Explicit Analysis on Effectiveness and Hiddenness of Moving Target Defense in AC Power Systems

Mengxiang Liu, *Student Member, IEEE*, Chengcheng Zhao, *Member, IEEE*, Zhenyong Zhang, *Member, IEEE*, and Ruilong Deng, *Senior Member, IEEE*

***Abstract*—Moving target defense (MTD) is becoming promising in thwarting the false data injection attacks (FDIAs) on power system state estimation (SE). However, due to the nonlinear dynamics of AC power systems, the investigation of the general evaluation metrics of MTD, namely the effectiveness in terms of attack detection and the hiddenness, is still challenging. To this end, in this paper, we attempt to conduct an explicit analysis on the MTD performance in AC power systems. First, we derive explicit approximations of measurement residuals to quantify the two metrics. Then, based on the projection matrix, maximizing the effectiveness is transformed to maximizing the lower bound of the approximated residual, under which the matrix inverse issue is addressed. Moreover, the maximization of hiddenness is achieved by the minimization of the approximated power flow difference caused by reactance perturbation. To balance the trade-off between effectiveness and hiddenness, the design of explicit residual-based MTD (EXR-MTD) is accomplished by aggregating the two sub-problems with an appropriate weight. Finally, extensive simulations are conducted to validate the performance of EXR-MTD. Numerical results indicate that EXR-MTD performs better than existing MTD strategies in terms of hiddenness, while the effectiveness of EXR-MTD is comparable to those of existing MTD strategies.**

***Index Terms*—False data injection attack, hidden moving target defense, AC power system, state estimation.**

I. Introduction

With the deep integration of information and communications technology into power systems, the control center is able to remotely monitor and control system's operation statuses. For the same reason, the power system is also suffering from the threat of cyberattacks. Recently, two state-owned utility companies in Brazil suffered separate ransomware attacks in June 2020, where sensitive data was stolen and dumped online, and some operations and services were forcibly shunt down [1]. Moreover, in March 2020, a power outage and fluctuations in supply across Venezuela knocked out approximately 35% of the country's telecommunications infrastructure, which was attributed to a cyberattack on the automatic control system [2]. Hence, it is crucial to investigate the cybersecurity issue in power systems.

Existing literature has revealed that once the attacker infers certain knowledge of the topology and branch parameters of the power system, and obtains the access to certain power flow and power injection measurements, then the false data injection attack (FDIA) against state estimation (SE) could be launched without being perceived by the bad data detector (BDD) [3]–[5]. A proactive defensive method named as moving target defense (MTD) has been recently proposed to thwart FDIAs by perturbing either branch reactances [6] or control gains in DC microgrids [7]. The basic idea behind MTD is to make the previously inferred/obtained model knowledge outdated, with which the constructed FDIA may be perceived. In particular, the perturbation on branch reactances can be achieved through the distributed flexible AC transmission system (D-FACTS) devices, which are small and light enough to be suspended from power lines [8].

There exist two general metrics that evaluate the performance of MTD, i.e., the effectiveness in detecting the FDIA and the hiddenness to deceive the attacker, which have been comprehensively investigated in the simplified DC (linear) model. Specifically, the effectiveness of MTD is quantified as the rank of the composite matrix, which is composed of the Jacobian matrices before and after MTD. The higher rank means the stronger effectiveness. In [9], Zhang *et al.* investigated the necessary condition for the *complete* MTD, under which the composite matrix has full column rank, and proposed algorithms to maximize the rank of composite matrix when the *complete* MTD is not feasible. Li *et al.* [10] systematically analyzed the feasibility and limitations of MTD in detecting FDIAs from the perspective of the topology constraints reflected by bus degrees. Liu *et al.* [11] proposed the MTD strategy under which the effectiveness is maximized and the branch power losses are minimized simultaneously. Liu *et al.* [12] solved the optimal placement problem for D-FACTS devices to maximize the effectiveness of MTD when the number of D-FACTS devices is limited. Lakshminarayana *et al.* [13] investigated the relationship between the effectiveness of MTD and the associated cost, based on the *smallest principal angle* of the Jacobian matrices before and after MTD, which is comparable to the rank of the composite matrix.

In addition to the effectiveness, the hiddenness of MTD is also indispensable as the attacker can easily perceive the implementation of MTD before launching FDIAs, by applying

This work was supported in part by the Science and Technology Innovation 2030 Program under Grant 2018AAA0101605, in part by the National Natural Science Foundation of China under Grants 61833015, 62073285, 62061130220, 61903328, in part by the Zhejiang Provincial Natural Science Foundation under Grants LZ21F020006, LZ22F030010, 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). (*Corresponding author: Chengcheng Zhao.*)

Mengxiang Liu, Chengcheng Zhao, and Ruilong Deng are with the State Key Lab. of Industrial Control Technology, College of Control Science and Engineering, Zhejiang University, Hangzhou, China (e-mails: {lmx329, chengchengzhao, dengruilong}@zju.edu.cn).

Zhenyong Zhang is with the State Key Lab. of Public Big Data, College of Computer Science and Technology, Guizhou University, Guiyang, China (e-mail: zyzhangnew@gmail.com).

BDD to eavesdropped measurements [14], which is usually adopted by the attacker to check the consistency between the inferred model knowledge [15], [16] and the current system model. According to [14], the enhanced hidden MTD can be obtained by solving a set of *linear* equations such that the power flows before and after MTD are invariant, named as the power flow invariant (PFI) MTD. Zhang *et al.* proved that the MTD can be hidden and completely effective regardless of the changes of power flows, by protecting a basic set of measurement points [17]. More recently, Liu *et al.* derived an analytical sufficient condition for the placement of D-FACTS devices utilizing topology analysis, based on which the DC hidden MTD (DC-HMTD) and AC-HMTD are proposed to maximize the effectiveness of MTD with the hiddenness being guaranteed [18].

However, there still exist nontrivial gaps between the reduced DC model and the practical power system such as the neglected series resistances and charging capacitances at power lines. Hence, many efforts are also devoted to the design of MTD in AC power systems. In [19], Liu *et al.* designed a joint reactance perturbation and meter protection strategy to improve the recoverability of system states under FDIAs. Nevertheless, this method relies heavily on the assumptions that only phase angles can be manipulated by attackers and the change of conductance caused by reactance perturbation is ignored, which are very similar to the assumptions made for the DC model. Moreover, Cui *et al.* [20] proposed the deeply hidden MTD in unbalanced distribution systems by perturbing the self and mutual reactances of phases together. Liu *et al.* [21] constructed a hidden MTD in the distribution network reconfiguration by minimizing the AC power flow difference before and after MTD. Nevertheless, there still lacks an explicit analysis on the effectiveness and hiddenness of MTD in AC power systems. Compared with the DC model, there exist two basic difficulties that make the explicit analysis in AC power systems challenging: (1) (*Effectiveness*) The linearized Jacobian matrix cannot be decomposed as analytically as that in the DC model without ignoring the change of conductance caused by reactance perturbation [19], and thus it is difficult to explicitly analyze the composite matrix. (2) (*Hiddenness*) The invariance of *complex* power flow before and after MTD cannot be guaranteed by merely perturbing reactances as practical power lines additionally have series resistances and charging capacitances [14], and moreover an explicit metric to quantify the hiddenness is yet missing.

Hence, in this paper, we develop two explicit and useful metrics to quantify the effectiveness and hiddenness of MTD in AC power systems based on the measurement residual, which acts as the detection metric in BDD. With the explicit metrics, we attempt to design the explicit residual-based MTD (EXR-MTD) to optimize the two metrics. Different from our previous work [22], we present an unified design method for MTD in both power transmission and distribution systems, and provide comprehensive validation results in standard test cases and rigorous proofs for the derivation of explicit metrics. The contributions of this paper are listed as follows:

- We derive explicit approximations of measurement residuals to quantify the effectiveness and hiddenness of MTD in AC power systems. Numerical results verify that the approximations precisely capture the impact of reactance perturbation and FDIAs on residuals.
- Based on the projection matrix, maximizing the effectiveness is transformed to maximizing the lower bound of the approximated residual, where the matrix inverse issue is addressed. The maximization of hiddenness is achieved by the minimization of the approximated power flow difference caused by reactance perturbation. To balance the trade-off between effectiveness and hiddenness, the design of EXR-MTD is accomplished by aggregating the two sub-problems with an appropriate weight.
- The EXR-MTD makes no assumption for the applied power systems and thus it can be employed in both power transmission and power distribution systems. Moreover, we find that the EXR-MTD in power distribution system cases has stronger effectiveness and hiddenness compared with that in power transmission system cases, and more performance metrics of EXR-MTD can be considered in power distribution systems besides effectiveness and hiddenness.

The remainder of this paper is organized as follows. Section II introduces the system model. Section III quantifies the effectiveness and hiddenness based on measurement residuals and introduces our problems of interest. Section IV derives the explicit approximations of measurement residuals and Section V provides the design of EXR-MTD. Section VI shows the simulation results and Section VII concludes this paper.

II. System Model

In this section, we introduce the AC power system model, SE model, BDD model, threat model and reactance perturbation model. Throughout this paper, we utilize $\dot{(\cdot)} \in \mathbb{C}$ to denote the complex number and $(\cdot) \in \mathbb{R}$ to indicate the real number. Moreover, $\dot{(\cdot)}^{\mathrm{H}}$ signifies the conjugate, $(\cdot)^{\mathrm{T}}$ denotes the transpose, and $||\cdot||_p$ represents the p-norm. The imaginary unit of complex number is denoted by $\dot{\jmath}$. Inequalities between vectors are compared by elements. The terms "bus" and "node", "branch" and "power line" are used interchangeably.

A. AC Power System Model

We focus on a symmetric and balanced power system, for which a single-phase model is commonly utilized. The model is composed of N nodes and L power lines. The set of nodes is denoted by $\mathcal{N} \triangleq \{0, \mathcal{N}^{\mathrm{PV}}, \mathcal{N}^{\mathrm{PQ}}\}$, where 0 signifies the reference bus, $\mathcal{N}^{\mathrm{PV}}$ represents the set of PV buses, and $\mathcal{N}^{\mathrm{PQ}}$ implies the set of PQ buses. The set of power lines is denoted by $\mathcal{L} \triangleq \{(j,k)\}$, and each branch (j,k) connects buses j and k. The set of nodes connecting to node $j \in \mathcal{N}$ is denoted by $\mathcal{N}_j$. In this paper, we only consider the steady states of the power system, where all voltages are sinusoidal signals at the same frequency. The voltage and current signals can therefore be characterized as $\dot{(\cdot)} = |\dot{\cdot}|e^{\dot{\jmath}\angle\dot{\cdot}}$, where $|\dot{\cdot}|$ is the root-mean-square value of the signal and $\angle\dot{\cdot}$ is the phase angle with respect to the reference bus.

The nodal voltages are taken to form the system state vector $\boldsymbol{x} \triangleq [\boldsymbol{\theta}_{\mathcal{N}^{\mathrm{PV}}}; \boldsymbol{\theta}_{\mathcal{N}^{\mathrm{PQ}}}; \boldsymbol{V}_{\mathcal{N}^{\mathrm{PQ}}}] \in \mathbb{R}^n$, where vectors $\boldsymbol{\theta}_{\mathcal{N}^{\mathrm{PV}}}$ and $\boldsymbol{\theta}_{\mathcal{N}^{\mathrm{PQ}}}$

contain the phase angles of PV and PQ buses, respectively, and vector $\boldsymbol{V}_{\mathcal{N}^{\mathrm{PQ}}}$ includes the voltage magnitudes of PQ buses. Here $n = 2(N-1) - N^{\mathrm{PV}}$ with N^{PV} being the number of PV buses. Once $\boldsymbol{x}$ is given, all power flow and power injection measurements can be determined. We usually have $m > n$ measurements to ensure that the state vector is fully observable from the meter measurements [23]. The mathematic relation between the measurement vector $\boldsymbol{z} \in \mathbb{R}^m$ and $\boldsymbol{x}$ is denoted by

$$\boldsymbol{z} \triangleq \boldsymbol{h}(\boldsymbol{x}) + \boldsymbol{e}. \tag{1}$$

where vector $\boldsymbol{h}(\cdot)$ contains the measurement functions and vector $\boldsymbol{e}$ is composed of measurement noises following normal distributions. We consider the standard π branch model as illustrated in Fig. 1, where $\vec{Z}_{jk} \triangleq R_{jk} + jX_{jk}$ denotes the series impedance and B_{jk} signifies the total charging susceptance. The series admittance is denoted by $\vec{Y}_{jk} \triangleq (\vec{Z}_{jk})^{-1}$.

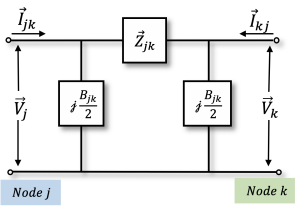


Fig. 1: The π branch model.

In practice, the measurements received from remote terminal units include active/reactive power flows, real/reactive power injections, and voltage magnitudes, i.e., $\boldsymbol{z} \triangleq [\boldsymbol{z}_1; \boldsymbol{z}_2; \boldsymbol{z}_3]$. Here, vector $\boldsymbol{z}_1 \triangleq [\boldsymbol{P}_{\mathscr{L}}^{\mathrm{fwd}}; \boldsymbol{Q}_{\mathscr{L}}^{\mathrm{fwd}}; \boldsymbol{P}_{\mathscr{L}}^{\mathrm{rvs}}; \boldsymbol{Q}_{\mathscr{L}}^{\mathrm{rvs}}]$ contains active and reactive power flows of branches $\mathscr{L}$ in both forward and reverse directions; vector $\boldsymbol{z}_2 \triangleq [\boldsymbol{P}_{\mathcal{N}}; \boldsymbol{Q}_{\mathcal{N}}]$ includes active and reactive power injections of buses $\mathcal{N}$; and vector $\boldsymbol{z}_3 \triangleq \boldsymbol{V}_{\mathcal{N}^{\mathrm{PQ}}}$ is composed of voltage magnitudes of PQ buses $\mathcal{N}^{\mathrm{PQ}}$. The measurement function of power flow $(j,k) \in \mathscr{L}$ is

$$h_{jk}^P(\boldsymbol{x}) + \mathscr{j} h_{jk}^Q(\boldsymbol{x}) \triangleq \vec{V}_j \left[\vec{Y}_{jk}(\vec{V}_j - \vec{V}_k) + \mathscr{j} \frac{B_{jk}}{2} \vec{V}_j \right]^{\mathrm{H}}.$$

The measurement function of power injection at bus $j \in \mathcal{N}$ is

$$h_j^P(\boldsymbol{x}) + \mathscr{j} h_j^Q(\boldsymbol{x}) \triangleq \sum_{i \in \mathcal{N}_j} \vec{V}_j \left[\vec{Y}_{ji}(\vec{V}_j - \vec{V}_i) + \mathscr{j} \frac{B_{ji}}{2} \vec{V}_j \right]^{\mathrm{H}}.$$

The measurement function of voltage magnitude at bus $j \in \mathcal{N}^{\mathrm{PQ}}$ is

$$h_j^V(\boldsymbol{x}) \triangleq |\vec{V}_j|.$$

For the large-scale power system with numerous measurement points, it is impractical to telemeter all points through real-time measuring devices such as phasor measurement units, intelligent electronic devices, and advanced metering infrastructure systems [24], [25]. To guarantee the observability from the measurements to the state vector, the pseudo measurements produced by the control center through historical customer load profiles, are usually utilized as the pseudo power injection measurements [26].

B. SE Model

SE is to obtain the estimate of $\boldsymbol{x}$, denoted by $\boldsymbol{x}^*$, that is the best fit of $\boldsymbol{z}$ following (1). The nonlinear weighted least squares (NWLS) problem is usually formulated to find $\boldsymbol{x}^*$ [27], i.e.,

$$\boldsymbol{x}^* \triangleq \arg\min_{\boldsymbol{x}} J(\boldsymbol{x}) = \arg\min_{\boldsymbol{x}} \boldsymbol{r}^{\mathrm{T}}(\boldsymbol{x}) W \boldsymbol{r}(\boldsymbol{x}), \tag{2}$$

where $\boldsymbol{r}(\boldsymbol{x}) \triangleq \boldsymbol{z} - \boldsymbol{h}(\boldsymbol{x})$ calculates the residual vector and the diagonal weight matrix $W \triangleq \mathrm{diag}([\delta_1^{-2}, \cdots, \delta_m^{-2}])$ with δ_i being the standard deviation of i-th measurement noise. The common method to solve (2) is the iterative Gauss-Newton method [28], which is based on a linear approximation to the objective function. Specifically, for the i-th iteration at $\boldsymbol{x} = \boldsymbol{x}_{[i]}$, when the step size $||\Delta_{[i]}||_2$ is small, the Taylor expansion of the residual function $\boldsymbol{r}(\boldsymbol{x}_{[i]} + \Delta_{[i]})$ can be approximated as

$$\begin{aligned} \boldsymbol{r}(\boldsymbol{x}_{[i]} + \Delta_{[i]}) &= \boldsymbol{r}(\boldsymbol{x}_{[i]}) - H_{\boldsymbol{x}_{[i]}} \Delta_{[i]} + O(||\Delta_{[i]}||_2^2) \\ &\approx \boldsymbol{l}(\Delta_{[i]}) \triangleq \boldsymbol{r}(\boldsymbol{x}_{[i]}) - H_{\boldsymbol{x}_{[i]}} \Delta_{[i]}, \end{aligned} \tag{3}$$

where $H_{\boldsymbol{x}_{[i]}}$ denotes the Jacobian matrix of $\boldsymbol{h}(\boldsymbol{x})$ at $\boldsymbol{x} = \boldsymbol{x}_{[i]}$. Substituting (3) into the objective function $J(\boldsymbol{x})$, we obtain

$$\begin{aligned} &J(\boldsymbol{x}_{[i]} + \Delta_{[i]}) \approx L(\Delta_{[i]}) \triangleq \frac{1}{2} \boldsymbol{l}^{\mathrm{T}}(\Delta_{[i]}) W \boldsymbol{l}(\Delta_{[i]}) \\ &= \frac{1}{2} J(\boldsymbol{x}_{[i]}) - \Delta_{[i]}^{\mathrm{T}} H_{\boldsymbol{x}_{[i]}}^{\mathrm{T}} W \boldsymbol{r}(\boldsymbol{x}_{[i]}) + \frac{1}{2} \Delta_{[i]}^{\mathrm{T}} H_{\boldsymbol{x}_{[i]}}^{\mathrm{T}} W H_{\boldsymbol{x}_{[i]}} \Delta_{[i]}, \end{aligned}$$

under which the gradient and Hessian of $L(\Delta_{[i]})$ can be calculated as

$$\begin{aligned} L^{'}(\Delta_{[i]}) &= -H_{\boldsymbol{x}_{[i]}}^{\mathrm{T}} W \boldsymbol{r}(\boldsymbol{x}_{[i]}) + H_{\boldsymbol{x}_{[i]}}^{\mathrm{T}} W H_{\boldsymbol{x}_{[i]}} \Delta_{[i]}, \\ L^{''}(\Delta_{[i]}) &= H_{\boldsymbol{x}_{[i]}}^{\mathrm{T}} W H_{\boldsymbol{x}_{[i]}}. \end{aligned}$$

If matrix $H_{\boldsymbol{x}_{[i]}}$ is of full column rank, then $L^{''}(\Delta_{[i]})$ will be positive definite. This indicates that $L(\Delta_{[i]})$ has a unique minimizer (by solving $L^{'}(\Delta_{[i]}) = \mathbf{0}$)

$$\Delta_{[i]} \triangleq \left[H_{\boldsymbol{x}_{[i]}}^{\mathrm{T}} W H_{\boldsymbol{x}_{[i]}} \right]^{-1} H_{\boldsymbol{x}_{[i]}}^{\mathrm{T}} W \boldsymbol{r}(\boldsymbol{x}_{[i]}), \tag{4}$$

which is utilized to update $\boldsymbol{x}_{[i]}$ as

$$\boldsymbol{x}_{[i+1]} \triangleq \boldsymbol{x}_{[i]} + \Delta_{[i]}.$$

The iteration is repeated until $\left\|\Delta_{[i]}\right\|_\infty$ and $\left|J\left(\boldsymbol{x}_{[i+1]}\right) - J\left(\boldsymbol{x}_{[i]}\right)\right|$ are small enough [29]. Indeed, the accuracy of the update rule (4) relies heavily on the approximation error of the Taylor expansion (3). In particular, the Taylor expansion will be more accurate if the step size $||\Delta_{[i]}||$ is smaller, which is mainly determined by the residual vector $\boldsymbol{r}(\boldsymbol{x}_{[i]})$ according to (4). This implies that if the initial value $\boldsymbol{x}_{[0]}$ is selected close to the optimal value, then the accuracy of the update rule (4) will be increased and can promote the convergence.

Due to stochastic meter failures and malicious cyber attacks, there may exist bad data in numerous measurements. Based on the result of SE, the system operator employs the residual-based BDD to perceive bad data, and to identify and eliminate it if possible [30]. In particular, the measurement residual is

obtained by comparing the actual measurement $\boldsymbol{z}$ with the estimated measurement $\hat{\boldsymbol{z}}$, i.e.,

$$r \triangleq ||\boldsymbol{r}(\boldsymbol{x}^*)||_2 = ||\boldsymbol{z} - \hat{\boldsymbol{z}}||_2 = ||\boldsymbol{z} - \boldsymbol{h}(\boldsymbol{x}^*)||_2.$$

When measurement noises follow normal distributions, r^2 will follow the chi-square distribution with $(m-n)$ freedom, i.e., χ^2_{m-n}, in the normal case. Through the hypothesis test, a predetermined threshold τ can be given with a significance level α [30]. If the residual r is larger than τ, i.e., $r > \tau$, then an abnormal alarm will be triggered by the BDD, whose false alarm rate is equal to the significance level; otherwise, $\boldsymbol{z}$ is taken as normal and the hypothesis is accepted.

C. Threat Model

In this paper, we consider the worst case where the attacker has the following capabilities:

- The attacker can eavesdrop and tamper with measurements through spoofed communication signals, intruded shared communications, or spoofed field devices [31].
- The attacker can infer the network topology and branch parameters of power system through topology leaking attacks [15] and subspace attacks [16], respectively, which typically requires the order of a few hours.
- The attacker can approximate the system state vector based on power flow or power injection measurements without too many efforts as shown in [4].

With the above capabilities, the attacker is able to launch the FDIA that can bypass the BDD. The adopted actions are summarized as follows: 1) inferring the measurement function $\boldsymbol{h}(\cdot)$; 2) approximating the system state $\boldsymbol{x}^*$ as $\boldsymbol{x}^{\text{appr}}$; 3) constructing the attack vector as

$$\boldsymbol{a} \triangleq \boldsymbol{h}(\boldsymbol{x}^{\text{appr}} + \boldsymbol{c}) - \boldsymbol{h}(\boldsymbol{x}^{\text{appr}}), \tag{5}$$

where $\boldsymbol{c} \in \mathbb{R}^n$ denotes the bias vector that the attacker intends to inject into the state vector; 4) tampering with $\boldsymbol{z}$ using $\boldsymbol{a}$. In the absence of MTD, it is evident that the measurement residual under the FDIA is

$$\begin{aligned} r_a &\triangleq ||\boldsymbol{z} + \boldsymbol{a} - \boldsymbol{h}(\boldsymbol{x}_a^*)||_2 \\ &= ||\boldsymbol{z} + \boldsymbol{h}(\boldsymbol{x}^{\text{appr}} + \boldsymbol{c}) - \boldsymbol{h}(\boldsymbol{x}^{\text{appr}}) - \boldsymbol{h}(\boldsymbol{x}_a^*)||_2 \\ &\approx ||\boldsymbol{z} - \boldsymbol{h}(\boldsymbol{x}^{\text{appr}})||_2 \approx ||\boldsymbol{z} - \boldsymbol{h}(\boldsymbol{x}^*)||_2 \approx r. \end{aligned}$$

due to the facts that $\boldsymbol{x}^{\text{appr}} \approx \boldsymbol{x}^*$ and $\boldsymbol{x}_a^* \approx \boldsymbol{x}^* + \boldsymbol{c} \approx \boldsymbol{x}^{\text{appr}} + \boldsymbol{c}$, where $\boldsymbol{x}_a^*$ denotes the estimated state vector under the FDIA. The falsified system states by the FDIA can make the system operator unconscious of the current system states, and thus will invalidate the application functions after SE such as the contingency analysis, emergency control, restorative control, and load forecasting [30], which may cause catastrophic failures to the power system.

D. Reactance Perturbation Model

For branch $(j,k) \in \mathscr{L}$ equipped with the D-FACTS device, the reactance can be arbitrarily perturbed within

$$X_{jk} + \Delta\underline{X}_{jk} \le X_{jk}^{\text{MTD}} \le X_{jk} + \Delta\overline{X}_{jk}, \tag{6}$$

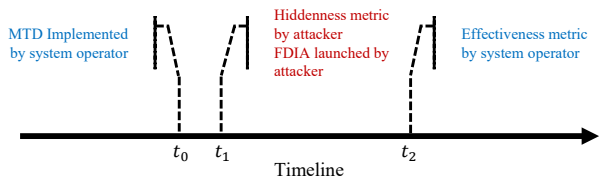


Fig. 2: Graphical illustration for the sequence of actions adopted by the attacker and the system operator, where $t_0 \le t_1 \le t_2$.

where X_{jk}^{MTD} denotes the branch reactance after MTD, and $\Delta\underline{X}_{jk}$ and $\Delta\overline{X}_{jk}$ signify the lower and upper bounds for the perturbation command ΔX_{jk}, respectively. Let vector $\boldsymbol{b}$ contain parameters R_{jk}, X_{jk}, and B_{jk} of all branches, and let vector $\Delta\boldsymbol{b}$ contain the perturbation commands. We have

$$\Delta\underline{\boldsymbol{b}} \le \Delta\boldsymbol{b} \le \Delta\overline{\boldsymbol{b}}, \tag{7}$$

where the elements in $\Delta\underline{\boldsymbol{b}}$ and $\Delta\overline{\boldsymbol{b}}$ are set as zeros when the elements correspond to series resistances, charging susceptances, or the branches equipped with no D-FACTS device. To defend against the FDIA, the system operator in the control center will command the remote D-FACTS devices to proactively perturb the branch reactances such that the previously inferred $\boldsymbol{h}(\cdot)$ can be antiquated. Here, the perturbation commands are transmitted through encrypted secure channels to guarantee the confidentiality and integrity. Since the attacker requires *several hours* to complete the inference process for the network topology and branch parameters (i.e., $\boldsymbol{h}(\cdot)$) [16], the perturbation commands should be updated quickly than that (e.g., hourly) to invalidate the inference process.

III. Problem Statement

In this section, we quantify the effectiveness and hiddenness of MTD based on measurement residuals and introduce our problems of interest. With some abuse of notations, we use symbols without subscript such as $\boldsymbol{h}(\cdot), \boldsymbol{x}, \boldsymbol{b}, \boldsymbol{z}$ to denote the quantities before MTD, and symbols with subscript $(\cdot)_{\text{MTD}}$ to signify those after MTD. For clarity, we provide a graphical illustration in Fig. 2 for the sequence of actions adopted by the attacker and the system operator.

A. The Hiddenness of MTD

Before launching FDIAs, the attacker will apply BDD to eavesdropped measurements to judge the consistency between the inferred model knowledge and the current system model. Here, we consider the worst case where the attacker can obtain the same measurements as the system operator, i.e., $\boldsymbol{z}_{\text{MTD}}$, to evaluate the hiddenness of MTD. The estimated system state is obtained by solving

$$\boldsymbol{x}_{\text{att}}^* \triangleq \arg\min_{\boldsymbol{x}} J_{\text{att}}(\boldsymbol{x}) = \arg\min_{\boldsymbol{x}} \boldsymbol{r}_{\text{att}}^{\text{T}}(\boldsymbol{x}) W \boldsymbol{r}_{\text{att}}(\boldsymbol{x}),$$

where $\boldsymbol{r}_{\text{att}}(\boldsymbol{x}) \triangleq \boldsymbol{z}_{\text{MTD}} - \boldsymbol{h}(\boldsymbol{x})$. We note that the power flow and voltage magnitude measurements of $\boldsymbol{z}_{\text{MTD}}$ can be different from those of $\boldsymbol{z}$. The hiddenness of MTD is quantified as

$$r_{\text{att}} \triangleq \left\|\boldsymbol{r}_{\text{att}}(\boldsymbol{x}_{\text{att}}^*)\right\|_2. \tag{8}$$

Due to the inconsistency between $\boldsymbol{h}(\cdot)$ and $\boldsymbol{h}_{\text{MTD}}(\cdot)$, $\boldsymbol{z}_{\text{MTD}}$ may not be totally explained by $\boldsymbol{h}(\cdot)$ in the absence of measurement noises, i.e., it may be difficult to find a $\boldsymbol{x}$ such that $\boldsymbol{h}(\boldsymbol{x})$ approaches $\boldsymbol{z}_{\text{MTD}}$ infinitely. Hence, r_{att} would be nontrivial if the perturbation commands are not properly designed. From the point view of the attacker, the smaller r_{att} means the stronger hiddenness. Only if the MTD strategy is hidden from the attacker, then the FDIA will be launched. Otherwise, the attacker will restart the inference process, and the FDIA will not be launched.

B. The Effectiveness of MTD

In the presence of MTD, the corrupted measurement vector is $\boldsymbol{z}^a_{\text{MTD}} = \boldsymbol{z}_{\text{MTD}} + \boldsymbol{a}_{\text{MTD}}$, where the construction of attack vector $\boldsymbol{a}_{\text{MTD}} = \boldsymbol{h}(\boldsymbol{x}^{\text{appr}}_{\text{MTD}}+\boldsymbol{c})-\boldsymbol{h}(\boldsymbol{x}^{\text{appr}}_{\text{MTD}})$ is similar to (5). Here, $\boldsymbol{x}^{\text{appr}}_{\text{MTD}}$ denotes the attacker's approximation of the estimated state vector by the system operator after MTD, i.e., $\boldsymbol{x}^*_{\text{MTD}}$, such that $\boldsymbol{h}_{\text{MTD}}(\boldsymbol{x}^*_{\text{MTD}}) = \boldsymbol{z}_{\text{MTD}} \approx \boldsymbol{h}_{\text{MTD}}(\boldsymbol{x}^{\text{appr}}_{\text{MTD}})$.[1] Due to the inconsistency between $\boldsymbol{h}(\cdot)$ and $\boldsymbol{h}_{\text{MTD}}(\cdot)$ caused by MTD, $\boldsymbol{z}^a_{\text{MTD}}$ would deviate from the expected vector $\boldsymbol{h}_{\text{MTD}}(\boldsymbol{x}^{\text{appr}}_{\text{MTD}}+\boldsymbol{c})$. Thus, it may be difficult to find a $\boldsymbol{x}$ such that $\boldsymbol{h}_{\text{MTD}}(\boldsymbol{x})$ approaches $\boldsymbol{z}^a_{\text{MTD}}$ infinitely in the absence of measurement noises, i.e., $\boldsymbol{z}^a_{\text{MTD}}$ may not be totally explained by the output of $\boldsymbol{h}_{\text{MTD}}(\cdot)$, under which the FDIA may be detected by the BDD. Specifically, the estimated state vector is obtained by solving

$$\boldsymbol{x}^*_{\text{sys}} \triangleq \arg\min_{\boldsymbol{x}} J_{\text{sys}}(\boldsymbol{x}) = \arg\min_{\boldsymbol{x}} \boldsymbol{r}^{\text{T}}_{\text{sys}}(\boldsymbol{x}) W \boldsymbol{r}_{\text{sys}}(\boldsymbol{x}),$$

where $\boldsymbol{r}_{\text{sys}}(\boldsymbol{x}) \triangleq \boldsymbol{z}^a_{\text{MTD}} - \boldsymbol{h}_{\text{MTD}}(\boldsymbol{x})$. The effectiveness of MTD is quantified as

$$r_{\text{sys}} \triangleq \left\| \boldsymbol{r}_{\text{sys}}(\boldsymbol{x}^*_{\text{sys}}) \right\|_2. \tag{9}$$

Obviously, r_{sys} needs to be large enough to expose the FDIA to BDD, and thus the larger r_{sys} means the stronger effectiveness.

C. Problems of Interest

In this paper, based on r_{att} and r_{sys}, we attempt to conduct an explicit analysis on the effectiveness and hiddenness and design EXR-MTD in AC power systems. We focus on the noiseless case where the residual is deterministic once the reactance perturbation and the FDIA are known, and simulations are conducted to validate the applicability of the proposed approach in the presence of measurement noises. Here the challenges lie in the implicit expressions of r_{sys} and r_{att} and the nontrivial trade-off between effectiveness and hiddenness [9]. Hence, our problems of interest include: 1) deriving explicit approximations for r_{sys} and r_{att}; 2) designing EXR-MTD such that r_{sys} is maximized and small r_{att} can be guaranteed.

[1]The impact of the reactance perturbation on the attacker's approximation of the estimated state vector is not considered.

IV. Approximations of Measurement Residuals

In this section, we derive explicit approximations for r_{att} and r_{sys} based on the sensitivity analysis, which discusses "how" and "how much" variations in the parameters of an optimization problem will change the optimal objective function value and the optimal solution [32]. Moreover, the accuracy of the derived approximations is validated through numerical results.

A. Sensitivity Analysis to the NWLS Problem

In this subsection, we apply sensitivity analysis to the general NWLS problem (2) and derive two essential sensitivities, with which r_{att} and r_{sys} can be approximated in a real-time manner. For brevity, let $\Theta^* \triangleq (\boldsymbol{x}^*, \boldsymbol{z}, \boldsymbol{b})$ denote the aggregated local optimal point. The first-order Karush-Kuhn-Tucker (KKT) condition for solving the NWLS problem (2) is established as

$$\nabla_{\boldsymbol{x}} J(\Theta^*) = \boldsymbol{0}. \tag{10}$$

The sensitivity is obtained by perturbing the system state $\boldsymbol{x}^*$ and corresponding parameters $\boldsymbol{z}, \boldsymbol{b}$ around Θ^* such that the KKT condition (10) still holds. Hence, by differentiating (2) and (10), we have

$$\begin{bmatrix} J^{\text{T}}_{\boldsymbol{x}} & J^{\text{T}}_{\boldsymbol{z}} & J^{\text{T}}_{\boldsymbol{b}} & -1 \\ J_{\boldsymbol{xx}} & J_{\boldsymbol{xz}} & J_{\boldsymbol{xb}} & 0 \end{bmatrix} \begin{bmatrix} d\boldsymbol{x} \\ d\boldsymbol{z} \\ d\boldsymbol{b} \\ dJ \end{bmatrix} = 0, \tag{11}$$

where

$$J_{\boldsymbol{x}} \triangleq \nabla_{\boldsymbol{x}} J(\Theta^*), J_{\boldsymbol{z}} \triangleq \nabla_{\boldsymbol{z}} J(\Theta^*), J_{\boldsymbol{b}} \triangleq \nabla_{\boldsymbol{b}} J(\Theta^*),$$
$$J_{\boldsymbol{xx}} \triangleq \nabla_{\boldsymbol{xx}} J(\Theta^*), J_{\boldsymbol{xz}} \triangleq \nabla_{\boldsymbol{xz}} J(\Theta^*), J_{\boldsymbol{xb}} \triangleq \nabla_{\boldsymbol{xb}} J(\Theta^*).$$

Proposition 1: When the objective function value $J(\Theta^*)$ approaches zero infinitely, the sensitivities $\frac{\partial \boldsymbol{x}}{\partial \boldsymbol{b}}$ and $\frac{\partial \boldsymbol{r}}{\partial \boldsymbol{z}}$ at point Θ^* are obtained as

$$\frac{\partial \boldsymbol{x}}{\partial \boldsymbol{b}}|_{\Theta^*} \triangleq -\left[(H^*_{\boldsymbol{x}})^{\text{T}} H^*_{\boldsymbol{x}}\right]^{-1} (H^*_{\boldsymbol{x}})^{\text{T}} H^*_{\boldsymbol{b}}, \tag{12}$$

$$\frac{\partial \boldsymbol{r}}{\partial \boldsymbol{z}}|_{\Theta^*} \triangleq I - H^*_{\boldsymbol{x}} \left[(H^*_{\boldsymbol{x}})^{\text{T}} H^*_{\boldsymbol{x}}\right]^{-1} (H^*_{\boldsymbol{x}})^{\text{T}}, \tag{13}$$

where $H^*_{\boldsymbol{x}}$ denotes the Jacobian matrix at $\boldsymbol{x} = \boldsymbol{x}^*$ and $H^*_{\boldsymbol{b}} \triangleq \partial \boldsymbol{h}(\boldsymbol{x}^*)/\partial \boldsymbol{b}$.

Proof: The proof can be found in Appendix A. ■

It is noted that $J(\Theta^*)$ can approach zero infinitely in the absence of measurement noises, and thus (12) and (13) are directly adopted hereafter. Moreover, the correctness of the derived sensitivities can be easily verified by linearizing the nonlinear measurement function (1) around $\boldsymbol{x}^*$ as $\Delta \boldsymbol{z} \triangleq \boldsymbol{z} - \boldsymbol{z}^* = H^*_{\boldsymbol{x}}(\boldsymbol{x} - \boldsymbol{x}^*) + \boldsymbol{e} = H^*_{\boldsymbol{x}} \Delta \boldsymbol{x} + \boldsymbol{e}$, and then according to the simplified DC model the alteration of residual $\Delta \boldsymbol{r} = \Delta \boldsymbol{z} - H^*_{\boldsymbol{x}} \Delta \hat{\boldsymbol{x}}$ can be calculated as $\Delta \boldsymbol{r} \triangleq \left[I - H^*_{\boldsymbol{x}} \left[(H^*_{\boldsymbol{x}})^{\text{T}} H^*_{\boldsymbol{x}}\right]^{-1} (H^*_{\boldsymbol{x}})^{\text{T}}\right] \Delta \boldsymbol{z}$, i.e., (13).

B. Approximations of Measurement Residuals

In this subsection, based on (12) and (13), explicit approximations of r_{att} and r_{sys} are derived.

1) Approximation of r_{att}: According to (8), the nontrivial r_{att} is caused by the measurement variations before and after MTD, i.e., $\Delta \boldsymbol{z}_{\text{att}} \triangleq \boldsymbol{h}_{\text{MTD}}(\boldsymbol{x}^*_{\text{MTD}}) - \boldsymbol{h}(\boldsymbol{x}^*)$, where $\boldsymbol{x}^*_{\text{MTD}}$ denotes the solution to (2) with measurement $\boldsymbol{z}_{\text{MTD}}$ and measurement function $\boldsymbol{h}_{\text{MTD}}(\cdot)$. Hence, via (13), r_{att} is approximated around Θ^* as

$$r_{\text{att}} \approx \left\| \frac{\partial \boldsymbol{r}}{\partial \boldsymbol{z}}|_{\Theta^*} \times \Delta \boldsymbol{z}_{\text{att}} \right\|_2. \tag{14}$$

Here, the computation of precise $\Delta \boldsymbol{z}_{\text{att}}$ requires to requires to solve the AC power flow problem [33], which is typically based on the iterative Newton-Raphson method and is time-consuming. We choose to approximate $\Delta \boldsymbol{z}_{\text{att}}$ utilizing $\Delta \boldsymbol{b}$ and $\Delta \boldsymbol{x}^* \triangleq \boldsymbol{x}^*_{\text{MTD}} - \boldsymbol{x}^*$, i.e.,

$$\begin{aligned} \Delta \boldsymbol{z}_{\text{att}} &\approx H^*_{\boldsymbol{b}} \Delta \boldsymbol{b} + H^*_{\boldsymbol{x}} \Delta \boldsymbol{x}^* \\ &\approx \Delta \boldsymbol{z}^{\text{appr}}_{\text{att}} \triangleq \Big(H^*_{\boldsymbol{b}} + H^*_{\boldsymbol{x}} \times \frac{\partial \boldsymbol{x}}{\partial \boldsymbol{b}}|_{\Theta^*} \Big) \Delta \boldsymbol{b}. \end{aligned} \tag{15}$$

Integrating (14) with (15), we obtain the explicit approximation of r_{att} as

$$r_{\text{att}} \approx r^{\text{appr}}_{\text{att}} \triangleq \left\| \Delta \boldsymbol{z}^{\text{appr}}_{\text{att}} \right\|_2, \tag{16}$$

which implies that the quantified metric for hiddenness is equivalent to the approximated power flow variations before and after MTD, which matches the PFI condition for the hidden MTD in the DC model [14].

2) Approximation of r_{sys}: In the presence of MTD, the solution to (2) with measurement $\boldsymbol{z}^a_{\text{MTD}}$ and measurement function $\boldsymbol{h}_{\text{MTD}}(\cdot)$ may slightly deviate from $\boldsymbol{x}^*_{\text{MTD}} + \boldsymbol{c}$ due to the bias $\Delta \boldsymbol{z}_{\text{sys}} \triangleq \boldsymbol{z}^a_{\text{MTD}} - \boldsymbol{h}_{\text{MTD}}(\boldsymbol{x}^*_{\text{MTD}} + \boldsymbol{c})$, which can result in nontrivial r_{sys}. Hence, r_{sys} is approximated around the shifted local optimal point $\Theta^*_{\text{MTDa}} \triangleq \big(\boldsymbol{x}^*_{\text{MTD}} + \boldsymbol{c}, \boldsymbol{h}_{\text{MTD}}(\boldsymbol{x}^*_{\text{MTD}} + \boldsymbol{c}), \boldsymbol{b}_{\text{MTD}}\big)$ by the attacker as

$$r_{\text{sys}} \approx \left\| \frac{\partial \boldsymbol{r}}{\partial \boldsymbol{z}}|_{\Theta^*_{\text{MTDa}}} \times \Delta \boldsymbol{z}_{\text{sys}} \right\|_2, \tag{17}$$

where $\Delta \boldsymbol{z}_{\text{sys}}$ is expanded as

$$\begin{aligned} \Delta \boldsymbol{z}_{\text{sys}} &= \boldsymbol{z}_{\text{MTD}} + \boldsymbol{a}_{\text{MTD}} - \boldsymbol{h}_{\text{MTD}}(\boldsymbol{x}^*_{\text{MTD}} + \boldsymbol{c}) \\ &\approx -\boldsymbol{h}_{\text{MTD}}(\boldsymbol{x}^*_{\text{MTD}} + \boldsymbol{c}) + \boldsymbol{h}(\boldsymbol{x}^*_{\text{MTD}} + \boldsymbol{c}) + \\ &\quad + \boldsymbol{h}_{\text{MTD}}(\boldsymbol{x}^*_{\text{MTD}}) - \boldsymbol{h}(\boldsymbol{x}^*_{\text{MTD}}), \end{aligned} \tag{18}$$

owing to the fact that $\boldsymbol{x}^*_{\text{MTD}}$ can be accurately approximated by the attacker as $\boldsymbol{x}^{\text{appr}}_{\text{MTD}}$ without too many efforts [4]. According to (18), there exist two directions for the further approximation of $\Delta \boldsymbol{z}_{\text{sys}}$, i.e., utilizing the reactance perturbation $\Delta \boldsymbol{b}$ or the induced state bias $\boldsymbol{c}$. Specifically, based on $\Delta \boldsymbol{b}$, we have

$$\Delta \boldsymbol{z}_{\text{sys}} \approx \Delta \boldsymbol{z}^{\text{apprb}}_{\text{sys}} \triangleq (H^{\text{MTD}*}_{\boldsymbol{b}} - H^{\text{MTDc}*}_{\boldsymbol{b}}) \times \Delta \boldsymbol{b}, \tag{19}$$

where

$$H^{\text{MTD}*}_{\boldsymbol{b}} \triangleq \frac{\partial \boldsymbol{h}(\boldsymbol{x}^*_{\text{MTD}})}{\partial \boldsymbol{b}}, \quad H^{\text{MTDc}*}_{\boldsymbol{b}} \triangleq \frac{\partial \boldsymbol{h}(\boldsymbol{x}^*_{\text{MTD}} + \boldsymbol{c})}{\partial \boldsymbol{b}}.$$

Based on $\boldsymbol{c}$, we have

$$\Delta \boldsymbol{z}_{\text{sys}} \approx \Delta \boldsymbol{z}^{\text{apprx}}_{\text{sys}} \triangleq (H^*_{\boldsymbol{x}_{\text{MTD}}} - H^{\text{MTD}*}_{\boldsymbol{x}_{\text{MTD}}}) \times \boldsymbol{c}, \tag{20}$$

where

$$H^*_{\boldsymbol{x}_{\text{MTD}}} \triangleq \frac{\partial \boldsymbol{h}(\boldsymbol{x}^*_{\text{MTD}})}{\partial \boldsymbol{x}}, \quad H^{\text{MTD}*}_{\boldsymbol{x}_{\text{MTD}}} \triangleq \frac{\partial \boldsymbol{h}_{\text{MTD}}(\boldsymbol{x}^*_{\text{MTD}})}{\partial \boldsymbol{x}}.$$

Substituting (19)-(20) into (17), the two explicit approximations of r_{sys} are obtained as

$$r_{\text{sys}} \approx r^{\text{apprb}}_{\text{sys}} \triangleq \left\| (I - P^{\text{MTD}*}_{\boldsymbol{x}_{\text{MTDc}}}) \times \Delta \boldsymbol{z}^{\text{apprb}}_{\text{sys}} \right\|_2, \tag{21}$$

and

$$r_{\text{sys}} \approx r^{\text{apprx}}_{\text{sys}} \triangleq \left\| (I - P^{\text{MTD}*}_{\boldsymbol{x}_{\text{MTDc}}}) \times \Delta \boldsymbol{z}^{\text{apprx}}_{\text{sys}} \right\|_2, \tag{22}$$

respectively, where

$$P^{\text{MTD}*}_{\boldsymbol{x}_{\text{MTDc}}} \triangleq H^{\text{MTD}*}_{\boldsymbol{x}_{\text{MTDc}}} \big[(H^{\text{MTD}*}_{\boldsymbol{x}_{\text{MTDc}}})^{\text{T}} H^{\text{MTD}*}_{\boldsymbol{x}_{\text{MTDc}}} \big]^{-1} (H^{\text{MTD}*}_{\boldsymbol{x}_{\text{MTDc}}})^{\text{T}} \tag{23}$$

and $H^{\text{MTD}*}_{\boldsymbol{x}_{\text{MTDc}}} \triangleq \partial \boldsymbol{h}_{\text{MTD}}(\boldsymbol{x}^*_{\text{MTD}} + \boldsymbol{c}) / \partial \boldsymbol{x}$. We note that the approximation $\boldsymbol{x}^*_{\text{MTD}} \approx \boldsymbol{x}^* + \frac{\partial \boldsymbol{x}}{\partial \boldsymbol{b}}|_{\Theta^*} \times \Delta \boldsymbol{b}$ is adopted to guarantee the real-time property when calculating (21)-(23).

Remark 1: To guarantee the approximation accuracy, we adopt the sensitivities derived around two optimal points to approximate r_{att} and r_{sys}. In particular, the approximation of r_{att} is based on the sensitivities derived around the original optimal point $\Theta^* = (\boldsymbol{x}^*, \boldsymbol{z}, \boldsymbol{b})$, while the approximation of r_{sys} is based on the sensitivities derived around the shifted optimal point by the attacker $\Theta^*_{\text{MTDa}} = \big(\boldsymbol{x}^*_{\text{MTD}} + \boldsymbol{c}, \boldsymbol{h}_{\text{MTD}}(\boldsymbol{x}^*_{\text{MTD}} + \boldsymbol{c}), \boldsymbol{b}_{\text{MTD}}\big)$. In practice, the injected bias vector $\boldsymbol{c}$ is not available to the system operator. Nevertheless, it will not affect the design of EXR-MTD with the derived sensitivities, as the elements in $\boldsymbol{c}$ merely act as the vulnerability factors of system states and do not have to be the true state biases injected by the attacker. Generally speaking, when designing EXR-MTD, the value of vector $\boldsymbol{c}$ is assigned in advance by the system operator. If the absolute value of the i-th element in $\boldsymbol{c}$ is significantly larger than others, then the designed EXR-MTD will make the FDIA targeting at the i-th state more perceivable to the BDD.

C. Numerical Results

In this subsection, we provide numerical results to validate the accuracy of derived approximations $r^{\text{appr}}_{\text{att}}$, $r^{\text{apprb}}_{\text{sys}}$, and $r^{\text{apprx}}_{\text{sys}}$. Let the set $\mathscr{L}_p$ include all branches that cover at least one PQ bus. In each scenario, we perturb one branch $(j,k) \in \mathscr{L}_p$ with the perturbation magnitude ratio $\frac{\Delta \boldsymbol{b}}{\boldsymbol{b}}$ ranging from 2% to 20% with step 2%, under which r_{att} and $r^{\text{appr}}_{\text{att}}$ are calculated. After introducing the FDIA against one PQ bus covered by (j,k), where the induced voltage magnitude bias varies from 0.01p.u. to 0.1p.u., r_{sys}, $r^{\text{apprb}}_{\text{sys}}$, and $r^{\text{apprx}}_{\text{sys}}$ are computed. We first show the results in the noiseless setting and then introduce the measurement noises with standard deviations $\delta_i = 5\%, \forall 1 \leq i \leq m$ to evaluate their impact. Due to the space limitation, we merely visualize the details of residuals in IEEE 14-bus (transmission system) and radial 18-bus (distribution system) cases with $\delta_i = 0$, where 18×10 and 17×10 scenarios are depicted, respectively. More details about the results under $\delta_i = 5\%$ can be found in Appendix C. According to Fig. 3 and Fig. 4, the approximation errors increase with the growth of $\Delta \boldsymbol{b}$ or $\boldsymbol{c}$, which is an intuitive phenomenon as the sensitivities are obtained around either Θ^*

or Θ^*_{MTDa}. Specifically, for the residual by the attacker, $r_{\text{att}}^{\text{appr}}$ is very close to r_{att} especially in the radial 18-bus case. For the residual by the system operator, $r_{\text{sys}}^{\text{apprx}}$ has higher accuracy than $r_{\text{sys}}^{\text{apprb}}$ in the IEEE 14-bus case as $||\Delta \boldsymbol{b}||_2$ is generally larger than $||\boldsymbol{c}||_2$. Differently, $r_{\text{sys}}^{\text{apprb}}$ performs better than $r_{\text{sys}}^{\text{apprx}}$ in the radial 18-bus case due to the small branch ratios X/R. Finally, the essential trade-off between r_{att} and r_{sys} can be qualitatively deduced from the results. Roughly speaking, the higher r_{sys} usually leads to the comparable r_{att}, indicating that the effectiveness and hiddenness of MTD are hard to be satisfied simultaneously without a systematic design method.

Furthermore, the average and maximum relative approximation errors (RAEs) under $\delta_i = 0$ and $\delta_i = 5\%$ are shown in TABLE I and TABLE II, respectively, to validate the applicability to numerous test cases. To make the results meaningful, the metrics are counted by excluding the residuals smaller than 0.01p.u., which are indistinguishable from the impact of measurement noises. From the results, the average RAEs of $r_{\text{att}}^{\text{appr}}$ and $r_{\text{sys}}^{\text{apprx}}$ are within 6% and 4%, respectively, in transmission system test cases. Moreover, in radial 69-bus and 141-bus cases, r_{att} and $r_{\text{att}}^{\text{appr}}$ are both smaller than 0.01p.u., indicating that **the impact of reactance perturbation is neglectable**. It is noted that the RAEs of $r_{\text{sys}}^{\text{apprb}}$ and $r_{\text{sys}}^{\text{apprx}}$ show similar characteristics as those reflected by Fig. 3 and Fig. 4. **Hence, we will utilize $r_{\text{att}}^{\text{appr}}$, $r_{\text{sys}}^{\text{apprx}}$ for the design of EXR-MTD in power transmission systems and $r_{\text{att}}^{\text{appr}}, r_{\text{sys}}^{\text{apprb}}$ for that in power distribution systems.**

As for the impact of measurement noises, it is clearly revealed that all RAEs increase as the introduction of measurement noises. The average RAEs are still within the acceptable range (smaller than 25%), while the maximum RAEs can be extremely large. Specifically, the approximation accuracy of $r_{\text{att}}^{\text{appr}}$ is almost not affected by measurement noises in the IEEE 14-bus case as the impact of measurement noises on the residual is far smaller than that of the reactance perturbation. While in the radial 18-bus case the accuracy decreases significantly as the impact of measurement noises on the residual is comparable to or larger than that of the reactance perturbation. This phenomenon is due to that the branch ratio X/R in the IEEE 14-bus case is far larger than that in the radial 18-bus case. The approximation accuracy of $r_{\text{sys}}^{\text{apprb}}$ and $r_{\text{sys}}^{\text{apprx}}$ are not significantly affected no matter in the IEEE 14-bus case or in the radial 18-bus case as the impact of measurement noises on the residual is far smaller than that of the FDIA and reactance perturbation. Furthermore, from the point view of effectiveness and hiddenness, the impact of measurement noises is beneficial to the hiddenness of MTD, as it can cover the impact caused by reactance perturbation. While measurement noises have a detrimental impact on the effectiveness of MTD, since it may prevent the FDIA from being detected by BDD. **In summary, we assert that the approximations $r_{\text{att}}^{\text{appr}}, r_{\text{sys}}^{\text{apprb}}$, and $r_{\text{sys}}^{\text{apprx}}$ exactly capture the impact of reactance perturbation and FDIAs on residuals. Moreover, from the above studies on the two representative cases, we can infer that measurement noises can almost guarantee the hiddenness of MTD in power distribution systems, while the hiddenness in power transmission systems and the effectiveness of MTD are almost not affected by measurement noises.** Although the impact of measurement noises on the approximated residuals has been illustrated through numerical results, it is still vital to reveal the theoretical relations between measurement noises and the approximated residuals, which is left as the future work.

TABLE I: Average and Maximum RAEs, $\delta_i = 0$

Metrics / Test cases	$\lvert r_{\text{att}}^{\text{appr}} - r_{\text{att}}\rvert / r_{\text{att}}$		$\lvert r_{\text{sys}}^{\text{apprb}} - r_{\text{sys}}\rvert / r_{\text{sys}}$		$\lvert r_{\text{sys}}^{\text{apprx}} - r_{\text{sys}}\rvert / r_{\text{sys}}$	
	Avg.	Max.	Avg.	Max.	Avg.	Max.
IEEE 14-bus	5.58%	14.54%	8.85%	16.74%	**2.30%**	4.88%
IEEE 57-bus	4.77%	13.02%	9.52%	22.70%	**3.42%**	27.94%
IEEE 118-bus	4.84%	16.81%	8.99%	18.14%	**1.98%**	9.09%
IEEE 300-bus	4.49%	44.77%	9.77%	31.24%	**1.87%**	31.59%
Radial 18-bus	0	0	**15.75%**	29.11%	35.47%	70.84%
Radial 69-bus	\[a]	\	**7.99%**	28.55%	38.08%	78.17%
Radial 85-bus	0.72%	0.76%	**3.83%**	12.69%	25.96%	80.07%
Radial 141-bus	\	\	**6.75%**	22.39%	14.02%	77.93%

[a] Residuals are smaller than 0.01p.u.

TABLE II: Average and Maximum RAEs, $\delta_i = 5\%$

Metrics / Test cases	$\lvert r_{\text{att}}^{\text{appr}} - r_{\text{att}}\rvert / r_{\text{att}}$		$\lvert r_{\text{sys}}^{\text{apprb}} - r_{\text{sys}}\rvert / r_{\text{sys}}$		$\lvert r_{\text{sys}}^{\text{apprx}} - r_{\text{sys}}\rvert / r_{\text{sys}}$	
	Avg.	Max.	Avg.	Max.	Avg.	Max.
IEEE 14-bus	5.53%	19.21%	10.12%	22.13%	**3.88%**	19.84%
IEEE 57-bus	22.82%	97.31%	18.31%	71.80%	**12.93%**	81.39%
IEEE 118-bus	25.93%	99.75%	12.25%	93.83%	**5.69%**	99.32%
IEEE 300-bus	29.96%	99.99%	29.37%	99.96%	**23.56%**	99.99%
Radial 18-bus	16.12%	25.54%	**20.18%**	31.73%	27.94%	72.23%
Radial 69-bus	\	\	**12.28%**	30.37%	37.68%	88.17%
Radial 85-bus	48.28%	52.07%	**10.25%**	54.26%	31.15%	85.04%
Radial 141-bus	\	\	**12.59%**	62.26%	18.29%	87.93%

V. EXR-MTD

In this section, based on the explicit approximations (16), (21)-(22), we propose EXR-MTD to jointly optimize the effectiveness and hiddenness. Essentially, the design of EXR-MTD can be decomposed as the following two sub-problems:

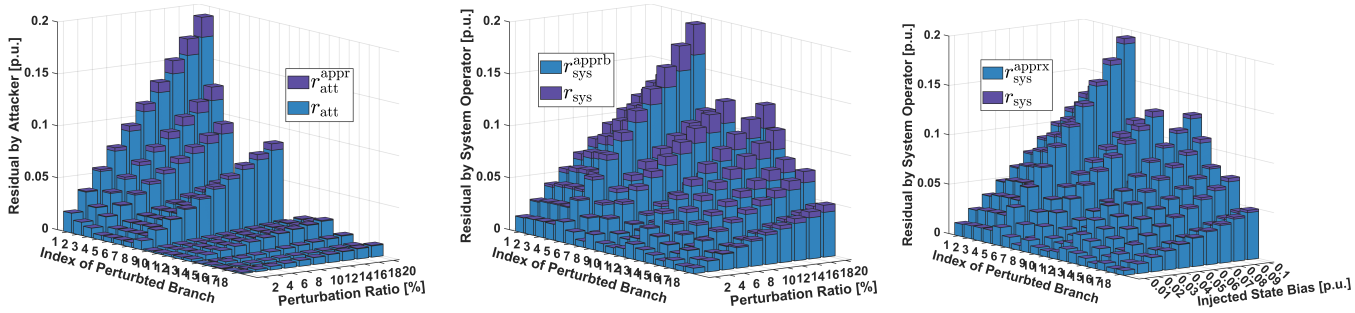
$$\max_{\boldsymbol{b}_{\text{MTD}}} \quad (r_{\text{sys}}^{\text{apprx}})^2 \text{ or } (r_{\text{sys}}^{\text{apprb}})^2 \qquad \text{Sub-Problem I}^1 \qquad (24)$$

and

$$\min_{\boldsymbol{b}_{\text{MTD}}} \quad (r_{\text{att}}^{\text{appr}})^2, \qquad \text{Sub-Problem II} \qquad (25)$$

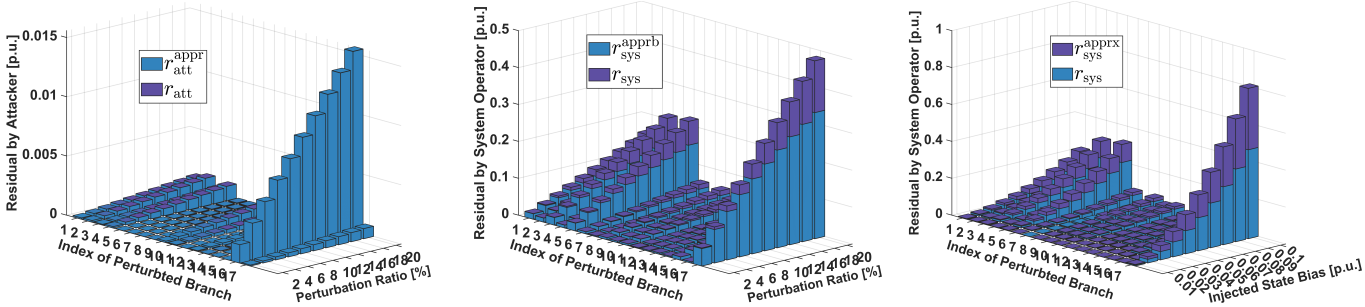
where (24) and (25) represent the maximization of effectiveness and hiddenness, respectively. Here the main challenge lies in the matrix inverse issue involved in $r_{\text{sys}}^{\text{apprx}}$ and $r_{\text{sys}}^{\text{apprb}}$, which can significantly enlarge the computation complexity of sub-problem I and even make the (local) optimum unavailable. Hence, we first make some transformations for sub-problem I to address the matrix inverse issue, after which the two sub-problems are aggregated together by multiplying an appropriate weight.

[1] $(r_{\text{sys}}^{\text{apprx}})^2$ is utilized for power transmission systems and $(r_{\text{sys}}^{\text{apprb}})^2$ is for power distribution systems.



(a) r_{att} and $r_{\text{att}}^{\text{appr}}$ (b) r_{sys} and $r_{\text{sys}}^{\text{apprb}}$ (c) r_{sys} and $r_{\text{sys}}^{\text{apprx}}$

Fig. 3: This figure visualizes the actual residuals r_{att} and r_{sys} and the approximated residuals $r_{\text{att}}^{\text{appr}}$, $r_{\text{sys}}^{\text{apprb}}$, and $r_{\text{sys}}^{\text{apprx}}$ when perturbing different branches in the IEEE 14-bus case (transmission system) with $\delta_i = 0$.



(a) r_{att} and $r_{\text{att}}^{\text{appr}}$ (b) r_{sys} and $r_{\text{sys}}^{\text{apprb}}$ (c) r_{sys} and $r_{\text{sys}}^{\text{apprx}}$

Fig. 4: This figure visualizes the actual residuals r_{att} and r_{sys} and the approximated residuals $r_{\text{att}}^{\text{appr}}$, $r_{\text{sys}}^{\text{apprb}}$, and $r_{\text{sys}}^{\text{apprx}}$ when perturbing different branches in the radial 18-bus case (distribution system) with $\delta_i = 0$.

A. *Transformations of Sub-Problem I*

To address the matrix inverse issue in sub-problem I, we deeply investigate the physical meaning behind matrix $I - P_{\boldsymbol{x}_{\text{MTDc}}}^{\text{MTD}*}$, which is named as the *projection matrix* in the field of linear regression [34] as it orthogonally projects vectors onto the subspace $\mathscr{R}_{\boldsymbol{x}}^{\perp}$ that is orthogonal to the image of $H_{\boldsymbol{x}_{\text{MTDc}}}^{\text{MTD}*}$. For convenience, the approximation of $\Delta \boldsymbol{z}_{\text{sys}}$ is omitted, under which (24) can be uniformly described by

$$\max_{\boldsymbol{b}_{\text{MTD}}} \quad \underbrace{\left\| (I - P_{\boldsymbol{x}_{\text{MTDc}}}^{\text{MTD}*}) \times \Delta \boldsymbol{z}_{\text{sys}} \right\|_2^2}_{a^2} \tag{26}$$

$$\Updownarrow$$

$$\max_{\boldsymbol{b}_{\text{MTD}}} \quad \underbrace{\left\| \Delta \boldsymbol{z}_{\text{sys}} \right\|_2^2}_{c^2} - \underbrace{\left\| P_{\boldsymbol{x}_{\text{MTDc}}}^{\text{MTD}*} \times \Delta \boldsymbol{z}_{\text{sys}} \right\|_2^2}_{b^2}, \tag{27}$$

where (27) is an equivalent formation of (26) and the equivalence can be graphically interpreted via a right triangle. Let $(H_{\boldsymbol{x}_{\text{MTDc}}}^{\text{MTD}*})^{\perp} \in \mathbb{R}^{m \times (m-n)}$ be a full column rank matrix and satisfy $(H_{\boldsymbol{x}_{\text{MTDc}}}^{\text{MTD}*})^{\text{T}} (H_{\boldsymbol{x}_{\text{MTDc}}}^{\text{MTD}*})^{\perp} = 0$. Then, the column vectors of matrices $H_{\boldsymbol{x}_{\text{MTDc}}}^{\text{MTD}*}$ and $(H_{\boldsymbol{x}_{\text{MTDc}}}^{\text{MTD}*})^{\perp}$ constitute a basis for the m-dimensional vector space. For any vector $\Delta \boldsymbol{z}_{\text{sys}} \in \mathbb{R}^m$, there exist $\boldsymbol{h}_1 \in \mathbb{R}^n$ and $\boldsymbol{h}_2 \in \mathbb{R}^{m-n}$ such that $\Delta \boldsymbol{z}_{\text{sys}} = H_{\boldsymbol{x}_{\text{MTDc}}}^{\text{MTD}*} \times \boldsymbol{h}_1 + (H_{\boldsymbol{x}_{\text{MTDc}}}^{\text{MTD}*})^{\perp} \times \boldsymbol{h}_2$, whose orthogonal projection onto image of $H_{\boldsymbol{x}_{\text{MTDc}}}^{\text{MTD}*}$ is captured with

$$P_{\boldsymbol{x}_{\text{MTDc}}}^{\text{MTD}*} \times \Delta \boldsymbol{z}_{\text{sys}} = H_{\boldsymbol{x}_{\text{MTDc}}}^{\text{MTD}*} \times \boldsymbol{h}_1. \tag{28}$$

Hence, the three variables a, b, and c can be regarded as the three sides of a right triangle, where a and b are the two sides adjacent to the right angle and c denotes the hypotenuse. The equivalence of (26) $\Leftrightarrow$ (27) is vividly demonstrated in Fig. 5.

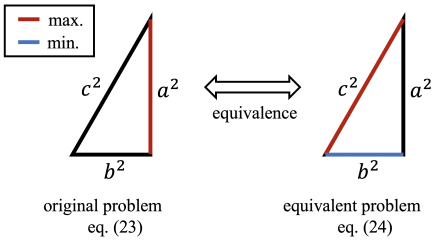


Fig. 5: Graphical illustration of the equivalence (26) $\Leftrightarrow$ (27).

Proposition 2 is established to avert the matrix inverse issue involved in (27), where maximizing $-b^2$ is transformed to maximizing the lower bound.

Proposition 2: Based on matrix norm inequalities, maximizing (27) is transformed to maximizing the lower bound, i.e.,

$$\max_{\boldsymbol{b}_{\text{MTD}}} \quad \left\| \Delta \boldsymbol{z}_{\text{sys}} \right\|_2^2 - \frac{\left\| (H_{\boldsymbol{x}_{\text{MTDc}}}^{\text{MTD}*})^{\text{T}} \times \Delta \boldsymbol{z}_{\text{sys}} \right\|_2^2}{\left(\sigma_{\min}(H_{\boldsymbol{x}_{\text{MTDc}}}^{\text{MTD}*}) \right)^2}, \tag{29}$$

where $\sigma_{\min}(\cdot)$ denotes the minimal singular value function.

Proof: The proof can be found in Appendix B. ■

Remark 2: Due to the existence of $\sigma_{\min}(\cdot)$, it is still challenging to directly solve (29). Fortunately, through numerical simu-

lations, we observe that the impact of reactance perturbation on $\left(\sigma_{\min}(H^{\text{MTD}*}_{\boldsymbol{x}_{\text{MTDc}}})\right)^2$ is neglectable, which may be further utilized to simplify (29). We simulate all scenarios where the reactance of one branch is perturbed with ratio 20%, and the average and maximum relative alterations of $\left(\sigma_{\min}(H^{\text{MTD}*}_{\boldsymbol{x}_{\text{MTDc}}})\right)^2$ under 8 test cases are presented in TABLE III. The average relative alterations are all 0, and the maximum relative alterations are within 3%. Hence, we consider that it is feasible to treat $\left(\sigma_{\min}(H^{\text{MTD}*}_{\boldsymbol{x}_{\text{MTDc}}})\right)^2$ as constant in the presence of MTD when the perturbation magnitude ratio is bounded by 20% and (29) is simplified as

$$\max_{\boldsymbol{b}_{\text{MTD}}} \quad \|\Delta \boldsymbol{z}_{\text{sys}}\|_2^2 - \frac{\left\|(H^{\text{MTD}*}_{\boldsymbol{x}_{\text{MTDc}}})^{\text{T}} \times \Delta \boldsymbol{z}_{\text{sys}}\right\|_2^2}{\left(\sigma_{\min}(H^{*}_{\boldsymbol{x}_{\text{c}}})\right)^2}, \tag{30}$$

where $H^{*}_{\boldsymbol{x}_{\text{c}}} \triangleq \partial \boldsymbol{h}(\boldsymbol{x}^* + \boldsymbol{c})/\partial \boldsymbol{x}$.

TABLE III: Average and Maximum Relative Alterations on $\sigma_{\min}$ [a]

Metrics / Test cases	$\Delta\sigma_{\min}/\sigma_{\min,0}$ [b][c] Avg.	Max.	Metrics / Test cases	$\Delta\sigma_{\min}/\sigma_{\min,0}$ Avg.	Max.
IEEE 14-bus	0[d]	0.09%	Radial 18-bus	0	0.64%
IEEE 57-bus	0	0	Radial 69-bus	0	0.09%
IEEE 118-bus	0	0.09%	Radial 85-bus	0	0.08%
IEEE 300-bus	0	2.33%	Radial 141-bus	0	0.12%

[a] $\left(\sigma_{\min}(H^{\text{MTD}*}_{\boldsymbol{x}_{\text{MTDc}}})\right)^2$ is written as $\sigma_{\min}$ for brevity.
[b] $\Delta\sigma_{\min}$ denotes the absolute alteration on $\sigma_{\min}$ caused by MTD.
[c] $\sigma_{\min,0}$ denotes the $\sigma_{\min}$ in the absence of MTD.
[d] The value is considered to be 0 if it is smaller than 0.0001.

B. Aggregation of Sub-problems

By aggregating sub-problems (25) and (30), we obtain

$$\begin{aligned} \min_{\boldsymbol{b}_{\text{MTD}}} \; & -\|\Delta \boldsymbol{z}_{\text{sys}}\|_2^2 + \frac{\left\|(H^{\text{MTD}*}_{\boldsymbol{x}_{\text{MTDc}}})^{\text{T}} \times \Delta \boldsymbol{z}_{\text{sys}}\right\|_2^2}{\left(\sigma_{\min}(H^{*}_{\boldsymbol{x}_{\text{c}}})\right)^2} + w_{\text{att}} \times \left\|\Delta \boldsymbol{z}_{\text{att}}^{\text{appr}}\right\|_2^2 \\ \text{s.t.} \quad & \boldsymbol{b} + \Delta \underline{\boldsymbol{b}} \le \boldsymbol{b}_{\text{MTD}} \le \boldsymbol{b} + \Delta \overline{\boldsymbol{b}}, \end{aligned} \tag{31}$$

where $w_{\text{att}} \ge 1$ is the weight parameter that should be appropriately chosen to maximize the effectiveness of MTD while guaranteeing the hiddenness [18]. Specifically, a larger w_{att} leads to the designed EXR-MTD possessing stronger hiddenness, and a smaller w_{att} results in the opposite result.

After substituting (19) and (20) into (31), the nonlinear and non-convex optimization problems can be obtained for power distribution and power transmission systems, respectively, which can be treated as the polynomial optimization problems (POPs) and are NP-hard. It is difficult to find the global optimums of the formulated PoPs, and further efforts are still required to develop approximation algorithms to approach them [35], which is left as the future work. In this study, we use the standard *fmincon* solver from Matlab equipped with the interior-point algorithm to solve the PoPs, where different local minimums could be found when started from different initial points. Since the larger perturbation magnitude usually makes the MTD possess stronger effectiveness, we consider the two boundary points, i.e., $\boldsymbol{b} + \Delta \underline{\boldsymbol{b}}$ and $\boldsymbol{b} + \Delta \overline{\boldsymbol{b}}$, as initial points, under which two (local) minimums can be obtained and the one with better performance is chosen as the output.

Finally, we note that the EXR-MTD is dedicated to enhancing the cybersecurity of SE against FDIAs based on the D-FACTS devices that have been installed to branches for the power flow regulation. While the installation of extra D-FACTS devices is not necessary for the implementation of EXR-MTD.

VI. Simulation Results

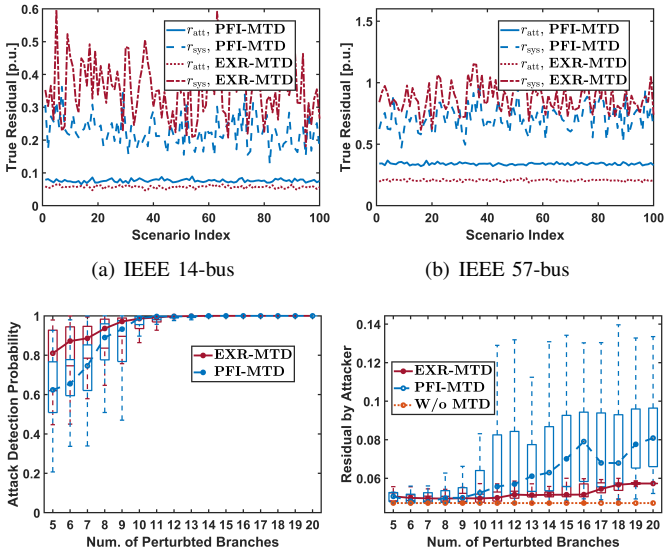
In this section, we conduct extensive simulations on the test cases extracted from MATPOWER to evaluate the performance of EXR-MTD. The standard deviations of real-time measurement noises are considered to be 1% for phasor and magnitude measurements. The pseudo measurement noises are considered to possess 10% standard deviations. The perturbation magnitude ratios are bounded by 20%, under which the power loss variations would be restricted within 1% in a sufficiently large number of perturbation cases [9]. When solving problem (31), the weight parameter w_{att} is set as 100 for power transmission systems and 1 for power distribution systems, and moreover all elements of vector $\boldsymbol{c}$ are set as 0.1. The significance level α utilized in BDD is set as 0.05. For the purpose of practicality, we assume that both the attacker and the system operator adopt the AC power flow model.

A. Performance in Power Transmission Systems

In this subsection, we compare the performance of EXR-MTD with that of PFI-MTD [14], DC-HMTD [18], and AC-HMTD [18]. In particular, the PFI-MTD is to make the power flow invariant in the simplified DC model, and the DC-HMTD and AC-HMTD are to optimize the effectiveness and hiddenness of MTD based on the DC and AC models, respectively.

1) EXR-MTD and PFI-MTD: The PFI-MTD is implemented with the perturbation magnitude ratio of at least one branch reaching 0.2 or -0.2 to maximize the effectiveness. First, when all branches can be perturbed, we depict residuals under EXR-MTD and PFI-MTD, and consider 100 scenarios. In each scenario, we sample each element of $\boldsymbol{c}$ from a uniform distribution $\mathscr{U}(-dm, dm)$ with $dm = 0.1$ being the maximum magnitude of the injected biases into state variables. As shown in (a)-(b) of Fig. 6, compared with PFI-MTD, EXR-MTD can lead to the smaller r_{att}, and moreover under more than 90% scenarios, the larger r_{sys} is induced. Then, we consider the case where only partial branches can be perturbed. According to [14], the number of perturbed branches ranges from 5 to 20 in the IEEE 14-bus case. For each setting, 1000 attacks generated from $\mathscr{U}(-0.1, 0.1)$ are launched, and based on Monte Carlo simulations, the attack detection probability is estimated as $\frac{\text{Num. of detected FDIAs}}{1000}$. Besides, 100 PFI-MTD strategies are randomly selected for each number of perturbed branches, and 100 EXR-MTD strategies are correspondingly designed with the same sets of perturbed branches. As illustrated in (c) of Fig. 6, the attack detection probability becomes higher as the number of perturbed branches increases, and EXR-MTD generally performs better than PFI-MTD in detecting FDI attacks. Additionally, it is observed that PFI-MTD is difficult to maintain hiddenness when the attacker uses the

AC power flow model, as the induced r_{att} is significantly larger than that without MTD. On the contrary, EXR-MTD has the evident advantage in preserving hiddenness since the incurred r_{att} is close to that without MTD. From the above results, it is asserted that EXR-MTD comprehensively performs better than PFI-MTD when the practical AC power flow model is adopted, despite the utilization of approximated residuals.



(a) IEEE 14-bus (b) IEEE 57-bus

(c) IEEE 14-bus

Fig. 6: This figure shows the comparison results between EXR-MTD and PFI-MTD [14] in transmission systems, where (a) and (b) depict the true residuals when all branches can be perturbed, and (c) shows the effectiveness and hiddenness of MTD when the number of perturbed branches increases.

2) EXR-MTD, DC-HMTD, and AC-HMTD: Based on the HMTD planning solutions in IEEE 14-bus and 57-bus cases [18], we solve the optimization problems formulated for EXR-MTD, DC-HMTD, and AC-HMTD and compare the effectiveness and hiddenness of obtained MTD strategies. In particular, the optimization problems are all solved by the standard *fmincon* function from Matlab equipped with the interior-point algorithm, in which the bound of perturbation magnitude ratio varies from 2% to 20%. Moreover, when solving the optimization problems, the initial points are chosen from the two boundary points, i.e., $\boldsymbol{b} + \Delta\underline{\boldsymbol{b}}$ and $\boldsymbol{b} + \Delta\bar{\boldsymbol{b}}$. The results indicate that the effectiveness increases with the growth of the perturbation bound, while the hiddenness continuously decreases. Specifically, the effectiveness of EXR-MTD is slightly weaker than those of DC-HMTD and AC-HMTD when the perturbation bound is smaller than 12.5%, and the attack detection probabilities can all reach 1 if the perturbation bound exceeds 12.5%. Moreover, the hiddenness of EXR-MTD is always stronger than those of DC-HMTD and AC-HMTD. The computation time of solving the three optimization problems in a core i9 computer, which has a 3.6GHz CPU and 32.0G memory, is listed in TABLE IV. In each test case, the problem is solved 100 times, and the average and maximum computation time is demonstrated. It is shown that the computation time of EXR-MTD is longer than that of DC-HMTD and is shorter than that of AC-HMTD.

TABLE IV: Computation Time [s]

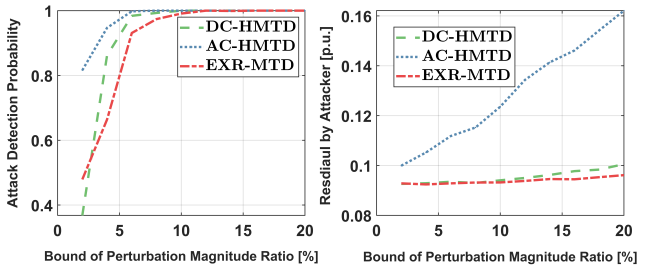
Metrics / Test cases	DC-HMTD		AC-HMTD		EXR-HMTD	
	Avg.	Max.	Avg.	Max.	Avg.	Max.
IEEE 14-bus	0.0260	0.0322	0.8723	1.0983	0.4233	0.5280
IEEE 57-bus	0.2691	0.6282	9.9994	10.205	6.9812	8.0752

Remark 3: Compared with DC-HMTD, the design of EXR-MTD considers the existence of series resistances and charging capacitances at power lines, and adopts sensitivity analysis to linearly approximate the ACPF model and obtain the approximated measurement residuals. Indeed, the approximation error increases with the growth of the perturbation magnitude. Nevertheless, in IEEE 14-bus and 57-bus cases, the average branch ratios R/X are 39.83% and 33.90%, respectively, which are both larger than the maximal perturbation magnitude ratio on branch reactances, i.e., 20%. Intuitively, although the accuracy of the approximated PF model decreases as the increase of the perturbation magnitude, the induced distortions are always smaller than those caused by the neglected branch resistances as in the DCPF model. Hence, the hiddenness of EXR-MTD can be stronger than that of DC-HMTD, and the stronger hiddenness will restrain the perturbation magnitude, under which the effectiveness of EXR-MTD can be slightly weaker than that of DC-HMTD when the perturbation bound is smaller than 12.5%. Once the perturbation bound exceeds 12.5%, the induced residuals will both trigger the attack alarm, and the attack detection probabilities are equal to 1.

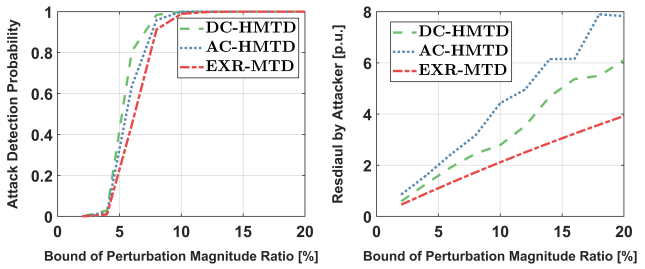
Remark 4: Moreover, since the AC-HMTD directly minimizes the ACPF variations caused by reactance perturbation, more decision variables such as the voltage magnitudes and angles after reactance perturbation are included in the formulated optimization problem. Given a non-convex optimization problem and the solver, the selection of the initial values of decision variables determines how good the attained local minimum is. The increase of the number of decision variables would make the selection of a good initial point more difficult and time-consuming. Thus, when using the voltage magnitudes and angles without reactance perturbation as initial values and adopting the standard solver *fmincon* from Matlab equipped with the interior-point algorithm, the hiddenness of obtained AC-HMTD can be weaker than that of EXR-MTD when the effectiveness of AC-HMTD is comparable to that of EXR-MTD. Furthermore, the increase of the number of decision variables would also enlarge the matrix dimensions involved in the interior-point algorithm when solving the optimization problem, under which the computation time of AC-HMTD can be longer than those of DC-HMTD and EXR-MTD. Moreover, the computation time of DC-HMTD is shorter than that of EXR-MTD as the order of the formulated polynomial optimization problem (PoP) for DC-HMTD (i.e., 2) is smaller than that of EXR-MTD (i.e., 6).

B. Performance in Power Distribution Systems

In this subsection, we investigate the performance of EXR-MTD in power distribution systems. First, we show the resid-

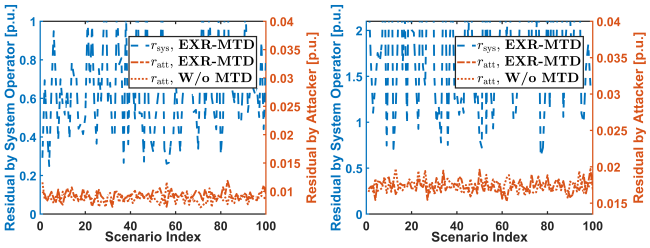


(a) IEEE 14-bus

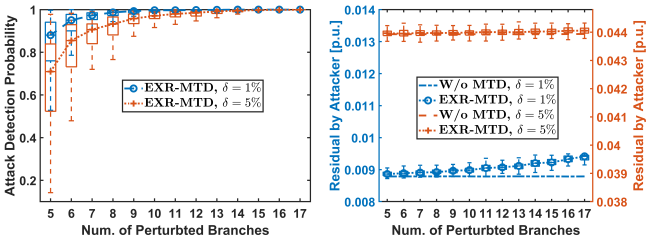


(b) IEEE 57-bus

Fig. 7: This figure compares the effectiveness and hiddenness of EXR-MTD with those of DC-HMTD and AC-HMTD, where (a) and (b) show the results in IEEE 14-bus and 57-bus cases, respectively.



(a) Radial 18-bus (b) Radial 69-bus



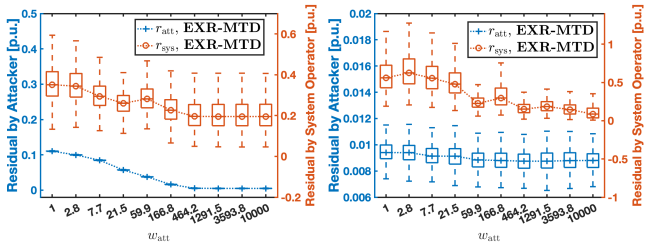
(c) Radial 18-bus

Fig. 8: This figure shows the results of EXR-MTD in power distribution systems, where (a) and (b) depict the true residuals when all branches can be perturbed, and (c) shows the effectiveness and hiddenness of EXR-MTD when the number of perturbed branches and δ_i increase.

uals r_{att} and r_{sys} in radial 18-bus and 69-bus cases, when all branches can be perturbed. The results depicted in (a)-(b) of Fig. 8 indicate that it is hard for the attacker to identify the existence of EXR-MTD as r_{att} is almost invariant after implementing it. Meanwhile, EXR-MTD can effectively expose the FDI attacks constructed with outdated branch parameters to the BDD due to the noticeable improvement of r_{sys}. Then, extensive simulations are conducted in the radial 18-bus case to validate the performance of EXR-MTD when merely partial branches can be perturbed. For each number of perturbed branches, 100 branch sets are randomly selected. Clearly, the attack detection probability increases when more branches are perturbed, i.e., more buses are covered by perturbed branches. In particular, we find that the attack detection probability is around 99% when more than 10 branches are perturbed. If the number of perturbed branches is 5, the attack detection probability can be smaller than 60% as merely 6 buses are covered. It is also worthwhile noting that r_{att} increases as the growth of the number of perturbed branches, but fortunately the discrimination compared with that without EXR-MTD is among 0.001p.u. Furthermore, it is observed that the larger standard deviations of measurement noises will decrease the attack detection probability as a larger detection threshold is required to tolerate the fluctuations caused by measurement noises. Oppositely, the hiddenness of EXR-MTD is improved because more impact of reactance perturbation on r_{att} can be covered by that of measurement noises.

C. Trade-off between Effectiveness and Hiddenness

In this subsection, we show the impact of weight parameter w_{att} on the effectiveness and hiddenness of EXR-MTD, where 10 logarithmically equally spaced points are selected between 10^0 and 10^4 as illustrated in Fig. 9. Evidently, in the IEEE 14-bus case, r_{att} and r_{sys} both decrease as the growth of w_{att}, indicating that w_{att} plays a vital role in balancing the trade-off between the two metrics. Specifically, the larger w_{att} means the stronger hiddenness and the weaker effectiveness of EXR-MTD. Moreover, the same phenomenon appears in the radial 18-bus case except that the variation of r_{att} is within 0.001p.u. Hence, we choose $w_{\text{att}} = 100$ for power transmission systems to guarantee that r_{att} is not too large, and $w_{\text{att}} = 1$ for power distribution systems to maximize r_{sys}.



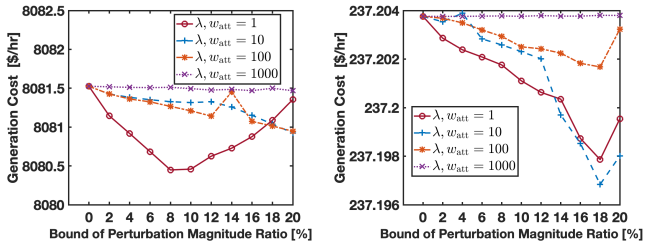
(a) IEEE 14-bus (b) Radial 18-bus

Fig. 9: This figure demonstrates the impact of weight w_{att} on the effectiveness and hiddenness of EXR-MTD.

D. Optimal Power Flow (OPF) Generation Cost

In this subsection, we show the impact of EXR-MTD on the OPF generation cost, where weight parameter w_{att} and the bound of perturbation magnitude ratio vary as shown in Fig. 10. It is noticed that the alteration of OPF generation cost is within 1.5$/hr in the IEEE 14-bus case, and bounded by 0.01$/hr in the radial 18-bus case. Though the OPF generation cost is not directly considered in (31), we observe that the alteration of OPF generation cost is reduced with the growth

of w_{att}, under which the designed EXR-MTD has the stronger hiddenness and the fluctuations of AC power flows caused by MTD is more limited. Hence, to reduce the impact of EXR-MTD on the OPF generation cost, one alternative method is to increase w_{att} when designing EXR-MTD.



(a) IEEE 14-bus (b) Radial 18-bus

Fig. 10: This figure depicts the OPF generation cost under EXR-MTD when weight parameter w_{att} and the bound of perturbation magnitude ratio vary.

E. Computation Time

In this subsection, we evaluate the computation time of solving (31) in the 8 test cases extracted from Matpower when all branches can be perturbed and show the results in TABLE V. Similarly, the problem is solved 100 times in the core i9 computer, and the average and maximum computation time is illustrated. We find that the computation time of designing EXR-MTD in power distribution systems is in the order of seconds and can be neglectable. While the computation time of designing EXR-MTD in power transmission systems increases with the number of buses and can reach at most 12.7 minutes in the IEEE 300-bus test case, which is feasible as the perturbation commands are updated hourly in practice [16].

TABLE V: Computation Time [s]

Metrics / Test cases	Avg.	Max.	Metrics / Test cases	Avg.	Max.
IEEE 14-bus	0.6028	1.0018	Radial 18-bus	0.7928	1.4860
IEEE 57-bus	11.075	13.934	Radial 69-bus	0.6836	1.0854
IEEE 118-bus	88.900	91.533	Radial 85-bus	0.8289	1.3299
IEEE 300-bus	674.32	762.02	Radial 141-bus	4.0657	5.1992

F. Scalability to Large-scale Systems

In this subsection, we test the scalability of EXR-MTD via 4 polish system test cases (including more than 2000 buses) extracted from MATPOWER. When designing EXR-MTD, we assume that all branches are equipped with D-FACTS devices and can be perturbed. The computation time and the performance of obtained EXR-MTD (reflected by r_{att} and r_{sys}) are illustrated in TABLE VI. It is observed that when the weight parameter ω_{att} is appropriately chosen, then the EXR-MTD strategy with strong effectiveness and hiddenness can be quickly obtained, where r_{sys} is significantly larger than r_{att}. Nevertheless, if ω_{att} is not well tuned, then the computation time of solving (31) can exceed 6 hours, which is caused by the operations of large-scale sparse matrices. Hence, in the future work, an efficient and dedicated solver is required to address this issue.

TABLE VI: Results in Polish System Test Cases

Metrics / Test cases	ω_{att}	r_{att} [p.u.]	r_{sys} [p.u.]	Time [s]
Case2383wp	50	2.7520	4.0290	1289.6
Case2737sop	200	1.2409	7.1925	725.38
Case3012wp	1	2.1738	22.892	864.92
Case3120sp	1	2.7163	22.022	980.19

G. Discussions

In this subsection, we discuss the differences when applying EXR-MTD to power transmission and power distribution systems. We find that the EXR-MTD in power distribution systems performs better than that in power transmission systems in terms of hiddenness and effectiveness, which are illustrated individually as follows.

1) Effectiveness: The effectiveness of MTD in detecting FDIAs is directly related to the number of covered buses by perturbed branches [9]. Simply, if there exist buses not covered by perturbed branches, then the FDIAs against these buses can still easily bypass BDD. In Fig. 11, we compare the bus coverage ratios in IEEE 14-bus and radial 18-bus cases. For each number of perturbed branches, EXR-MTD is designed under 100 randomly selected branch sets, and the number of the buses covered by the branches whose perturbation magnitude ratios are larger than 0.1% is counted. The bus coverage ratio is computed via dividing the number of covered buses by the number of total buses excluding the reference bus. It is observed that the bus coverage ratio in the radial 18-bus case is generally larger than that in the IEEE 14-bus case. Hence, when the numbers of the branches equipped with D-FACTS devices are the same, the EXR-MTD in the radial 18-bus case is likely to induce higher attack detection probability as demonstrated by Fig. 6 and Fig. 8. Two reasons are presented to explain the phenomenon. First, the impact of reactance perturbation on r_{att} in power distribution systems is small and even can be neglectable as indicated by TABLE I, and thus more branches can be perturbed therein compared with those in power transmission systems when guaranteeing the same value of r_{att}. Secondly, the *radial* network is also helpful to improve the bus coverage ratio as the same number of branches therein is likely to cover more buses compared with that in the *mesh* network.

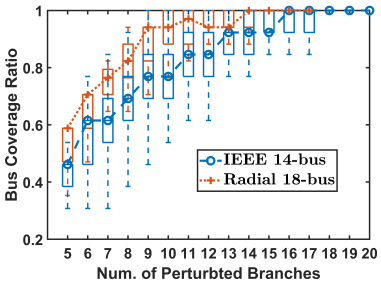


Fig. 11: This picture compares the bus coverage ratios of EXR-MTD in IEEE 14-bus and radial 18-bus cases.

2) Hiddenness: According to Fig. 3 and Fig. 4, the impacts of reactance perturbation on measurement residual r_{att}

in power transmission and power distribution systems are totally different. Specifically, perturbing any single branch in the IEEE 14-bus case (transmission system) is likely to induce $r_{\text{att}} > 0.02$p.u., while $r_{\text{att}} < 0.016$p.u. can be always guaranteed in the radial 18-bus case (distribution system). Moreover, the hiddenness of EXR-MTD behaves similarly in IEEE 14-bus and radial 18-bus cases as indicated by (c) of Fig. 6 and (c) of Fig. 8, respectively. Concretely, the EXR-MTD in the IEEE 14-bus case can improve r_{att} by at least 0.01p.u., while in the radial 18-bus case the increment on r_{att} is bounded by 0.001p.u., which is almost indistinguishable from the impact of measurement noises. The strong hiddenness of EXR-MTD in power distribution systems is due to the small branch ratios X/R, under which the reactance perturbation merely has neglectable impact on the branch impedance.

VII. Conclusion

In this paper, we attempted to conduct an explicit analysis on the MTD performance in AC power systems based on measurement residuals. To handle the nonlinear dynamics, we adopted the sensitivity analysis around the optimum point and derived explicit approximations of residuals, with which we designed EXR-MTD to jointly optimize the effectiveness and hiddenness. Through simulation results, EXR-MTD was shown to have the stronger hiddenness than existing MTD strategies, while the effectiveness is stronger than or comparable to those of existing MTD strategies. It was observed that the impact of EXR-MTD on the OPF generation cost is negligible as the strong hiddenness limits the fluctuations of power flows, and the computation time of EXR-MTD is tolerable even for the polish system test cases that includes more than 2000 buses, both indicating that EXR-MTD has the potential to be applied in real-world power systems. Furthermore, the EXR-MTD in power distribution systems possesses natural hiddenness as the branches usually have small X/R ratios, which means that more metrics are required for the better design of MTD therein besides effectiveness and hiddenness.

Appendix

A. Proof of Proposition 1

Proof: Based on (11), we have

$$J_{\boldsymbol{xx}} d\boldsymbol{x} = -J_{\boldsymbol{xz}} d\boldsymbol{z} - J_{\boldsymbol{xb}} d\boldsymbol{b}, \tag{32a}$$

$$J_{\boldsymbol{x}}^{\mathrm{T}} d\boldsymbol{x} - dJ = -J_{\boldsymbol{z}}^{\mathrm{T}} d\boldsymbol{z} - J_{\boldsymbol{b}}^{\mathrm{T}} d\boldsymbol{b}. \tag{32b}$$

With (32a), we can derive the sensitivities of system states $\boldsymbol{x}$ with respect to $\boldsymbol{z}$ and $\boldsymbol{b}$ as follows

$$\frac{\partial \boldsymbol{x}}{\partial \boldsymbol{z}} = -J_{\boldsymbol{xx}}^{-1} J_{\boldsymbol{xz}}, \tag{33}$$

$$\frac{\partial \boldsymbol{x}}{\partial \boldsymbol{b}} = -J_{\boldsymbol{xx}}^{-1} J_{\boldsymbol{xb}}. \tag{34}$$

It follows from (32b) that

$$\frac{\partial J}{\partial \boldsymbol{z}} = (\frac{\partial \boldsymbol{x}}{\partial \boldsymbol{z}})^{\mathrm{T}} J_{\boldsymbol{x}} + J_{\boldsymbol{z}}. \tag{35}$$

Substituting (33) into (35), we obtain

$$\frac{\partial J}{\partial \boldsymbol{z}} = J_{\boldsymbol{z}} - (J_{\boldsymbol{xx}}^{-1} J_{\boldsymbol{xz}})^{\mathrm{T}} J_{\boldsymbol{x}}. \tag{36}$$

Moreover, the expressions of $J_{\boldsymbol{x}}$, $J_{\boldsymbol{z}}$, and $J_{\boldsymbol{xz}}$ can be derived from (2) as

$$\begin{aligned} &J_{\boldsymbol{x}} = -(H_{\boldsymbol{x}}^*)^{\mathrm{T}} \big[\boldsymbol{z} - \boldsymbol{h}(\boldsymbol{x}^*)\big], \\ &J_{\boldsymbol{z}} = \boldsymbol{z} - \boldsymbol{h}(\boldsymbol{x}^*), \quad J_{\boldsymbol{xz}} = -(H_{\boldsymbol{x}}^*)^{\mathrm{T}}. \end{aligned} \tag{37}$$

Substituting (37) into (36), we have

$$\frac{\partial J}{\partial \boldsymbol{z}} = \big[I - H_{\boldsymbol{x}}^* (J_{\boldsymbol{xx}}^{-1})^{\mathrm{T}} (H_{\boldsymbol{x}}^*)^{\mathrm{T}}\big] \boldsymbol{r}(\boldsymbol{x}^*). \tag{38}$$

With $\boldsymbol{r}(\boldsymbol{x}^*) = \boldsymbol{z} - \boldsymbol{h}(\boldsymbol{x}^*)$, we can derive $\frac{\partial J}{\partial \boldsymbol{z}} = (\frac{\partial \boldsymbol{r}}{\partial \boldsymbol{z}})^{\mathrm{T}} \boldsymbol{r}$. Hence, according to (38), we have

$$\frac{\partial \boldsymbol{r}}{\partial \boldsymbol{z}} = I - H_{\boldsymbol{x}}^* J_{\boldsymbol{xx}}^{-1} (H_{\boldsymbol{x}}^*)^{\mathrm{T}}. \tag{39}$$

Nevertheless, the sensitivities (34) and (39) are still implicit due to the existence of $J_{\boldsymbol{xx}}$ and $J_{\boldsymbol{xt}}$. To this end, we expand $J_{\boldsymbol{xx}}$ and $J_{\boldsymbol{xt}}$ as follows

$$J_{\boldsymbol{xx}} = (H_{\boldsymbol{x}}^*)^{\mathrm{T}} H_{\boldsymbol{x}}^* - \tilde{J}_{\boldsymbol{xx}}, \tag{40}$$

$$J_{\boldsymbol{xt}} = (H_{\boldsymbol{x}}^*)^{\mathrm{T}} H_{\boldsymbol{b}}^* - \tilde{J}_{\boldsymbol{xt}}, \tag{41}$$

where $\tilde{J}_{\boldsymbol{xx}} \in \mathbb{R}^{n*n}$ and its (i,j)th entry is $(\tilde{J}_{\boldsymbol{xx}})_{ij} = \big[\frac{\partial \boldsymbol{h}^2(\boldsymbol{x}^*)}{\partial x_i \partial x_j}\big]^{\mathrm{T}} \boldsymbol{r}(\boldsymbol{x}^*)$, and similarly $\tilde{J}_{\boldsymbol{xt}} \in \mathbb{R}^{n*3L}$ and its (i,j)th entry is $(\tilde{J}_{\boldsymbol{xt}})_{ij} = \big[\frac{\partial \boldsymbol{h}^2(\boldsymbol{x}^*)}{\partial x_i \partial t_j}\big]^{\mathrm{T}} \boldsymbol{r}(\boldsymbol{x}^*)$. If the optimal objective value $J^* = \boldsymbol{r}(\boldsymbol{x}^*)^{\mathrm{T}} \boldsymbol{r}(\boldsymbol{x}^*) \to 0$, then $\boldsymbol{r}(\boldsymbol{x}^*) \to \boldsymbol{0}$ also holds, under which we obtain $J_{\boldsymbol{xx}} \to (H_{\boldsymbol{x}}^*)^{\mathrm{T}} H_{\boldsymbol{x}}^*$ and $J_{\boldsymbol{xt}} \to (H_{\boldsymbol{x}}^*)^{\mathrm{T}} H_{\boldsymbol{b}}^*$. Hence, Proposition 1 is proved by substituting (40) into (34) and (39). ■

B. Proof of Proposition 2

Proof: Following (27) and (28), the length of the side signified by b satisfies

$$b^2 = \big\| H_{\boldsymbol{x}_{\text{MTDc}}}^{\text{MTD}*} \times \boldsymbol{h}_1 \big\|_2^2 .$$

Moreover, with $\Delta \boldsymbol{z}_{\text{sys}} = H_{\boldsymbol{x}_{\text{MTDc}}}^{\text{MTD}*} \times \boldsymbol{h}_1 + (H_{\boldsymbol{x}_{\text{MTDc}}}^{\text{MTD}*})^{\perp} \times \boldsymbol{h}_2$, we have

$$\begin{aligned} &\big\| (H_{\boldsymbol{x}_{\text{MTDc}}}^{\text{MTD}*})^{\mathrm{T}} \times \Delta \boldsymbol{z}_{\text{sys}} \big\|_2^2 = \big\| (H_{\boldsymbol{x}_{\text{MTDc}}}^{\text{MTD}*})^{\mathrm{T}} \times H_{\boldsymbol{x}_{\text{MTDc}}}^{\text{MTD}*} \times \boldsymbol{h}_1 \big\|_2^2 \\ &= (H_{\boldsymbol{x}_{\text{MTDc}}}^{\text{MTD}*} \times \boldsymbol{h}_1)^{\mathrm{T}} \times H_{\boldsymbol{x}_{\text{MTDc}}}^{\text{MTD}*} \times (H_{\boldsymbol{x}_{\text{MTDc}}}^{\text{MTD}*})^{\mathrm{T}} \times H_{\boldsymbol{x}_{\text{MTDc}}}^{\text{MTD}*} \times \boldsymbol{h}_1 \\ &= \sum_{i=1}^{n} \lambda_i \times \alpha_i^2 \times \|\boldsymbol{v}_i\|_2^2 , \end{aligned} \tag{42}$$

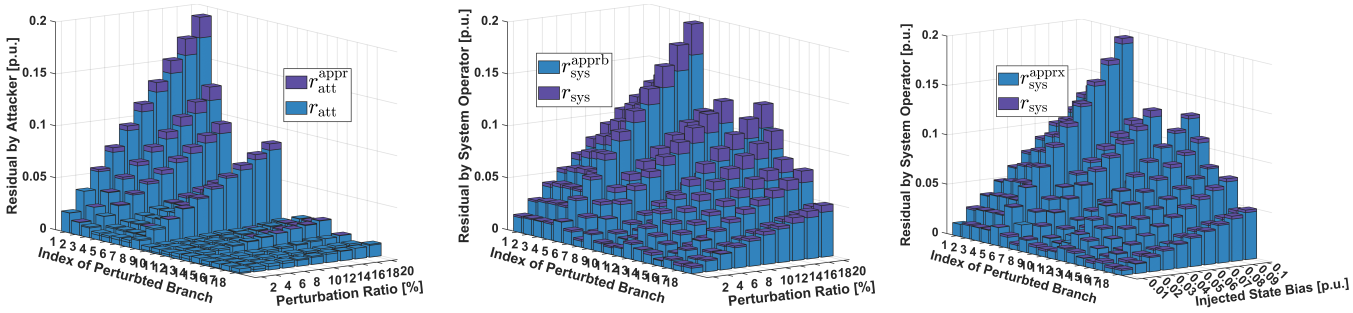
where λ_i and $\boldsymbol{v}_i, \forall i \in \{1, \cdots, n\}$ represent positive eigenvalues and corresponding unit orthogonal eigenvectors of matrix $(H_{\boldsymbol{x}_{\text{MTDc}}}^{\text{MTD}*})^{\mathrm{T}} \times H_{\boldsymbol{x}_{\text{MTDc}}}^{\text{MTD}*}$, respectively. Here eigenvalues are ordered in a non-decreasing manner, and parameters α_i satisfy

$$H_{\boldsymbol{x}_{\text{MTDc}}}^{\text{MTD}*} \times \boldsymbol{h}_1 = \sum_{i=1}^{n} \alpha_i \times \boldsymbol{v}_i .$$

Hence, by replacing all λ_i in (42) with λ_1, we obtain

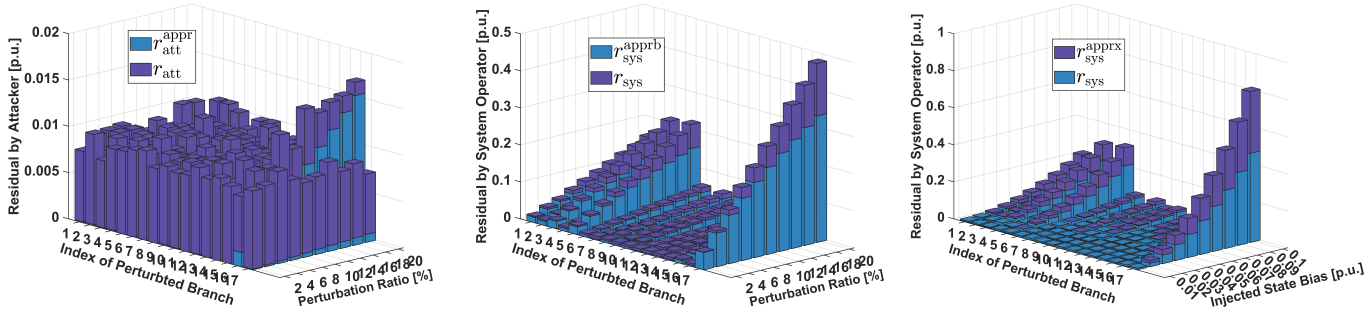
$$\big\| (H_{\boldsymbol{x}_{\text{MTDc}}}^{\text{MTD}*})^{\mathrm{T}} \times \Delta \boldsymbol{z}_{\text{sys}} \big\|_2^2 \geq \lambda_1 \times \sum_{i=1}^{n} \alpha_i^2 = \lambda_1 \times b^2, \tag{43}$$

which is a upper bound of b^2. The result follows after substituting (43) into (27) as $\sigma_{\min}(H_{\boldsymbol{x}_{\text{MTDc}}}^{\text{MTD}*}) = \sqrt{\lambda_1}$. ■



(a) r_{att} and $r_{\text{att}}^{\text{appr}}$ (b) r_{sys} and $r_{\text{sys}}^{\text{apprb}}$ (c) r_{sys} and $r_{\text{sys}}^{\text{apprx}}$

Fig. 12: This figure visualizes the actual residuals r_{att} and r_{sys} and the approximated residuals $r_{\text{att}}^{\text{appr}}$, $r_{\text{sys}}^{\text{apprb}}$, and $r_{\text{sys}}^{\text{apprx}}$ when perturbing different branches in the IEEE 14-bus case (transmission system) with $\delta_i = 5\%$.



(a) r_{att} and $r_{\text{att}}^{\text{appr}}$ (b) r_{sys} and $r_{\text{sys}}^{\text{apprb}}$ (c) r_{sys} and $r_{\text{sys}}^{\text{apprx}}$

Fig. 13: This figure visualizes the actual residuals r_{att} and r_{sys} and the approximated residuals $r_{\text{att}}^{\text{appr}}$, $r_{\text{sys}}^{\text{apprb}}$, and $r_{\text{sys}}^{\text{apprx}}$ when perturbing different branches in the radial 18-bus case (distribution system) with $\delta_i = 5\%$.

C. Details of Residual Approximations in the Presence of Measurement Noises

REFERENCES

[1] T. Seals, "Ransomware attacks hit major utilities," [EB/OL], https://threatpost.com/ransomware-attacks-major-utilities/163687/, Accessed July 23, 2021.

[2] P. Dobson, "Western venezuela rocked by rolling blackouts," [EB/OL], https://venezuelanalysis.com/news/14873/, Accessed July 23, 2021.

[3] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security*, vol. 14, no. 1, p. 13, 2011.

[4] 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.

[5] X. Liu and Z. Li, "False data attacks against AC state estimation with incomplete network information," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2239–2248, 2016.

[6] Z. Zhang, R. Deng, P. Cheng, and M.-Y. Chow, "Strategic protection against FDI attacks with moving target defense in power grids," *IEEE Transactions on Control of Network Systems*, pp. 1–1, 2021.

[7] M. Liu, C. Zhao, Z. Zhang, R. Deng, P. Cheng, and J. Chen, "Converter-based moving target defense against deception attacks in DC microgrids," *IEEE Transactions on Smart Grid*, pp. 1–1, 2021.

[8] D. Divan and H. Johal, "Distributed FACTS-A new concept for realizing grid power flow control," in *IEEE PESC*. IEEE, 2005, pp. 8–14.

[9] 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.

[10] B. Li, G. Xiao, R. Lu, R. Deng, and H. Bao, "On feasibility and limitations of detecting false data injection attacks on power grid state estimation using d-facts devices," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 2, pp. 854–864, 2019.

[11] 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.

[12] B. Liu and H. Wu, "Optimal D-FACTS placement in moving target defense against false data injection attacks," *IEEE Transactions on Smart Grid*, vol. 11, no. 5, pp. 4345–4357, 2020.

[13] S. Lakshminarayana and D. K. Yau, "Cost-benefit analysis of moving-target defense in power grids," *IEEE Transactions on Power Systems*, vol. 36, no. 2, pp. 1152–1163, 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] 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.

[16] 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.

[17] 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.

[18] B. Liu and H. Wu, "Optimal planning and operation of hidden moving target defense for maximal detection effectiveness," *IEEE Transactions on Smart Grid*, vol. 12, no. 5, pp. 4447–4459, 2021.

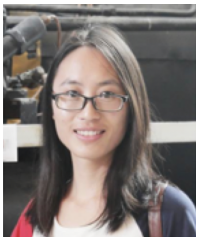
[19] C. Liu, H. Liang, T. Chen, J. Wu, and C. Long, "Joint admittance perturbation and meter protection for mitigating stealthy FDI attacks against power system state estimation," *IEEE Transactions on Power Systems*, vol. 35, no. 2, pp. 1468–1478, 2019.

[20] 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.

[21] 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*, 2018, pp. 1–5.
[22] M. Liu, C. Zhao, Z. Zhang, R. Deng, and P. Cheng, "Analysis of moving target defense in unbalanced and multiphase distribution systems considering voltage stability," *SmartGridComm*, pp. 207–213, 2021.
[23] A. Monticelli, *State estimation in electric power systems: a generalized approach*. Springer Science & Business Media, 2012.
[24] 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.
[25] C. Rakpenthai, S. Premrudeepreechacharn, S. Uatrongjit, and N. R. Watson, "An optimal PMU placement method against measurement loss and branch outage," *IEEE Transactions on Power Delivery*, vol. 22, no. 1, pp. 101–107, 2007.
[26] C. Muscas, M. Pau, P. A. Pegoraro, and S. Sulis, "Effects of measurements and pseudomeasurements correlation in distribution system state estimation," *IEEE Transactions on Instrumentation and Measurement*, vol. 63, no. 12, pp. 2813–2823, 2014.
[27] 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.
[28] K. Madsen, H. B. Nielsen, and O. Tingleff, "Methods for non-linear least squares problems," 2004.
[29] 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.
[30] A. Abur and A. G. Exposito, *Power system state estimation: theory and implementation*. CRC Press, 2004.
[31] 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.
[32] E. Castillo, J. M. Gutiérrez, and A. S. Hadi, "Sensitivity analysis in discrete Bayesian networks," *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, vol. 27, no. 4, pp. 412–423, 1997.
[33] P. A. Garcia, J. L. R. Pereira, S. Carneiro, V. M. Da Costa, and N. Martins, "Three-phase power flow calculations using the current injection method," *IEEE Transactions on Power Systems*, vol. 15, no. 2, pp. 508–514, 2000.
[34] S. Chatterjee and A. S. Hadi, *Sensitivity analysis in linear regression*. John Wiley & Sons, 2009, vol. 327.
[35] Z. Li, S. He, and S. Zhang, *Approximation methods for polynomial optimization: Models, Algorithms, and Applications*. Springer Science & Business Media, 2012.

Mengxiang Liu (S'20) received the B.Sc. degree in automation from Tongji University, Shanghai, in 2017. He is currently pursuing the Ph.D. degree with the College of Control Science and Engineering, Zhejiang University, Hangzhou, China. His research interests include cybersecurity, microgrid, and smart grid.



Chengcheng Zhao (M'18) received the B.Sc. degree in measurement and control technology and instrument from Hunan University, Changsha, China, in 2013 and the Ph.D. degree in control science and engineering from Zhejiang University, Hangzhou, China, in 2018, respectively. She worked as a postdoctoral fellow in the College of Control Science and Engineering, Zhejiang University, from 2018 to 2021. Currently, she is an Associate Researcher in the College of Control Science and Engineering, Zhejiang university. Her research interests include consensus and distributed optimization, distributed energy management and synchronization in smart grids, and security and privacy in networked systems.

Zhenyong Zhang (M'20) received his Ph.D. degree from Zhejiang University, Hangzhou, China, in 2020, and bachelor degree from Central South University, Changsha, China, in 2015. He was a visiting scholar in Singapore University of Technology and Design, Singapore, from 2018 to 2019. Currently, he is a professor in the college of Computer Science and Technology, Guizhou University, Guiyang, China. His research interests include cyber-physical system security, applied cryptography and machine learning security.

Ruilong Deng (S'11-M'14-SM'19) received the B.Sc. and Ph.D. degrees in control science and engineering from Zhejiang University, Hangzhou, China, in 2009 and 2014, respectively. He was a Research Fellow with Nanyang Technological University, Singapore, from 2014 to 2015; an AITF Postdoctoral Fellow with the University of Alberta, Edmonton, AB, Canada, from 2015 to 2018; and an Assistant Professor with Nanyang Technological University, from 2018 to 2019. Currently, he is a Professor with the College of Control Science and Engineering, Zhejiang University, where he is also affiliated with the School of Cyber Science and Technology. He serves/served as Associate Editors for IEEE Transactions on Smart Grid, IEEE Power Engineering Letters, IEEE/CAA Journal of Automatica Sinica, and IEEE/KICS Journal of Communications and Networks, and Guest Editors for IEEE Transactions on Emerging Topics in Computing, IEEE Transactions on Cloud Computing, and IET Cyber-Physical Systems: Theory & Applications. His research interests include cybersecurity, smart grid, and wireless networking.