any line (i,j)
Output: a PFI-MTD $\mathbf{H}'$
1: $\hat{\mathbf{x}} = (\mathbf{H}^T\mathbf{H})^{-1}\mathbf{H}^T\mathbf{z}$
2: construct $\widetilde{\mathbf{H}}$ from the $\mathbf{H}$'s rows corresponding to all the transmission lines not in $\mathbf{K}_D$
3: **if** $\text{rank}(\widetilde{\mathbf{H}}) == \text{rank}(\mathbf{H})$ **then**
4: **return** null
5: **end if**
6: $s = \text{rank}(\mathbf{H}) - \text{rank}(\widetilde{\mathbf{H}})$
7: compute $\mathbf{u}_l \in \mathbb{R}^n$, $1 \le l \le s$, i.e., the kernel bases of $\widetilde{\mathbf{H}}$
8: randomly generate a set of $w_l \in \mathbb{R}$, $1 \le l \le s$, such that $\mathbf{x}''$ meets (1), where $\mathbf{x}'' = \hat{\mathbf{x}} + \sum_{1\le l\le r} w_l \cdot \mathbf{u}_l$
9: compute $\mathbf{H}'$ using $\mathbf{x}''$ from (2)
10: **return** $\mathbf{H}'$

In fact, the sufficiency proof of Proposition 2 encompasses a method to construct the PFI-MTD. Algorithm 1 gives the pseudocode of this method.

We now use Case 3 in Table II to illustrate, where only two lines of the 3-bus system in Fig. 1 are equipped with D-FACTS devices. We have $\widetilde{\mathbf{H}} = [0\ -17.48]$. As $\text{rank}(\widetilde{\mathbf{H}}) = 1 < \text{rank}(\mathbf{H})$, we have $\widetilde{\mathbf{x}} = \mathbf{x} + w_1[1\ 0]^T$. By setting $w_1 = 0.16$, $\widetilde{\mathbf{x}}$ meets the constraint in (1). Thus, $\mathbf{x}'' = \widetilde{\mathbf{x}} = [-2.94\ -0.81]^T$. Then, we can compute the susceptances using (2). The table gives the corresponding susceptance perturbations. Note that for Case 1 in Table II, $\mathbf{K}_D = \{(1,2)\}$ and $\widetilde{\mathbf{H}} = \left[\begin{smallmatrix} 0 & -17.48 \\ 15.72 & -15.72 \end{smallmatrix}\right]$. As $\text{rank}(\widetilde{\mathbf{H}}) = \text{rank}(\mathbf{H})$, there does not exist a PFI-MTD.

We now discuss the impact of noisy measurements and load changes on the construction of hidden MTD. When the measurements are noiseless, the $\hat{\mathbf{x}}$ obtained from Line 1 of Algorithm 1 is exactly the actual state $\mathbf{x}$, i.e., $\hat{\mathbf{x}} = \mathbf{x}$. In this case, the MTD constructed by Algorithm 1 ensures invariant power flows and is thus hidden. When the measurements contain noises, $\hat{\mathbf{x}}$ given by Line 1 will be slightly different from $\mathbf{x}$. As a result, the MTD constructed by Algorithm 1 may lead to small changes of power flows. Thus, the MTD may not be stealthy, depending on the non-zero BDD threshold chosen by the attackers to reduce the false alarm rate. Thus, the attackers also face a trade-off between the false negative and positive rates in choosing the threshold. The impact of the load changes is similar to that of measurement noises. In Section VIII-A, we will evaluate their impacts through simulations.

C. Hidden MTD Under Ac Model

This section presents the approach to constructing hidden MTD under the ac model that captures both the line loss and reactive power flows. The measurement vector $\mathbf{z}$ consists of the active and reactive power flows measured at the two ends of each line. The system state consists of voltage magnitudes (denoted by $\mathbf{v}$) and voltage phases (denoted by $\boldsymbol{\theta}$). We adopt a branch model [39] illustrated in Fig. 2, which simultaneously captures the electrical characteristics of a transmission line and a transformer. Specifically, the transmission line is modeled as a standard π line with series admittance $g_{ij} + jb_{ij}$ and total charging susceptance y_{ij}. We note that $g_{ij} + jb_{ij} = \frac{1}{r_{ij} + j\mathcal{X}_{ij}}$, for

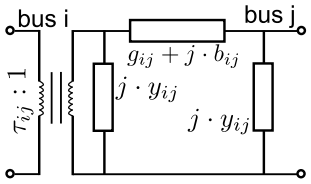


Fig. 2. Branch model.

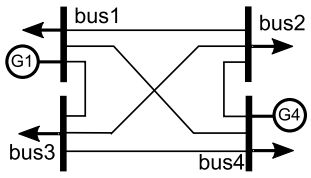


Fig. 3. 4-bus system ($n = 3$, $m = 6$).

all $(i, j) \in \mathbf{K}$, where $r_{ij} + j\mathcal{X}_{ij}$ denotes the impedance of the line (i, j). The transformer with a tap ratio magnitude of τ_{ij} is located at the from end of the branch. Under the above branch model, the network power flows are given by $\mathbf{z} = \mathbf{h}(\mathbf{v}, \boldsymbol{\theta}, \mathbf{r}, \boldsymbol{\mathcal{X}}, \mathbf{y}, \boldsymbol{\tau})$, where $\mathbf{r}$, $\boldsymbol{\mathcal{X}}$, $\mathbf{y}$ and $\boldsymbol{\tau}$ represent the vectors of line resistance, line reactance, total charging susceptance, and tap ratio, respectively. Specifically,

$$p_{ij} = \frac{1}{\tau_{ij}^2} v_i^2 g_{ij} - \frac{1}{\tau_{ij}} v_i v_j b_{ij} sin\theta_{ij} - \frac{1}{\tau_{ij}} v_i v_j g_{ij} cos\theta_{ij},$$

$$p_{ji} = v_j^2 g_{ij} + \frac{1}{\tau_{ij}} v_i v_j b_{ij} sin\theta_{ij} - \frac{1}{\tau_{ij}} v_i v_j g_{ij} cos\theta_{ij},$$

$$q_{ij} = -\frac{1}{\tau_{ij}^2} v_i^2 \big(b_{ij} + y_{ij}\big) + \frac{1}{\tau_{ij}} v_i v_j b_{ij} cos\theta_{ij} - \frac{1}{\tau_{ij}} v_i v_j g_{ij} sin\theta_{ij},$$

$$q_{ji} = -v_j^2 \big(b_{ij} + y_{ij}\big) + \frac{1}{\tau_{ij}} v_i v_j b_{ij} cos\theta_{ij} + \frac{1}{\tau_{ij}} v_i v_j g_{ij} sin\theta_{ij},$$

where p_{ij} and q_{ij} denote the active and reactive line flows of line (i, j) measured at bus i, respectively; v_i and θ_i represent the ith element of $\mathbf{v}$ and $\boldsymbol{\theta}$, respectively, and $\theta_{ij} = \theta_i - \theta_j$.

We construct the PFI-MTD as follows. First, we choose the targeted voltage phases after MTD, which are denoted by $\boldsymbol{\theta}$. Then, we use Newton's method to solve the nonlinear equations system $\mathbf{h}(\mathbf{v}, \boldsymbol{\theta}, \mathbf{r}, \boldsymbol{\mathcal{X}}, \mathbf{y}, \boldsymbol{\tau}) = \mathbf{h}(\mathbf{v}, \boldsymbol{\theta}, \mathbf{r}', \boldsymbol{\mathcal{X}}', \mathbf{y}', \boldsymbol{\tau}')$ to obtain the new four line parameters after MTD, i.e., $\mathbf{r}'$, $\boldsymbol{\mathcal{X}}'$, $\mathbf{y}'$, and $\boldsymbol{\tau}'$. Thus, after applying these new line parameters, the system state will change to $\langle \mathbf{v}, \overset{\circ}{\boldsymbol{\theta}} \rangle$ and the power flows remain unchanged. Compared with the PFI-MTD under the dc model that adjusts a single line parameter (i.e., reactance), the PFI-MTD under the ac model adjusts four line parameters to maintain the active and reactive power flows at the two ends of each line unchanged. Note that we maintain the voltage magnitude $\mathbf{v}$ to ensure voltage stability. The Newton's method can start from the original line parameters for quick convergence. We have applied the above MTD construction algorithm to the IEEE 14-bus test system and show that the resulted MTD can maintain the active and reactive power flows at the two ends of each line. This result can be found in Appendix A in the supplementary file of this paper.[1]

[1]Due to space limitations, all appendixes are omitted and can be found in the supplementary file of this paper.

In practice, the D-FACTS devices may not support changing all the four line parameters. We now discuss an approach to mitigate this potential limitation using an example situation where the D-FACTS device can only perturb the line reactance $\boldsymbol{\mathcal{X}}$. Due to the limited degree of freedom, the equations system $\mathbf{h}(\mathbf{v}, \boldsymbol{\theta}, \mathbf{r}, \boldsymbol{\mathcal{X}}, \mathbf{y}, \boldsymbol{\tau}) = \mathbf{h}(\mathbf{v}, \overset{\circ}{\boldsymbol{\theta}}, \mathbf{r}, \boldsymbol{\mathcal{X}}', \mathbf{y}, \boldsymbol{\tau})$ generally has no exact solutions. Instead, the new line reactance $\boldsymbol{\mathcal{X}}'$ is chosen to minimize the power flow changes:

$$\boldsymbol{\mathcal{X}}' = \arg\min_{\boldsymbol{\mathcal{X}}'} \left\| \mathbf{h}(\mathbf{v}, \boldsymbol{\theta}, \mathbf{r}, \boldsymbol{\mathcal{X}}, \mathbf{y}, \boldsymbol{\tau}) - \mathbf{h}\left(\mathbf{v}, \overset{\circ}{\boldsymbol{\theta}}, \mathbf{r}, \boldsymbol{\mathcal{X}}', \mathbf{y}, \boldsymbol{\tau}\right) \right\|_2.$$

We call the MTD that perturbs the lines' reactance only by following the above result as *constrained PFI-MTD*. When $\mathbf{h}(\mathbf{v}, \boldsymbol{\theta}, \mathbf{r}, \boldsymbol{\mathcal{X}}, \mathbf{y}, \boldsymbol{\tau}) \neq \mathbf{h}(\mathbf{v}, \overset{\circ}{\boldsymbol{\theta}}, \mathbf{r}, \boldsymbol{\mathcal{X}}', \mathbf{y}, \boldsymbol{\tau})$, the system state after MTD, i.e., $\langle \mathbf{v}', \boldsymbol{\theta}' \rangle$, is not exactly equal to $\langle \mathbf{v}, \overset{\circ}{\boldsymbol{\theta}} \rangle$ and the power flows will change after applying the new line parameter $\boldsymbol{\mathcal{X}}'$. We have applied the above approach to the IEEE 14-bus test system. The resulted MTD can maintain the active power flows nearly unchanged. The details of this numeric example can be found in Appendix B in the supplementary file of this paper.

VI. Completeness of MTD

This section analyzes the completeness of MTD in terms of attack space under the dc model. Then, we analyze a class of highly structured FDI attacks against incomplete MTD and propose an approach to enhancing incomplete MTD. Lastly, we discuss the taxonomy of the MTDs analyzed in this paper.

A. Complete and Incomplete MTDs

The attackers cannot detect the activation of a hidden MTD. Thus, they will launch the FDI attack crafted based on their old knowledge $\mathbf{H}$. This section studies the possibility for the attack to bypass the hidden MTD $\mathbf{H}'$ using the concepts of *attack space* and *completeness of MTD*. We define these two concepts for the general MTD as follows.

Definition 3: The attack space of an MTD is $\text{col}(\mathbf{H}) \cap \text{col}(\mathbf{H}')$.

Definition 4: If an MTD gives an attack space of $\{\mathbf{0}\}$, it is complete; otherwise, it is incomplete and the dimension of its attack space is called degree of incompleteness (DoI).

If an attack belongs to the attack space of an incomplete MTD, it cannot be detected by the MTD. As the attackers may randomly choose a vector $\mathbf{c}$ to construct the attack as $\mathbf{a} = \mathbf{Hc}$, the DoI indicates the chance that the attack can bypass the incomplete MTD. On the other hand, there does not exist an attack that can bypass a complete MTD.

Complete MTDs exist. For instance, for a 4-bus system in Fig. 3 with Bus 1 as the reference bus, the original line susceptance values are $b_{12} = -19.84$, $b_{13} = -26.88$, $b_{24} = -26.88$, $b_{34} = -15.72$, $b_{14} = -23.09$, $b_{23} = -17.42$. For an MTD $\mathbf{H}'$ with susceptance perturbations of $\Delta b_{12} = -0.99$, $\Delta b_{13} = 0.80$, $\Delta b_{24} = 0.98$, $\Delta b_{34} = 0$, $\Delta b_{14} = 0$, $\Delta b_{23} = 0$, we can verify that $\text{col}(\mathbf{H}) \cap \text{col}(\mathbf{H}') = \{\mathbf{0}\}$. Thus, $\mathbf{H}'$ is complete.

Proposition 3: For a given system with n system states and m transmission lines, a complete MTD exists only if $m \geq 2n$.

Proof: We use $\dim(\cdot)$ to denote the dimension of a space. Thus, $\dim(\text{col}(\mathbf{H}) \cap \text{col}(\mathbf{H}')) = \dim(\text{col}(\mathbf{H})) + \dim(\text{col}(\mathbf{H}')) - \dim(\text{col}(\mathbf{H}) \cup \text{col}(\mathbf{H}')) = \text{rank}(\mathbf{H}) + \text{rank}(\mathbf{H}') - \text{rank}([\mathbf{H}\ \mathbf{H}'])$. Since $\text{rank}(\mathbf{H}) = \text{rank}(\mathbf{H}') = n$ and $\text{rank}([\mathbf{H}\ \mathbf{H}']) \leq \min(m, 2n)$, we have $\dim(\text{col}(\mathbf{H}) \cap \text{col}(\mathbf{H}')) \geq 2n - \min(m, 2n)$. For a complete MTD $\mathbf{H}'$, $\text{col}(\mathbf{H}) \cap \text{col}(\mathbf{H}') = \{\mathbf{0}\}$, i.e., $\dim(\text{col}(\mathbf{H}) \cap \text{col}(\mathbf{H}')) = 0$. Thus, $\min(m, 2n) \geq 2n$ and $m \geq 2n$. ■

The 4-bus system in Fig. 3 satisfies the necessary condition for complete MTD given by Proposition 3. However, only one out of totally 38 test systems contained in the MATPOWER package [39] satisfies the condition. The details of eight IEEE test systems are given in Appendix C in the supplementary file of this paper. Note that most real-world power grids have low degrees of connectivity (i.e., small m values) for the sake of high costs in deploying transmission lines. Thus, complete MTD may not be implementable in real-world power grids. Nevertheless, as the attackers do not know $\mathbf{H}'$, the chance for that their attacks happen to bypass an incomplete MTD is low.

Proposition 4: Any hidden MTD is incomplete.

Proof: From Lemma 1 and Proposition 1, for any hidden MTD $\mathbf{H}'$, $\exists \mathbf{x}''$ such that $\mathbf{H}\mathbf{x} = \mathbf{H}'\mathbf{x}''$. Thus, an attack $\mathbf{a} = \mathbf{H}\mathbf{x} \in \text{col}(\mathbf{H})$ also belongs to $\text{col}(\mathbf{H}')$, since $\exists \mathbf{x}''$ such that $\mathbf{a} = \mathbf{H}\mathbf{x} = \mathbf{H}'\mathbf{x}''$. As $\mathbf{a} \neq \mathbf{0}$, $\mathbf{H}'$ is incomplete. ■

Proposition 4 suggests that the objectives of achieving hidden MTD and complete MTD are conflicting. If a complete MTD is applied, although the defenders are sure that any attack constructed based on the old measurement matrix $\mathbf{H}$ must be detected, alert attackers must be able to detect the activation of the complete MTD, which motivates them to cancel the FDI attacks and launch further data exfiltration attacks to obtain $\mathbf{H}'$. On the other hand, if a hidden MTD is applied, there is always a possibility that the FDI attack happens to bypass the MTD.

We now discuss the impacts of measurement noises and load changes on a complete MTD. To deal with measurement noises, a positive η is needed to reduce BDD's false alarm rates. Thus, the FDI attacks with small magnitudes may bypass a complete MTD designed under the assumption of noiseless measurements. Besides, according to Definition 3 and 4, the completeness of MTD is related to the measurement matrix $\mathbf{H}$ and $\mathbf{H}'$. Since the measurement matrix encompasses both the system topology and the susceptances of all lines, the completeness of MTD is independent of the load changes.

B. Enhancing Incomplete MTD

This section analyzes a class of highly structured FDI attacks against incomplete MTD and proposes an approach to enhancing incomplete MTD. First, we restate a concept of *critical set* that is related to attack detection.

Definition 5 [40]: A subset of lines $\mathbf{K}_C$ is a *critical set* if removing $\mathbf{H}$'s rows corresponding to all the lines in $\mathbf{K}_C$ decreases $\mathbf{H}$'s rank, whereas removing $\mathbf{H}$'s rows corresponding to all the lines in any strict subset of $\mathbf{K}_C$ does not.

Note that a system can have multiple critical sets. The studies [7], [40] showed that an FDI attack can bypass BDD when $\mathbf{K}_A$ contains at least one critical set, where $\mathbf{K}_A$ is the set of the transmission lines under attack. Thus, a critical set $\mathbf{K}_C$ is said to be uncovered by MTD if $\mathbf{K}_C \cap \mathbf{K}_D = \varnothing$, where $\mathbf{K}_D$ is the set of D-FACTS-equipped lines. Now, we describe a class of structured attacks against incomplete MTD.

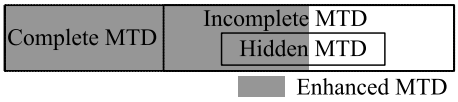


Fig. 4. Relationships between various MTDs studied in this paper.

Proposition 5: For a given $\mathbf{K}_D$, if $\mathbf{K}_A$ is the union of the uncovered critical sets, any MTD cannot detect the attack.

Proof: Since $\mathbf{K}_A$ is the union of uncovered critical sets, $\mathbf{K}_A \cap \mathbf{K}_D = \varnothing$. We prove by contradiction. Suppose that an FDI attack $\mathbf{a}$ is detected by an MTD $\mathbf{H}'$ when $\mathbf{K}_A \cap \mathbf{K}_D = \varnothing$. For $\mathbf{a} = \mathbf{H}\mathbf{c}$, we have $a_{ij} = -b_{ij}(c_i - c_j)$, $\forall (i,j) \in \mathbf{K}$, where c_i is the ith element of $\mathbf{c}$. From $\mathbf{K}_A \cap \mathbf{K}_D = \varnothing$, we have $a_{ij} = 0$ and $c_i - c_j = 0$, $\forall (i,j) \in \mathbf{K}_D$. Therefore, $0 = a_{ij} = -b'_{ij}(c_i - c_j) = \mathbf{H}'_{ij}\mathbf{c}$, $\forall (i,j) \in \mathbf{K}_D$. Moreover, the susceptances of the lines not belonging to $\mathbf{K}_D$ are immutable, that is, $\mathbf{H}_{ij} = \mathbf{H}'_{ij}$, $\forall (i,j) \notin \mathbf{K}_D$. Thus, $a_{ij} = \mathbf{H}_{ij}\mathbf{c} = \mathbf{H}'_{ij}\mathbf{c}$, $\forall (i,j) \notin \mathbf{K}_D$. Then, we have $\mathbf{a} = \mathbf{H}'\mathbf{c}$. Therefore, the attack $\mathbf{a}$ is undetected, which contradicts the supposition. ■

We now use Case 1 in Table II to illustrate the above result, where $\mathbf{K}_D = \{(1,2)\}$. The 3-bus system contains three critical sets: $\{(1,2),(1,3)\}$, $\{(1,2),(2,3)\}$, $\{(1,3),(2,3)\}$. The critical set $\{(1,3),(2,3)\}$ is uncovered. Under the structured attack, i.e., $\mathbf{a} = \mathbf{H}[0\ \varepsilon]^T$, where $\mathbf{H}$ has been given in Section IV-B and $\varepsilon \in \mathbb{R}$ is arbitrary, the residual computed by the defender is always zero. Thus, the attack is undetected.

To launch the structured attacks, the attackers need $\mathbf{K}_D$ to compute all uncovered critical sets and then decide $\mathbf{K}_A$. The attackers can launch data exfiltration attacks to obtain $\mathbf{K}_D$ or infer $\mathbf{K}_D$ by observing the historical $\mathbf{H}$ matrices.

To defend against the structured attacks, we may enhance MTD by deploying D-FACTS devices such that all critical sets are covered by MTD. Such MTD is called *enhanced MTD*. It can be easily proved that enhanced MTD requires $\text{rank}(\mathbf{H}_D) = n$, where $\mathbf{H}_D$ consists of $\mathbf{H}$'s rows corresponding to all the lines in $\mathbf{K}_D$. Now, we use Case 3 in Table II to illustrate this result, where $\mathbf{K}_D = \{(1,2),(2,3)\}$. The three critical sets are covered. Thus, the MTD is an enhanced MTD.

C. MTD Taxonomy

Fig. 4 illustrates the relationships between the MTD strategies studied in this paper. Any MTD is either complete or incomplete. From Proposition 4, hidden MTD is a subset of incomplete MTD. Since any complete MTD must be able to detect the structured attack analyzed in Section VI-B, complete MTD is a subset of enhanced MTD. Note that, as the hidden MTD can also be enhanced by following the D-FACTS deployment strategy proposed in Section VI-B, in Fig. 4, hidden MTD and enhanced MTD intersect. As discussed in Section VI-A, complete MTD may not be realizable in practice because of limited transmission lines. Thus, enhanced hidden MTD is a desirable defense strategy.

VII. Operational Cost of MTD

The MTD's operational cost is defined as the difference between the power system's generation costs before and after MTD. We assume that the system operates at the security-constrained optimal power flow (SCOPF) operation point before MTD. Denote by C_0 the generation cost under SCOPF. Right after MTD, the primary and secondary frequency controls will take effect. Denote by C_1 the total generation cost after the convergence of the frequency controls. Then, the system can redispatch the generations to achieve SCOPF. Denote by C_2 the total generation cost after the generation redispatch. This section discusses the relationships between C_0, C_1 and C_2 under the PFI-MTD and arbitrary MTD, respectively. We separately consider the dc and ac models as follow. Table III summaries the analysis results.

A. Dc Model

As discussed in Remark 1, under the dc model that assumes zero line loss, the generators' power outputs will not be adjusted by the frequency controls because the MTD will not affect the already established balance between generation and load. Therefore, for both the arbitrary MTD and PFI-MTD, $C_0 = C_1$. For PFI-MTD, the power flows remain unchanged after MTD. Thus, $C_1 = C_2$. For arbitrary MTD, we consider two cases:

- Case A: The power system has no congested line (i.e., the power flow through each line is under the line capacity) before arbitrary MTD. If the power flows through all lines do not exceed the line capacities right after the arbitrary MTD, the generators' outputs will not be adjusted by the SCOPF operation and $C_1 = C_2$; If the power flow through any line exceeds the line capacity right after arbitrary MTD, the total generation cost will increase after the SCOPF-based generation redispatch, i.e., $C_1 < C_2$.
- Case B: The power system has a congested line before the arbitrary MTD. If the power flow through this line becomes larger than the line capacity after MTD, the generation cost will increase after the SCOPF-based generation redispatch, i.e., $C_1 < C_2$; If the power flow through this line decreases and the line is no longer congested, the generation cost will decrease, i.e., $C_1 > C_2$. In summary, the relationship between C_1 and C_2 depends on the power flows after the arbitrary MTD. We use $C_1 \lesseqgtr C_2$ to denote these two possibilities.

B. Ac Model

Under the ac model, the line loss should be considered. We first consider the PFI-MTD. Since the power flows and generators' power outputs remain unchanged right after PFI-MTD, we have $C_0 = C_1$. As all the controlled power system variables (including all the generators' power outputs and the power flows through all the lines) before and right after MTD must satisfy the SCOPF's constraints, the current value of generators' power outputs is a feasible solution under the security constraints. Thus, the total generation cost will not increase after the SCOPF-based generation redispatch. In particular, the generation cost may decrease since the line resistance will be changed by the MTD (see Section V-C), i.e., $C_1 \geq C_2$. In summary, for PFI-MTD, $C_0 = C_1 \geq C_2$.

TABLE III
Summary of MTD's Operational Cost

Model	MTD Type	Operational cost
dc	PFI-MTD	$C_0 = C_1 = C_2$
	arbitrary MTD (no congestion before MTD)	$C_0 = C_1 \leq C_2$
	arbitrary MTD (congestion before MTD)	$C_0 = C_1 \lesseqgtr C_2$
ac	PFI-MTD	$C_0 = C_1 \geq C_2$
	arbitrary MTD	$C_0 \lesseqgtr C_1 \lesseqgtr C_2$

Then, we consider the arbitrary MTD. After the arbitrary MTD, the line loss may increase or decrease and the generation will accordingly increase or decrease by the frequency controls. Thus, we have $C_0 \lesseqgtr C_1$. We now consider two cases for the relationship between C_1 and C_2.

- Case A: For the power system has no congested line before arbitrary MTD, if all the controlled power system variables satisfy the SCOPF's constraints right after the arbitrary MTD, similar to the analysis of the PFI-MTD under the ac model, we have $C_1 \geq C_2$; if any controlled variable is beyond the security constraints, the generator cost may increase, i.e., $C_1 \leq C_2$. In summary, $C_1 \lesseqgtr C_2$.
- Case B: For the power system with a congested line before the arbitrary MTD, similar to the analysis of the arbitrary MTD under the dc model, we have $C_1 \lesseqgtr C_2$.

C. Numerical Results

Now we use the 3-bus system shown in Fig. 1 as an example to illustrate. We impose the following constraints: Generator's output limit is $0 \leq p_{gi} \leq 500$ MW, $i = 1$ or 3; transmission line capacity is $|z_{ij}| \leq 100$ MW, $(i, j) \in \mathbf{K}$. The generators' cost functions are $cost_{g1} = 0.05p_{g1}^2 + 1.2p_{g1} + 600$ \$/hr and $cost_{g3} = 0.11p_{g3}^2 + 5p_{g3} + 300$ \$/hr. The loads before MTD are $p_{d1} = 50$ MW, $p_{d2} = 170$ MW, $p_{d3} = 280$ MW. Therefore, we can compute the power flows, generators' outputs and the total generation cost under SCOPF, which are given in the first row of Table IV. Note that we use the superscript $\{\cdot\}'^*$ to denote SCOPF operation point after MTD. The line $(1, 2)$ is congested. The result of PFI-MTD is given in Case 1 of the table. We can see that $C_0 = C_1 = C_2$. The results of arbitrary MTD are given in Case 2 and 3 of the table, which correspond to the two situations in Case B in Section VII-A. In Case 2, the power flow through the line $(1, 2)$ is larger than the line capacity right after MTD, and we can see that $C_0 = C_1 < C_2$. In Case 3, the power flow through line $(1, 2)$ decreases, and we can see that $C_0 = C_1 > C_2$. These results are consistent with our analysis in Section VII-A.

VIII. Simulations

We conduct simulations using MATPOWER [39] based on the IEEE 14-bus system model, which consists of 14 buses ($n = 13$) and 20 transmission lines ($m = 20$).

A. Impact of Measurement Noises and Variable Loads

Our analysis assumes noiseless measurements and steady loads. Here, we evaluate the impact of measurement noises

TABLE IV
MTD'S OPERATIONAL COST OF SEVERAL MTD APPROACHES ON THE 3-BUS SYSTEM

Case	Δb_{12}	Δb_{13}	Δb_{23}	z'_{12}	z'_{13}	z'_{23}	p'_{g1}	p'_{g3}	C_1	z'^*_{12}	z'^*_{13}	z'^*_{23}	p'^*_{g1}	p'^*_{g3}	C_2
Original										-100.00	-10.28	70.00	160.3	339.7	16770.50
Case 1	-1.04	0.83	-1.06	-100.00	-10.28	70.00	160.3	339.7	16770.50	-100.00	-10.28	70.00	160.3	339.7	16770.50
Case 2	-1.26	0	0	-101.78	-8.50	68.22	160.3	339.7	16770.50	-100.00	-5.03	70.00	155.0	345.0	17102.76
Case 3	1.11	0	0	-98.28	-12.00	71.72	160.3	339.7	16770.50	-100.00	-15.52	70.00	165.5	334.5	16447.05

*Power quantities in MW; line susceptance quantifies in p.u.; phase quantifies in deg; cost quantifies in $/hr.

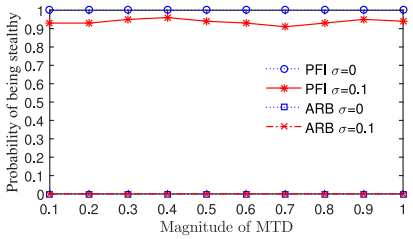


Fig. 5. PFI-MTD vs. arbitrary MTD (ARB) and impact of noises.

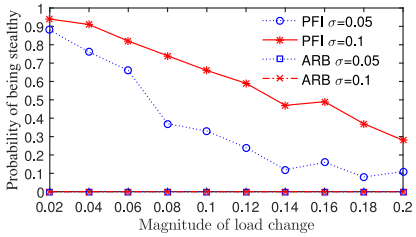


Fig. 6. Impact of variable loads and noises on PFI-MTD.

and variable loads on hidden MTD and arbitrary MTD. In the simulations, all the lines are equipped with D-FACTS devices. We use the probability for MTD to be stealthy to the attackers and attack detection probability as the evaluation metrics.

Fig. 5 shows the probability for MTD to be stealthy to the attackers under different MTD magnitudes and steady loads. For an MTD magnitude of q_m, we set $b_{ij}^{min} = (1+q_m)\cdot b_{ij}$ and $b_{ij}^{max} = b_{ij}/(1+q_m)$. Note that b_{ij} is negative. In other words, for a larger MTD magnitude, the line susceptance can be chosen from a larger range, which requires more line susceptance adjusting capability. In practice, 0.2 is a typical setting for q_m and 0.9 is achievable [41]. Thus, we vary q_m from 0.1 to 1. The measurement noises are sampled from the normal distribution $\mathcal{N}(0, \sigma^2)$. For the noiseless case (i.e., $\sigma = 0$), the PFI-MTD is always stealthy to the attackers, which is consistent with our analysis. For the noisy case, the PFI-MTD constructed based on an imperfect system state estimate may not maintain the power flows exactly. Thus, it may be detected by the attackers (with a probability of less than 10% as shown in Fig. 5). The arbitrary MTD can be always detected by the attackers.

Fig. 6 shows the probability for PFI-MTD to be stealthy to the attackers under different load change magnitudes. For a load change magnitude q_d, the load when the attackers try to detect MTD is randomly selected between $1/(1+q_d)$ and $(1+q_d)$ times of the original load. From the figure, the probability of being stealthy decreases with the magnitude of load change, because the changed load will lead to power flow changes, making the MTD detectable by the attackers. This implies that the PFI-MTD should be performed frequently enough such that the load will not change too much from the last PFI-MTD. From the figure, a higher noise level leads to higher MTD's stealthiness probability. This is because, for a higher noise level, the BDD should tolerate more deviations between the measured and estimated power flows to ensure a certain false alarm rate, which, however, reduces the attackers' capability in detecting MTD. The arbitrary MTD can be always detected by the attackers.

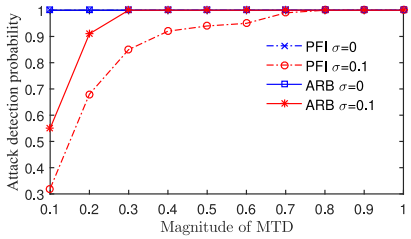


Fig. 7. Attack detection probability of PFI-MTD and arbitrary MTD.

Fig. 7 shows the MTD's attack detection probability under different MTD magnitudes. The magnitude of load change is fixed at 0.1. We construct the attack as follows. We choose a vector $\mathbf{c}$ and then compute the attack vector $\mathbf{a}$ from $\mathbf{a} = \mathbf{Hc}$. The $\mathbf{c}$'s elements are sampled from the uniform distribution $\mathcal{U}(-\frac{d}{2}, \frac{d}{2})$, where d characterizes the magnitude of attack. In this experiment, we set $d = 0.01$. For the noiseless case, the PFI-MTD and arbitrary MTD can always detect the attack. For the noisy case, the attack detection probability drops, which is consistent with intuition. In particular, PFI-MTD performs worse than the arbitrary MTD when the MTD magnitude is low. This is because, PFI-MTD needs to satisfy additional constraints to maintain power flows, which reduces its detection capability. However, the performance gap between PFI-MTD and arbitrary MTD diminishes for larger MTD magnitudes. The result in Fig. 7 suggests that, to implement the hidden MTD for stealthiness to attackers, more line susceptance adjusting capability is needed to achieve a certain level of attack detection probability, compared with the arbitrary MTD.

B. Incompleteness and Uncovered Critical Sets

This section evaluates the DoI and the number of uncovered critical sets of the hidden MTD and arbitrary MTD. Fig. 8 shows the DoI under different numbers of D-FACTS-equipped lines (denoted by $\|\mathbf{K}_D\|$). Given $\|\mathbf{K}_D\|$, we enumerate all possible D-FACTS deployments. The error bars show the maximum and minimum of DoI. From the figure, the global minimum of DoI is 6, which is consistent with our analytic result of

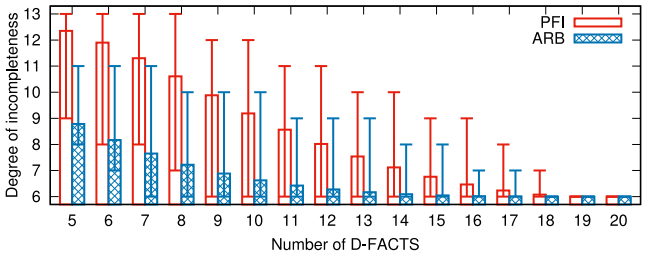


Fig. 8. DoI vs. $\|\mathbf{K}_D\|$.

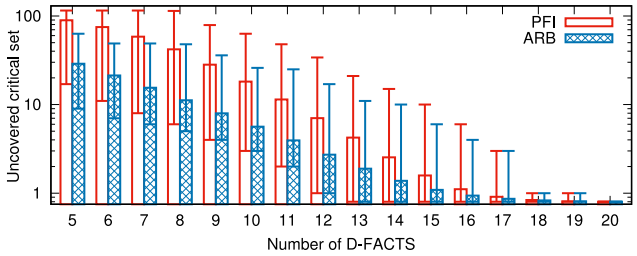


Fig. 9. Number of uncovered critical sets vs. $\|\mathbf{K}_D\|$.

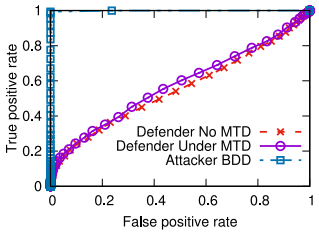


Fig. 10. ROC curves when defenders adopt dc and attackers adopt ac model.

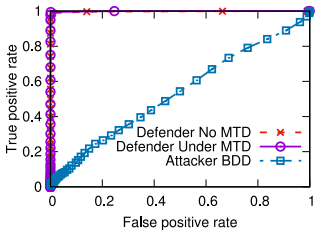


Fig. 11. ROC curves when defenders adopt ac and attackers adopt dc model.

$2n - \min(m, 2n)$. The DoI decreases with $\|\mathbf{K}_D\|$. For arbitrary MTD, the DoI is no less than $n - \|\mathbf{K}_D\|$. PFI-MTD generally yields higher DoI, because it needs to satisfy additional constraints to maintain power flows. The difference between the minimum DoIs achieved by PFI-MTD and arbitrary MTD diminishes when $\|\mathbf{K}_D\|$ is larger than 8. This suggests that by carefully deploying D-FACTS devices, hidden MTD can achieve similar (or even the same) DoI as the arbitrary MTD.

The IEEE 14-bus system has totally 115 critical sets. Fig. 9 shows the error bars for the number of uncovered critical sets. The Y-axis is in logarithmic scale. (In the figure, we use 0.8 to represent the logarithm of 0.) The number of uncovered critical sets decreases with $\|\mathbf{K}_D\|$. PFI-MTD generally leads to more uncovered critical sets, because the susceptances of several D-FACTS-equipped lines may not be modifiable to maintain power flows. From the figure, when $\|\mathbf{K}_D\| = 13$ (i.e., $\text{rank}(\mathbf{H}_D) = n$), there are 3909 and 485 instances of D-FACTS deployments to achieve enhanced MTD (i.e., the number of uncovered critical sets is zero). When $\|\mathbf{K}_D\| < 13$, there is no D-FACTS deployments to achieve enhanced MTD. This is consistent with our analysis in Section VI-B.

C. Different Power Flow Models Adopted by Defenders and Attackers

This section discusses the effectiveness of PFI-MTD when the defenders and attackers adopt different power flow models. Note that the defenders adopt the power flow model to construct PFI-MTD and detect the attacks; the attackers adopt the model to construct the FDI attacks and detect the activation of MTD. We assume that the power flows in the real system can be characterized by the ac power flow model. We adopt the following settings: the MTD magnitude $q_m = 0.5$; the load change rate $q_d = 0$; the noise's standard deviation $\sigma = 0.1$; the attack magnitude $d = 0.01$. We consider the following two cases.

i) *The defenders adopt the dc model and the attackers adopt the ac model:* Fig. 10 shows the receiver operating characteristic (ROC) curves in this situation. The ROC curve is a graphical plot that illustrates the true positive rate (TPR) against the false positive rate (FPR) at various threshold settings. Different points on an ROC curve correspond to different detection thresholds η adopted by the defenders or attackers. The TPR is measured as the ratio of the correct positive detection results over the total number of detections made when the target in question (i.e., the FDI attack or the activation of PFI-MTD) is actually present. Specifically, $TPR = \frac{TP}{TP+FN}$, where TP is the number of true positives and FN is the number of false negatives (i.e., mis-detections). The FPR, on the other hand, is measured as the ratio of incorrect positive detection results over the total number of detections made when the target in question (i.e., the FDI attack or the activation of PFI-MTD) is actually absent. Specifically, $FPR = \frac{FP}{FP+TN}$, where FP is the number of false positives and TN is the number of true negatives. The curves labeled "Defender No MTD" and "Defender Under MTD" refer to the ROC curves for the defenders to detect the FDI attacks when the PFI-MTD is absent and present, respectively. The curve labeled "Attacker BDD" refers to the ROC curve for the attackers to detect the activation of PFI-MTD. Thus, $TPR = 1$ means that there are no false negatives (i.e., no mis-detections) and $FPR = 0$ means that there are no false positives in detecting the FDI attacks by the defenders or in detecting the PFI-MTD by the attackers. Thus, the (0, 1) point on an ROC curve implies perfect detection performance. The first and second curves are the results for the attack detection before and after MTD, respectively. We can see that the MTD improves the defenders' attack detection performance. However, the two ROC curves are close to each other because the discrepancy between the defenders' dc model and the actual system model (i.e., the ac model) is the dominating factor for the inaccuracy of the attack detection. The third curve is the ROC of the attackers' BDD in detecting the PFI-MTD activations. Since the ROC curve nearly passes

through the $(0, 1)$ point, the PFI-MTD constructed from the dc model will be always detected by the attackers who adopt the ac model and appropriately select the detection threshold. Note that, in our evaluation, we assume that the actual power flows are characterized by the ac model. Thus, the PFI-MTD constructed from the dc model that approximates the actual power flows is inaccurate and can be detected by the attackers who adopt the accurate ac model. In addition, the selection of the detection threshold under the ac model is similar to that under the dc model in Section III-A. Specifically, the threshold η under the ac model can be set to be $\sigma\sqrt{\chi^2_{(m-n),\alpha}}$ to ensure a false alarm rate of $(1-\alpha)$, where m denotes the number of sensor measurements and n denotes the number of system states.

ii) *The defenders adopt the ac model and the attackers adopt the dc model:* Fig. 11 shows the ROC curves in this situation. The first and second curves are the results for the attack detection before and after MTD, respectively. We can see that the FDI attack constructed by the dc model can be always detected when the defenders adopt the ac model. The third curve is the ROC of the attackers' BDD in detecting the PFI-MTD activations. From the ROC curve, the attacker's detection performance is poor. For instance, when the false positive rate is 0.5, the true positive rate is also about 0.5. This is also caused by the discrepancy between the attackers' dc model and the actual ac model.

Moreover, when both the attackers and defenders adopt the dc model, the performance of the defenders' BDD in detecting FDI attacks and the attackers' BDD in detecting the PFI-MTD activations is not high, which is also caused by the discrepancy between the adopted dc model and the actual ac model. Specifically, for any detection threshold η, the defenders' detector cannot achieve a high TPR and a low FPR simultaneously. Note that in the numerical results presented in previous sections, we assume that the power flows in the real system can be characterized by the dc model. When both the attackers and defenders adopt the ac model, the FDI attacks can be detected reliably by the defenders' BDD after MTD and the PFI-MTD cannot be detected by the attackers' BDD.

Table V summarizes the effectiveness of the BDD, MTD, and PFI-MTD from the perspective of the attackers, when the defenders and attackers adopt different power flow models. From the table, if the defenders adopt the dc model, the attackers can succeed for sure or with some probability when they adopt the ac and dc models, respectively; if the defenders adopt the ac model to design MTD, the attackers cannot succeed no matter which power flow model they use. Thus, the ac model is a better choice for the defenders. In addition, if the defenders adopt the dc model, by adopting the ac model, the attackers can always succeed; if the defenders adopt the ac model, by adopting the ac model, the attackers can at least bypass the BDD without MTD. In summary, the ac model is more advantageous than the dc model for the attackers. However, considering that the dc power flow analysis is faster and more robust than the ac power flow analysis, both the attackers and defenders face the trade-off between (i) attack/MTD detection performance and (ii) overheads in the implementation, computation, and reliability of the detection algorithms.

TABLE V
EFFECTIVENESS OF BDD, MTD, AND PFI-MTD FROM THE ATTACKERS' PERSPECTIVE WHEN THE ATTACKERS AND DEFENDERS ADOPT DIFFERENT POWER FLOW MODELS

Power flow model			Bypass BDD	Bypass BDD	Detect
Actual	Defenders	Attackers	without MTD	with MTD	PFI-MTD
ac	dc	ac	✓	✓	✓
	ac	dc	×	×	×
	dc	dc	✓	uncertain*	uncertain
	ac	ac	✓	×	×

* The 'uncertain' means that the defenders' detector cannot achieve a high TPR and a low FPR simultaneously.

IX. DISCUSSIONS

A. System Settings

Based on the above simulation results, we now discuss the settings of several important system parameters.

1) MTD's Execution Cycle: In Section III-B, we require that the MTD's execution cycle T should be no longer than the attackers' model learning time T_a. In Section VIII-A, we found through simulations that the PFI-MTD should be performed frequently enough to ensure MTD's stealthiness. In summary, we require $T \leq \min(T_a, T_l)$, where T_l denotes the maximum number of SE periods to ensure MTD's stealthiness in the presence of load changes. Now we discuss the settings of T_a and T_l, respectively.

According to the attackers' Capability 1 and 2, the attackers can eavesdrop on the measurements of the sensors on all the lines and try to learn the new system construction. Now, we consider two cases.

Case 1: The attackers can identify but cannot locate the source sensors of the measurements. Thus, no topology information can be utilized in the power system model learning process. We name this process as *blind model learning* process. For simplicity of exposition, we assume that the MTD is not activated. For the noiseless system, from Section III-A, we have $\mathbf{z}_t = \mathbf{H}\mathbf{x}_t = \mathbf{H}\mathbf{B}^{-1}\mathbf{p}_t$. Then, $\mathbf{Z}_t = \mathbf{H}\mathbf{B}^{-1}\mathbf{P}_t$, where $\mathbf{Z}_t$ and $\mathbf{P}_t$ respectively consist of the vectors of historical sensor measurements and bus power injections, i.e., $\mathbf{Z}_t = [\mathbf{z}_1, \ldots, \mathbf{z}_t]$ and $\mathbf{P}_t = [\mathbf{p}_1, \ldots, \mathbf{p}_t]$. Denote by $\mathbb{Z}$ the space of all the possible sensor measurement vectors, i.e., $\mathbb{Z} = \lim_{t\to\infty} \mathrm{col}(\mathbf{Z}_t)$. Since $\mathbb{Z} \subseteq \mathrm{col}(\mathbf{H})$, the attackers can construct the stealthy FDI attacks directly through the Hamel base of $\mathbb{Z}$. Denote by u the number of non-zero injection buses, i.e., the buses that are connected with at least one generator or load. We have $\mathrm{rank}(\mathbf{H}) = \mathrm{rank}(\mathbf{B}) = n$, and $\mathrm{rank}(\mathbf{P}_t) \leq u$, where n is the number of buses. Since $u \leq n$, we have $\mathrm{rank}(\mathbf{Z}_t) \leq u$ and $\dim(\mathbb{Z}) = u$. Thus, if the attackers collect the power flow measurements during more than u SE periods, they can compute a Hamel base of $\mathbb{Z}$. For the noisy system, to compute the Hamel base of $\mathbb{Z}$, the attackers additionally need the data during more SE periods to reduce the influence of system noises. We note that for the weak attackers who can obtain read access to a subset of sensor measurements only, they generally cannot construct the stealthy FDI attacks through blind model learning, since they cannot utilize the system topology information and thus do not know the correlation among the sensor measurements. Thus, u is a reference setting for T_a in this case.

Case 2: The attackers can identify and locate the source sensors of the measurements. Thus, the topology information can be utilized in the power system model learning process. In this situation, the model learning process can be conducted in several subsystems in parallel. The model learning times in the subsystems are different, and the attackers can launch local FDI attacks in a subsystem once the model learning process of the subsystem is completed. We leave the detailed analysis of this case for future study.

We set T_l to ensure the stealthiness of PFI-MTD in the presence of load changes. Note that T_l is related to the load change rate q_d. Thus, we firstly select q_d by $q_d = \max_{q_d}(\Pr\{|\bar{r}(q_m, q_d, \sigma)| \leq \eta\} \geq \beta)$, where $\bar{r}(\cdot)$ denotes the residual computed by the attackers, which is a random variable due to random PFI-MTD constructed by Algorithm 1, random load change and system noise; the threshold η is selected according to the system noise deviation σ to ensure a certain level of the attackers' false alarm rate; β denotes a desired probability for the MTD being stealthy. Thus, if we can ensure that the load change is within $1/(1+q_d)$ and $(1+q_d)$ times of the original load, a constructed PFI-MTD within the MTD's magnitude q_m can remain stealthy to the attacker with a probability of no less than β. As there is no closed-form formula for $\bar{r}$, the q_d selection problem can be solved through numeric simulations. Then, we set T_l according to q_d. Specifically, we set it as the maximum value that ensures that the load change rate during T_l SE periods will be no more than q_d.

2) Magnitude of MTD: From the simulations in Section VIII-A, we found that the magnitude of MTD has substantial impact on attack detection probability. Now, we discuss its setting. We select the MTD's magnitude by $q_m = \min_{q_m}(\Pr\{|r(q_m, \sigma, d)| > \eta\} \geq \beta)$, where $r(\cdot)$ denotes the residual computed by the defender, which is a random variable due to random PFI-MTD constructed by Algorithm 1, random system noise and attack vector; the threshold η is selected according to the system noise deviation σ to ensure a certain level of the defenders' false alarm rate; β denotes a desired attack detection rate. Thus, if the attackers launch the attacks with the attack magnitude deviation d, a constructed PFI-MTD within the MTD's magnitude q_m can detect the attacks with a probability of no less than β. As there is no closed-form formula for r, the q_m selection problem can be solved through numeric simulations. We note that the setting of MTD's magnitude greatly depends on the target power system. For example, for the 14-bus system with $\sigma = 0.1$, $d = 0.01$, and $\beta = 90\%$, the magnitude of MTD q_m should be set as 0.4; for the 39-bus system, q_m can be set less than 0.2.

B. Attack Identification and Mitigation

On the detection of FDI attacks, it is desirable to identify the attacks, i.e., to identify which sensors have been compromised (i.e., $\mathbf{K}_A$). Then, the impact of the attacks should be mitigated, or the attacks should be isolated. Note that the mitigation approach of simply discarding all the compromised data may make the system unobservable. We discuss a possible approach to identify and mitigate the FDI attacks through the MTD approach. The FDI attacks detected by MTD can be identified through distributed SE proposed in [42], since the residual of BDD based on the normal sensor measurements in the distributed SE will not exceed the threshold. Now we discuss whether the attack signals and actual measurements can be separated to mitigate the attack. For noiseless system, the power flow model under MTD $\mathbf{H}'$ in the absence of the attack is $\mathbf{z}' = \mathbf{H}'\mathbf{x}'$. Then, we have $\mathbf{z}' + \mathbf{a} = \mathbf{H}'\mathbf{x}' + \mathbf{H}\mathbf{c} = \begin{bmatrix}\mathbf{H}' & \mathbf{H}\end{bmatrix}\begin{bmatrix}\mathbf{x}' \\ \mathbf{c}\end{bmatrix}$. Therefore, the attack signal $\mathbf{a}$ and actual measurement $\mathbf{z}'$ can be separated when the equation system $\mathbf{z}' + \mathbf{a} = \begin{bmatrix}\mathbf{H}' & \mathbf{H}\end{bmatrix}\mathbf{x}_e$ has a unique solution, i.e., $\mathbf{x}_e = \begin{bmatrix}\mathbf{x}' \\ \mathbf{c}\end{bmatrix}$, where $\mathbf{x}_e \in \mathbb{R}^{2n}$. Then, we have $\text{rank}([\mathbf{H}' \ \mathbf{H}]) = 2n$. According to the proof of Proposition 3, we have $\text{col}(\mathbf{H}') \cap \text{col}(\mathbf{H}) = \{\mathbf{0}\}$. That is, the attack can be mitigated when $\mathbf{H}'$ is a complete MTD.

X. Conclusion and Future Work

This paper studies PCF-FDI that tries to detect the activation of MTD before launching an FDI attack. To defend against PCF-FDI, we propose a hidden MTD approach that maintains the power flows and develop an algorithm to construct the hidden MTD. We analyze the completeness of MTD and show that the stealthiness and completeness are two conflicting goals in MTD design. Moreover, we propose an approach to enhancing incomplete MTD (including hidden MTD) against a class of highly structured FDI attacks. Finally, we analyze MTD's operational cost and present numerical results. Simulations are conducted to compare the stealthiness and completeness of our hidden MTD approach with the existing arbitrary MTD approach.

We now discuss several issues that can be studied in future work. First, the relationship between MTD's operational cost and attack detection performance can be studied quantitatively. The D-FACTS devices are originally used to maintain desirable power flows and reduce the generation cost. In Section VII, we have performed preliminary and qualitative analysis of MTD's operational cost. In Section VIII-A, we have conducted simulations to evaluate MTD's attack detection performance. It is interesting to study any trade-off between the two aspects such that the defenders can better schedule the MTD perturbations to achieve a satisfactory balance. Second, existing industry standards, such as those from International Electrotechnical Commission (IEC) and the Critical Infrastructure Protection (CIP) from North American Electric Reliability Corporation (NERC), provide guidelines to enhance smart grid cybersecurity. However, these standards do not specifically address open cybersecurity issues, such as those caused by zero-day vulnerability exploits and the threats studied in this paper. Therefore, recommending our approach as an option in these evolving standards can be considered, in order to bring the state-of-the-art research to the practice. Third, besides MTD against FDI attacks on state estimation, it is also interesting to study MTD against FDI attacks on closed-loop control systems. Detecting FDI attacks on either sensor or control data in a closed loop has been extensively studied. However, detecting FDI attacks on both sensor and control data, which are similar to the Stuxnet attack, has not

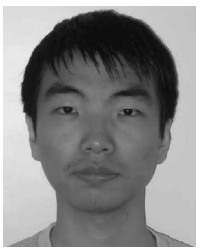
received adequate research. MTD is applied to detect such Stuxnet-like attacks in [43]. In future work, the stealthiness and the completeness of the MTD against Stuxnet-like attacks can be studied.

ACKNOWLEDGMENT

The authors wish to thank the editors and the anonymous reviewers for providing valuable feedbacks on this work.

REFERENCES

[1] S. Karnouskos, "Stuxnet worm impact on industrial cyber-physical system security," in *Proc. IECON*, 2011, pp. 4490–4494.
[2] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Security*, vol. 14, no. 1, p. 13, 2011.
[3] R. B. Bobba *et al.*, "Detecting false data injection attacks on DC state estimation," in *Proc. Workshop Secure Control Syst.*, 2010, pp. 18–26.
[4] J. Kim and L. Tong, "On topology attack of a smart grid: Undetectable attacks and countermeasures," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 7, pp. 1294–1305, Jul. 2013.
[5] L. Yang and F. Li, "Detecting false data injection in smart grid in-network aggregation," in *Proc. SmartGridComm*, 2013, pp. 408–413.
[6] X. Yang *et al.*, "A novel en-route filtering scheme against false data injection attacks in cyber-physical networked systems," *IEEE Trans. Comput.*, vol. 64, no. 1, pp. 4–18, Jan. 2015.
[7] A. Giani *et al.*, "Smart grid data integrity attacks: Characterizations and countermeasures$^{\pi}$," in *Proc. SmartGridComm*, 2011, pp. 232–237.
[8] K. L. Morrow, E. Heine, K. M. Rogers, R. B. Bobba, and T. J. Overbye, "Topology perturbation for detecting malicious data injection," in *Proc. Int. Conf. Syst. Sci.*, 2012, pp. 2104–2113.
[9] K. R. Davis, K. L. Morrow, R. Bobba, and E. Heine, "Power flow cyber attacks and perturbation-based defense," in *Proc. SmartGridComm*, 2012, pp. 342–347.
[10] M. A. Rahman, E. Al-Shaer, and R. B. Bobba, "Moving target defense for hardening the security of the power system state estimation," in *Proc. ACM Workshop Moving Target Defense*, 2014, pp. 59–68.
[11] NESCOR. (2017). *Electric Sector Failure Scenarios and Impact Analyses—Version 3.0*. [Online]. Available: http://smartgrid.epri.com/doc/NESCOR Failure Scenarios v3 12-11-15.pdf
[12] (2014). *Scada Cyber Attacks Double in 2014*. [Online]. Available: https://www.automationworld.com/scada-attacks-double-2014
[13] R. Khan, P. Maynard, K. Mclaughlin, D. Laverty, and S. Sezer, "Threat analysis of blackenergy malware for synchrophasor based real-time control and monitoring in smart grid," in *Proc. Int. Symp. ICS Scada Cyber Security Res.*, 2016, pp. 1–11.
[14] J. Leyden. (2017). *Polish Teen Derails Tram After Hacking Train Network*. [Online]. Available: https://www.theregister.co.uk/2008/01/11/tram_hack
[15] M. Clayton. (2017). *Cyberattack on Illinois Water Utility May Confirm Stuxnet Warnings*. [Online]. Available: https://www.csmonitor.com/USA/2011/1118/Cyberattack-on-Illinois-water-utility-may-confirm-Stuxnet-warnings
[16] D. Gewirtz, "Night dragon: Cyberwar meets corpoiate espionage," *J. Counterterrorism Homeland Security Int.*, vol. 17, no. 2, p. 6, 2011.
[17] B. Bencsáth, G. Pék, L. Buttyán, and M. Félegyházi. (2011). *Duqu: A Stuxnet-Like Malware Found in the Wild*. [Online]. Available: http://www.crysys.hu/publications/files/bencsathPBF11duqu.pdf
[18] *Flame Malware—Like Stuxnet and Duqu Before It*, Venafi, Salt Lake City, UT, USA, 2012.
[19] N. Nelson. (2017). *The Impact of Dragonfly Malware on Industrial Control Systems*. [Online]. Available: https://www.sans.org/reading-room/whitepapers/ICS/impact-dragonfly-malware-industrial-control-systems-36672
[20] Z.-H. Yu and W.-L. Chin, "Blind false data injection attack using PCA approximation method in smart grid," *IEEE Trans. Smart Grid*, vol. 6, no. 3, pp. 1219–1226, May 2015.
[21] I. Markwood, Y. Liu, K. Kwiat, and C. A. Kamhoua, "Electric grid power flow model camouflage against topology leaking attacks," in *Proc. IEEE INFOCOM*, 2017, pp. 1–9.
[22] 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.
[23] M. A. Rahman and H. Mohsenian-Rad, "False data injection attacks with incomplete information against smart power grids," in *Proc. IEEE Glob. Commun. Conf. (GLOBECOM)*, 2012, pp. 3153–3158.
[24] X. Liu and Z. Li, "Local load redistribution attacks in power systems with incomplete network information," *IEEE Trans. Smart Grid*, vol. 5, no. 4, pp. 1665–1676, Jul. 2014.
[25] L. Xie, Y. Mo, and B. Sinopoli, "False data injection attacks in electricity markets," in *Proc. 1st IEEE Int. Conf. Smart Grid Commun.*, 2010, pp. 226–231.
[26] L. Jia, R. J. Thomas, and L. Tong, "Impacts of malicious data on real-time price of electricity market operations," in *Proc. Hawaii Int. Conf. Syst. Sci.*, 2012, pp. 1907–1914.
[27] J. Kim, L. Tong, and R. J. Thomas, "Dynamic attacks on power systems economic dispatch," in *Proc. Asilomar Conf. Signals Syst. Comput.*, 2015, pp. 345–349.
[28] G. Hug and J. A. Giampapa, "Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1362–1370, Sep. 2012.
[29] C. Wang, C.-W. Ten, Y. Hou, and A. Ginter, "Cyber inference system for substation anomalies against alter-and-hide attacks," *IEEE Trans. Power Syst.*, vol. 32, no. 2, pp. 896–909, Mar. 2017.
[30] A. Ginter, *SCADA Security—What's Broken and How to Fix It*. Abterra Technol. Inc., Calgary, AB, Canada, 2016.
[31] Y. Huang, H. Li, K. A. Campbell, and Z. Han, "Defending false data injection attack on smart grid network using adaptive CUSUM test," in *Proc. Annu. Conf. Inf. Sci. Syst.*, 2011, pp. 1–6.
[32] L. Liu, M. Esmalifalak, Q. Ding, V. A. Emesih, and Z. Han, "Detecting false data injection attacks on power grid by sparse optimization," *IEEE Trans. Smart Grid*, vol. 5, no. 2, pp. 612–621, Mar. 2014.
[33] X. Liu, P. Zhu, Y. Zhang, and K. Chen, "A collaborative intrusion detection mechanism against false data injection attack in advanced metering infrastructure," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2435–2443, Sep. 2015.
[34] C. Gu, P. Jirutitijaroen, and M. Motani, "Detecting false data injection attacks in AC state estimation," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2476–2483, Sep. 2015.
[35] A. Ashok, M. Govindarasu, and V. Ajjarapu, "Online detection of stealthy false data injection attacks in power system state estimation," *IEEE Trans. Smart Grid*, to be published.
[36] E. Al-Shaer, Q. Duan, and J. H. Jafarian, "Random host mutation for moving target defense," in *Proc. Int. Conf. Security Privacy Commun. Syst.*, 2012, pp. 310–327.
[37] J. Tian, R. Tan, X. Guan, and T. Liu, "Hidden moving target defense in smart grids," in *Proc. 2nd Workshop Cyber-Phys. Security Resilience Smart Grids*, 2017, pp. 21–26.
[38] S. Liu, S. Mashayekh, D. Kundur, T. Zourntos, and K. Butler-Purry, "A framework for modeling cyber-physical switching attacks in smart grid," *IEEE Trans. Emerg. Topics Comput.*, vol. 1, no. 2, pp. 273–285, Dec. 2013.
[39] *Matpower*. (2017). [Online]. Available: http://www.pserc.cornell.edu/matpower/manual.pdf
[40] J. Kim, L. Tong, and R. J. Thomas, "Data framing attack on state estimation," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 7, pp. 1460–1470, Jul. 2014.
[41] K. M. Rogers and T. J. Overbye, "Some applications of distributed flexible AC transmission system (D-FACTS) devices in power systems," in *Proc. 40th North Amer. Power Symp.*, 2008, pp. 1–8.
[42] D. Wang *et al.*, "Extended distributed state estimation: A detection method against tolerable false data injection attacks in smart grids," *Energies*, vol. 7, no. 3, pp. 1517–1538, 2014.
[43] S. Weerakkody and B. Sinopoli, "Detecting integrity attacks on control systems using a moving target approach," in *Proc. IEEE Conf. Decis. Control (CDC)*, 2015, pp. 5820–5826.



Jue Tian received the B.S. degree in automation engineering from the School of Electronic and Information, Xi'an Jiaotong University, Xi'an, China, in 2011, where he is currently pursuing the Ph.D. degree with the Systems Engineering Institute and the MOE KLINNS Laboratory. He visited the School of Computer Science and Engineering, Nanyang Technological University, Singapore, from 2016 to 2017. His research interests include smart grid and cyber-physical system security. He was a recipient of the Best Paper Awards from CPSR-SG'17.

Rui Tan (M'08) received the B.S. and M.S. degrees from Shanghai Jiao Tong University in 2004 and 2007, respectively, and the Ph.D. degree in computer science from the City University of Hong Kong, in 2010. He is an Assistant Professor with the School of Computer Science and Engineering, Nanyang Technological University, Singapore. He was a Research Scientist from 2012 to 2015 and a Senior Research Scientist in 2015 with Advanced Digital Sciences Center, a Singapore-based research center of the University of Illinois at Urbana–Champaign (UIUC), a Principle Research Affiliate from 2012 to 2015 with the Coordinated Science Laboratory, UIUC, and a Post-Doctoral Research Associate from 2010 to 2012 with Michigan State University. His research interests include cyber-physical systems, sensor networks, and pervasive computing systems. He was a recipient of the Best Paper Awards from IPSN'17 and CPSR-SG'17, and the Best Paper Runner-Ups from IEEE PerCom'13 and IPSN'14.

Xiaohong Guan (M'93–SM'95–F'07) received the B.S. and M.S. degrees in automatic control from Tsinghua University, Beijing, China, in 1982 and 1985, respectively, and the Ph.D. degree in electrical engineering from the University of Connecticut, Storrs, CT, USA, in 1993. He was a Senior Consulting Engineer with PG&E, San Francisco, CA, USA, from 1993 to 1995. He visited the Division of Engineering and Applied Science, Harvard University, Cambridge, MA, USA, from 1999 to 2000. Since 1995, he has been with the Systems Engineering Institute, Xi'an Jiaotong University, Xi'an, China, where he was appointed as the Cheung Kong Professor of systems engineering in 1999, and the Dean of School of Electronic and Information Engineering in 2008. Since 2001, he has been the Director of the Center for Intelligent and Networked Systems, Tsinghua University, and served as the Head of the Department of Automation, from 2003 to 2008. His research interests include optimization of power and energy systems, electric power markets, and cyber-physical systems, such as smart grid and sensor networks.

Ting Liu received the B.S. degree in information engineering and the Ph.D. degree in system engineering from the School of Electronic and Information, Xi'an Jiaotong University, Xi'an, China, in 2003 and 2010, respectively, where he is an Associate Professor. He was a Visiting Professor with Cornell University from 2016 to 2017. His researches include software engineering and smart grids. He was a recipient of the Best Paper Award in 2017 IEEE CPSWEEK CPSR-SG, the Best Research Paper in 2016 IEEE ISSRE, and the Best Demo Award in 2014 SEKE.