Hidden Moving Target Defense in Smart Grids

Jue Tian*
Xi'an Jiaotong University, P.R. China
Nanyang Technological University, Singapore
juetian@sei.xjtu.edu.cn

Rui Tan
Nanyang Technological University
Singapore
tanrui@ntu.edu.sg

Xiaohong Guan
Xi'an Jiaotong University, P.R. China
Tsinghua University, P.R. China
xhguan@sei.xjtu.edu.cn

Ting Liu
Xi'an Jiaotong University, P.R. China
Cornell University, U.S.
tliu@sei.xjtu.edu.cn

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 less adversarial setting, in that they ignore the possibility that an alert attacker can also try to detect the activation of MTD and then cancel any FDI attack until they learn the new system configuration after MTD. Indeed, in this paper, we show that this can be achieved easily by the attacker. To improve the stealthiness of MTD against the attacker, we propose a *hidden MTD* approach that maintains the power flows of the whole grid after MTD. We develop an algorithm to construct the hidden MTD and analyze its feasibility condition when only a subset of transmission lines can adjust susceptance. Simulations are conducted to demonstrate the effectiveness of the hidden MTD against alert attackers under realistic settings.

CCS CONCEPTS

•Security and privacy →Intrusion detection systems; •Networks →*Cyber-physical networks;*

KEYWORDS

Smart grid, state estimation, false data injection attack, moving target defense

ACM Reference format:
Jue Tian, Rui Tan, Xiaohong Guan, and Ting Liu. 2017. Hidden Moving Target Defense in Smart Grids. In *Proceedings of The 2nd Workshop on Cyber-Physical Security and Resilience in Smart Grids, Pittsburgh, PA USA, April 2017 (CPSR-SG 2017),* 6 pages.
DOI: http://dx.doi.org/10.1145/3055386.3055388

*This work was completed while Jue Tian was a visiting student at Nanyang Technological University.

CPSR-SG 2017, Pittsburgh, PA USA

DOI: http://dx.doi.org/10.1145/3055386.3055388

1 INTRODUCTION

As critical infrastructures, power grids must remain stable, safe, and secure. However, recent security incidents such as the Stuxnet attack, which tampers with control and sensing data in Iranian nuclear facilities, have alerted us to a general class of data integrity attacks called *false data injection* (FDI). 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 [6], if the attacker knows 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 against SE, existing studies have resorted to securing the sensor measurements and adding more data integrity check mechanisms. In [1], a minimum subset of sensors and their data links are identified such that securing them can preclude the FDI attacks. Secure data collection protocols [9] 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 [3]. However, providing a high level of security guarantee to the sensors' and PMUs' data is often very costly.

Alternatively, we can invalidate the attacker's knowledge about the power system and thus preclude or reveal stealthy FDI attacks. To this end, recent studies [2, 7, 8] 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 [2, 7, 8] were conducted under a less adversary setting, in that they ignore the possibility that an alert attacker can also try to detect the activation of MTD and then cancel any FDI attack until they obtain the new system configuration after MTD. Indeed, in this paper, we show that the attacker can detect the activation of MTD by applying the BDD based on the original power system configuration to the eavesdropped sensor measurements. The detection will drive the attacker to launch data

exfiltration attacks to obtain the new system configuration. In this sense, existing MTD approaches may not decrease the risk faced by the power system substantially.

To improve the stealthiness of MTD against the attacker, in this paper, we propose a *hidden MTD* approach that maintains the power flows of the whole grid after MTD. As a result, the attacker's BDD based on the original system configuration will not raise an alarm. The FDI attacks, crafted based on the original system configuration, will be almost surely caught by the system's BDD, and then discarded or redirected to a honeypot for further analysis. Hence, the hidden MTD approach can induce the attacker to launch futile attacks and increase their chance of getting exposed. Specifically, we make the following contributions:

- We analyze the condition to maintain the power flows unchanged after MTD. We also develop an algorithm to compute the needed susceptance perturbations to the D-FACTS-equipped lines.
- 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 conduct simulations based on the IEEE 14-bus system to compare the hidden MTD with the existing MTD and evaluate the impact of various realistic factors, including measurement noises and load changes, on the performance of the hidden MTD.

Paper organization: Section 2 reviews related works. Section 3 introduces background. Section 4 and 5 present the hidden MTD and simulation results. Section 6 concludes.

2 RELATED WORK

Recent research has studied the FDI attacks against the SE of power grids. Liu et al. [6] analyzed the condition for bypassing the BDD of SE. To detect the stealthy FDI attacks, Bobba et al. [1] proposed to protect a set of strategically selected sensor measurements such that no FDI attack vectors satisfying the stealthy condition analyzed in [6] can be found. Better attack detection algorithms have also been developed. For instance, Huang et al. [4] used adaptive CUSUM test to improve detection performance. Liu et al. [5] designed a new detector based on the separation of nominal and abnormal power grid states. 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 [3] shows that $(p+1)$ PMUs deployed at carefully chosen locations in a grid can neutralize a collection of p irreducible FDI attacks.

MTD, originally proposed to enhance network security, has been recently applied to increase the barrier for the attacker to launch stealthy FDI attacks against power grids. Morrow et al. [2, 7] 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. [8] proposed an ex-ante MTD approach that randomly selects a subset of transmission lines and randomly perturbs their susceptance, such that the attacker lacks the knowledge of the system to launch FDI attacks. However, as discussed in Section 1, the activation of this ex-ante MTD approach can be detected by the attacker. In contrast, our hidden MTD is stealthy to the attacker due to the unchanged power flows.

Table 1: Summary of notations

Symbol	Definition
m	number of meter measurements
n	number of buses
$\mathbf{x}$	system state vector
$\hat{\mathbf{x}}$	estimated system state vector
$\mathbf{z}$	measurement vector
$\mathbf{H}$	measurement matrix
$\mathbf{H}_{ij}$	row vector of $\mathbf{H}$ corresponding to line (i,j)
$\mathbf{B}$	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
b_{ij}	susceptance of line (i,j)
b'_{ij}	line susceptance after MTD
Δb_{ij}	variation of line susceptance
$b_{ij}^{max}, b_{ij}^{min}$	bounds of line susceptance modification
$\widetilde{\mathbf{H}}$	immutable part of $\mathbf{H}$

3 PRELIMINARIES

This section presents the preliminaries including FDI attacks against SE and our MTD model. Table 1 summarizes the notations used in this paper. Note that we use a superscript $(\cdot)'$ (e.g., $\mathbf{z}'$) to modify a quantity after MTD.

3.1 FDI Attacks against SE

This paper considers the dc power flow model that ignores transmission line resistance and assumes identical bus voltage magnitude. Although the dc model is less accurate than the ac model, the dc power flow analysis is much faster and more robust than the ac power flow analysis. Under the dc model, the system state, denoted by $\mathbf{x} \in \mathbb{R}^n$ (n is the number of buses), contains the voltage phases of all the buses. It is determined by bus power injections and the bus susceptance matrix. Specifically, $\mathbf{p} = \mathbf{B}\mathbf{x}$, where $\mathbf{p} \in \mathbb{R}^n$ 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, $\mathbf{x} = \mathbf{B}^{-1}\mathbf{p}$. Moreover, we have

$$\mathbf{z} = \mathbf{H}\mathbf{x} + \mathbf{e},$$

where $\mathbf{z} \in \mathbb{R}^m$ denotes the vector of the active power flow measurements through a total of m monitored lines and $m \geq n$; $\mathbf{e} \in \mathbb{R}^m$ is the vector of measurement noises; $\mathbf{H} \in \mathbb{R}^{m\times n}$ is the *measurement matrix* with full column rank, i.e., $\text{rank}(\mathbf{H}) = n$. Denote by z_{ij} the measurement of the power flow through the line (i,j) that connects bus i and j, and by e_{ij} the measurement noise contained in z_{ij}. We have $z_{ij} = -b_{ij}(x_i - x_j) + e_{ij}$, where b_{ij} is the line susceptance. Thus, the corresponding row vector of $\mathbf{H}$, denoted by $\mathbf{H}_{ij}$, is given

by

$$\mathbf{H}_{ij} = \big(0 \dots 0 \quad \underbrace{-b_{ij}}_{i\text{th column}} \quad 0 \dots 0 \quad \underbrace{b_{ij}}_{j\text{th column}} \quad 0 \dots 0\big).$$

If the measurement noises are Gaussian, the following estimated system state gives the minimum mean squared error:

$$\hat{\mathbf{x}} = (\mathbf{H}^T\mathbf{W}\mathbf{H})^{-1}\mathbf{H}^T\mathbf{W}\mathbf{z},$$

where $\mathbf{W}$ is a diagonal weight matrix. The BDD of SE detects existence of corrupted measurements by comparing the following 2-norm weighted estimation residual with a threshold τ:

$$r = \left\| \sqrt{\mathbf{W}} \left(\mathbf{z} - \mathbf{H}\hat{\mathbf{x}}\right) \right\|_2,$$

where $\sqrt{\mathbf{W}}$ means applying square root operation to each element of $\mathbf{W}$. Specifically, if $r > \tau$, the corruption is assumed. As the r^2 follows a $\chi^2_{(m-n)}$ distribution, the threshold τ can be set to be

$$\tau = \sqrt{\chi^2_{(m-n),\alpha}},$$

which ensures a false alarm rate of $(1-\alpha)$, where $\chi^2_{(m-n),\alpha}$ represents the 100α%-percentile of the $\chi^2_{(m-n)}$ distribution. The study [6] showed that, in a stealthy FDI attack, the compromised measurement vector $(\mathbf{z}+\mathbf{a})$ will not trigger the BDD if the attack vector $\mathbf{a} \in \mathbb{R}^m$ satisfies

$$\mathbf{a} = \mathbf{H}\mathbf{c},$$

where $\mathbf{c} \in \mathbb{R}^n$ is an arbitrary vector.

3.2 MTD Model

In general, MTD actively introduces controlled changes to increase uncertainty and complexity for attackers. This section describes our MTD model under an adversarial setting. Specifically, the defender actively perturbs the susceptances of D-FACTS-equipped transmission lines, aiming at precluding FDI attacks, while the attacker tries to detect the activation of MTD before launching an FDI attack. Note that we consider an ex-ante scenario in this paper, i.e., there are no ongoing FDI attacks on the time of MTD. Note that, if the MTD is performed frequently, it mostly operates in the ex-ante scenario considered in this paper.

Defender: 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'_{ij}, where $b^{min}_{ij} \le b'_{ij} \le b^{max}_{ij}$, b^{min}_{ij} and b^{max}_{ij} denote the susceptance limits that the D-FACTS device can achieve. We denote by $\mathbf{K}_D$ the set of lines equipped with D-FACTS devices. Similar to [8], the defender assumes that the attacker has obtained the original susceptances of all lines and hence they know the original measurement matrix $\mathbf{H}$, but they do not know the new susceptance values and the new measurement matrix $\mathbf{H'}$ after MTD. If the attacker still crafts the attack vector as $\mathbf{a} = \mathbf{H}\mathbf{c}$, the defender's estimation residual becomes

$$r = \left\| \sqrt{\mathbf{W}} \left((\mathbf{z'} + \mathbf{H}\mathbf{c}) - \mathbf{H'}(\mathbf{H'}^T\mathbf{W}\mathbf{H'})^{-1}\mathbf{H'}^T\mathbf{W}(\mathbf{z'} + \mathbf{H}\mathbf{c}) \right) \right\|_2,$$

where $\mathbf{z'}$ denotes the measurement vector after MTD. As the attacker does not know $\mathbf{H'}$, the above residual is mostly non-zero and the attack will be detected.

Attacker: Before launching an FDI attack, an alert attacker can test the eavesdropped sensor measurements using the BDD based on the original measurement matrix $\mathbf{H}$ that they know. Specifically, the 2-norm weighted estimation residual computed by the attacker using the sensor measurements after MTD (i.e., $\mathbf{z'}$), denoted by $\bar{r}$, is given by

$$\bar{r} = \left\| \sqrt{\mathbf{W}} \left(\mathbf{z'} - \mathbf{H}(\mathbf{H}^T\mathbf{W}\mathbf{H})^{-1}\mathbf{H}^T\mathbf{W}\mathbf{z'} \right) \right\|_2.$$

Similar to the BDD described in Section 3.1, the attacker claims the activation of MTD if $\bar{r}$ exceeds a predefined threshold. To avoid being detected, the attacker should cancel any FDI attack until the new measurement matrix $\mathbf{H'}$ is obtained.

To simplify the discussion and capture the essence of the problem, our analysis in this paper assumes that the sensor measurements are noiseless (i.e., $\mathbf{e} = \mathbf{0}$ and $\mathbf{z}$ consists of the actual power flows) and the loads do not change in a time duration around the activation of the MTD (which are referred to as *steady loads*). Given noiseless measurements, the SE can be simplified as

$$\hat{\mathbf{x}} = (\mathbf{H}^T\mathbf{H})^{-1}\mathbf{H}^T\mathbf{z}.$$

Thus, the presence of attack is assumed if $\mathbf{z} \neq \mathbf{H}\hat{\mathbf{x}}$. Our simulations in Section 5 will evaluate the impact of measurement noises and load changes on the effectiveness of our MTD approach.

4 HIDDEN MTD

In this section, we demonstrate through a case the limitation of the existing MTD approaches that chooses arbitrary susceptance values. Then, we propose a new hidden MTD approach that maintains the power flows and an algorithm to compute the new susceptances of lines.

4.1 MTD's Stealthiness to Attacker

An MTD approach is stealthy to the attacker if the sensor measurements after MTD can bypass the BDD computed by the attacker based on original measurement matrix $\mathbf{H}$. The existing studies [2, 7, 8] mainly focus on an *arbitrary MTD* approach, i.e., the set-points of the D-FACTS devices are arbitrarily chosen for MTD. The activation of such an arbitrary MTD can be easily detected by the attacker. We now use a 3-bus system shown in Fig. 1 to illustrate. 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 $d_1 = 50$ MW, $d_2 = 170$ MW, $d_3 = 280$ MW, $g_1 = 182$ MW, $g_3 = 318$ MW, where d_i denotes the active load on bus i, and g_j 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,

$$\mathbf{H} = \begin{pmatrix} -19.84 & 0 \\ 0 & -17.48 \\ 15.72 & -15.72 \end{pmatrix}.$$

Under the dc model, the system state can be derived as $\mathbf{x} = \binom{-3.10}{-0.81}$. The first row of Table 2 shows the original system state and the power flow measurements. Note that, in the table, Δb_{ij} denotes the line susceptance perturbation in an MTD. 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 $\Delta b_{12} = -1.98$. As a result, after the MTD, the estimation residual computed by the attacker, i.e., $\bar{r}$, is 5.09 and the MTD is not stealthy to the attacker.

Table 2: 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		0	0	0	-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	5.09
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 quantities in MW; line susceptance quantities in p.u.; phase quantities in deg.

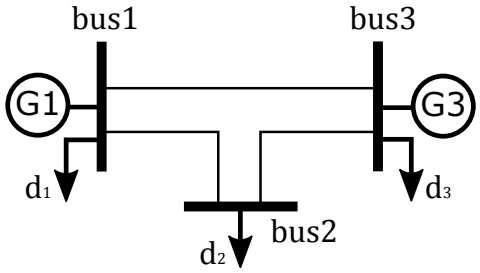

Figure 1: 3-bus system.

4.2 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 4.1. Considering noiseless measurements, a hidden MTD ensures zero estimation residual computed by the attacker, that is,

$$\bar{r} = \|\mathbf{z}' - \mathbf{H}(\mathbf{H}^T\mathbf{H})^{-1}\mathbf{H}^T\mathbf{z}'\|_2 = 0.$$

Definition 4.2. An MTD approach is a PFI-MTD approach if the power flows remain unchanged after the prescribed changes to the susceptance of transmission lines are applied.

Proposition 4.3. *Considering noiseless measurements and steady loads, 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. Since the bus power injections remain unchanged right after the MTD, 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

$$\begin{aligned}\mathbf{B}_i\mathbf{x} &= \sum_{\forall j,(i,j)\in\mathbf{K}} \mathbf{H}_{ij}\mathbf{x} \\ &= \sum_{\forall j,(i,j)\in\mathbf{K}} \mathbf{H}'_{ij}\mathbf{x}'' \\ &= \mathbf{B}'_i\mathbf{x}''.\end{aligned}$$

Thus,

$$\mathbf{p} = \mathbf{B}'\mathbf{x}'' = \mathbf{B}'\mathbf{x}'.$$

As $\mathbf{B}'$ is non-singular, we have $\mathbf{x}'' = \mathbf{x}'$. Thus,

$$\mathbf{z}' = \mathbf{H}'\mathbf{x}' = \mathbf{H}'\mathbf{x}'' = \mathbf{H}\mathbf{x} = \mathbf{z}.$$

That is, 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 $\mathbf{H}\mathbf{x} = \mathbf{H}'\mathbf{x}'$. □

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 2, the MTD is

$$\mathbf{H}' = \begin{pmatrix} -20.89 & 0 \\ 0 & -16.65 \\ 17.19 & -17.19 \end{pmatrix}.$$

There exists $\mathbf{x}'' = \binom{-2.94}{-0.85}$, 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 attacker because $\bar{r} = 0$ as shown in the table.

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

Proposition 4.4. *Considering noiseless measurements and steady loads, 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 attacker, i.e.,

$$\begin{aligned}\bar{r} &= \|\mathbf{z}' - \mathbf{H}(\mathbf{H}^T\mathbf{H})^{-1}\mathbf{H}^T\mathbf{z}'\|_2 \\ &= \|\mathbf{z} - \mathbf{H}(\mathbf{H}^T\mathbf{H})^{-1}\mathbf{H}^T\mathbf{z}\|_2 \\ &= \|\mathbf{z} - \mathbf{H}\mathbf{x}\|_2 \\ &= 0.\end{aligned}$$

Thus, $\mathbf{H}'$ is a hidden MTD.

(*Necessity*) For a hidden MTD $\mathbf{H}'$, we have

$$\bar{r} = \|\mathbf{z}' - \mathbf{H}(\mathbf{H}^T\mathbf{H})^{-1}\mathbf{H}^T\mathbf{z}'\|_2 = 0.$$

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. □

4.3 Construction of Hidden MTD

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

Our approach firstly finds the system state after MTD (i.e., $\mathbf{x}''$). Then, since the power flow should remain unchanged, our approach computes the new line susceptance b'_{ij} using

$$z_{ij} = -b_{ij}(x_i - x_j) = -b'_{ij}(x''_i - x''_j).$$

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:

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

$$\begin{cases} b'_{ij} = b_{ij}\dfrac{x_i - x_j}{x''_i - x''_j}, & \text{if } x_i \ne x_j, (i,j) \in \mathbf{K}; \\ b_{ij}^{min} \le b'_{ij} \le b_{ij}^{max}, & \text{if } x_i = x_j, (i,j) \in \mathbf{K}. \end{cases} \quad (2)$$

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 4.5. *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 $rank(\widetilde{\mathbf{H}}) < rank(\mathbf{H})$.*

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 $\mathbf{x} = (\widetilde{\mathbf{H}}^T\widetilde{\mathbf{H}})^{-1}\widetilde{\mathbf{H}}^T\mathbf{z}$. If there exists a PFI-MTD $\mathbf{H}'$, we have $\mathbf{z}' = \mathbf{z}$. 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, $\mathbf{x}' = (\widetilde{\mathbf{H}}^T\widetilde{\mathbf{H}})^{-1}\widetilde{\mathbf{H}}^T\mathbf{z}'$. 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 $\mathbf{H}'$

```
x̂ = (H^T H)^{-1} H^T z
construct H̃ from the H's rows corresponding to all the transmission lines not in K_D
if rank(H̃) == rank(H) then
    return null
end if
s = rank(H) − rank(H̃)
compute u_l ∈ R^n, 1 ≤ l ≤ s, i.e., the kernel bases of H̃
randomly generate a set of w_l ∈ R, 1 ≤ l ≤ s, such that x'' meets (1), where x'' = x̂ + Σ_{1≤l≤r} w_l · u_l
compute H' using x'' from (2)
return H'
```

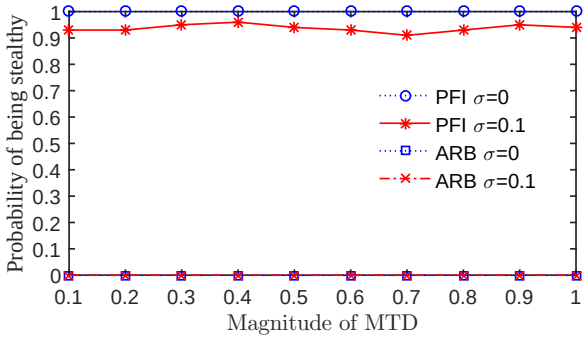

Figure 2: PFI-MTD vs. arbitrary MTD (ARB) and impact of noises.

In fact, the sufficiency proof of Proposition 4.5 encompasses a method to construct the PFI-MTD. Algorithm 1 gives the pseudocode of this method.

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

5 SIMULATIONS

We conduct simulations using MATPOWER to compare our hidden MTD with the arbitrary MTD and evaluate the impact of measurement noises and variable loads. The simulations are based on the IEEE 14-bus system model. We use the probability for MTD to be stealthy to the attacker and attack detection probability as the evaluation metrics.

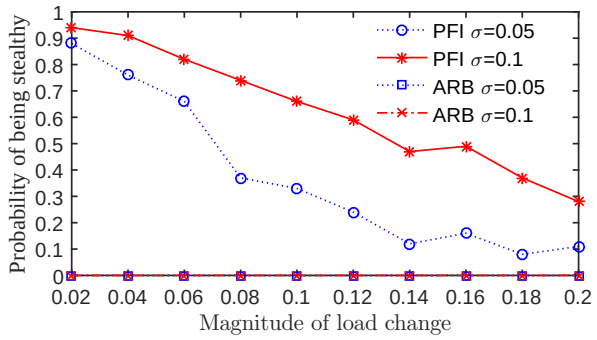

Figure 3: Impact of variable loads and noises on PFI-MTD.

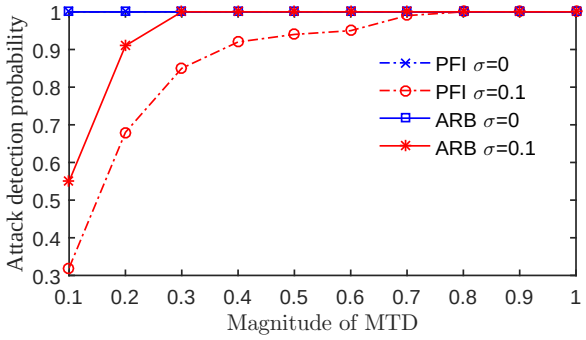

Figure 4: Attack detection probability of PFI-MTD and arbitrary MTD.

Fig. 2 shows the probability for MTD to be stealthy to the attacker under different MTD magnitudes and steady loads. For an MTD magnitude of q, we set $b_{ij}^{min} = (1+q) \cdot b_{ij}$ and $b_{ij}^{max} = b_{ij}/(1+q)$. 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, however. 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 attacker, which is consistent with our analysis. For the noisy case (i.e., $\sigma = 0.1$), 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 attacker (with a probability of less than 10% as shown in Fig. 2). The arbitrary MTD can be always detected by the attacker.

Fig. 3 shows the probability for PFI-MTD to be stealthy to the attacker under different load change magnitudes. For a load change magnitude q, the load when the attacker tries to detect MTD is randomly selected between $1/(1+q)$ and $(1+q)$ 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 attacker. 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 attacker's capability in detecting MTD. The arbitrary MTD can be always detected by the attacker.

Fig. 4 shows the MTD's attack detection probability under different MTD magnitudes. The magnitude of load change is fixed at 0.1. 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. 4 suggests that, to implement the hidden MTD for stealthiness to attacker, more line susceptance adjusting capability is needed to achieve a certain level of attack detection probability, compared with the arbitrary MTD.

6 CONCLUSION

This paper shows that the activation of the existing arbitrary MTD against FDI attacks on smart grids can be easily detected by the attacker. To improve the stealthiness of MTD, we propose a hidden MTD approach that maintains the power flows and develop an algorithm to construct the hidden MTD. Simulations show the effectiveness of the hidden MTD approach under realistic settings.

ACKNOWLEDGMENTS

This research was funded by a Start-up Grant at Nanyang Technological University, National Key Research and Development Program of China (2016YFB0800202), National Natural Science Foundation of China (U1301254), and Fok Ying-Tong Education Foundation (151067).

REFERENCES

[1] Rakesh B Bobba, Katherine M Rogers, Qiyan Wang, Himanshu Khurana, Klara Nahrstedt, and Thomas J Overbye. 2010. Detecting false data injection attacks on dc state estimation. In *Workshop on Secure Control Systems*.

[2] Katherine R Davis, Kate L Morrow, Rakesh Bobba, and Erich Heine. 2012. Power flow cyber attacks and perturbation-based defense. In *SmartGridComm*.

[3] Annarita Giani, Eilyan Bitar, Manuel Garcia, Miles McQueen, Pramod Khargonekar, and Kameshwar Poolla. 2011. Smart grid data integrity attacks: characterizations and countermeasures. In *SmartGridComm*.

[4] Yi Huang, Husheng Li, Kristy A Campbell, and Zhu Han. 2011. Defending false data injection attack on smart grid network using adaptive cusum test. In *Annual Conf. Inf. Sci. & Syst.*

[5] Lanchao Liu, Mohammad Esmalifalak, Qifeng Ding, Valentine A Emesih, and Zhu Han. 2014. Detecting false data injection attacks on power grid by sparse optimization. *IEEE Trans. Smart Grid* 5, 2 (2014).

[6] Yao Liu, Peng Ning, and Michael K Reiter. 2011. False data injection attacks against state estimation in electric power grids. *ACM Trans. Info. & Syst. Security* 14, 1 (2011).

[7] Kate L Morrow, Erich Heine, Katherine M Rogers, Rakesh B Bobba, and Thomas J Overbye. 2012. Topology perturbation for detecting malicious data injection. In *Intl. Conf. Syst. Sci.*

[8] Mohammad Ashiqur Rahman, Ehab Al-Shaer, and Rakesh B Bobba. 2014. Moving target defense for hardening the security of the power system state estimation. In *ACM Workshop on Moving Target Defense*.

[9] Xinyu Yang, Jie Lin, Wei Yu, Paul-Marie Moulema, Xinwen Fu, and Wei Zhao. 2015. A novel en-route filtering scheme against false data injection attacks in cyber-physical networked systems. *IEEE Trans. Comput.* 64, 1 (2015).