# Analysis of Moving Target Defense in Unbalanced and Multiphase Distribution Systems Considering Voltage Stability

Mengxiang Liu, Chengcheng Zhao, Zhenyong Zhang, Ruilong Deng, and Peng Cheng

*Abstract*—**Moving Target Defense (MTD) is a new technology to defend against the false data injection attack (FDIA) on distribution system state estimation (DSSE). It works by proactively perturbing the branch reactance. However, due to the challenges induced by the nonlinear dynamics and the coupling phases in the three-phase AC DSSE model, the analysis on the effectiveness and hiddenness of MTD, which are two essential performance metrics, has not yet been conducted. In this paper, we attempt to optimize the effectiveness and hiddenness of MTD while considering voltage stability. Firstly, we quantify the two metrics with approximated measurement residuals. Based on the quantified metrics, we formulate an optimization problem to maximize the effectiveness with guaranteed hiddenness and ensure voltage stability by minimizing the voltage variation induced by MTD. The original problem is transformed to a polynomial optimization problem based on the observation that the alteration of the *projection matrix* caused by reactance perturbation is neglectable, such that the near-optimal result can be obtained. Finally, extensive simulations are conducted on the IEEE 13-bus test feeder to evaluate the performance of the proposed MTD.**

*Index Terms*—**False data injection attack, unbalanced and multiphase distribution system, hidden moving target defense, reactance perturbation**

## I. Introduction

With the popularity of information and communications technology (ICT) in power distribution systems (PDSs), it is promising for the control center to achieve real-time monitoring and control of system states such that the efficiency, safety, and reliability would be significantly enhanced [1]. Nevertheless, the wide adoption of ICT also exposes PDSs to the threat of cyberattacks [2]. In 2015, the Ukrainian electricity distribution companies suffered a well-planned cyberattack, which firstly switched substations off and then disabled information technology infrastructure components, causing approximately 225,000 customers across various areas to lose power for a period from 1 to 6 hours [3]. In 2019, the government of Venezuela repeatedly claimed that the widespread outage of power was caused by a series of coordinated cyberattacks [4], affecting the electricity sectors in Venezuela in most of its 23 states. Thus, it is important to model the cyberattack and design defend strategies to ensure the cybersecurity of PDSs.

The false data injection attack (FDIA) has been recognized as one of the most threating issues in PDSs [5]. It can bypass the bad data detection (BDD) and mislead the distribution system state estimation (DSSE) with an arbitrary bias, once the attacker has certain knowledge of PDSs [6]. Recently, the technology of *moving target defense (MTD)*, which is originated from the field of computer science and seeks to enhance the security and resilience of an application through increasing the *diversity* of software and network paths, has been shown to have the potential of thwarting FDIAs in PDSs [7], [8]. The philosophy behind MTD is to proactively perturb branch reactances such that the previously inferred branch parameters by the attacker are outdated, with which the constructed FDIA may be detected by BDD. The MTD can be implemented through the real-world device, named as *SmartValve*, which has been widely deployed in existing power systems to realize the active control of power flow, by receiving real-time commands from the control center based on encrypted secure channels [9]. Generally, the two essential metrics to evaluate the performance of MTD are the effectiveness in terms of attack detection and the hiddenness to cheat attackers [10], [11]. If the attacker can perceive the existence of MTD, then she/he would not rashly launch FDIAs, which could invalidate the effectiveness of MTD. Hence, the two metrics are closely related and indispensable.

Numerous studies have been devoted to the design of MTD in both PDSs and power transmission systems (PTSs). In PDSs, Cui *et al.* [7] designed a deeply hidden MTD to elaborately hide both the self and mutual reactance of each phase at the transmission line in unbalanced PDSs, while the joint optimization of effectiveness and hiddenness has not been investigated. Liu *et al.* [8] introduced a hidden MTD by minimizing the system loss and line power flow differences before and after MTD, yet only the balanced and symmetrical PDSs are considered. In PTSs, the original three-phase AC TSSE model can be simplified to the single-phase DC (linear) TSSE model, given the symmetrical branch parameters between phases and the negligible branch resistance. In the single-phase DC TSSE model, the effectiveness of MTD is measured via the

This work was supported in part by Science and Technology Innovation 2030 Program under Grant 2018AAA0101605, in part by the National Natural Science Foundation of China under Grants 62073285, 62061130220, 61833015, 61903328, in part by the Zhejiang Provincial Natural Science Foundation under Grant LZ21F020006, in part by the Fundamental Research Funds for the Central Universities (Zhejiang University NGICS Platform), and in part by the GZU cultivation project of NSFC (No. [2020]80).

Mengxiang Liu, Chengcheng Zhao, Ruilong Deng, and Peng Cheng are with State Key Lab. of Industrial Control Technology, College of Control Science and Engineering, Zhejiang University, Hangzhou, China (e-mails: {lmx329, chengchengzhao, dengruilong, lunarheart}@zju.edu.cn). Zhenyong Zhang is with State Key Lab. of Public Big Data, College of Computer Science and Technology, Guizhou University, Guiyang, China (e-mail: zyzhangnew@gmail.com).

rank of the composite matrix, which comprises the Jacobian matrices before and after MTD. Higher rank typically means stronger effectiveness. While the hiddenness is maintained by keeping the power flows before and after MTD invariant, which can be achieved by solving a set of linear equations. In terms of effectiveness, Zhang *et al.* [10] thoroughly explored the necessary conditions for the composite matrix possessing full column rank (i.e., complete effectiveness) and designed a heuristic algorithm to maximize the rank of composite matrix. Liu *et al.* [12] proposed the MTD under which the attack detection and identification probability is maximized and the system loss is minimized. As for the hiddenness of MTD, Zhang *et al.* [11] proved that by protecting a basic set of measurements, the hidden MTD with *complete effectiveness* can be achieved regardless of the variation of power flow. Liu *et al.* [13] derived a sufficient condition on the placement of *SmartValve* devices for the enhanced hidden MTD.

Although the design of MTD has been comprehensively investigated in the single-phase DC TSSE model, the developed methods are not applicable to the three-phase AC DSSE model due to the following three limitations: 1) It is difficult to use the rank of composite matrix for the analysis of MTD effectiveness in the AC model as the linearized Jacobian matrix cannot be decomposed as perfectly as that in the DC model [10]; 2) Perturbing branch reactances only is not enough to make the *complex* power flows invariant due to the existence of branch resistances, charging susceptances, and tap changer transformers [14], indicating that the hidden MTD cannot be achieved by solving a set of linear equations; 3) The coupling phases make the branch admittance matrix (i.e., the inverse of branch impedance matrix) under MTD implicit, hence hindering the explicit analysis of linearized Jacobian matrices. Therefore, it is of great importance to conduct exhaustive analysis on the effectiveness and hiddenness for a practical three-phase AC DSSE model. In this paper, we attempt to quantify the effectiveness and hiddenness utilizing measurement residuals and jointly optimize the two quantified metrics considering voltage stability. The contributions are listed as follows:

- We quantify the effectiveness and hiddenness with approximated measurement residuals, which are derived by applying sensitivity analysis to the nonlinear SE problem. Here the implicit sensitivity of branch admittance matrix to reactance, resulted from the coupling phases, is represented as an explicit function of impedance matrix.
- Based on the quantified metrics, we formulate the optimization problem for MTD to jointly optimize the effectiveness and hiddenness considering voltage stability. To obtain the near-optimal result, the original problem is transformed to a polynomial optimization problem based on the observation that the *projection* matrix is almost invariant under reactance perturbation.
- Extensive simulations are conducted on the IEEE 13-bus test feeder to evaluate the accuracy of the derived residual approximations and the effectiveness and hiddenness of the proposed MTD.

The remainder of this paper is organized as follows. Section II introduces the three-phase and unbalanced PDS model, the DSSE model, the BDD model, and the attack model. Section III presents the MTD model and our problems of interest. Section IV illustrates the derived residual approximations and the designed MTD. Section V demonstrates the simulation results and Section VI concludes this paper.

## II. System Model

In this section, we introduce the modeling of PDS via the bus admittance matrix (Y-Bus) [15], the nodal voltage based DSSE [16], the BDD model, and the attack model. Throughout this paper, we utilize $(\vec{\cdot}) \in \mathbb{C}$ to denote complex variables, $(\cdot) \in \mathbb{R}$ to denote real variables, and $(\vec{\cdot})^*$ to denote conjugate variables, respectively. Subscripts $_{\text{re}}$ and $_{\text{im}}$ signify the real and image parts of complex variables, respectively. Moreover, $|\cdot|$ denotes the element-by-element absolute value of a real vector or matrix, and $||\cdot||_2$ signifies the 2-norm of a real vector or matrix. The terms of bus and node, and edge and branch are used interchangeably.

### A. Three-Phase and Unbalanced PDS Model

The PDS can be mathematically described by an undirected graph $(\mathcal{N}, \mathcal{E})$, where $\mathcal{N} \triangleq \{1, \cdots, N\} \cup \{S\}$ denotes the set of nodes and includes loads and shunt capacitors, and $\mathcal{E} \triangleq \{(n,m)\} \subseteq \mathcal{N} \times \mathcal{N}$ represents the set of edges comprising transmission lines, step-voltage-regulators and transformers, which are referred as series elements. Let $\boldsymbol{\psi}_{nm}$ denote the set of available phases corresponding to edge $(n,m)$. The set of nodes neighboring to $n$ is denoted by $\mathcal{N}_n = \{j|(n,j) \in \mathcal{E}\}$. The model of edge $(n,m)$ is defined as

$$\begin{aligned} \vec{\boldsymbol{I}}_{nm} &= \vec{Y}^{(n)}_{nm}\vec{\boldsymbol{V}}_n - \vec{Y}^{(m)}_{nm}\vec{\boldsymbol{V}}_m, \\ \vec{\boldsymbol{I}}_{mn} &= \vec{Y}^{(m)}_{mn}\vec{\boldsymbol{V}}_m - \vec{Y}^{(n)}_{mn}\vec{\boldsymbol{V}}_n \end{aligned} \tag{1}$$

where $\vec{Y}^{(n)}_{nm}, \vec{Y}^{(m)}_{nm}, \vec{Y}^{(m)}_{mn}$, and $\vec{Y}^{(n)}_{mn}$ are all $3 \times 3$ complex matrices determined by the model of the series element, and their rows and columns are set to zero for missing phases. $\vec{\boldsymbol{I}}_{nm}$ denotes the complex current flow of edge $(n,m)$, and $\vec{\boldsymbol{V}}_n$ represents the complex voltage of node $n$.

### B. DSSE

The DSSE is crucial as it enables the control center to achieve real-time monitoring of system states with meter measurements. The measurements utilized in the DSSE typically include real-time, pseudo, and virtual measurements [17]. In particular, real-time voltage, current, and power measurements are collected from phasor measurement units, intelligent electronic devices and advanced metering infrastructure systems. Pseudo power injection measurements are generated at the control center based on historical load consumption profile to relieve the measurement paucity in the DSSE. Virtual measurements are defined as the information provided by the buses of zero injections, and thus are also treated as equality constraints in the DSSE [18]. The DSSE is to determine the system state with the acquired measurements, which comprises the set of complex bus voltages in rectangular forms, i.e., $\boldsymbol{x} = [\boldsymbol{V}_{\mathcal{N},\text{re}}^{\text{T}}, \boldsymbol{V}_{\mathcal{N},\text{im}}^{\text{T}}]^{\text{T}} \in \mathbb{R}^{6*(N+1)}$. Once $\boldsymbol{x}$ is fixed, then the operating point of PDS can be uniquely determined.

In this paper, we focus on the overdetermined DSSE problem, where the sufficient number of measurements can be obtained to make the PDS observable. Specifically, the obtained measurements comprise branch current flow $\vec{\boldsymbol{I}}_{\text{bra}}$ (derived from (1)), branch power plow $\vec{\boldsymbol{S}}_{\text{bra}}$, bus power injection $\vec{\boldsymbol{S}}_{\text{bus}}$, complex bus voltage $\vec{\boldsymbol{V}}_{\text{bus}}$, and bus voltage magnitude $\boldsymbol{V}_{\text{bus,mag}}$. Here the power measurements are elaborated as

$$\vec{\boldsymbol{S}}_{nm} = \vec{\boldsymbol{V}}_n \times \left[\vec{Y}_{nm}^{(n)}\vec{\boldsymbol{V}}_n - \vec{Y}_{nm}^{(m)}\vec{\boldsymbol{V}}_m\right], (n,m) \in \mathcal{E}, \quad (2)$$

$$\vec{\boldsymbol{S}}_n = \vec{\boldsymbol{V}}_n \times \sum_{j \in \mathcal{N}_n} \left[\vec{Y}_{nj}^{(n)}\vec{\boldsymbol{V}}_n - \vec{Y}_{nj}^{(j)}\vec{\boldsymbol{V}}_j\right], n \in \mathcal{N}, \quad (3)$$

and the voltage magnitude of node $n \in \mathcal{N}$ is $\boldsymbol{V}_{n,\text{mag}} = \sqrt{\boldsymbol{V}_{n,\text{re}}^2 + \boldsymbol{V}_{m,\text{im}}^2}$, where the mathematical operations are implemented by element. Let $\boldsymbol{z}_{\text{comp}} = [\vec{\boldsymbol{I}}_{\text{bra}}; \vec{\boldsymbol{S}}_{\text{bra}}; \vec{\boldsymbol{S}}_{\text{bus}}; \vec{\boldsymbol{V}}_{\text{bus}}; \boldsymbol{V}_{\text{bus,mag}}]$, and then the real measurement vector can be constructed as $\boldsymbol{z} = [\boldsymbol{z}_{\text{comp,re}}; \boldsymbol{z}_{\text{comp,im}}] \in \mathbb{R}^m$. We note that subscripts $_{\text{bra}}$ and $_{\text{bus}}$ do not mean measuring all branches and buses. The relations between $\boldsymbol{z}$ and $\boldsymbol{x}$ obey

$$\boldsymbol{z} = \boldsymbol{h}(\boldsymbol{x}, \boldsymbol{b}) + \boldsymbol{e}, \quad (4)$$

where $\boldsymbol{h}(\cdot)$ denotes the measurement function vector constructed from (1)-(3), vector $\boldsymbol{b} \in \mathbb{R}^l$ collects the parameters of series elements (including transmission lines, step-voltage-regulators, and transformers), and $\boldsymbol{e}$ represents measurement noises following normal distributions with zero mean and variances $\sigma_i^2, 1 \leq i \leq m$. The estimated state $\boldsymbol{x}^*$ that best fits $\boldsymbol{z}$ is viewed as the solution of the following nonlinear weighted least squares (NWLS) problem:

$$\boldsymbol{x}^* \triangleq \arg\min_{\boldsymbol{x}} J(\boldsymbol{x}, \boldsymbol{z}, \boldsymbol{b}) = \left[\boldsymbol{z} - \boldsymbol{h}(\boldsymbol{x}, \boldsymbol{b})\right]^{\text{T}} W \left[\boldsymbol{z} - \boldsymbol{h}(\boldsymbol{x}, \boldsymbol{b})\right], \quad (5)$$

where the diagonal matrix $W$ weights the measurements according to the reciprocals of noise variances, namely $W = \text{diag}([\sigma_1^{-2}, \cdots, \sigma_m^{-2}])^{\text{T}}$. The iterative Gauss Newton method is adopted to approach $\boldsymbol{x}^*$. At flat-start, the real and image parts of bus voltages are set to $[1, -0.5, -0.5, 0, \frac{\sqrt{3}}{2}, -\frac{\sqrt{3}}{2}]^{\text{T}}$p.u. For the $k$-th iteration, (6) is calculated to compute the forward step $\Delta\boldsymbol{x}^{(k)}$, i.e.,

$$\Delta\boldsymbol{x}^{(k)} \triangleq (H_{\boldsymbol{x}^{(k)}}^{\text{T}} W H_{\boldsymbol{x}^{(k)}})^{-1} H_{\boldsymbol{x}^{(k)}}^{\text{T}} W \left[\boldsymbol{z} - \boldsymbol{h}(\boldsymbol{x}^{(k)})\right], \quad (6)$$

with which the system state is updated as $\boldsymbol{x}^{(k+1)} = \boldsymbol{x}^{(k)} + \Delta\boldsymbol{x}^{(k)}$. Here $H_{\boldsymbol{x}} \triangleq \partial\boldsymbol{h}(\boldsymbol{x}, \boldsymbol{b})/\partial\boldsymbol{x}$ denotes the Jacobian matrix. The iteration is terminated until $||\Delta\boldsymbol{x}^{(k)}||_\infty$ and $|J(\boldsymbol{x}^{(k+1)}) - J(\boldsymbol{x}^{(k)})|$ are small enough [19].

### C. BDD Model

Based on the DSSE, the residual-based BDD is employed to perceive and filter out possible bad data in measurements caused by link failures or malicious cyberattacks. The calculation of residual is formally described by $r \triangleq ||\boldsymbol{r}||_2 = ||\boldsymbol{z} - \boldsymbol{h}(\boldsymbol{x}^*)||_2$. To tolerate the impact of measurement noises, a predetermined threshold $\tau > 0$ is given through a hypothesis test with a significance level $\alpha$. The measurements will be regarded as tainted if $r > \tau$. Otherwise, $\boldsymbol{z}$ will be viewed as normal ones. Note that $r > \tau$ detects the bad data with the false alarm probability $\alpha$ when all measurement noises follow normal distributions.

### D. Attack Model

In this paper, we consider that the attacker has the following capabilities:

- The attacker can infer model knowledge (network topology and branch parameters) of PDSs through topology leaking attacks or subspace attacks [20], [21].
- The attacker can easily approximate system states $\boldsymbol{x}^{\text{appr}}$ based on power flow/injection measurements [5].
- The attacker can eavesdrop and tamper with measurements through spoofed wireless signals, intruded shared communications, or spoofed substation field devices [22].

To guarantee the stealthiness of FDIAs, the injected attack vector should conform the underlying physical model and is constructed as $\boldsymbol{a} \triangleq \boldsymbol{h}(\boldsymbol{x}^{\text{appr}} + \boldsymbol{c}) - \boldsymbol{h}(\boldsymbol{x}^{\text{appr}})$, where $\boldsymbol{c} \in \mathbb{R}^n$ denotes the state bias injected by the attacker.

## III. MTD in Unbalanced and MultiPhase PDSs

The basic principle behind MTD is to proactively perturb branch reactances such that the well-designed FDIAs may be exposed to BDD, which can be potentially achieved through revolutionary power electronics based products, named as *SmartValve*, designed by the Smart Wire Incorporation. *SmartValve* is essentially a Static Synchronous Series Compensator (SSSC), injecting a leading or lagging voltage in quadrature with the line current and providing the *functionality* of a series capacitor or series reactor, respectively [9]. Fig. 1 depicts a three-phase transmission line equipped with *SmartValve* devices, where the branch impedance $\vec{Z}_{nm}$ is perturbed by a diagonal complex matrix $j\Delta X_{nm} \in \mathbb{C}^{3\times3}$. The rows and columns in $\Delta X_{nm}$ corresponding to missing phases are set to zeros. Since the impedance of branch is actually not impacted, the mutual impedance between phases in three-phase PDSs cannot be perturbed by the *SmartValve* device. For clarity, we utilize symbols with subscript $_{\text{MTD}}$ to denote quantities after MTD, while those without $_{\text{MTD}}$ represent quantities before MTD. Hence, the matrices involved in the edge model $(n,m)$ after MTD are

$$\begin{aligned} \vec{Y}_{nm,\text{MTD}}^{(n)} &= \vec{Y}_{mn,\text{MTD}}^{(m)} = \frac{1}{2}\vec{Y}_{nm}^{s} + (\vec{Z}_{nm} + j\Delta X_{nm})^{-1} \\ \vec{Y}_{nm,\text{MTD}}^{(m)} &= \vec{Y}_{mn,\text{MTD}}^{(n)} = (\vec{Z}_{nm} + j\Delta X_{nm})^{-1}. \end{aligned} \quad (7)$$

The above operations are limited to rows and columns included in $\boldsymbol{\psi}_{nm}$ to make the branch impedance matrix invertible. Depending on the number of installed *SmartValve* devices, the reactance perturbation is bounded by

$$\Delta\underline{X}_{nm} \leq \Delta X_{nm} \leq \Delta\overline{X}_{nm}. \quad (8)$$

Further, integrated with ICT, *SmartValve* devices can receive real-time perturbation commands from the control center, and the SHA-256 encryption algorithm is adopted to ensure the integrity of communicated data [23].

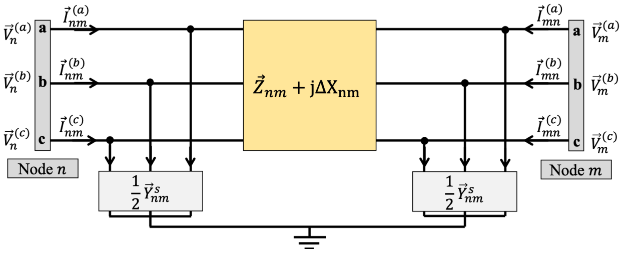

Fig. 1. Three-phase transmission line equipped with *SmartValve* devices.

### A. *Effectiveness and Hiddenness of MTD*

The effectiveness of MTD measures the capability in detecting FDIAs, while the hiddenness describes the ability to realizing concealment from attackers. A well-designed MTD strategy should possess strong effectiveness and hiddenness simultaneously, which requires a systematical method as non-trivial trade-off exists between the two metrics according to [14]. In this paper, we quantify the effectiveness and hiddenness of MTD in unbalanced and multiphase PDSs utilizing measurement residuals, which are elaborated as follows.

*1) Effectiveness:* The effectiveness is directly related to the residual under FDIAs, which is denoted by $r_{\text{sys}}$, and larger $r_{\text{sys}}$ typically means stronger effectiveness. The calculation of $r_{\text{sys}}$ is detailed as follows. By solving the WLS problem (5) with tainted measurements $\boldsymbol{z}_a \triangleq \boldsymbol{z}_{\text{MTD}} + \boldsymbol{a}$ and branch parameters after MTD, i.e., $\boldsymbol{b}_{\text{MTD}}$, the system operator obtains $\boldsymbol{x}_{\text{sys}}^*$, which is applied to BDD and the residual is calculated as $r_{\text{sys}} \triangleq ||\boldsymbol{r}_{\text{sys}}||_2 = ||\boldsymbol{z}_a - \boldsymbol{h}(\boldsymbol{x}_{\text{sys}}^*, \boldsymbol{b}_{\text{MTD}})||_2$.

*2) Hiddenness:* Before launching FDIAs, the attacker will implement a self-check process to evaluate the consistency between the inferred model knowledge and obtained measurements, which can be simply described by feeding $\boldsymbol{z}$ into BDD and a residual $r_{\text{att}}$ is computed. Only if $r_{\text{att}}$ is small enough, then the FDIA will be launched. Otherwise, the inferring process will be restarted[1]. Hence, smaller $r_{\text{att}}$ means stronger hiddenness. The calculation of $r_{\text{att}}$ is detailed as follows. With normal measurements $\boldsymbol{z}_{\text{MTD}}$ and outdated branch parameters $\boldsymbol{b}$, the attacker solves (5) and obtains $\boldsymbol{x}_{\text{att}}^*$, and the residual is calculated as $r_{\text{att}} \triangleq ||\boldsymbol{r}_{\text{att}}||_2 = ||\boldsymbol{z}_{\text{MTD}} - \boldsymbol{h}(\boldsymbol{x}_{\text{att}}^*, \boldsymbol{b})||_2$.

### B. *Problems of Interest*

The analysis of effectiveness and hiddenness is still challenging due to the implicit expressions of $r_{\text{sys}}$ and $r_{\text{att}}$. In this paper, we derive analytical approximations of the two residuals and then present a comprehensive MTD design method considering voltage stability in unbalanced and multiphase PDSs. To simplify the analysis, we focus on the noiseless setting in our main results and simulation results are demonstrated to evaluate the impact of noises.

## IV. Main Results

In this section, we derive analytical residual approximations of $\boldsymbol{r}_{\text{sys}}$ and $\boldsymbol{r}_{\text{att}}$ based on sensitivity analysis, and present a method to jointly optimize the effectiveness and hiddenness of MTD with voltage stability being maintained.

### A. *Residual Approximation*

We use sensitivity analysis [24] to investigate ”how” and ”how much” variations of measurements will impact the estimated system state and the corresponding residual in (5).

***Lemma 1:*** Let $\Phi^* = (\boldsymbol{x}^*, \boldsymbol{b})$ denotes the optimal point. when $J(\Phi^*)$ approaches zero infinitely, then sensitivities $\frac{\partial \boldsymbol{x}}{\partial \boldsymbol{b}}$ and $\frac{\partial \boldsymbol{r}}{\partial \boldsymbol{z}}$ can be calculated as

$$\frac{\partial \boldsymbol{x}}{\partial \boldsymbol{b}}|_{\Phi^*} \triangleq -\big[(H_{\boldsymbol{x}}^*)^{\mathrm{T}} H_{\boldsymbol{x}}^*\big]^{-1}(H_{\boldsymbol{x}}^*)^{\mathrm{T}} H_{\boldsymbol{b}}^*, \tag{9}$$

$$\frac{\partial \boldsymbol{r}}{\partial \boldsymbol{z}}|_{\Phi^*} \triangleq I - H_{\boldsymbol{x}}^*\big[(H_{\boldsymbol{x}}^*)^{\mathrm{T}} H_{\boldsymbol{x}}^*\big]^{-1}(H_{\boldsymbol{x}}^*)^{\mathrm{T}}, \tag{10}$$

where $H_{\boldsymbol{x}}^*$ denotes the Jacobian matrix at point $(\boldsymbol{x}^*, \boldsymbol{b})$ and $H_{\boldsymbol{b}}^* = \partial \boldsymbol{h}(\boldsymbol{x}^*, \boldsymbol{b})/\partial \boldsymbol{b}$. Here $H_{\boldsymbol{x}}^*(:, \boldsymbol{\psi}_{\text{bus}})$ and $H_{\boldsymbol{b}}^*(:, \boldsymbol{\psi}_{\text{bra}})$ are simplified as $H_{\boldsymbol{x}}^*$ and $H_{\boldsymbol{b}}^*$ respectively, with $\boldsymbol{\psi}_{\mathcal{N}}$ and $\boldsymbol{\psi}_{\mathcal{E}}$ being the sets of available bus and branch phases.

***Proof:*** The proof is omitted due to the space limitation. ■

***Remark 1:*** We use a small trick to handle the implicit sensitivity of branch admittance matrix to reactance when calculating $H_{\boldsymbol{b}}^*$. That is, for branch admittance matrix $\vec{Y}_{nm} \in \mathbb{C}^{3\times 3}$, its sensitivity to the self-reactance of phase A $X_{nm}^{(1,1)}$, i.e., the imaginary part of the first diagonal element in $\vec{Z}_{nm}$, can be expressed as

$$\frac{\partial \vec{Y}_{nm}}{\partial X_{nm}^{(1,1)}} = -\vec{Z}_{nm}^{-1} \times \frac{\partial \vec{Z}_{nm}}{\partial X_{nm}^{(1,1)}} \times \vec{Z}_{nm}^{-1}, \tag{11}$$

which makes the calculation of $H_{\boldsymbol{b}}^*$ explicit.

*1) Approximation of $\boldsymbol{r}_{sys}$:* Intuitively, the effectiveness of MTD is to make the constructed $\boldsymbol{a}$ *inconsistent* with the current branch parameters $\boldsymbol{b}_{\text{MTD}}$, under which $r_{\text{sys}}$ is likely to be enlarged. The *inconsistency* can be captured by the following measurement error

$$\begin{aligned}\Delta \boldsymbol{z}_{\text{sys}} &\triangleq \boldsymbol{z}_{\text{MTD}} + \boldsymbol{a} - \boldsymbol{h}(\boldsymbol{x}_{\text{MTD}}^* + \boldsymbol{c}, \boldsymbol{b}_{\text{MTD}}) \\ &\approx -\boldsymbol{h}(\boldsymbol{x}_{\text{MTD}}^* + \boldsymbol{c}, \boldsymbol{b}_{\text{MTD}}) + \boldsymbol{h}(\boldsymbol{x}_{\text{MTD}}^* + \boldsymbol{c}, \boldsymbol{b}) + \\ &\quad \boldsymbol{h}(\boldsymbol{x}_{\text{MTD}}^*, \boldsymbol{b}_{\text{MTD}}) - \boldsymbol{h}(\boldsymbol{x}_{\text{MTD}}^*, \boldsymbol{b}),\end{aligned} \tag{12}$$

where the approximated system state $\boldsymbol{x}^{\text{appr}}$ involved in $\boldsymbol{a}$ can be very close to $\boldsymbol{x}_{\text{MTD}}^*$ [5]. Further, the form of (12) can be viewed as the increment of function $\boldsymbol{h}(\boldsymbol{x}_{\text{MTD}}^*, \boldsymbol{b}) - \boldsymbol{h}(\boldsymbol{x}_{\text{MTD}}^* + \boldsymbol{c}, \boldsymbol{b})$ caused by $\Delta \boldsymbol{b} = \boldsymbol{b}_{\text{MTD}} - \boldsymbol{b}$ and is approximated through sensitivity as

$$\Delta \boldsymbol{z}_{\text{sys}} \approx \Delta \boldsymbol{z}_{\text{sys}}^{\text{appr}} \triangleq (H_{\boldsymbol{b}}^{\text{MTD}*} - H_{\boldsymbol{b}}^{\text{MTDc}*}) \times \Delta \boldsymbol{b}, \tag{13}$$

where $H_{\boldsymbol{b}}^{\text{MTD}*} = \partial \boldsymbol{h}(\boldsymbol{x}_{\text{MTD}}^*, \boldsymbol{b})/\partial \boldsymbol{b}$ and $H_{\boldsymbol{b}}^{\text{MTDc}*} = \partial \boldsymbol{h}(\boldsymbol{x}_{\text{MTD}}^* + \boldsymbol{c}, \boldsymbol{b})/\partial \boldsymbol{b}$. We define the point after MTD and FDIA as $\Phi_{\text{MTDa}}^* = (\boldsymbol{x}_{\text{MTD}}^* + \boldsymbol{c}, \boldsymbol{b}_{\text{MTD}})$, of which the residual $\boldsymbol{r}_{\text{sys}}$ is approximated based on (10), (12), and (13) as

$$\boldsymbol{r}_{\text{sys}} \approx \boldsymbol{r}_{\text{sys}}^{\text{appr}} \triangleq \frac{\partial \boldsymbol{r}}{\partial \boldsymbol{z}}|_{\Phi_{\text{MTDa}}^*} \times \Delta \boldsymbol{z}_{\text{sys}}^{\text{appr}}. \tag{14}$$

[1] The perturbation period should be designed smaller than the time required for the inferring process to invalid the inferred branch parameters.

*2) Approximation of $\boldsymbol{r}_{att}$:* Similarly, from the perspective of attackers, the *inconsistency* caused by MTD can be measured by the measurement alteration $\Delta \boldsymbol{z}_{\text{att}} \triangleq \boldsymbol{z}_{\text{MTD}} - \boldsymbol{z} = \boldsymbol{h}(\boldsymbol{x}_{\text{MTD}}^*, \boldsymbol{b}_{\text{MTD}}) - \boldsymbol{h}(\boldsymbol{x}^*, \boldsymbol{b})$, which is approximated through sensitivity as

$$\begin{aligned}\Delta \boldsymbol{z}_{\text{att}} \approx \Delta \boldsymbol{z}_{\text{att}}^{\text{appr}} &\triangleq H_{\boldsymbol{x}}^* \times \frac{\partial \boldsymbol{x}}{\partial \boldsymbol{b}}|_{\Phi^*} \times \Delta \boldsymbol{b} + H_{\boldsymbol{b}}^* \times \Delta \boldsymbol{b} \\ &= P_{\boldsymbol{x}}^* \times H_{\boldsymbol{b}}^* \times \Delta \boldsymbol{b}, \qquad (15)\end{aligned}$$

where $P_{\boldsymbol{x}}^* = \left[I - H_{\boldsymbol{x}}^* \left[(H_{\boldsymbol{x}}^*)^{\text{T}} H_{\boldsymbol{x}}^*\right]^{-1} (H_{\boldsymbol{x}}^*)^{\text{T}}\right]$ and the state deviation $\boldsymbol{x}_{\text{MTD}}^* - \boldsymbol{x}^*$ is approximated utilizing (9). Finally, based on (10) and (15), $\boldsymbol{r}_{\text{att}}$ is approximated at $\Phi^*$ as

$$\boldsymbol{r}_{\text{att}} \approx \boldsymbol{r}_{\text{att}}^{\text{appr}} \triangleq \Delta \boldsymbol{z}_{\text{att}}^{\text{appr}}, \qquad (16)$$

indicating that the approximated residual $\boldsymbol{r}_{\text{att}}^{\text{appr}}$ (i.e., the reflection of hiddenness) is directly determined by $\Delta \boldsymbol{z}_{\text{att}}^{\text{appr}}$.

### *B. Our Proposed MTD*

In this subsection, we present the design of MTD, where the effectiveness and hiddenness are jointly optimized and the voltage stability is maintained. The corresponding optimization problem is formally defined as

$$\min_{\Delta \boldsymbol{b}} -\left|\left|\boldsymbol{r}_{\text{sys}}^{\text{appr}}\right|\right|_2^2 + \omega_{\text{att}}\left|\left|\boldsymbol{r}_{\text{att}}^{\text{appr}}\right|\right|_2^2 + \omega_{\text{volt}}\left|\left|\frac{\partial \boldsymbol{x}}{\partial \boldsymbol{b}}|_{\Phi^*} \times \Delta \boldsymbol{b}\right|\right|_2^2, \qquad (17)$$

$$\text{s.t.} \qquad \Delta \underline{\boldsymbol{b}} \leq \Delta \boldsymbol{b} \leq \Delta \overline{\boldsymbol{b}},$$

where $\omega_{\text{att}} > 0, \omega_{\text{volt}} > 0$ denote the weight parameters, $\underline{\boldsymbol{b}}$ and $\overline{\boldsymbol{b}}$ signify the lower and upper bounds for reactance perturbation, and the last term in the objective function measures the voltage deviation by $\Delta \boldsymbol{b}$.

The challenge of solving problem (17) lies in the first term $\boldsymbol{r}_{\text{sys}}^{\text{appr}}$ as it involves the matrix inverse operation $\left[(H_{\boldsymbol{x}_{\text{MTDc}}}^{\text{MTD}*})^{\text{T}} H_{\boldsymbol{x}_{\text{MTDc}}}^{\text{MTD}*}\right]^{-1}$, which is related to the decision variable $\Delta \boldsymbol{b}$. Here $H_{\boldsymbol{x}_{\text{MTDc}}}^{\text{MTD}*} = \partial \boldsymbol{h}(\boldsymbol{x}_{\text{MTD}}^* + \boldsymbol{c}, \boldsymbol{b}_{\text{MTD}})/\partial \boldsymbol{x}$. To address the matrix inverse operation, (14) is rewritten as

$$\boldsymbol{r}_{\text{sys}}^{\text{appr}} = \left(I - P_{\boldsymbol{x}_{\text{MTDc}}}^{\text{MTD}*}\right) \times \Delta \boldsymbol{z}_{\text{sys}}^{\text{appr}}, \qquad (18)$$

where $P_{\boldsymbol{x}_{\text{MTDc}}}^{\text{MTD}*} = H_{\boldsymbol{x}_{\text{MTDc}}}^{\text{MTD}*}\left[(H_{\boldsymbol{x}_{\text{MTDc}}}^{\text{MTD}*})^{\text{T}} H_{\boldsymbol{x}_{\text{MTDc}}}^{\text{MTD}*}\right]^{-1}(H_{\boldsymbol{x}_{\text{MTDc}}}^{\text{MTD}*})^{\text{T}}$ is called the *projection matrix* as it orthogonally projects vectors into the column space of matrix $H_{\boldsymbol{x}_{\text{MTDc}}}^{\text{MTD}*}$ [25]. It is difficult to directly eliminate the matrix inverse operation, but fortunately, due to the small branch ratio $X/R$, we observe that matrix $P_{\boldsymbol{x}_{\text{MTDc}}}^{\text{MTD}*}$ is almost invariant under reactance perturbation. For example, when $\frac{\Delta \boldsymbol{b}}{\boldsymbol{b}} = 0.2$, the induced variation $\left|\left|P_{\boldsymbol{x}}^* - P_{\boldsymbol{x}_{\text{MTDc}}}^{\text{MTD}*}\right|\right|_2 = 0.0084$ is trivial. Hence, (17) is reformulated as

$$\begin{aligned}\min_{\Delta \boldsymbol{b}} -\left|\left|(I - P_{\boldsymbol{x}}^*) \times \Delta \boldsymbol{z}_{\text{sys}}^{\text{appr}}\right|\right|_2^2 + \omega_{\text{att}}\left|\left|\Delta \boldsymbol{z}_{\text{att}}^{\text{appr}}\right|\right|_2^2 + \\ + \omega_{\text{volt}}\left|\left|\frac{\partial \boldsymbol{x}}{\partial \boldsymbol{b}}|_{\Phi^*} \times \Delta \boldsymbol{b}\right|\right|_2^2, \qquad (19)\end{aligned}$$

$$\text{s.t.} \qquad \Delta \underline{\boldsymbol{b}} \leq \Delta \boldsymbol{b} \leq \Delta \overline{\boldsymbol{b}},$$

where $\boldsymbol{x}_{\text{MTD}}^*$ involved in $\Delta \boldsymbol{z}_{\text{sys}}^{\text{appr}}$ is approximated as $\boldsymbol{x}^* + \frac{\partial \boldsymbol{x}}{\partial \boldsymbol{b}}|_{\Phi^*} \times \Delta \boldsymbol{b}$. Problem (19) is a typical polynomial optimization problem with order 4, which is basically NP-hard, and it is difficult to directly find the global optimum. In this paper, we use the *fmincon* function provided by Matlab to find a local optimum from a given initial point, which is chosen as either $\Delta \underline{\boldsymbol{b}}$ or $\Delta \overline{\boldsymbol{b}}$. It is noted that an alternative for solving (19) is to approximate the original problem to a solvable one [26], which is left as our future work.

***Remark 2:*** The utilization of $\boldsymbol{c}$ in designing MTD reflects the vulnerability factors of system states, and a larger absolute value indicates that the state is more vulnerable to FDIAs. For an attacker intending to cause voltage violation in the feeder via irregular tap changes, she/he can reduce the end-bus voltage in low-load period to cause overvoltage violation or increase the end-bus voltage at heavy load period to cause undervoltage violation [27]. Here the end-bus voltage is more favored by attackers as it usually deviates a lot from the slack bus and is difficult to be predicted by the control center due to the integration of stochastic distributed energy resources. Hence, the absolute values of elements in $\boldsymbol{c}$ are set to be proportional to their distances away from the reference bus.

## V. Simulations

We evaluate the performance of the proposed MTD on the very unbalanced IEEE 13-bus test feeder [28]. In the case study, the standard deviations of real-time measurements are considered to be $1\%$ and the pseudo measurements are considered to have $20\%$ standard deviations. The significance level used in BDD is set to 0.05. The system topology and measurements of 13-bus test feeder are depicted in Fig. 2, where the buses 671 and 692, connected via the closed switch, are combined to bus 671 for simplification. When solving the optimization problem (19), the weight parameters are chosen as $\omega_{\text{att}} = 1$ and $\omega_{\text{volt}} = 100$, and all elements of $\boldsymbol{c}$ belong to $[0.09, 0.1]$ and are chosen according to the distances of their corresponding buses away from the slack bus. The perturbation ratios $\Delta \boldsymbol{b}/\boldsymbol{b}$ are assumed to be bounded by $20\%$.

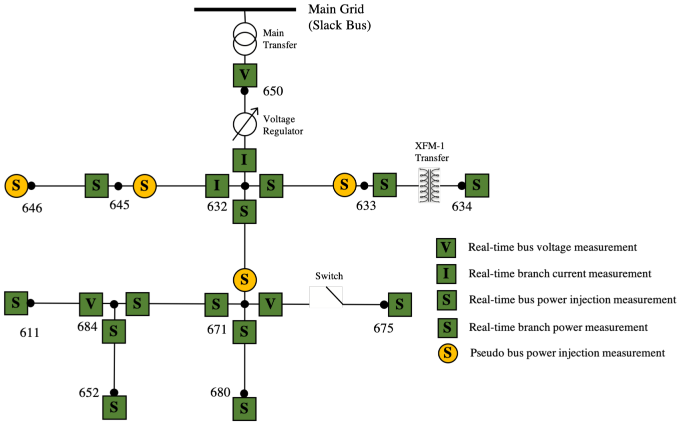
Main Grid
(Slack Bus)
Main
Transfer
V
650
Voltage
Regulator
I
S
646
645
632
633
XFM-1
Transfer
634
Switch
611
684
671
675
652
680
V Real-time bus voltage measurement
I Real-time branch current measurement
S Real-time bus power injection measurement
S Real-time branch power measurement
S Pseudo bus power injection measurement

Fig. 2. The system topology and measurements of IEEE 13-bus test feeder.

### *A. Residual Approximation Accuracy*

The subsection validates the accuracy of the derived residual approximations through numerical results. In each scenario, 26 branches in the test case are perturbed separately with the perturbation ratio ranging from 2% to 20% (10 steps), where residuals $r_{\text{att}}$ and $r_{\text{att}}^{\text{appr}}$ are calculated. $r_{\text{sys}}$ and $r_{\text{sys}}^{\text{appr}}$ are computed by further introducing the FDIA against one bus covered by the perturbed branch. Here the injected bias on the bus voltage is set to be 0.1 p.u. The results in the noiseless setting are demonstrated in Fig. 3. The approximated residuals $r_{\text{att}}^{\text{appr}}$ and $r_{\text{sys}}^{\text{appr}}$ are very close to their true values when the perturbation ratio is small. The approximation error increases with the perturbation ratio. Specifically, the average and maximum relative approximation errors are

$$\text{Mean}(\frac{|r_{\text{att}} - r_{\text{att}}^{\text{appr}}|}{r_{\text{att}}}) = 5.65\text{e-}4\%, \text{Mean}(\frac{|r_{\text{sys}} - r_{\text{sys}}^{\text{appr}}|}{r_{\text{sys}}}) = 0.35\%$$

$$\text{Max}(\frac{|r_{\text{att}} - r_{\text{att}}^{\text{appr}}|}{r_{\text{att}}}) = 2.01\text{e-}2\%, \text{Max}(\frac{|r_{\text{sys}} - r_{\text{sys}}^{\text{appr}}|}{r_{\text{sys}}}) = 8.52\%.$$

Further, the details of residual approximation with real-time measurement noises $\delta_i = 1\%$ are shown in Fig. 4. The approximation accuracy degrades significantly especially when the residual is dominated by measurement noises, which is an intuitive result as the residual approximations cannot predict the impact of measurement nosies.

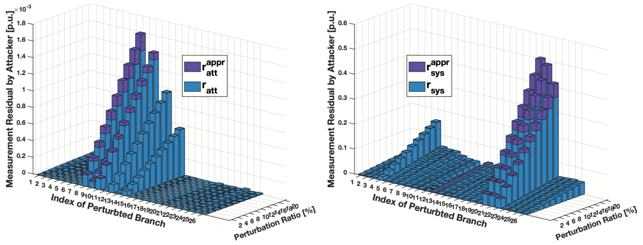

Fig. 3. The accuracy of approximated residuals in the noiseless setting.

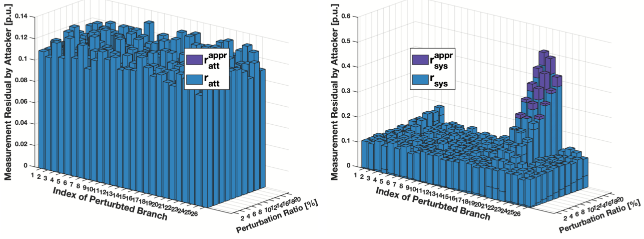

Fig. 4. The accuracy of approximated residuals with $\delta_i = 1\%$.

## B. Effectiveness and Hiddenness

This subsection evaluates the effectiveness and hiddenness of the proposed MTD. Fig. 5 shows residuals $r_{\text{att}}, r_{\text{sys}}$ and the voltage variation induced by MTD. Here we assume that all branches are equipped with *SmartValve* devices and 100 attack scenarios are simulated, where FDIAs are generated with each element of $\boldsymbol{c}$ sampled from the uniformly distribution $\mathcal{U}(-dm, dm)$. Here $dm = 0.03$ denotes the maximum magnitude of the injected bias into state variables. It can be observed that $r_{\text{att}}$ is almost equal to $r$, indicating that the attacker is hard to perceive the existence of MTD via $r_{\text{att}}$. Moreover, under the FDIAs generated from $\mathcal{U}(-0.03, 0.03)$, $r_{\text{sys}}$ can be significantly larger than $r$, and thus the probability of detecting FDIAs will be enhanced. Moreover, the voltage magnitudes and phases after MTD are both very close to those without MTD, meaning that the proposed MTD can maintain voltage stability. Specifically, the relative average voltage magnitude and phase variations are

$$\text{Mean}(\frac{||V_{\text{MTD}}| - |V||}{|V|}) = 9.48\text{e-}3\%,$$

$$\text{Mean}(\frac{|\theta_{\text{MTD}} - \theta|}{\theta}) = 1.4\text{e-}2\%.$$

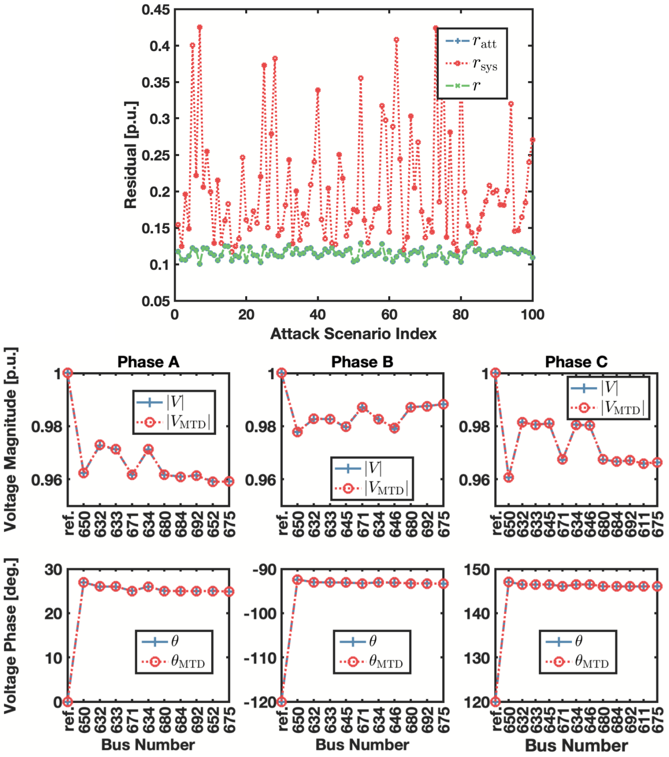

Fig. 5. Residuals and voltage variations by the proposed MTD.

Since it is not practical to install *SmartValve* devices onto all branches, we conduct simulations to evaluate the effectiveness and hiddenness of MTD when only partial branches can be perturbed. As shown in Fig. 6, the number of perturbed branches ranges from 17 to 26. For each number of perturbed branches, we randomly choose 100 sets of branches, and FDIAs are constructed with $\boldsymbol{c}$ sampled from $\mathcal{U}(-0.03, 0.03)$. Through Monte Carlo simulations, the attack detection probability (ADP) and MTD hidden probability (MHP) are estimated with $\frac{\text{Num. of detected attacks}}{1000}$ and $\frac{\text{Num. of being hidden}}{1000}$. The results indicate that the ADP increases with the number of perturbed branches, and the MHP is always around 95%, which means that $r_{\text{att}}$ is dominated by measurement noises. In addition, when the standard deviation of measurement noise is improved, the ADP will degrade as a higher detection threshold is required to tolerate the impact of noises. Moreover, it should be noticed that the ADP is closely related to the set of perturbed branches, and a good choose of branches contributes to the improvement of ADP and the maintenance of voltage stability, which is left as our future work.

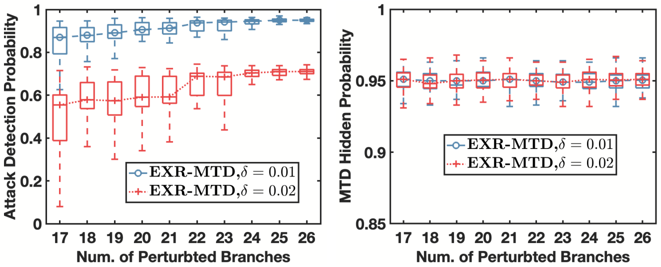

Fig. 6. Attack detection probability and MTD hidden probability under the proposed MTD.

## VI. Conclusion

In this paper, we quantified the effectiveness of hiddenness of MTD in unbalanced and multiphase PDSs with approximated measurement residuals, and provided a systematic design method for MTD to optimize the two metrics considering voltage stability. It was validated that the residual approximation errors for hiddenness are neglectable, while those for effectiveness were limited by $9\%$ when the reactance perturbation ratio was bounded by $20\%$, which is acceptable for the design of MTD. Moreover, the proposed MTD was shown to be completely hidden to the attacker with significantly enhanced detectability against FDIAs, while the voltage variation induced by MTD is neglectable. In future works, we will analytically investigate the effectiveness and hiddenness of MTD in unbalanced and multiphase PDSs and evaluate the performance of the proposed MTD in more test feeders.

## References

[1] A. Abur and A. G. Exposito, *Power system state estimation: theory and implementation*. CRC Press, 2004.

[2] Z. Cheng and M.-Y. Chow, "Resilient collaborative distributed energy management system framework for cyber-physical DC microgrids," *IEEE Transactions on Smart Grid*, vol. 11, no. 6, pp. 4637–4649, 2020.

[3] M. J. A. Robert M. Lee and T. Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid," Electricity Information Sharing and Analysis Center (E-ISAC), Tech. Rep., 2016.

[4] "Could venezuela's power outage really be a cyber attack?" https://www.bbc.com/news/world-latin-america-49079175, 2019.

[5] R. Deng, P. Zhuang, and H. Liang, "False data injection attacks against state estimation in power distribution systems," *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 2871–2881, 2019.

[6] P. Zhuang, R. Deng, and H. Liang, "False data injection attacks against state estimation in multiphase and unbalanced smart distribution systems," *IEEE Transactions on Smart Grid*, vol. 10, no. 6, pp. 6000–6013, 2019.

[7] M. Cui and J. Wang, "Deeply hidden moving-target-defense for cyber-secure unbalanced distribution systems considering voltage stability," *IEEE Transactions on Power Systems*, vol. 36, no. 3, pp. 1961–1972, 2021.

[8] B. Liu, H. Wu, A. Pahwa, F. Ding, E. Ibrahim, and T. Liu, "Hidden moving target defense against false data injection in distribution network reconfiguration," in *IEEE PESGM*. IEEE, 2018, pp. 1–5.

[9] G. Drewry, J. Herman, B. Green, S. McGuiness, and A. D. Rosso, "Evaluation of SmartValve$^{\text{TM}}$ Devices Installation at Central Hudson," Electric Power Research Institute (EPRI), Tech. Rep., Palo Alto, CA: 2020, 3002019771.

[10] Z. Zhang, R. Deng, D. K. Y. Yau, P. Cheng, and J. Chen, "Analysis of moving target defense against false data injection attacks on power grid," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2320–2335, 2020.

[11] Z. Zhang, R. Deng, D. K. Yau, P. Cheng, and J. Chen, "On hiddenness of moving target defense against false data injection attacks on power grid," *ACM Transactions on Cyber-Physical Systems*, vol. 4, no. 3, pp. 1–29, 2020.

[12] C. Liu, J. Wu, C. Long, and D. Kundur, "Reactance perturbation for detecting and identifying fdi attacks in power system state estimation," *IEEE Journal of Selected Topics in Signal Processing*, vol. 12, no. 4, pp. 763–776, 2018.

[13] B. Liu and H. Wu, "Optimal planning and operation of hidden moving target defense for maximal detection effectiveness," *IEEE Transactions on Smart Grid*, pp. 1–1, 2021.

[14] J. Tian, R. Tan, X. Guan, and T. Liu, "Enhanced hidden moving target defense in smart grids," *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 2208–2223, 2018.

[15] M. Bazrafshan and N. Gatsis, "Comprehensive modeling of three-phase distribution systems via the bus admittance matrix," *IEEE Transactions on Power Systems*, vol. 33, no. 2, pp. 2015–2029, 2017.

[16] M. E. Baran and A. W. Kelley, "State estimation for real-time monitoring of distribution systems," *IEEE Transactions on Power Systems*, vol. 9, no. 3, pp. 1601–1609, 1994.

[17] A. Primadianto and C.-N. Lu, "A review on distribution system state estimation," *IEEE Transactions on Power Systems*, vol. 32, no. 5, pp. 3875–3883, 2016.

[18] K. Clanents, G. Krutnpholz, and P. Davis, "Power system state estimation with measurement deficiency: An observability/measurement placement algorithm," *IEEE Transactions on Power Apparatus and Systems*, no. 7, pp. 2012–2020, 1983.

[19] J. Allemong, L. Radu, and A. Sasson, "A fast and reliable state estimation algorithm for AEP's new control center," *IEEE Transactions on Power Apparatus and Systems*, no. 4, pp. 933–944, 1982.

[20] I. Markwood, Y. Liu, K. Kwiat, and C. Kamhoua, "Electric grid power flow model camouflage against topology leaking attacks," in *IEEE INFOCOM*. IEEE, 2017, pp. 1–9.

[21] J. Kim, L. Tong, and R. J. Thomas, "Subspace methods for data attack on state estimation: A data driven approach," *IEEE Transactions on Signal Processing*, vol. 63, no. 5, pp. 1102–1114, 2014.

[22] NESCOR, "Electric sector failure scenarios and impact analyses version 3.0." Accessed: 2020, [Online]. Available: https://smartgrid.epri.com/doc/NESCOR%20Failure%20Scenarios%20v3%2012-11-15.pdf.

[23] "Specifications of smartvalve v1.04," Accessed: 2021, [Online]. Available: https://www.smartwires.com/download/20801/.

[24] E. Castillo, J. M. Gutiérrez, and A. S. Hadi, "Sensitivity analysis in discrete bayesian networks," *IEEE Transactions on Systems, Man, and Cybernetics*, vol. 27, no. 4, pp. 412–423, 1997.

[25] S. Chatterjee and A. S. Hadi, *Sensitivity analysis in linear regression*. John Wiley & Sons, 2009, vol. 327.

[26] Z. Li, S. He, and S. Zhang, *Approximation methods for polynomial optimization: Models, Algorithms, and Applications*. Springer Science & Business Media, 2012.

[27] Y. Isozaki, S. Yoshizawa, Y. Fujimoto, H. Ishii, I. Ono, T. Onoda, and Y. Hayashi, "Detection of cyber attacks against voltage control in distribution power grids with pvs," *IEEE Transactions on Smart Grid*, vol. 7, no. 4, pp. 1824–1835, 2015.

[28] K. P. Schneider, B. Mather, B. Pal, C.-W. Ten, G. J. Shirek, H. Zhu, J. C. Fuller, J. L. R. Pereira, L. F. Ochoa, L. R. de Araujo *et al.*, "Analytic considerations and design basis for the IEEE distribution test feeders," *IEEE Transactions on Power Systems*, vol. 33, no. 3, pp. 3181–3188, 2017.