electronics

Article

Optimal Deployment in Moving Target Defense against Coordinated Cyber–Physical Attacks via Game Theory

Jian Yu * and Qiang Li

School of Automation, Nanjing University of Science & Technology, Nanjing 210094, China
* Correspondence: 22008025@nustti.edu.cn

Abstract: This work proposes a method for the intelligent deployment of distributed flexible AC transmission system (D-FACTS) devices. In recent years, in the field of moving target defense (MTD) strategies to detect coordinated cyber–physical attacks (CCPAs), establishing how to deploy D-FACTS devices has become an important research point. Although some research results have been proposed, the obtained deployment solutions are unintelligent due to not carefully considering smart attackers' behaviors. A method for achieving the intelligent deployment of D-FACTS devices is proposed in this paper. First, the basic concept of corrupting CCPAs is summarized; second, based on considering practical constraints and the basic concept, a protected transmission line set is confirmed; and third, a zero-sum game model is formulated, and a robust Nash equilibrium solution is computed. Due to the game's characteristics, this solution reflects the smart attackers' sense of action. Relying on the solution, those lines that are most likely to be tripped form a new protected transmission line set. Finally, a comprehensive algorithm using a metric proposed in previous studies is proposed for finding an intelligent solution for the deployment of D-FACTS devices. We validated our results through extensive simulations using IEEE 14-bus, 30-bus, and 118-bus power systems provided by MATPOWER and the real-world load profiles from New York State. Our work, in tracking the targets that attackers are most likely to attack, opens up new ideas for the intelligent deployment of D-FACTS devices.

Keywords: moving target defense; coordinated cyber–physical attacks; intelligent deployment; game theory

Citation: Yu, J.; Li, Q. Optimal Deployment in Moving Target Defense against Coordinated Cyber–Physical Attacks via Game Theory. *Electronics* **2023**, *12*, 2484. https://doi.org/10.3390/electronics12112484

Academic Editor: Yannis Papaefstathiou

Received: 3 May 2023
Revised: 25 May 2023
Accepted: 29 May 2023
Published: 31 May 2023

1. Introduction

In recent years, rapid research and development in cyber–physical systems (CPS) have fueled the transformation of physical infrastructures into smarter and more intelligent ones [1]. Due to the enormous and advanced devices used in CPS, the safety of CPS is gradually gaining attention [2]. A smart grid (SG) is a typical CPS. In a modern power system, the deep integration of information and communication transforms a power system into a SG, which facilitates the operation and maintenance of the power system. However, due to the introduction of new computing and communication devices, there are various vulnerabilities in these devices. These vulnerabilities cause SGs to be prone to cyber-attacks.

In the last decade, false data injection attacks [3] (FDIAs) have become a significant form of covert cyber-attack on SGs. To detect FDIAs, various methods have been proposed. Due to the integration and mutual cooperation of highly synthetic cyber–physical attacks (CPAs), the harm caused to the power grid is even greater than that caused by FDIAs alone (e.g., Black Energy [4]). This new type of so-called coordinated CPA denoted as CCPA, is gradually becoming a major focus due to its dangerously covert performance. When a CCPA is launched, a transmission line, generator, or transformer is cut off by the physical attack, and a simultaneous cyber-attack may mask the physical attack by manipulating sensor measurements conveyed to the control center. CCPAs can cause a

dangerous situation in the SG due to undiscovered line/generator outages potentially triggering cascading faults, thus attracting significant concern.

To protect SGs against CCPAs, diverse defense methods have been proposed. To guarantee the validity of sensor measurements from field devices, recent studies [5,6] have presented various strategies. The former was based on securing a set of measurements by encryption, while the latter was based on measurements from known-secure phasor measurement units (PMUs) distributed in the SG. Nevertheless, there is a great deal of devices whose life cycles could last for a very long time in an SG, which makes security upgrades troublesome due to their expensive cost. Moreover, extensive research has indicated that FDIAs can steal measurements from PMUs due to their vulnerabilities [7]. Machine learning (ML)-based approaches have been proposed to detect FDIAs in the literature [8,9]. However, in adversarial scenarios, ML-based algorithms seem vulnerable, which was verified by a recent study, and so can significantly reduce their efficacy [10].

In recent years, many studies related to the moving target defense (MTD) detection of CCPAs have been carried out. Deng et al. [6] first derived the production mechanism of CCPAs and proposed some countermeasures for defending against CCPAs. Lakshminarayana et al. [11] proposed sufficient conditions for destroying the construction of CCPAs and first applied a zero-sum game-theoretic framework to defend against CCPAs in the context of MTD. Zhenyong et al. [12] proposed more comprehensive sufficient conditions for destroying the construction of CCPAs and presented an algorithm for acquiring an optimal distributed flexible AC transmission system (D-FACTS) deployment, which minimized the number of used D-FACTS devices without sacrificing the protection performance of MTD.

In summary, in terms of detecting cyber-attacks via the MTD strategy, there are basically only two research points: one is the detection capability against FDIAs or CCPAs, and the other is how to deploy D-FACTS devices in a way that ensures minimal operational cost and maximum detection effectiveness. Refs. [11,12] performed research on this issue and achieved some meaningful results. However, they acquired their deployment solutions without considering the attackers' point of view and without knowing the targeted lines that are most likely to be attacked by the attackers; therefore, their deployments are unintelligent. Therefore, their suggested deployments could be further optimized.

In our works, based on fully considering the targeted lines that are most likely attacked by the smart attacker, the result of deploying D-FACTS devices is intelligent, which is the most important innovation in this paper, as shown in Figure 1. When analyzing unintelligent deployments of D-FACTS devices, the deployments are essentially based on the knowledge of system topology and mathematical statistics. Despite valuable results being acquired, these results are unintelligent when they do not consider the human factor. When considering the intelligent deployment of D-FACTS devices, subject to practical constraints and real load profiles, there are differences in the flow of power on each line; eventually, the smart attacker will only attack critical lines. Therefore, intelligent deployment can only be achieved by taking into account the aggressive behavior of the smart attacker and confirming the target lines most likely to be attacked.

In addition to the above innovation, there are also two other innovations. Refs. [11,12] both proposed sufficient conditions for disrupting the construction of CCPAs, which did not relate to the essence of the MTD defense against CCPAs. In the paper, the essence is presented, representing the second innovation. In Ref. [11], a novel metric formulated as a derivative of the optimal power flow (OPF) cost to each transmission line's reactance was presented, enduring a weight to each line, such that when the MTD's efficient detection capability against CCPAs was guaranteed, the optimal operational cost was implemented. In addition, taking into account the practical constraints, Zhenyong et al. [12] presented a heuristic algorithm to achieve the deployment of D-FACTS devices; however, the algorithm was not comprehensive and most likely powerless for a large-scale power system. We design a new heuristic algorithm fused with the metric mentioned above, which can acquire more optimal deployment for a large-scale power system.

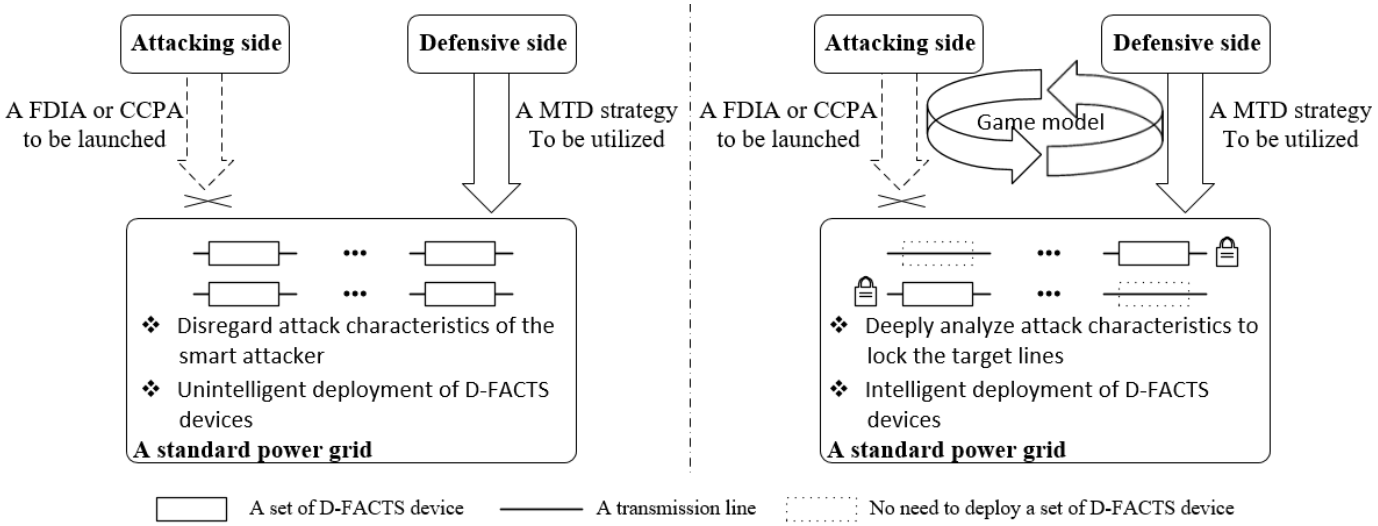

Figure 1. Comparative diagram of unintelligent and intelligent deployments of D-FACTS devices.

In brief, the contributions of our works are three-fold.

1. We summarize the essence of MTD against CCPAs. When abiding by the essence and considering the practical constraints, an initial protected transmission line set is obtained;
2. Based on a game model presented in Ref. [11], we compute a Nash equilibrium (NE) Minimax robust solution. To acquire the true solution, some real load profiles from New York State are used. This is the first time that the NE robust solution has been analyzed from the perspective of the attacker. Relying on the solution, those lines that are most likely to be tripped form a new protected transmission line set. Due to the game's characteristics, the new protected transmission line set reflects the smart attacker's sense of action;
3. On the basis of the new protected transmission lines, we design a more comprehensive algorithm fueled by a metric developed in Ref. [11] for achieving the ultimately intelligent deployment of D-FACTS devices.

The rest of this paper is organized as follows. Section 2 provides the related works. Section 3 reviews the theory analysis. The proposed Methodology is introduced in Section 4. Case studies are implemented in Section 5. The discussion is presented in Section 6. Section 7 provides the conclusions and suggestions for future work.

2. Related Works

When talking about cyber-attacks, there are multiple countermeasures considering FDIAs [13,14]. An FDIA is a significant covert attack on a SG. To detect FDIAs, various methods have been proposed, e.g., game theory [15,16] and ML-based approaches [17]. Since MTD is a dynamic strategy that has the potential to increase the cost and complexity for potential attackers, MTD is a primary method for detecting FDIAs. To enhance state security, deploying D-FACTS devices in power grids was first proposed in Refs. [13,14]. Ref. [18] first proposed an MTD mechanism to secure state estimation (SE) and presented a formal MTD design to ensure its effectiveness in detecting FDIAs. Qingyu et al. [19] investigated data integrity attacks against OPF requiring the least effort from the adversary's perspective and proposed effective defense schemes to combat data integrity attacks. Refs. [20,21] proposed a design criterion in terms of reactance perturbations to detect FDIAs. Effective MTD perturbations actually sacrifice operational costs. Tian Jue et al. [22] proposed a hidden MTD approach to prevent detection from smart attackers. Ref. [23] presented sufficient system topology conditions ensuring MTD's capability for detecting all FDIAs. Ref. [24] designed a D-FACTS device placement algorithm, which guarantees

MTD's detection capability against FDIAs by utilizing the minimum number of D-FACTS devices. Zhenyong et al. [25] first pointed out the relationship between the construction of MTD and the detection of FDIAs and presented a sufficient condition to design a specific MTD to detect FDIAs.

As time goes on, attack forms are also upgraded, gradually moving toward synthesis. In recent years, the attacks on SGs have tended to be CCPAs. Many recent studies have been carried out to obstruct and address the imminent threats caused by CPAs. In Ref. [26], when choking the information flow transmitted from the attacked zone to the control center, a CPA was launched. Deng et al. [6] first proposed a new coordinated CPA, denoted as CCPA, which is a synchronous/concurrent attack. When such a CCPA is launched, the physical attack comprises cutting off a transmission line, generator, or transformer, and the simultaneous cyber-attack can mask the physical attack by falsifying the sensor measurements. Therefore, after a CCPA is launched, cascading failures may be triggered due to undetected line/generator outages. In Ref. [11], a zero-sum game-theoretic framework designed to defend against CCPAs via the MTD method was formulated. In Ref. [12], an algorithm for acquiring optimal D-FACTS devices deployment was presented.

Based on the reviewed studies, the key findings on the subject investigated, the suggested techniques, and the advantages and limitations of each study are presented in Table 1.

Table 1. Summary of related works.

Author	Publication Year	Subject Investigated	Main Contributions	Limitations
Kate L. Morrow et al. [13]	2012	FDIA	A 'probing' approach for detecting FDIAs based on perturbing the power system by changing the impedance on a set of chosen lines was proposed.	How to deploy the D-FACTS was not mentioned.
Katherine R. Davis et al. [14]	2012	FDIA	A proactive defense strategy that was capable of detecting FDIAs was introduced.	There was not enough discussion about the proposed approach's detection capability against FDIAs.
Mohammad Esmalifalak et al. [15]	2013	FDIA	A two-person zero-sum strategic game was formulated to find the Nash equilibrium and maximize the attacker's and defender's profits.	The simulation experiment was only conducted in a PJM-5-BUS test system, which was slightly less convincing.
Anibal Sanjab et al. [16]	2016	FDIA	1. A Stackelberg game was proposed in which the defender acted as a leader that could anticipate the actions of the adversaries. Simultaneously, a distributed learning algorithm was presented for solving the game solution; 2. A hybrid game was considered in which the defender could not anticipate the action of the adversaries. Simultaneously, a search-based algorithm was presented for finding the equilibrium of this hybrid game.	The simulation experiment was only conducted on the IEEE 30-bus test system, which was slightly less convincing.
Mohammad Reza Habibi et al. [17]	2021	FDIA	An effective and proper strategy based on an artificial-neural-network-based reference tracking application was introduced to remove the FDIAs in the DC microgrid.	The training data should be large enough to support the neural network performance. In this paper, the amount of data used for the neural networks was unclear. In addition, the DC microgrids were constructed by parallel DC/DC converters in this paper; other types of microgrids were not considered.

Table 1. *Cont.*

Author	Publication Year	Subject Investigated	Main Contributions	Limitations
Mohammad Ashiqur Rahman et al. [18]	2014	FDIA MTD	An MTD mechanism to secure state estimation was proposed, and a formal MTD design to ensure its effectiveness in detecting FDIAs was presented	How to deploy the D-FACTS was not mentioned.
Qingyu Yang et al. [19]	2017	FDIA	1. The equality constraints and the physical property of the transmission line in the OPF process were investigated to determine the lowest number of target nodes attacked; 2. The problem of finding the critical attack vector to increase the minimum fuel cost as an objective of OPF was formalized; 3. Two types of defense schemes were proposed to defend against the FDIA.	The attacker needed comprehensive information on the power grid, such as the system topology, all nodal load active powers, and power flow limits on each transmission line, when an FDIA was successfully launched.
Chensheng Liu et al. [20]	2018	FDIA MTD	1. The FDIA detection conditions under a noiseless setting that were practical to apply and that relate the probability of FDIA detection to the rank of a composite matrix were derived; 2. A secure reactance perturbation optimization problem was formulated, and an associated algorithm for solving the perturbation settings was proposed.	The scientific research achievements were limited to the premise of the system full column rank. If the system was a non-full column rank, the relevant issues were not addressed.
Subhash Lakshminarayana et al. [21]	2021	FDIA MTD	1. Formal design criteria to select MTD reactance perturbations that were truly effective were presented; 2. The important trade-offs between the MTD's detection capability and its associated required cost were characterized.	A metric, denoted as the smallest principal angle (SPA), was proposed for characterizing MTD effectiveness against FDIAs. However, there was not enough discussion about the SPA. In particular, the SPA's calculation was fuzzy.
Jue Tian et al. [22]	2019	FDIA MTD	A hidden MTD approach that could not be detected by the attackers was proposed.	No limitations were found.
Zhenyong Zhang et al. [23]	2020	FDIA MTD	The conditions for thwarting all FDIAs via an MTD strategy were proposed.	No limitations were found.
Bo Liu et al. [24]	2020	FDIA MTD	1. The D-FACTS placement algorithms by using the minimum number of D-FACTS devices to achieve the maximum MTD effectiveness were designed; 2. A novel MTD-based ACOPF model was proposed to find a trade-off between the system loss and the MTD effectiveness.	The presented algorithm to acquire the D-FACTS placement for the incomplete MTD seems too complicated. When applied in practice, it can be simplified.
Zhenyong Zhang et al. [26]	2022	FDIA MTD	The correlation between MTD design and FDI detection was revealed, and the MTD's performance was optimized in terms of detecting FDIAs.	No limitations were found.
Ruilong Deng et al. [6]	2017	CCPA	Two potential CCPAs, namely replay and optimized CCPAs, were presented, and countermeasures were proposed to detect them based on the analytical results.	The method of detecting optimized CCPAs was slightly complicated and confusing.
Subhash Lakshminarayana et al. [11]	2021	CCPA MTD	1. Sufficient conditions for disrupting the construction of CCPAs were presented; 2. A novel metric was developed, which was devoted to finding the optimal deployment of D-FACTS devices; 3. To minimize the defense cost, a zero-sum game was formulated to identify the best subset of links to perturb against a strategic attacker.	The presented sufficient conditions were not comprehensive. When formulating the game model, the practical constraints were not considered, which affected the game solution's efficiency.
Zhenyong Zhang et al. [12]	2022	CCPA MTD	1. More comprehensive sufficient conditions for disrupting the construction of CCPAs were presented; 2. On the basis of considering the practical constraints, an algorithm for minimizing the number of used D-FACTS devices was designed.	The presented conditions could also be further summarized. The proposed algorithm was not comprehensive.

To date, in the field of MTD defense against malicious attacks, the deployment of D-FACTS devices has been a crucial area of research. Many previous research results have been obtained, and various methods have been proposed, as shown in Table 2.

Table 2. Summary of related works associated with deployment methods of D-FACTS devices.

Indexes of the Literature	The Type of Attack	Specific Deployment Method of D-FACTS Devices	MTD Categories
Ref. [27]	-	The devices can be incrementally deployed as needed, providing a precedented level of scalability [27].	Economy-oriented scheme
Ref. [28]	-	The best k lines were chosen corresponding to the k sensitivities in power loss to impedance (PLI), which are the furthest from zero [28].	Economy-oriented scheme
Ref. [29]	-	Relying with line impedance sensitivities, the result of placing D-FACTS devices for line flow control was achieved.	Economy-oriented scheme
Ref. [13]	FDIAs	The placement was primarily based on sensitivity analysis [13].	Economy-oriented scheme
Ref. [18]	FDIAs	Originally, in an arbitrary set of D-FACTS deployed lines, L was selected. Then, based on the judgment results of whether L can satisfy the system security and MTD criteria, L was finally confirmed.	Economy-oriented scheme
Ref. [20]	FDIAs	Due to the MTD detection efficiency against FDIAs being closely correlated with the composite matrix rank, following this principle, the deployment was properly implemented.	Security-oriented scheme
Ref. [22]	FDIAs	To defend against a class of highly structured FDIAs, all critical sets were covered by MTD, which means enhanced MTD was accomplished.	Security-oriented scheme
Ref. [23]	FDIAs	With the aim of minimizing the dimension of the stealthy attack space and maximizing the number of covered buses, two algorithms were adopted. Based on the obtained results, eventually, deployment was acquired.	Security-oriented scheme
Ref. [24]	FDIAs	D-FACTS placement algorithms for both complete and incomplete MTDs were designed, which achieved the maximum rank of the composite matrix with the minimum number of D-FACTS devices; Additionally, the concept of power loss sensitivity was leveraged into the proposed algorithms to account for the economic benefits.	Combination of economy-oriented scheme and security-oriented scheme
Ref. [30]	FDIAs	D-FACTS devices deployed on a branch were able to detect the existence of effective FDIAs targeted on either end bus(es) (with degrees both larger than 1) of this branch if and only if the injected phase angle difference between the two end buses is larger than a tolerance threshold [30].	Combination of economy-oriented scheme and security-oriented scheme
Ref. [21]	FDIAs	In the paper, the trade-off between the MTD's detection capability and its cost was mainly concerned. But no specific deployment method was depicted.	Combination of economy-oriented scheme and security-oriented scheme
Ref. [31]	FDIAs	A depth-first-search-based D-FACTS placement algorithm was proposed to guarantee the hiddenness of MTD while maximizing the rank of its composite matrix [31].	Security-oriented scheme
Ref. [32]	FDIAs	Initially, the power loss to impedance sensitivity (PLIS) to each line as its weight was calculated and assigned. After two algorithms were simulated, the deployment solution was obtained.	Combination of economy-oriented scheme and security-oriented scheme
Ref. [33]	FDIAs	To balance the trade-off between effectiveness and hiddenness, the design of explicit residual-based MTD was accomplished. Howeverno specific deployment approach was proviede.	Combination of economy-oriented scheme and security-oriented scheme
Ref. [26]	FDIAs	A heuristic algorithm to compute a near-optimal solution for the deployment of D-FACTS devices was developed.	Security-oriented scheme

Table 2. *Cont.*

Indexes of the Literature	The Type of Attack	Specific Deployment Method of D-FACTS Devices	MTD Categories
Ref. [34]	FDIAs	In an MTD perturbation cycle, during the initial time, a security-oriented MTD scheme was implemented, and an economy-oriented MTD scheme was followed at the reset of time, so a multi-stage MTD was conducted.	Combination of economy-oriented scheme and security-oriented scheme
Ref. [35]	FDIAs	A new D-FACTS devices placement algorithm, which could reach all necessary buses with the smallest number of D-FACTS devices, was proposed.	Security-oriented scheme
Ref. [36]	FDIAs	An efficient algorithm to minimize the number of required D-FACTS devices for protecting a specific set of buses was proposed.	Combination of economy-oriented scheme and security-oriented scheme
Ref. [11]	CCPAs	A sufficient condition for destroying the construction of undetectable was presented. Based on the condition, a random assignment of D-FACTS devices was given. When adjusting the load profiles in the power grid and applying a zero-sum game model, a specific deployment of D-FACTS devices was acquired through computing the NE robust solution of the game.	Combination of economy-oriented scheme and security-oriented scheme
Ref. [12]	CCPAs	Due to the practical constraints, the protected transmission lines were specific, and the number of deployed D-FACTS devices was limited. In this context, an algorithm seeking optimal deployment was proposed.	Combination of economy-oriented scheme and security-oriented scheme

Limitations of Existing Works

According to the summary provided in Table 2, the evolution of deployment methods of D-FACTS devices can be further summarized, as shown in Figure 2.

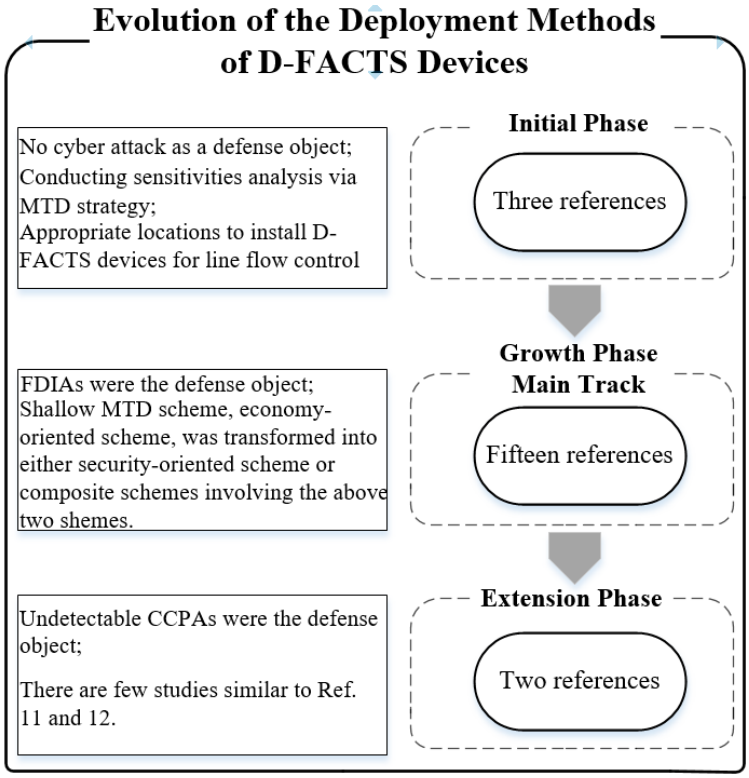

Figure 2. The evolution of the deployment methods of D-FACTS devices. In initial phase, three references refer to Refs. [27–29]. In growth phase (Main Track), fifteen references refer to Refs. [13,18,20–24,26,30–36]. In extension phase, two references refer to Refs. [11,12].

As the above analysis shows, there are many literatures that focus on the deployment of D-FACTS devices, and these have provided several valuable results. In the field of detecting FDIAs, the economy-oriented MTD scheme is gradually being transformed into either a security-oriented scheme or a composite scheme. The MTD approach is also used for defending against undetectable CCPAs. However, despite the existence of the above two MTD schemes, two schemes completely depend on the knowledge of power system topology, mathematical statistics, and simulation technology without considering the human factor. The deployment solutions of D-FACTS devices are not intelligent without considering the initiative of the smart attacker. So-called "optimal deployment" is superficial, meaning that these deployment solutions should be further modified.

Main Innovations in our Work:

(1) Intelligent deployment of D-FACTS devices

Through formulating a zero-sum game model and computing a robust NE solution, the set of transmission lines that are most likely to be attacked by the smart attacker is locked. The lines that are less likely to be attacked can be completely ignored. Eventually, acquired deployment becomes intelligent. The least effort can successfully defend against undetectable CCPAs.

(2) More comprehensive algorithm

After discovering the set of lines that are most likely to be attacked, based on the sufficient condition associated with destroying the construction of undetectable CCPAs and applying a new metric, a more comprehensive algorithm for seeking the intelligent deployment of D-FACTS devices is proposed in the paper. The larger the size of the power system is, the smarter the deployment solution is. In addition, the new metric, which is the OPF cost to the impedance (OCI) sensitivity factor, is used in the algorithm, which makes intelligent deployment more economically effective.

(3) Efficient localization of CCPAs

After undetected CCPAs, the location of tripping lines is the most cutting-edge research point. So far, only one study in the literature [37] has examined this issue. In Ref. [37], a convolution neural network (CNN) was applied to localize the line outage position from the compromised measurements. The results of this paper are very beneficial to localize the line outage position. Although CNN can be used as a classifier for localizing tripped lines, the hardware and software requirements are very high. For example, although the 14-bus power system is relatively small, there are 20 transmission lines in it. Suppose no more than two lines were simultaneously cut off. There are a total of 210 combinations, meaning that the output layer in a CNN requires 210 neurons. The training and testing of this network are very hardware-demanding and take a lot of time. If the system is larger, locking the faulty lines will be even more difficult. The research results of this paper will be very beneficial to localize the tripped lines. Considering only the lines that are most likely to attack for the smart attacker, this must significantly reduce the number of fault combinations and the number of neurons in the output layer of a CNN, which makes it possible to solve via a CNN.

3. Theory Analysis

3.1. State Estimation and Bad Data Detection

In general, a power grid can be characterized by a graph $\mathcal{G} = (\mathcal{N}, \mathcal{L})$, where $\mathcal{N} = \{1, \ldots, n\}$ is a set of buses, $\mathcal{L} = \{1, \ldots, l\}$ represents the set of transmission lines. The total number of transmission lines is L. A bus is used as the slack bus. For one line $k = \{i, j\}$, let b_{ij} be its susceptance. Under the DC power flow model, the power flowing on line k is denoted as

$$F_{ij} = -b_{ij}(\theta_i - \theta_j) \tag{1}$$

where θ_i and θ_j are the voltage phase angles at bus i and j, respectively. Sensor measurements are denoted as

$$\boldsymbol{z} = \boldsymbol{H\theta} + \boldsymbol{e} \tag{2}$$

where $\boldsymbol{z} \in \mathbb{R}^M$, $\boldsymbol{H} \in \mathbb{R}^{M\times n-1}$, and $\boldsymbol{\theta} \in \mathbb{R}^{n-1}$ represent the sensor measurements, the measurement matrix, and the vector of voltage phase angles, respectively. $\boldsymbol{e}$ represents the independent measurement noises that are usually assumed to be sampled from a Gaussian distribution [i.e., $e_i \sim \mathcal{N}\left(0, \sigma_i^2\right)$]. Assume that the system is a full measurement system. According to the composition rule of the measurement matrix elements in the DC power flow model, the k^{th} row of $\boldsymbol{H}$ i

$$\boldsymbol{H}_k = \begin{cases} [0 \ldots 0 {-} b_{ij}\ 0 \ldots 0\ b_{ij}\ 0 \ldots 0], & i \neq i\prime,\ j \neq i\prime \\ [0 \ldots 0 \quad 0 \quad 0 \ldots 0 \quad b_{ij}\ 0 \ldots 0], & i{=}i\prime,\ \ j \neq i\prime \end{cases} \tag{3}$$

where i' is the reference bus and b_{ij} is the susceptance of the transmission line $k = \{i, j\}$. Based on the weighted least squares (WLS) technique, the estimate of a system's state is denoted as

$$\hat{\boldsymbol{\theta}} = \left(\boldsymbol{H}^T \boldsymbol{W} \boldsymbol{H}\right)^{-1} \boldsymbol{H}^T \boldsymbol{W} \boldsymbol{z} \tag{4}$$

where $\boldsymbol{W}$ is a diagonal matrix whose elements are reciprocals of the variances of measurement errors. r, usually represents the measurement residual, is formulated as

$$r = \boldsymbol{z} - \boldsymbol{H}\hat{\boldsymbol{\theta}} \tag{5}$$

In bad data detection (BDD), the 2-norm of the measurement residual is compared with a predetermined threshold τ. If $\|r\|_2 > \tau$, a bad data alarm is triggered.

3.2. Coordinated Cyber–Physical Attacks

3.2.1. Undetectable FDIAs

After the attack vector $\mathbf{a} \in \mathbb{R}^M$ is injected into the sensor measurements, the corrosive sensor measurement is expressed as

$$\boldsymbol{z}^{\mathrm{a}} = \boldsymbol{z} + \mathbf{a} \tag{6}$$

If $\mathbf{a}$ is randomly set, $\boldsymbol{z}^{\mathrm{a}}$ seldom passes the BDD. However, if the attack vector is expressed as

$$\mathbf{a} = \boldsymbol{H}\boldsymbol{c} \tag{7}$$

where $\mathbf{c} \in \mathbb{R}^{n-1}$, $\boldsymbol{z}^{\mathrm{a}}$ can bypass the BDD [3]. Such a situation is called an undetectable FDIA.

3.2.2. CCPA

A CPA is a symbiotic attack. In a CPA, the physical attack and the cyber-attack are launched simultaneously. The physical attack disconnects a subset of the transmission lines. The system topology and power flow may be changed. Similar to an undetectable FDIA, the destruction of the power grid caused by a physical attack cannot pass the BDD if the cyber-attack is randomly set. However, if the cyber-attack is carefully designed, the negative effect of the physical attack on the measurement residual can be perfectly eliminated, which can bypass the BDD. In the end, the undesirable destruction in the power grid can be perfectly masked [6]. Therefore, this CPA is undetectable and termed as a CCPA.

The system parameters, denoted by the subscript "p", are different from the original state. After a physical attack is launched, the sensor measurements are expressed as $\boldsymbol{z}_p = \boldsymbol{z} + \mathbf{a}_p$, where $\mathbf{a}_p$ is a physical attack vector given by

$$\mathbf{a}_p = \boldsymbol{H}\Delta\boldsymbol{\theta} + \Delta\boldsymbol{H}\boldsymbol{\theta}_p \tag{8}$$

where $\Delta\boldsymbol{H}$ is the difference in the measurement matrix between post-attack and pre-attack, given by

$$\Delta\boldsymbol{H} = \boldsymbol{H}_p - \boldsymbol{H} \tag{9}$$

and $\Delta\boldsymbol{\theta}$ is the difference in the nodal voltage state variable between post-attack and pre-attack, denoted by

$$\Delta\boldsymbol{\theta} = \boldsymbol{\theta}_p - \boldsymbol{\theta} \tag{10}$$

For constructing a CCPA [6], the impact of the $\mathbf{a}_p$ on the measurement residual must be erased, which must be realized by a well-designed FDIA denoted as

$$\mathbf{a} = -\Delta\boldsymbol{H}\boldsymbol{\theta}_p \tag{11}$$

3.2.3. Knowledge Required to Launch a CCPA

Assume that a single branch $l = \{i, j\}$ is disconnected due to a physical attack. Relying on the composition mechanism of the elements in the measurement difference matrix $\Delta\boldsymbol{H}$ **[6]**, the tripped branch reactance x_l only needs to be known for constructing $\Delta\boldsymbol{H}$. Moreover, due to Equation (11), the knowledge required to launch a CCPA includes the branch reactance x_l and the difference in phase angles of buses i and j, i.e., $\theta_{i,p} - \theta_{j,p}$. In Ref. [11], the equation of the difference phase angles between buses i and j is given as:

$$\theta_{i,p} - \theta_{j,p} = -\sum_{m \in p_l^k} x_{lm} F_{lm,p} \tag{12}$$

When $\boldsymbol{z}_p$ is added with Equation (11), eventually, the sensor measurement may evolve as follows.

$$\boldsymbol{z}_{CPA} = \boldsymbol{z}_P - \Delta\boldsymbol{H}\boldsymbol{\theta}_p = \boldsymbol{H}_p\boldsymbol{\theta}_p - \Delta\boldsymbol{H}\boldsymbol{\theta}_p + \boldsymbol{e} = (\boldsymbol{H} + \Delta\boldsymbol{H})\boldsymbol{\theta}_p - \Delta\boldsymbol{H}\boldsymbol{\theta}_p + \boldsymbol{e} = \boldsymbol{H}\boldsymbol{\theta}_p + \boldsymbol{e} \tag{13}$$

At this point, the measurement residual is denoted by

$$||\boldsymbol{r}_{CPA}|| = ||\boldsymbol{z}_{CPA} - \hat{\boldsymbol{z}}_{CPA}|| = ||\boldsymbol{r}|| \tag{14}$$

So, the measurement residual must bypass the BDD.

3.3. Preliminary Moving Target Defense and Accurate Limitation of the Protected Lines

3.3.1. Preliminary of MTD

In Ref. [3], the D-FACTS devices were first introduced. These devices can change the transmission lines' impedances, protect the branch power flows from overflow, and eliminate transmission bottlenecks. They are light and small and can easily be hung on power lines. Moreover, they do not affect the communication of the power grid. At present, the research on their performance and application in different power systems has become a research hotspot.

The method of detecting FDIAs via MTD technology has been a major research point in the last decade years. This method was first named MTD by Rahman et al. [18], and the uncertainty caused by MTD distorts the information obtained by potential attackers, which leads to a less successful attack on the targeted power system.

The essence of the MTD is to invalidate the knowledge obtained by the potential attackers, which involves the network topology and system parameters, by actively perturbing the reactances of the transmission lines on which D-FACTS devices are deployed. Consequently, the attackers cannot acquire accurate knowledge again during an MTD's activity cycle.

Recently, Lakshminarayana et al. [11] were the first researchers to propose using the MTD approach to defend against CCPAs. Following this, Zhenyong et al. [12] further studied this research point.

3.3.2. Practical Constraints

Any research should be limited by practical constraints. Not all transmission lines in power grids can be tripped by attackers. For example, a cut line [38] will not be cut off by a strategic and smart attacker since the power flow's fluctuations will be easily

discovered by the system operator due to system connectivity disruption. As a result, different transmission lines have different probabilities of being cut off by smart attackers. Naturally, the lines most likely to be tripped lines must be considered most. In addition, the number of D-FACTS devices is limited to reduce operational costs. Above all, evaluated according to the practical constraints, the set of protected transmission lines, denoted as L_p, is specific.

3.3.3. Protected Transmission Lines' Accurate Reconstruction via Game Theory [39]

Assume that the whole system works at an optimal level pre-MTD activation, making generation costs cost-effective. However, due to MTD's activation, the workstation of the power grid experiences a deviation from the initial optimally operating station, and then an increasing operational cost is incurred. Additionally, to destroy the construction of CCPAs, the deployment of D-FACTS devices is critical to the operational cost, in addition to the efficiency of MTD against CCPAs. A different attack target can affect the deployment of D-FACTS devices, and different deployments of D-FACTS devices can also change the operational cost. So, the interconnection between the attacker and the defender is worthy of being studied. The interconnection between both sides may be formulated as a game model, as presented in Ref. [11]. Once several of the most likely attack targets are probed, the deployment of D-FACTS devices will obtain an optimal scheme, which leads to a positive effect on the operational cost in addition to the effectiveness of MTD against CCPAs.

Zero-Sum Game Formulation [40]

A two-player zero-sum game is described in the above interconnection and defined as a triplet $\Gamma \triangleq (\{A, D\}, \{S_A, S_D\}, \{u_A, u_D\})$ where the elements are: (i) the set of players {A,D}; (ii) S_A and S_D represent the set of actions used by the attacker and the defender, respectively; and (iii) the payoffs of two players $u_k : S_A \times S_D \rightarrow \mathbb{R}$ for $k \in \{A, D\}$, where $u_k(S_A, S_D)$ is the benefit acquired by player k when the action profile that has been played is $s = (s_A, s_D)$. In a zero-sum game, the attacker's payoff is opposite to that of the defender.

$S_A = \{a_0, a_1, \ldots a_{N_A-1}\}$ is depicted as the attacker's action set and N_A is the cardinality of the set S_A. $S_D = \{d_0, d_1, \ldots d_{N_D-1}\}$ is depicted as the defender's action set and N_D is the cardinality of the set S_D. Every action used by the attacker represents the subset of lines tripped physically, and the number of tripped lines is no more than two due to the power flow fluctuations being easily discovered with a larger number of tripped lines. If the action a_0 is taken, this means that no line is tripped. Each action applied by the defender indicates which lines are to be mounted with D-FACTS devices. Each line is only installed with one D-FACTS device. If the action d_0 is taken, this means that no line has its reactance perturbed.

$C_{OPF}(a_m, d_n)$ denotes the OPF cost when a_m and d_n are used by the attacker and defender, respectively. The OPF cost problem is formulated as Equation (4), which was provided in Ref. [11]. Note that 4 is the sequence number provided in Ref. [11]. Meanwhile, the payoff computation is completely depicted as Algorithm 3 that was also provided in Ref. [11].

According to the above, the attacker's payoff is computed by

$$u_D(S_A, S_D) = \begin{cases} C_{OPF}(a_0,d_0) - C_{OPF}(a_0,S_D), \ if \ \mathfrak{T}_S=1 \\ C_{OPF}(a_0,d_0) - C_{OPF}(S_A,S_D), \ if \ \mathfrak{T}_S=0 \end{cases} \quad (15)$$

The indicator variable, $\mathfrak{T}_S$, denotes the success ($\mathfrak{T}_S = 1$) or failure ($\mathfrak{T}_S = 0$) of a defense. To maximize their own interests, both players select the appropriate action. Obviously, their objectives are conflicting. The specific implications of Equation (15) may be inferred from the literature [11].

NE Solution and Machine Learning to Solve the Game

The reason for using the NE is shown in Ref. [11]. In our works, the selected machine learning (ML) approach is the exponential weights for exploration and exploitation (EXP3)

algorithm. An algorithm (4), together with Equations (6)–(8), is used in this paper. Note that 4, 6, 7, and 8 are sequence numbers provided by [11].

First, based on the practical constraints, the set of protected lines is specific and denoted as L_p. Then, from the attacker's point of view, the robust NE solution is analyzed. It is expected that L_p can be ultimately reconstructed by selecting the maximal actions of the attacker.

4. Proposed Methodology

4.1. MTD against CCPAs

As described in the literature [11,12], the concept of using MTD against CCPAs is to wreck the construction of CCPAs. That is, if Equations (12) and (14) are disrupted in the attack-preparation stage, there are no CCPAs. To achieve this objective, both [11,12] give concretely sufficient conditions which are equivalent to each other. Note that we make use of a graph to depict a power grid. In nature, the essence of the sufficient conditions for using MTD against CCPAs is as follows:

Proposition 1. *In any simple graph, there is no loop whose information is transparent for attackers via the MTD strategy, thus enabling no CCPAs, regardless of the tripped transmission lines.*

Proof of Proposition 1 . First, the information in the proposition includes the specific topology and parameters of one loop. The specific topology and parameters indicate the connection sequences and all reactances of the transmission lines which form the loop. Second, in any simple graph, assume that there exists a transmission line $T_k = \{i, j\}$ in a loop. When other loops are excluded, obviously, there are only two paths from bus i to j in the loop. No matter which line is attacked, if the information of any path among the above two paths is not transparent for attackers via the MTD strategy, Equation (12) is corrupted. If this is true for any other loop, for the whole graph, Equation (12) is still corrupted, and thus there are no CCPAs. □

4.2. Deployment of D-FACTS Devices

Considering the practical constraints, Zhenyong et al. [12] provided an algorithm (called the old algorithm in the rest of this paper) for obtaining the optimal deployment of D-FACTS devices. Although this algorithm provides an optimal deployment of D-FACTS devices which implements a trade-off between the defending performance and the invested infrastructure cost, there are two deficiencies. One is primary. In line 6 of the old algorithm, a concept of the so-called "border bus" is presented, but there likely are several cases where the number of "border buses" is no less than two. In these cases, it is not clear to which node "the border bus" refers, so the next step of the algorithm is indistinct; the other is less important.

If the metric provided in Ref. [11] is integrated, the above question can easily be solved. So we present a more comprehensive algorithm (Algorithm 1), as follows for seeking the optimal deployment of D-FACTS devices.

Algorithm 1: Minimizing the number of used D-FACTS devices

Input: Power grid graph $\boldsymbol{\mathcal{G}} = (\boldsymbol{\mathcal{N}}, \mathcal{L})$, $\boldsymbol{L_p}$

Output: $\widetilde{\mathcal{L}}^o$

Set the weight of link $l \in \mathcal{L}$ as dC_{OPF}/dx_l;

Based on the specific set L_p, through injecting the real-world load profiles from New York State, compute the robust NE solution;

From the attacker's angle, implement to reconstruct the set L_p through selecting several maximal actions used by the attacker;

Based on the new set L_p, construct the subgraph $\mathcal{G}_P$ according to $\mathcal{N}_P$ and $\mathcal{G}$;

Use the breath-first search (BFS) to find the connected subgraph $\mathcal{G}_P^1, \mathcal{G}_P^2, \ldots, \mathcal{G}_P^t$ of $\mathcal{G}_P$, and find the spanning tree $\mathcal{T}_i$, the remaining transmission lines $\mathcal{R}_i$, the cut lines $\mathcal{C}_i$, and the protected transmission lines $\mathcal{L}_P^i$, for each subgraph $\mathcal{G}_P^i$;

for each $\mathcal{G}_P^i$ **do**

    Compute $\widetilde{\mathcal{L}}_i^* = \min(\mathcal{T}_i \backslash \mathrm{C}_i, \mathcal{R}_i)$;

    Find the set $\widetilde{\mathcal{L}}_i'$ of outside transmission lines incident to $\mathcal{G}_P^i$ and the set C_i' of cut lines in $\widetilde{\mathcal{L}}_i'$; Sum up the number of the border buses of $\mathcal{G}_P^i$ which has the greatest number of transmission lines incident to the outside buses;

    if the number of border buses is equal to one

        the set of transmission lines that connect the outside buses to the border bus are denoted as $\widetilde{\mathcal{L}}_i''$;

    else

        for each of the border buses **do**

            Sum up the weight of every transmission line which connects the outside buses to a border bus;

        end for

        Select the appropriate border bus corresponding to the least sum of weights, and the set of transmission lines that connect the border bus to the outside buses are denoted as $\widetilde{\mathcal{L}}_i''$;

    end if

    Compute $\widetilde{\mathcal{L}}_i^* = \left(\widetilde{\mathcal{L}}_i^* \cup \widetilde{\mathcal{L}}_i'\right) \backslash \left(C_i' \cup \widetilde{\mathcal{L}}_i''\right)$;

    if the two cardinalities of $\widetilde{\mathcal{L}}_i^*$ and $\mathcal{L}_P^i$ are different

        Calculate the minimum set $\widetilde{\mathcal{L}}_i^o = \min\left(\widetilde{\mathcal{L}}_i^*, \mathcal{L}_P^i\right)$;

    else

        Select a set with the bigger sum of weights between $\widetilde{\mathcal{L}}_i^*$ and $\mathcal{L}_P^i$ and the selected set is $\widetilde{\mathcal{L}}_i^o$;

    end if

end for

Compute $\widetilde{\mathcal{L}}_i^o = \widetilde{\mathcal{L}}_1^o \cup \widetilde{\mathcal{L}}_2^o \cup \cdots \cup \widetilde{\mathcal{L}}_t^o$;

The Algorithm 1 can be fundamentally divided into two steps. The first step is the reconstruction of the protected, denoted as the set L_p. Note that the lines in the L_p are the most likely to be attacked by smart attackers. Due to the real-world load profiles injected, from the perspective of sophisticated and smart attackers, the lines to be tripped are only selected from the L_p. The second step is the process of finding the optimal solution for the deployment of D-FACTS devices. The main implication of the more comprehensive Algorithm 1 may be understood by combining the correlative context of [12]. In addition, the flow chart of the Algorithm 1 is shown in Figure 3.

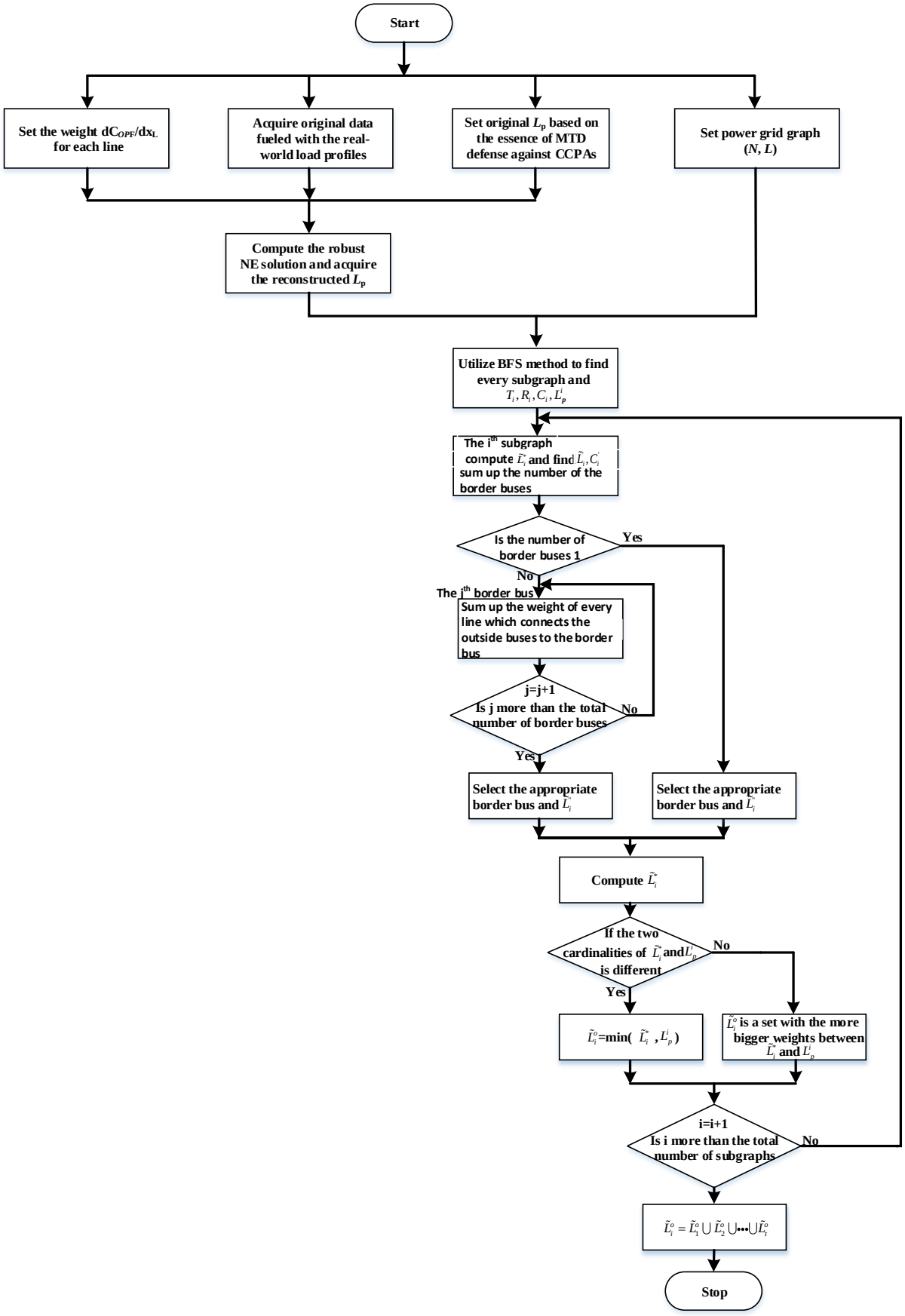

Figure 3. The flow chart of the comprehensive Algorithm 1 for the deployment of D-FACTS devices.

5. Simulation

Below, our simulation results performed with the MATPOWER toolbox are presented to show the effectiveness and comprehensiveness of the proposed reconstruction method and algorithm. To be more convincing, we performed extensive simulations for IEEE 14-, 30-, and 118-bus power systems. In the simulations, the real-world load profiles from New York State on 7 June 2020 [41] were added to the IEEE 14-bus, IEEE 30-bus, and IEEE 118-bus power systems, respectively.

5.1. Reconstruction of the Specific Protected Transmission Lines

First, based on the practical constraints, assume that the original sets of protected transmission lines, named Lp, are {10, 11, 16, 17, 19, 20}, {7, 17, 18, 21, 22, 24}, and {1, 2, 3, 6, 10, 12, 16, 17, 21, 22, 24, 30, 36, 38, 41, 54, 93, 147, 151, 161, 171, 172} for the IEEE 14-bus power system, IEEE 30-bus power system, and IEEE 118-bus power system, respectively.

Second, set the weight of every line as dC_{OPF}/dx_l for the abovementioned power systems. Applying the method from [11], the different numbers of MTD perturbation strategies and attack strategies are considered for the defender and attacker, respectively, in the above power systems. Relying on the Lp, we set the appropriate attack strategies for every power system. By avoiding huge fluctuations in the power flow, we limit the number of tripped lines, which is no more than two in each attack strategy. Moreover, the transmission lines are selected from the Lp. Then, after constructing a game model for every power system, the robust NE solutions for each system are obtained by injecting the real-world load profiles from New York State on 7 June 2020 into the three systems. We make use of the EXP3 algorithm [11] for computing robust NE solutions.

Lastly, after analyzing the NE solutions, the lines most likely to be cut off are identified for every power system. This causes the number of lines in Lp to be small, which implements the reconstruction of the specific protected transmission lines. We indicate the defender's and the attacker's action sets by $S_D = \{d_0, d_1, \ldots, d_{N_D-1}\}$ and $S_A = \{a_0, a_1, \ldots, a_{N_A-1}\}$, respectively, where N_D and N_A are the cardinality of the above sets, respectively. d_0 denotes that no defenders take action to defend the power systems; a_0 denotes that no attackers take action to disrupt the power systems.

5.1.1. New Lp Reconstructed for the IEEE 14-Bus System

In the IEEE 14-bus power system, five MTD perturbation strategies are considered for the defender, i.e., $d_1 = [1]$, $d_2 = [1,3]$, $d_3 = [1,3,5]$, $d_4 = [1,3,5,8]$, and $d_5 = [1,3,8,9,18,19]$. Twenty-one attacker's strategies are considered, i.e., $a_1 = [10]$, $a_2 = [11]$, $a_3 = [16]$, $a_4 = [17]$, $a_5 = [19]$, $a_6 = [20]$, $a_7 = [10,11]$, $a_8 = [10,16]$, $a_9 = [10,17]$, $a_{10} = [10,19]$, $a_{11} = [10,20]$, $a_{12} = [11,16]$, $a_{13} = [11,17]$, $a_{14} = [11,19]$, $a_{15} = [11,20]$, $a_{16} = [16,17]$, $a_{17} = [16,19]$, $a_{18} = [16,20]$, $a_{19} = [17,19]$, $a_{20} = [17,20]$, and $a_{21} = [19,20]$.

The used parameters in the game model are mainly referred to in Ref. [11], i.e., the generation cost model is denoted as $C_i(G_{i,t}) = c_i G_{i,t}$, and all of the generators' capacities are G_{max} = 300, 2000, 1500, 1000, 20 MW and c_i = 20, 30, 40, 50, and 35 USD/MW, respectively. The maximal power flow, $\mathbf{f}_{max}$, is 160 MW for link 1 and 60 MW for all other links. The operator factors used in the EXP3 algorithm are selected as follows. $\gamma_t = \beta_t = 0$, $\eta_t = 0.01$.

In the first simulation, the real-world load data injected came from time zero in New York State on 7 June 2020. The specific load data are shown in Ref. [30]. Specifically, the corresponding relationship between load buses with system buses is referred to in Ref. [12]. The real-world load data are injected at 2 h intervals. When injecting the real-world load data, the convergence rate of EXP3 is also reasonably fast, and the number of iterations is 173. In the end, all of the NE robust solutions are acquired, which are depicted in Figure 4.

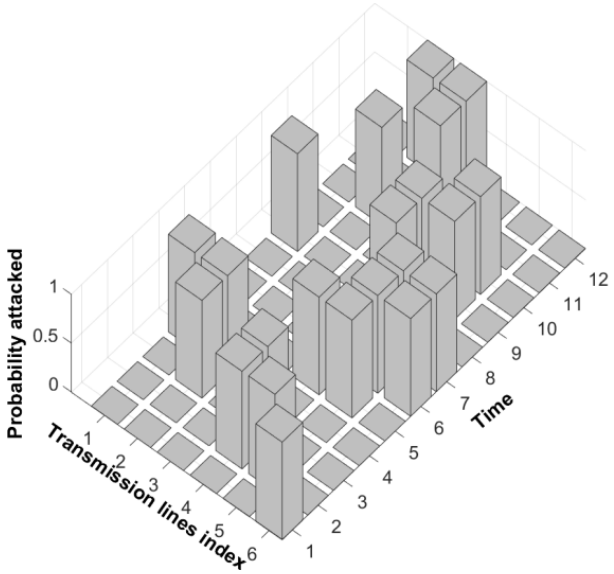

Figure 4. The robust NE solution to restructure the transmission lines in Lp for the IEEE 14-bus power system.

In Figure 4, the numbers on the time axis represent the time, i.e., number 1 represents time zero; number 2 represents two o'clock; number 3 represents four o'clock, and so on. The numbers on the other axis in the horizontal plane denote the indexes of links affiliated with the Lp, i.e., every number between 1 and 6 corresponds to one link index, denoting 10, 11, 16, 17, 19, and 20 in sequence. The vertical axis indicates the situation in which the line is being attacked, i.e., the number 1 denotes that the corresponding line has been attacked; the number 0 indicates that the corresponding line has not been attacked. Clearly, from Figure 4, we can see that the most likely lines to be attacked are lines 11, 17, 19, and 20. Compared with the original Lp, The 10th and 16th lines are removed. Lp is reconstructed, which accurately locks the target of the resourceful and sophisticated attacker. The reconstructed set of protected transmission lines is Lp = {11, 17, 19, 20}.

5.1.2. New Lp Reconstructed for the IEEE 30-Bus System

For the IEEE 30-bus power system, the approach and process of computing the robust NE solutions are similar to those for the IEEE 14-bus power system. We consider N_D and N_A as 8 and 22, respectively. Specifically, besides d_0, the detailed information regarding the remaining MTD strategies considered is as follows: $d_1 = [4]$, $d_2 = [4,7]$, $d_3 = [4,7,9]$, $d_4 = [4,7,9,10]$, $d_5 = [4,7,9,10,14,18]$, $d_6 = [4,7,9,10,14,18,24,26,28]$, and $d_7 = [4,\ 7,\ 9,\ 10,\ 14,\ 18,\ 24,\ 26,\ 28,\ 29,\ 37,\ 41]$. In addition to a_0, based on Lp, we assign the attacker's strategies as follows: $a_1 = [7]$, $a_2 = [17]$, $a_3 = [18]$, $a_4 = [21]$, $a_5 = [22]$, $a_6 = [24]$, $a_7 = [7,17]$, $a_8 = [7,18]$, $a_9 = [7,21]$, $a_{10} = [7,22]$, $a_{11} = [7,24]$, $a_{12} = [17,18]$, $a_{13} = [17,21]$, $a_{14} = [17,22]$, $a_{15} = [17,24]$, $a_{16} = [18,21]$, $a_{17} = [18,22]$, $a_{18} = [18,24]$, $a_{19} = [21,22]$, $a_{20} = [21,24]$, $a_{21} = [22,24]$. There are six generators in the IEEE 30-bus system. All of the generators' capacities are $G_{max} = 300, 1600, 300, 400,$ and 350 MW and $c_i = 20, 30, 40, 50, 35,$ and 30 USD/MWh, respectively.

The maximal power flow, $\mathbf{f}_{max}$, is 160 MW for link 1 and 60 MW for all other links. The operational factors in the EXP3 algorithm are invariant, $\gamma_t = \beta_t = 0$, $\eta_t = 0.01$. As in the case above, the real-world load data at different times are injected into the game model to compute every robust NE solution in sequence. All of the solutions are presented in Figure 5. In Figure 5, the meaning of the numbers on the three axes remains basically unchanged. One difference is that the numbers on the axis marked as "transmission lines index" indicate different lines, i.e., numbers 1, 2, 3, 4, 5, and 6 refer to the 7th, 17th, 18th, 21st, 22nd, and 24th lines in the IEEE 30-bus system.

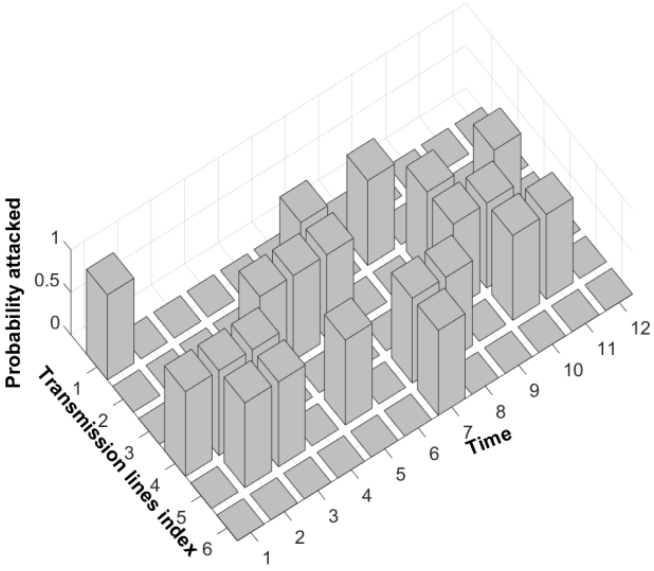

Figure 5. The robust NE solution to restructure the transmission lines in Lp for the IEEE 30-bus power system.

Figure 5 shows that the reconstructed set of protected transmission lines should be {17, 18, 21, 22}. Similarly, the target of the resourceful and sophisticated attacker is accurately locked, which reduces the expenditure of the defender in the context of the deployment of D-FACTS devices.

5.1.3. New Lp Reconstructed for the IEEE 118-Bus System

For the IEEE 118-bus power system, according to the successful results of the above two cases, we consider the number of transmission lines tripped in every attack strategy to be only one. We consider N_D and N_A as 14 and 23, respectively. Specifically, besides d_0 the detailed information regarding the remaining MTD strategies considered is as follows: $d_1 = [2,3,6]$, $d_2 = [2,3,6,8,11,12]$, $d_3 = [2,3,6,8,11,12,17,21,24]$, $d_4 = [2,3,6,8,11,12,17,21,24,26,30,32]$, $d_5 = [2,3,6,8,11,12,17,21,24,26,30,32,40,43,46]$, $d_6 = [2,3,6,8,11,12,17,21,24,26,30,32,40,43,46,50,51,55]$, $d_7 = [2,3,6,8,11,12,17,21,24,26,30,32,40,43,46,50,51,55,56,63,65]$, $d_8 = [2,3,6,8,11,12,17,21,24,26,30,32,40,43,46,50,51,55,56,63,65,68,69,71,75,76]$, $d_9 = \begin{bmatrix} 2,3,6,8,11,12,17,21,24,26,30,32,40,43,46,50,51, \\ 55,56,63,65,68,69,71,75,76,77,81,87,88,89,91 \end{bmatrix}$,

$d_{10} = \begin{bmatrix} 2,3,6,8,11,12,17,21,24,26,30,32,40,43,46,50,51,55,56,63, \\ 65,68,69,71,75,76,77,81,87,88,89,91,92,98,99,100,106 \end{bmatrix}$,

$d_{11} = \begin{bmatrix} 2,3,6,8,11,12,17,21,24,26,30,32,40,43,46,50,51,55, \\ 56,63,65,68,69,71,75,76,77,81,87,88,89,91,92,98, \\ 99,100,106,112,113,115,117,119,121,124,127 \end{bmatrix}$,

$d_{12} = \begin{bmatrix} 2,3,6,8,11,12,17,21,24,26,30,32,40,43,46,50, \\ 51,55,56,63,65,68,69,71,75,76,77,81,87,88,89, \\ 91,92,98,99,100,106,112,113,115,117,119,121, \\ 124,127,132,135,139,140,143,148,150,152,154 \end{bmatrix}$,

$d_{13} = \begin{bmatrix} 2,3,6,8,11,12,17,21,24,26,30,32,40,43,46,50,51, \\ 55,56,63,65,68,69,71,75,76,77,81,87,88,89,91, \\ 92,98,99,100,106,112,113,115,117,119,121, \\ 124,127,132,135,139,140,143,148,150,152,154, \\ 156,158,161,162,166,171,175,178 \end{bmatrix}$.

In addition to a_0, based on Lp, we assign the attacker's strategies as follows: $a_1 = [1]$, $a_2 = [2]$, $a_3 = [3]$, $a_4 = [6]$, $a_5 = [10]$, $a_6 = [12]$, $a_7 = [16]$, $a_8 = [17]$, $a_9 = [21]$, $a_{10} = [22]$, $a_{11} = [24]$, $a_{12} = [30]$, $a_{13} = [36]$, $a_{14} = [38]$, $a_{15} = [41]$, $a_{16} = [54]$, $a_{17} = [93]$, $a_{18} = [147]$, $a_{19} = [151]$, $a_{20} = [161]$, $a_{21} = [171]$, and $a_{22} = [172]$.

In the IEEE 118-bus power system, there are fifty-four generators. The first six generators' capacities are G_{max} = 2000, 1000, 1000, 1500, 500, and 1000 MW and c_i = 20, 30, 40, 50, 35, and 30 USD/MWh. The rest of the generators' capacities are the same, $G_{max} = 500$ MW and $c_i = 36$ USD/MWh.

The maximal power flow, $\mathbf{f}_{max}$, is 500 MW for all links. The operational factors and the injection method with regard to the real-world load data are completely unchanged. All of the robust NE solutions are presented in Figure 6. Homoplastically, in Figure 6, the numbers on the axis marked as "transmission lines index" indicate different lines, i.e., the numbers 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, and 22 refer to the 1st, 2nd, 3rd, 6th, 10th, 12th, 16th, 17th, 21st, 22nd, 24th, 30th, 36th, 38th, 41st, 54th, 93rd, 147th, 151st, 161st, 171st, and 172nd lines in the IEEE 118-bus power system. Figure 6 indicates that the reconstructed set of protected transmission lines should be {30, 36, 38, 41, 54, 93, 147, 151, 161, 171, and 172}. The number of original protected transmission lines is 22; however, through the results of the robust NE solutions, the number of authentically protected transmission lines is greatly reduced to only 11 links, which evidently reduces the expenditure of the defender in the context of the deployment of D-FACTS devices.

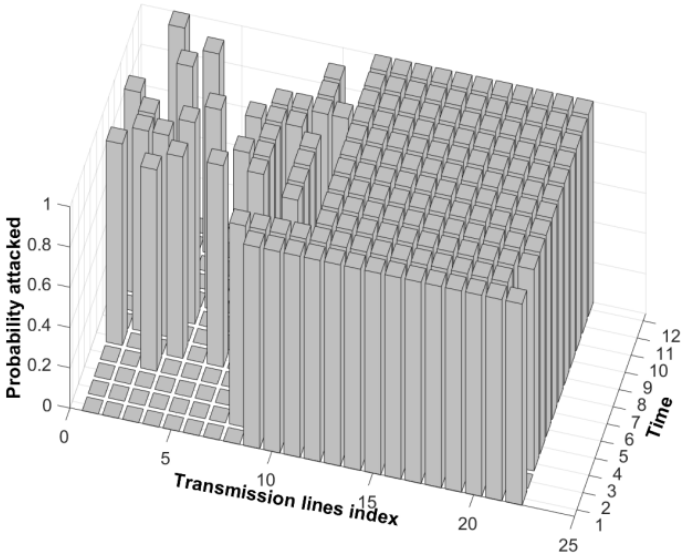

Figure 6. The robust NE solution to restructure the transmission lines in Lp for the IEEE 118-bus power system.

Note that we mainly use the fmincon package during the process of computing the robust NE solutions. For a large-scale power system, i.e., the IEEE 118 system, it is non-trivial to make sure that a feasible solution can be invariably acquired in every iteration with the fmincon package and the convergence of the EXP3 algorithm. Therefore, for the IEEE 118-bus power system, we consider using the relaxed constraints during the process of computing the NE solutions.

5.1.4. Analysis of the Results of the New Lp Reconstructed

The detailed results of the reconstruction of the protected transmission lines are shown in Table 3 as follows. In Table 3, after reconstruction, the number of protected transmission lines is small. Moreover, the larger the system size, the more significant the effect is. In the IEEE 118-bus power system, the number of original required transmission lines is 22, and the number of required lines in the new system is only 11. Although the number of required lines is small, all remaining lines are the main targets for resourceful and sophisticated attackers who do not randomly select their targets. So, on the basis of defense effectiveness, the number of required lines is small, which facilitates the better deployment of D-FACTS devices and will improve operational costs.

Table 3. The two sets of protected transmission lines before reconstruction and after reconstruction.

Original Lp	New Lp	Standard Power System
{10, 11, 16, 17, 19, 20}	{11, 17, 19, 20}	IEEE 14-bus power system
{7, 17, 18, 21, 22, 24}	{17, 18, 21, 22}	IEEE 30-bus power system
{1, 2, 3, 6, 10, 12, 16, 17, 21, 22, 24, 30, 36, 38, 41, 54, 93, 147, 151, 161, 171, 172}	{30, 36, 38, 41, 54, 93, 147, 151, 161, 171, 172}	IEEE 118-bus power system

5.2. Optimal Deployment of D-FACTS Devices and Analysis of the Results

For the IEEE 14-bus system, the new set of the protected lines, Lp, is {11, 17, 19, 20}, as depicted in Figure 7. In Figure 7, the new protected transmission lines are represented by red circles. The covered buses, shown as $\mathcal{N}_P$, are $\mathcal{N}_P = \{6,\ 9,\ 11,\ 12,\ 13,\ 14\}$. According to the old algorithm, the buses in $\mathcal{N}_P$ and the transmission lines in $\mathcal{L}_P^* = \{\{6,11\},\{6,12\},\{6,13\},\{12,13\},\{13,14\},\{9,14\}\}$ form a subgraph $\mathcal{G}_P$. In $\mathcal{G}_P$, a spanning tree $\mathcal{T} = \{\{6,11\},\{6,12\},\{6,13\},\{9,14\},\{13,14\}\}$ may be obtained, then $\mathcal{R} = \{\{12,13\}\}$. So, $\widetilde{\mathcal{L}}^* = \{\{12,13\}\}$ is acquired, and the output set is $\widetilde{\mathcal{L}}' = \{\{5,6\},\{10,11\},\{9,10\},\{4,9\},\{7,9\}\}$. The border bus denoted in the old algorithm is bus 9 and $\widetilde{\mathcal{L}}'' = \{\{9,10\},\{4,9\},\{7,9\}\}$. In the end, $\widetilde{\mathcal{L}}^* = \{\{12,13\},\{5,6\},\{10,11\}\}$ is computed, then $\widetilde{\mathcal{L}}^o = \widetilde{\mathcal{L}}^*$, in which the transmission lines are deployed with D-FACTS devices. The minimum number of required D-FACTS devices is three. In Figure 7, based on the original set of protected lines, the transmission lines requiring D-FACTS devices are {{4, 9},{7, 9},{9, 10}}. The minimum number of required D-FACTS devices is also three. Due to the IEEE 14-bus power system being small, the new approach does not seem to have any advantage, and the process seeking the results of the deployment of D-FACTS devices relies on the old algorithm. However, once the power system is large-scale, the situation will be completely different.

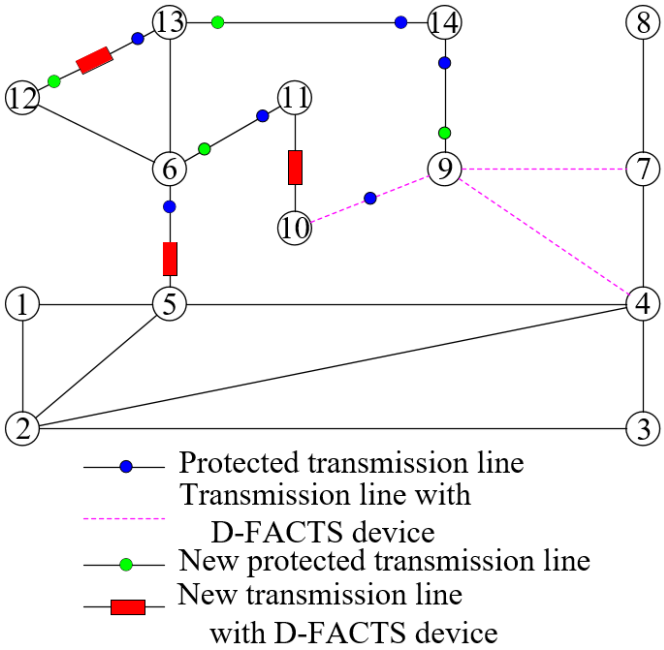

Figure 7. The two optimal deployments of D-FACTS devices with the IEEE 14-bus power system.

For the IEEE 30-bus power system, the new set of protected transmission lines, Lp, is {17,18,21,22}, as depicted in Figure 8. The covered buses, shown as $\mathcal{N}_P$, are $\mathcal{N}_P = \{12,14,15,16,17,18\}$. A subgraph $\mathcal{G}_P$ is formed with the buses in $\mathcal{N}_P$ and transmission lines in $\mathcal{L}_P^* = \{\{12,14\},\{12,15\},\{14,15\},\{15,18\},\{12,16\},\{16,17\}\}$. In $\mathcal{G}_P$, a spanning tree $\mathcal{T} = \{\{12,14\},\{12,15\},\{12,16\},\{16,17\},\{15,18\}\}$ may be selected,

then $\mathcal{R} = \{\{14,15\}\}$. So, $\widetilde{\mathcal{L}}^*$ is confirmed, depicted as $\{\{14,15\}\}$. The output set is $\widetilde{\mathcal{L}}' = \{\{4,12\},\{12,13\},\{15,23\},\{18,19\},\{10,17\}\}$ and the set of cut lines in $\widetilde{\mathcal{L}}'$ is $\mathcal{C}' = \{\{12,13\}\}$. Then, there is a question to be considered. From Figure 8, based on the old algorithm, the border bus is bus 12. However, the line {{12, 13}} is a cut line, and a D-FACTS device does not need to be deployed on it, so this line should not be considered. Therefore, there are four schemes for confirming the border bus. Buses 12, 15, 17, and 18 are all likely to be the border bus. The old algorithm is powerless to confirm the bus. Meanwhile, the border bus is easily determined based on the proposed algorithm in this paper. Through separately examining the weights of the four lines, which are {{4, 12}}, {{15, 23}}, {{18, 19}} and {{17, 10}}, respectively, we can finally confirm that bus 15 is selected as the border bus due to the minimum weight in {{15, 23}}. Next, it is easy to determine $\widetilde{\mathcal{L}}'' = \{\{15,\ 23\}\}$ and $\widetilde{\mathcal{L}}^* = \{\{14,15\},\{4,12\},\{18,19\},\{10,17\}\}$. According to the old algorithm, there is also an intractable question since the numbers for both the set $\widetilde{\mathcal{L}}^*$ and Lp is four. How do we achieve the suitable deployment of D-FACTS devices? Similarly, after computing the sum of the line weights in the above two sets, we confirm that the suitable set of transmission lines requiring D-FACTS devices is $\widetilde{\mathcal{L}}^*$ due to the sum of the weights corresponding to $\widetilde{\mathcal{L}}^*$ being bigger, and thus $\widetilde{\mathcal{L}}^o = \widetilde{\mathcal{L}}^*$. Clearly, the new algorithm proposed in this paper is more comprehensive than the old algorithm. In particular, we can also guarantee both defense effectiveness and operational costs.

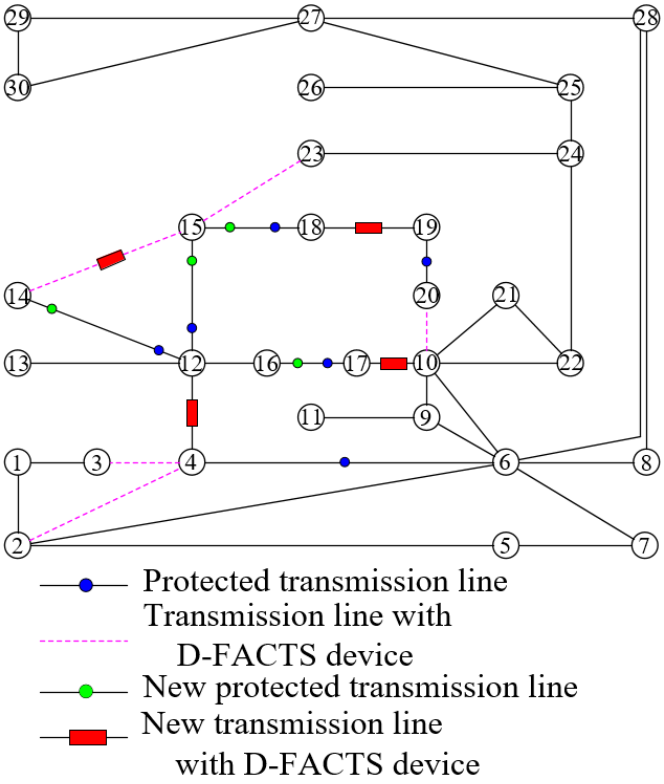

Figure 8. The two optimal deployments of D-FACTS devices with the IEEE 30-bus power system.

For the more large-scale IEEE 118-bus power system, the approach toward the reconstruction of the specific protected transmission lines and the proposed algorithm in our work is more powerful. In Figure 9, the new set of protected transmission lines is {30, 36, 38, 41, 54, 93, 147, 151, 161, 171, 172}. The covered buses are $\mathcal{N}_P = \{17,\ 23,\ 24,\ 26,\ 30,\ 32,\ 38,\ 65,\ 92,\ 98,\ 100,\ 104,\ 105,\ 113\}$. The two subgraphs $\mathcal{G}_P^1$ *and* $\mathcal{G}_P^2$ are formed by $\mathcal{N}_P$ and transmission lines $\mathcal{L}_P^* = \{\{17,113\},\{113,32\},\{17,30\},\{26,30\},\{23,32\},\{23,24\},\{30,38\},\{38,65\},\{92,100\},\{98,100\},\ \{100,104\},\{104,105\}\}$. The following steps are carried out according to the new algorithm. In $\mathcal{G}_P^1$, $\mathcal{G}_P^1$ is just a spanning tree and $\mathcal{R}_1$ is a null set. So, $\widetilde{\mathcal{L}}_1^*$ is also a null set. $\widetilde{\mathcal{L}}_1' = \{\{31,32\},\{32,114\},\{27,32\},$

$\{15,17\},\{16,17\},\{17,18\},\{17,31\}$, $\{23,25\},\{25,26\},\{24,70\},\{24,72\}$, $\{37,38\},\{64,65\}$, $\{65,66\},\{65,68\},\{22,23\}\}$ and the set $\mathcal{C}_1'$={} are known. In $\mathcal{G}_P^1$, the border bus is bus 17, and the set $\widetilde{\mathcal{L}}_1'' = \{\{15,17\},\{16,17\},\{17,18\},\{17,31\}\}$ is obtained. The set $\widetilde{\mathcal{L}}_1^* = \{\{31,32\},\{32,114\},\{27,32\},\{23,25\},\{25,26\},\{24,70\},\{24,72\},\{37,38\},\{64,65\}$, $\{65,66\},\{65,68\},\{22,23\}\}$, and it cardinality is 12; nevertheless, the number for the set $\mathcal{L}_P^1$ is 8, so the set $\widetilde{\mathcal{L}}_1^o = \mathcal{L}_P^1$ is confirmed. In another subgraph, $\mathcal{G}_P^2$ is also a spanning tree and $\mathcal{R}_2$ is a null set. So, $\widetilde{\mathcal{L}}_2^*$ is also null. $\widetilde{\mathcal{L}}_2' = \{\{89,92\},\{91,92\},\{92,93\},\{92,94\},\{92,102\}$, $\{80,98\}$, $\{94,100\}$, $\{99,100\},\{100,106\}$, $\{101,100\}$, $\{100,103\}$, $\{103,104\}$, $\{103,105\}$, $\{105,106\},\{105,107\}\}$. Although the number of transmission lines incident to buses 92 and 100 is 5, by computing the sum of the weights of the selected transmission lines, we can confirm that the border bus is bus 92, and then $\widetilde{\mathcal{L}}_2'' = \{\{89,92\}$, $\{91,92\}$, $\{92,93\}$, $\{92,94\}$, $\{92,102\}\}$ due to the first sum is more smaller. Then, $\widetilde{\mathcal{L}}_2^* = \{\{80,98\},\{94,100\},\{99,100\}$, $\{100,106\}$, $\{101,100\}$, $\{100,103\}$, $\{103,104\}$, $\{103,105\}$, $\{105,106\}$, $\{105,107\}\}$ is obtained. In the end, $\widetilde{\mathcal{L}}_2^o = \mathcal{L}_P^2$ = {{92, 100},{98, 100},{104, 105}} is acquired. So, the suitable set of transmission lines for the deployment of D-FACTS devices is just the new set of protected transmission lines reconstructed. The required number of D-FACTS devices is only 11, in contrast to the required number of D-FACTS devices being 22 based on the original set of protected transmission lines. Obviously, this provides a quite competitive cost-benefit on the basis of guaranteeing defensive effectiveness.

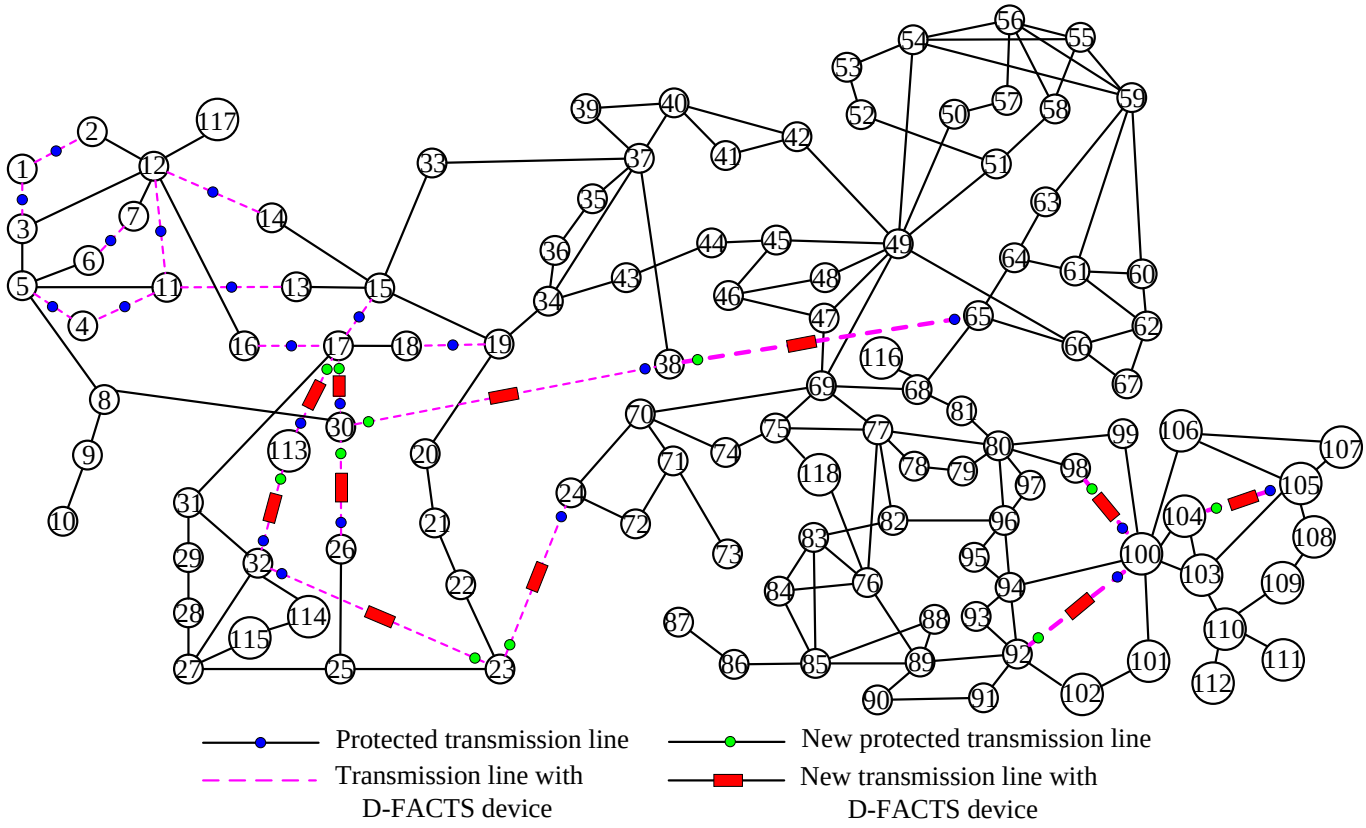

Figure 9. The two optimal deployments of D-FACTS devices with the IEEE 118-bus power system.

Overall, although the topologies of the three abovementioned power systems are completely different, the new algorithm presented in this study can be easily used for acquiring the optimal deployment of D-FACTS devices in all three cases.

6. Discussion

6.1. Research Motivation

Section 2 presents the achievements of using the MTD method to defend against malicious attacks on SGs in detail and fully analyzes previous methods to solve the deployment of D-FACTS devices, and this graphically shows the evolution in the field of deploying D-FACTS devices. Some findings have been revealed. (1) As the MTD method has become mainstream in the field of defense against multiple covert cyber-attacks, how to deploy D-FACTS devices has become a research hotspot. (2) Although several valuable approaches have been presented on how to deploy D-FACTS devices, they are essentially based on the knowledge of system topology and mathematical statistics knowledge. However, from the macro level of defending against malicious attacks, attack, and defense are opposite and unified, which is an organic whole. Without considering the attack characteristics of a smart attacker, the followed defense is certainly not the most effective and intelligent. In fact, for one specific medium and large-scale power system, due to different system topologies and load profiles, the power flow distribution must be distinct. The aggressive behavior of a smart attacker is intelligent, e.g., a line constituting a "cut" set is not attacked, nor are lines with small power flows. As long as it is deciphered, which lines are most likely to be attacked, the defender can afford the targeted deployment of D-FACTS devices. This is certainly better than the deployments merely based on mathematical knowledge, which ensures not only MTD's effectiveness against cyber-attacks but also achieves optimal cost and operational loss. In our works, a zero-sum game is formulated. After acquiring a robust NE solution utilizing the EXP3 algorithm, from the point of view of the sophisticated attacker, the lines of the most likely to be attacked may be identified, and then the deployment of D-FACTS devices can be intelligent. This is the first time that the game result was analyzed from the perspective of an attacker.

6.2. Research Value

By analyzing a game solver from the perspective of the attacker and confirming the lines that the attacker is most likely to attack, the defender can intelligently deploy D-FACTS devices. This may represent the research value of our work. Moreover, in the field of MTD defense against CCPAs, the accurate location associated with tripped lines should be the next research point. At present, the research results are very rare, and only one study in the literature [37] has provided a method. The authors in Ref. [37] proposed finding the location of tripped lines by applying a CNN. We believe that this approach is feasible. However, locating faulty lines is a multi-classification problem. As the system becomes larger, the number of categories becomes larger and larger. For example, when supposing that the maximum number of tripped lines is two, there are 210 categories for the IEEE 14-bus power system, and for the IEEE 118-bus system, the number is 15931. The larger the number of categories, the more complex the composition of CNN. In addition to these conditions, the data to train and test the CNN will also be huge, which puts forward higher requirements for computer hardware and software. Thus, this is likely to be unsolved. If the concept of this paper is adopted, the actual number of classifications will significantly decrease. For example, the number of classifications is 10 for the IEEE 14-bus power system; the number is only 66 for the IEEE 118-bus power system. From 15,931 to only 66 on the IEEE 118-bus power system, when applying a CNN to locate tripped lines, it undoubtedly greatly reduces the requirements of computer hardware and software. At present, we are conducting this work. Considering the attackers' attack behaviors, this method can also be applied to intelligent detection and operational maintenance.

7. Conclusions and Future Work

In the MTD strategies against CCPAs, defensive effectiveness and operational cost are two of the main research points. The relationship between the two points is often opposite, and so an important question as to what the optimal deployment strategy for D-FACTS devices is has evolved to effectively eliminate this antagonism. For any resourceful

and sophisticated attacker, when completely dividing their aggressive behaviors, the deployment solutions must not be intelligent.

In this paper, we propose a new method for finding intelligent deployment solutions for D-FACTS devices. Specifically, first, the basic concept of corrupting CCPAs is summarized; second, based on the practical constraints and the basic concept, a protected transmission line set is confirmed; and third, a zero-sum game model is formulated, and a robust NE solution is computed. Due to the game's characteristics, this solution reflects the smart attackers' sense of action. Relying on the solution, those lines that are most likely to be tripped form a new protected transmission line set. Finally, a comprehensive algorithm using a metric proposed in predecessors is proposed for finding an intelligent solution for the deployment of D-FACTS devices. We validated the results through extensive simulations using IEEE 14-bus, 30-bus, and 118-bus power systems provided by MATPOWER and real-world load profiles from New York State. Our study, in tracking the targets that attackers are most likely to attack, opens up new ideas for the intelligent deployment of D-FACTS devices.

In addition, tracking the target most likely to be attacked will achieve efficient defense. The work in this paper is a meaningful attempt to improve defense efficiency. In the future, on the basis of making use of the concepts presented in this study, we can explore several meaningful questions, such as establishing the location of tripped transmission line [37] and better MTD strategies.

Author Contributions: Conceptualization and methodology J.Y.; software, J.Y.; validation, J.Y. and Q.L.; formal analysis, J.Y. and Q.L.; writing—original draft, J.Y.; writing—review and editing, Q.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The original data used to support the results of this study are from MATPOWER and the literature [11].

Acknowledgments: The authors would like to thank the editors and anonymous reviewers for their careful reading and insightful remarks.

Conflicts of Interest: The authors declare no conflict of interest.

Nomenclature

CPS	Cyber–physical system
SG	Smart grid
FDIAs	False data injection attacks
CCPAs	Coordinated cyber–physical attacks
PMUs	Phasor measurement units
ML	Machine learning
MTD	Moving target defense
D-FACTS	Distributed flexible AC transmission system
NE	Nash equilibrium
SE	State estimation
OPF	Optimal power flow
SPA	Smallest principal angle
WLS	Weighted least squares
BDD	Bad data detection
EXP3	Exploration and exploitation
BFS	Breath-first search

$\mathcal{G}$	Graph representing the topology of the system
$\mathcal{N}$	Set of the buses in the system
$\mathcal{L}$	Set of the lines in the system
i, j	Bus index
b_{ij}	Susceptance of the line between buses i and j
z	Vector of all measurements
$\boldsymbol{H}$	Measurement matrix
$\boldsymbol{e}$	Measurement error vector
$\boldsymbol{\theta}$	Voltage phase angles vector
θ_i	Voltage phase angle at bus i
$\boldsymbol{H}_k$	The kth row of $\boldsymbol{H}$
$\boldsymbol{r}$	Measurement residual vector
τ	Threshold of BDD system
$\boldsymbol{A}$	Reduced branch-bus incidence matrix
$\boldsymbol{D}$	Diagonal branch susceptance matrix
$\boldsymbol{a}$	Attack vector
z^a	Compromised vector of all measurements
$\boldsymbol{a}_p$	Physical attack vector
$\boldsymbol{H}_p$	Measurement matrix after a physical attack
$\boldsymbol{\theta}_p$	Voltage phase angles vector after a physical attack
$\Delta \boldsymbol{H}$	Measurement difference matrix between post-attack and pre-attack

References

1. Lydia, M.; Kumar, G.E.P.; Selvakumar, A.I. Securing the cyber-physical system: A review. *Cyber-Physical Syst.* **2022**, 1–31. [CrossRef]
2. Shetu, S.F.; Saifuzzaman, M.; Moon, N.N.; Nur, F.N. A survey of botnet in cyber security. In Proceedings of the ICCT, Jaipur, India, 28–29 September 2019; pp. 174–177.
3. Liu, Y.; Ning, P.; Reiter, M.K. False data injection attacks against state estimation in electric power grids. In Proceedings of the 16th of ACM Conference on Computer and Communications Security, Chicago, IL, USA, 9–13 November 2009.
4. E-ISAC. *Analysis of the Cyber Attack on the Ukrainian Power Grid*; DUC Tech. Rep. 5; Electricity Information Sharing and Analysis Center: Washington, DC, USA, 2016; Available online: https://ics.sans.org/media/E-ISACsANSUkraineDUC5.pdf (accessed on 18 March 2016).
5. Li, Z.; Shahidehpour, M.; Alabdulwahab, A.; Abusorrah, A. Bilevel model for analyzing coordinated cyber-physical attacks on power systems. *IEEE Trans. Smart Grid* **2016**, *7*, 2260–2272. [CrossRef]
6. Deng, R.; Zhuang, P.; Liang, H. CCPA: Coordinated cyber-physical attacks and countermeasures in smart grid. *IEEE Trans. Smart Grid* **2017**, *8*, 2420–2430. [CrossRef]
7. Shepard, D.P.; Humphreys, T.E.; Fansler, A.A. Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks. *Int. J. Crit. Infrastruct. Prot.* **2012**, *5*, 146–153. [CrossRef]
8. Ozay, M.; Esnaola, I.; Vural, F.T.Y.; Kulkarni, S.R.; Poor, H.V. Machine learning methods for attack detection in the smart grid. *IEEE Trans. Neural Netw. Learn. Syst.* **2016**, *27*, 1773–1786. [CrossRef]
9. He, Y.; Mendis, G.J.; Wei, J. Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism. *IEEE Trans. Smart Grid* **2017**, *8*, 2505–2526. [CrossRef]
10. Sayghe, A.; Anubi, O.M.; Konstantinou, C. Adversarial examples on power systems state estimate. In Proceedings of the IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 1–5 February 2020.
11. Lakshminarayana, S.; Belmega, E.V.; Poor, H.V. Moving-target defense against cyber-physical attacks in power grids via game theory. *IEEE Trans. Smart Grid* **2021**, *12*, 5244–5257. [CrossRef]
12. Zhang, Z.; Tian, Y.; Deng, R.; Ma, J. A double-benefit moving target defense against cyber-physical attacks in smart grid. *IEEE Internet Things J.* **2022**, *9*, 17912–17925. [CrossRef]
13. Morrow, K.L.; Heine, E.; Rogers, K.M.; Bobba, R.B.; Overbye, T.J. Topology perturbation for detecting malicious data injection. In Proceedings of the Hawaii ICSS, Maui, HI, USA, 4–7 February 2012.
14. Davis, K.R.; Morrow, K.L.; Bobba, R.; Heine, E. Power flow cyberattacks and perturbation-based defense. In Proceedings of the IEEE SmartGridComm, Taiwan, China, 5–8 November 2012.
15. Esmalifalak, M.; Shi, G.; Han, Z.; Song, L. Bad data injection attack and defense in electricity market using game theory study. *IEEE Trans. Smart Grid* **2013**, *4*, 160–169. [CrossRef]
16. Sanjab, A.; Saad, W. Data injection attacks on smart grids with multiple adversaries: A game-theoretic perspective. *IEEE Trans. Smart Grid* **2016**, *7*, 2038–2049. [CrossRef]
17. Habibi, M.R.; Baghaee, H.R.; Dragičević, T.; Blaabjerg, F. False data injection cyber-attacks mitigation in parallel DC/DC converters based on artificial neural networks. *IEEE Trans. Circuits Syst. II Express Briefs* **2021**, *68*, 717–721. [CrossRef]

18. Rahman, M.A.; Al-Shaer, E.; Bobba, R.B. Moving target defense for hardening the security of the power system state estimation. In Proceedings of the ACM MTD, Scottsdale, AZ, USA, 3 November 2014.
19. Yang, Q.; Li, D.; Yu, W.; Liu, Y.; An, D.; Yang, X.; Lin, J. Toward data integrity attacks against optimal power flow in smart gird. *IEEE Internet Things J.* **2017**, *4*, 1726–1738. [CrossRef]
20. Liu, C.; Wu, J.; Long, C.; Kundur, D. Reactance perturbation for detecting and identifying fdi attacks in power system state estimation. *IEEE J. Sel. Top. Signal Process.* **2018**, *12*, 763–776. [CrossRef]
21. Lakshminarayana, S.; Yau, D.K. Cost-benefit analysis of moving target defense in power grids. *IEEE Trans. Power Syst.* **2021**, *36*, 1152–1163. [CrossRef]
22. Tian, J.; Tan, R.; Guan, X.; Liu, T. Enhanced hidden moving target defense in smart grids. *IEEE Trans. Smart Grid* **2019**, *10*, 2208–2223. [CrossRef]
23. Zhang, Z.; Deng, R.; Yau, D.K.Y.; Cheng, P.; Chen, J. Analysis of moving target defense against false data injection attacks on power grid. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 2320–2335. [CrossRef]
24. Liu, B.; Wu, H. Optimal D-FACTS placement in moving target defense against false data injection attacks. *IEEE Trans. Smart Grid* **2020**, *11*, 4345–4357. [CrossRef]
25. Soltan, S.; Yannakakis, M.; Zussman, G. Joint cyber and physical attacks on power grids: Graph theoretical approaches for information recovery. In Proceedings of the ACM SIGMETRICS, Portland, OR, USA, 15–19 June 2015.
26. Zhang, Z.; Deng, R.; Cheng, P.; Chow, M.-Y. Strategic protection against FDI attacks with moving target defense in power grids. *IEEE Trans. Control Netw. Syst.* **2022**, *9*, 245–256. [CrossRef]
27. Divan, D.; Johal, H. Distributed FACTS—A new concept for realizing grid power flow control. *IEEE Trans. Power Electron.* **2007**, *22*, 2253–2260. [CrossRef]
28. Rogers, K.M.; Overbye, T.J. Some applications of distributed flexible AC transmission system (D-FACTS) devices in power systems. In Proceedings of the 2008 40th North American Power Symposium, Calgary, AB, Canada, 28–30 September 2008.
29. Rogers, K.M.; Overbye, T.J. Power flow control with distributed flexible AC transmission system (D-FACTS) devices. In Proceedings of the 41st North American Power Symposium, Starkville, MS, USA, 4–6 October 2009.
30. Li, B.; Xiao, G.; Lu, R.; Deng, R.; Bao, H. Data injection attacks on power grid state estimation using D-FACTS devices. *IEEE Trans. Ind. Inform.* **2020**, *16*, 854–864. [CrossRef]
31. Liu, B.; Wu, H. Optimal planning and operation of hidden moving target defense for maximal detection effectiveness. *IEEE Trans. Smart Grid* **2021**, *12*, 4447–4459. [CrossRef]
32. Liu, B.; Wu, H. Systematic planning of moving target defense for maximizing detection effectiveness against false data injection attacks in smart grid. *IET Cyber-Phys. Syst. Theory Appl.* **2021**, *6*, 151–163. [CrossRef]
33. Liu, M.; Zhao, C.; Zhang, Z.; Deng, R. Explicit analysis on effectiveness and hiddenness of moving target defense in AC power systems. *IEEE Trans. Power Syst.* **2022**, *37*, 4732–4746. [CrossRef]
34. Wang, J.; Tian, J.; Liu, Y.; Yang, D.; Liu, T. MMTD: Multi-stage moving target defense for security-enhanced D-FACTS operation. *IEEE Internet Things J.* **2023**, 1. [CrossRef]
35. Xu, W.; Jaimoukha, I.M.; Teng, F. Robust moving target defense against false data injection attacks in power grids. *IEEE Trans. Inf. Forensics Secur.* **2023**, *18*, 29–40. [CrossRef]
36. Zhang, Z.; Deng, R.; Yau, D.K.Y.; Cheng, P.; Chow, M.-Y. Security enhancement of power system state estimation with an effective and low-cost moving target defense. *IEEE Trans. Syst. Man Cybern. Syst.* **2023**, *53*, 3066–3081. [CrossRef]
37. Chen, Y.; Lakshminarayana, S.; Teng, F. Localization of coordinated cyber-physical attacks in power grids using moving target defense and deep learning. In Proceedings of the IEEE SmartGridComm, Singapore, 25–28 October 2022.
38. Biswas, R.S.; Pal, A.; Werho, T.; Vittal, V. A graph theoretic approach to power system vulnerability identification. *IEEE Trans. Power Syst.* **2021**, *36*, 923–935. [CrossRef]
39. Tushar, W.; Yuen, C.; Saha, T.K.; Nizami, S.; Alam, M.R.; Smith, D.B.; Poor, H.V. A survey of cyber-physical systems from a game-theoretic perspective. *IEEE Access* **2023**, *11*, 9799–9834. [CrossRef]
40. Etesami, S.R.; Başar, T. Dynamic games in cyber-physical security: An overview. *Dyn. Games Appl.* **2019**, *9*, 884–913. [CrossRef]
41. NYISO Load Data. 2020. Available online: https://www.nyiso.com/load-data (accessed on 7 June 2020).