Letter

Impact Analysis of MTD on the Frequency Stability in Smart Grid

Zhenyong Zhang and Ruilong Deng, *Senior Member, IEEE*

Dear Editor,

In order to accommodate the effects of false data injection attacks (FDIAs), the moving target defense (MTD) strategy is recently proposed to enhance the security of the smart grid by perturbing branch susceptances. However, most pioneer work only focus on the defending performance of MTD in terms of detecting FDIAs and the impact of MTD on the static factors such as the power and economic losses. Considering the system dynamics, in this letter, the impact of MTD on the frequency stability is analytically studied. The condition required to maintain the stability of the grid frequency is provided and how the susceptance perturbation of each branch affects the frequency stability is given. The defending cost of MTD is also optimized considering both the defending performance and frequency stability constraints.

Low-carbon goals, energy crisis, and demand increasing lead to the integration of advanced electronic and communication devices into the smart grid to enable the environmental-friendly, real-time, and economic control and operation. However, the vulnerabilities exposed in the Internet protocol (IP)-based devices and communication network make smart grid prone to cyberattacks. The FDIA [1] is one of the cyberattacks that threatens the system operations.

To alleviate the impact of FDIAs, there are many studies devoting to detect and identify the attacks. In our opinion, the countermeasures can be classified according to the DC model $\mathbf{z} = \mathbf{H}\mathbf{x}$. From the angle of measurements z, the smart grid is protected from being attacked by FDIAs by protecting the sensory data or analyzing the statistic characteristics of the historical data. The typical examples are the measurement protection strategy (MPS) [2] that aims to reduce the impact of FDIAs and the data-driven methods to extract the abnormal properties of FDIAs [3]. From the angle of states $\mathbf{x}$, the secure phasor measurement units (PMUs) are strategically deployed to verify the consistency of the state estimates and state measurements [4]. From the angle of the measurement matrix $\mathbf{H}$, the smart grid is prevented from FDIAs by comparing the real branch parameters or dynamically changing the network parameters. For example, the true branch parameters are validated using the voltage and current sensor measurements [5] and the MTD is proposed to obfuscate the information of the communication and/or power networks [6], [7]. Since the MPS and secure PMUs protect the system in a static manner, they can be cracked by the attacker by continuously exploiting the device and protocol vulnerabilities. The data-driven methods highly depend on the quality of the dataset and thus lack of scalability and performance-guarantee. The MTD is a newly emerged approach that introduces uncertainties into the power system to increase the efforts and difficulties for the attacker to launch the attack. It is a promising method to defend against FDIAs since it has a dynamic manner and does not depend on the data properties.

Based on our knowledge, the related work leverage the MTD idea from the aspects of defending against direct-current (DC) FDIAs and alternating current (AC0 FDIAs. To thwart DC FDIAs, Rahman *et al.* [8] first proposed the idea of MTD and presented a formal design of it to guarantee its effectiveness in terms of detecting FDIAs. The AC FDIAs are more complicated but can also be detected with MTD. Cui and Wang [9] proposed a deeply hidden MTD to confuse the attacker and promote the defending performance simultaneously. However, most pioneering work only focus on improving the defending performance. The impact of MTD on the system operation is ignored. Although the impact of MTD on the static factors (e.g., the power and economic losses) have been analyzed in [10] and [11], the impact of MTD on the system dynamics (e.g., frequency stability) has not been investigated.

In this letter, we devote our efforts to analyzing the impact of MTD on the frequency stability. The considered MTD is constructed by perturbing the branch susceptances, which is also the mostly studied approach by the related work. Since the susceptance change affects the parameters such as the power transfer capacity, voltages, and generation outputs, the grid frequency might not be maintained after the MTD. This issue has not yet been deeply analyzed. To fill this gap, we propose a stability-guaranteed MTD in this letter. Our contributions are summarized as follows: 1) The Grassmann distance is adopted to quantify the defending performance of MTD; 2) An analytical relationship between the frequency stability and perturbation parameters is derived based on the theory of eigenvalue sensitivity; 3) The defending cost is minimized, and simultaneously, the defending performance is guaranteed and the frequency stability is not affected.

System model: Consider a power system with a set $\mathcal{G}$ of generation buses and a set $\mathcal{L}$ of load buses ($|\mathcal{G}| = N_1$, $|\mathcal{L}| = N_2$, $N = N_1 + N_2$) and the power system has a set $\mathcal{T}$ ($|\mathcal{T}| = T$) of branches.

The power flow equations are as follows:

$$\mathbf{p}^I = \mathbf{B}^{GG}\boldsymbol{\mu} + \mathbf{B}^{GL}\boldsymbol{\theta},\ \ \boldsymbol{p}^L = -\mathbf{B}^{LL}\boldsymbol{\theta} - \mathbf{B}^{LG}\boldsymbol{\mu} \tag{1}$$

where $\mathbf{p}^I \in \mathbb{R}^{N_1}$ is a vector of power injections of generators, $\boldsymbol{p}^L$ is a vector of power consumptions of loads, $\boldsymbol{\mu} \in \mathbb{R}^{N_1}$ is a vector of voltage phase angles of generators, and $\boldsymbol{\theta} \in \mathbb{R}^{N_2}$ is a vector of voltage phase angles of load buses. The susceptance matrix $\mathbf{B} \in \mathbb{R}^{N\times N}$ is formed according to the system topology and susceptance values and $\mathbf{B} = \begin{bmatrix} \mathbf{B}^{GG} & \mathbf{B}^{GL} \\ \mathbf{B}^{LL} & \mathbf{B}^{LG} \end{bmatrix}$, where $\mathbf{B}^{GG} \in \mathbb{R}^{N_1\times N_1}$, $\mathbf{B}^{LL} \in \mathbb{R}^{N_2\times N_2}$, $\mathbf{B}^{GL} \in \mathbb{R}^{N_1\times N_2}$, and $\mathbf{B}^{LG} \in \mathbb{R}^{N_2\times N_1}$.

Considering the generatordynamics, the swing equation is

$$\dot{\mu}_i = \omega_i,\ \ m_i\dot{\omega}_i = -d_i\omega_i + p_i^M - p_i^I \tag{2}$$

where $\dot{y}$ is the derivative of y, ω_i is the frequency deviation at the generation bus i, $m_i > 0$ is the inertial of the rotor, $d_i > 0$ is the damping ratio, and p_i^M is the mechanical power input. To maintain the grid's frequency, the rotor frequency is controlled by the turbine-governor controller by adjusting the mechanical power to keep the primary system at a steady state and the load-frequency controller pushes the frequency deviation ω_i back to 0. The proportional-integral (PI) controller is usually used to model these two controllers together, given by $p_i^M = -(k_i^P\omega_i + k_i^I\mu_i)$, where $k_i^P > 0$ and $k_i^I > 0$ are the proportional and integral coefficients, respectively. In power systems, the power loads are usually divided into frequency-sensitive and frequency-insensitive types. That is, for each load bus i, the load is compromised of $p_i^L = r_i\phi_i + p_i^{L_0}$, where $r_i > 0$ is the coefficient of the frequency-sensitive load (every load bus is assumed to have frequency-sensitive load), $\phi_i = -\dot{\theta}_i$ is the frequency deviation of load bus i, and $p_i^{L_0}$ is the frequency-insensitive load. Using the state-space descriptor, the system dynamics is

Corresponding author: Zhenyong Zhang.

Citation: Z. Y. Zhang and R. L. Deng, "Impact analysis of moving target defense the frequency stability in smart grid," *IEEE/CAA J. Autom. Sinica*, vol. 10, no. 1, pp. 275–277, Jan. 2023.

Z. Y. Zhang is with the State Key Laboratory of Public Big Data and the College of Computer Science and Technology, Guizhou University, Guiyang 550025, China (e-mail: zyzhangnew@gmail.com).

R. L. Deng is with the State Key Laboratory of Industrial Control Technology, Zhejiang University, Hangzhou 310027, China (e-mail: dengrui long@>zju.edu.cn).

Digital Object Identifier 10.1109/JAS.2023.123039

$$\begin{bmatrix} \mathbf{I} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{I} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & -\mathbf{M} \end{bmatrix} \begin{bmatrix} \dot{\boldsymbol{\mu}} \\ \dot{\boldsymbol{\theta}} \\ \dot{\boldsymbol{\omega}} \end{bmatrix} = \begin{bmatrix} \mathbf{0} & \mathbf{0} & \mathbf{I} \\ \mathbf{R}^{-1}\mathbf{B}^{LG} & \mathbf{R}^{-1}\mathbf{B}^{LL} & \mathbf{0} \\ \mathbf{K}^{I}+\mathbf{B}^{GG} & \mathbf{B}^{GL} & \mathbf{K}^{P}+\mathbf{D} \end{bmatrix} \begin{bmatrix} \boldsymbol{\mu} \\ \boldsymbol{\theta} \\ \boldsymbol{\omega} \end{bmatrix} + \begin{bmatrix} \mathbf{0} \\ \mathbf{R}^{-1} \\ \mathbf{0} \end{bmatrix} \mathbf{p}^{L_0} \quad (3)$$

where $\boldsymbol{\omega} \in \mathbb{R}^{N_1}$ is a vector of frequency deviations of generation buses, $\mathbf{M} \in \mathbb{R}^{N_1 \times N_1}$, $\mathbf{D} \in \mathbb{R}^{N_1 \times N_1}$, $\mathbf{K}^P \in \mathbb{R}^{N_1 \times N_1}$, and $\mathbf{K}^I \in \mathbb{R}^{N_1 \times N_1}$ are diagonal matrices with diagonal entries equal to the inertial, damping ratio, proportional and integral factors of the PI controller, respectively, $\mathbf{R} \in \mathbb{R}^{N_2 \times N_2}$ is a diagonal matrix with elements equal to the coefficients of frequency-sensitive loads, and $\mathbf{p}^{L_0} \in \mathbb{R}^{N_2}$ is a vector of frequency-insensitive loads.

Main results: Recently, the cybersecurity researchers of power systems proposed the MTD to defend against FDIAs by perturbing branch susceptances. The physical perturbations can disable the attacker's capability to infer the valid network information to launch the attacks. Normally, the attacker constructs the attack vector for the FDIA as $\mathbf{a} = \mathbf{Hc}$, where $\mathbf{H} \in \mathbb{R}^M$ is the measurement matrix related to the branch susceptance and system topology. The FDIA targets the state estimation and inserts the bias $\mathbf{c} \in \mathbb{R}^N$ into the state estimate by stealthily modifying the sensor measurement with an error $\mathbf{a}$ [1]. Since the branch susceptances contained in $\mathbf{H}$ are necessary information to design the attack, the MTD defends against FDIAs by dynamically perturbing them with an equipment named the distributed flexible AC transmission system (D-FACTS), which is smaller and can be suspended from power lines. Comparing with the cyber side MTDs that change the system configurations and network attributes [12], the proposed MTD perturbs the parameters of physical systems. Although the authors in [13] proposed the ZDIA based on the specific network structure called the cut line, the ZDIA can only insert random errors into the state estimates. The MTD is still effective to protect the state estimates from being injected with targeted biases.

Suppose the attacker knows a measurement matrix $\mathbf{H}$ before the MTD. The possible stealthy attack vectors constructed by the attacker falls into the column space of $\mathbf{H}$, i.e., $\mathbf{a} \in \text{col}(\mathbf{H})$, where $\text{col}(\cdot)$ represents the column space of a matrix. After the MTD, the measurement matrix changes to $\tilde{\mathbf{H}}$, which is not known by the attacker. To meet the stealthy requirement, the attack vector for the FDIA should fall into the column space of $\tilde{\mathbf{H}}$ after the MTD. Therefore, with the knowledge of $\mathbf{H}$, the attacker has the chance to keep the FDIA stealthy only if $\mathbf{a} \in \text{col}(\mathbf{H})$ and $\mathbf{a} \in \text{col}(\tilde{\mathbf{H}})$. The defending performance of MTD depends on the dissimilarity [to make $\mathbf{a} \in \text{col}(\mathbf{H})$ but $\mathbf{a} \notin \text{col}(\tilde{\mathbf{H}})$] between these two subspaces. In this letter, the Grassmann distance is adopted to quantify the separation between $\text{col}(\mathbf{H})$ and $\text{col}(\tilde{\mathbf{H}})$, given by $G\left(\text{b}(\mathbf{H}), \text{b}(\tilde{\mathbf{H}})\right) = \sqrt{\sum_{i=1}^{n} \psi_i^2}$, where $\text{b}(\mathbf{H})$ and $\text{b}(\tilde{\mathbf{H}})$ are orthonormal bases of the column spaces $\text{col}(\mathbf{H})$ and $\text{col}(\tilde{\mathbf{H}})$, $\psi_i = \cos^{-1}\left(\sigma_i\left(\text{b}(\mathbf{H})^T \text{b}(\tilde{\mathbf{H}})\right)\right)$, $\sigma_i(\cdot)$ computes the ith singular value of the matrix, and $G(\cdot)$ represents the Grassmann distance. The defender's goal is to maximize the defending performance given the limited defending resource.

Apart from the defending performance, the impact of MTD on the system operation should also be analyzed to support its implementation. According to the system model (3), the system dynamics is closely related to the perturbation parameters (i.e., the perturbed branches and susceptance perturbations) of MTD. The susceptance perturbation might inflict the frequency stability. Therefore, although the defending performance is important to design MTD, the impact of it on the system dynamics cannot be ignored, which is the premise to deploy this approach.

Analytical results based on the eigenvalue sensitivity: Here, the frequency stability is analyzed by deriving the eigenvalue sensitivity against the susceptance perturbations. First of all, the state-space model (3) is transformed into the second-order dynamic system

$$\mathbf{P}\ddot{\mathbf{y}} + \mathbf{C}\dot{\mathbf{y}} + \mathbf{Z}\mathbf{y} = \mathbf{0} \quad (4)$$

where $\mathbf{y} = \begin{bmatrix} \boldsymbol{\phi} \\ \boldsymbol{\omega} \end{bmatrix} \in \mathbb{R}^N$, $\mathbf{P} = \begin{bmatrix} \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{M} \end{bmatrix} \in \mathbb{R}^{N \times N}$, $\mathbf{C} = \begin{bmatrix} -\mathbf{R} & \mathbf{0} \\ \mathbf{0} & \mathbf{K}^P + \mathbf{D} \end{bmatrix} \in \mathbb{R}^{N \times N}$, $\mathbf{Z} = \begin{bmatrix} \mathbf{B}^{LL} & -\mathbf{B}^{LG} \\ -\mathbf{B}^{GL} & \mathbf{K}^I + \mathbf{B}^{GG} \end{bmatrix} \in \mathbb{R}^{N \times N}$, and $\boldsymbol{\phi} \in \mathbb{R}^{N_2}$ is a vector of frequency deviations of load buses. The left and right eigenvalue problems are represented by

$$s_i^2 \mathbf{P}\mathbf{r}_i + s_i \mathbf{C}\mathbf{r}_i + \mathbf{Z}\mathbf{r}_i = \mathbf{0}, \;\; s_i^2 \mathbf{l}_i^T \mathbf{P} + s_i \mathbf{l}_i^T \mathbf{C} + \mathbf{l}_i^T \mathbf{Z} = \mathbf{0} \quad (5)$$

where s_i is the ith latent root (eigenvalue), $\mathbf{r}_i \in \mathbb{C}^N$ and $\mathbf{l}_i \in \mathbb{C}^N$ are the ith right and left latent vector (eigenvector). These variables are all complex values. Suppose the perturbed susceptances are denoted by $\mathbf{b} = \{b_1, b_2, \ldots\}$, where b_i is the susceptance of branch i. Therefore, the matrices $\mathbf{P}$, $\mathbf{C}$, $\mathbf{Z}$, and s_i are functions of $\mathbf{b}$, that is, $\mathbf{P} \triangleq \mathbf{P}(\mathbf{b})$, $\mathbf{C} \triangleq \mathbf{C}(\mathbf{b})$, $\mathbf{Z} \triangleq \mathbf{Z}(\mathbf{b})$, and $s_i \triangleq s_i(\mathbf{b})$. Therefore, we have:

Proposition 1: The first-order derivative of the eigenvalue for the ith eigenvalue is

$$\frac{\partial s_i(\mathbf{b})}{\partial \mathbf{b}} = -\frac{\mathbf{l}_i^T \left(s_i^2 \frac{\partial \mathbf{P}(\mathbf{b})}{\partial \mathbf{b}} + s_i \frac{\partial \mathbf{C}(\mathbf{b})}{\partial \mathbf{b}} + \frac{\partial \mathbf{Z}(\mathbf{b})}{\partial \mathbf{b}}\right)\mathbf{r}_i}{\mathbf{l}_i^T (2s_i \mathbf{P} + \mathbf{C})\mathbf{r}_i} = -\frac{\mathbf{l}_i^T \mathbf{F}_i \mathbf{r}_i}{\mathbf{l}_i^T (2s_i \mathbf{P} + \mathbf{C})\mathbf{r}_i}$$

where $\mathbf{F}_i = \frac{\partial \mathbf{Z}(\mathbf{b})}{\partial \mathbf{b}} = \begin{bmatrix} \frac{\partial \mathbf{B}^{LL}}{\partial \mathbf{b}} & -\frac{\partial \mathbf{B}^{LG}}{\partial \mathbf{b}} \\ -\frac{\partial \mathbf{B}^{GL}}{\partial \mathbf{b}} & \frac{\partial \mathbf{B}^{GG}}{\partial \mathbf{b}} \end{bmatrix} \in \mathbb{R}^{N \times N}$.

The above result is derived because only the matrix $\mathbf{Z}$ is related to the susceptance perturbation. Therefore, the ith eigenvalue after the MTD is given by $\tilde{s}_i = s_i + \sum_j \frac{\partial s_i(b_j)}{\partial b_j} \Delta b_j$, where Δb_j is the susceptance perturbation of branch j. If all eigenvalues fall into the left complex plane, then the grid frequency remains at the nominal value after the MTD. That is, the system is stable if $Re(\tilde{s}_i) < 0, 1 \le i \le N + N_1$, where $Re(\cdot)$ extracts the real part of the complex number. Besides, based on the derived result, we can screen out the impact of the susceptance perturbation for each branch on the change of eigenvalues. The impact of the susceptance perturbation of branch j on the ith eigenvalue s_i is quantified by $e_{ij} = Re(\frac{\partial s_i(b_j)}{\partial b_j}), 1 \le j \le T$. Therefore, if $|e_{ij}|$ is larger, the eigenvalue s_i is more sensitive to the change of the susceptance perturbation on branch j. The most sensitive branch is $j^* = \text{argmax}_j\{|e_{ij}|, 1 \le j \le T\}$. Besides, to make $Re(\tilde{s}_i) < 0$, it is better to make $\Delta b_j > 0$ if $e_{ij} < 0$ and $\Delta b_j < 0$ if $e_{ij} > 0$.

Stability-constrained defending cost optimization: Next, the defending cost is minimized to implement the MTD. Here the generation cost output from the optimal power flow (OPF) is regarded as the defending cost. Suppose the generation cost calculated by the OPF before the MTD is C_0. Then the stability-constrained defending cost optimization problem is formulated as

$$\begin{aligned} \Delta C \;\triangleq\; & \max_{\mathbf{p}^G, \Delta b_j, \pi_j, 1 \le j \le T} \; C_0 - \mathbf{g}^T \mathbf{p}^G \\ \text{s.t.} \;\; & Re(\tilde{s}_i) < 0, \;\; 1 \le i \le N + N_1 \\ & \Delta b_j^{\min} \le \pi_j \Delta b_j \le \Delta b_j^{\max}, \;\; \pi_j \in \{0,1\}, \;\; 1 \le j \le T \\ & \mathbf{p}_{\min}^G \le \mathbf{p}^G \le \mathbf{p}_{\max}^G, \;\; \mathbf{p}_{\min}^F \le \mathbf{p}^F \le \mathbf{p}_{\max}^F \\ & \sum \mathbf{p}^G = \sum \mathbf{p}^L \\ & \mathbf{p}^F = \begin{bmatrix} \tilde{\mathbf{S}}^{GG} & \mathbf{0} \\ \mathbf{0} & \tilde{\mathbf{S}}^{LL} \end{bmatrix} \mathbf{W}\left(\tilde{\mathbf{B}}^{LL}\right)^{-1} (\mathbf{p}^G - \mathbf{p}^L) \\ & G\left(\text{b}(\mathbf{H}), \text{b}(\tilde{\mathbf{H}})\right) \ge \varsigma \end{aligned} \quad (6)$$

where $\Delta b_j^{\min}$ and $\Delta b_j^{\max}$ are perturbation limits for the susceptance of branch j, π_j determines whether the susceptance of branch j is perturbed or not, $\mathbf{g} \in \mathbb{R}^{N_1}$ is a vector of coefficients for the generation costs, $\mathbf{p}^G \in \mathbb{R}^{N_1}$ is a vector of generation outputs, $\mathbf{p}_{\min}^G \in \mathbb{R}^{N_1}$ and $\mathbf{p}_{\max}^G \in \mathbb{R}^{N_1}$ are the limits of generation outputs, $\mathbf{p}_{\min}^F \in \mathbb{R}^T$ and $\mathbf{p}_{\max}^F \in \mathbb{R}^T$ are the overloaded thresholds for the power transmissions, $\tilde{\mathbf{S}}^{GG}$, $\tilde{\mathbf{S}}^{LL}$, $\tilde{\mathbf{B}}^{LL}$ are parametric matrices after the MTD, ς is the threshold to guarantee the defending performance of MTD, and $\mathbf{W}$ is the incident matrix. The measurement matrix is constructed as $\mathbf{H} = \begin{bmatrix} \mathbf{S}^{GG} & \mathbf{0} \\ \mathbf{0} & \mathbf{S}^{LL} \end{bmatrix} \mathbf{W}$. The $\mathbf{S}^{GG}$ and $\mathbf{S}^{LL}$ are diagonal matrices with elements equal to the susceptances of branches connected the generation buses and load buses and two load buses, respectively. To solve the nonlinear and non-convex problem (6), we adopt the monte-carlo method to approximate the optimal result.

Experimental results: Next, we evaluate the the defending perfor-

mance of MTD, the MTD's impact on the frequency stability, and the defending cost introduced by MTD. The 9-bus power system from [14] and 14-bus power systems from MATPOWER [15] are used as examples. The real-world load profiles from New York State on 20-01-2021 [16] are injected into the 14-bus power system for simulations. The perturbation ratio for each branch is calculated by $\Delta b/b$, where b is the original branch susceptance and Δb is the susceptance perturbation.

First, we analyze the FDIA detection rate and Grassmann distance with respect to the perturbation ratio. An attacking pool of FDIA attack vectors are constructed with the measurement matrix before the MTD. After the MTD, the attack vectors in the attacking pool are injected into the 9-bus system to test the defending performance of MTD in terms of detecting FDIAs. The susceptances of branches $\{1,5\}$ and $\{3,6\}$ are perturbed with the same perturbation ratio. From Fig. 1, we find that the FDIA detection rate increases with the perturbation ratio and is proportional to the Grassmann distance, which means that the Grassmann distance can represent the defending performance of MTD in terms of detecting FDIAs. We also find that the frequency stability is violated if the perturbation ratio increases to a certain value.

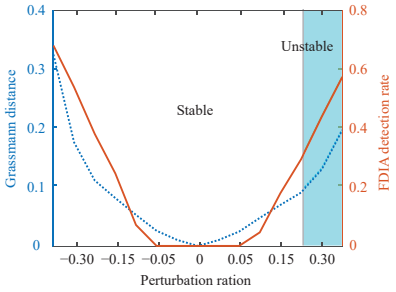

Fig. 1. Defending performance.

Second, we analyze the change of eigenvalues with respect to the perturbation ratio. Again, the susceptances of branches $\{1,5\}$ and $\{3,6\}$ are perturbed with the same perturbation ratio. The 8th and 9th eigenvalues of the second-order system (4) are used as examples. From Fig. 2, the real part of the 8th eigenvalue decreases while the 9th eigenvalue increases when the perturbation ratio increases, and the 9th eigenvalue becomes an unstable eigenvalue when the perturbation ratio is larger than 0.18 since it has positive real part. Therefore, the impact of MTD on the frequency stability can be analyzed based on the eigenvalue sensitivity against the susceptance perturbation.

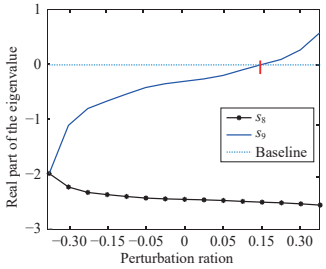

Fig. 2. Eigenvalue change w.r.t. perturbation ratio.

Third, we analyze the impact of MTD on the defending cost considering the stability and defending performance constraints. The 14-bus power system is adopted and the threshold for the defending performance is $\varsigma = 0.1$. The perturbed branches are $\{5,6\}$, $\{10,11\}$, and $\{12,13\}$. They are perturbed within the limits $[-0.2, 0.2]$. The sum of power loads is also presented in the figure. From Fig. 3, the value of ΔC fluctuates with the power loads. From the optimization problem (6), if $\Delta C > 0$, it means that the system operator can gain benefits from the generation cost by deploying the MTD. If $\Delta C < 0$, system operator needs to pay additional generation cost to deploy the MTD. The figure shows that the system operator can obtain benefits from the generation cost most of the time in the day. Therefore, it is possible for the system operator to alleviate the defending cost of MTD

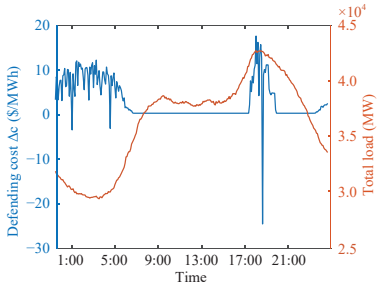

Fig. 3. Optimized defending cost.

considering the defending performance and stability constraints simultaneously.

Acknowledgments: This work was supported in part by the Guizhou Provincial Science and Technology Projects (ZK[2022]149), the Natural Science Foundation of Guizhou University ([2021]47), the GZU Cultivation project of the National Natural Science Foundation of China (NSFC) ([2020]80), NSFC (62073285, 62061130220), the Natural Science Foundation of Zhejiang Province (LZ21F020006), the Fundamental Research Funds for the Central Universities (226-2022-00120), and the Key Laboratory of Collaborative Sensing and Autonomous Unmanned Systems of Zhejiang Province.

References

[1] A. S. Musleh, G. Chen, and Z.-Y. Dong, "A survey on the detection algorithms for false data injection attacks in smart grids," *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2218–2234, May 2020.

[2] X. Liu, Z. Li, and Z. Li, "Optimal protection strategy against false data injection attacks in power systems," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1802–1810, Jul. 2017.

[3] B. Li, T. Ding, C. Huang, J. Zhao, Y. Yang, and Y. Chen, "Detecting false data injection attacks against power system state estimation with fast go-decomposition approach," *IEEE Trans. Industrial Informatics*, vol. 15, no. 5, pp. 2892–2904, May 2019.

[4] J. Qi, K. Sun, and W. Kang, "Optimal PMU placement for power system dynamic state estimation by using empirical observability," *IEEE Trans. Power Syst.*, vol. 30, no. 4, pp. 2041–2054, Jul. 2015.

[5] S. Pal, B. Sikdar, and J. H. Chow, "Classification and detection of PMU data manipulation attacks using transmission line parameters," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 5057–5066, Sept. 2018.

[6] Z. Zhang, *et al*., "Analysis of moving target defense against false data injection attacks on power grid," *IEEE Trans. Inform. Forens. Secur.*, vol. 15, no. 1, pp. 2320–2335, Feb. 2020.

[7] T. Liu, J. Tian, J. Wang, H. Wu, L. Sun, Y. Zhou, C. Shen, and X. Guan, "Integrated security threats and defense of cyber-physical systems," *Acta Automa. Sinica*, vol. 45, no. 1, pp. 5–24, Jan. 2019.

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

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

[10] S. Lakshminaraytana and D. Yau, "Cost-benefit analysis of moving-target defense in power grids," *IEEE Trans. Power Syst.*, vol. 36, no. 2, pp. 1152–1163, July. 2020.

[11] C. Liu, *et al*., "Reactance perturbation for detecting and identifying FDI attacks in power system state estimation," *IEEE J. Selected Topics Signal Processing*, vol. 12, no. 4, pp. 763–776, Aug. 2018.

[12] J.-H. Cho, *et al*., "Toward proactive, adaptive defense: A survey on moving target defense," *IEEE Commun. Surveys Tutorials*, vol. 22, no. 1, pp. 709–745, 2020.

[13] Z. Zhang, *et al*., "Zero-parameter-information data integrity attacks and countermeasures in IoT-based smart grid," *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6608–6623, Apr. 2021.

[14] S. Amini, H. Mohsenian-Rad, and F. Pasqualetti, "Dynamic load altering attacks in smart grid," in *Proc. IEEE ISGT*, Feb. 2015, pp. 1–5.

[15] R. D. Zimmerman, C. E. Murillo-Sanchez, and R. J. Thomas, "MATPOWER: Steady-state operations, planning, and analysis tools for power systems research and education," *IEEE Trans. Power Syst.*, vol. 26, no. 1, pp. 12–19, Feb. 2011.

[16] NYISO. [Online], Available: https://www.nyiso.com/load-data, 2021.