Optimal Planning and Operation of Hidden Moving Target Defense for Maximal Detection Effectiveness

Bo Liu, *Student Member, IEEE* and Hongyu Wu, *Senior Member, IEEE*

***Abstract*—Moving target defense (MTD) in the power system is a promising defense strategy to detect false data injection (FDI) attacks against state estimation using distributed flexible AC transmission system (D-FACTS) devices. A hidden MTD (HMTD) is a superior MTD method, as it is stealthy to sophisticated attackers. However, the optimal planning and operation of D-FACTS devices that ensure the MTD hiddenness and maximal detection effectiveness are challenging yet unresolved issues. In this paper, we tackle these challenges by first deriving a novel hiddenness operation condition. Then, we propose an analytical sufficient condition on the D-FACTS placement for HMTDs using a graph-theory-based topology analysis. A depth-first-search-based D-FACTS placement algorithm is proposed to guarantee the MTD hiddenness while maximizing the rank of its composite matrix, i.e., an indicator of the MTD effectiveness, and covering all necessary buses. Additionally, we proposed DC- and AC-HMTD operation models to determine the setpoints of D-FACTS devices. The optimization-based DC-HMTD model overcomes the drawbacks of the existing HMTD operation. The ACOPF-based HMTD operation model minimizes the generation cost to utilize the economic benefit of D-FACTS devices. Comparative numerical results on the IEEE 14-bus and IEEE 57-bus systems show the efficacy of the proposed planning and operation approaches.**

***Index Terms*— False data injection attacks, hidden moving target defense, state estimation, D-FACTS, ACOPF.**

I. Introduction

The smart grid is expected to have control and automation processes in the entire power grid to allow efficient and reliable bidirectional power flow [1]. The integration of information and communication technology (ICT) enabled devices into the grid brings increased efficiency with growing vulnerability concerns. The U.S. Department of Energy received 362 power interruption reports related to cyber-physical attacks between 2011 and 2014 [2]. These attacks have become a significant threat to modern power systems. These attacks can undermine or even disrupt the control system of power grids, potentially resulting in tremendous economic loss and severe consequences.

Power system monitoring is critical for reliable system operation. Currently, supervisory control and data acquisition (SCADA) systems collect the measurements from the grid. System operators apply state estimation (SE) to monitor system states and use bad data detection (BDD) to detect erroneous measurements. However, recent work emphasizes that dedicatedly designed false data injection (FDI) attacks can bypass BDD and mislead SE through sensor measurement manipulation [3]–[5]. Even though IEC-61850 protocols are used in power systems, not all packets are encrypted during communication. For example, substation automation systems transmit synchronized phase current and voltage measurements as Sampled Measured Values (SMV) in IEC-61850 protocols. However, encryption of these measurements is impractical due to the high transmission rate and strict time constraints on SMV. The lack of encryption provides attack surfaces for FDI attacks [6]. The system states compromised by the FDI attacks will be used in the economic dispatch, optimal power flow, and fault analysis. Thus, FDI attacks can lead to economic loss, erroneous controls, and physical security issues.

The concept of moving target defense (MTD) has been introduced in the physical layer of power systems in the face of emerging FDI attacks. MTD actively perturbs the branch impedance using distributed flexible AC transmission system (D-FACTS) devices to invalidate attackers' knowledge about the power system configurations. The power system configurations are essential for constructing stealthy FDI attacks [7]–[18]. D-FACTS devices, such as Static Var Compensators (SVC), Thyristor Controlled Series Capacitors (TCSC), and Static Synchronous Series Compensators (SSSC), are originally utilized to control power flows, manage the power congestion, and minimize system losses by altering the impedance of power lines [19]. The recent proliferation of D-FACTS devices [20] has attracted increasing attention in the research community due to their add-on cyber-physical security benefits via MTD. Most MTD approaches in the literature are designed to detect FDI attacks against SE [11]–[18]. The MTD approach has been recently applied to detect coordinated FDI attacks and Stuxnet-like attacks against power grids [9], [10], in which fake sensor measurements are injected to cover the ongoing attacks on the control signals. MTD is also used in the distribution system in which inverter-based distributed energy resources (DERs) are utilized to create low magnitude perturbation signal in voltage, and a developed detection mechanism checks the perturbation sequence in sensors [21].

Existing work in the literature concentrates on MTD operational issues, namely the setpoint selection of D-FACTS devices. A DCOPF-based MTD is proposed in [22], in which the generation cost is minimized and detection effectiveness is ensured in constraints. A random MTD (RMTD) approach was proposed in [11], in which the reactance of D-FACTS equipped lines was randomly changed without considering the detection effectiveness. However, one inherent drawback of the RMTD is that a strong adversary can easily detect whether an MTD is in place by eavesdropping measurements. For example, an alert and sophisticated attacker can detect the existence of MTDs, if the attacker conducts the well-known residual-based BDD based on the eavesdropped measurements and his knowledge

about the system parameters. The detection of the existence of MTD can drive the attacker to postpone the planned attacks, invest more resources to gain updated system knowledge, and potentially intrude into more critical parts. Consequently, a power grid may face a higher level of cyber threats. To overcome this drawback, hidden MTD (HMTD) operation approaches were initially presented in the DC transmission system [12], and the AC distribution system [13], in which setpoints of the D-FACTS devices were delicately changed to make system measurements unchanged after the HMTD.

In the construction of an HMTD, the MTD hiddenness and detection effectiveness are two primary objectives that are closely related and mostly conflicting. Specifically, the hiddenness is not achievable in a system with the highest detection effectiveness, i.e., a complete MTD system, which can detect all FDI attacks [12]. On the other hand, while incomplete MTD systems have limited detection effectiveness, their incompleteness provides viability for the MTD hiddenness. Fortunately, HMTDs can be constructed in the majority of power systems since most systems belong to incomplete MTD systems owning to the restrictive requirements of a complete MTD [15], [17]. It is worth noting that some HMTDs are ineffective in detecting FDI attacks, even though they are hidden to attackers [12], [14]. Consequently, the main concern in the construction of HMTDs becomes how to maximize detection effectiveness.

D-FACTS placement in the context of MTDs has been recently studied to improve the detecting effectiveness. Liu et al. [15] proved that the rank of the composite matrix, i.e., one metric on the detection effectiveness, could be determined by the topology of D-FACTS placement regardless of the D-FACTS setpoints. Optimal D-FACTS placement algorithms were proposed in [15] to achieve the maximum rank of the composite matrix using the minimum number of D-FACTS devices. Zhang et al. [16] proposed a heuristic-based D-FACTS placement algorithm to maximize the rank of the composite matrix and cover the largest number of buses. Tian et al. [12] showed that the rank of the composite matrix in HMTD is related to D-FACTS placements, but no solution was further proposed to construct an HMTD with the maximum rank of the composite matrix. Zhang et al. [14] proposed a joint HMTD algorithm by combining D-FACTS placement with protected meters placement. More specifically, the joint algorithm places a protected meter in each loop to achieve an HMTD with the maximum rank of the composite matrix. They concluded that an MTD is hidden only if the reactance of branches in a loop is modified by a unity factor. However, this is an overly strong condition for an HMTD. In this paper, we will show, for the first time, that HMTDs are achievable and their detection effectiveness is guaranteed without using a unity factor or protected meters.

Towards practical applications of HMTD, a system operator must first install D-FACTS devices on an appropriately identified subset of transmission lines at the planning stage. Then, the D-FACTS setpoints should be optimally determined in the real-time operation. In this paper, we aim at addressing these two intertwined issues by establishing a systematic planning and operation approach for HMTDs. In the planning stage, our objective is to identify a D-FACTS placement, which ensures HMTDs can always be constructed under different load conditions and D-FACTS setpoints. During the operation stage, our objective is to achieve the hiddenness operation condition efficiently. Additionally, the proposed planning and operation together ought to guarantee the maximum detection effectiveness of HMTDs.

The contributions of this paper are separately summarized in terms of MTD planning and operation as follows. For the MTD planning, we

- Derive a sufficient condition to ensure the existence of HMTD and the maximum rank of the composite matrix based on graph-theory topology analysis.
- Propose a depth-first-search-based D-FACTS placement algorithm, in which an HMTD that has the maximum rank of the composite matrix and covering all necessary buses can be constructed.

For the MTD operation, we

- Derive a novel and explicit hiddenness condition in HMTD, which can be easily integrated into MTD operation methods.
- Demonstrate the characteristics of voltage angle changes in HMTD, which bridge the HMTD operation and HMTD planning.
- Propose an optimization-based DC-HMTD operation model that maximizes the reactance changes. This model overcomes the drawbacks of the existing HMTD operation algorithm and obtains the D-FACTS setpoints more efficiently.
- Propose an ACOPF-based HMTD operation model that minimizes the generation cost and presents a trade-off between the generation cost and the MTD hiddenness.

The rest of this paper is organized as follows. We provide preliminaries and related work in Section II. In Section III, we analyze the requirements of D-FACTS placement and the operating characteristics of HMTD. We conduct case studies in Section IV. Conclusions are drawn in Section V.

II. Preliminaries

In this section, we provide background knowledge of FDI attacks, MTD, and the optimal D-FACTS placement as preliminaries for the follow-up sections.

A. Notation

Variables used throughout the paper are summarized in Table I, where boldfaced lower- and upper-case letters stand for vectors and matrices, respectively. "D-FACTS lines" and "non-D-FACTS lines" stand for the set of lines equipped with and without D-FACTS devices, respectively. Let G be the graph of a power system composed of all transmission lines and buses. Let G_{DF}, termed as D-FACTS graph, be a subgraph of G consisting of D-FACTS lines and all buses. Similarly, let $G_{\overline{DF}}$, termed as non-D-FACTS graph, be a subgraph of G consisting of non-D-FACTS lines and all buses. Subscript 0 denotes variables before the implementation of an MTD. A D-FACTS device works in an idle state if it is installed on a given line but doesn't modify the line reactance, i.e., $x_{ij} = x_{ij,0}$. For a D-FACTS device such as a SVC, TCSC, and SSSC, its idle state

corresponds to zero reactive power compensation. Otherwise, it works in a non-idle state.

TABLE I
NOMENCLATURE

Symbol	Definition
$\boldsymbol{\theta}$	Voltage angle of buses excluding reference bus
$\mathbf{z}$	Measurement vector
$\mathbf{a}$	FDI attack vector
$\mathbf{z}_a$	Compromised measurement vector
$\mathbf{H_0}$	DC measurement matrix in SE before MTD
$\mathbf{H}$	DC measurement matrix in SE after MTD
$\mathbf{M}$	Composite matrix of $\mathbf{H}_0$ and $\mathbf{H}$
$\mathbf{A}$	Incident matrix of power system graph
$\mathbf{X}$	Diagonal line reactance matrix
x_{ij}	The reactance of line *i–j* (between bus *i* and *j*)
n	Total number of system buses
m	Total number of measurements
p	Total number of lines
p_1	Total number of lines equipped with D-FACTS
p_2	Total number of lines free from D-FACTS devices
lp	Number of loops in a graph
t	Number of connected components in a graph
$r(\cdot)$	Matrix rank operator
$Null(\cdot)$	Null space operator

B. FDI Attacks against SE

DC flow analysis is faster and more robust than its AC counterpart [3], [12], and thus has been widely used in the planning and operation of transmission systems. In DC-SE, system states, i.e., nodal voltage angles, $\boldsymbol{\theta} \in \mathbb{R}$ are estimated by a set of measurements $\mathbf{z} \in \mathbb{R}$ corresponding to nodal power injections and branch power flows. The measurement vector and states are related as $\mathbf{z} = \mathbf{H} \cdot \boldsymbol{\theta} + \mathbf{e}$, where $\mathbf{e}$ is measurement noises. The maximum likelihood estimate is given by $\hat{\boldsymbol{\theta}} = (\mathbf{H}^T\mathbf{W}\mathbf{H})^{-1}\mathbf{H}^T\mathbf{W}\mathbf{z}$.

Measurement residual is calculated in the BDD to detect bad data in the system [23]. Based on the χ^2 test, a system is free of bad data if the inequality $\gamma = \| \mathbf{z} - \mathbf{H} \cdot \hat{\boldsymbol{\theta}} \|_2 < \gamma_{th}$ holds, where $\gamma_{th} = \chi^2_{(m-n),\alpha}$ is a preset threshold to ensure the BDD has a false alarm rate of $1-\alpha$.

An FDI attack [5] can compromise estimated states by injecting false data into the measurements, i.e., $\mathbf{z}_a = \mathbf{z} + \mathbf{a}$. The FDI attack can bypass the BDD and falsify the SE as long as the attack vector belongs to the column space of $\mathbf{H}$, i.e., $\mathbf{a} \in col(\mathbf{H})$. A stealthy FDI attack requires the attacker's knowledge about $\mathbf{H}$, and the attack vector $\mathbf{a}$ can be equivalently expressed as $\mathbf{a} = \mathbf{H} \cdot \Delta\boldsymbol{\theta}_a$, where $\Delta\boldsymbol{\theta}_a$ is malicious voltage angle injection vector [17].

C. MTD Hiddenness and Detection Effectiveness

Encrypted commands from the system operator's control room can be securely transmitted to the D-FACTS gateway for changing the setpoint in D-FACTS devices through DNP3, IEC 61850, and 60870-5-104 protocol [20]. MTD takes advantage of D-FACTS devices to create uncertainties for attackers. The incremental reactance of line *i–j* can be periodically modified by the D-FACTS device within $|x_{ij} - x_{ij}^0| \le \eta x_{ij}^0|$, where the upper bound $\eta = 20\%$, generally referred to as the MTD magnitude, reflects the physical capacity of D-FACTS devices [12], [15], [17]. Consequently, the measurement matrix $\mathbf{H}$ used in the SE becomes a time-variant matrix. If attackers construct FDI attacks based on an outdated knowledge of $\mathbf{H}$, the estimation residual in the defender's BDD is no longer zero.

HMTD, a superior MTD, is stealthy to alert attackers who use the well-known, residual-based BDD to detect the existence of MTD [12]–[14]. The key idea of HMTD is to create little to no changes in system measurements after HMTD is applied, i.e., $\mathbf{H}_0\boldsymbol{\theta}_0 = \mathbf{H}\boldsymbol{\theta}$, such that the estimation residual in the attacker's BDD verification remains the same after HMTD. The defense stealthiness probability (DSP) is a widely used metric to quantify the MTD hiddenness from the perspective of attackers, which is defined as:

$$DSP = \frac{\text{Number of MTDs hidden to attackers}}{\text{Total number of MTDs}}$$

Since HMTD cannot be constructed in all power systems [12], whether or not the hiddenness of an MTD can be attained in a particular power system becomes a primary concern. A sufficient and necessary condition for the existence of HMTD was proposed in [12]. Let us denote the immutable part of $\mathbf{H}$ by $\underline{\mathbf{H}}$, consisting of the $\mathbf{H}$'s rows corresponding to all non-D-FACTS lines. An HMTD exists if and only if $r(\underline{\mathbf{H}}) < r(\mathbf{H})$ [12]. This condition is beneficial for checking the existence of HMTD when the locations and setpoints of D-FACTS devices are all given. Nevertheless, this condition provides no guidance on how to optimally place and operate D-FACTS devices in a particular system. This paper bridges this gap by deriving the existence requirements of HMTD for the D-FACTS placement and operation.

Once the existence of HMTDs is guaranteed, the detection effectiveness of HMTDs becomes a prominent concern. The rank of the composite matrix $\mathbf{M} = [\mathbf{H}_0 \ \mathbf{H}]$ is a good metric to quantify the MTD detection effectiveness [17]. The HMTD with the maximum rank of the composite matrix, which is referred to as a max-rank MTD, is desirable. Besides, the attack detection probability (ADP), another widely utilized metric to measure the detection effectiveness of an MTD, is defined as:

$$ADP = \frac{\text{Number of FDIs detected by the MTD}}{\text{Total number of FDIs}}$$

A max-rank MTD with both high ADP and high DSP is a more desired MTD. An MTD with high ADP and low DSP is good at detecting FDI attacks but can be easily detected by alert attackers. An MTD with low ADP is least desirable as detection capability is the primary concern of an MTD.

D. Existing D-FACTS Placements

The power system topology can be treated as an edge-weighted graph with buses as nodes and lines as edges. The rank of the composite matrix of an MTD is determined by the D-FACTS placement [15]. We summarize below the relation between the D-FACTs placement and the rank of the composite matrix. Suppose all D-FACTS devices work in non-idle (compensating) states and G_{DF} is loopless, the rank of the composite matrix in MTDs is determined by the number of loops in $G_{\overline{DF}}$ as follows:

$$r(\mathbf{M}) = p - lp_{\overline{DF}} \quad (1)$$

where $lp_{\overline{DF}}$ is the number of loops in $G_{\overline{DF}}$. Note that equation (1) does not hold if there exists any loop in G_{DF} and each loop

in $G_{\overline{DF}}$ decreases $r(\mathbf{M})$ by one. Thus, an MTD is a max-rank MTD if the D-FACTS placement ensures either G_{DF} or $G_{\overline{DF}}$ is loopless [15]. It is worth mentioning that neither the number of connected components in G_{DF} nor that in $G_{\overline{DF}}$ influence the rank of the composite matrix. In this paper, we utilize the connected components to construct HMTDs and apply the relationship (1) to achieve a max-rank MTD.

III. Proposed HMTD Planning and Operation

A. Proposed Hiddenness Condition of MTD

In DC-SE, the objective of HMTD is to remain all measurements on active power flow and active power injection unchanged after the setpoint changes of D-FACTS devices. After the control signal is sent to D-FACTS devices from the control room, the line reactance can be changed within seconds. During the activation of the MTD, the change in nodal active power injection measurements is minute. Thus, it is reasonable to assume that the system loads are constant during the activation of the MTD for analysis. This assumption was also made in other HMTD analyses [12], [14]. In cases that this assumption does not hold, the influence of variant loads on the hiddenness of the proposed HMTD will be evaluated in the subsequent case studies of this paper. We focus on the power flow measurements in the HMTD model to facilitate the analysis.

Suppose power flow measurements are arranged in the following order, i.e., $\mathbf{z}=[\overline{\mathbf{z}}^T \quad \tilde{} \quad$, where $\bar{\mathbf{z}}$ and $\tilde{}$ are power flow measurements of the D-FACTS lines and non-D-FACTS lines, respectively. Accordingly, the measurement matrices before and after the HMTD in the DC model are expressed as $\mathbf{H}_0=\begin{bmatrix}\overline{\mathbf{H}}_0\\ \mathbf{H}\end{bmatrix}$ and $\mathbf{H}=\begin{bmatrix}\overline{\mathbf{H}}\\ \mathbf{H}\end{bmatrix}$, where $\overline{\mathbf{H}}_0$ and $\overline{\mathbf{H}}$ are the submatrices of the measurement matrix and represent power flow measurements of the D-FACTS lines before and after the HMTD, respectively; and $\mathbf{H}$ corresponds to power flow measurements of non-D-FACTS lines. Thus, the power flow measurements before and after the HMTD are $\mathbf{z}_0=\begin{bmatrix}\overline{\mathbf{H}}_0\\ \mathbf{H}\end{bmatrix}\boldsymbol{\theta}_0+\mathbf{e}$ and $\mathbf{z}=\begin{bmatrix}\overline{\mathbf{H}}\\ \mathbf{H}\end{bmatrix}(\boldsymbol{\theta}_0+\Delta\boldsymbol{\theta})+\mathbf{e}$, respectively, where $\Delta\boldsymbol{\theta}$ is the incremental voltage angle introduced by the HMTD. Since all measurements remain unchanged after the HMTD, i.e., $\mathbf{z}_0=\mathbf{z}$, we can derive the hiddenness condition in the noiseless condition as follows:

$$\overline{\mathbf{H}}_0\boldsymbol{\theta}_0=\overline{\mathbf{H}}(\boldsymbol{\theta}_0+\Delta\boldsymbol{\theta}) \tag{4}$$

$$\mathbf{H}\Delta\boldsymbol{\theta}=\mathbf{0} \tag{5}$$

As $\mathbf{H}$ is a fixed matrix, (5) indicates that $\Delta\boldsymbol{\theta}$ determined by the system operator (defender) must belong to the null space of $\mathbf{H}$:

$$\Delta\boldsymbol{\theta}=\mathbf{U}\mathbf{W} \tag{6}$$

where $\mathbf{U}=[u_1,u_2,...,u_s]\in\mathbb{R}$ is the matrix of kernel bases of $\mathbf{H}$; $\mathbf{W}=[w_1,w_2,...,w_s]^T\in\mathbb{R}$ is the weight determined by the system operator; and s is the dimension of kernel bases. In addition, D-FACTS setpoints ought to be delicately chosen to make $\overline{\mathbf{H}}$ satisfying equation (4). The hiddenness condition demonstrates that the D-FACTS setpoints are closely related to incremental voltage angle.

B. Requirements of D-FACTS Placement for HMTD

We utilize the topology analysis to derive a sufficient condition for D-FACTS placement to achieve the MTD hiddenness. The decomposition of $\mathbf{H}$ in [17] can be applied on $\overline{\mathbf{H}}$ and $\mathbf{H}$, respectively, as follows:

$$\overline{\mathbf{H}}=\mathbf{D}_1\cdot\mathbf{X}_1\cdot\mathbf{A}_1^T \tag{8}$$

$$\mathbf{H}=\mathbf{D}_2\cdot\mathbf{X}_2\cdot\mathbf{A}_2^T \tag{9}$$

where $\mathbf{X}_1\in\mathbb{R}$ and $\mathbf{X}_2\in\mathbb{R}$ are the diagonal reactance matrix of the D-FACTS lines and non-D-FACTS lines, respectively; $\mathbf{A}_1\in\mathbb{R}$ and $\mathbf{A}_2\in\mathbb{R}$ are the reduced bus-branch incidence matrix of G_{DF} and $G_{\overline{DF}}$, respectively, in which the row of the slack bus is removed; In a power flow fully measured power system, $\mathbf{D}_1$ and $\mathbf{D}_2$ are of full column rank since $\mathbf{D}_1=[\mathbf{I}_1 \quad -\mathbf{I}_1]^T$ and $\mathbf{D}_2=[\mathbf{I}_2 \quad -\mathbf{I}_2]^T$, where $\mathbf{I}_1\in\mathbb{R}$ and $\mathbf{I}_2\in\mathbb{R}$ are identity matrices. Note that if the system is not power flow fully measured, the decomposition in (8) and (9) become $\overline{\mathbf{H}}=\mathbf{C}_1\cdot\mathbf{D}_1\cdot\mathbf{X}_1\cdot\mathbf{A}_1^T$ and $\mathbf{H}=\mathbf{C}_2\cdot\mathbf{D}_2\cdot\mathbf{X}_2\cdot\mathbf{A}_2^T$, where $\mathbf{C}_1$ and $\mathbf{C}_2$ are meter selection matrices defined in [17]. As long as $\mathbf{C}_1\cdot\mathbf{D}_1$ and $\mathbf{C}_2\cdot\mathbf{D}_2$ are of full column rank, the conclusions in a fully measured system can be extended to a partially measured system. More specifically, $\mathbf{C}_1\cdot\mathbf{D}_1$ with a full column rank indicates the power flow of each D-FACTS line is at least measured either at the from-bus or the to-bus. The same requirements apply for non-D-FACTS lines to achieve the full column rank of $\mathbf{C}_2\cdot\mathbf{D}_2$.

A sufficient condition for the existence of HMTD is given by the following lemma from the perspective of D-FACTS placement.

Lemma 1: an HMTD exists if no D-FACTS devices work in the idle state and $G_{\overline{DF}}$ is a disconnected graph, i.e., $t_{\overline{DF}}>1$.

Proof: Since $\mathbf{D}_2$ and $\mathbf{X}_2$ are of full column rank, the rank of $\mathbf{H}$ equals to $r(\mathbf{A}_2)$, i.e., $r(\mathbf{H})=r(\mathbf{A}_2)$. According to graph theory, the rank of incidence matrix $\mathbf{A}$ in a planar graph with n nodes and t components is $n-t$, i.e., $r(\mathbf{A})=n-t$ [24]. Thus, in $G_{\overline{DF}}$, the following equation holds:

$$r(\mathbf{H})=rank(\mathbf{D}_2\cdot\mathbf{X}_2\cdot\mathbf{A}_2^T)=rank(\mathbf{A}_2^T)=n-t_{\overline{DF}} \tag{10}$$

Suppose $G_{\overline{DF}}$ is a disconnected graph, i.e., $t_{\overline{DF}}>1$, $r(\mathbf{H})<n-1$ holds. Thus, $r(\mathbf{H})<r(\mathbf{H})=n-1$ holds. Thus, an HMTD exists according to the sufficient and necessary condition of HMTD mentioned in Section II. C. ■

As mentioned earlier, not all HMTDs are effective in detecting FDI attacks. The hiddenness and the detection effectiveness must be simultaneously considered in the D-FACTS placement. To ensure the detection effectiveness, HMTDs constructed on a D-FACTS placement ought to have

the maximum rank of the composite matrix. Here, we propose Lemma 2 to present the requirements of D-FACTS placement for constructing max-rank HMTDs.

Lemma 2: a max-rank HMTD exists if the following conditions are satisfied: 1) all D-FACTS devices work in the non-idle states; 2) G_{DF} is loopless; and 3) $G_{\overline{DF}}$ is a disconnected loopless graph.

Proof: According to (1), if both G_{DF} and $G_{\overline{DF}}$ are loopless, any MTD under this topology is a max-rank MTD, i.e., $r(\mathbf{M}) = p$ [15]. According to Lemma 1, if $G_{\overline{DF}}$ is a disconnected and loopless graph, an HMTD exists. Therefore, a max-rank HMTD exists in the D-FACTS placement. ■

In addition to maximizing the rank of the composite matrix, it is important to cover all necessary buses using D-FACTS lines [14], [18]. If a bus is not in any loop, an FDI attack on this bus is undetectable regardless of D-FACTS placement and setpoints [14]. Thus, there is no need to cover these buses, whereas the other buses need to be covered.

As no D-FACTS devices work in the idle state is the prerequisite of Lemma 2, it is necessary to consider this MTD operation requirement during the MTD planning. According to the hiddenness condition (4), setpoints of D-FACTS devices are closely related to the nodal incremental voltage angle in HMTD. Understanding how voltage angles change is the key to constructed HMTD. Here, we propose Lemma 3 to demonstrate how the nodal incremental voltage angle is related to the D-FACTS placement.

Lemma 3: In an HMTD, all buses in a connected component in $G_{\overline{DF}}$ must have the same nodal incremental voltage angle.

Proof: Assume Bus *i* and Bus *j* are two neighbor nodes in the same connected component in $G_{\overline{DF}}$, and their voltage angle before the HMTD is θ_i and θ_j, respectively. Before the HMTD, the power flow on branch *i-j* is $p_{ij}^0 = (\theta_i - \theta_j)/x_{ij}$, where x_{ij} is the reactance of branch *i-j*. Note that x_{ij} cannot be modified by the D-FACTS device, as branch *i-j* is a non-D-FACTS line. Assume Buses *i* and *j* have different incremental voltage angles after the HMTD, i.e., $\Delta\theta_i$ and $\Delta\theta_j$ ($\Delta\theta_i \neq \Delta\theta_j$). The power flow on branch *i-j* becomes $p_{ij} = (\theta_i + \Delta\theta_i - \theta_j - \Delta\theta_j)/x_{ij}$ after the HMTD. It is obvious that $p_{ij}^0 \neq p_{ij}$, which conflicts with the fact that power flow remains the same before and after the HMTD. Therefore, any pair of neighbor nodes in $G_{\overline{DF}}$ has the same nodal incremental voltage angle in an HMTD. It infers all nodes in the same connected component have the same nodal incremental voltage angle in the HMTD. ■

We can further explain the HMTD operation characteristics by combining Lemma 3 and (6). The i^{th} kernel base in (6), i.e., i^{th} column in **U**, identifies all buses in the i^{th} connected component in $G_{\overline{DF}}$. Weight w_i in (6) indicates that all buses in the i^{th} connected component have the same incremental voltage angle, which is equal to w_i. For example, in Fig. 1 (a), Buses 1 and 6 are in the same connected component in the $G_{\overline{DF}}$, and they need to have the same incremental voltage angle in an HMTD. Let an isolated node refers to a bus whose branches are all D-FACTS lines. For each isolated node in $G_{\overline{DF}}$, it has its own kernel base and weight. For example, in Fig. 1 (a), Buses 2 and 5 are two isolated nodes in the $G_{\overline{DF}}$.

We further propose Corollaries 1 and 2 to identify two special cases in which D-FACTS devices must work in the idle state.

***Corollary 1*:** In an HMTD, if a D-FACTS line's two nodes belong to the same connected component in $G_{\overline{DF}}$, the D-FACTS device associated with this line must work in the idle state.

Corollary 2: In an HMTD, if a D-FACTS line's two nodes are two isolated nodes in $G_{\overline{DF}}$ and have the same incremental nodal voltage angle, i.e., $w_i = w_j$, the D-FACTS device associated with this line must work in the idle state.

Note that Corollary 1 is in the context of the HMTD planning, whereas Corollary 2 is on the HMTD operation. Based on the above theoretical foundations, the requirements of D-FACTS placement to construct a max-rank HMTD covering all necessary buses is summarized as follows: 1) $G_{\overline{DF}}$ is a disconnected and loopless graph; 2) G_{DF} is a loopless graph, and its links should cover all buses except for the buses not in any loops; and 3) no D-FACTS devices should work in the idle state. In the following subsection, we will design D-FACTS placement rules and an algorithm to achieve these requirements.

C. Hidden D-FACTS Placement Algorithm

We design the following D-FACTS placement rules in each loop of power system topology. Rule 1 is proposed for two purposes. Firstly, it can effectively prevent D-FACTS devices from working in the idle state identified in Corollary 1. In a loop (with more than two links), if two end-nodes of a D-FACTS line belong to the same connected component in $G_{\overline{DF}}$, there must be at least two successive non-D-FACTS lines in the loop, which is forbidden according to Rule 1. Secondly, it makes D-FACTS lines to cover all nodes in the loop. Since the degree of each node in the loop is no less than two, any end-node of a non-D-FACTS line has to connect to another D-FACTS line due to Rule 1. By extending Rule 1 from a single loop to all loops in the entire system, all buses in all loops of the system are covered by D-FACTS lines.

***Rule 1*:** In each loop of system topology, two or more than two successive non-D-FACTS lines are not allowed.

Further, we design Rule 2 to avoid the appearance of idle D-FACTS devices identified in Corollary 2. This is because that if three or more than three successive D-FACTS lines may generate two or more isolated nodes in $G_{\overline{DF}}$. As two successive D-FACTS lines generate no more than one isolated node in $G_{\overline{DF}}$, the scenario described in Corollary 2 is excluded in the MTD planning.

***Rule 2*:** In each loop of the system, more than two successive D-FACTS lines are not allowed.

Note that Rules 1 and 2 propose requirements on the topology of non-D-FACTS and D-FACTS lines in each loop, respectively. Thus, they provide essential guidance on the D-FACTS placement. We take a loop with six transmission lines as an example. Figure 1 demonstrates all five feasible solutions subject to Rules 1 and 2. It is seen that all these solutions effectively cover all buses in the loop and avoid idle D-FACTS devices identified in Corollaries 1 and 2.

Based on these two rules, we propose a depth-first-search (DFS)-enabled, hidden D-FACTS placement algorithm, which is illustrated in Algorithms 1 and 2. Since the existence of HMTD directly relies on the topology of $G_{\overline{DF}}$ as demonstrated

in Lemma 1, here we focus on finding the location of non-D-FACTS lines. In Algorithm 1, we initialize all lines as D-FACTS lines by using the system graph G as G_{DF} and utilize the DFS algorithm to place non-D-FACTS lines. Note that we use set E_{DF} and E_{NDF} to store the D-FACTS and non-D-FACTS lines determined by DFS, respectively.

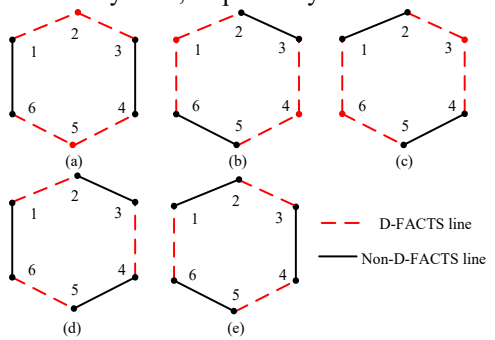


Fig. 1. An illusion of D-FACTS placement solution in HMTD.

The proposed DFS algorithm (Algorithm 2) traverses all loops in the order of a stack (first-in, last-out) based on recursion. In each iteration, we first check whether the following stopping criteria are simultaneously met: 1) G_{DF} is are loopless; 2) $G_{\overline{DF}}$ is a loopless and disconnected graph, and 3) the placement satisfies Rules 1 and 2. If they are satisfied, the algorithm returns the D-FACTS placement solution and stops searching. Otherwise, the algorithm continues to deal with the next loop in G_{DF}, where the D-FACTS lines already placed are identified. Then, all solutions in the loop subject to Rules 1 and 2 are found and saved in a set called *solutionsInSingleLoop*. For each of the stored solutions, we make the recursive call to search in the next loop by updating the latest D-FACTS and non-D-FACTS lines in the system. Algorithm 1 stops after finding a feasible solution or traversing all loops.

Algorithm 1: Hidden D-FACTS Placement Algorithm

Input: The edge-weighted graph $G(V, E)$ of a power grid topology
Output: *Results:* set of non-D-FACTS line placement solution
1: **Initialization:** Suppose all lines are D-FACTS lines, i.e., $G_{DF}= G$. $E_{DF} = \emptyset$, $E_{NDF} = \emptyset$, Global variable *Results* = $\emptyset$
2: dfs (G_{DF}, E_{DF}, E_{NDF}, V)
3: **return** *Results*

Algorithm 2: Depth-First Search (DFS)

Input: D-FACTS graph G_{DF}, set of placed D-FACTS line E_{DF}, set of placed non-D-FACTS line E_{NDF}, System buses V
1: **dfs** (G_{DF}, E_{DF}, E_{NDF}, V)
2: Generate a non-D-FACTS graph G_{NDF} composed of E_{NDF} and V
3: **if** (G_{DF} has no loops and G_{NDF} is a disconnected graph without loops && placement subjects to Rules 1 and 2)
4: Add E_{NDF} to *Results*
5: **return**
6: **end if**
7: Select a loop in G_{DF} and add all lines in the loop to a set, denoted by E_i
8: $E_{DF0} = E_i \cap E_{DF}$ // DF lines already placed in the loop
9: Find all feasible solutions in the loop subject to Rules 1 and 2, and save in *solutionsInSingleLoop*
10: **if** (*PlaceSet* == $\emptyset$) **return** **end if**
11: **for** each feasible *placement* solution in *solutionsInSingleLoop*
12: ΔE_{DF} = DF lines in *placement*$-E_{DF0}$ // new DF lines placed
13: ΔE_{NDF} =NDF lines in *placement* // new NDF lines placed
14: $G_{DF1} = G_{DF}$, and update G_{DF1} by removing new NDF lines ΔE_{NDF}
15: dfs (G_{DF1}, $E_{DF} + \Delta E_{DF}$, $E_{NDF} + \Delta E_{NDF}$, V)
16: **end for**
17: **end dfs**

When a system operator has a constrained budget for D-FACTS devices, the number of D-FACTS devices can be reduced by removing D-FACTS devices from the hidden placement solution until the budget is met. Additionally, if D-FACTS devices are also used to minimize the power losses in the system operation, D-FACTS devices on lines with lower power loss to impedance sensitivity (PLIS) are suggested to be removed. However, one must take into consideration the impact of removing D-FACTS devices on the MTD hiddenness and detection effectiveness. Hiddenness can still exist after removing D-FACTS devices as long as $t_{\overline{DF}} > 1$ according to Lemma 1. This is because the removal of D-FACTS devices, equivalent to adding links to $G_{\overline{DF}}$, doesn't necessarily reduce $t_{\overline{DF}}$ to one. However, the D-FACTS placement ought to simultaneously guarantee the max rank of the composite matrix and cover all buses in loops to achieve the maximal detection effectiveness. Removing D-FACTS devices can result in uncovered buses and forming loops in $G_{\overline{DF}}$. Consequently, the rank of the composite matrix will decrease by the number of loops in $G_{\overline{DF}}$ and MTD cannot detect FDI attacks on uncovered buses.

The differences between the proposed hidden placement and the optimal D-FACTS placement established in our prior work [15] are summarized into the following two aspects. From the aspect of hiddenness, the proposed hidden placement requires the number of connected components in a non-D-FACTS graph to be greater than one to guarantee the existence of HMTD, whereas the optimal D-FACTS placement in [15] has no such requirement. From the aspect of detection capability, both placement methods ensure the max-rank MTDs. In [15], the optimal placement focuses on the minimum number of D-FACTS devices and certain buses may thus be uncovered. In contrast, the proposed hidden placement in this paper places D-FACTS lines and non-D-FACTS lines alternately in each loop such that all buses in loops are covered, contributing to much improved detection effectiveness.

In summary, the proposed hidden D-FACTS placement algorithm ensures 1) the maximum rank of the composite matrix; 2) the coverage of all necessary buses; and 3) the existence of the HMTD. To further achieve the HMTD with maximal detection effectiveness, we propose an HMTD operation model to determine setpoints of D-FACTS devices in the following subsections.

D. DC-HMTD Operation Model

The non-idle setpoints of D-FACTS devices ought to be delicately chosen in the HMTD operation. We propose a non-convex, nonlinear, optimization-based DC-HMTD operation model in (11), which maximizes the susceptance changes of D-FACTS lines and utilizes the hiddenness condition as constraints.

$$\max_{\mathbf{b},\mathbf{W}} \quad \left\|\mathbf{b}-\mathbf{b}_0\right\|_2 \tag{11}$$

$$s.t. \quad \bar{\mathbf{H}}_0\hat{\boldsymbol{\theta}}_0 = \bar{\mathbf{H}}(\mathbf{b})(\hat{\boldsymbol{\theta}}_0 + \Delta\boldsymbol{\theta}) \tag{11a}$$

$$\Delta\boldsymbol{\theta} = \mathbf{U}\mathbf{W} \tag{11b}$$

$$\mathbf{b}_0^{\min} \le \mathbf{b} \le \mathbf{b}_0^{\max} \tag{11c}$$

where $\mathbf{b}$ is the susceptance of each D-FACTS line, which is the reciprocal of reactance $\mathbf{x}$; $\mathbf{b}_0^{\min}$ and $\mathbf{b}_0^{\max}$ are the vector of lower and upper bound of susceptance for D-FACTS lines due to the physical capacity of D-FACTS devices;

$\mathbf{W} = [w_1, w_2, ..., w_s]^T \in \mathbb{R}$ is the vector of voltage angle incremental in each connected component of $G_{\overline{DF}}$. Note that we replace $\boldsymbol{\theta}_0$ in (4) with estimated nodal voltage angle $\hat{\boldsymbol{\theta}}_0$ in SE as $\boldsymbol{\theta}_0$ is unknown to system operators. Constraint (11a) aims to remain measurements of non-D-FACTS lines unchanged in HMTD. As measurements contain noises, we use the estimated measurements $\bar{\mathbf{H}}_0\hat{\boldsymbol{\theta}}_0$ instead to reduce the impact of noise. If significant measurement errors occur, BDD can detect and identify the erroneous measurements before running the proposed HMTD operation model.

The proposed model can be seamlessly integrated into the existing energy management system (EMS) in the system control room. Specifically, after determining the optimal generation and power flow using DC optimal power flow (OPF), the system operator can calculate the setpoints of the D-FACTS devices by solving model (11), and then send the calculated setpoints to the field devices for implementation. Note that while model (11) retains the power flow unchanged, it maximizes the susceptance changes for two purposes: 1) further deviating D-FACTS devices from their idle states; and 2) allowing sufficient changes to accommodate measurement noises. The proposed method is more robust and efficient in calculating the setpoints of D-FACTS devices due to its optimization-based model, compared with the random-weight-based HMTD method [12], referred to as RW-HMTD hereafter.

E. AC-HMTD Operation Model

In the construction of an AC-HMTD, a set of system measurements before HMTD is needed as a reference. This reference operating point is usually obtained by running ACOPF before HMTD, where the system operation cost and/or system losses are minimized. In a transmission system, it is reasonable to assume the voltage magnitude of each bus and the active power flow of each transmission line are measured in AC-SE [12]. An AC-HMTD operation model needs to reduce the measurement changes as much as possible to achieve MTD hiddenness. Additionally, this model ought to consider the economic benefits of D-FACTS devices in the power system operation [25]. Therefore, we propose an ACOPF-based HMTD operation model in (12), in which the reactance of each D-FACTS line is introduced as a decision variable in the traditional ACOPF. The proposed model minimizes a weighted sum of 1) the generation cost; 2) the negative of reactance changes, which is consistent with the proposed DC-HMTD model; and 3) the normalized difference in active power measurements before and after HMTD by relaxing the AC counterpart of the DC hiddenness equality constraint (11a).

$$\min_{\mathbf{Y}} \quad \lambda_0 cost(\mathbf{Y}) + \lambda_1 distP(\mathbf{Y}) - \lambda_2 distX(\mathbf{x}) \tag{12}$$

$$s.t. \quad cost(\mathbf{Y}) = \sum_{i=1}^{n_g} f^i(p_g^i) \tag{12a}$$

$$distP(\mathbf{Y}) = \sum_{i=1}^{n_l} (P_i^f - P_{i,0}^f)^2 / P_{i,0}^{f2} \tag{12b}$$

$$distX(\mathbf{x}) = \sum_{i \in E_{DF}} (x_i - x_i^0)^2 \tag{12c}$$

$$g_P(\boldsymbol{\theta}, \mathbf{V}, \mathbf{P_g}, \mathbf{x}) = 0 \tag{12d}$$

$$g_Q(\boldsymbol{\theta}, \mathbf{V}, \mathbf{Q_g}, \mathbf{x}) = 0 \tag{12e}$$

$$h_f(\boldsymbol{\theta}, \mathbf{V}, \mathbf{x}) \le 0 \tag{12f}$$

$$h_t(\boldsymbol{\theta}, \mathbf{V}, \mathbf{x}) \le 0 \tag{12g}$$

$$\theta_{ref} \le \theta_i \le \theta_{ref} \qquad i = 1 \tag{12h}$$

$$v_i^{\min} \le v_i \le v_i^{\max}, \qquad i = 1, ..., n_b \tag{12i}$$

$$p_i^{\min} \le p_i \le p_i^{\max}, \qquad i = 1, ..., n_g \tag{12j}$$

$$q_i^{\min} \le q_i \le q_i^{\max}, \qquad i = 1, ..., n_g \tag{12k}$$

$$| x_i - x_i^0 | \le \eta x_i^0, \qquad i \in E_{DF} \tag{12l}$$

In (12), $\mathbf{Y} = [\boldsymbol{\theta} \quad \mathbf{V} \quad \mathbf{P_g} \quad \mathbf{Q_g} \quad \mathbf{x}]$ are decision variables corresponding to voltage angle, voltage magnitude, generator active generation, generator reactive generation, and the reactance of D-FACTS lines, respectively; $cost(\mathbf{Y})$ is the system generation cost; $distP(\mathbf{Y})$ is the squared Euclidean distance between the normalized active power flow measurements before and after HMTD; $distX(\mathbf{x})$ is the squared Euclidean distance between the reactance before and after HMTD; λ_0, λ_1 and λ_2 are finely tuned weight parameters. In (12), active power flows and voltage magnitudes with subscript 0 are the measurements before HMTD; E_{DF} is the index set of D-FACTS lines; x_i^0 is the original reactance of i-th transmission line equipped with a D-FACTS device before HMTD; n_b, n_l, and n_g are the number of buses, lines, and generators, respectively. Constraints (12d) and (12e) are nonlinear equality constraints of the nodal active and reactive power balance, respectively. Constraints (12f) and (12g) are nonlinear inequality of line power flow limits corresponding to lines starting from from-end and to-end, respectively. Constraints (12h) and (12i) are voltage angle and magnitude constraints. Constraints (12j) and (12k) are generator constraints. In (12l), η in % reflects the physical capacity of D-FACTS devices and $\eta = 20\%$ is generally used in MTD [11]–[18]. In (12i), the per unit voltage magnitude boundary of Bus i is set as $v_i^{\max} = \min\{(1+\tau)v_{i,0},\ 1.05\}$ and $v_i^{\min} = \max\{(1-\tau)v_{i,0},\ 0.95\}$, where τ is the voltage perturbation magnitude. Note that a small τ ($\tau < 0.5\%$) is suggested to ensure the voltage stability and MTD hiddenness. We solve the proposed AC-HMTD operation model (12) by using a modified MATLAB Interior Point Solver based on our prior work [26].

It is worth mentioning that this paper focuses on constructing HMTD with maximal detection effectiveness in transmission systems traditionally equipped with SCADA measurements. If PMU devices are installed at certain buses in the transmission system, one can add specific constraints in the proposed DC-HMTD operation model (11) and introduce extra terms in the objective function of the proposed AC-HMTD model (12). For example, in the DC-HMTD operation model (11), we can set the elements in $\mathbf{W}$ corresponding to the buses equipped with PMU devices to zero such that the voltage angle of buses equipped with PMU devices remains unchanged after HMTD. In the AC-HMTD operation model (12), an additional term regarding the difference of PMU measurements before and after HMTD can be added into the objective function. However, this is beyond the scope of this work and will be investigated in our future work.

F. Cost-Benefit Analysis of DC- and AC-HMTD Models

We conduct qualitative cost-benefit analyses of HMTD in both the DC and AC models. We compare the system generation cost in the following four cases, as summarized in Table II. Case 0 is the base case, where the traditional OPF is conducted without MTD. Case 1 and Case 2 are the HMTD and RMTD, respectively. Case 3 is the OPF-based MTD [26], in which only generation cost is minimized while the hiddenness is not considered. The relationship among C_0, C_1, and C_2 has been discussed in [12]. In the DC model, the relationship is $C_0=C_1\leq C_2$ in a no-congestion condition and $C_0=C_1\geq\leq C_2$ in a transmission congestion condition [12]. In the AC model, the relationship is $C_1\leq C_0\geq\leq C_2$ [12]. Here, we focus on discussing the relationship between C_1 and C_3.

TABLE II
GENERATION COST IN OPF AND DIFFERENT MTD METHODS

C_0	Generation cost in OPF without MTD
C_1	Generation cost in HMTD
C_2	Generation cost in RMTD
C_3	Generation cost in OPF-based MTD

Compared with HMTD, the OPF-based MTD can dispatch the line reactance through D-FACTS devices to relieve line congestion within the physical operation range of D-FACTS devices. If the congestion is relieved, generation cost will decrease, i.e., $C_3\leq C_0$. If the congestion is not relieved at all or there is no congestion in the system, the generation cost in the OPF-based MTD is the same as that in OPF, i.e., $C_3=C_0$. In summary, we have $C_3=C_0=C_1\leq C_2$ in a no-congestion condition and $C_3\leq C_0=C_1\geq\leq C_2$ in a congestion condition in the DC model.

Since the constraints in the AC-HMTD operation model (12) are a subset of the constraints in the OPF-based MTD [26], the optimal solution obtained from AC-HMTD must be a feasible (but may not be the optimal) solution of the OPF-based MTD, i.e., $C_3\leq C_1$. Therefore, we have $C_3\leq C_1\leq C_0\geq\leq C_2$ in the AC model.

The qualitative cost-benefit analysis in both the DC and AC models above shows that HMTD will not increase generation costs as opposed to RMTD, but it may lead to a higher generation cost than that in the OPF-based MTD. As a result, HMTD accomplishes the MTD hiddenness by compromising the maximum economic benefits that D-FACTS devices could potentially achieve, representing a trade-off between the system economic and cybersecure operations.

IV. NUMERICAL RESULTS

A. Test Systems and Simulation Setting

We perform the proposed MTD planning and operation approach in the IEEE 14-bus system and the IEEE 57-bus system [27]. We use the former to show the hidden placement solution and the latter to evaluate both the hiddenness and detection effectiveness as opposed to other existing methods. In either system, we take a customary approach where multiple lines sharing the same from-bus and to-bus are merged as a single line. The D-FACTS placement algorithm is implemented using the Java programming language. We solve the DC-HMTD operation model using *fmincon* function of MATLAB. In a noisy condition, the measurement noise is assumed to be Gaussian distributed with zero mean and the standard deviation as 1% of the actual measurement. The threshold of BDD used by attackers and defenders is set to have a 1% false-positive rate. The algorithms are performed on a laptop with Intel Core i5 processor CPU 2.70 GHz dual-core with 8 GB RAM.

B. HMTD Planning Solution

The D-FACTS placement solution for the IEEE 14-bus system obtained by using Algorithms 1 and 2 is shown in Fig. 2. It is seen that both G_{DF} (the red graph) and $G_{\overline{DF}}$ (the black graph) are loopless, indicating the HMTD under this placement solution is a max-rank MTD. In addition, $G_{\overline{DF}}$ is a disconnected graph, which ensures the existence of HMTD. The D-FACTS and non-D-FACTS lines in each loop satisfy Rules 1 and 2, which prevents the D-FACTS devices from working idly. Furthermore, D-FACTS lines cover all buses except for Bus 8, which is not in any loop.

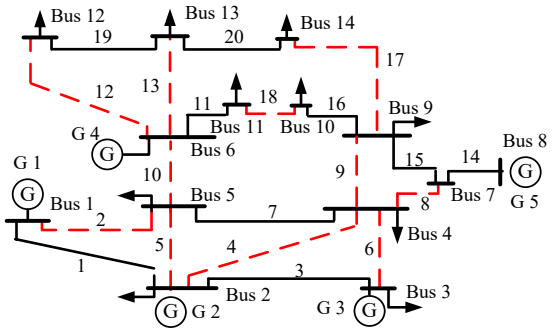


Fig. 2. Hidden D-FACTS placement of the IEEE 14-bus system.

In the IEEE 57-bus system, the proposed algorithms place D-FACTS devices on 47 lines, i.e., 60% of the transmission lines in this system, which are indexed by L_{DF}={2, 3, 4, 6, 9, 10, 11, 12, 13, 14, 15, 17, 19, 21, 22, 26, 29, 31, 32, 33, 35, 37, 39, 40, 43, 45, 46, 48, 50, 51, 52, 54, 57, 58, 59, 60, 63, 64, 67, 69, 71, 74, 75, 77, 78, 79, 80}.

C. DC-HMTD Operation Solutions

In this subsection, based on the hidden D-FACTS placement in the IEEE 57-bus system, we compare the HMTD operation model with the simplest MTD operation method, i.e., RMTD, in terms of the hiddenness and the detection effectiveness. We assume the attackers have the knowledge about the original line parameters and have read and write access to all measurements. In addition, the SE and BDD are used by attackers to detect if an MTD is in place.

We adopt a 24-hour load profile, which can be found at http://motor.ece.iit.edu/data. Under each load, we constructed 100 HMTDs and 100 RMTDs, respectively. For each MTD, we assume the attacker launch BDD 100 times. Then, the DSP of each MTD is calculated and their mean value is treated as the DSP under that given load.

Regarding DC-FDI attacks $\mathbf{a}=\mathbf{H}_0\Delta\boldsymbol{\theta}_a$, we generate 560 attack vectors, i.e., $\Delta\boldsymbol{\theta}_a$ with a single attack target bus, i.e., $\|\Delta\boldsymbol{\theta}_a\|_0=1$ as an attack pool. More specifically, we generate ten attack vectors for each bus in the IEEE 57-bus system (except for the reference bus), where the manipulated incremental voltage angle on the bus is uniformly distributed between (0.2, 0.4). For each MTD under each load, these 560 attacks, i.e., $\mathbf{a}=\mathbf{H}_0\Delta\boldsymbol{\theta}_a$, are injected into the real measurement

vector. Then, SE and BDD launched by system operators are used to detect the attacks. Similar to DSP, the ADP of each MTD is calculated, and their mean value is treated as the ADP under that given load.

Figure 3 demonstrates the ADP and the DSP of HMTDs and RMTDs versus different MTD magnitudes. Each node in Fig. 3 represents the corresponding ADP and DSP under one load condition. It is seen that the HMTD operation method is always hidden to attackers regardless of MTD magnitudes, while a larger MTD magnitude contributes to an improved DSP of the HMTD. With the same MTD magnitude, the HMTD outperforms RMTD in terms of detection effectiveness since the proposed HMTD operation model maximizes the susceptance changes to introduce more uncertainties for attackers. Additionally, when the MTD magnitude is small, the RMTD has very limited detection effectiveness, but it is hidden to attackers. This is because the susceptance changes introduced by the RMTD are too small to cause any change in power flow measurements. In RMTD, its DSP decreases while its ADP increases with an increase in the MTD magnitude.

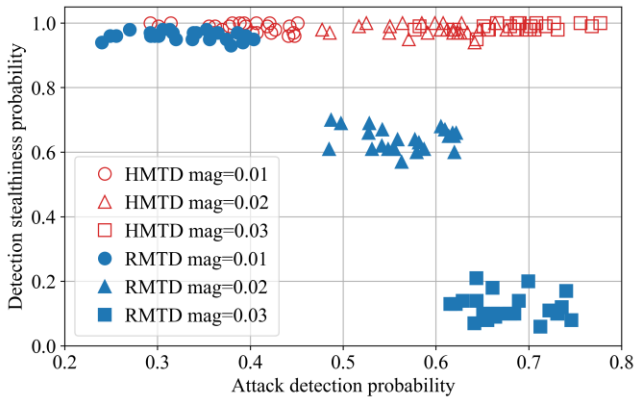


Fig. 3. ADP and DSP of HMTD and RMTD under different MTD magnitudes.

We evaluate the influence of variant loads on the hiddenness of the proposed HMTDs through simulations. Suppose the system operator launches MTDs every T time period and setpoints of D-FACTS devices only change at the beginning of each time period by the proposed HMTD operation model, while the load of each bus can vary during this time period. Thus, we test the hiddenness of the proposed HMTD method under different levels of load changes in the IEEE 57-bus system. First, we assume the load of each bus randomly varies in the following range, i.e., $d \in [(1-\lambda)d_0, (1+\lambda)d_0]$, where λ is the load changing magnitude and d_0 is the load used to construct HMTDs. In the attackers' point of view, an average DSP of 100 HMTDs is calculated when the system loads keep changing under the given load magnitude.

The impact of variant loads on the hiddenness of the proposed HMTD method under different levels of noise standard deviation σ is shown in Fig. 4. It is seen that the DSP decreases as the load magnitude increases. This is because the load changes result in power flow changes that deteriorate the hiddenness condition. In Fig. 4, a higher noise level mitigates the negative impact of variant load on the hiddenness, leading to a higher DSP. This can be explained by investigating the attacker's BDD. Specifically, a higher noise level makes the attacker's BDD tolerate higher deviations between the measured and estimated power flows.

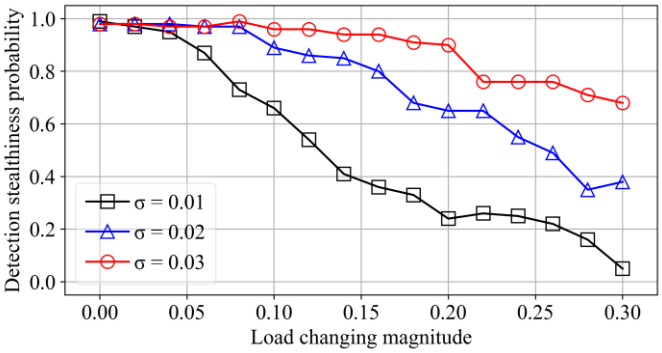


Fig. 4. The impact of variant loads on the hiddenness of proposed HMTD.

D. AC-HMTD Operation Solutions

In this subsection, we compare the proposed AC-HMTD operation model with the traditional ACOPF model based on the proposed hidden placement in the IEEE 14-bus system in terms of the generation cost, DSP and ADP. First, the traditional ACOPF is conducted in the IEEE 14-bus system, denoted as Case 0 (i.e., a no-MTD case), and its resultant measurements are adopted as the reference before HMTD. In Case 1, only the generation cost is minimized without considering the hiddenness or reactance changes. Accordingly, let λ_1 and λ_2 be zeros, and the lower and upper bounds on the voltage magnitude in (12i) be 0.95 and 1.05, respectively. In Cases 2, 3, and 4, we apply the proposed HMTD operation approach with a decreasing value of λ_0 in (12) to show the impact of λ_0 on the hiddenness.

A comparison of these five cases is summarized in Table III. Here, we choose the system without MTD (Case 0) as a baseline. We calculate the generation cost savings accrued by a MTD as MTD savings, and compare this to the generation cost in the baseline. In Table III, the average reactance changes in percentage (RCP) in the proposed HMTDs are more than 10%, which ensures the attack detection capability of HMTDs. It is observed that the proposed HMTD operation approach creates MTD savings compared to the baseline generation cost. Table III exhibits a trade-off between the MTD savings and its hiddenness. As seen in Table III, the MTD without considering the hiddenness in Case 1 has the highest MTD savings. When DSP increases to 90% in Case 4, its MTD savings decreases to $7.57. We further demonstrate the trade-off in Fig. 5, where λ_0 varies from 10^{-6} to 10^{-4}. With a decreasing λ_0, the hiddenness of MTD increases but the MTD savings decreases. The simulation results in Table III and Fig. 5 verify the cost-benefit analysis of HMTD in Section III.F.

We further evaluate the detection effectiveness of the proposed AC-HMTD operation model in the IEEE 14-bus system. We construct 130 single-bus AC-FDI attacks, in which each bus is attacked ten times except for the reference bus. Each attack is launched on each of MTDs outlined in Table III. The ADP of each MTD is calculated as shown in the last column of Table III. As the node degree of Bus 8 is one, attacks on Bus 8 are undetectable due to a limitation of MTD [18]. Thus, the largest ADP in the IEEE 14-bus system is 92.3%. The ADP of HMTDs in Cases 3 and 4 is lower than 92.3% since the reactance change of Line 4-7 is low under the given load. The

attack detection performance of the AC-HMTD is consistent with that in the DC model.

TABLE III
THE PERFORMANCE OF AC-HMTD OPERATION

Case	λ_0	λ_1	λ_2	Cost ($)	MTD saving ($)	DSP (%)	RCP (%)	ADP (%)
0	1	N/A	N/A	8131.52	0	N/A	0	N/A
1	1	0	0	8115.69	15.83	0	18.0	92.3
2	1e-4	0.01	0.05	8119.36	12.16	1.0	11.0	92.3
3	1e-5	0.01	0.05	8122.67	8.85	83.0	12.2	83.1
4	1e-6	0.01	0.05	8123.95	7.57	90.0	12.2	85.4

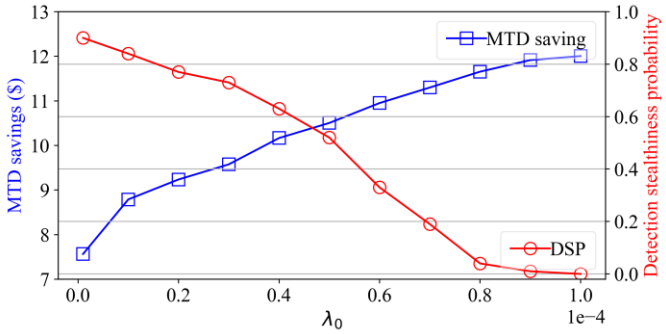


Fig. 5. The trade-off between MTD savings and MTD hiddenness under different λ_0.

E. Comparison between Proposed and Existing HMTD Operations

In this section, we compare the proposed HMTD operating method (11) with RW-HMTD [12] under the proposed D-FACTS placement in both the IEEE 14-bus and 57-bus systems.

In the RW-HMTD, a weight searching range must be initialized to find a feasible solution. However, strategies of searching range initialization are not provided in [12]. In this case, we design two simple strategies, i.e., a direct searching and an indirect searching strategy. The direct searching method sets the searching boundary using searching radius γ, i.e., $w \in [-\gamma, \gamma]$. The indirect searching method takes the solution w_0 from (11) as the center and then specifies the searching radius using a factor β, i.e., $w \in [(1-\beta)w_0, (1+\beta)w_0]$. Note that 4 weights and 25 weights need to be determined by HMTD in IEEE 14-bus and 57-bus systems, respectively. In RW-HMTD, we apply the direct searching method in the IEEE 14-bus system and the indirect searching method in the IEEE 57-bus system. This is because the direct searching method fails to find feasible solutions in the IEEE 57-bus system in a reasonable amount of time. We have to take advantage of the results in our proposed method and narrow down the searching range using the indirect searching method.

The performance of the proposed HMTD operation is summarized in Table IV. It is observed that the reactance changes more than 14% compared with the original line reactance in both systems. The CPU time of the proposed HMTD operation is less than 1.1 seconds in both systems. The performance of the RW-HMTD in the 14-bus and 57-bus systems is summarized in Tables V and VI, respectively. We obtain five feasible solutions in each searching range and then calculate the minimum, maximum, and mean of the reactance changes in percentage (RCP) as well as the CPU time. It is observed that the CPU time dramatically increases as the searching radius increases, especially in the IEEE 57-bus system. The RCP can be as low as 3.16% in the IEEE 14-bus system. In the IEEE 57-bus system, the RCP decreases accordingly when the searching radius increases. This is because the RW-HMTD solutions obtained within a larger searching range may deviate further from the optimal solution (i.e., the largest RCP point) provided by our proposed model (11).

We further compare the detection effectiveness of the proposed HMTD and three RW-HMTDs under FDI attacks with different voltage angle injection magnitudes (VAIM) in the IEEE 14-bus system. Specifically, FDI attacks with $\Delta\boldsymbol{\theta}_a$ are randomly generated in the range $\Delta\boldsymbol{\theta}_a \in [0.8, 1.2] \cdot \bar{\boldsymbol{\theta}} \cdot VAIM$, where VAIM reflects the strength of FDI attacks. Comparative results are shown in Fig. 6. The proposed HMTD has the largest ADP. Low reactance changes in RW-HMTD decrease the detection capability of MTDs, especially under the FDI attacks with the small voltage angle injection magnitude. Note that these three RW-HMTDs are constructed under the proposed HMTD placement solution, which has maximal detection effectiveness. If an RW-HMTD is constructed under other placements, its ADP can further decrease.

In summary, the drawbacks of the RW-HMTD method [12] are two-fold. First, this method may generate an MTD with small reactance changes resulting in a low attack detection capability. Second, its CPU time heavily depends on the weight searching range. A larger searching radius will result in a much longer searching time, especially in large-scale systems. To make things worse, an improper searching range can cause no solution obtained. The proposed method circumvents these drawbacks by utilizing optimization to find the largest reactance changes in HMTD efficiently.

TABLE IV
PERFORMANCE OF THE PROPOSED HMTD OPERATION

System	RCP (%)	CPU Time (s)
14-bus System	14.50	0.31
57-bus System	14.71	1.06

TABLE V
PERFORMANCE OF RW-HMTD USING DIRECT SEARCHING IN THE IEEE 14-BUS SYSTEM

Searching range	RCP (%)			CPU Time (s)		
	min	max	mean	min	max	mean
[-0.01,0.01]	3.16	12.10	7.35	0.001	0.021	0.007
[-0.05,0.05]	6.48	8.70	7.76	0.002	0.506	0.200
[-0.10,0.10]	3.54	11.00	7.69	0.868	3.901	1.950
[-0.15,0.15]	5.11	9.64	7.84	2.872	31.351	19.702
[-0.20,0.20]	5.90	8.97	7.51	0.348	91.923	30.409

TABLE VI
PERFORMANCE OF RW-HMTD USING INDIRECT SEARCHING IN THE IEEE 57-BUS SYSTEM

Factor β	RCP (%)			CPU Time (s)		
	min	max	mean	min	max	mean
0.05	12.62	12.84	12.73	1.4	20.1	9.1
0.10	11.45	12.76	12.10	20.0	192.2	97.5
0.15	10.79	11.57	11.31	20.4	2488.2	741.9

0.20	10.01	11.30	10.80	400.2	3185.2	2374.9

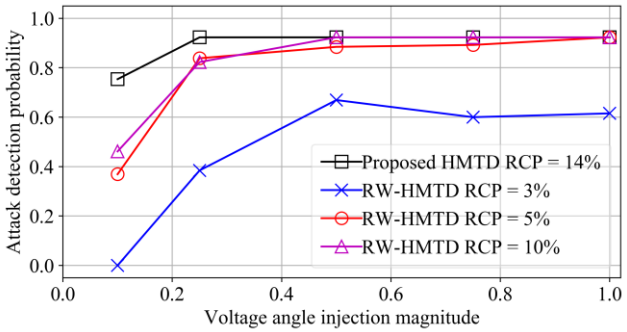


Fig. 6. ADP of RW-HMTD and proposed HMTD under FDI attacks with different VAIMs.

F. Comparison between Hidden and Existing Placements

In this subsection, we compare the proposed D-FACTS placement with the other four existing D-FACTS placements, including the optimal placement [15], a full placement, the arbitrary placement [11], and the spanning-tree placement [18]. These D-FACTS placements are summarized in Table VII. Except for the optimal placement and the hidden placement, the rank of the composite matrix under other placements depends on the setpoints of D-FACTS devices.

TABLE VII
EXISTING D-FACTS PLACEMENT ALGORITHMS

Placement Algorithm	Description of D-FACTS Placement	p_1
Arbitrary placement [11]	Install on the randomly selected lines	47
Full placement	Install on all transmission lines	78
Spanning-tree placement [18]	Install on lines that form a spanning tree of the system topology	56
Optimal placement [15]	Non-D-FACTS lines form a spanning tree, and D-FACTS are placed on the remaining lines	22

Consistent with the experiment setup in the previous subsection, we apply MTDs under the above placement and calculate the ADP and the DSP under each load with a fixed MTD magnitude of 0.2. We run the HMTD operation model under the hidden D-FACTS placement and RMTDs under other D-FACTS placements. It is worthwhile to mention that the same attack pool is used to calculate the ADP. The ADP and the DSP under five D-FACTS placements are shown in Fig. 7. As seen, MTDs under the hidden placement are hidden to attackers, while MTDs under the optimal placement can be detected by attackers. In addition, the ADP of MTDs under the hidden placement is higher than that under the optimal placement due to the covered buses in the hidden placement. RMTDs under the other placements can always be detected by attackers.

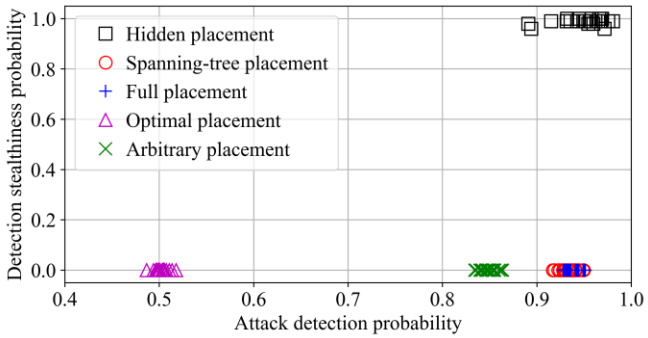


Fig. 7. ADP and DSP of five D-FACTS placements under 0.2 MTD magnitude.

Even though the rank of the composite matrix is maximized, the optimal placement has the worst detection effectiveness due to 27 uncovered buses. Arbitrary placement uses extra 25 D-FACTS devices compared with that in the optimal placement. The arbitrary placement used in this case study has five uncovered buses. Thus, its detection effectiveness is better than the optimal placement but worse than either the spanning-tree placement or the full placement. Both the spanning-free and the full placements have similar detection effectiveness since they both cover all the buses using the D-FACTS devices. However, their ADPs are still worse than that of the hidden placement. This is because their rank of the composite matrix depends on the setpoints of D-FACTS devices. Specifically, if the reactance of all lines connected to one bus is modified by multiplying a unity factor, their rank of the composite matrix will decrease by one. Consequently, any FDI attack on this bus is undetectable.

Figure 8 demonstrates a transition between the MTD hiddenness and the detection effectiveness in each D-FACTS placement. For each placement, we apply six discrete MTD magnitudes, i.e., 1%, 2%, 3%, 4%, 5%, and 20%, to calculate the ADP and the DSP. Note that the green arrows on each line in Fig. 8 show the direction in which the MTD magnitude is increasing. We observe, for the first time, that the proposed MTD planning and operation method is always hidden to attackers and provides an excellent ADP under the MTD magnitude of 0.2. In comparison, when the MTD magnitude is increased, each other placement shows a clear transition from a low ADP with a high DSP to a high ADP with a low DSP. As opposed to the MTD hiddenness, the detection effectiveness of MTDs is the fundamental requirement. Therefore, a large MTD magnitude is always desirable for the RMTD operation.

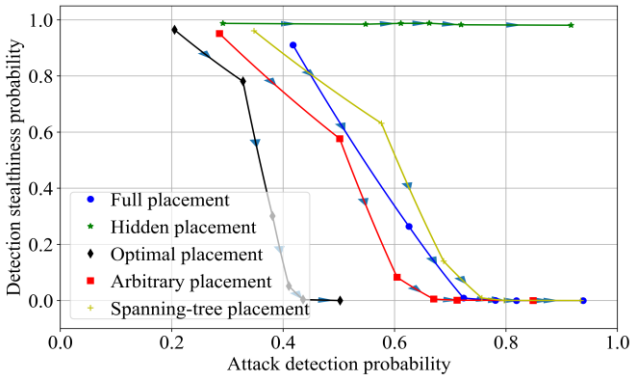


Fig. 8. ADP and DSP of five D-FACTS placements with MTD magnitude varying from 1% to 20%.

V. CONCLUSIONS

In this paper we propose a DFS-based hidden D-FACTS devices planning algorithm as well as the DC- and AC-HMTD operation models. We emphasize that the MTD hiddenness and detection effectiveness can be achieved simultaneously in incomplete MTDs. The proposed planning algorithm ensures the existence of HMTD and enables MTDs to have maximal detection effectiveness. The proposed placement uses fewer D-FACTS devices to reach the maximal detection effectiveness compared to the full placement and spanning-tree placement.

We propose an optimization-based DC-HMTD operation model, which integrates the derived hiddenness condition as

constraints. Case studies show that the proposed model is superior to the existing HMTD operation method in terms of computational time and detection effectiveness. The transition between the MTD hiddenness and the detection effectiveness versus the MTD magnitude is also presented. Additionally, we propose an ACOPF-based HMTD operation model, which minimizes the generation cost and achieves the MTD hiddenness. Simulation results show a trade-off between the generation cost savings by MTD and MTD hiddenness in the AC-HMTD operation. The results demonstrate that the attack detection performance of AC-HMTD is consistent with that in the DC model. With the advent of PMU devices in the smart grid, we will integrate these devices into HMTD planning and operation methods in our future work.

ACKNOWLEDGMENT

This material is based upon work supported in part by the U.S. National Science Foundation under Grant No. 1929147 and in part by the U.S. Department of Energy under Award No. DE-EE0008767.

REFERENCES

[1] G. Simard, "IEEE Grid Vision 2050," *IEEE Grid Vis. 2050*, pp. 1–93, Apr. 2013.

[2] A. S. Musleh, G. Chen, and Z. Y. Dong, "A Survey on the Detection Algorithms for False Data Injection Attacks in Smart Grids," *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2218–2234, May 2020.

[3] 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.

[4] C. Liu, J. Wu, C. Long, and Y. Wang, "Dynamic State Recovery for Cyber-Physical Systems Under Switching Location Attacks," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 1, pp. 14–22, Mar. 2017.

[5] 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, p. 13:1-13:33, Jun. 2011.

[6] T. A. Youssef, M. E. Hariri, N. Bugay, and O. A. Mohammed, "IEC 61850: Technology standards and cyber-threats," in *2016 IEEE 16th International Conference on Environment and Electrical Engineering (EEEIC)*, Jun. 2016, pp. 1–6.

[7] H. Zhang, B. Liu, and H. Wu, "Smart Grid Cyber-Physical Attack and Defense: A Review," *IEEE Access*, vol. 9, pp. 29641–29659, 2021.

[8] K. L. Morrow, E. Heine, K. M. Rogers, R. B. Bobba, and T. J. Overbye, "Topology Perturbation for Detecting Malicious Data Injection," in *2012 45th Hawaii International Conference on System Sciences*, Jan. 2012, pp. 2104–2113.

[9] S. Lakshminarayana, E. V. Belmega and H. V. Poor, "Moving-Target Defense for Detecting Coordinated Cyber-Physical Attacks in Power Grids," *2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, Beijing, China, 2019, pp. 1-7.

[10] 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.

[11] M. A. Rahman, E. Al-Shaer, and R. B. Bobba, "Moving Target Defense for Hardening the Security of the Power System State Estimation," in *Proceedings of the First ACM Workshop on Moving Target Defense*, New York, NY, USA, 2014, pp. 59–68.

[12] 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.

[13] 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 *2018 IEEE Power Energy Society General Meeting (PESGM)*, Aug. 2018, pp. 1–5.

[14] Z. Zhang, R. Deng, D. Yau, P. Cheng, and J. Chen, "On Hiddenness of Moving Target Defense against False Data Injection Attacks on Power Grid," in *ACM Transactions on Cyber-Physical Systems*, vol. 4, no. 3, pp. 1–29, 2020.

[15] B. Liu and H. Wu, "Optimal D-FACTS Placement in Moving Target Defense against False Data Injection Attacks," *IEEE Trans. Smart Grid*, pp. 1–1, 2020.

[16] 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. Forensics Secur.*, pp. 1–1, 2019.

[17] 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.

[18] 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. Inform.*, pp. 1–1, 2019.

[19] D. Divan and H. Johal, "Distributed FACTS - A New Concept for Realizing Grid Power Flow Control," in *2005 IEEE 36th Power Electronics Specialists Conference*, Jun. 2005, pp. 8–14.

[20] "A Mobile Unit Tours Europe, Smart Wires in India and More," *Smart Wires Inc.* https://www.smartwires.com/portfolio-item/8245/ (accessed Dec. 29, 2019).

[21] K. Jhala, P. Pradhan, and B. Natarajan, "Perturbation-Based Diagnosis of False Data Injection Attack Using Distributed Energy Resources," *IEEE Trans. Smart Grid*, vol. 12, no. 2, pp. 1589–1601, Mar. 2021.

[22] S. Lakshminarayana and D. K. Y. Yau, "Cost-Benefit Analysis of Moving-Target Defense in Power Grids," in *2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, Jun. 2018, pp. 139–150.

[23] Y. Huang *et al.*, "Bad data injection in smart grid: attack and defense mechanisms," *IEEE Commun. Mag.*, vol. 51, no. 1, pp. 27–33, Jan. 2013.

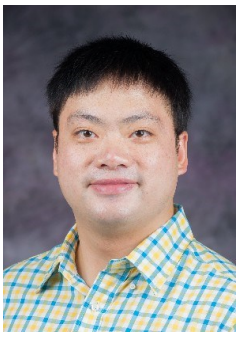
[24] U. Agarwal and U. P. Singh, *Graph Theory*. Laxmi Publications, 2009.

[25] K. M. Rogers and T. J. Overbye, "Some applications of Distributed Flexible AC Transmission System (D-FACTS) devices in power systems," in *2008 40th North American Power Symposium*, Sep. 2008, pp. 1–8.

[26] B. Liu, L. Edmonds, H. Zhang, and H. Wu, "An Interior-Point Solver for Optimal Power Flow Problem Considering Distributed FACTS Devices," in *2020 IEEE Kansas Power and Energy Conference (KPEC)*, Jul. 2020, pp. 1–5.

[27] R. D. Zimmerman, C. E. Murillo-Sanchez, and R. J. Thomas, "MATPOWER: Steady-State Operations, Planning, and Analysis Tools for Power Systems Research and Education," *IEEE Trans. Power Syst.*, vol. 26, no. 1, pp. 12–19, Feb. 2011.

Bo Liu (S'18) received his B.S. and M.S. degree in Electrical Engineering at Harbin Institute of Technology, China in 2013 and 2015, respectively. He received his Ph.D. degree in Electical Engineering at Kansas State University, Manhattan, KS, USA in 2021. He is a Senior Research Associate in Smart Energy System Group at the Mike Wiegers Department of Electrical and Computer Engineering, Kansas State University, Manhattan, KS, USA. His current research interests include cyber-physical security of power systems, smart grid technologies, machine learning, and state estimation in smart grids.



Hongyu Wu (SM'15) received his B.S. degree in Energy and Power Engineering and the Ph.D. degree in Control Science and Engineering from Xi'an Jiaotong University, Xi'an, China, respectively. He is an Associate Professor and a Michelle Munson-Serban Simu Keystone Research Faculty Scholar with the Mike Wiegers Department of Electrical and Computer Engineering, Kansas State University (K-State), Manhattan, KS, USA. He is a National Science Foundation EPSCoR research fellow and a team member of the IEEE-NERC Security Integration Project. Before joining K-State, he was a Research Engineer with Power Systems Engineering Center, National Renewable Energy Laboratory, Golden, CO, USA. From 2011 to 2014, he was a Postdoctoral Researcher with the Robert W. Galvin Center for Electricity Innovation, Illinois Institute of Technology, Chicago, IL, USA. His research interests include cyber-physical security of smart grids, power system planning, operation and energy management, as well as grid integration of renewable energy.