ORIGINAL RESEARCH PAPER

Systematic planning of moving target defence for maximising detection effectiveness against false data injection attacks in smart grid

Bo Liu  |  Hongyu Wu

Mike Wiegers Department of Electrical and Computer Engineering, Kansas State University, Manhattan, Kansas, USA

Correspondence
Hongyu Wu, Department of Electrical and Computer Engineering, Kansas State University, 1707D Pratt St., Manhattan, KS 66506, USA.
Email: hongyuwu@ksu.edu

Funding information
U. S. Department of Energy; United States, Grant/Award Number: DE-EE0008767; National Science Foundation; United States, Grant/Award Number: 1929147

Abstract
Moving target defence (MTD) has been gaining traction to thwart false data injection attacks against state estimation (SE) in the power grid. MTD actively perturbs the reactance of transmission lines equipped with distributed flexible AC transmission system (D-FACTS) devices to falsify the attacker’s knowledge about the system configuration. However, the existing literature has not systematically studied what influences the detection effectiveness of MTD and how it can be improved based on the topology analysis. These problems are tackled here from the perspective of an MTD plan in which the D-FACTS placement is determined. We first exploit the relation between the rank of the composite matrix and the detecting effectiveness. Then, we rigorously derive upper and lower bounds on the attack detecting probability of MTDs with a given rank of the composite matrix. Furthermore, we analyse existing planning methods and highlight the importance of bus coverage by D-FACTS devices. To improve the detection effectiveness, we propose a novel graph theory–based planning algorithm to retain the maximum rank of the composite matrix while covering all necessary buses. Comparative results on multiple systems show the high detecting effectiveness of the proposed algorithm in both DC- and AC-SE.

1 | INTRODUCTION

Modern power systems have been more efficient in production, more intelligent in system operations and more flexible in integrating new devices based on interconnections with underlying cyber components in recent years. However, this interdependence between the physical power system and cybercommunication system also brings vulnerabilities to the system [1]. Cyberattacks targeting power systems have resulted in both tremendous economic loss and security issues [2]. For instance, a cyberattack took place in Ukraine on 23 December 2015, resulting in a wide blackout, which affected seven 110-kV and 23-kV substations and 225,000 customers [3].

The supervisory control and data acquisition (SCADA) system uses state estimation (SE) to monitor the grid operation and uses residual-based bad data detection (BDD) to detect erroneous measurements and malicious cyberattacks. However, false data injection (FDI) attacks have become a growing threat to power systems. FDI attacks inject malicious data into SCADA measurements to modify grid voltage estimated in SE without being detected by the BDD algorithm. In the literature, FDI attacks gained much interest in modelling FDI attacks in DC and AC systems [4–6] constructing FDI attacks with concrete attack objectives [7, 8], detecting and preventing FDI attacks [9–13], and evaluating the consequence of FDI attacks [8]. This is because the attack surface in smart grids for FDI attacks is huge, and the consequence of FDI attacks is non-negligible. First, an FDI attack can cheat the power system SE, which is the basis of many power system applications, such as contingency analysis and economic dispatch [14]. Falsified SE results could potentially mislead the operation and the autocontrol mechanism of energy management system [15]. Second, FDI attacks can attack energy markets [16, 17], which can represent a serious financial deviation.
sophisticated FDI attacks can have consequences for grid operation conditions, such as transmission line overload [8] and nodal voltage violation [7], resulting in blackout and even cascading failures. Therefore, it is greatly important to detect and thwart FDI attacks in power systems.

Moving target defence (MTD) is a proactive defence algorithm originally used in the network system; it was introduced into the power grid to thwart FDI attacks. It actively perturbs branch impedance using distributed flexible AC transmission system (D-FACTS) devices [18, 19] and invalidates attackers' knowledge about power system configurations essential for constructing stealth FDI attacks. There are two essential problems in constructing an MTD: MTD planning and operation. In the planning stage, a system operator must figure out how to install D-FACTS devices on an appropriately identified subset of transmission lines, which corresponds to a D-FACTS placement problem. Then, the system operator needs to dispatch D-FACTS setpoints in a real-time operation, namely an MTD operation problem.

The MTD approach has been applied to detect coordinated cyber-physical attacks and Stuxnet-like attacks against power grids [20, 21], in which fake sensor measurements are injected to cover ongoing attacks. However, most MTD approaches are designed to detect FDI attacks against SE buses, uncoordinated multibus FDI attacks will degrade to an uncoordinated attack. Furthermore, the spanning-tree planning method cannot guarantee the maximum rank of the composite matrix. A heuristic-based planning method was proposed to minimise the stealthy attack space, which is equivalent to maximising the rank of the composite matrix [29]. Meanwhile, it used D-FACTS devices to cover the largest number of buses. This algorithm maximised the rank of the composite matrix by updating the reactance of each transmission line one by one. In Liu et al. [30], it was proven that the rank of the composite matrix could be determined by MTD planning regardless of the D-FACTS setpoints. Furthermore, a max-rank planning method was proposed in Liu et al. [30] to achieve the maximum rank of the composite matrix using the minimum number of D-FACTS devices.

These max-rank planning methods focus on constructing MTDs with the maximum rank of the composite matrix through a rank maximisation–based method [26] or graph-based method [30]. Although a larger rank of the composite matrix indicates better detection effectiveness (Remark 3 [26]), as we will point out, the maximum rank of the composite matrix is not strictly equivalent to maximal MTD detection effectiveness. In fact, constructing max-rank MTDs is far from achieving the maximal detection effectiveness, which is revealed through both theoretical analysis and numerical results in this work. Therefore, it is still an open and pressing issue to enhance the max-rank planning methods and improve their detection effectiveness, one of the most important concerns in a defence algorithm.

In the literature, two knowledge gaps exist. First, the lack of a metric that measures the MTD detection effectiveness and lays a theoretical foundation for analysing MTD operation and planning. Specifically, a novel metric is needed to quantify the detection effectiveness of an MTD after the maximum rank of the composite matrix is achieved. Second, the lack of an MTD planning method that ensures the maximal detection effectiveness while considering economic benefits from D-FACTS devices. Hence, how to reflect the MTD detection effectiveness accurately and improve detection effectiveness are essential yet unresolved issues.

This work addresses these issues from the standpoint of MTD planning. Specifically, MTD detection effectiveness is theoretically analysed and an MTD planning algorithm is proposed that ensures maximal detection effectiveness while considering economic benefits from D-FACTS devices. We first define protected and unprotected buses in MTDs. Then, we introduce attack detection probability (ADP) as a new detection effectiveness metric into both MTD operation and planning. For MTD planning, the number of protected buses determines its ADP lower bound, whereas the number of unprotected buses decides its ADP upper bound that was neglected in all existing max-rank planning methods in the literature. The contributions of this work are that:

1. Attention has been increasingly paid to the relation between MTD planning and MTD detecting effectiveness. In Li et al. [28], installing D-FACTS devices on a spanning tree of the power system topology could effectively detect three specific types of FDI attacks: single-bus, uncoordinated multibus, and coordinated multibus attacks. However, the spanning-tree planning method, which was designed to detect coordinated multibus FDI attacks, seems unnecessary. Without the accurate location of D-FACTS devices, which is strictly classified and may not be accessible to attackers, a coordinated multibus FDI attack will degrade to an uncoordinated attack.

2. In Liu et al. [30], it was proven that the rank of the composite matrix could be determined by MTD planning regardless of the D-FACTS setpoints. Furthermore, a max-rank planning method was proposed in Liu et al. [30] to achieve the maximum rank of the composite matrix using the minimum number of D-FACTS devices.

3. These max-rank planning methods focus on constructing MTDs with the maximum rank of the composite matrix through a rank maximisation–based method [26] or graph-based method [30]. Although a larger rank of the composite matrix indicates better detection effectiveness (Remark 3 [26]), as we will point out, the maximum rank of the composite matrix is not strictly equivalent to maximal MTD detection effectiveness. In fact, constructing max-rank MTDs is far from achieving the maximal detection effectiveness, which is revealed through both theoretical analysis and numerical results in this work. Therefore, it is still an open and pressing issue to enhance the max-rank planning methods and improve their detection effectiveness, one of the most important concerns in a defence algorithm.
• We prove that the rank of the composite matrix reflects only the minimum number of protected buses. We show, for the first time, that the rank of the composite matrix, a widely used indicator of MTD detection effectiveness, is merely an ADP lower bound.

• We identify and prove three types of unprotected buses in MTDs (end buses, non-D-FACTS buses, and buses fully covered by D-FACTS lines), whose reactances are modified using a unity factor. We highlight the importance of eliminating unprotected buses in MTD planning to improve the ADP upper bound.

• We mathematically derive and prove the ADP range of different MTD planning methods, which is verified by extensive simulations. Furthermore, we identify a class of MTD planning solutions with a fixed ADP.

• We propose a novel graph theory–based MTD planning method to ensure maximal detection effectiveness while considering economic benefits from D-FACTS devices. Specifically, the proposed method maximises the ADP lower and upper bound by maximising the rank of the composite matrix and eliminating unprotected buses simultaneously.

• We conduct case studies on IEEE 14-bus, IEEE 118-bus, and 3012-bus systems. We compare the ADP of the proposed planning method with that of the max-rank planning method, the arbitrary planning method, and the full planning method in both DC- and AC-SE.

The rest of this work is organised as follows. We provide preliminaries and related work in Section 2. In Section 3, we analyse MTD detection effectiveness and propose a graph theory–based planning method. We compare the ADP of the proposed planning method with that of other planning methods in Section 4. Conclusions are drawn in Section 5.

2 | PRELIMINARIES

In this section, we review FDI attacks against SE, the MTD in the power system, as well as existing MTD planning methods.

2.1 | Notation

We summarise variables frequently used throughout this work in Table 1, where boldfaced lower- and upper-case letters stand for vectors and matrices, respectively. Subscript 0 represents variables before the implementation of an MTD. For example, $H_0$ represents the original measurement matrix before an MTD, whereas $H$ stands for the one after implementing the MTD. ‘D-FACTS lines’ and ‘non-D-FACTS lines’ denote the set of lines equipped with and without D-FACTS devices, respectively. ‘Non-D-FACTS buses’ represent the set of buses only connected to non-D-FACTS lines, whereas the remaining buses in the system are ‘D-FACTS buses’, referring to the set of buses connected to at least one D-FACTS line. An end bus refers to a bus that is only connected by one single line. Let $G$ be a graph of a power system composed of all transmission lines and buses. Let $G_{DF}$, termed a D-FACTS graph, be a subgraph of $G$ consisting of D-FACTS lines and all buses. Similarly, let $G_{TF}$ be a subgraph of $G$ consisting of non-D-FACTS lines and all buses. Let a reduced D-FACTS graph denote a graph only composed of D-FACTS lines and D-FACTS buses.

| Symbol | Definition |
|--------|------------|
| $\theta$ | Voltage angle of buses excluding reference bus |
| $z$ | Measurement vector |
| $a$ | False data injection attack vector |
| $z_0$ | Compromised measurement vector |
| $H$ | DC measurement matrix in state estimation |
| $h_i$ | The $i$-th column in $H$ (corresponding to bus $i$) |
| $M$ | Composite matrix of $H_0$ and $H$ |
| $x_{ij}$ | Reactance of line $i$-$j$ (between bus $i$ and bus $j$) |
| $n$ | Total number of system buses |
| $n_1$ | Total number of D-FACTS buses |
| $n_2$ | Total number of non-D-FACTS buses |
| $n_e$ | Total number of end buses |
| $n_{1e}$ | Total number of end buses belonging to D-FACTS buses |
| $n_{2/e}$ | Total number of non-D-FACTS buses excluding end buses |
| $m$ | Total number of measurements |
| $p$ | Total number of lines |
| $p_{1}$ | Total number of D-FACTS-equipped lines |
| $p_{2}$ | Total number of lines without D-FACTS |
| $lp$ | Total number of loops in a graph |
| $t$ | Total number of disconnected components in a graph |
| $r(\cdot)$ | Matrix rank operator |
| $\text{col}(\cdot)$ | Column space operator |

Abbreviation: D-FACTS, distributed flexible AC transmission system.

2.2 | False data injection attacks against state estimation

This work mainly uses the DC flow model to study MTD planning because it is faster and more robust than AC power flow analysis [4, 23]. DC SE uses measurements sampled from nodal power injection sensors and branch power flow sensors, denoted by $z \in \mathbb{R}^m$, to estimate the voltage angles $\theta \in \mathbb{R}^{n-1}$. The relation of the measurements and voltage angle can be modelled as $z = H \cdot \theta + e$, where $e$ is measurement noises. The voltage angle can be estimated by $\theta = (H^T WH)^{-1} H^T W z$.

The measurement residual is calculated in the BDD to detect bad data in the system [31]. Based on the $\chi^2$ test, a system is free of bad data if the inequality $\gamma = \|z - H \cdot \theta\|^2 < \gamma_{ib}$.
holds, where \( y_{ik} = \chi_{(m-n),i}^2 \) is a preset threshold to ensure the BDD has a false alarm rate of \( 1 - \alpha \).

An FDI attack against SE is a type of cyberattack to compromise measurements without triggering BDD. More specifically, FDI attack injects false data into the measurements, that is, \( a \in \text{col}(H) \) for keeping the attack stealthy [6]. Thus, it requires the attacker’s knowledge about system topology and line parameters, that is, \( H \) matrix. For simplicity, attack vector \( a \) is expressed as \( a = H \cdot \Delta \theta \), where \( \Delta \theta \) is the increase in voltage angle injected by attackers [26].

2.3 Moving target defence in power system

\[ z_a = z + a \text{MTD} \]

MTD takes advantage of D-FACTS devices to create uncertainties for attackers. D-FACTS devices can receive remote control commands to alter their operating setpoints through the communication infrastructure [32, 33]. The incremental reactance of line \( i-j \) can be periodically modified by the D-FACTS device within \( |x_{ij}^0| \leq |\Delta x_{ij}| \leq |x_{ij}^0| \), where upper bound \( \eta \) reflects the physical capacity of D-FACTS devices, and lower bound \( \tau \) prevents the D-FACTS devices from working in an idle state, i.e., \( \Delta x_{ij} = 0 \). Consequently, \( H \) used in the SE becomes a time-variant matrix. If attackers construct FDI attacks using outdated knowledge of \( H \), the estimation residual in defender’s BDD is no longer zero.

With MTDs deployed in the power system, an FDI attack constructed using the outdated measurement matrix, that is, \( a = H_0 \cdot \Delta \theta \), where \( \Delta \theta \neq 0 \), is detectable if and only if \( H_0 \cdot \theta \neq \text{H}_0 \cdot \Delta \theta \) for any \( \theta \). In addition, any FDI attacks can be detected in the noiseless environment if attack vector \( a \) is not in the column space of \( H \) after MTDs, that is, \( a \notin \text{col}(H) \) [26].

2.4 MTD detection effectiveness and planning

MTD detection effectiveness can be measured by the rank of the composite matrix, \( M = [H_0, H] \) [26]. An MTD with \( r(M) = 2(n-1) \) is a complete MTD, which can detect all FDI attacks [26]. However, the requirements of a complete MTD on the system topology are stringent for most power systems. Only incomplete MTDs are achievable for most power systems whose \( r(M) \) is less than \( 2(n-1) \). An MTD with a larger value of \( r(M) \) is desirable because it has better detection effectiveness [26].

The rank of the composite matrix, that is, \( r(M) \), can be determined by MTD planning, as shown in Equation (1), if \( G_{DF} \) is loopless [30]. It indicates that each loop in \( G_{DF} \) decreases \( r(M) \) by 1. Therefore, an MTD is an incomplete MTD with the maximum rank of the composite matrix, if the MTD plan ensures that there exists no loop in either \( G_{DF} \) or \( G_{TDF} \) [30]:

\[
r(M) = p - l_{G_{TDF}}
\]

where \( l_{G_{TDF}} \) is the number of loops in the \( G_{TDF} \).

The max-rank planning algorithms proposed in Liu et al. [30] guarantee that \( G_{DF} \) and \( G_{TDF} \) are loopless using the minimum number of D-FACTS devices. Thus, they ensure that MTDs constructed under this planning method have the maximum rank of the composite matrix as long as no D-FACTS devices work in idle states. The spanning-tree planning method proposed in Li et al. [28] installs D-FACTS devices on the lines, which form a spanning tree of the system. The rank of the composite matrix in the spanning-tree plan varies case by case. If the selected planning solution happens to keep \( G_{TDF} \) loopless, the maximum rank of the composite matrix is achievable. Otherwise, the rank is determined by \( l_{G_{TDF}} \) according to Equation (1). The arbitrary planning method and full planning method are the two simplest MTD planning methods. The arbitrary planning method [22] randomly selects a subset of lines to install D-FACTS devices. The full planning method is the most expensive method, in which D-FACTS devices are installed on every transmission line. However, the rank of the composite matrix in these planning methods seriously depends on D-FACTS setpoints.

To date, no explicit metric is available in AC-SE to measure the MTD detection effectiveness quantitatively. In addition, it may be difficult to decompose the linearised measurement matrix obtained from the Jacobian matrix in AC-SE to provide analytical outcomes as the MTD analysis in DC-SE does. Because of these challenges, it is customary for a DC model to use an approximation of an AC model. To the best of our knowledge, almost all related D-FACTS device-based MTD works [23, 26, 28, 29] use a DC model to quantify MTD detection effectiveness. Some efforts exist that evaluate the performance of MTD on detecting AC-FDI attacks [30, 34]; however, in those, no explicit metric is used or no theoretical analysis is conducted on MTD detection effectiveness.

3 GRAPH-THEORY-BASED PLANNING IN INCOMPLETE MOVING TARGET DEFENCE

In this section, we study the metrics of MTD detecting effectiveness from the perspective of the MTD planning method. Then, we highlight the drawbacks of max-rank planning and propose a novel graph theory–based planning algorithm.

3.1 Analysis of moving target defence detection effectiveness

We next define protected and unprotected buses in MTDs in the noiseless condition to facilitate the presentation.

**Definition 1** In an MTD, Bus \( i \) is a protected bus if the corresponding column of this bus in \( H_0 \) is linear-independent to \( H \), that is, \( h^i_1 \notin \text{col}(H) \); otherwise, it is an unprotected bus in the MTD, that is, \( h^i_1 \in \text{col}(H) \).
The protected and unprotected buses are defined from the perspective of detection effectiveness. This is superior to the definition in Li et al. [28], in which protected buses are merely associated with D-FACTS devices. The drawback of the definition in Li et al. [28] is that whereas D-FACTS devices are installed on lines connected to a bus, this bus can still be unprotected under certain circumstances. We propose Lemmas 1 and 2 to illustrate the characteristics of protected and unprotected buses in MTDs against single-bus attacks. A single-bus attack is the simplest FDI attack requiring the minimum effort from attackers who manipulate measurements only with respect to one bus. We focus on analysing MTD detection effectiveness against such single-bus attacks. However, these theoretical results can be extended to analyse multiple-bus attacks, because a multiple-bus attack can be treated as multiple single-bus attacks launched at the same time.

**Lemma 1** Any FDI attack on a protected bus is detectable, whereas any FDI attack on an unprotected bus is undetectable by an MTD.

The proof of Lemma 1 is apparent and thus is omitted here. The number of protected buses determines the MTD detecting effectiveness. We further propose Lemma 2 to demonstrate the exact relation between the rank of the composite matrix and the number of protected buses.

**Lemma 2** If the rank of the composite matrix in an MTD is \( r([H_0, H]) \), there are at least \( r([H_0, H]) - (n - 1) \) protected buses.

**Proof** Because both \( H \) and \( H_0 \) are of full column rank, that is, \( r(H) = r(H_0) = n - 1 \), there are at least \( r([H_0, H]) - n + 1 \) columns in \( H_0 \) that are linear-independent to \( H \) in the MTD. Thus, there are at least \( r([H_0, H]) - n + 1 \) protected buses in the MTD with a composite matrix rank \( r([H_0, H]) \).

According to Lemma 2, the rank of the composite matrix merely reflects the minimum number of protected buses in an MTD. Therefore, all existing MTD operation and planning methods in the literature based on the rank maximisation of the composite matrix [26, 29, 30] are equivalent to attaining a maximised lower bound on the number of protected buses, that is, a lower bound on the MTD detection effectiveness. This rank as the only indicator of the MTD detection effectiveness is insufficient to compare the detection effectiveness of different MTDs analytically with the same lower bound. Hence, it is necessary to introduce an upper bound of MTD detection effectiveness. This upper bound can be determined by the number of unprotected buses according to Definition 1. One can maximise this upper bound of MTD detection effectiveness by minimising the number of unprotected buses via MTD planning. We propose the following lemma to show what constitutes an unprotected bus.

**Lemma 3** (1) An end bus, (2) a non-D-FACTS bus, and (3) a bus fully covered by D-FACTS lines, whose reactances are modified using a unity factor are unprotected buses.

**Proof** Because there are three types of unprotected buses, this lemma is proved as follows: (1) End Bus i has only one transmission line, i–j, and its reactances before and after an MTD are \( x_{ij}^0 \) and \( x_{ij} \), respectively. It is evident that \( b_i^0 x_{ij}^0 = b_i x_{ij} \) holds. In this case, for any value of \( x_{ij} \) in different MTDs, \( b_i^0 \) is always linear-dependent to \( H \) owing to \( b_i^0 = (x_{ij}^0/\Delta x_{ij}) \times b_i \in col(H) \). Thus, an end bus is an unprotected bus in any MTDs. (2) If Bus i is a non-D-FACTS bus, \( b_i = b_i^0 \) holds. It is apparent that \( b_i^0 \in col(H) \) holds. Thus, a non-D-FACTS bus is an unprotected bus. (3) Suppose all lines connected to Bus i are D-FACTS lines. An MTD modifies the reactances of these lines with the same factor \( k \), that is, \( x_{ij} = k x_{ij}^0, j \in S_i \), where \( S_i \) is the set of lines connected to Bus i. It is evident that \( b_i^0 = k b_i \) holds. Thus, this bus becomes an unprotected bus under the MTD.

End buses and non-D-FACTS buses can be identified based on the power system topology or MTD plan, whereas a bus fully covered by D-FACTS lines whose reactances are modified using a unity factor involves both MTD planning and MTD operation. In addition, Lemma 3 points out a limitation of the MTD, that a single-bus FDI attack on any end bus is undetectable regardless of the D-FACTS setpoints and planning solutions. Therefore, leaving an end bus as a non-D-FACTS bus can reduce the number of D-FACTS devices without affecting the detection effectiveness. Installing protected sensors to secure measurements related to the end buses can thwart FDI attacks against end buses. However, securing measurement sensors to detect and prevent FDI attacks belongs to another defence algorithm well-studied in the literature [9–13], which is beyond the scope of this work.

The difference between Lemmas 1–3 and Remark 3 in Liu et al. [26] are summarised here. Remark 3 claims for an MTD with \( H \), \( r([H_0, H]) = n - 1 + |S_d| \) holds, where \( S_d \) is a set of columns in \( H_0 \) independent to \( H \) [26]. However, the following important issues are not discussed in Liu et al. [26]. First, Liu et al. [26] only provides a highly abstracted set of states without concrete instances. Here, we instantiate the columns in \( S_d \) as protected buses from the standpoint of power systems. Second, \( r([H_0, H]) \) is the MTD detection metric, but the relation between \( r([H_0, H]) \) and \( r([H_0, H]) \) is not directly presented in Liu et al. [26]. In Lemma 1, we clarify the relation between FDI attacks and unprotected/protected buses. In Lemma 2, we clarify the relation between \( r([H_0, H]) \) and the number of protected buses. Third, Liu et al. [26] do not discuss which buses are included in \( S_d \) in an MTD or under an MTD planning solution. In Lemma 3, we point out three types of unprotected buses.

Here, we use the ADP of an MTD to measure its detection effectiveness against FDI attacks accurately, which is widely used as attack detection evaluation metric in the numerical results in [23–26], rather than in the theoretical analysis.
Definition 2 The ADP of an MTD is defined as the ratio of the number of the FDI attacks detected by this MTD to the total number of FDI attacks.

In a specific MTD, a bus is either a protected bus or an unprotected bus in accordance with Definition 1. Without a loss of generality, we assume that targeted buses in single-bus FDI attacks are uniformly distributed. The reference bus is not considered in calculating the ADP because this bus cannot be a target bus of FDI attacks. Thus, the ADP of an MTD against single-bus FDI attacks is equal to the ratio of the number of protected buses \( n_p \) to the total number of buses excluding the reference bus, that is, \( ADP_{MTD} = \frac{n_p}{n-1} \), according to Lemmas 1 and 2. Because \( n_0 \) in different MTDs varies as their D-FACTS setpoints change, we propose Theorem 1 to demonstrate the ADP range of an MTD. Lemmas 1 and 2 are used to derive the ADP lower bound of an MTD in Theorem 1, and Lemma 3 is used to derive the ADP upper bound.

Theorem 1 For an MTD with \( r([H_0, H]) \), \( n_2 \) non-D-FACTS buses and \( n_{1e} \) end buses belonging to the D-FACTS buses, its ADP against single-bus FDI attacks satisfies:

\[
\frac{r([H_0, H]) - n + 1}{n - 1} \leq ADP_{MTD} \leq 1 - \frac{n_2 + n_{1e}}{n - 1} \tag{2}
\]

Proof In an MTD with \( r([H_0, H]) \), \( n_p \geq r([H_0, H]) - (n - 1) \) holds according to Lemma 2. In addition to \( n_2 + n_{1e} \) unprotected buses identified by Lemma 3, D-FACTS setpoints can convert some protected buses to unprotected buses. Thus, \( n_p \leq (n - 1) - (n_2 + n_{1e}) \) holds. Therefore, the ADP of the MTD satisfies Equation (2).

The ADP of a complete MTD [23, 26, 30] is a particular case of Theorem 1, in which the ADP upper and lower bounds are both equal to 1. For the upper bound, there is neither an end bus nor a non-D-FACTS bus in the complete MTDs, that is, \( n_{1e} = 0 \) and \( n_2 = 0 \), because the D-FACTS lines form a spanning tree [30]. For the lower bound, \( r([H_0, H]) = 2(n - 1) \) in the complete MTD.

In addition, we define a novel metric for measuring the detection effectiveness of an MTD planning solution.

Definition 3 The ADP of an MTD planning solution is defined as the average ADP of MTDs under this planning solution.

The ADP of an MTD planning solution is not a fixed value because the number of protected buses varies depending on the D-FACTS setpoints in each MTD under this planning solution. Instead, we can calculate an ADP range of an MTD planning solution, as shown in the following theorem, to represent its detection effectiveness.

Theorem 2 For an MTD planning solution with a fixed rank of the composite matrix equal to \( r([H_0, H]) \), \( n_2 \) non-D-FACTS buses, and \( n_{1e} \) end buses belonging to the D-FACTS buses, its ADP against single-bus FDI attacks satisfies:

\[
\frac{r([H_0, H]) - n + 1}{n - 1} \leq ADP_{planning} \leq 1 - \frac{n_2 + n_{1e}}{n - 1} \tag{3}
\]

It is trivial to prove Theorem 2 using Theorem 1. This work focuses on MTD planning with a fixed rank of the composite matrix rather than a varying rank relevant to the D-FACTS setpoints. The selection of D-FACTS setpoints falls into the MTD operational issue and thus is out of the scope of this research. MTD planning with a fixed rank of the composite matrix is preferable in the power system operation. This is because such MTD planning can provide the system operator with more freedom to dispatch D-FACTS setpoints to meet system economic and reliability criteria while ensuring MTD detection effectiveness.

To elucidate Theorem 2, we demonstrate the relation between protected and unprotected buses under an MTD planning solution in Figure 1. The rank of the composite matrix solely determines the minimum number of protected buses, that is, the ADP lower bound. The system topology and MTD planning jointly decide the number of unprotected buses, that is, the ADP upper bound. With this MTD planning solution, the boundary between the protected and the unprotected buses (dashed line in Figure 1) moves between the two shadow areas subject to the specific D-FACTS setpoints in an MTD.

One can use Theorem 2 to analyse the MTD detection effectiveness of any MTD planning solutions with a loopless D-FACTS graph because the rank of the composite matrix in this plan is fixed regardless of D-FACTS setpoints [17]. For example, max-rank MTD planning [17] achieves the maximum rank of the composite matrix, that is, \( r([H_0, H]) = p \). This indicates that any MTD under max-rank planning has the maximum ADP lower bound. Besides, \( G_{MTD} \) forms a spanning tree in max-rank planning [30], leading to \( n_{1e} = 0 \). We illustrate the ADP range of incomplete MTDs constructed under max-rank MTD planning in the following corollary.

Corollary 1 The ADP of the max-rank MTD plan [30] against single-bus FDI attacks satisfies:

\[
\text{Protected Buses} \quad \quad \text{Unprotected Buses}
\]

\[
\text{ Determined by } r([H, H]) \quad \quad \text{Boundary} \quad \quad \text{Determined by MTD planning & system topology}
\]

\[
\text{Determined by D-FACTS setpoints}
\]

**Figure 1** Relation of protected and unprotected buses in moving target defence plan.
\[ \frac{p - (n - 1)}{n - 1} \leq ADP_{\text{planning}} \leq 1 - \frac{n_2}{n - 1} \]  

Corollary 1 shows the merits and drawbacks of max-rank MTD planning. Compared with Equation (3), max-rank MTD planning increases both the ADP lower and upper bounds. Nevertheless, the existence of non-D-FACTS buses reduces the ADP upper bound significantly.

We further propose Corollary 2 to identify a special class of MTD planning solutions with a fixed ADP (i.e., the ADP lower bound equates to the upper bound) regardless of the setpoints of D-FACTS devices. Here, we define a reduced D-FACTS graph as a graph composed of D-FACTS lines and D-FACTS buses.

**Corollary 2** If the reduced D-FACTS graph is a loopless and connected graph and \( G_{DF} \) is a spanning tree, the ADP of this MTD planning solution is a fixed value regardless of D-FACTS setpoints, that is, \( ADP_{\text{planning}} = \frac{(p - n + 1)}{(n - 1)} \).

**Proof** According to the theorem of Euler’s formula for a disconnected graph \([35]\), in any planar graph with \( n \) vertices, \( p \) edges, \( f \) faces, and \( t \) components, the following equality holds: \( n + f - p = 1 + t \). Because the number of faces equals the sum of the number of interfaces (loops in the graph) and one external face, i.e., \( f = lp + 1 \), we have \( n - t = p - lp \). Thus, \( n_1 - t_1 = p_1 - lp_1 \) holds in the reduced D-FACTS graph, in which \( t_1 \) and \( lp_1 \) are the number of disconnected components and the number of loops in the reduced D-FACTS graph, respectively. If the reduced D-FACTS graph is connected and loopless, that is, \( t_1 = 1 \) and \( lp_1 = 0 \), \( n_1 - 1 = p_1 \) holds. Because the sum of the number of D-FACTS and non-D-FACTS buses equals the number of buses in the system, that is, \( n_1 + n_2 = n \), we have \( n_1 - 1 = (n - 1) - n_2 \). Therefore, \( p_1 = (n - 1) - n_2 \) holds. Because \( G_{DF} \) is a spanning tree with \((n - 1)\) lines, the number of D-FACTS lines is \( p_1 = p - (n - 1) \). Then, the ADP lower bound in Equation (4) equals the ADP upper bound, that is, \( p - (n - 1) = (n - 1) - n_2 \). Therefore, this class of MTD planning solutions has a fixed ADP, that is, \( ADP = \frac{(p - n + 1)}{(n - 1)} \).

Although the MTDs under the MTD plan solutions identified in Corollary 2 have a fixed ADP, one ought to avoid these MTD planning solutions because they have the lowest ADP among all max-rank planning solutions.

### 3.2 Graph-theory-based planning

We propose a graph theory–based planning method to ensure the ADP lower bound and increase the ADP upper bound simultaneously. The proposed method is composed of Algorithms 1 and 2. In these algorithms, we calculate and assign the power loss to impedance sensitivity (PLIS) to each line as its weight in \( G \), because PLIS is an indicator to determine the most appropriate D-FACTS locations to minimise system losses \([36]\). A line with a larger absolute PLIS value indicates that installing a D-FACTS device on this line can reduce more system losses.

In Algorithm 1, we aim to maximise the rank of the composite matrix by ensuring both \( G_{DF} \) and \( G_{NDF} \) loopless. Algorithm 1 initialises \( G_{NDF} \) as a minimum spanning tree (MST) of \( G \) such that the remaining lines in \( G_{DF} \) have large PLIS values. If \( G_{DF} \) is loopless, Algorithm 1 terminates with the solution obtained. Otherwise, Algorithm 1 iteratively adjusts weights of edges in \( G_{DF} \) until the updated \( G_{DF} \) and \( G_{NDF} \) are both loopless. A loop exists in \( G_{DF} \) because all edges in the loop have relatively large weights. Therefore, we iteratively reduce the weight of edges in the loop in the descending order of their weights. If the loop no longer exists, Algorithm 1 handles the next loop in the same way until the updated \( G_{DF} \) is loopless.

In Algorithm 2, we keep the maximal rank of the composite matrix and use extra D-FACTS lines to cover all unprotected buses, excluding end buses. Algorithm 2 takes the result in Algorithm 1 as its input. In Algorithm 2, four crucial objectives are holistically accounted for: (1) reducing the investment cost of extra D-FACTS devices; (2) retaining the maximum rank of the composite matrix; (3) achieving better operational economics in the system; and (4) elevating the ADP upper bound. We establish three rules, each corresponding to one of the first three objectives.

**Rule 1**: Placing a D-FACTS device only on the line whose two nodes are neither D-FACTS bus nor end bus. Thus, we can use one D-FACTS device to eliminate two non-D-FACTS buses simultaneously to reduce the number of extra D-FACTS devices.

**Rule 2**: Installing an extra D-FACTS device on a line if the updated D-FACTS graph containing this line remains loopless. We design Rule 2 to retain the maximum rank of the composite matrix in MTDs by keeping both \( G_{DF} \) and \( G_{NDF} \) loopless.

**Rule 3**: Sorting non-D-FACTS lines in descending order of their PLIS values and sequentially deciding whether to install a D-FACTS device on the non-D-FACTS lines. We design Rule 3 to select lines with large PLIS values.

Algorithm 2 identifies all end buses, D-FACTS buses and non-D-FACTS lines in the system during the initialisation. In the first part (as shown in Rows 1–14 of Algorithm 2), we sort non-D-FACTS lines in descending order of their weights according to Rule 3 and iteratively check each non-D-FACTS line. We place a D-FACTS device on this line if Rules 1 and 2 can be simultaneously satisfied; otherwise, we skip this line and consider the next one. After the first step, non-D-FACTS buses excluding end buses might still exist, that is, \( n_{2|e} \neq 0 \), if their neighbour buses are either end buses or D-FACTS buses. Then, we identify all of these nodes in set \( V_{NDF} \). In the second part of Algorithm 2 (Rows 16–26), we convert all buses in \( V_{NDF} \) to D-FACTS buses according to Rules 2 and 3.
Algorithm 2 stops after eliminating all non-D-FACTS buses, excluding end buses.

**Algorithm 1 : Maximising the rank of composite matrix**

**Input:** The edge-weighted graph \( G(L, E) \) of a power grid topology.

**Output:** \( \varepsilon_{DF} \): set of D-FACTS lines; \( \varepsilon_{NDF} \): set of non-D-FACTS lines

1: **Initialisation:** \( \varepsilon_{IP} = \emptyset \) // set of edges in a loop.
2: \( \varepsilon_{NDF} = \) find the MST in \( G \) // NDF candidates.
3: \( \varepsilon_{DF} = E - \varepsilon_{NDF} \)
4: Generate a graph \( G_{DF} \) composed of DF lines and alright nodes
5: while \( G_{DF} \) has loops
6: Add alright edges in the first loop to set \( \varepsilon_{IP} \)
7: Arrange edges in \( \varepsilon_{IP} \) in ascending order of their weights
8: for each edge \( \epsilon \) in \( \varepsilon_{IP} \) // start from the lowest-weight edge
9: \( \epsilon \cdot \omega = \epsilon \cdot \omega \times \lambda \) // decrease the positive weight (\( \lambda < 1 \))
10: \( \varepsilon_{NDF} = \) find the MST in weight-updated \( G \)
11: \( \varepsilon_{DF} = E - \varepsilon_{NDF} \)
12: Update \( G_{DF} \) using new DF lines
13: if \( G_{DF} \) has no loops
14: return \( \varepsilon_{DF}, \varepsilon_{NDF} \)
15: else if the same loop \( \varepsilon_{IP} \) still exists in \( G_{DF} \)
16: \( \epsilon \cdot \omega = \epsilon \cdot \omega + \lambda \) // restore \( \epsilon \), try the next edge in loop
17: else
18: break // loop \( \varepsilon_{IP} \) doesn't exist, move to the next loop
19: end if
20: end for
21: end while
22: return \( \varepsilon_{DF}, \varepsilon_{NDF} \)

**Algorithm 2 : Covering all unprotected buses, excluding end buses**

**Input:** The edge-weighted graph \( G(V, E) \) of a power grid topology

\( \varepsilon_{DF} \): set of D-FACTS lines in Algorithm 1.

**Output:** \( \varepsilon_{DF} \): set of D-FACTS lines in proposed MTD planning

1: **Initialisation:** \( \varepsilon_{DF} = \varepsilon_{DF}^{0} \)
2: \( \varepsilon_{Vend} = \) find all end nodes in \( G \)
3: \( \varepsilon_{VDF} = \) find all nodes of edges in \( \varepsilon_{DF} \) // set of D-FACTS buses
4: \( \varepsilon_{NDF} = E - \varepsilon_{DF} \) // set of non-D-FACTS lines
5: Arrange edges in \( \varepsilon_{NDF} \) in descending order of their weights // Rule 3
6: for each edge \( \epsilon \) in \( \varepsilon_{NDF} \) // start from the largest-weight edge
7: if two nodes of \( \epsilon \) are neither in \( V_{end} \) nor in \( \varepsilon_{DF} \) // Rule 1
8: Generate a graph \( G_{1} \) composed of \( \varepsilon_{DF} \) and \( \epsilon \); \( G_{1}(V, \varepsilon_{DF} + \epsilon) \)
9: if \( G_{1} \) has no loops // Rule 2
10: Remove \( \epsilon \) from \( \varepsilon_{NDF} \), and add \( \epsilon \) to \( \varepsilon_{DF} \)
11: Add two nodes of \( \epsilon \) to \( \varepsilon_{DF} \)
12: end if
13: end if
14: end for
15: \( \varepsilon_{NDF} = E - \varepsilon_{DF} \) // non-D-FACTS nodes failed to meet Rules 1 & 2
16: for each node \( v \) in \( \varepsilon_{NDF} \)
17: Generate an empty set \( \varepsilon_{1} \), and add alright edges connected to \( v \) to \( \varepsilon_{1} \)
18: Arrange edges in \( \varepsilon_{1} \) in descending order of their weights // Rule 3
19: for edge \( \epsilon \) in \( \varepsilon_{1} \) // start from the largest-weight edge
20: Generate a graph \( G_{2} \) composed of \( \varepsilon_{DF} \) and \( \epsilon \); \( G_{2}(V, \varepsilon_{DF} + \epsilon) \)
21: if \( G_{2} \) has no loops // Rule 2
22: Remove \( \epsilon \) from \( \varepsilon_{NDF} \), and add \( \epsilon \) to \( \varepsilon_{DF} \)
23: break // deal with the next node in \( \varepsilon_{NDF} \)
24: end if
25: end for
26: end for
27: return \( \varepsilon_{DF} \)

The ADP range of the proposed planning solution is shown in the following corollary.

**Corollary 3** The ADP of the graph theory–based planning method against single-bus FDI attacks satisfies:

\[
\frac{p - (n - 1)}{n - 1} \leq ADP_{Planning} \leq 1 - \frac{n_e}{n - 1}
\]  

(5)

The ADP lower bound of the proposed MTD plan is no less than that in the max-rank plan because it remains the maximum rank of the composite matrix. Because all end buses are non-D-FACTS buses in max-rank planning, \( n_{2} = n_{2e} + n_{e} \) holds. Compared with the ADP upper bound in Equation (4), the proposed plan increases the ADP upper bound by \( \frac{n_{2e}}{(n - 1)} \) but eliminates \( 2e \) non-D-FACTS buses, excluding the end buses in max-rank MTD planning.

Based on Theorem 2, we derive the ADP range of different MTD planning methods in Corollaries 1, 2, and 3. Specifically, we present the ADP range in max-rank planning methods in Corollary 1 and derive the ADP range in the proposed plan in
Corollary 3. In Corollary 2, we identify a class of planning methods that have a fixed ADP.

4 | NUMERICAL RESULTS

4.1 | Test systems

We perform the proposed MTD planning method on the IEEE 14-bus system, IEEE 118-bus system, ACTIVSg 500-bus system, 2746-bus system, and 3012-bus system [37]. The proposed MTD planning method is programmed in the Java programing language. The MTD, FDI attacks, and SE are implemented using MATLAB.

4.2 | Solutions of graph-theory-based planning method

The proposed MTD planning method for the IEEE 14-bus system is shown in Figure 2. The system shows that there are no non-D-FACTS buses except an end bus: Bus 8. The minimum number of non-D-FACTS buses contributes to an improvement in the ADP upper bound. Furthermore, both \( G_{DF} \) and \( G_{MTD} \) are loopless such that any MTDs under this planning solution retain the maximum rank of the composite matrix. Compared with max-rank planning [30], the proposed plan installs only two extra D-FACTS devices on Lines 17 and 18 to transform four non-D-FACTS buses (i.e., Buses 9, 10, 11, and 14) in max-rank planning to D-FACTS buses according to Rule 1. Although Lines 2, 5, and 6 have large PLIS values, placing D-FACTS devices on any of them would form a loop and in turn reduce the rank of the composite matrix. Therefore, no D-FACTS device is installed on these three lines.

For the IEEE 118-bus system, D-FACTS devices in the proposed MTD plan are installed on 97 branches indexed by \( L_{DF} = \{2, 3, 4, 5, 7, 8, 12, 13, 15, 18, 19, 21, 22, 23, 25, 27, 28, 29, 31, 35, 36, 38, 39, 41, 42, 43, 47, 48, 49, 50, 51, 52, 56, 59, 61, 63, 66, 67, 68, 69, 70, 72, 73, 76, 79, 81, 83, 84, 86, 87, 91, 93, 94, 95, 96, 99, 100, 101, 102, 103, 104, 106, 107, 110, 112, 114, 118, 119, 120, 122, 124, 126, 127, 128, 131, 132, 133, 135, 136, 139, 140, 141, 144, 148, 151, 152, 154, 155, 157, 160, 161, 163, 166, 167, 171, 175, 178\}. In max-rank planning, there is a total of 46 non-D-FACTS buses, including seven end buses. In the proposed MTD plan, an additional 35 D-FACTS devices are used to cover these 39 non-D-FACTS buses and all seven end buses are left as non-D-FACTS buses. No loops exist in either \( G_{DF} \) or \( G_{MTD} \), which guarantees the maximum rank of the composite matrix.

We test the computational efficiency of the proposed MTD plan in medium to large-scale power systems. The CPU time of the proposed algorithm in each system is shown in Table 2. The results show the proposed MTD plan is computationally efficient even on large-scale power systems.

4.3 | Comparison of planning methods

We compare the proposed planning method with four other planning methods on a medium-scale system and a large-scale system in Table 3. There are seven end buses and 179 lines in the IEEE 118-bus system, and 550 end buses and 3566 lines in the 3012-bus system. Thus, the maximum rank of the composite matrix in the IEEE 118-bus and 3012-bus systems are 179 and 3566, respectively. Furthermore, the ADP ranges in Table 3 are derived based on Theorem 1 and Corollaries 1–3.

As seen, the proposed planning method has no non-D-FACTS buses, excluding end buses in both systems. Thus, the ADP upper bound of the proposed planning method is much higher than that of max-rank planning. In addition, the proposed plan has the same ADP lower bound as max-rank planning. Compared with arbitrary planning, the proposed plan has a higher ADP range and a larger PLIS sum, resulting in better performance in detecting FDI attacks and minimising system losses. The proposed plan has the same ADP range as that of the full plan and spanning-tree plan. However, the proposed plan uses a much smaller number of D-FACTS devices than full planning and spanning-tree planning, especially in the 3012-bus system. Although the price of a D-FACTS device is lower than that of a conventional FACTS device, the cost of D-FACTS devices is still not negligible. Therefore, the proposed plan can significantly reduce the cost of deploying D-FACTS devices, especially in such a large-scale system with thousands of lines.

**FIGURE 2** Proposed moving target defence planning solution of IEEE 14-bus system

**TABLE 2** CPU time of proposed algorithm on different systems

| Power system | 118-bus system | 500-bus system | 2746-bus system | 3012-bus system |
|--------------|----------------|---------------|----------------|----------------|
| CPU time (ms) | 12             | 69            | 515            | 402            |
4.4 Comparison of attack detection probability in both DC and AC state estimation

In this section, we compare the ADP of four MTD planning methods in both DC- and AC-SE in an IEEE 118-bus system, including proposed planning, arbitrary planning, full planning, and max-rank planning.

To simulate FDI attacks, we randomly generate a voltage angle increment vector \( \Delta \theta \) with a fixed number of attack buses, that is, \( \| \Delta \theta \|_0 = q \), \( q = 1, 2, \ldots \). For each \( q \), we simulate 1000 distinct voltage angle increment vectors. Using these vectors, we construct both a DC-FDI attack pool and an AC-FDI attack pool, each of which has 5000 FDI attacks. For the DC-FDI attacks, we inject \( a = H_0 \Delta \theta \) in the real measurement vectors. For the AC-FDI attacks, we assume that attackers know the actual system states after the MTD through data infiltration and use the original line parameters before the MTD, that is, \( x_0 \), to calculate the manipulated measurements, that is, \( z_2 = \varpi(x, \theta + \Delta \theta, x_0) \). The RMTD operation method, the simplest MTD operation method, is adopted in all four planning methods to determine the setpoints of D-FACTS devices. In RMTD, we set \( \eta = 0.2 \) and \( \tau = 0.05 \), consistent with the settings in Liu et al. [26]. For each planning method, 100 different RMTDs are constructed as a defence pool. We generate 100 different D-FACTS random placement solutions for the arbitrary planning method.

For each planning method, all attacks generated in the attack pool are sequentially launched on each MTD in the corresponding defence pool. Then, the average ADP of each MTD is calculated as an indicator of detection effectiveness of this planning method. In the noisy condition, the measurement noise is assumed to be Gaussian distributed with zero mean and the standard deviation is 3\% of the actual measurement. The SE and BDD are used to detect the FDI attacks, the threshold of which is set to have a 0.5\% false-positive rate.

The ADP of the four planning methods against FDI attacks with \( q \) varying from 1 to four in the DC noisy condition is demonstrated in Figure 3. As seen, the max-rank planning method has the lowest ADP, consistent with the range derived in Table 3. This is because there are 39 non-D-FACTS buses excluding end buses, which seriously reduces the MTD detection effectiveness. In Figure 3, the proposed planning has the best detection effectiveness, because it ensures the maximum rank of the composite matrix and efficiently eliminates all non-D-FACTS buses at the same time. The comparison between max-rank planning and proposed planning highlights the importance of covering buses with D-FACTS devices.

It is interesting to compare the ADPs between the full and proposed planning. Although full planning has no non-D-FACTS buses, its detection performance is not as good as proposed planning. This is because if an RMTD happens to change the reactance of all lines connected to one bus using a unity factor, any single-bus FDI attack on this bus is undetectable, according to Lemma 3. Because D-FACTS devices are placed on all lines connected to each bus in full planning, this special case happens many times in the IEEE 118-bus system under the 100 RMTDs. However, it rarely occurs in the RMTDs under the proposed planning owing to Rule 1, in which there are only 10 buses whose connecting lines are all D-FACTS lines.

With the same number of D-FACTS devices as the proposed planning, the 100 arbitrary planning solutions have 18 non-D-FACTS buses on average, which limits the performance...
of detecting single-bus FDI attacks. Furthermore, there are 21 buses whose connecting lines are all D-FACTS lines on average in the 100 arbitrary planning. The ADP of the arbitrary planning method further decreases when an RMTD happens to modify the reactance of all lines connected to one of these buses using a unity factor. In addition, the ADP range of the four planning methods under the single-bus FDI attacks in Figure 3 is consistent with the analytically derived ADP range in Table 3. The consistency shows the validity of Theorem 2 and Corollaries 1–3.

It is necessary to investigate the MTD detection effectiveness under each MTD planning method against FDI attacks with different magnitudes of injected false data. Here, we introduce voltage angle injection magnitudes (VAIMs) to measure the magnitude of injected false data. For an FDI attack with a given VAIM, injected voltage angle increment $\Delta \theta$ is randomly generated in the range $\Delta \theta \in [0.9, 1.1] \cdot \bar{\theta} \cdot VAIM$, where $\bar{\theta}$ is the average voltage angle. According to the attack vector equation $a = H \cdot \Delta \theta$, the injected false data are proportional to VAIM. We generate FDI attack pools under 13 different VAIMs, ranging from 0.001 to 1.5. For each VAIM, we simulate 1170 single-bus FDI attacks, in which each bus, except the slack bus, in the IEEE 118-bus system is attacked 10 times. We adopt the defence pool of each planning method generated previously. The standard deviation of Gaussian noise is 1% of the actual measurement.

Comparative results are shown in Figure 4. The MTD detection effectiveness increases with an increase in VAIM. MTDs under all planning methods have limited ability to detect FDI attacks with a VAIM less than 0.02. This is because when the VAIM is extremely small, the injected false data in FDI have the same order of magnitude as measurement noises. When the VAIM is less than 0.1, MTDs fail to detect part of these FDI attacks. MTDs increase the estimation residual in these attacks compared with a situation free of attacks, but the increased residual is not large enough to alert the BDD threshold. When the VAIM is more than 0.25, MTDs under each planning method reach their best detection effectiveness. In addition, simulation results demonstrate that the proposed graph theory–based planning method has the best detection performance under each magnitude of injected false data magnitude.

We further investigate MTD detection effectiveness under each MTD planning method under different noise magnitudes. The standard deviation of Gaussian noise increases from 1% to 4% of the actual measurements. Here, we use the attack pool composed of 1170 single-bus FDI attacks with a 0.5 VAIM. The simulation results demonstrate that low measurement noises contribute to improving MTD detection effectiveness. This is because a higher noise level causes the BDD to tolerate more deviations between the measured and estimated power flows. However, this tolerance reduces the defenders’ ability to detect FDI attacks. In Figure 5, although the standard deviation of measurement noise reaches 4%, the ADP of the proposed planning method is still more than 0.80. The proposed graph theory–based planning method has the best detection performance under each level of measurement noise.

We evaluated the detection effectiveness of MTD under the proposed D-FACTS placement under AC-FDI attacks. The average ADP of the four planning methods in the AC noisy condition is illustrated in Figure 6. The ADP is calculated by sequentially launching attacks in the AC-FDI attack pool against AC-SE and BDD, when the system operator uses the same D-FACTS setpoints in the generated defence pool of each plan. For the sensor deployment, we adopt a 2.5 redundant factor (i.e., a ratio of the number of measurements to the number of system states) to guarantee the observability in AC-
Figure 6 shows that the ADP of the max-rank plan and the proposed plan in AC-SE are consistent with those in DC-SE in Figure 3. The ADP of the full plan in AC-SE is higher than that in DC-SE. This is because the end bus belonging to the D-FACTS bus is no longer an unprotected bus in AC-SE owing to the non-linear relation between the system state and measurements in AC-SE.

5 | CONCLUSIONS

We have shown that the rank of the composite matrix merely determines a lower bound on MTD detection effectiveness. It is necessary to introduce its upper bound as an additional metric. We demonstrate that the upper bound of detection effectiveness is determined by the number of unprotected buses identified through MTD planning. In addition, we rigorously derive the ADP range of several MTD planning methods. We propose a graph theory–based planning method that ensures maximal detection effectiveness while considering the economic benefits from D-FACTS devices. The proposed method eliminates non-D-FACTS buses to increase the ADP upper bound and simultaneously retains the maximum rank of the composite matrix to achieve a high ADP lower bound. Numerical results show that the ADP range in the proposed plan is consistent with the range we mathematically derive. The ADP of the proposed plan is better than that of the arbitrary plan, max-rank plan, and full plan in DC-SE. However, it is slightly less than that of the full plan in AC-SE. Furthermore, we investigate the impact of measurement noises and the magnitude of injected false data on MTD detection effectiveness. Simulation results indicate that low measurement noises contribute to improved MTD detection effectiveness, and MTDs can effectively detect FDI attacks with a VAIM more than 0.25.

In future work, it is necessary to address the challenge of no explicit metric in AC-SE that quantifies MTD detection effectiveness and to analyse the detection effectiveness of different MTD operations and planning methods in AC-SE. In addition, we will leverage the high efficiency of the proposed algorithm in real-time FDI attack detection under several other adversary models.

ACKNOWLEDGEMENT

This material is based on 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.

ORCID

Hongyu Wu https://orcid.org/0000-0002-5223-6635

REFERENCES

1. Hadzisamanovic, D: The Process Matters: Cyber Security in Industrial Control Systems. (2014)
2. Dafalla, Y, et al.: Prosumer nanogrids: a cybersecurity assessment. IEEE Access. 8, 131150–131164 (2020)
3. Liang, G, et al.: The 2015 Ukraine blackout: implications for false data injection attacks. IEEE Trans. Power Syst. 32(4), 3317–3318 (2017)
4. Hug, G, Giampapa, J.A.: Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks. IEEE Trans. Smart Grid. 3(3), 1362–1370 (2012)
5. Liu, C, et al.: Dynamic state recovery for cyber-physical systems under switching location attacks. IEEE Trans. Control Netw. Syst. 4(1), 14–22 (2017)
6. Liu, Y, Ning, P, Reiter, M.K.: False data injection attacks against state estimation in electric power grids. ACM Trans. Inf. Syst. Secur. 14(1), 13 (2011)
7. Zhang, H., Liu, B., Wu, H.: Net load redistribution attacks on nodal voltage magnitude estimation in AC distribution networks. In: 2020 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe), pp. 46–50 (2020)
8. Liang, J., Sankar, L., Konst, O.: Vulnerability analysis and consequences of false data injection attack on power system state estimation. IEEE Trans. Power Syst. 31(5), 3864–3872 (2016)
9. Bi, S., Zhang, Y.J.: Graphical methods for defence against false-data injection attacks on power system state estimation. IEEE Trans. Smart Grid. 5(3), 1216–1227 (2014)
10. Bi, S., Zhang, Y.J.: Using covert topological information for defence against malicious attacks on DC state estimation. IEEE J. Select. Areas Commun. 32(7), 1471–1485 (2014)
11. Zhao, J., Mi, L., Wang, M.: A generalized false data injection attacks against power system nonlinear state estimator and Countermeasures. IEEE Trans. Power Syst. 33(5), 4866–4877 (2018)
12. Qi, J., Sun, K., Kang, W.: Optimal PMU placement for power system dynamic state estimation by using empirical observability Gramian. IEEE Trans. Power Syst. 30(4), 2041–2054 (2015)
13. Bobba, R.B., et al.: Detecting false data injection attacks on dc state estimation. In: Preprints of the First Workshop on secure control systems. CPSWEEK (2010)
14. Zhang, H., Liu, B., Wu, H.: Smart grid cyber-physical attack and defence: a review. IEEE Access. 9, 29641–29650 (2021)
15. Tan, R., et al.: Modelling and mitigating impact of false data injection attacks on automatic generation control. IEEE Trans. Infor. Forensic Seucr. 12(7), 1609–1624 (2017)
16. Xie, L., Mo, Y., Sinopoli, B.: Integrity data attacks in power market operations. IEEE Trans. Smart Grid. 2(4), 659–666 (2011)
17. Jia, L., et al.: Impact of data quality on real-time locational marginal price. IEEE Trans. Power Syst. 29(2), 627–636 (2014)
18. Davis, K.R., et al.: Power flow cyber attacks and perturbation-based defence. In: 2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm), pp. 342–347 (2012)
19. Morrow, K.L., et al.: Topology perturbation for detecting malicious data injection. In: 2012 45th Hawaii International Conference on System Sciences, pp. 2104–2113 (2012)
20. Lakshminarayana, S., Belmega, E.V., Poor, H.V.: Moving-target defence for detecting coordinated cyber-physical attacks in power grids. In: 2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), Beijing, pp. 1–7 (2019)
21. Tian, J., et al.: Moving target defence approach to detecting Stuxnet-like attacks. IEEE Trans. Smart Grid. 11(1), 291–300 (2020)
22. Rahman, M.A., Al-Shaer, E., Bobba, R.B.: Moving target defence for hardening the security of the power system state estimation. In: Proceedings of the First ACM Workshop on Moving Target Defence, New York, pp. 59–68 (2014)
23. Tian, J., et al.: Enhanced hidden moving target defence in smart grids. IEEE Trans. Smart Grid. 10(2), 2208–2223 (2019)
24. Liu, B., et al.: Hidden moving target defence against false data injection in distribution network reconfiguration. In: 2018 IEEE Power Energy Society General Meeting (PESGM), pp. 1–5 (2018)
25. Lakshminarayana, S., You, D.K.Y.: Cost-benefit analysis of moving-target defence in power grids. In: 2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), pp. 139–150 (2018)
26. Liu, C., et al.: Reactance perturbation for detecting and identifying FDI attacks in power system state estimation. IEEE J. Select. Top. Signal Process. 12(4), 763–776 (2018)

27. Liu, B., et al.: An interior-point solver for optimal power flow problem considering distributed FACTS devices. In: 2020 IEEE Kansas Power and Energy Conference (KPEC), pp. 1–5 (2020)

28. Li, B., et al.: On Feasibility and limitations of detecting false data injection attacks on power grid state estimation using D-FACTS devices. IEEE Trans. Ind. Infor. 1 (2019)

29. Zhang, Z., et al.: Analysis of moving target defence against false data injection attacks on power grid. IEEE Trans. Inf. Forensics Secur. 1 (2019)

30. Liu, C., Liang, H., Chen, T.: Network parameter coordinated false data injection attacks against power system AC state estimation. IEEE Trans. Smart Grid. 1 (2020)

31. Huang, Y., et al.: Bad data injection in smart grid: attack and defence mechanisms. IEEE Commun. Mag. 51(1), 27–33 (2013)

32. Divan, D., Johal, H.: Distributed FACTS – a new concept for realizing grid power flow control. In: 2005 IEEE 36th Power Electronics Specialists Conference, pp. 8-14 (2005)

33. Johal, H., Divan, D.: Design considerations for series-connected distributed FACTS converters. IEEE Trans. Ind. Appl. 43(6), 1609–1618 (2007)

34. Cui, M., Wang, J.: Deeply hidden moving-target-defence for cybersecure unbalanced distribution systems considering voltage stability. IEEE Trans. Power Syst. 1 (2020)

35. Harary, F.: A Seminar on Graph Theory. Courier Dover Publications (2015)

36. Rogers, K.M., Overbye, T.J.: Some applications of distributed flexible AC transmission system (D-FACTS) devices in power systems. In: 2008 40th North American Power Symposium, pp. 1–8 (2008)

37. Zimmerman, R.D., Murillo-Sanchez, C.E., Thomas, R.J., MATPOWER: steady-state operations, planning, and analysis tools for power systems research and education. IEEE Trans. Power Syst. 26(1), 12–19 (2011)