A Dynamic and Static Combined State Recovery Method Against FDI Attacks in Power Grids

Jiazhou Wang, Jue Tian, Nanpeng Yu, *Senior Member, IEEE*, Yang Liu, *Member, IEEE*, Haichuan Zhang, Yadong Zhou, *Member, IEEE*, and Ting Liu, *Member, IEEE*

***Abstract*—The widespread integration of information technology into power systems increases their vulnerability to false data injection (FDI) attacks, where attackers can mislead the power system state estimator to produce incorrect results. Consequently, it is critical to identify the attack and recover the real system state of the power grid. The primary method of state recovery is to derive the real state from measurements covered by the static measurement protection (SMP) methods, which are expensive to apply. The dynamic reactance perturbation (DRP) methods are low-cost but may fail in some conditions to detect attacks due to the topology limitation. In this paper, we propose a dynamic and static combined defense (DSCD) method, which combines the DRP and SMP methods to identify attacks and enhance the resilience of the state estimator at a lower cost. First, we propose the framework of DSCD and derive the necessary and sufficient conditions for recovering the system state. Second, we develop a non-convex optimization model to implement DSCD and propose heuristic algorithms under two extreme scenarios. Using these algorithms, defenders have the flexibility to balance between cost and delay. Simulation results on four IEEE test systems validated the superior performance of the proposed DSCD method.**

***Index Terms*—False data injection attacks, state recovery, measurement protection, smart grid security, state estimation.**

I. Introduction

As ONE of the most critical infrastructures in modern society, the communication system of smart grids involves an increasing number of Internet-based protocols, increasing their vulnerability to cyber threats and the risks to data integrity. Recent studies have highlighted the menace of false data injection (FDI) attacks on power grids, wherein adversaries can circumvent state estimation (SE) and bad data detection (BDD) systems by deliberately fabricating erroneous electrical measurements [1], [2], [3].

To mount such attacks, the attacker must first obtain the measurement matrix through methods such as subspace estimation [4]. To counter such attacks, scholars have introduced various strategies aimed at safeguarding crucial measurements, thereby impeding the formulation of attacks and strengthening the integrity of data verification processes [5], [6], [7], [8], [9], [10]. The wide deployment of distributed flexible AC transmission system (D-FACTS) devices within the power grid has led to the emergence of the dynamic reactance perturbation (DRP) defense strategy, which has garnered significant interest. DRP methods employ existing D-FACTS devices to nullify the attacker's system knowledge by dynamically perturbing the branch reactance at a low cost [11].

After detecting FDI attacks, it is imperative for system operators to identify FDI attacks and recover the real system state. Recoverability of the system state enables retroactively calculating the real measurements and identifying the injected FDI attacks. Existing static measurement protection (SMP) methods for recovering the system state aim to protect a set of measurements by combining strategies such as encryption, continuous monitoring, separation from the Internet, etc. They then estimate the real system state based on these trusted measurements [5], [6]. However, the feasibility of protecting all necessary measurements in large systems is often hindered by prohibitive costs [12]. Conversely, while the DRP approach is cost-effective, its efficacy in system state recovery is inherently constrained by the system's topology. As described in [13], [14], DRP with one perturbation requires the number of branches to be at least twice the number of states to recover the system state, which is unattainable in most systems. In this paper, we propose a novel dynamic and static combined defense (DSCD) method, which integrates DRP with SMP to identify FDI attacks and recover the system state in any system topology at a lower cost. The main contributions of this paper are as follows:

- We elucidate the shared mechanism underlying DRP and SMP, and propose a framework to combine them as DSCD. We derive the necessary and sufficient conditions for system state recovery via DSCD. The proposed DSCD can recover the system state with any system topology at a lower cost.

Manuscript received 1 December 2023; revised 9 April 2024 and 10 June 2024; accepted 16 June 2024. Date of publication 19 June 2024; date of current version 23 October 2024. This work was supported in part by the National Natural Science Foundation of China under Grant 62293501, Grant 62272373, Grant 62293502, Grant 62003263, and Grant 62002281; in part by the Key Research and Development Program of Shaanxi under Program 2024GX-ZDCYL-02-19; in part by the Science and Technology Project of China Southern Power Grid Corporation under Grant 030000KC23040079 and Grant GDKJXM20230394; in part by the China Postdoctoral Science Foundation under Grant 2020M683520; and in part by the Fundamental Research Funds for the Central Universities. Paper no. TSG-02018-2023. *(Corresponding author: Ting Liu.)*

Jiazhou Wang, Yang Liu, Yadong Zhou, and Ting Liu are with the Ministry of Education Key Lab for Intelligent Networks and Network Security, School of Cyber Science and Engineering, Xi'an Jiaotong University, Xi'an 710049, China (e-mail: wangjiazhou@stu.xjtu.edu.cn; yangliu@xjtu.edu.cn; ydzhou@xjtu.edu.cn; tingliu@mail.xjtu.edu.cn).

Jue Tian is with the School of Computer, Xi'an University of Posts and Telecommunications, Xi'an 710061, China (e-mail: juetian@xupt.edu.cn).

Nanpeng Yu is with the Department of Electrical and Computer Engineering, University of California at Riverside, Riverside, CA 92521 USA (e-mail: nyu@ece.ucr.edu).

Haichuan Zhang is with the School of the Gifted Young, University of Science and Technology of China, Hefei 230026, China (e-mail: zhanghaichuan@mail.ustc.edu.cn).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TSG.2024.3416699.

Digital Object Identifier 10.1109/TSG.2024.3416699

- We construct an optimization model to implement DSCD. Considering the conflict between the cost and delay, we split this non-convex model into two cases, i.e., a delay minimization problem under minimum cost and a cost minimization problem under minimum delay.
- We propose the corresponding algorithms for these two cases, where the defender can tradeoff between delay and cost. Simulation results show that DSCD can accurately identify the FDI attack and recover the system state at a lower cost than existing methods.

The rest of this paper is organized as follows. Section II presents related works. Section III provides the preliminaries. Section IV proposes the framework of DSCD and the state recovery conditions with DSCD. Section V puts forward the implementation strategy of DSCD. Section VI verifies the proposed strategy through numerical simulation, and Section VIII concludes this paper.

II. Related Works

FDI attacks assume the attacker can access the power system's topology and real-time configuration information, enabling them to tamper with the electricity meter's measurement data [1]. Considering the multitude of remote and unattended devices in the power grid, ensuring the security of all transmission branches is impractical [15]. In general, FDI attacks pose a significant threat to the power system's data integrity. This section summarizes the works related to SMP and DRP to illustrate the necessity of our proposed DSCD method.

SMP is the main method for identifying attacks and recovering the real system state. Ideally, SMP safeguards all meter measurements; however, this is impractical for large-scale power systems. A method that identifies a set of protected measurements and verified state variables to prevent the construction of FDI attacks was proposed in [5]. The SMP methods that maximize the minimum attack cost and the average attack cost with a limited protection budget was presented in [16]. To compare scenarios where the costs and benefits of protecting different measurements differ, a metric called "return on investment" (ROI) was proposed in [17], which quantifies the costs and benefits of protecting a set of measurements from the FDIA, and the set of lines with the greatest ROI will be protected. However, securing state estimation results requires protecting as many meters as the system states [12]. Protecting such many meters is costly and time-consuming, especially in large power systems.

Since the stealthiness of FDI attacks closely depends on the prior information of power systems, such as branch reactance and online measurements, active detection strategies based on DRP have been extensively studied [11]. For example, an ex-ante DRP strategy called moving target defense (MTD) was proposed in [18], where the operator can obfuscate the measurement matrix by randomizing the branch reactance with D-FACTS devices. However, this random MTD is impractical due to the need for a more quantitative analysis of its efficiency and cost. To quantify the detection capability of MTD, the rank of composite measurement matrix [14] and the minimal principal angle between the measurement matrices before and after MTD [19] were proposed as design criteria. Based on these analysis, the optimal D-FACTS deployment strategies, which optimize the detection effectiveness with the minimum devices, were discussed in [20], [21] and [22]. The completeness of MTD was discussed in [21], where the number of transmission branches should be no less than twice the number of system states to detect all attacks. The limitation of MTD on detecting FDI attacks that target at some weak buses was analyzed in [15]. The MTD strategy to address the attacks without knowledge of parameters was proposed in [23]. The coordination MTD strategy for consecutive perturbation schemes to enhance the detection capability was proposed in [22]. A real-time robust MTD against FDI attacks was proposed in [24]. The MTD's effectiveness in AC systems was analyzed in [25], and an MTD considering the voltage stability of AC systems was proposed in [26]. An enhancement to MTD for AC state estimation involves coordinated adjustments to both the series reactance and parallel susceptance of lines was proposed in [27]. The MTD against Stuxnet-like attacks was proposed in [28]. The cost-benefit of MTD was analyzed in [19]. A double-benefit MTD against FDI attacks while gaining generation-cost benefits was proposed in [29]. A game theory method to minimize the defense cost while ensuring safety was proposed in [30]. An event-triggered MTD to reduce the cost was proposed in [31]. A multi-stage MTD that maximizes detection capability by performing multiple MTD protocols at minimal cost was proposed in [32]. The meter coding method was integrated with MTD in [33] to improve the detection cost-effectively. An effective and low-cost MTD was developed in [34], and the minimum number of required D-FACTS devices to protect a specific set of buses was also analyzed.

Since smarter attackers may detect the activation of MTD according to the variation of power flow, the hidden MTD (HMTD) that keeps the system power flow after MTD unchanged was discussed in [13], [35]. The optimal planning and operation of HMTD was proposed in [36]. Although the HMTD cannot be perceived by attackers, their detection capabilities are imperfect [13].

In recent years, MTD has also been used to detect FDI attacks in distribution systems. A D-FACTS-based MTD strategy in distribution systems is presented in [37], where the line parameters are perturbed to achieve optimal operating cost while exposing concealed data manipulation attacks. A deeply hidden MTD strategy for the unbalanced AC distribution system was proposed in [38], which elaborately hides each phase's self and mutual reactance at the transmission line installed with D-FACTS devices. A modified matrix completion-based MTD was proposed in [39] to detect attacks in low observable distribution systems. The effectiveness and hiddenness of MTD considering voltage stability in unbalanced and multiphase distribution systems were analyzed in [40].

Though the aforementioned DRP studies can effectively improve the detection capability of the system, recovering the system state via DRP methods like MTD requires the number of branches to be at least twice the number of states, which is not satisfied in most systems [14]. Since both DRP and SMP methods defend against FDI attacks by reducing the attack space for attackers, combining the low-cost DRP and SMP to recover the system state received scholarly attention. A joint admittance perturbation and meter protection method has been proposed in [41], where admittance perturbation was introduced to reduce the cost of state recovery. While this approach offers some cost reduction, it still grapples with constraints imposed by the system's topology. In this paper, we propose a DSCD method that combines DRP and SMP, which recovers the system state with minimum cost.

III. Preliminaries

A. FDI Attacks Against State Estimation

In this paper, we use boldface uppercase (e.g., $\mathbf{H}$) and lowercase (e.g., $\mathbf{x}$) letters to indicate matrices and vectors, respectively. The nonlinear AC model is computationally complex and difficult to converge for large power systems [42]. Thus, a linearized DC model is widely used for state estimation, which ignores transmission branch resistance and assumes identical bus voltage magnitude.

Let $\mathbf{z} = (z_1, z_2, z_3, \dots, z_m)^\mathsf{T}$ denote the measurements on m branches and $\boldsymbol{\theta} = (\theta_1, \theta_2, \theta_3, \dots, \theta_n)^\mathsf{T}$ be the state variables ($n+1$ is the number of buses). In general, $m \geq n$. In DC model, the relation between the measurement data and the state variables is $\mathbf{z} = \mathbf{H}\boldsymbol{\theta} + \mathbf{w}$, where $\mathbf{H} \in \mathbb{R}^{m\times n}$ is the measurement matrix and $\mathbf{w} \in \mathbb{R}^m$ is the vector of measurement noises. The matrix is generally full rank, i.e., $rank(\mathbf{H}) = n$. If the measurement noises are independent and identically distributed Gaussian variables, the system state is estimated by $\hat{\boldsymbol{\theta}} = (\mathbf{H}^\mathsf{T}\mathbf{R}^{-1}\mathbf{H})^{-1}\mathbf{H}^\mathsf{T}\mathbf{R}^{-1}\mathbf{z}$ [43]. $\mathbf{R} = diag(\sigma_1^{-2}, \sigma_2^{-2}, \dots, \sigma_m^{-2})$ is the covariance matrix of $\mathbf{w}$, where σ_i represents the standard deviation of $\mathbf{w}_i$.

BDD compares the 2-norm estimation residual $r = \|\mathbf{z} - \mathbf{H}\hat{\boldsymbol{\theta}}\|_2$ with the pre-determined threshold η to determine whether the system has erroneous data. Specifically, BDD yields a positive detection result if $r > \eta$. Assume that the attacker tampers with the system measurement as $\mathbf{z}^a$ in an FDI attack, i.e., $\mathbf{z}^a = \mathbf{z}+\mathbf{a}$, where $\mathbf{z}^a \in \mathbb{R}^m$ and $\mathbf{a} \in \mathbb{R}^m$. The attack can bypass BDD if the attack vector $\mathbf{a}$ satisfies $\mathbf{a} = \mathbf{Hc}$, where $\mathbf{c} \in \mathbb{R}^n$ is an arbitrary vector [1]. In other words, $\mathbf{a} \in \mathrm{col}(\mathbf{H})$, where col $(\cdot)$ represents the column space of a matrix.

B. Dynamic Reactance Perturbation With D-FACTS

The DRP method modifies the system's measurement matrix by perturbing the branch reactance dynamically with D-FACTS devices. For a transmission branch l, we have $z_l = -b_l(\theta_{l,f} - \theta_{l,t}) + w_l$, where $\theta_{l,f}$ and $\theta_{l,t}$ are the state variables of the *from* and *to* buses of branch l, respectively; b_l is the susceptance of branch l; z_l is the measurement value of power flow of branch l, and w_l is the measurement noise of z_l. Therefore, the row vector corresponding to branch l in the measurement matrix $\mathbf{H}$ (denoted as $\mathbf{H}_{l\cdot}$) is [13]:

$$\mathbf{H}_{l\cdot} = \begin{bmatrix} 0 \dots 0 & \underbrace{-b_l}_{l,f \text{ column}} & 0 \dots 0 & \underbrace{b_l}_{l,t \text{ column}} & 0 \dots 0 \end{bmatrix}. \tag{1}$$

Denote the system's incidence matrix as $\mathbf{A} \in \mathbb{R}^{(n+1)\times m}$. In a fully measured system, $\mathbf{H}$ can be obtained as:

$$\mathbf{H} = \mathbf{X}^{-1} \cdot \mathbf{A}_{-r}^\mathsf{T}, \tag{2}$$

where $\mathbf{X} = diag(x_1, x_2, \dots, x_m)$ is a diagonal reactance matrix, $\mathbf{A}_{-r} \in \mathbb{R}^{n\times m}$ is a sub-matrix of $\mathbf{A}$, including all rows in $\mathbf{A}$ except the row corresponding to the reference bus. Now, we can modify $\mathbf{H}$ to $\mathbf{H}'$ by perturbing the transmission branches' reactance. The defender can detect the highly structured FDI attacks $\mathbf{a} = \mathbf{Hc}$ with the new measurement matrix $\mathbf{H}'$.

Specifically, if the reactance of branch l, x_l, is modified by D-FACTS devices to x_l', where x_l' is a value within its physical limit (usually $\pm 20\%$ [44]), the measurement matrix $\mathbf{H}$ becomes $\mathbf{H}'$. If the attack vector $\mathbf{a} = \mathbf{Hc}$ cannot be detected after DRP, there must be $\mathbf{a} \in \mathrm{col}(\mathbf{H}) \bigcap \mathrm{col}(\mathbf{H}')$ [13]. In other words, if there is no $\mathbf{c}'$ that satisfies $\mathbf{a} = \mathbf{Hc} = \mathbf{H}'\mathbf{c}'$, $\mathbf{a}$ can be detected by BDD. Then, the rank of the composite matrix $\mathbf{M} = [\mathbf{H}\ \mathbf{H}']$ can be used to characterize the detection capability of DRP, where $\mathbf{M} \in \mathbb{R}^{m\times 2n}$. The detection capability increases as $rank(\mathbf{M})$ increases.

C. Static Measurement Protection

The static measurement protection (SMP) method against FDI attacks has been proposed in [5], where an attacker cannot modify a measurement when it is protected. Suppose the set of protected measurements is $\mathbb{P}$. For an FDI attack $\mathbf{a} = \mathbf{Hc}$, we have $\mathbf{a}_\mathbb{P} = \mathbf{0}$, where $\mathbf{a}_\mathbb{P}$ is the attack vector injected in $\mathbb{P}$. Let $\mathbf{H}_\mathbb{P}$ be the matrix formed by rows of $\mathbf{H}$ corresponding to $\mathbb{P}$; we can get the necessary and sufficient conditions for recovering the system state under measurement protection as [5]:

$$rank(\mathbf{H}_\mathbb{P}) = n. \tag{3}$$

This means that at least n measurements need protection to recover the real system state, and these n measurements are linearly independent of each other. Such a set of measurements can be derived from a set of tree branches or measurements at each bus in the system [5].

IV. Dynamic and Static Combined Defense for State Recovery

In this section, we propose the DSCD for state recovery. We first present how to unify DRP and SMP into the comprehensive framework for DSCD. Based on this framework, we further derive the necessary and sufficient conditions for recovering the system state.

A. DSCD Framework

In this subsection, we present the DSCD framework and analyze its impact on FDI attacks. The measurements on buses can be expressed as linear combinations of the measurements

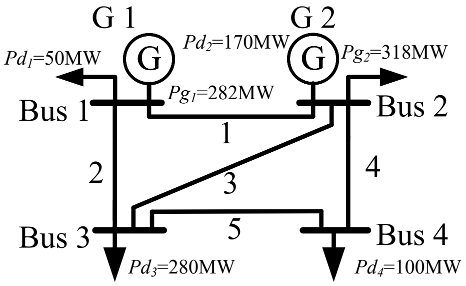


Fig. 1. A 4-bus system.

on branches, while the measurements on branches cannot be obtained directly from the measurements on the buses. To explain the structure of DSCD intuitively, we only consider measurements on branches in this paper.

For a DC system, suppose $\mathbf{X}_0$ is the diagonal reactance matrix before DSCD, where the measurement matrix $\mathbf{H}_0 = \mathbf{X}_0^{-1} \cdot \mathbf{A}_{-r}^{\mathsf{T}}$. Let the loop matrix of the system be $\mathbf{C}$, where $\mathbf{C} \in \mathbb{R}^{(m-n)\times m}$. The i-th row of $\mathbf{C}$ represents a fundamental loop C_i of the system, where $i = 1, \dots, m-n$. The l-th column of $\mathbf{C}$ represents line l of the system, where $l = 1, \dots, m$. We have $|\mathbf{C}_{il}| = \begin{cases} 0, & l \notin C_i \\ \pm 1, & l \in C_i \end{cases}$. Specifically, $\mathbf{C}_{il} = 1$ when $l \in C_i$ and the power flow in l is in the same direction as C_i; $\mathbf{C}_{il} = -1$ when $l \in C_i$ and the line flow in l is in the inverse direction as C_i. For the incidence matrix $\mathbf{A}$ and loop matrix $\mathbf{C}$ of the system, $\mathbf{A}\mathbf{C}^{\mathsf{T}} = \mathbf{C}\mathbf{A}^{\mathsf{T}} = \mathbf{0}$ always holds [45]. The system's circuit basis matrix can be derived as $\mathbf{F}_0 = \mathbf{C}\mathbf{X}_0$. For example, Fig. 1 shows a 4-bus system, where bus 1 is the reference bus. The line reactance profile in per unit form is $x_1 = 0.0504$, $x_2 = 0.0572$, $x_3 = 0.0636$, $x_4 = 0.0595$, $x_5 = 0.0612$. The 4-bus system contains two fundamental loops, and the loop matrix and the circuit basis matrix can be derived as:

$$\mathbf{C} = \begin{bmatrix} 1 & -1 & 1 & 0 & 0 \\ -1 & 1 & 0 & -1 & 1 \end{bmatrix},$$

$$\mathbf{F}_0 = \begin{bmatrix} 0.0504 & -0.0572 & 0.0636 & 0 & 0 \\ -0.0504 & 0.0572 & 0 & -0.0595 & 0.0612 \end{bmatrix},$$

where each column of $\mathbf{C}$ and $\mathbf{F}$ corresponds to a branch of the system. $\mathbf{F}_0\mathbf{H}_0 = \mathbf{X}_0^{-1}\mathbf{X}_0\mathbf{C}\mathbf{A}_{-r}^{\mathsf{T}} = \mathbf{0}$. Thus, for any FDI attack $\mathbf{a} = \mathbf{H}_0\mathbf{c}$, $\mathbf{F}_0\mathbf{a} = \mathbf{0}$ holds.

Since $\mathbf{F}_0 \in \mathbb{R}^{(m-n)\times m}$, the initial dimension of the attack space (DoA) is n. Suppose the set of protected measurements in SMP is $\mathbb{P}$, where the attacker cannot modify the measurements in $\mathbb{P}$. Then we have:

$$\mathbf{a}_{\mathbb{P}} = (\mathbf{H}_0\mathbf{c})_{\mathbb{P}} = \mathbf{0}, \tag{4}$$

where $\mathbb{P}$ is the set of protected measurements.

Denote $\mathbf{I} \in \mathbb{R}^m$ as the unit diagonal matrix, and $\mathbf{I}_{\mathbb{P}}$ is the submatrix formed by rows corresponding to $\mathbb{P}$ in $\mathbf{I}$. (4) can be transformed into:

$$\mathbf{I}_{\mathbb{P}}\mathbf{a} = \mathbf{0}. \tag{5}$$

In other words, a stealthy FDI attack after SMP must satisfy

$$\begin{bmatrix} \mathbf{F}_0 \\ \mathbf{I}_{\mathbb{P}} \end{bmatrix} \mathbf{a} = \mathbf{0}. \tag{6}$$

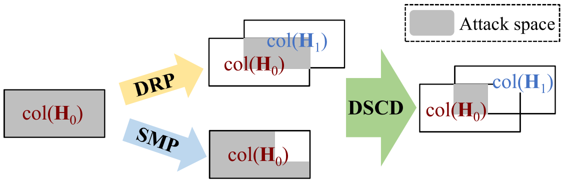


Fig. 2. Variation of the attack space in a DSCD.

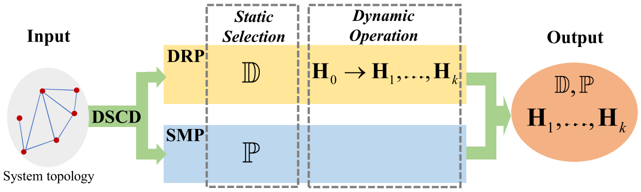


Fig. 3. Framework of the DSCD.

Next, we discuss the role of the DRP. Suppose the DRP modifies the system measurement matrix to $\mathbf{H}_1$ after a branch reactance perturbation and the attack $\mathbf{a} = \mathbf{H}_0\mathbf{c}$ is still undetectable, there must have $\mathbf{a} \in \text{col}(\mathbf{H}_0) \bigcap \text{col}(\mathbf{H}_1)$. We can obtain $\mathbf{F}_1$ from $\mathbf{H}_1$, and the undetectable attack after DRP needs to satisfy $\begin{bmatrix} \mathbf{F}_0 \\ \mathbf{F}_1 \end{bmatrix} \mathbf{a} = \mathbf{0}$.

Assuming that we execute k branch reactance perturbations in the DRP, the corresponding measurement matrices and circuit basis matrices after k branch reactance perturbations are $\mathbf{H}_1, \dots, \mathbf{H}_k$ and $\mathbf{F}_1, \dots, \mathbf{F}_k$, respectively. A stealthy FDI attack after DRP must satisfy $\mathbf{a} \in \text{col}(\mathbf{H}_0) \bigcap \dots \bigcap \text{col}(\mathbf{H}_k)$, where the attack space is $\text{col}(\mathbf{H}_0) \bigcap \dots \bigcap \text{col}(\mathbf{H}_k)$. Let $\mathbf{L}_k = \left[\mathbf{F}_0^{\mathsf{T}}\ \mathbf{F}_1^{\mathsf{T}}\ \dots\ \mathbf{F}_k^{\mathsf{T}}\right]^{\mathsf{T}}$, we have $\mathbf{F}_0\mathbf{a} = \mathbf{F}_1\mathbf{a} = \dots = \mathbf{F}_k\mathbf{a} = \mathbf{0}$, $\mathbf{L}_k\mathbf{a} = \mathbf{0}$, i.e., $\mathbf{a} \in \ker(\mathbf{L}_k)$. Similarly, if $\mathbf{a} \in \ker(\mathbf{L}_k)$, then $\mathbf{L}_k\mathbf{a} = \mathbf{0}$. We further get $\mathbf{F}_0\mathbf{a} = \mathbf{F}_1\mathbf{a} = \dots = \mathbf{F}_k\mathbf{a} = \mathbf{0}$, i.e., $\mathbf{a} \in \text{col}(\mathbf{H}_0) \bigcap \dots \bigcap \text{col}(\mathbf{H}_k)$. Therefore, we can obtain:

$$\text{col}(\mathbf{H}_0) \bigcap \dots \bigcap \text{col}(\mathbf{H}_{\text{k}}) = \ker(\mathbf{L}_{\text{k}}). \tag{7}$$

Thus, an undetectable FDI attack after the DRP with k perturbations must satisfy $\mathbf{a} \in \text{col}(\mathbf{H}_0) \bigcap \dots \bigcap \text{col}(\mathbf{H}_k)$, i.e., $\mathbf{L}_k\mathbf{a} = \mathbf{0}$. The DoA decreases with the increase of $rank(\mathbf{L}_k)$.

Overall, as shown in Fig. 2, both SMP and DRP improve the accuracy of power system state estimation by reducing the DoA. It is meaningful to combine these two approaches to defend against FDI attacks. Since an FDI attack that remains undetectable after DSCD must be in the zero space of both $\mathbf{L}_k$ and $\mathbf{I}_{\mathbb{P}}$, We can obtain Lemma 1 as follows:

Lemma 1: A stealthy FDI attack after DSCD must satisfy $\begin{bmatrix} \mathbf{L}_k \\ \mathbf{I}_{\mathbb{P}} \end{bmatrix} \mathbf{a} = \mathbf{0}$.

Proof: According to the analysis of (7), if an FDI attack $\mathbf{a}$ is still undetectable after the DSCD with k perturbations, it must satisfy $\mathbf{a} \in \text{col}(\mathbf{H}_0) \bigcap \dots \bigcap \text{col}(\mathbf{H}_k)$. When the measurements in $\mathbb{P}$ cannot be modified by the attacker, $\mathbf{I}_{\mathbb{P}}\mathbf{a} = \mathbf{0}$. If $[\begin{smallmatrix} \mathbf{L}_k \\ \mathbf{I}_{\mathbb{P}} \end{smallmatrix}]\mathbf{a} \neq \mathbf{0}$, there must be $\mathbf{a} \notin \text{col}(\mathbf{H}_0) \bigcap \dots \bigcap \text{col}(\mathbf{H}_k)$ or $\mathbf{I}_{\mathbb{P}}\mathbf{a} \neq \mathbf{0}$, which contradicts the known conditions. ■

The framework of DSCD is shown in Fig. 3, which includes a static selection stage and a dynamic operation stage. The static selection stage determines the measurements to be protected ($\mathbb{P}$) in SMP and the branches to be perturbed ($\mathbb{D}$) in DRP according to the topology. The dynamic operation stage determines the specific branch reactance perturbation schemes ($\mathbf{H}_1, \ldots, \mathbf{H}_k$) of DRP. The final output of DSCD includes the static selection result ($\mathbb{D}$, $\mathbb{P}$) and the dynamic perturbation schemes ($\mathbf{H}_1, \ldots, \mathbf{H}_k$). Since the attacker usually has limited resources and access to meters, they can hardly realize the changes in the measurement matrix at first time [1]. Therefore, we assume that the attacker does not change the attack strategy during DRP, i.e., the attack vector still satisfies $\mathbf{a} = \mathbf{H}_0\mathbf{c}$ within DRP [41].

B. Conditions of State Recovery With DSCD

In this subsection, we derive the conditions for recovering the system state through DSCD. In general, power systems keep redundant measurements to ensure state estimation accuracy. The capability to obtain the system state from impaired measurements is related to system observability, typically analyzed in the noiseless environment [46]. If the system state can be recovered in a noiseless environment, it can be generalized to a noisy environment.

In the noiseless environment, when the system is not attacked, the system satisfies $\mathbf{z}_0 = \mathbf{H}_0\boldsymbol{\theta}_0$, where $\mathbf{H}_0$ has full column rank. The state value $\boldsymbol{\theta}_0$ can be uniquely determined from the measurement $\mathbf{z}_0$. When an attacker injects an FDI attack $\mathbf{a} = \mathbf{H}_0\mathbf{c}$, the measurement is modified from $\mathbf{z}_0$ to $\mathbf{z}_0^a$. We have $\mathbf{z}_0^a = \mathbf{H}_0(\boldsymbol{\theta}_0 + \mathbf{c})$, $\mathbf{c} \neq \mathbf{0}$. At this time, the false state value $\boldsymbol{\theta}_0 + \mathbf{c}$ can be uniquely solved from the modified measurement $\mathbf{z}^a$, but the real state value $\boldsymbol{\theta}_0$ cannot be separated. This is because there are infinitely many sets of $\boldsymbol{\theta}'$ and $\mathbf{c}'$ that satisfy $\boldsymbol{\theta}_0 + \mathbf{c} = \boldsymbol{\theta}' + \mathbf{c}'$. To obtain the real system state $\boldsymbol{\theta}_0$, we must identify and isolate the attack $\mathbf{a}$ at first. After the DSCD with one perturbation in DRP, we have:

$$\mathbf{z}_1^a = \mathbf{z}_1 + \mathbf{a} = \mathbf{H}_1\boldsymbol{\theta}_1 + \mathbf{H}_0\mathbf{c} \text{ and } (\mathbf{H}_0\mathbf{c})_{\mathbb{P}} = \mathbf{0}, \tag{8}$$

where $\mathbb{P}$ is the set of protected measurements. If the system state is recoverable, for any $\boldsymbol{\theta}_1, \boldsymbol{\theta}_1', \mathbf{c}'$, the following equation holds:

$$\mathbf{H}_1\boldsymbol{\theta}_1 + \mathbf{H}_0\mathbf{c} \neq \mathbf{H}_1\boldsymbol{\theta}_1' + \mathbf{H}_0\mathbf{c}'. \tag{9}$$

Thus, we can obtain the definition of state recovery as follows:

Definition 1: Under a DSCD with k perturbation, the system state can be recovered after an FDI attack of $\mathbf{a} = \mathbf{H}_0\mathbf{c}, \mathbf{c} \neq \mathbf{0}$, if and only if for any $\boldsymbol{\theta}_1, \ldots, \boldsymbol{\theta}_k, \boldsymbol{\theta}_1', \ldots, \boldsymbol{\theta}_k', \mathbf{c}'$, the following equation holds:

$$\sum_{i=1}^{k} \mathbf{H}_i\boldsymbol{\theta}_i + \mathbf{H}_0\mathbf{c} \neq \sum_{i=1}^{k} \mathbf{H}_i\boldsymbol{\theta}_i' + \mathbf{H}_0\mathbf{c}', \tag{10}$$

where $(\mathbf{H}_0\mathbf{c})_{\mathbb{P}} = \mathbf{0}$. Note that the attack vector $\mathbf{a}$ remains unchanged during DSCD as analyzed in Section IV-A.

Based on Definition 1, we can further obtain Theorem 1.

Theorem 1: The system state is recoverable if and only if there exists k such that $rank\left(\begin{bmatrix}\mathbf{L}_k \\ \mathbf{I}_{\mathbb{P}}\end{bmatrix}\right) = m$.

Proof: (Sufficiency): Suppose there exists a undetectable attack $\mathbf{a} = \mathbf{H}_0\mathbf{c}, \mathbf{c} \neq \mathbf{0}$ after the DSCD with k perturbations, there must be $\mathbf{c}_1, \ldots, \mathbf{c}_k \neq \mathbf{0}$ that satisfy $\mathbf{a} = \mathbf{H}_0\mathbf{c} = \mathbf{H}_1\mathbf{c}_1 = \ldots = \mathbf{H}_k\mathbf{c}_k$. Thus, we have:

$$\begin{cases} \mathbf{H}_1\mathbf{c}_1 - \mathbf{H}_0\mathbf{c} = \mathbf{0} \\ \mathbf{H}_2\mathbf{c}_2 - \mathbf{H}_0\mathbf{c} = \mathbf{0} \\ \qquad\vdots \\ \mathbf{H}_k\mathbf{c}_k - \mathbf{H}_0\mathbf{c} = \mathbf{0} \end{cases}. \tag{11}$$

According to (5), we have:

$$\begin{bmatrix} \mathbf{H}_1 & 0 & \cdots & 0 & -\mathbf{H}_0 \\ 0 & \mathbf{H}_2 & \cdots & 0 & -\mathbf{H}_0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & \mathbf{H}_k & -\mathbf{H}_0 \\ 0 & 0 & \cdots & 0 & -\mathbf{H}_{0,\mathbb{P}} \end{bmatrix} \begin{bmatrix} \mathbf{c}_1 \\ \mathbf{c}_2 \\ \vdots \\ \mathbf{c}_k \\ \mathbf{c} \end{bmatrix} = \mathbf{0}. \tag{12}$$

When $rank\left(\begin{bmatrix}\mathbf{L}_k \\ \mathbf{I}_{\mathbb{P}}\end{bmatrix}\right) = m$, the DoA is zero, indicating no undetectable attack in the system. Thus, (12) only has zero solution, and the coefficient matrix (denoted as $\mathbf{H}^{\#}$) is full column rank. Suppose the real measurements and states after each perturbation can be described as $\mathbf{z}_1 = \mathbf{H}_1\boldsymbol{\theta}_1, \mathbf{z}_2 = \mathbf{H}_2\boldsymbol{\theta}_2, \ldots, \mathbf{z}_k = \mathbf{H}_k\boldsymbol{\theta}_k$, the attacked measurements after each perturbation are:

$$\begin{cases} \mathbf{z}_1^a = \mathbf{z}_1 + \mathbf{a} = \mathbf{H}_1\boldsymbol{\theta}_1 + \mathbf{H}_0\mathbf{c} \\ \mathbf{z}_2^a = \mathbf{z}_2 + \mathbf{a} = \mathbf{H}_2\boldsymbol{\theta}_2 + \mathbf{H}_0\mathbf{c} \\ \quad\vdots \\ \mathbf{z}_k^a = \mathbf{z}_k + \mathbf{a} = \mathbf{H}_k\boldsymbol{\theta}_k + \mathbf{H}_0\mathbf{c} \end{cases}. \tag{13}$$

Based on (5), we have:

$$\begin{bmatrix} \mathbf{z}_1^a \\ \mathbf{z}_2^a \\ \vdots \\ \mathbf{z}_k^a \\ \mathbf{0} \end{bmatrix} = \begin{bmatrix} \mathbf{H}_1 & 0 & \cdots & 0 & \mathbf{H}_0 \\ 0 & \mathbf{H}_2 & \cdots & 0 & \mathbf{H}_0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & \mathbf{H}_k & \mathbf{H}_0 \\ 0 & 0 & \cdots & 0 & \mathbf{H}_{0,\mathbb{P}} \end{bmatrix} \begin{bmatrix} \boldsymbol{\theta}_1 \\ \boldsymbol{\theta}_2 \\ \vdots \\ \boldsymbol{\theta}_k \\ \mathbf{c} \end{bmatrix}. \tag{14}$$

Denote the coefficient matrix in (14) as $\mathbf{H}^*$, there must be $rank(\mathbf{H}^*) = rank(\mathbf{H}^{\#})$. Then, (14) only has one unique solution $[\boldsymbol{\theta}_1\ \boldsymbol{\theta}_2 \cdots \boldsymbol{\theta}_k\ \mathbf{c}]^{\mathsf{T}}$. Thus, the attack vector is separable, and the system state is recoverable.

Necessity: When the state is recoverable after the DSCD with k perturbations, (14) only has one unique solution and $rank(\mathbf{H}^*) = (k+1)n$, i.e., $\mathbf{H}^*$ has full column rank. Since $rank(\mathbf{H}^*) = rank(\mathbf{H}^{\#})$, $\mathbf{H}^{\#}$ also has full column rank. Then, (12) only has zero solution, indicating that all FDI attacks are detectable. In other words, $rank\left(\begin{bmatrix}\mathbf{L}_k \\ \mathbf{I}_{\mathbb{P}}\end{bmatrix}\right) = m$. ■

The method of deriving the true state of the system is shown in the proof of Theorem 1. When $\mathbf{H}^*$ has full column rank, (14) only has one unique solution $[\boldsymbol{\theta}_1\ \boldsymbol{\theta}_2 \cdots \boldsymbol{\theta}_k\ \mathbf{c}]^{\mathsf{T}}$. Then, the attack vector can be derived as $\mathbf{a} = \mathbf{H}_0\mathbf{c}$, and the real system state $\boldsymbol{\theta}_0$ can be obtained according to $\mathbf{z}_0^a = \mathbf{H}_0\boldsymbol{\theta}_0 + \mathbf{a}$. In addition, the state recovery condition can be derived as Theorem 2.

Theorem 2: The system state is recoverable only if $\mathbb{P} \bigcup \mathbb{D}$ contains a spanning tree of the system.

Proof: The system's circuit basis matrix $\mathbf{F}_0 = \mathbf{C}\mathbf{X}_0$. Each row of the loop matrix $\mathbf{C}$ corresponds to a fundamental loop of the system, formed by adding an edge to a spanning tree

$\mathbb{T}$. The loop corresponding to each row has a unique edge, which belongs to the cotree $\bar{\mathbb{T}}$ corresponding to the tree $\mathbb{T}$ [45]. The Hermite Normal form of the loop matrix $\mathbf{C}$ is $[\mathbf{C}_{\bar{\mathbb{T}}}\ \mathbf{C}_{\mathbb{T}}]$, where $\mathbf{C}_{\bar{\mathbb{T}}} \in \mathbb{R}^{(m-n)\times(m-n)}$ is a diagonal matrix representing the cotree part and $\mathbf{C}_{\mathbb{T}} \in \mathbb{R}^{(m-n)\times n}$ is the tree part [47]. Obviously, $rank(\mathbf{C}) = m - n$. Suppose only the reactance of branch k is modified in the k-th perturbation as:

$$x_{k,l} = \begin{cases} (1+\delta_k)x_{0,l}, & l = k \\ x_{0,l}, & l \neq k \end{cases},$$

where $\delta_k \neq 0$. Then a row vector $[0 \ldots \delta_k x_{0,k} \ldots 0]$ can be obtained by $\mathbf{F}_k - \mathbf{F}_0$. If k does not belong to $\bar{\mathbb{T}}$, then the DRP introduces a row vector that is linearly independent of $\mathbf{F}_0$. The effect of the SMP is the same as that of the DRP. When the system state is recoverable, $rank\left(\begin{bmatrix}\mathbf{L}_k \\ \mathbf{I}_{\mathbb{P}}\end{bmatrix}\right) = m$, which requires at least n row vectors that are linearly independent of $\mathbf{F}_0$. And the pivot positions of these row vectors are the spanning tree $\mathbb{T}$ corresponding to $\bar{\mathbb{T}}$ [48]. Thus, $\mathbb{P} \bigcup \mathbb{D}$ must contain a spanning tree of the system. ■

V. Implementation of DSCD

In this section, we establish an implementation model for DSCD, which considers both the cost and the delay due to multiple reactance perturbations in the DRP. Since this problem is non-convex, we analyze two extreme cases and propose the corresponding algorithms. The defender can trade between these two cases according to the specific context.

A. DSCD Optimization Formulation

Cost minimization is the first objective when performing DSCD. Since SMP is more costly, minimizing the cost is equivalent to minimizing $|\mathbb{P}|$. This requires maximizing the capability of the DRP, which can be achieved by increasing the number of perturbations in the DRP. However, the delay for state recovery also increases with this number. Thus, the execution of DSCD is a multi-objective optimization problem requiring joint consideration of cost and delay as follows:

$$\min_{\mathbf{Y},\mathbb{P}} \begin{cases} f_{cost}\text{: } \sum_{k=1}^{u}\left(\alpha\|\mathbf{x}_k-\mathbf{x}_0\|_0+\beta\Delta P_{loss,k}\right)+|\mathbb{P}| \\ f_{delay}\text{: } u\Delta T \end{cases} \tag{15a}$$

$$s.t. \quad \tau x_{0,i} \leq |x_{k,i} - x_{0,i}| \leq \eta x_{0,i},\ i \in \mathbb{D} \tag{15b}$$

$$rank\left(\begin{bmatrix}\mathbf{L}_u \\ \mathbf{I}_{\mathbb{P}}\end{bmatrix}\right) = m, \tag{15c}$$

where u is the number of all perturbations of DRP, and $\mathbf{Y} = [\mathbf{x}_1\ \mathbf{x}_2 \cdots \mathbf{x}_u]$ is all reactance perturbation schemes in DRP. f_{cost} is the function of cost, where the cost of DRP and SMP are calculated independently. The cost of the k-th perturbation in DRP includes the cost of branch reactance perturbation and the increase in power losses after perturbation ($\Delta P_{loss,k} = P_{loss,k} - P_{loss,0}$, where $P_{loss,k}$ and $P_{loss,0}$ are the power losses after the k-th perturbation and the initial power losses before DSCD, respectively), which are determined by the number of perturbed branches ($\|\mathbf{x}_k - \mathbf{x}_0\|_0$) and the specific perturbation scheme, respectively [49]. The cost of SMP is determined by the number of measurements to be protected, i.e., $|\mathbb{P}|$. α and β are the price weight factors. Since D-FACTS devices are widely deployed in power systems, the cost introduced by DRP is much smaller than that of the SMP, i.e., the weight factor $0 < \alpha < 1$ [41]. f_{delay} is the function of delay, where ΔT is the delay of each perturbation. (15b) determines the physical operation limit of D-FACTS devices. η is the maximum physical limit of D-FACTS devices, and τ is the minimum perturbation to guarantee the detection rate. (15c) is the condition for recovering the system state, consistent with Theorem 1.

Algorithm 1 DSCD Implementation With Minimum Delay

```
Input: $\mathbf{x}_0$, $\mathbf{C}$, $\mathbf{A}$ and PLRS;
Output: $\mathbb{D}$, $\mathbb{P}$ and $\mathbf{x}_1$;
$\mathbf{F}_0 \leftarrow \mathbf{C}\mathbf{X}_0$; $\mathbf{L}_{old} \leftarrow \mathbf{F}_0$;
Generate a spanning tree $\mathbb{T}$ with maximum |PLRS|, and
  arrange $\mathbb{T}$ in descending order of |PLRS|;
$\mathbb{K}_U \leftarrow \mathbb{T}$;
for $j \in \mathbb{K}_U$ do
    if PLRS$_j < 0$ then
        $x_{1,j} \leftarrow x_{0,j} + x_{0,j} * r,\ \ r \sim U(\tau, \eta)$;
    else if PLRS$_j > 0$ then
        $x_{1,j} \leftarrow x_{0,j} - x_{0,j} * r,\ \ r \sim U(\tau, \eta)$;
    end if // Perturb the branch reactance in the
      direction where the PLRS decreases
    $\mathbf{X}_1 \leftarrow diag(\mathbf{x}_1)$; $\mathbf{F}_1 \leftarrow \mathbf{C}\mathbf{X}_1$; $\mathbf{L}_{new} \leftarrow \begin{bmatrix}\mathbf{F}_0 \\ \mathbf{F}_1\end{bmatrix}$;
    if $rank(\mathbf{L}_{new}) > rank(\mathbf{L}_{old})$ then
        $\mathbb{D} \leftarrow \mathbb{D} \bigcup j$;
    else
        $x_{1,j} \leftarrow x_{0,j}$;
    end if
    $\mathbb{K}_U \leftarrow \mathbb{K}_U \backslash j$; $\mathbf{L}_{old} \leftarrow \mathbf{L}_{new}$;
end for
$\mathbb{P} \leftarrow \mathbb{T} \backslash \mathbb{D}$;
```

Since the objective of optimization (15) is non-convex and contains rank constraints, we discuss two extreme cases of this model, which can be traded off in practice.

B. Case I: DSCD With Minimum Delay

Case I of DSCD has a minimum delay, which implies that the DRP contains only one perturbation. Then, the optimization (15) can be transformed into a minimum-delay-based cost minimization problem as:

$$\min_{\mathbf{x}_1,\mathbb{P}} \quad \alpha\|\mathbf{x}_1 - \mathbf{x}_0\|_0 + \beta\Delta P_{loss,1} + |\mathbb{P}| \tag{16a}$$

$$s.t. \quad \tau x_{0,i} \leq |x_{1,i} - x_{0,i}| \leq \eta x_{0,i},\ i \in \mathbb{D} \tag{16b}$$

$$rank\left(\begin{bmatrix}\mathbf{L}_1 \\ \mathbf{I}_{\mathbb{P}}\end{bmatrix}\right) = m. \tag{16c}$$

The system's power losses can only be determined when the specific reactance perturbation scheme is obtained, and adding this factor to the optimization objective for constructing the DSCD would greatly increase the problem's complexity, making it difficult to solve in polynomial time. Here, we consider the costs associated with system power losses to be negligible if:

$$\Delta P_{loss,1} \le 0. \tag{17}$$

This implies that there is no increase in the system's power losses after the DRP implementation. Then, we can simplify the problem in (16) as:

$$\begin{aligned} \min_{\mathbf{x}_1,\mathbb{P}} \quad & \alpha\|\mathbf{x}_1 - \mathbf{x}_0\|_0 + |\mathbb{P}| \\ s.t. \quad & (15b), (15c),\ (17), \end{aligned} \tag{18}$$

where (17) can be obtained by calculating the power losses to reactance sensitivity (PLRS) and perturbing the branch reactance in the direction where the PLRS decreases [49]. Specifically, the PLRS is calculated as:

$$\frac{dP_{loss}}{dx_l} = \frac{\partial P_{loss}}{\partial P_l}\left[\frac{\partial P_l}{\partial s_{(\theta,V)}}\frac{\partial s_{(\theta,V)}}{\partial x_l} + \frac{\partial P_l}{\partial G_l}\frac{\partial G_l}{\partial x_l} + \frac{\partial P_l}{\partial B_l}\frac{\partial B_l}{\partial x_l}\right],$$

where P_l is the real power flow in branch l, and $s_{(\theta,V)}$ is the state vector containing all angular and voltage states of the system [49]. Based on the result of PLRS, the branches with the greatest impact on the power losses can be determined.

According to Section IV, each row of $\mathbf{C}$ corresponds to a loop in the system. A branch that does not belong to any loop (i.e., the connected component of the system increases when the branch is disconnected) is called a single-line cut [32]. The corresponding columns of all single-line cuts in $\mathbf{C}$ only have zero elements. Denote the set of all single-line cuts in the system as $\mathbb{K}_s$. If $\mathbb{K}_s \neq \varnothing$, for an attack $\mathbf{a} = [a_1\ a_2\ \ldots\ a_m]$, $\mathbf{L}_1\mathbf{a} = \mathbf{0}$ always holds when the attack satisfies $a_l = 0, l \notin \mathbb{K}_s$. Therefore, all measurements on single-line cuts must be protected. According to Section IV-A, $\mathbf{L}_1 \in \mathbb{R}^{2(m-n)\times m}$. Thus, $\max rank(\mathbf{L}_1) = \min(2(m-n), m-|\mathbb{K}_s|)$. Specifically, if $2(m-n) \ge m - |\mathbb{K}_s|$, i.e., $m \ge 2n - |\mathbb{K}_s|$, we have $|\mathbb{D}| = n - |\mathbb{K}_s|$, $|\mathbb{P}| = |\mathbb{K}_s|$. If $m < 2n-|\mathbb{K}_s|$, we have $|\mathbb{D}| = m-n$, $|\mathbb{P}| = 2n - m$.

Since the capability of the DRP in case I is limited by the system topology, we first maximize the capability of the DRP in case I and cover the remaining attack space with SMP. Specifically, we find a spanning tree, traverse the branches in the tree until $rank(\mathbf{L}_1)$ is maximized, and then protect the measurements on the remaining branches in the tree.

The DSCD implementation strategy with minimum delay is shown in Algorithm 1. The input includes the initial branch reactance of the system $\mathbf{x}_0$, the loop matrix $\mathbf{C}$, the incidence matrix $\mathbf{A}$ and the PLRS. We derive the spanning tree $\mathbb{T}$ with maximum |PLRS| according to the maximum weighted spanning tree algorithm proposed in [50], since these branches have the most significant impact on power losses (Line 2). Then, arrange $\mathbb{T}$ in descending order of |PLRS|, and traverse the branches in $\mathbb{K}_U$ (Lines 4-17) and perturb all the branches in the direction of reducing power losses (Lines 5-9), where $\mathbb{K}_U$ is the set of branches in $\mathbb{T}$ that have not yet been perturbed. If $rank(\mathbf{L}_{new}) > rank(\mathbf{L}_{old})$ after this perturbation, add the branch to $\mathbb{D}$ (Line 12); else, reset the branch reactance (Line 14). Then, remove the branch from $\mathbb{K}_U$ and update the $\mathbf{L}_{old}$ (Line 16). The final outputs are the set of branches to be perturbed ($\mathbb{D}$), the set of measurements to be protected ($\mathbb{P}$), and the perturbation scheme of DRP ($\mathbf{x}_1$).

Algorithm 2 DSCD Implementation With Minimum Cost

```
Input: $\mathbb{K}_s$, $\mathbf{x}_0$, $\mathbf{C}$, $\mathbf{A}$, $\mathbf{rl}$ and PLRS;
Output: $\mathbb{D}$, $\mathbb{P}$ and $\mathbf{Y}$;
$\mathbf{F}_0 \leftarrow \mathbf{C}\mathbf{X}_0$; $k \leftarrow 0$; $\mathbf{L}_k \leftarrow \mathbf{F}_0$; $\mathbb{P} \leftarrow \mathbb{K}_s$;
Generate a spanning tree $\mathbb{T}$ with maximum |PLRS|, and arrange $\mathbb{T}$ in descending order of |PLRS|;
$\mathbb{D} \leftarrow \mathbb{T}\backslash\mathbb{K}_s$, $\mathbb{K}_U \leftarrow \mathbb{D}$;
while $rank\left(\begin{bmatrix}\mathbf{L}_k \\ \mathbf{I}_{\mathbb{P}}\end{bmatrix}\right) < m$ do
    $k \leftarrow k+1$; $\mathbf{x}_k \leftarrow \mathbf{x}_0$; $\mathbb{K}_V \leftarrow \mathbb{K}_U(1{:}rl_k)$; // The first $rl_k$ elements of $\mathbb{K}_U$
    $\mathbf{X}_k \leftarrow diag(\mathbf{x}_k)$; $\mathbf{F}_k \leftarrow \mathbf{C}\mathbf{X}_k$;
    while $rank\left(\begin{bmatrix}\mathbf{L}_{k-1} \\ \mathbf{F}_k\end{bmatrix}\right) - rank(\mathbf{L}_{k-1}) < rl_k$ do
        for $j \in \mathbb{K}_V$ do
            if $PLRS_j < 0$ then
                $x_{k,j} \leftarrow x_{0,j} + x_{0,j} * r,\ \ r \sim U(\tau, \eta)$;
            else if $PLRS_j > 0$ then
                $x_{k,j} \leftarrow x_{0,j} - x_{0,j} * r,\ \ r \sim U(\tau, \eta)$;
            end if
        end for
    end while // Maximize the rank lift of each perturbation
    $\mathbf{X}_k = diag(\mathbf{x}_k)$; $\mathbf{F}_k = \mathbf{C}\mathbf{X}_k$; $\mathbf{L}_k = \begin{bmatrix}\mathbf{L}_{k-1} \\ \mathbf{F}_k\end{bmatrix}$;
    $\mathbb{K}_U \leftarrow \mathbb{K}_U\backslash\mathbb{K}_V$; $\mathbf{Y} \leftarrow [\mathbf{Y}\ \mathbf{x}_k]$;
end while
```

C. Case II: DSCD With Minimum Cost

This subsection proposes the DSCD with minimum cost to minimize the number of protected measurements.

Since the capability of the DRP is no longer limited by topology, the SMP only needs to protect the single-line cuts of the system. Thus, $|\mathbb{P}| = |\mathbb{K}_s|$, $|\mathbb{D}| = n - |\mathbb{P}|$ always holds in case II. Then the optimization problem (15) can be transformed into a minimum-cost-based delay minimization problem as:

$$\begin{aligned} \min_{\mathbf{Y}} \quad & u && \text{(19a)} \\ s.t. \quad & (15b),\ (15c) && \\ & |\mathbb{P}| = |\mathbb{K}_s| && \text{(19b)} \\ & \sum_{k=1}^{u} \|\mathbf{x}_k - \mathbf{x}_0\|_0 = n - |\mathbb{K}_s|. && \text{(19c)} \end{aligned}$$

Note that (19) is a rank-constrained optimization, which has been proven to be NP-hard [51]. Since $\max rank\left(\begin{bmatrix}\mathbf{L}_k \\ \mathbf{I}_{\mathbb{P}}\end{bmatrix}\right) = m$, an effective way to minimize u is to maximize the rank lift of $\begin{bmatrix}\mathbf{L}_k \\ \mathbf{I}_{\mathbb{P}}\end{bmatrix}$ after each perturbation. Therefore, an approximate solution of the NP-hard problem (19) can be obtained by solving the following subproblem sequentially.

$$\begin{aligned} \max_{\mathbf{x}_k} \quad & rank(\mathbf{L}_k) - rank(\mathbf{L}_{k-1}) && \text{(20a)} \\ s.t. \quad & rank\left(\begin{bmatrix}\mathbf{L}_{k-1} \\ \mathbf{I}_{\mathbb{P}}\end{bmatrix}\right) < m && \text{(20b)} \\ & (15b),\ (15c),\ (19b), (19c). && \end{aligned}$$

In summary, we can determine the strategy to perform DSCD with minimum cost as finding the spanning tree with maximum |PLRS|, protecting the measurement of all single-line cuts, and perturbing the other tree branches in batches until the system satisfies (15c).

The DSCD implementation strategy with minimum cost is shown in Algorithm 1. In addition to the initialization conditions of Algorithm 1, we need to obtain the set of single-line cuts $\mathbb{K}_s$ and the maximum rank lift of $\mathbf{L}_k$ at each reactance perturbation, denoted as rl_k. Suppose the number of perturbations in case II is u, then $\mathbf{rl} = [rl_1 \ldots rl_u]$ describes the maximum rank lift of all perturbations, where the method to calculate $\mathbf{rl}$ is proposed in [32]. According to the previous conclusions, it is straightforward to derive the set of protected measurements as $\mathbb{P} = \mathbb{K}_s$. $\mathbb{D} = \mathbb{T} \backslash \mathbb{K}_s$ is the set of tree branches removing all single-line cuts. $\mathbb{K}_V$ is the set of branches to be perturbed in the current iteration. The objective of the k-th perturbation scheme is to increase the rank lift of $\mathbf{L}_k$ versus $\mathbf{L}_{k-1}$ to rl_k (Lines 7-15), so as to minimize the number of perturbations in DRP. The search program terminates if (15c) is met (Lines 4-18), where all adopted perturbation schemes are recorded in $\mathbf{Y}$ (Line 17). The final outputs are the set of branches to be perturbed ($\mathbb{D}$), the set of measurements to be protected ($\mathbb{P}$), and the whole perturbation scheme of DRP ($\mathbf{Y}$).

D. Tradeoff of Case I and Case II

Section V-B and V-C propose two cases of DSCD execution, and the operator can choose the appropriate mode according to the specific context. We present the transformation methods for these two cases in this subsection.

Suppose the number of perturbations in case II is u, then $\mathbf{rl} = [rl_1 \ldots rl_u]$ describes the maximum rank lift of all perturbations. According to Theorem 2, we have:

$$rl_1 + \ldots + rl_u + |\mathbb{P}| = n. \tag{21}$$

Due to topological constraints, there must be $rl_1 \geq \ldots \geq rl_u$. For example, the DRP in the IEEE 57-bus system requires at least 5 perturbations with $\mathbf{rl} = [24, 18, 6, 4, 3]$ and $|\mathbb{P}| = 1$. That is, the capability of the last perturbation to reduce the attack space is much smaller than the first perturbation, even though the delays they introduce are the same. Then, the defender can protect the 3 lines of the last perturbation by SMP to recover the system state with 4 perturbations in DRP. In general, the defender can get a DSCD scheme with a delay of t ($t \in [1, u]$) by making $\mathbb{P} = \mathbb{K}_s \cup \mathbb{D}_u \cup \ldots \cup \mathbb{D}_{t+1}$, where $\mathbb{D}_k$ is the set of perturbed branches in the k-th perturbation of case II. The result is the same as case I when $t = 1$.

VI. Numerical Simulation

A. System Setup

We evaluate the performance of the proposed DSCD in terms of attack detection, attack identification, state recovery, and application cost on the IEEE 6-bus system, 14-bus system, 57-bus system, and 118-bus system in MATPOWER [52]. We assume that D-FACTS devices are sufficiently deployed in the system and cover at least one spanning tree. All attack vectors in this study only modify the phase angles of the system, so we only consider the active part of power flow measurements. In this paper, we set τ to 5% for efficiency and η to 20% for system security performance [44]. To assess the impact of measurement noise on state recovery, we introduced noise to the measurements. The noise follows a zero-mean Gaussian distribution with a standard deviation of $\delta_i = 10^{-4}$ p.u. [53]. For comparisons, the control groups are set as follows:

PFDD: The proactive false data detection approach, which deploys D-FACTS devices on a spanning tree of the system, and the perturbation magnitude of x_l, denoted as Δx_l, satisfies $0 \leq |\Delta x_l| \leq \eta x_l$ [15].

OMTD: The MTD with optimal D-FACTS deployment achieves the maximum detection capability with minimum D-FACTS devices [20]. n and $m - n$ D-FACTS devices are deployed in complete and incomplete systems. The perturbation magnitude satisfies $\tau x_l \leq |\Delta x_l| \leq \eta x_l$.

EMTD: The effective and low-cost MTD, which is to protect all buses with minimal D-FACTS devices and does not increase the generation cost [34]. At least n D-FACTS devices are needed to protect all buses, and the perturbation magnitude satisfies $0 \leq |\Delta x_l| \leq \eta x_l$.

All these three MTD strategies achieve the maximum detection capability for one perturbation by maximizing $rank([\mathbf{H}_0\ \mathbf{H}_1])$.

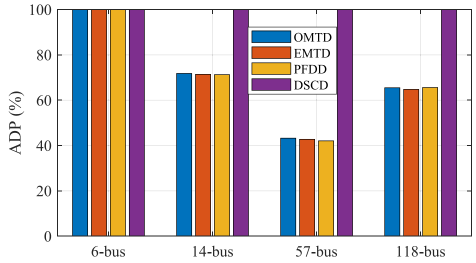
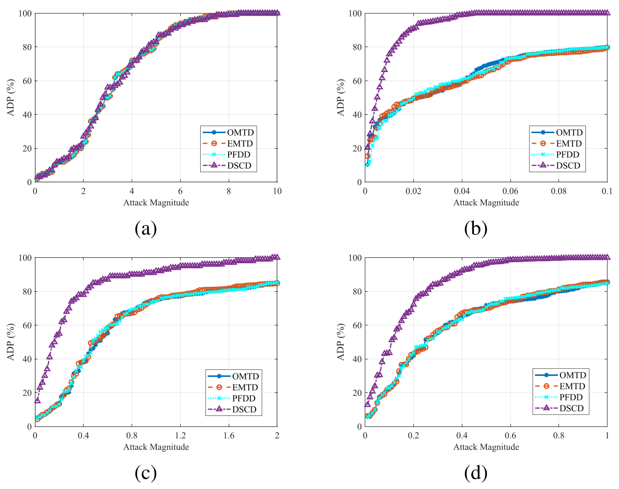


Fig. 4. ADP comparison in four test systems in noiseless environments.

B. Comparison of Attack Detection Capabilities

In this subsection, we conduct attack detection experiments and evaluate the detection capability using Attack Detection Probability (ADP). We perform 10,000 random attack experiments at each setting and count the number of successful detections to calculate ADP. In the DC model, all attack vectors satisfy $\mathbf{a} = \mathbf{H}_0\mathbf{c}$, which are randomly generated within the column space of the initial measurement matrix $\mathbf{H}_0$. Specifically, to emulate the behavior of an attacker attacking at minimal cost, all attacks only modify a minimal set of branches, i.e., they are performed on only one basic cutset of the system. Measurement data is augmented with Gaussian noise with a standard deviation of $\delta_i = 10^{-4}$ p.u. BDD is used to detect FDI attacks, with a threshold set at a false positive rate of $\alpha = 0.05$.

As shown in Fig. 4, the ADP of DSCD is always 100% in noiseless environments, which is consistent with the theoretical analysis in Section IV. The three baseline MTDs can detect all FDI attacks in the 6-bus system, which satisfies $m \geq 2n$, while their ADPs are great less than DSCD in the other three systems. In noisy environments, the ADP



(a) (b) (c) (d)

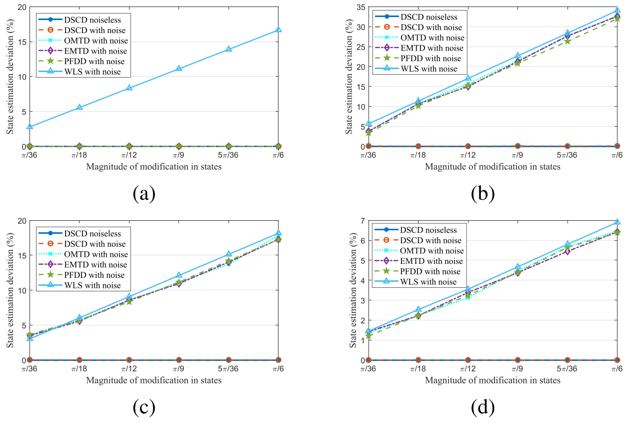
Fig. 5. ADP versus attack magnitude in noisy environments in the (a) 6-bus, (b) IEEE 14-bus, (c) IEEE 57-bus, and (d) IEEE 118-bus test systems.

varies with the magnitude of the attack, as minor attacks may be difficult to distinguish from system noise. The ADP versus attack magnitude is shown in Fig. 5, and the x-axis is the ratio of $\frac{\|\mathbf{a}\|_2}{\|\mathbf{w}\|_2}$, where $\mathbf{w}$ is the system noise. The ADPs of all the methods increase with the attack magnitude. In the 6-bus system, all the ADPs reach 100% as the attack magnitude increases, while DSCD has a significantly superior performance in the other three test systems.

C. Comparison of State Recovery and Attack Identification

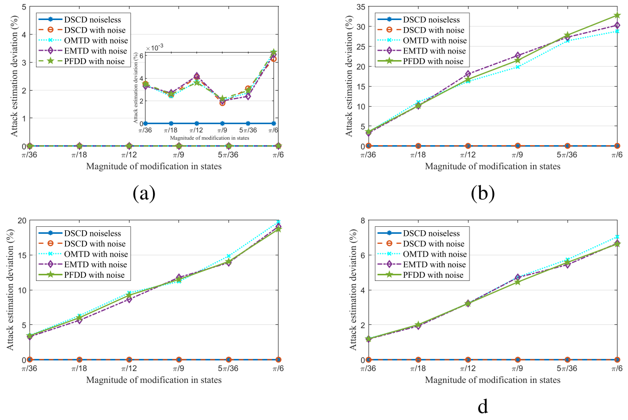
To evaluate the performance of the proposed DSCD in system state recovery, we compare DSCD with three baseline MTD strategies mentioned above and the commonly used Weighted Least Squares (WLS) estimator in terms of their state recovery capabilities in each system. Note that $|\mathbb{P}| = 0$ in all control groups. Specifically, we utilize normalized distance between the estimated and the real states as a metric, where the state is considered as successfully recovered if $\frac{\|\hat{\boldsymbol{\theta}}_0-\boldsymbol{\theta}_0\|_2}{\|\boldsymbol{\theta}_0\|_2}\times 100\% \leq 1\%$. To evaluate the effect of the attacks on the performance of state recovery, the system state deviations guided by the attacker, $\mathbf{c}$, are randomly generated following uniform distribution within $[-\lambda, \lambda]$, i.e., $\|\mathbf{c}\|_\infty \leq \lambda$, where $\lambda = \pi/36, \ldots, \pi/6$ [41].

As shown in Fig. 6, the state estimation deviation of DSCD in noiseless environments is always 0 in the four test systems, i.e., the system state can actually be recovered. The state estimation deviation of DSCD in noisy environments is always less than 1%, even if λ and the system size change. The estimation deviation of the WLS estimator for the system state becomes more significant with the growth of the magnitude of the attack vector. The three baseline MTDs can completely recover the system state in the 6-bus system, which satisfies $m \geq 2n$. In contrast, their trends of state estimation deviation in the other three systems are consistent with WLS. Note that the effect of the same λ on the system decreases as the system size increases. However, even for the smallest λ, the estimation deviations of other methods are still larger than 1%.



(a) (b) (c) (d)

Fig. 6. Estimation deviations of system state in the (a) 6-bus, (b) IEEE 14-bus, (c) IEEE 57-bus, and (d) IEEE 118-bus test systems.



(a) (b) d

Fig. 7. Estimation deviations of attack in the (a) 6-bus, (b) IEEE 14-bus, (c) IEEE 57-bus, and (d) IEEE 118-bus test systems.

In addition, we compare the results of DSCD and three MTD strategies for estimating and identifying the attacks injected by the attacker. We also use the normalized distance between the estimated and the real attacks as a metric, where the attack is considered as successfully identified if $\frac{\|\hat{\mathbf{a}}-\mathbf{a}\|_2}{\|\mathbf{a}\|_2} \times 100\% \leq 1\%$. We conducted 1,000 attack experiments for each attack magnitude in four test systems, and the estimated results are shown in Fig. 7. Obviously, the estimation of attack is consistent with the estimate of the system state in Fig. 6. It can be found that DSCD has a more accurate estimation of attacks in all systems. In the 6-bus system, the control groups also estimate the attack accurately. In the other three test systems, their attack estimation deviations increase with attack magnitude.

D. Comparison of Economic Performance

To validate the cost-effectiveness of DSCD, we compare the two cases of the proposed DSCD with MP and the Joint Admittance Perturbation and Meter Protection (JAPMP) [41]. JAPMP is another approach that combines branch parameter perturbation and measurement protection, which also contains only one branch reactance perturbation, as in case I of DSCD. Since D-FACTS devices are widely deployed in power systems, the cost introduced by DRP is relatively low

TABLE I
PROTECTION COSTS IN DIFFERENT TEST SYSTEMS

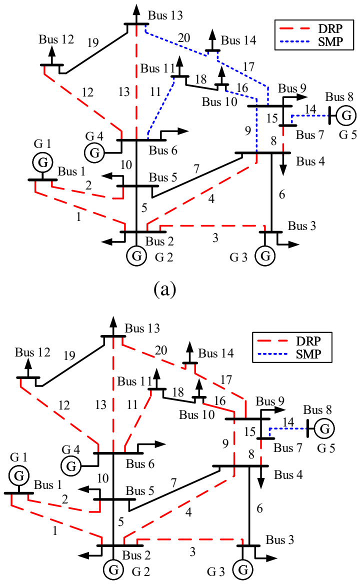
Test System	α	MP	JAPMP	DSCD-I	DSCD-II
6-bus	0.1	5	0.5	0.5	0.5
	0.3		1.5	1.5	1.5
14-bus	0.1	13	8.5	6.7	2.2
	0.3		9.5	8.1	4.6
57-bus	0.1	56	39.8	34.4	6.5
	0.3		43.4	39.2	17.5
118-bus	0.1	117	82.7	55.8	19.8
	0.3		96.1	69.4	41.4

compared to SMP. To visually analyze DSCD's ability to reduce costs, we take the cost of protecting one measurement as the base value to normalize each cost of DSCD. For example, when $\alpha = 0.1$, the cost of protecting a measurement in SMP is 1, and the cost of perturbing a branch in DRP is 0.1.

As shown in Table I, the protection cost of DSCD is significantly lower than MP. This is primarily because of the low-cost DRP involved in DSCD. Since the sum of measurements to be protected and branches to be perturbed in DSCD is equal to the measurements to be protected in MP, DSCD substantially reduces the application cost by replacing most of the measurement protection with branch reactance perturbation. In the 6-bus system, the cost of JAPMP is the same as in both cases of DSCD. This is because the 6-bus system satisfies $m \geq 2n$, and only one perturbation is required to recover the system state. Hence, the number of measurements that need protection is 0. In the other three systems, JAPMP needs to protect more measurements to recover the system state due to the limitation of system topology. Specifically, JAPMP needs to protect 8, 38, and 76 measurements in the IEEE 14-bus, 57-bus, and 118-bus test systems, respectively. In contrast, DSCD's case I needs to protect 6, 32, and 49 measurements in these three systems, and DSCD's case II needs to protect 1, 1, and 9 measurements, respectively. The branches to be perturbed and the measurements to be protected in the IEEE 14-bus system are shown in Fig. 8. Since the cost of DRP is much lower than that of SMP, both cases of DSCD have better economic performance compared to existing methods.

E. Tradeoff on the Two Cases of DSCD

Operators can trade between delay and cost to choose the appropriate application scheme. For a fixed ΔT, the delay is only related to the number of perturbations in the DRP. The minimum delay for both cases of DSCD in four test systems is shown in Fig. 9. The label DoA$/n$ on the y-axis denotes the ratio of DoA after this perturbation to the initial DoA before DSCD, and the system state is recoverable when DoA$/n = 0$. All systems, in case I, contain only one perturbation. In case II, the 57-bus system requires the most perturbations, which is 5. It can be noticed that the reduction of DOA for the last two perturbations is relatively small, so the operator can reduce the number of perturbations by protecting a few more measurements based on case II. Fig. 10 shows the trend of total cost and number of perturbations versus different numbers of protected measurements in the IEEE 57-bus system. The number of perturbations is reduced to 4 when $|\mathbb{P}| = 4$, and the total cost increases from 6.5 to 9.2. As the defender protects more measurements, the number of perturbations decreases, and the total cost increases. When $|\mathbb{P}| = 32$, the results are the same as in case I.



(a)

(b)

Fig. 8. The DSCD scheme in the IEEE 14-bus system under (a) case I, (b) case II.

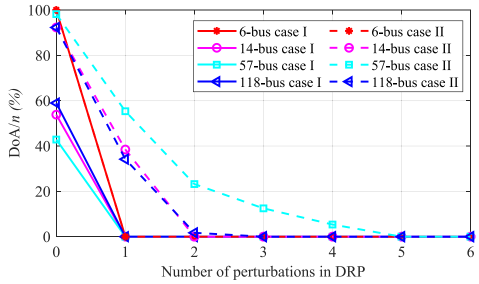


Fig. 9. DoA$/n$ in the two cases versus number of perturbations in four test systems.

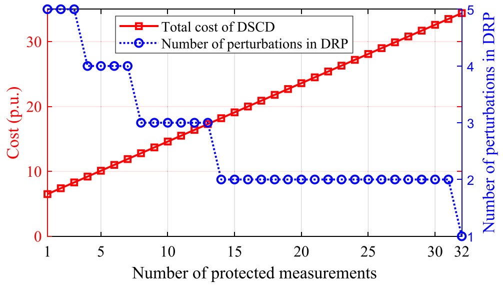


Fig. 10. The trend of cost and number of perturbations versus different numbers of protected measurements in the IEEE 57-bus system.

VII. DISCUSSIONS

All DRP-based defense methods exploit the information asymmetry between the attacker and the defender, rendering the stealthy FDI attacks ineffective. Notably, perturbation of line parameters will likely change the system power flow. Smarter attackers with more resources may eavesdrop on real-time system measurements to update their attack strategies. Recent work has proposed a parameter-estimate-first false data injection (PEF-FDI) attacks, where attackers can estimate new line parameters based on changed power flows at a single sampling instant, thereby adjusting their attack strategies. Such attacks would render most DRP based MTD strategies ineffective [54].

A practical approach to tackle this threat is to protect key measurements from eavesdropping by attackers using stronger SMP methods. As stated in [54], attackers need to know at least five measurement values to deduce the parameters of target branch, which is much more than the protection measurements to recover the system state. Thus, the DSCD that integrates SMP and DRP is still effective against such attacks. Another approach is maintaining the system power flow unchanged after perturbing the line parameters [13]. For the same power flow, there are an infinite number of corresponding line parameters and system states. When the attacker cannot eavesdrop on the system state, estimating the precise line parameters is unfeasible.

VIII. Conclusion

This paper proposes a DSCD method to identify FDI attacks and recover system states with minimal cost. Initially, we outline the DSCD framework based on the unification of DRP and SMP, and delineate the necessary and sufficient conditions for recovering the real system state via DSCD. Subsequently, we formulate an implementation model for DSCD that accounts for both cost and delay associated with multiple reactance perturbations in DRP. Given the non-convex nature of the problem, we examine two extreme scenarios: minimizing delay within a constrained cost, and minimizing cost while maintaining an acceptable level of delay. We then propose algorithms tailored to each scenario and explore the interplay between them, offering the defender the flexibility to adjust according to the specific context. Simulation results demonstrate that the proposed DSCD can accurately identify the attack and recover the system state at a considerably lower cost compared to existing methods.

References

[1] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, pp. 1–33, 2011.

[2] M. A. Rahman and H. Mohsenian-Rad, "False data injection attacks with incomplete information against smart power grids," in *Proc. IEEE Glob. Telecommun. Conf. (GLOBECOM)*, 2012, pp. 3153–3158.

[3] Z. Zhang, R. Deng, P. Cheng, and Q. Wei, "On feasibility of coordinated time-delay and false data injection attacks on cyber-physical systems," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8720–8736, Jun. 2022.

[4] J. Kim, L. Tong, and R. J. Thomas, "Subspace methods for data attack on state estimation: A data driven approach," *IEEE Trans. Signal Process.*, vol. 63, no. 5, pp. 1102–1114, Mar. 2015.

[5] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. J. Overbye, "Detecting false data injection attacks on DC state estimation," in *Proc. Preprints First Workshop Secure Control Syst. (CPSWEEK)*, 2010, pp. 1–9.

[6] T. T. Kim and H. V. Poor, "Strategic protection against data injection attacks on power grids," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 326–333, Jun. 2011.

[7] A. Ashok, M. Govindarasu, and V. Ajjarapu, "Online detection of stealthy false data injection attacks in power system state estimation," *IEEE Trans. Smart Grid*, vol. 9, no. 3, pp. 1636–1646, May 2018.

[8] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 645–658, Dec. 2011.

[9] K. Manandhar, X. Cao, F. Hu, and Y. Liu, "Detection of faults and attacks including false data injection attack in smart grid using Kalman filter," *IEEE Trans. Control Netw. Syst.*, vol. 1, no. 4, pp. 370–379, Dec. 2014.

[10] Y. Huang, H. Li, K. A. Campbell, and Z. Han, "Defending false data injection attack on smart grid network using adaptive CUSUM test," in *Proc. 45th Annu. Conf. Inf. Sci. Syst. (CISS)*, 2011, pp. 1–6.

[11] K. L. Morrow, E. Heine, K. M. Rogers, R. B. Bobba, and T. J. Overbye, "Topology perturbation for detecting malicious data injection," in *Proc. 45th Annu. Hawaii Int. Conf. Syst. Sci.*, 2012, pp. 2104–2113.

[12] S. Bi and Y. J. Zhang, "Graphical methods for defense against false-data injection attacks on power system state estimation," *IEEE Trans. Smart Grid*, vol. 5, no. 3, pp. 1216–1227, May 2014.

[13] J. Tian, R. Tan, X. Guan, and T. Liu, "Enhanced hidden moving target defense in smart grids," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 2208–2223, Mar. 2019.

[14] C. Liu, J. Wu, C. Long, and D. Kundur, "Reactance perturbation for detecting and identifying FDI attacks in power system state estimation," *IEEE J. Sel. Top. Signal Process.*, vol. 12, no. 4, pp. 763–776, Aug. 2018.

[15] 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 Trans. Ind. Informat.*, vol. 16, no. 2, pp. 854–864, Feb. 2020.

[16] G. Dán and H. Sandberg, "Stealth attacks and protection schemes for state estimators in power systems," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, 2010, pp. 214–219.

[17] J. Wang, D. Shi, Y. Li, J. Chen, and X. Duan, "Realistic measurement protection schemes against false data injection attacks on state estimators," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, 2017, pp. 1–5.

[18] M. A. Rahman, E. Al-Shaer, and R. B. Bobba, "Moving target defense for hardening the security of the power system state estimation," in *Proc. ACM Conf. Comput. Commun. Secur.*, 2014, pp. 59–68.

[19] S. Lakshminarayana and D. K. Yau, "Cost-benefit analysis of moving-target defense in power grids," *IEEE Trans. Power Syst.*, vol. 36, no. 2, pp. 1152–1163, Mar. 2021.

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

[21] 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 Trans. Inf. Forensic Security*, vol. 15, pp. 2320–2335, 2020.

[22] Z. Zhang, R. Deng, P. Cheng, and M.-Y. Chow, "Strategic protection against FDI attacks with moving target defense in power grids," *IEEE Trans. Control Netw. Syst.*, vol. 9, no. 1, pp. 245–256, Mar. 2022.

[23] Z. Zhang, R. Deng, D. K. Y. Yau, and P. Chen, "Zero-parameter-information data integrity attacks and countermeasures in IoT-based smart grid," *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6608–6623, Apr. 2021.

[24] W. Xu, I. M. Jaimoukha, and F. Teng, "Robust moving target defence against false data injection attacks in power grids," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 29–40, 2023.

[25] M. Liu, C. Zhao, Z. Zhang, and R. Deng, "Explicit analysis on effectiveness and hiddenness of moving target defense in AC power systems," *IEEE Trans. Power Syst.*, vol. 37, no. 6, pp. 4732–4746, Nov. 2022.

[26] H. Zhang, B. Liu, X. Liu, A. Pahwa, and H. Wu, "Voltage stability constrained moving target defense against net load redistribution attacks," *IEEE Trans. Smart Grid*, vol. 13, no. 5, pp. 3748–3759, Sep. 2022.

[27] M. Zhang, X. Fan, R. Lu, C. Shen, and X. Guan, "Extended moving target defense for ac state estimation in smart grids," *IEEE Trans. Smart Grid*, vol. 14, no. 3, pp. 2313–2325, May 2023.

[28] J. Tian, R. Tan, X. Guan, Z. Xu, and T. Liu, "Moving target defense approach to detecting Stuxnet-like attacks," *IEEE Trans. Smart Grid*, vol. 11, no. 1, pp. 291–300, Jan. 2020.

[29] Z. Zhang, Y. Tian, R. Deng, and J. Ma, "A double-benefit moving target defense against Cyber-physical attacks in smart grid," *IEEE Internet Things J.*, vol. 9, no. 18, pp. 17912–17925, Sep. 2022.

[30] S. Lakshminarayana, E. V. Belmega, and H. V. Poor, "Moving-target defense against cyber-physical attacks in power grids via game theory," *IEEE Trans. Smart Grid*, vol. 12, no. 6, pp. 5244–5257, Nov. 2021.

[31] W. Xu, M. Higgins, J. Wang, I. M. Jaimoukha, and F. Teng, "Blending data and physics against false data injection attack: An event-triggered moving target defence approach," *IEEE Trans. Smart Grid*, vol. 14, no. 4, pp. 3176–3188, Jul. 2023.

[32] J. Wang, J. Tian, Y. Liu, D. Yang, and T. Liu, "MMTD: Multi-stage moving target defense for security-enhanced D-FACTS operation," *IEEE Internet Things J.*, vol. 10, no. 14, pp. 12234–12247, Jul. 2023.

[33] C. Liu, Y. Tang, R. Deng, M. Zhou, and W. Du, "Joint Meter coding and moving target defense for detecting stealthy false data injection attacks in power system state estimation," *IEEE Trans. Ind. Informat.*, vol. 20, no. 3, pp. 3371–3381, Mar. 2024.

[34] Z. Zhang, R. Deng, D. K. Yau, P. Cheng, and M.-Y. Chow, "Security enhancement of power system state estimation with an effective and low-cost moving target defense," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 53, no. 5, pp. 3066–3081, May 2023.

[35] J. Tian, R. Tan, X. Guan, and T. Liu, "Hidden moving target defense in smart grids," in *Proc. Workshop Cyber-Phys. Secur. Resil. Smart Grids (CPSR-SG)*, 2017, pp. 21–26.

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

[37] 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 *Proc. IEEE Power Energy Soc. Gen. Meeting*, 2018, pp. 1–5.

[38] M. Cui and J. Wang, "Deeply hidden moving-target-defense for cybersecure unbalanced distribution systems considering voltage stability," *IEEE Trans. Power Syst.*, vol. 36, no. 3, pp. 1961–1972, May 2021.

[39] J. R. K. Rajasekaran, B. Natarajan, and A. Pahwa, "Modified matrix completion-based detection of stealthy data manipulation attacks in low observable distribution systems," *IEEE Trans. Smart Grid*, vol. 14, no. 6, pp. 4851–4862, Nov. 2023.

[40] 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," in *Proc. IEEE Int. Conf. Commun., Control, Comput. Technol. Smart Grids (SmartGridComm)*, 2021, pp. 207–213.

[41] 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 Trans. Power Syst.*, vol. 35, no. 2, pp. 1468–1478, Mar. 2020.

[42] G. Hug and J. A. Giampapa, "Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1362–1370, Sep. 2012.

[43] A. Abur and A. G. Exposito, "Weighted least-squares state estimation," in *Power System State Estimation: Theory and Implementation*. Boca Raton, FL, USA: CRC press, 2004.

[44] D. Divan and H. Johal, "Distributed FACTS—A new concept for Realizing grid power flow control," *IEEE Trans. Power Electron.*, vol. 22, no. 6, pp. 2253–2260, Nov. 2007.

[45] R. Diestel, "The basics," in *Graph Theory*. Berlin, Germany: Springer, 2017, pp. 1–34.

[46] A. Abur and A. G. Exposito, "Network observability analysis," in *Power System State Estimation: Theory and Implementation*. Boca Raton, FL, USA: CRC press, 2004.

[47] L. W. Johnson, R. D. Riess, and J. T. Arnold, *Introduction to Linear Algebra*. London, U.K.: Pearson, 2002.

[48] D. C. Lay, *Linear Algebra and its Applications*. Harlow, U.K.: Pearson Educ. India, 2003.

[49] K. Rogers and T. J. Overbye, "Some applications of distributed flexible AC transmission system (D-FACTS) devices in power systems," in *Proc. 40th North Am. Power Symp. (NAPS)*, 2008, pp. 1–8.

[50] C. Chow and C. Liu, "Approximating discrete probability distributions with dependence trees," *IEEE Trans. Inf. Theory*, vol. 14, no. 3, pp. 462–467, May 1968.

[51] C. Sun and R. Dai, "Rank-constrained optimization and its applications," *Automatica*, vol. 82, pp. 128–136, Aug. 2017.

[52] "Matpower." Accessed: May 30, 2024. [Online]. Available: https://matpower.org/

[53] J. Wang, L. C. Hui, and H. Yiu, "System-state-free false data injection attack for nonlinear state estimation in smart grid," *Int. J. Smart Grid Clean Energy*, vol. 4, no. 3, pp. 170–176, 2015.

[54] C. Liu, Y. Li, H. Zhu, Y. Tang, and W. Du, "Parameter-estimate-first false data injection attacks in AC state estimation deployed with moving target defense," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 71, no. 4, pp. 1842–1851, Apr. 2024.

Jiazhou Wang received the B.S. degree in electrical engineering and automation from North China Electric Power University in 2017. He is currently pursuing the Ph.D. degree with the School of Cyber Science and Engineering, Xi'an Jiaotong University, Xi'an, China. His research interests include smart grids security.

Jue Tian received the B.S. degree in automation engineering and the Ph.D. degree in cyberspace security from the School of Electronic and Information, Xi'an Jiaotong University, China, in 2011 and 2018, respectively. He is an Assistant Professor with the Xi'an University of Posts and Telecommunications, China. He visited the School of Computer Science and Engineering, Nanyang Technological University, Singapore, from August 2016 to August 2017. His research interests include smart grid and cyber-physical system security. He received the Best Paper Awards from CPSR-SG in 2017.

Nanpeng Yu (Senior Member, IEEE) received the B.S. degree in electrical engineering from Tsinghua University, Beijing, China, in 2006, and the M.S. and Ph.D. degrees in electrical engineering from Iowa State University, Ames, IA, USA, in 2007 and 2010, respectively. He is currently a Full Professor with the Department of Electrical and Computer Engineering, University of California at Riverside, Riverside, CA, USA. His research interests include machine learning in smart grid, electricity market design and optimization, and smart energy communities. He is an Associate Editor of the IEEE TRANSACTIONS ON SMART GRID and *IEEE Power Engineering Letters*.

Yang Liu (Member, IEEE) received the B.S. degree in automation and the Ph.D. degree from the School of Electronic and Information, Xi'an Jiaotong University, China, in 2012 and 2019, respectively, where he is an Associate Professor. From September 2015 to April 2017, he was a Visiting Scholar with the Department of Electrical and Computer Engineering, University of California at Riverside. His research interests include smart grid security, demand response, and cyber-physical system.

Haichuan Zhang is currently pursuing the B.S. degree with the School of the Gifted Young, University of Science and Technology of China. His research interests include industry intelligence, data science, and cyber security.

Yadong Zhou (Member, IEEE) received the B.S. and Ph.D. degrees in control science and engineering from Xi'an Jiaotong University, China, in 2004 and 2011, respectively, where he is currently an Associate Professor with Systems Engineering Institute. He was a Postdoctoral Researcher with The Chinese University of Hong Kong in 2014. His research interests include CPS security.

Ting Liu (Member, IEEE) received the B.S. degree in information engineering and the Ph.D. degree in systems engineering from the School of Electronic and Information, Xi'an Jiaotong University, China, in 2003 and 2010, respectively, where he is a Professor. He was a Visiting Professor with Cornell University from 2016 to 2017. His research interests include software engineering and cyber-physical system.