Extended Moving Target Defense for AC State Estimation in Smart Grids

Meng Zhang, Xuzhen Fan, Rongxing Lu, *Fellow, IEEE,* Chao Shen, Xiaohong Guan, *Fellow, IEEE*

***Abstract*—The moving target defense (MTD) that proactively changes series reactance of transmission lines has recently been proposed as an effective defense approach to resist false data injection attacks in smart grids. However, the defense effectiveness analyses of MTD in existing research are mainly focused on linear DC state estimation. To bring the state-of-the-art research to practice, MTD for AC state estimation is investigated in this paper. Specifically, based on a thorough analysis, an extended MTD (EMTD) approach that coordinately changes series reactance and parallel susceptance of lines in smart grids is proposed to improve the traditional MTD. Moreover, the impact of EMTD on electricity market is analyzed. On this basis, the variation of locational marginal price, the variation of active power loss and the cost of devices for executing EMTD are treated as the cost of system defense. Furthermore, to find the trade-off between the defense effectiveness and the cost of EMTD, optimal construction of cost-minimization EMTD topology parameter scheme and defense time interval are also proposed. Finally, extensive simulations are conducted on the standard IEEE test system to demonstrate the effectiveness of the proposed approach.**

***Index Terms*—False data injection attack, moving target defense, electricity market, smart grid.**

I. Introduction

False data injection (FDI) attacks are one of the most destructive types of malicious attacks for smart grids, which utilize the topology and parameter information of smart grids to design attack strategies and tamper with measurement data [1]. By designing attack vectors using complete or even incomplete system information, FDI attacks can be launched against both DC and AC state estimation while keeping stealthy to the bad data detection (BDD) mechanism [2]–[5]. Attackers can modify the estimated states by compromising measurements in SCADA system, causing severe consequences such as key lines overloading and load shedding [6].

To defend against FDI attacks, moving target defense (MTD) that proactively perturbs the series reactance of transmission lines using distributed flexible AC transmission system (D-FACTS) devices has been proposed. Since its introduction, MTD has drawn increasing attention of researchers. [7] and [8] early proposed to proactively change the topology parameters of smart grids to detect ongoing FDI attacks. [9] combined the concept of MTD with changing topological parameters and proposed a randomly-generated MTD scheme where the series reactance on an arbitrary subset of D-FACTS equipped lines can be randomly changed. [10] pointed out powerful attackers can notice the existence of MTD and thus proposed a hidden MTD to improve the stealthiness of MTD, based on which [11] analyzed the optimal D-FACTS devices planning of hidden MTD. Considering the voltage stability, [12] proposed a deeply-hidden MTD to hide both the self and mutual reactance of lines in the unbalanced distribution system. [13] designed a converter-based MTD by proactively perturbing the primary control gains to defend against deception attacks in DC microgrids. [14] utilized MTD to detect stealthy Stuxnet-like attacks that constructed based on the knowledge of the systems configuration.

Since the core of the MTD's defense effectiveness is to proactively disturb smart grids such that attackers can not exploit the right system parameters to construct attack vectors, recent researches have been devoted to analyzing the defense effectiveness of MTD. [15] analyzed the relationship between the completeness of MTD and the system topology, then concluded MTD has the capability in thwarting all FDI attacks under certain conditions. [16] showed the necessary and sufficient condition for three types of FDI attacks being detectable is that the branches covered by D-FACTS devices should contain at least a spanning tree of the grid graph. [17] proposed novel D-FACTS placement algorithms that can achieve the maximum MTD effectiveness with the minimum number of D-FACTS devices. [18] proposed a game theory method to minimize the defense cost while ensuring safety. However, most of the above analyses are based on DC state estimation and the impact of MTD on electricity market has not been considered. Besides, the relationship between the defense effectiveness and the defense cost of MTD has also not been fully investigated.

In response to above discussions, this paper proposes a MTD scheme for AC state estimation in smart grids. Specifically, an extended MTD (EMTD) approach that coordinately changes series reactance and parallel susceptance is proposed to enhance the defense effectiveness of traditional MTD (TMTD). The impact of EMTD on electricity market is analyzed, then the variation of electricity price, the variation of active power loss and the cost of devices for executing EMTD are treated as the cost of EMTD. To find the trade-off between the defense effectiveness and the cost of EMTD, optimal construction methods of EMTD topology parameter scheme and defense time interval are proposed. Finally, the effectiveness of the proposed EMTD is verified on the standard IEEE test

This work is supported in part by the National Key Research and Development Program of China (2019YFB1312000) and in part by the National Natural Science Foundation of China (61903292, 62033005 and 62273270). (Corresponding author: Meng Zhang).

M. Zhang, X. Fan, C. Shen and X. Guan are with the School of Cyber Science and Engineering, Xi'an Jiaotong University, Xi'an 710049, China. (E-mail: mengzhang2009@xjtu.edu.cn; fxz3783@stu.xjtu.edu.cn; chaoshen@xjtu.edu.cn; xhguan@xjtu.edu.cn).

R. Lu is with the Faculty of Computer Science, University of New Brunswick, Fredericton, Canada E3B 5A3. (e-mail: rlu1@unb.ca).

system. Particularly, the main contributions of this paper are summarized as follows:

- MTD's effectiveness to detect FDI attacks is analyzed based on the more practical AC state estimation. Based on the analysis, EMTD that coordinately changes series reactance and parallel susceptance is proposed. We prove that the defense effectiveness of EMTD can be stronger than that of TMTD both in the sense of state estimation residual and Kullback Leibler Distance (KLD), where the corresponding comparison results are presented in the case studies.
- Possible effects of EMTD bringing to smart grids such as transmission power and voltage drop variations are discussed, according to which rationality constraints are thus proposed to avoid the adverse effects. In particular, we analyze the impact of EMTD on locational marginal price (LMP). Then the variation of LMP, the variation of active power loss and the cost of devices for executing EMTD are used as defense cost to design optimal EMTD.
- An EMTD-based ACOPF model with the objective of minimizing cost of EMTD while ensuring sufficient defense effectiveness is proposed. Considering the problem is non-convex and nonlinear, the particle swarm optimization (PSO) algorithm is used to solve the optimal EMTD scheme. Furthermore, the optimal defense time interval for executing EMTD is derived by minimizing the sum of the single defense cost and the estimated adverse effects caused by the forthcoming attack.

The rest of this paper is organized as follows. Section II introduces some preliminaries. Section III designs EMTD and derives the rational constraints. Section IV presents details on the construction of the optimal EMTD scheme. Section V conducts simulations on the standard IEEE test system and Section VI concludes the paper.

II. Preliminaries

A. AC State Estimation and BDD

The AC power system model is used for formulation and analysis in this paper, while most existing analyses on MTD are based on the DC model where reactive power flows and injections, as well as the parallel charging susceptance are ignored.

In smart grids, the processing object of state estimation is a high-dimensional system on a time section, and the least square method is generally adopted. The nonlinear measurement equation of the system can be expressed as

$$\boldsymbol{z} = \boldsymbol{h}(\boldsymbol{x}) + \boldsymbol{e}, \tag{1}$$

where $\boldsymbol{z}$ is the measurement vector; $\boldsymbol{h}(\cdot)$ is the nonlinear measurement equation; $\boldsymbol{x}$ is the state variable composed of the amplitude and phase angle of bus voltage; $\boldsymbol{e}$ is the measurement error. $\boldsymbol{h}(\boldsymbol{x})$ can be expressed as

$$\boldsymbol{h}(\boldsymbol{x}) = \begin{bmatrix} P_{ij} \\ Q_{ij} \\ P_i \\ Q_i \\ U_i \end{bmatrix}, i = 1, 2, \cdots, N; \forall j \in \Omega_i, \tag{2}$$

where P_{ij} is the active power flow from bus i to bus j, Q_{ij} is the reactive power flow from bus i to bus j, P_i is the active power injection of bus i, Q_i is the reactive power injection of bus i, U_i is voltage amplitude of bus i, and Ω_i is the set of buses connected to bus i. Given the measurements in $\boldsymbol{z}$, the result of state estimation is the value $\hat{\boldsymbol{x}}$ that minimizes the following objective function

$$J(\boldsymbol{x}) = [\boldsymbol{z} - \boldsymbol{h}(\boldsymbol{x})]^T \boldsymbol{R}^{-1} [\boldsymbol{z} - \boldsymbol{h}(\boldsymbol{x})], \tag{3}$$

where $\boldsymbol{R}$ is a diagonal matrix whose elements are noise variances of measurements. The first-order optimal condition for this model can be written as [19]:

$$\boldsymbol{H}^T(\hat{\boldsymbol{x}}) \boldsymbol{R}^{-1} [\boldsymbol{z} - \boldsymbol{h}(\hat{\boldsymbol{x}})] = 0, \tag{4}$$

where $\boldsymbol{H}$ is the Jacobian matrix of $\boldsymbol{h}(\boldsymbol{x})$ and details about how to solve the nonlinear equation (4) can be found in [20].

BDD is one of the important functions of state estimation. The system operators use the redundant information provided by SCADA system to judge and process bad data, that is, the following 2-norm estimation residual

$$\begin{aligned} r &= ||\boldsymbol{z} - \boldsymbol{h}(\hat{\boldsymbol{x}})||_2 \\ &= ||\boldsymbol{h}(\boldsymbol{x}) - \boldsymbol{h}(\hat{\boldsymbol{x}}) + \boldsymbol{e}||_2 \end{aligned} \tag{5}$$

with a predefined η are utilized. If $r \geqslant \eta$, the measurements are considered to be contain bad data; otherwise, the measurements are considered to be normal. In general, when the measurement noises follow the normal distribution $N(0, \sigma^2)$, the threshold η can be taken as [10]

$$\eta = \sigma \sqrt{\chi^2_\alpha (m - n)}, \tag{6}$$

where α is the confidence in hypothesis testing, m is the number of measurements used for state estimation and n is the number of system state variables.

B. False Data Injection Attack

FDI attacks generally construct an attack vector $\boldsymbol{a}$ as [21]:

$$\boldsymbol{a} = \boldsymbol{h}(\hat{\boldsymbol{x}} + \boldsymbol{c}) - \boldsymbol{h}(\hat{\boldsymbol{x}}), \tag{7}$$

where $\boldsymbol{c}$ is the injected false data set by the attacker. After attacker launches FDI attacks, the tampered measurement data $\boldsymbol{z}_a$ received by control center is

$$\begin{aligned} \boldsymbol{z}_a &= \boldsymbol{z} + \boldsymbol{a} \\ &= \boldsymbol{z} + \boldsymbol{h}(\hat{\boldsymbol{x}} + \boldsymbol{c}) - \boldsymbol{h}(\hat{\boldsymbol{x}}). \end{aligned} \tag{8}$$

The corresponding residual is

$$\begin{aligned} r_a &= ||\boldsymbol{z}_a - \boldsymbol{h}(\hat{\boldsymbol{x}}_a)||_2 \\ &= ||\boldsymbol{z} + \boldsymbol{h}(\hat{\boldsymbol{x}} + \boldsymbol{c}) - \boldsymbol{h}(\hat{\boldsymbol{x}}) - \boldsymbol{h}(\hat{\boldsymbol{x}}_a)||_2 \\ &= ||\boldsymbol{z} - \boldsymbol{h}(\hat{\boldsymbol{x}})||_2 \\ &= r, \end{aligned} \tag{9}$$

where $\hat{\boldsymbol{x}}_a = \hat{\boldsymbol{x}} + \boldsymbol{c}$ is the false state. From equation (9) it is clear that, the residual r_a under FDI attacks is the same as the residual r without attacks, so the FDI attacks are stealthy and will not trigger the BDD mechanism.

C. Moving Target Defense

After system executes MTD, the topology parameters change, and the measurement equation changes accordingly. Since attackers do not have the latest system topology information and use the old topology information to construct the attack vector. The current state of the system estimated by attackers is

$$\begin{aligned}\hat{\boldsymbol{x}}' &= \arg\min_{\boldsymbol{x}} \quad [\boldsymbol{z}' - \boldsymbol{h}(\boldsymbol{x})]^T \boldsymbol{R}^{-1} [\boldsymbol{z}' - \boldsymbol{h}(\boldsymbol{x})] \\ &= \arg\min_{\boldsymbol{x}} \quad [\boldsymbol{h}'(\boldsymbol{x}') - \boldsymbol{h}(\boldsymbol{x}) + \boldsymbol{e}]^T \boldsymbol{R}^{-1} [\boldsymbol{h}'(\boldsymbol{x}') - \boldsymbol{h}(\boldsymbol{x}) + \boldsymbol{e}],\end{aligned} \tag{10}$$

where $(\cdot)'$ represents the values after executing MTD. Because $\boldsymbol{h}'(\cdot)$ and $\boldsymbol{h}(\cdot)$ are not equal, an error is introduced into $\hat{\boldsymbol{x}}'$ and transmitted to the attack vector. It is worth noting that the current topology parameter of the system is $\boldsymbol{h}'(\cdot)$ while the attacker uses $\boldsymbol{h}(\cdot)$ to construct $\boldsymbol{a}'$, so another error is introduced. These two errors continue to be transmitted to $\boldsymbol{z}'_a = \boldsymbol{z}' + \boldsymbol{h}(\hat{\boldsymbol{x}}' + \boldsymbol{c}) - \boldsymbol{h}(\hat{\boldsymbol{x}}')$ and the resulting residual becomes

$$\begin{aligned} r'_a &= ||\boldsymbol{z}'_a - \boldsymbol{h}'(\hat{\boldsymbol{x}}'_a)||_2 \\ &= ||\boldsymbol{z}' + \boldsymbol{h}(\hat{\boldsymbol{x}}' + \boldsymbol{c}) - \boldsymbol{h}(\hat{\boldsymbol{x}}') - \boldsymbol{h}'(\hat{\boldsymbol{x}}'_a)||_2 .\end{aligned} \tag{11}$$

It is obvious that the introduced errors can lead to the residual r'_a greater than r, therefore the system may be able to detect an attack by executing MTD.

III. Extended Moving Target Defense

In this section, based on the defense principle of MTD for AC state estimation, a more flexible and powerful MTD scheme—EMTD is proposed. Further, the possible effects of EMTD on smart grids are discussed and the rationality constraints are proposed to avoid the adverse effects.

A. Extended MTD for AC State Estimation

In this paper, we suppose all transmission lines and transformers are modeled with a standard π transmission line model, with series impedance $\mathcal{R} + j\mathcal{X}$ and parallel charging susceptance $\mathcal{B}_c$. In order to be consistent with idiomatic usage, we sometimes use admittance $\mathcal{G} + j\mathcal{B} = 1/(\mathcal{R} + j\mathcal{X})$ rather than series impedance $\mathcal{B}$ (is the series susceptance), e.g., in power flow equations.

Since most existing researches only use D-FACTS devices to change the series reactance $\mathcal{X}$ of transmission lines to realize MTD and rely on DC state estimation, the following EMTD is proposed to improve TMTD.

Definition 1. EMTD coordinately changes the series reactance $\mathcal{X}$ and parallel susceptance $\mathcal{B}_c$ of transmission lines.

Proposition 1. The defense effectiveness of EMTD to resist FDI attacks can be stronger than that of TMTD.

Proof: The items in $\boldsymbol{h}(\boldsymbol{x})$ are expressed as

$$\begin{aligned} &P_{ij} = U_i^2 \mathcal{G}_{ij} - U_i U_j (\mathcal{G}_{ij} \cos\theta_{ij} + \mathcal{B}_{ij} \sin\theta_{ij}), \\ &Q_{ij} = U_i U_j (\mathcal{B}_{ij} \cos\theta_{ij} - \mathcal{G}_{ij} \sin\theta_{ij}) - U_i^2 (\mathcal{B}_{ij} + \mathcal{B}_{ijc}), \\ &P_i = \sum_{j \in \Omega_i} P_{ij}, \\ &Q_i = \sum_{j \in \Omega_i} Q_{ij}, \\ &U_i = U_i. \end{aligned} \tag{12}$$

In view of $\mathcal{G} + j\mathcal{B} = 1/(\mathcal{R} + j\mathcal{X})$, the change of $\mathcal{X}_{ij}$ will lead to the change of $\mathcal{G}_{ij}$ and $\mathcal{B}_{ij}$. According to formula (12), the items in $\boldsymbol{h}'(\boldsymbol{x})$ after system executes TMTD are expressed as

$$\begin{aligned} &P'_{ij} = U_i^2 \mathcal{G}'_{ij} - U_i U_j (\mathcal{G}'_{ij} \cos\theta_{ij} + \mathcal{B}'_{ij} \sin\theta_{ij}), \\ &Q'_{ij} = U_i U_j (\mathcal{B}'_{ij} \cos\theta_{ij} - \mathcal{G}'_{ij} \sin\theta_{ij}) - U_i^2 (\mathcal{B}'_{ij} + \mathcal{B}_{ijc}), \\ &P'_i = \sum_{j \in \Omega_i} P'_{ij}, \\ &Q'_i = \sum_{j \in \Omega_i} Q'_{ij}, \\ &U'_i = U_i, \end{aligned} \tag{13}$$

while the items in $\boldsymbol{h}'(\boldsymbol{x})$ after system executes EMTD are expressed as

$$\begin{aligned} &P'_{ij} = U_i^2 \mathcal{G}'_{ij} - U_i U_j (\mathcal{G}'_{ij} \cos\theta_{ij} + \mathcal{B}'_{ij} \sin\theta_{ij}), \\ &Q'_{ij} = U_i U_j (\mathcal{B}'_{ij} \cos\theta_{ij} - \mathcal{G}'_{ij} \sin\theta_{ij}) - U_i^2 (\mathcal{B}'_{ij} + {\mathcal{B}_{ijc}}'), \\ &P'_i = \sum_{j \in \Omega_i} P'_{ij}, \\ &Q'_i = \sum_{j \in \Omega_i} Q'_{ij}, \\ &U'_i = U_i. \end{aligned} \tag{14}$$

According to formula (12)-(14), the difference between the measurement variation $|\boldsymbol{h}(\cdot) - \boldsymbol{h}'(\cdot)|$ is introduced by Q'_{ij} and Q'_i. As $Q'_i = \sum_{j \in \Omega_i} Q'_{ij}$, we thus focus on Q'_{ij}. In high voltage transmission systems, the voltage amplitude difference at both ends of a line and the phase angle are small, i.e., $\cos\theta_{ij} \approx 1$ and $\sin\theta_{ij} \approx 0$. Then Q'_{ij} after executing EMTD is

$$Q'_{ij} \approx U_i U_j \mathcal{B}'_{ij} - U_i^2 (\mathcal{B}'_{ij} + {\mathcal{B}_{ijc}}'), \tag{15}$$

and Q'_{ij} after executing TMTD is

$$Q'_{ij} \approx U_i U_j \mathcal{B}'_{ij} - U_i^2 (\mathcal{B}'_{ij} + \mathcal{B}_{ijc}). \tag{16}$$

As

$$Q_{ij} \approx U_i U_j \mathcal{B}_{ij} - U_i^2 (\mathcal{B}_{ij} + \mathcal{B}_{ijc}), \tag{17}$$

then $|Q_{ij} - Q'_{ij}|$ after executing EMTD is

$$\begin{aligned} |Q_{ij} - Q'_{ij}| \approx & |U_i U_j (\mathcal{B}_{ij} - \mathcal{B}'_{ij}) - U_i^2 (\mathcal{B}_{ij} - \mathcal{B}'_{ij}) \\ & - U_i^2 (\mathcal{B}_{ijc} - \mathcal{B}'_{ijc})|, \end{aligned} \tag{18}$$

and $|Q_{ij} - Q'_{ij}|$ after executing TMTD is

$$|Q_{ij} - Q'_{ij}| \approx |U_i U_j (\mathcal{B}_{ij} - \mathcal{B}'_{ij}) - U_i^2 (\mathcal{B}_{ij} - \mathcal{B}'_{ij})|. \tag{19}$$

It is clear that EMTD has one more controllable item $-U_i^2(\mathcal{B}_{ijc}-\mathcal{B}'_{ijc})$ in $|Q_{ij}-Q'_{ij}|$ compared with TMTD. When

$$U_i^2(\mathcal{B}_{ijc}-\mathcal{B}'_{ijc})\times[U_iU_j(\mathcal{B}_{ij}-\mathcal{B}'_{ij})-U_i^2(\mathcal{B}_{ij}-\mathcal{B}'_{ij})]<0, \tag{20}$$

the changes of $\mathcal{B}_{ijc}$ will increase the changes on Q_{ij}, causing possible increases for $|\boldsymbol{h}(\cdot)-\boldsymbol{h}'(\cdot)|$.

Noting (11), it is indicated the residual of state estimation of EMTD can be larger than that of TMTD. That is, for the same attack and defense magnitude, the possibility that EMTD detects the attack can be greater. In other words, EMTD can further increase the state estimation residual by improving flexibility and controllability of system defense compared with TMTD, thereby reducing missed detection. ■

In essence, EMTD introduces more degrees of freedom and its search space completely includes TMTD, i.e., TMTD is a special case of EMTD. Under the constrains in Subsection III-C, EMTD can do much more than TMTD, which will be shown in Section V. Whether an attack can be detected heavily depends on what the attack scheme $\hat{\boldsymbol{x}}_a$ is, which is uncontrollable for defenders. What defenders can do is to increase the possibility of detecting malicious attacks, and that is the motivation for proposing EMTD. The attack detection probability of TMTD and EMTD are presented in subsection V-A, which shows EMTD is much more powerful.

Besides state estimation residual, KLD of system measurement variation is also used to detect FDI attacks in AC state estimation by measuring the distribution inconsistency [22]. Specifically, for distribution of measurement variation $q(\boldsymbol{x})$ from the historical data and distribution of measurement variation $p(\boldsymbol{x})$ between the current time step and the previous time step, the KLD is defined as

$$D(p||q)=\sum_{\boldsymbol{x}}p(\boldsymbol{x})\ln\frac{p(\boldsymbol{x})}{q(\boldsymbol{x})}. \tag{21}$$

Noting (1) that $\boldsymbol{h}(\boldsymbol{x})$ and $\boldsymbol{h}'(\boldsymbol{x})$ are directly related to distribution of measurement variation $p(\boldsymbol{x})$. Therefore, after executing MTD, if the attacker uses the old topology information to construct attack vector $\boldsymbol{a}$, the KLD may be significantly larger than that without executing MTD and EMTD can be more effective than TMTD.

According to capabilities of the compensation equipment in smart grids, we give the realization instructions of EMTD in transmission networks, where the system operator can regulate the series reactance $\mathcal{X}$ and parallel susceptance $\mathcal{B}_c$ of lines simultaneously to execute EMTD. Specifically, flexible AC transmission system (FACTS) devices such as thyristor switched capacitors (TSC) and thyristor controlled reactors (TCR) deployed in important substations are used to regulate the parallel susceptance $\mathcal{B}_c$ of lines. D-FACTS devices such as small-capacity distributed static serial compensators (DSSC) deployed on lines are used to regulate the series reactance $\mathcal{X}$. The parameters of transmission lines and the implementation of EMTD are shown in Fig.1.

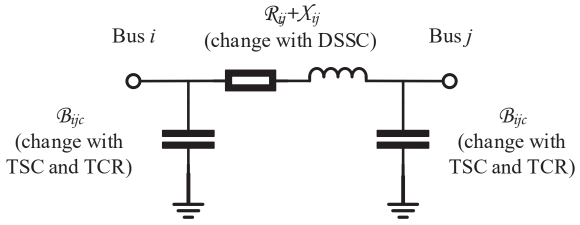

$\mathcal{R}_{ij}+\mathcal{X}_{ij}$
(change with DSSC)
Bus i
Bus j
$\mathcal{B}_{ijc}$
(change with TSC and TCR)
$\mathcal{B}_{ijc}$
(change with TSC and TCR)

Fig. 1. The parameters of transmission lines and the implementation of EMTD

B. Possible Effects Induced by Executing EMTD

EMTD detects FDI attacks by changing topological parameters $\mathcal{X}$ and $\mathcal{B}_c$ of the system, which may cause adverse effects to the system. This subsection analyzes possible adverse effects, where we take the increase of $\mathcal{X}$ and the decrease of $\mathcal{B}_c$ for examples.

First, we analyze the effects caused by the increase of $\mathcal{X}$, e.g., the increase in voltage drop of some lines.

- During electric energy flows from the generator to the load, the voltage drop across a line is [23]

$$\Delta U=\frac{P_d\mathcal{R}+(Q_d-Q_C)\mathcal{X}}{U}, \tag{22}$$

where P_d is active power demand of the load, Q_d is reactive power demand of the load, Q_C is the inductive reactive power emitted by the equivalent charging capacitor C at ends of the line. After executing EMTD, if the line series reactance $\mathcal{X}$ increases, it will cause the line voltage drop to increase

$$\Delta U_{\mathcal{X}}=\frac{(Q_d-Q_C)\times\Delta\mathcal{X}}{U}=\Delta\frac{(Q_d-Q_C)\mathcal{X}}{U}. \tag{23}$$

Next, we analyze the effects caused by the decrease of $\mathcal{B}_c$, e.g., the increase in transmission power and voltage drop of some lines.

- Equipment such as transformers and induction motors consume inductive reactive power, which is sent from generators and substations equipped with reactive power compensation devices and flows through the lines. As $\mathcal{B}_c=\omega C$ and ω is the angular frequency, the equivalent charging capacitor C will change when system executes EMTD. As $Q_C=\omega CU^2$, a decrease in C will leads to a decrease in Q_C. At this time, generators need to send out more reactive power, i.e., $\Delta Q=\omega\times\Delta C\times U^2$, where ΔC is the reduction of capacitance C. And the extra reactive power ΔQ will flow through the lines, i.e., leading to a increase in transmission power of some lines.
- If the capacitance C is reduced, transmission lines will deliver extra reactive power to the load, which will further cause the line voltage drop to increase as

$$\Delta U_C=\omega\times\Delta C\times U\times\mathcal{X}=\Delta\frac{Q_C\mathcal{X}}{U}. \tag{24}$$

Since Quantity Breeds Quality, when the changes of $\mathcal{X}$ and $\mathcal{B}_c$ are large enough, the voltage drop across the line will affect the power quality. Take rated voltage as U_0. In smart grids, the normal operating range of bus voltage is generally $[0.95U_0, 1.05U_0]$. According to formula (23) and (24), if the increase of $\mathscr{X}$ satisfies $\Delta\mathscr{X} > 0.05U_0^2/(Q_d - Q_C)$ or the decrease of $\mathscr{B}_c$ satisfies $\Delta\mathscr{B}_c > 0.05/\mathscr{X}$, the line voltage drop will increase by 5%. And the voltage of the bus at the end may less than $0.95U_0$, which can destroy the normal operation of smart grids or even cause accidents. Therefore, defenders must avoid to cause these negative effects and the corresponding constraints on rational EMTD are presented in the next subsection.

C. Rational EMTD and Its Properties

In order to avoid the adverse effects mentioned above as well as not yet mentioned, this subsection defines the rational EMTD and presents the corresponding rationality constraints.

Definition 2. A rational EMTD scheme ensures smart grids operate normally after it is executed.

The Definition 2 means that after executing EMTD, smart grids should keep important physical quantities unchanged and satisfy all system operation constraints under new topological parameters:

- In order to ensure the power quality, the voltage amplitude of PV buses and the slack bus should be maintained, and the voltage amplitude of other buses should be kept near the rated value, e.g., [$0.95U_0$, $1.05U_0$].
- In order to ensure system safety, safety constraints such as the bounds on line transmission power and generator output have to be satisfied.

Consider a smart grid with N buses and L lines, among which M buses are PQ buses, $N - M - 1$ buses are PV buses and the remaining bus is a slack bus. It is inferred that the rational EMTD has $2N - 1$ equality constraints for power balance equation and the detailed expressions of the constraints in polar coordinates are

$$\begin{aligned}
p_{gi} - p_{di} &= U_i \sum_{j\in\Omega_i} U_j(\mathscr{G}_{ij}\cos\theta_{ij} + \mathscr{B}_{ij}\sin\theta_{ij}) \\
&= U_i' \sum_{j\in\Omega_i} U_j'(\mathscr{G}_{ij}'\cos\theta_{ij}' + \mathscr{G}_{ij}'\sin\theta_{ij}'), \\
&\qquad\qquad i \in \text{PQ buses} \cup \text{PV buses} \\
q_{gi} - q_{di} &= U_i \sum_{j\in\Omega_i} U_j(\mathscr{G}_{ij}'\sin\theta_{ij} - \mathscr{B}_{ij}'\cos\theta_{ij}) \\
&= U_i' \sum_{j\in\Omega_i} U_j'(\mathscr{G}_{ij}'\sin\theta_{ij}' - \mathscr{B}_{ij}'\cos\theta_{ij}'), \\
&\qquad\qquad i \in \text{PQ buses} \\
U_i &= U_i', i \in \text{PV buses} \cup \text{slack bus},
\end{aligned} \tag{25}$$

where p_{gi}, q_{gi} represent the active and reactive power output of generator at bus i, and p_{di}, q_{di} represents the active and reactive power demand at bus i. It is noted that there are $2L + N + M - 1$ unknowns in the rationality problem, that is, $2L$ adjustable topological parameters of EMTD, which are the series reactance $\mathscr{X}$ and parallel susceptances $\mathscr{B}_c$ of L lines; and $N + M - 1$ unknowns in state variables of the system, which are voltage phase angles of $N - 1$ buses except for the slack bus and voltage amplitude of M PQ buses.

In most smart grids, each bus is connected to at least one line, so a smart grid with N buses has at least $N - 1$ lines, i.e., $L \geqslant N - 1$. Therefore, the number of unknowns $2L + N + M - 1$ is bigger than the number of equality constraints $2N - 1$, which means the rationality problem is under-determined and must have multiple solutions without considering the inequality constraints. The expressions of inequality constraints are

$$h_{kf} \leqslant Limit_k,\ k = 1, 2, \cdots, L \tag{26}$$

$$h_{kt} \leqslant Limit_k,\ k = 1, 2, \cdots, L \tag{27}$$

$$U_i^{\min} \leqslant U_i \leqslant U_i^{\max},\ i = 1, 2, \cdots, N \tag{28}$$

$$p_{gi}^{\min} \leqslant p_{gi} \leqslant p_{gi}^{\max},\ i = 1, 2, \cdots, N \tag{29}$$

$$q_{gi}^{\min} \leqslant q_{gi} \leqslant q_{gi}^{\max},\ i = 1, 2, \cdots, N, \tag{30}$$

where formula (26)-(30) are bounds on the power h_{kf} transmitted at the beginning of line k, the power h_{kt} transmitted at the end of line k, the voltage amplitude U_i of bus i, the active output p_{gi} of the generator at bus i, and reactive output q_{gi} of the generator at bus i, respectively.

The defender can test whether an EMTD scheme is rational by Algorithm 1, and the selection of the optimal defense scheme is discussed in Section IV.

Algorithm 1 Rationality Verification for EMTD

```
Input: topology and topology parameters $\mathscr{X}$, $\mathscr{B}_c$ of system
    after executing EMTD; measured values with noises,
    including power injections $P_i$ of PQ and PV buses, $Q_i$
    of PQ buses and voltage magnitude $U_i$ of PV and slack
    buses
Output: True or False
construct the node admittance matrix $\boldsymbol{Y}'$ with $\mathscr{X}$, $\mathscr{B}_c$ and
    topology of the system;
use $P_i$ of PQ and PV buses, $Q_i$ of PQ buses, $U_i$ of PV
    and slack buses and $\boldsymbol{Y}'$ to calculate AC power flow;
get the physical quantities at this operating point of
    system: power flow $h_{kf}$, $h_{kt}$, voltage magnitude $U_i$, active
    and reactive output of generator $p_{gi}$, $q_{gi}$
substitute the physical quantities into the inequality con-
    straints (26)-(30);
if all inequality constraints are satisfied then
    return True;
else
    return False;
end if
```

IV. Construction of Optimal EMTD

In this section, the impact of EMTD on the electricity market is analyzed and treated as part of the cost of EMTD. Considering the defense cost and effectiveness of EMTD comprehensively, an optimal problem is established for solving cost-minimization EMTD topology parameters and defense time interval while ensuring sufficient defense effectiveness.

A. Impact of EMTD on Electricity Market

In deregulated electricity markets, FDI attacks may lead to financial improprieties by making a false virtual bidding [24]. Powerful attacks not only bypassing bad data detection in the state estimation but also disguising the compromised LMP as regular LMP to avoid market operators' alerts [25]. With MTD, the defender can effectively detect FDI attacks, thus preventing these economic crimes.

This paper considers the day-ahead electricity market [26] where LMP is widely adopted. For ACOPF-based LMP in [27], a general model for the ACOPF has the form

$$\min_{p_{gi},q_{gi},U_{gi}} \ f_{ac}(p_{gi},q_{gi},U_{gi};p_{di},q_{di},\mathcal{C}) \tag{31}$$

$$s.t. \quad p_{gi}-p_{di}-h_{Pi}(p_{gi},q_{gi},U_{gi};p_{di},q_{di},\mathcal{C})=0 \quad i=1,2,\cdots,N \tag{32}$$

$$q_{gi}-q_{di}-h_{Qi}(p_{gi},q_{gi},U_{gi};p_{di},q_{di},\mathcal{C})=0 \quad i=1,2,\cdots,N \tag{33}$$

$$(26)-(30), \tag{34}$$

where U_{gi} is the voltage amplitude of generator at bus i, $\mathcal{C}$ is the production cost of electricity; $f_{ac}(p_{gi},q_{gi},U_{gi};p_{di},q_{di},\mathcal{C})$ represents total generation cost, $h_{Pi}(\cdot)$ is the active power injection of bus i while $h_{Qi}(\cdot)$ is the reactive power injection, and (32) and (33) are the corresponding constraints. The LMP of each node is the Lagrange multiplier λ_i of the equality constraint (32) (see (35) and (36)).

$$\left.\begin{array}{r} \psi = f_{ac}(p_{gi},q_{gi},U_{gi};p_{di},q_{di},\mathcal{C}) - \sum\limits_{i=1}^{N}\lambda_i \\ \times\big(p_{gi}-p_{di}-h_{Pi}(p_{gi},q_{gi},U_{gi};p_{di},q_{di},\mathcal{C})\big) \\ \dfrac{\partial\psi}{\partial p_{gi}}=0 \\ \dfrac{\partial\psi}{\partial q_{gi}}=0 \\ \dfrac{\partial\psi}{\partial U_{gi}}=0 \end{array}\right\} \Rightarrow \text{LMP}, \tag{35}$$

$$\left.\begin{array}{r} \psi' = f_{ac}(p'_{gi},q'_{gi},U'_{gi};p'_{di},q'_{di},\mathcal{C}') - \sum\limits_{i=1}^{N}\lambda'_i \\ \times\big(p'_{gi}-p'_{di}-h'_{Pi}(p'_{gi},q'_{gi},U'_{gi};p'_{di},q'_{di},\mathcal{C}')\big) \\ \dfrac{\partial\psi'}{\partial p'_{gi}}=0 \\ \dfrac{\partial\psi'}{\partial q'_{gi}}=0 \\ \dfrac{\partial\psi'}{\partial U'_{gi}}=0 \end{array}\right\} \Rightarrow \text{LMP}', \tag{36}$$

where ψ is generalized Lagrange function, $(\cdot)'$ represents the value after executing EMTD.

After executing EMTD, the series reactance $\mathcal{X}$ and parallel susceptance $\mathcal{B}_c$ of the line will change. The coefficients of power injection equations (32) of the buses with FACTS devices or connected to the lines with D-FACTS devices will change accordingly. As a result, the LMP of each node will also change as (35) to (36). Variations in LMP caused by executing EMTD will directly affect transactions in the electricity market, and we will show the specific impact in section V-B.

B. Cost of system defense

According to the analysis in Section IV-A, the LMP of each node will change after executing EMTD, and these changes will affect the operation of electricity market. In order to protect the interests of the buyer and the seller in electricity markets, MTD is expected to affect LMP as weakly as possible. Therefore, this paper regards the change of LMP as indirect economic cost of system defense. And the metric to measure the impact of MTD on LMP is defined as the sum of the absolute values of LMP changes of all buses before and after system executing MTD.

$$\Delta LMP = \sum_{i=1}^{N} \left|\Delta LMP_i\right|, \tag{37}$$

where ΔLMP_i is the LMP variation of node i before and after executing EMTD.

In addition, this paper regards the change of active power loss and equipment adjustment costs as direct economic costs of system defense. The overall active power loss is

$$P_{loss} = \sum_{k=1}^{L} [(U_i^2+U_j^2)\mathcal{G}_k - 2U_iU_j\mathcal{G}_k\cos\theta_{ij}], \tag{38}$$

where $\mathcal{G}_k$ is the equivalent series conductance of line k. After system executes EMTD, series reactance $\mathcal{X}_k$ will change, which means $\mathcal{G}_k$ will change accordingly. Therefore, the system operator can reduce active power loss while defending, i.e., performing operating mode optimization. The variation of the active power loss is

$$\Delta P_{loss} = P'_{loss} - P_{loss}, \tag{39}$$

where P_{loss} and P'_{loss} are the active power loss before and after executing EMTD, respectively.

An EMTD regulates topological parameters by FACTS and D-FACTS devices, and the price of common FACTS devices is generally a quadratic function of their rated capacity [28]. Therefore, considering the loss of devices when using them, this paper uses the quadratic function of parameter variations to describe economic cost of using devices, that is,

$$Cost_{eq} = e_1\Delta\mathcal{X}^2 + e_2\Delta\mathcal{B}_c^2, \tag{40}$$

where e_1 and e_2 are the cost coefficients.

C. Construction of Cost-minimization EMTD Scheme

Attack detection capability is always the most important characteristic for EMTD. When constructing the cost-minimization EMTD scheme, its defense capability must be ensured. In this paper, the

$attack\ detection\ probability(ADP)$ is used as quantitative metric of defense capability of MTD/EMTD [10].

$$ADP = \frac{number\ of\ attcks\ being\ detected}{number\ of\ all\ attacks} \tag{41}$$

As the lower bound of attack detection capability of EMTD, the optimal scheme should satisfy $ADP \geqslant \alpha$, where α is the confidence in formula (6).

Considering the defense cost and defense effect comprehensively, an EMTD-based ACOPF model is proposed to construct the cost-minimization EMTD scheme, in which the series reactance $\mathcal{X}$ and parallel susceptance $\mathcal{B}_c$ of lines are introduced as decision variables. The EMTD-based ACOPF model with the objective of minimizing the total cost while ensuring sufficient defense effectiveness is formulated as

$$\min_{\mathcal{X}_k, \mathcal{B}_{ck}, p_{gi}, q_{gi}} \quad \Delta LMP + l\Delta P_{loss} + Cost_{eq} \tag{42}$$

$$s.t. \qquad ADP \geqslant \alpha \tag{43}$$

$$\mathcal{X}_k^{\min} \leqslant \mathcal{X}_k \leqslant \mathcal{X}_k^{\max}, k = 1, 2, \cdots, L \tag{44}$$

$$\mathcal{B}_{ck}^{\min} \leqslant \mathcal{B}_{ck} \leqslant \mathcal{B}_{ck}^{\max}, k = 1, 2, \cdots, L \tag{45}$$

$$(25) - (30), \tag{46}$$

where decision variable $\mathcal{X}_k$ is the series reactance and $\mathcal{B}_{ck}$ is the parallel susceptance of the k-th line, respectively. l is a regulation coefficient for active power loss. The inequality constraint (43) enforces sufficient effectiveness to defend against FDI attacks, i.e., guarantees the ADP is greater than the confidence α in formula (6), where (43) can also be written as $\mathrm{P}(r_a'(\mathcal{X}_k, \mathcal{B}_{ck}, p_{gi}, q_{gi}) \geqslant \eta) \geqslant \alpha$ here. Inequality constraints (44) and (45) are bounds on physical capacity of FACTS/D-FACTS devices.

Since objective function (42) and constraints (43), (46) are non-convex and nonlinear, it is difficult to solve the above optimal problem. Meanwhile, there are lots of attack-defense simulations for each point, where the gradient of objective function is not available. Thus, the traditional solvers are not suitable for this problem and we turn to artificial computational methods. In this paper, the PSO algorithm is utilized to solve the optimal problem. Define the fitness function as

$$\begin{aligned}
&\phi(\mathcal{X}_k, \mathcal{B}_{ck}, p_{gi}, q_{gi}) \\
=&\Delta LMP + l\Delta P_{loss} + Cost_{eq} \\
&+ \zeta_1 max(0, \alpha - \mathrm{P}(r_a'(\mathcal{X}_k, \mathcal{B}_{ck}, p_{gi}, q_{gi}) \geqslant \eta)) \\
&+ \zeta_2 \sum_{k=1}^{L} max(0, h_{kf}(\mathcal{X}_k, \mathcal{B}_{ck}, p_{gi}, q_{gi}) - Limit_k) \\
&+ \zeta_2 \sum_{k=1}^{L} max(0, h_{kt}(\mathcal{X}_k, \mathcal{B}_{ck}, p_{gi}, q_{gi}) - Limit_k) \\
&+ \zeta_3 \sum_{i=1}^{N} [max(0, U_i - U_i^{\max}) + max(0, U_i^{\min} - U_i)] \\
&+ \zeta_4 \sum_{g=1}^{G} [max(0, p_{gi} - p_{gi}^{\max}) + max(0, p_{gi}^{\min} - p_{gi})] \\
&+ \zeta_5 \sum_{g=1}^{G} [max(0, q_{gi} - q_{gi}^{\max}) + max(0, q_{gi}^{\min} - q_{gi})] \\
&+ \zeta_6 \sum_{k=1}^{L} [max(0, \mathcal{X}_k - \mathcal{X}_k^{\max}) + max(0, \mathcal{X}_k^{\min} - \mathcal{X}_k)] \\
&+ \zeta_7 \sum_{k=1}^{L} [max(0, \mathcal{B}_{ck} - \mathcal{B}_{ck}^{\max}) + max(0, \mathcal{B}_{ck}^{\min} - \mathcal{B}_{ck})],
\end{aligned} \tag{47}$$

where $\zeta_1 \sim \zeta_7$ are non-negative penalty coefficients. The value of fitness function is the basis for determining the best global position and the best personal position of each particle. The solution of (47) is the cost-minimization EMTD topology parameters.

D. Optimization of The Defense Time Interval

It is obvious that the smaller the time interval between two defenses, the shorter the average attack duration, and the higher the total cost of smart grids. In order to balance the defense cost and effect, this subsection seeks the optimal defense time interval according to economic cost of a single defense and economic loss that a FDI attack is expected to impose on smart grids.

The cost of a single defense has been analyzed in section IV-B. In what follows, we analyze the economic losses that a FDI attack is expected to impose on smart grids. In general, the longer the FDI attack duration, the greater economic loss smart grids will suffer. Because defender cannot foresee when FDI attacks will be launched, this paper uses the average attack duration instead.

1) The average attack duration: An alert attacker can find the execution of EMTD and stop the attack [10]. After reacquiring new topology information and subjectively waiting for a period of time, the attacker will launch an attack again. Take the last time the defender executed EMTD and successfully detected FDI attacks as starting time $t_0 = 0$. Assume each EMTD is effective and the attacker will launch attacks again at t_a with $t_a \sim U(0, T_{amax})$, where T_{amax} can be obtained based on long-term observation of attackers' behaviors. Taking the defender's defense time interval as t_d, the average attack duration can be calculated as

- If $t_d \geqslant T_{amax}$, EMTD must be able to detect the attack during $[0, t_d]$, and the average time system $\overline{T}$ affected by a FDI attack is

$$\begin{aligned}
\overline{T} &= \mathbb{E}_{t_a}[t_d - t_a] \\
&= t_d - \frac{T_{amax}}{2}.
\end{aligned} \tag{48}$$

- If $t_d < T_{amax}$, EMTD may not detect the attack during $[0, t_d]$. When $T_{amax}/2 \leqslant t_d \leqslant T_{amax}$, the attack may be detected by the current EMTD or the next one. Therefore,

$$\begin{aligned}
\overline{T} =& \mathbb{E}_{t_a}[t_d - t_a | 0 < t_a < t_d] \\
&+ \mathbb{E}_{t_a}[2t_d - t_a | t_d < t_a < T_{amax}] \\
=& 2t_d - \frac{t_d^2}{T_{amax}} - 0.5T_{amax}.
\end{aligned} \tag{49}$$

Similarly, when $T_{amax}/(n+1) \leqslant t_d \leqslant T_{amax}/n$ for any $n \geqslant 1$,

$$\overline{T} = (1+n)t_d - \frac{n(n+1)t_d^2}{2T_{amax}} - 0.5T_{amax}. \qquad (50)$$

2) Estimate of the adverse effects caused by the forthcoming attack: The defender is capable of identifying specific attack plan, e.g., through reactance perturbation [29]. After a defender gets previous attack plan, he/she can evaluate adverse effects accordingly. For the sake of generality, this paper uses the false data $\boldsymbol{c}$ injected by attackers to measure the adverse effects. Specifically, the larger the injected false data $\boldsymbol{c}$, the more false system state $\boldsymbol{x}_a$ deviates from the real state and the more serious consequences attacker may bring to smart grids. The behavior pattern of the same attacker usually has certain rules, hence the average effects of multiple attacks are used to estimate the adverse effect caused by FDI attacks. The estimated value of the adverse effect is

$$f_{ae}(\overline{T}, c_{sum}) = f_{ae}(\overline{T}, \sum_{j=1}^{W}(\sum_{i=1}^{2N-1} \beta_i \times c_{ij})), \qquad (51)$$

where W is the window size of historical attack times used to estimate the effect of the forthcoming attack, β_i is the weight coefficient used to measure the importance of i-th state variable and c_{ij} is the false data injected into i-th state variable in the j-th attack.

3) Optimization of defense time interval: According to the economic cost of a single defense and the estimated adverse effect of the forthcoming attack, the following objective function is used for the optimization of defense time interval

$$\min_{t_d} \ \mu_1 \frac{cost_{\text{EMTD}}}{t_d} + \mu_2 \frac{f_{ae}(\overline{T}, c_{sum})}{t_d} \qquad (52)$$

$$s.t. \quad T_{dmin} \leqslant t_d \leqslant T_{dmax}, \qquad (53)$$

where $cost_{\text{EMTD}}$ is the solution of objective function (42) in section IV-C, T_{dmin} is the minimum defense time interval that determined by functional recovery period of devices; T_{dmax} is the maximum defense time interval. The objective function (52) represents the total attack effects and defense cost of smart grids per unit time, and the solution is the time for next execution of EMTD, i.e., the optimal defense time interval t_d^*.

The construction of optimal EMTD is described as Algorithm 2.

Algorithm 2 Construction of optimal EMTD

```
Input: topology and topology parameters $\mathscr{X}$, $\mathscr{B}_c$; measured
    values with noises, including power injections $P_i$ of PQ
    and PV buses, $Q_i$ of PQ buses and voltage magnitude $U_i$
    of PV and slack buses; $LMP$ of all buses; coefficients
    $m_i$, $i = 1, 2, \cdots, N$; $l$; $e_1$, $e_2$; $\zeta_l$, $l = 1, 2, \cdots, 7$
Output: optimal EMTD parameters $\mathscr{X}^*$, $\mathscr{B}_c^*$ and defense time
    interval $t_d^*$
 1: use $P_i$, $Q_i$, $U_i$, $\mathscr{X}$, $\mathscr{B}_c$ and topology of the system to
    calculate AC power flow and get $P_{loss}$;
 2: solve the optimal problem in (47) using PSO algorithm
    and get $\mathscr{X}^*$, $\mathscr{B}_c^*$;
 3: do Detection Effectiveness Verification for EMTD according to formula (43) and get the result $flag1$;
 4: if $flag1$ == False then
 5:     increase $\zeta_1$ and go back to step 2;
 6: end if
 7: do Rationality Verification for EMTD according to Algorithm (1) and get the result $flag2$;
 8: if $flag2$ == False then
 9:     increase $\zeta_2$-$\zeta_7$ and go back to step 2;
10: end if
11: optimize defense time interval according to formula (52),
    (53) and get $t_d^*$;
12: output $\mathscr{X}^*$, $\mathscr{B}_c^*$ and $t_d^*$.
```

V. Case Studies

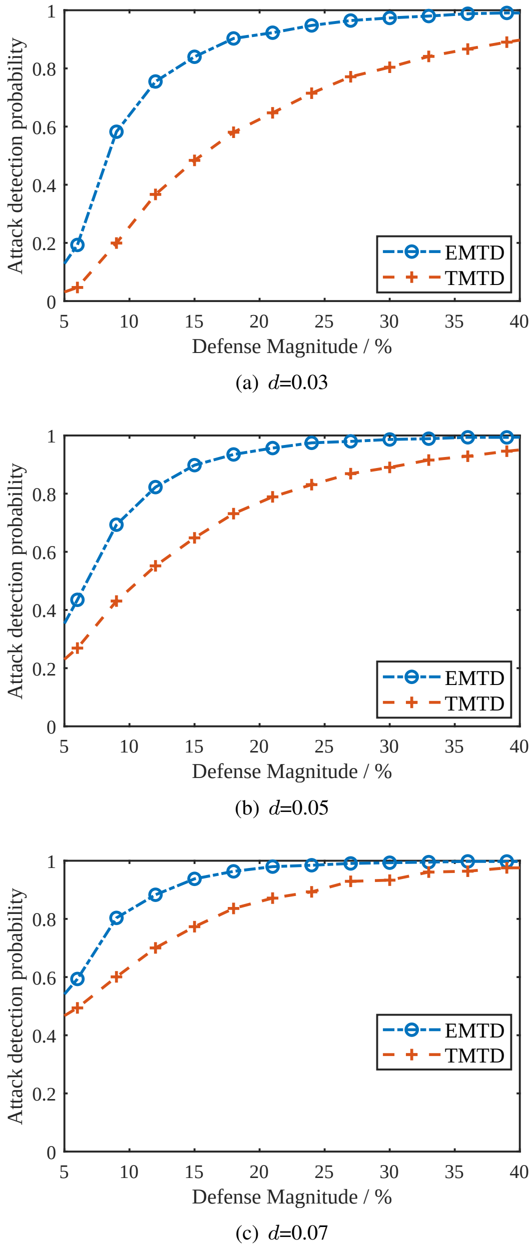
In this section, the case studies conducted on the IEEE 9-bus system in MATPOWER [30] are provided to demonstrate the proposed method.

A. Effectiveness Comparison of EMTD and TMTD

This subsection evaluates the effectiveness of EMTD and compares it with that of the TMTD, where the ADP, the average estimation residual and KLD are used as evaluation metrics.

For a defense magnitude q_m, set $\mathscr{X}_k^{max} = (1+q_m)\mathscr{X}_k$, $\mathscr{B}_{ck}^{max} = (1+2.5q_m)\mathscr{B}_{ck}$, ${\mathscr{X}_k}^{min} = (1-q_m)\mathscr{X}_k$, and $\mathscr{B}_{ck}^{min} = (1-2.5q_m)\mathscr{B}_{ck}$. In practice, 20% is a typical setting for q_m, 70% is achievable [31] and a larger regulation range requires stronger parameter changing capabilities accordingly. Therefore, we vary q_m from 5% to 40%. The measurement errors are sampled from the normal distribution $N(0, \sigma^2)$ with $\sigma = 0.01$. We construct the attack as follows: choose a vector $\boldsymbol{c}$ and then compute the false states $\boldsymbol{x}_a = \boldsymbol{x} + \boldsymbol{c}$ and false measurements $\boldsymbol{h}(\boldsymbol{x}_a)$. The $\boldsymbol{c}$'s elements are sampled from the uniform distribution $U(-\frac{d}{2}, \frac{d}{2})$, where d characterizes the magnitude of attack. It is easy for defenders to detect sudden and large changes in measurements. In order not to alert the defender, the attacker may gradually increase the attack magnitude from a small value until the target is reached. In the simulation, we set $d = 0.02,\ 0.05,\ 0.10$, which represent all stages of the attack process. Confidence α=0.95, m=45, n=17. For each defense magnitude, 4000 random multi-bus attacks and defenses are tested.

Fig.2 shows the ADP of EMTD and TMTD under different defense magnitudes in IEEE 9-bus, from which it is clear that EMTD performs better than TMTD in most cases. In addition, it is observed that the detection effectiveness of EMTD and TMTD increases along with the defense magnitude. The farther the false state $\boldsymbol{x}_a$ deviates from the real state, the more likely it is to be detected by EMTD and TMTD. The performance of MTD to detect FDI attacks mainly depends on whether it can distinguish real attacks from noise. The bad scenario of TMTD is when the attack and noise are particularly similar, i.e., $d = 0.02,\ 0.05$, and EMTD performs better at this time. This means that EMTD can detect attacks earlier than TMTD. Fig.3 shows the average estimation residual $\overline{r}$ under different defense magnitudes. When the system doesn't execute MTD, the system average residual $\overline{r}$ under attack is very small. As analyzed in section III-A, after executing EMTD or TMTD, the system residual $\overline{r}$ will significant increase. Besides, the $\overline{r}$ for EMTD is obviously greater that that of TMTD, verifying the claim that EMTD improves the system's effectiveness of detecting attacks compared with TMTD.

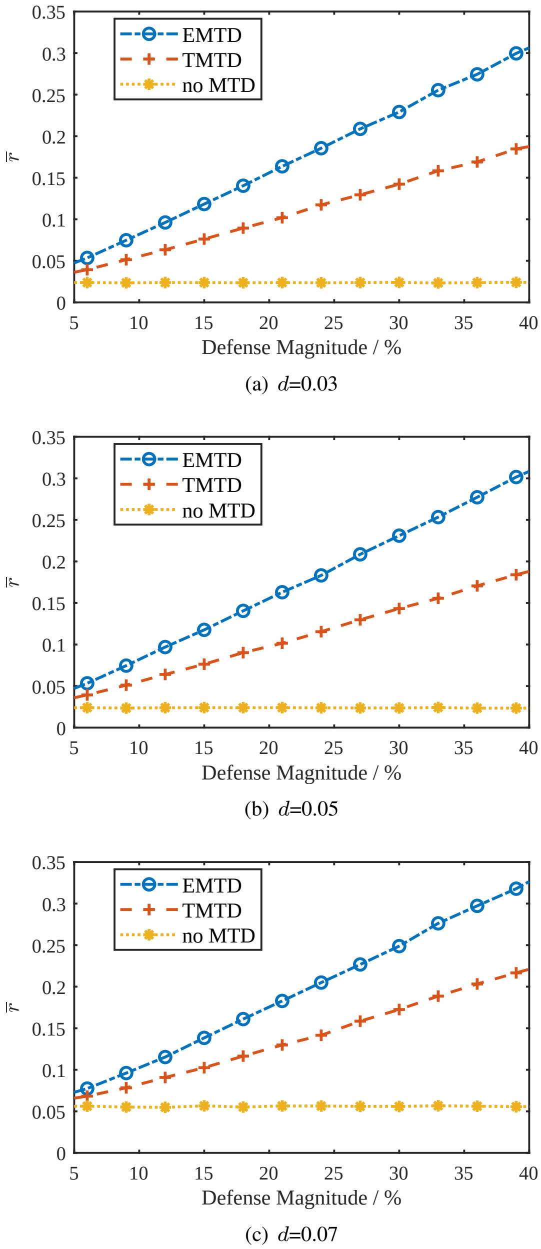


(a) d=0.03

(b) d=0.05

(c) d=0.07

Fig. 2. Attack detection probability of EMTD and TMTD



(a) d=0.03

(b) d=0.05

(c) d=0.07

Fig. 3. Average estimation residual of EMTD and TMTD

Since when a FDI attack is launched, the KLD of system measurement variation will increase. For the attack whose false data is 5% to 10% of the real system state, it can be easily detected. However, the false data less than 1% of the real system state can not be effectively detected [32]. In what follows, we use KLD as the metric to show TMTD and EMTD can detect FDI attacks with tiny false data, i.e., magnitudes less than 1% of the real system states, and show the detection performance of EMTD outperforms that of TMTD. The test system in this part is the same as that in [22], where the load data are based on the New York independent system operator (NYISO) from February 2021. There are 8236 measurement time points, of which the data of the 1st to 4000th measurement are used as historical data while the rest are used to construct real time measurements. In this experiment, the attacker only tamper with the voltage magnitude of bus 2 and the false data $c_{U_2} = -0.001$, which is about 0.1% of the real value of U_2. Set $\mathcal{X}_k^{max} = (1+q_m)\mathcal{X}_k$, $\mathcal{B}_{ck}^{max} = (1+3q_m)\mathcal{B}_{ck}$, $\mathcal{X}_k{}^{min} = (1-q_m)\mathcal{X}_k$, and $\mathcal{B}_{ck}^{min} = (1-3q_m)\mathcal{B}_{ck}$ here, where q_m varies from 10% to 30%. Considering that the distribution of KLD in this scenario is similar to the the long-tailed distribution [22], we use the median of KLD as the evaluation metric such that the center change of KLD distribution can be described accurately.

Fig.4 shows the median of KLD of system measurement variation for various attack and defense cases. It is observed that the median of KLD in the case of no defense and under attack is very close to the case of no defense and no attack, thus it is difficult to detect this kind of FDI attack. After executing MTD and EMTD, the median of KLD significantly increases when smart grids are under attack and EMTD performs better than TMTD, which is in accordance with our claim. Moreover, it is noted from the curves that executing TMTD and EMTD don't affect the median of KLD when there is no attack, implying system defense will not influence the false alarm rate in the sense of KLD.

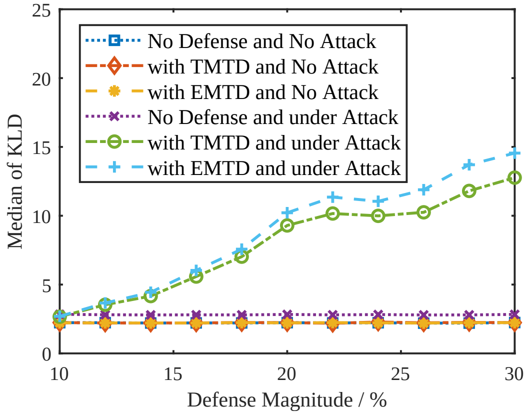


Fig. 4. The median of KLD for various attack and defense cases

Fig.5 shows the lowest voltage amplitude under different parameter change ratios for EMTD and TMTD in IEEE 9-bus system. Take rated voltage as U_0, the normal operating range of bus voltage as $[0.95U_0, 1.05U_0]$, and parameter change ratio as r_p. Under the condition of $\Delta\mathcal{X} = r_p\mathcal{X}$ for TMTD/EMTD and $\Delta\mathcal{B}_c = -r_p\mathcal{B}_c$ for EMTD, the lowest voltage amplitude of the system decreases with the increase of r_p. When the changes of $\mathcal{X}$ and $\mathcal{B}_c$ exceed 40% for EMTD and the change of $\mathcal{X}$ exceeds 80% for TMTD, the voltage of some buses will be out of the normal operating range, i.e., $U_{min} \leqslant 0.95U_0$. To avoid the adverse effect, defenders must check the defense scheme with Algorithm 1 in the subsection III-C.

B. Verifications of cost-minimization EMTD

This subsection first verifies the impact of EMTD on LMP, then compares the effects of random EMTD and optimal EMTD (TABLE I), showing the effectiveness of the proposed cost-minimization EMTD. Meanwhile, the cost of TMTD and EMTD are also compared (TABLE II).

Fig.6 shows the ΔLMP increases with the defense magnitude of EMTD and TMTD in IEEE 9-bus system, which together with the Fig. 2 implies the ΔLMP increases with the defense effectiveness of EMTD and TMTD in IEEE 9-bus system. Since system defenders expect to achieve desired defense effectiveness while resulting in the minimal ΔLMP, it is clear that there exists a trade-off according to Fig.6. Therefore, when choosing the defense scheme, the defender has to consider the impact of defense on LMP.

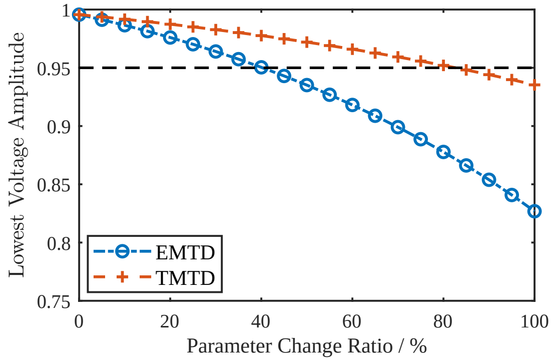


Fig. 5. The lowest voltage amplitude under different parameter change ratios

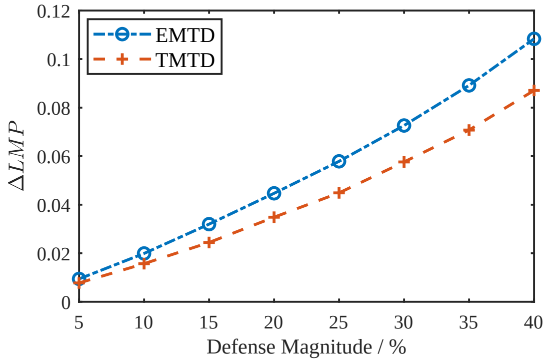


Fig. 6. ΔLMP in IEEE 9-bus system

To solve the optimal cost-minimization EMTD scheme, the parameters in the PSO algorithm is chosen as follows. The swarm size is 150, the function tolerance is 0.01, the self adjustment weight is 1.49, and the social adjustment weight is 1.49. In addition, defense magnitude q_m is 20%, the weight of LMP_i variations $m_i = 200$, penalty coefficients $\zeta_1 \sim \zeta_7 = 10$ and the coefficient of active power loss l is set to the value of LMP of the slack bus. 100 attack-defense simulations are conducted in each step for each particle to verify the detect capability. On the other hand, the cost of FACTS devices is generally higher than that of D-FACTS devices in smart grids [33]. This paper considers transmission network, where FACTS devices are used to change parallel susceptance $\mathcal{B}_c$ and D-FACTS devices are used to change series reactance $\mathcal{X}$. Therefore, the economic cost of changing $\mathcal{B}_c$ is higher than that of changing $\mathcal{X}$ and we set $e_1 = 100$, $e_2 = 500$. The rest parameters such as upper and lower limits in simulations are directly taken from the standard test system.

After calculation, the best values of the fitness function (47) show a downward trend and the minimum cost is 1.72. The overall active power loss of the original system is 4.64MW, nevertheless after changing topology parameters according to the solved optimal scheme, the overall active power loss is 4.61MW. The results show the cost-minimization EMTD scheme optimizes the active power loss while ensuring the security of the smart grid. Meanwhile, the verification shows

TABLE I. LMP of each node before and after executing EMTD

Bus number	before defense	after defense 1	variation 1/%	after defense 2	variation 2/%	after optimal defense	variation 3/%
1	24.7557	24.7610	0.0213	24.7573	0.0066	24.7556	-0.0004
2	24.0345	24.0248	-0.0404	24.0301	-0.0183	24.0330	-0.0062
3	24.0759	24.1032	0.1131	24.1053	0.1222	24.0765	0.0025
4	24.7559	24.7618	0.0240	24.7589	0.0121	24.7559	0.0000
5	24.9985	25.0183	0.0791	25.0165	0.0719	24.9984	-0.0004
6	24.0759	24.1032	0.1131	24.1053	0.1222	24.0765	0.0026
7	24.2539	24.2642	0.0426	24.2713	0.0718	24.2517	-0.0090
8	24.0345	24.0274	-0.0298	24.0325	-0.0085	24.0330	-0.0062
9	24.9985	25.0215	0.0921	25.0331	0.1383	24.9984	-0.0002

the obtained EMTD scheme satisfies the rationality constraints. Table I presents the LMP before and after defense, showing the designed cost-minimization EMTD has much smaller impact on the LMP (the defense 1 and defense 2 are random).

The comparison of costs of TMTD and EMTD under different attack magnitudes is shown in the table II. For each attack magnitude, the cost of defense is optimized with (42)-(46). With the increase of attack amplitude, the difficulty of detecting attacks decreases gradually, so the cost of MTD also decreases gradually. Due to the greater freedom of EMTD, the impact of EMTD on LMP is less than TMTD, and it can better optimize the active network loss. Therefore, the cost of EMTD is lower than that of TMTD.

TABLE II. Costs of TMTD and EMTD under different attack magnitude

	$d = 0.03$	$d = 0.05$	$d = 0.07$
TMTD	1.8202	1.7811	0.8675
EMTD	1.7680	1.7249	0.8309
Reduction/%	2.8678	3.1553	4.2190

Next, we demonstrate the selection of optimal defense time interval based on the optimal cost solved above, and present the comparison results. For most attack targets such as overloading key lines to cause physical disasters [34], the economic losses of smart grids increase with the attack duration. Therefore, we express formula (51) as:

$$f_{ae}(\overline{T}, c_{sum}) = \frac{\overline{T}^2 \times \sum_{j=1}^{W} (\sum_{i=1}^{2N-1} \beta_i \times c_{ij})}{W}, \tag{54}$$

where the window size W is 10, the β_i of each bus is 1, the average value of c_{ij} is 0.1, and the cost of a single defense is 1.71. According to the mean time of attacks in [35], we take T_{amax} as one month, and set the time unit of the simulation results as month. Take the weight for cost of a single defense per unit time as $\mu_1 = 1$, and take the weight for adverse effect per unit time as $\mu_2 = 10$. Considering that the defense interval in engineering practice is usually an integer number of days, we round the solutions. According to formula (52)-(54) and the above parameters, we can get the optimal defense time interval is 0.5 month.

The following shows the effectiveness of the above optimal defense time interval is 0.5 month by calculating the total cost of the defender over a long period of time. In the experiment, the adverse effects of FDI attack imposed on the system are calculated using the time that the system is actually affected by attack, which is shown in the following formula:

$$f_{ae}(\overline{T}, c_{sum}) = {t_{actual}}^2 \times (\sum_{i=1}^{2N-1} \beta_i \times c_i). \tag{55}$$

In addition, the attack and defense scenarios are settled as:

- Attacker makes 10,000 consecutive FDI attacks, and attack time interval $t_a \sim U(0, T_{amax})$.
- Defender 1 defends at the optimal time interval which varies according to the method proposed above.
- Defender 2 defends at a fixed time interval $t_d = 0.25$ month.
- Defender 3 defends at a fixed time interval $t_d = 0.75$ month.
- Defender 4 defends at a fixed time interval $t_d = 1$ month.
- Defender 5 randomly selects the time interval for each defense with $t_d \sim U(0, T_{amax})$.

Fig. 7 shows the total cost of defenders over a long period of time. It is observed that the total cost of defender 1 who uses the method proposed in this paper to select the defense time interval is the smallest, and the total costs of other defenders are obviously much larger. Therefore, the defense time interval optimization model proposed is effective, and the proposed optimal approach can help defenders choose the cost-minimization EMTD scheme.

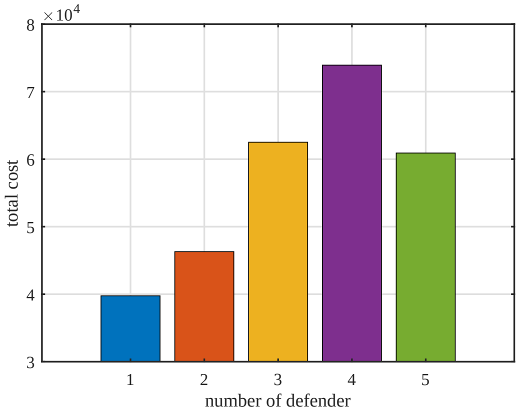


Fig. 7. The total cost of defender i ($i = 1, 2, \cdots, 5$)

VI. Conclusion

This paper has investigated MTD in terms of thwarting stealthy FDI attacks with the AC power flow model. An EMTD approach has been designed to enhance the defense capability of smart grids for AC state estimation. Rationality constraints are proposed to avoid possible adverse effects of EMTD on smart grids. Moreover, the impact of EMTD on the electricity market, active power loss, and device costs are regarded as system defense costs. EMTD topology parameter scheme and defense time interval are optimized with the objective of minimizing system defense costs while ensuring sufficient defense effectiveness. Simulations are carried out to validate and illustrate the theoretical approach.

References

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

[2] Z. Zhang, R. Deng, D. K. Y. Yau, P. Cheng, and J. Chen, “Zero-parameter-information FDI attacks against power system state estimation,” in *2020 American Control Conference (ACC)*, pp. 2987–2992, 2020.

[3] M. Zhang, Z. Wu, J. Yan, R. Lu, and X. Guan, “Attack-resilient optimal pmu placement via reinforcement learning guided tree search in smart grids,” *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 1919–1929, 2022.

[4] X. Liu and Z. Li, “False data attacks against AC state estimation with incomplete network information,” *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2239–2248, 2017.

[5] M. Zhang, C. Shen, N. He, S. Han, Q. Li, Q. Wang, and X. Guan, “False data injection attacks against smart gird state estimation: Construction, detection and defense,” *Science China Technological Sciences*, vol. 62, no. 12, pp. 2077–2087, 2019.

[6] Y. Yuan, Z. Li, and K. Ren, “Modeling load redistribution attacks in power systems,” *IEEE Transactions on Smart Grid*, vol. 2, no. 2, pp. 382–390, 2011.

[7] K. R. Davis, K. L. Morrow, R. Bobba, and E. Heine, “Power flow cyber attacks and perturbation-based defense,” in *2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm)*, pp. 342–347, 2012.

[8] K. L. Morrow, E. Heine, K. M. Rogers, R. B. Bobba, and T. J. Overbye, “Topology perturbation for detecting malicious data injection,” in *2012 45th Hawaii International Conference on System Sciences*, pp. 2104–2113, 2012.

[9] M. A. Rahman, E. Al-Shaer, and R. B. Bobba, “Moving target defense for hardening the security of the power system state estimation,” in *Proceedings of the First ACM Workshop on Moving Target Defense*, MTD ’14, (New York, NY, USA), pp. 59–68, Association for Computing Machinery, 2014.

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

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

[12] M. Cui and J. Wang, “Deeply hidden moving-target-defense for cyber-secure unbalanced distribution systems considering voltage stability,” *IEEE Transactions on Power Systems*, vol. 36, no. 3, pp. 1961–1972, 2021.

[13] M. Liu, C. Zhao, Z. Zhang, R. Deng, P. Cheng, and J. Chen, “Converter-based moving target defense against deception attacks in dc microgrids,” *IEEE Transactions on Smart Grid*, vol. 13, no. 5, pp. 3984–3996, 2022.

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

[15] Z. Zhang, R. Deng, D. K. Y. Yau, P. Cheng, and J. Chen, “Analysis of moving target defense against false data injection attacks on power grid,” *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2320–2335, 2020.

[16] B. Li, G. Xiao, R. Lu, R. Deng, and H. Bao, “On feasibility and limitations of detecting false data injection attacks on power grid state estimation using D-FACTS devices,” *IEEE Transactions on Industrial Informatics*, vol. 16, no. 2, pp. 854–864, 2020.

[17] B. Liu and H. Wu, “Optimal D-FACTS placement in moving target defense against false data injection attacks,” *IEEE Transactions on Smart Grid*, vol. 11, no. 5, pp. 14345–4357, 2020.

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

[19] R. Deng, P. Zhuang, and H. Liang, “False data injection attacks against state estimation in power distribution systems,” *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 2871–2881, 2019.

[20] A. Monticelli, *State Estimation in Electric Power Systems, A Generalized Approach*. Boston, MA: Springer, 1999.

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

[22] G. Chaojun, P. Jirutitijaroen, and M. Motani, “Detecting false data injection attacks in AC state estimation,” *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2476–2483, 2015.

[23] D. Xia and Z. Du, *Power Systems Analysis (Third Edition)*. Beijing, China: China Electric Power Press, 2018.

[24] L. Xie, Y. Mo, and B. Sinopoli, “False data injection attacks in electricity markets,” in *2010 First IEEE International Conference on Smart Grid Communications*, pp. 226–231, 2010.

[25] Q. Zhang, F. Li, H. Cui, R. Bo, and L. Ren, “Market-level defense against fdia and a new lmp-disguising attack strategy in real-time market operations,” *IEEE Transactions on Power Systems*, vol. 36, no. 2, pp. 1419–1431, 2021.

[26] D. Asija and R. Viral, “Chapter 13 - renewable energy integration in modern deregulated power system: challenges, driving forces, and lessons for future road map,” in *Advances in Smart Grid Power System* (A. Tomar and R. Kandari, eds.), pp. 365–384, Academic Press, 2021.

[27] A. J. Conejo, E. Castillo, R. Minguez, and F. Milano, “Locational marginal price sensitivities,” *IEEE Transactions on Power Systems*, vol. 20, no. 4, pp. 2026–2033, 2005.

[28] L. J. Cai, I. Erlich, and G. Stamtsis, “Optimal choice and allocation of FACTS devices in deregulated electricity market using genetic algorithms,” in *IEEE PES Power Systems Conference and Exposition, 2004.*, pp. 201–207 vol.1, 2004.

[29] C. Liu, J. Wu, C. Long, and D. Kundur, “Reactance perturbation for detecting and identifying FDI attacks in power system state estimation,” *IEEE Journal of Selected Topics in Signal Processing*, vol. 12, no. 4, pp. 763–776, 2018.

[30] R. D. Zimmerman, C. E. Murillo-Snchez, and R. J. Thomas, “MATPOWER: Steady-state operations, planning, and analysis tools for power systems research and education,” *IEEE Transactions on Power Systems*, vol. 26, no. 1, pp. 12–19, 2011.

[31] K. M. Rogers and T. J. Overbye, “Some applications of distributed flexible AC transmission system (D-FACTS) devices in power systems,” in *2008 40th North American Power Symposium*, pp. 1–8, 2008.

[32] S. K. Singh, K. Khanna, R. Bose, B. K. Panigrahi, and A. Joshi, “Joint-transformation-based detection of false data injection attacks in smart grid,” *IEEE Transactions on Industrial Informatics*, vol. 14, no. 1, pp. 89–97, 2018.

[33] D. Divan and H. Johal, “Distributed FACTS-a new concept for realizing grid power flow control,” *IEEE Transactions on Power Electronics*, vol. 22, no. 6, pp. 2253–2260, 2007.

[34] Z. Li, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, “Bilevel model for analyzing coordinated cyber-physical attacks on power systems,” *IEEE Transactions on Smart Grid*, vol. 7, no. 5, pp. 2260–2272, 2016.

[35] Y. Xiang, Z. Ding, Y. Zhang, and L. Wang, “Power system reliability evaluation considering load redistribution attacks,” *IEEE Transactions on Smart Grid*, vol. 8, no. 2, pp. 889–901, 2017.

Meng Zhang received the B.S. degree from Xi'an Jiaotong University, Xi'an, China, in 2013, and the Ph.D. degrees from Zhejiang University, Hangzhou, China, in 2018. He is currently an associate professor with the School of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an, China. His research interests include nonlinear control, filtering, power systems and cyber-physical systems.

Xuzhen Fan received the B.S. degree from Xi'an Jiaotong University, Xi'an China, in 2020, where he is currently pursuing the M.S. degree with the School of Electronic and Information Engineering. His research interests include smart grid security, data mining and multi-task learning. He was a recipient of the 15th International Conference on Innovative Computing, Information and Control (ICICIC) Best Application Paper Award, in 2021.

Rongxing Lu (Fellow, IEEE) received the Ph.D. degree from the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada, in 2012. He was an Assistant Professor with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, from 2013 to 2016. He has been an Associate Professor with the Faculty of Computer Science (FCS), University of New Brunswick (UNB), Fredericton, NB, Canada, since 2016. He was a Post-Doctoral Fellow with the University of Waterloo, from 2012 to 2013. His research interests include applied cryptography, privacy enhancing technologies, and the IoT-big data security and privacy. He has published extensively in his areas of expertise. He was awarded the most prestigious ”Governor Generals Gold Medal” for his Ph.D. degree. He won the 8th IEEE Communications Society (ComSoc) Asia-Pacific (AP) Outstanding Young Researcher Award in 2013. He was a recipient of nine best (student) paper awards from some reputable journals and conferences. He is the Winner of the 2016-2017 Excellence in Teaching Award, FCS, UNB. Currently, he serves as the Chair for IEEE Communications and Information Security Technical Committee (IEEE ComSoc CIS-TC) and the Founding Co-Chair for IEEE TEMS Blockchain and Distributed Ledgers Technologies Technical Committee (BDLT-TC).

Chao Shen received the B.S. degree in Automation from Xi'an Jiaotong University, China in 2007; and the Ph.D. degree in Control Theory and Control Engineering from Xi'an Jiaotong University, China in 2014. He is currently a Professor in the Faculty of Electronic and Information Engineering, Xi'an Jiaotong University of China. His current research interests include AI Security, insider/intrusion detection, behavioral biometrics, and measurement and experimental methodology.

Xiaohong Guan (Fellow, IEEE) received the B.S. and M.S. degrees in control engineering from Tsinghua University, Beijing, China, in 1982 and 1985, and the Ph.D. degree in electrical and systems engineering from the University of Connecticut in 1993.

He is currently a professor at the Systems Engineering Institute, Xian Jiaotong University, Xian, China. He was appointed Cheung Kong Professor of Systems Engineering in 1999, and dean of the Faculty of Electronic and Information Engineering in 2008. He has been the director of the Center for Intelligent and Networked Systems since 2001, Tsinghua University, and served as head of the Department of Automation, 2003-2008. His research interests include economics and security of networked systems, optimization based planning and scheduling of power and energy systems, manufacturing systems, and cyber-physical systems, including smart grid and sensor networks. He is the member of Chinese Academy of Science.