Computers, Materials & Continua

Tech Science Press

Doi:10.32604/cmc.2025.070577

ARTICLE

Mitigating the Dynamic Load Altering Attack on Load Frequency Control with Network Parameter Regulation

Yunhao Yu[1], **Boda Zhang**[1], **Meiling Dizha**[1], **Ruibin Wen**[1], **Fuhua Luo**[1], **Xiang Guo**[1] and **Zhenyong Zhang**[2,*]

[1]Electric Power Dispatching and Control Center, Guizhou Power Grid Co., Ltd., Guiyang, 550002, China

[2]State Key Laboratory of Public Big Data, College of Computer Science and Technology, Guizhou University, Guiyang, 550025, China

*Corresponding Author: Zhenyong Zhang. Email: zyzhangnew@gmail.com

Received: 19 July 2025; Accepted: 24 September 2025; Published: 09 December 2025

ABSTRACT: Load frequency control (LFC) is a critical function to balance the power consumption and generation. The grid frequency is a crucial indicator for maintaining balance. However, the widely used information and communication infrastructure for LFC increases the risk of being attacked by malicious actors. The dynamic load altering attack (DLAA) is a typical attack that can destabilize the power system, causing the grid frequency to deviate from its nominal value. Therefore, in this paper, we mathematically analyze the impact of DLAA on the stability of the grid frequency and propose the network parameter regulation (NPR) to mitigate the impact. To begin with, the dynamic LFC model is constructed by highlighting the importance of the network parameter. Then, we model the DLAA and analyze its impact on LFC using the theory of second-order dynamic systems. Finally, we model the NPR and prove its effect in mitigating the DLAA. Besides, we construct a least-effort NPR considering its infrastructure cost and aim to reduce the operation cost. Finally, we carry out extensive simulations to demonstrate the impact of the DLAA and evaluate the mitigation performance of NPR. The proposed cost-benefit NPR approach can not only mitigate the impact of DLAA with 100% and also save 41.18 $/MWh in terms of the operation cost.

KEYWORDS: Smart grid cybersecurity; dynamic load altering attack; load frequency control; network parameter modification

1 Introduction

Load frequency control (LFC) plays a crucial role in maintaining the grid's frequency at a nominal value. Through the Supervisory Control and Data Acquisition (SCADA) system, LFC can efficiently handle frequency issues in a wide area. However, as more and more devices are operated through the open communication network, the number of exposed vulnerabilities increases at an unexpected rate. Therefore, the LFC is facing cyber threats from different attack entry points. The power loads on the consumer side can be maliciously modified due to the widespread deployment of charging stations [1]. The attack events indicate that the attacker has the capability to take over the electricity equipment and disrupt the system's regular operation. The researcher at Argonne National Laboratory destroyed a generator within 100 lines of code [2]. The attacker can modify vulnerable loads, such as intelligent appliances based on the Internet of Things (e.g., air conditioners and electric vehicles), to cause frequency deviation or transmission line overloading [3,4].

The attack on power loads can be divided into two types: load measurement attack and load altering attack. For the load measurement attack, only the load measurements are compromised, while the actual loads remain unchanged. The goal of the load measurement attack is to bypass bad data detection, such as the load redistribution attack [5] and the false data injection attack [6]. This attack aims to cheat the operator into redistributing the generation and cause an increase or decrease in the nodal price [7]. The load redistribution attack maintains the sum of loads unchanged, which corresponds to the generation cost for both the pre- and post-real-time dispatch [8]. The dummy data attack enhances the stealthiness of the load measurement attack by concealing the measurements among normal measurements [9]. This attack can bypass the cluster-based and machine learning-based detectors. As for the load-altering attack, the actual power load is physically altered. The goal of the load-altering attack is to destabilize the power system. The static load-altering attack modifies the frequency-insensitive load to cause frequency excursion [10]. The dynamic load altering attack (DLAA) corrupts the frequency-sensitive loads to cause frequency deviation [11]. By analyzing the trajectory of the frequency change, the attacker can manipulate the load by changing the price signals in price-based demand response programs. The electronic vehicles can also be used as targets of the DLAA [4]. Although the DLAA has been revealed to be vulnerable, its principle in affecting system stability, especially grid frequency, still needs to be analyzed in depth.

To defend against the attack on power loads, various approaches exist from the aspects of detection, identification, and mitigation. The sliding model observer is used to estimate the system states to detect the abnormal states [12]. A robust sliding mode observer can detect the DLAA with the signal residual [13]. The low-rank Kalman filter can be used to estimate the attack parameter using the rank-1 method [14]. The physics-informed machine learning algorithm is a data-driven approach that can detect and localize the abnormal load measurements [15]. The Fast Fourier Transform can be used to analyze the spectral and further localize the attacked load measurements [16]. A significant and robust machine learning model was proposed to mitigate the false data injection attack (FDIA) in dynamic line rating systems, focusing on statistical data processing, feature ranking, selection, training, validation, and evaluation [17]. Multiple metrics were proposed in this reference to evaluate the detection performance of FDIAs with BGLM-LR, Gaussian naive Bayes (GNB), linear support vector machine (LSVM), wide neural network (WNN), and decision tree (DT). As a precise measurement device, the data collected from the phasor measurement unit (PMU) can be used to localize the abnormal load measurements and states combined with a convolutional neural network. From the perspective of information security, unauthorized load control signals are prevented by minimizing access permissions based on the edge-computing infrastructure [18]. The generation-consumption imbalance can be captured by the fast-acting inverter [19]. The charge and discharge actions of the electric vehicles can be used to compensate for the DLAA impact [20]. Although the above approaches are practical in defending against the attacks on the power loads, they work reactively. However, the mitigation strategy should be proactive and mitigate the impact of DLAA on the physical side.

As a proactive defense strategy, the network parameter regulation (NPR) approach leverages the physical property. Compared to cyber defense, NPR focuses on the physical side, enhancing the integration of cyber and physical systems. In this paper, the NPR is realized using a series capacitor compensator (SCC), a typical device designed to stabilize the system. Since the power system must operate close to its limits to meet high demand and profit goals, the SCC device is used to maintain the grid's safety when it is on a large scale and distributed renewable energies are highly penetrated. Since the SCC has the capability to modify capacitance injection, it can be used to create a proactive defense mechanism from the physical side.

Therefore, with a special emphasis on the DLAA, we propose an NPR strategy to mitigate the impact of the attack on the stability of the grid frequency. To reveal the insight why the DLAA can cause grid frequency divergence, we model the DLAA and analyze its effect on the stability of the grid frequency with a second-order dynamic system. For NPR, it is designed to alleviate the DLAA by maintaining the stable modes. As the deployment of NPR may introduce additional costs, an optimization problem is formulated to develop a cost-effective defense strategy. In summary, the contributions are as follows: (1) First, we model the DLAA using both the first-order and second-order dynamic systems. The DLAA's impact on the stability of the grid frequency is analyzed with the eigenvalue sensitivity; (2) Second, we theoretically reveal the effect of NPR to mitigate the DLAA by guaranteeing the Lyapunov criteria; (3) Third, we conduct extensive simulations to demonstrate the impact of the DLAA and evaluate the defense performance of NPR.

2 Background Knowledge

2.1 Power Network Model

The power system operates stably by balancing the generation and load. To represent the power network, the power facilities are described by generation buses and load buses. The generation bus is equipped with a generator, and the load bus has a load consumption. The generation buses are included in the set $\mathbb{G}$, and the load buses are contained in the set $\mathbb{L}$. Overall, suppose the power system has N_1 load buses and N_2 generation buses. Given a bus, it is either a generation bus or a load bus. The power transmission network is described by $\mathcal{G} =< \mathbb{G}, \mathbb{L}, \mathbb{T} >$. The transmission lines are included in $\mathbb{T}$. The transmission line $t \doteq \{i, j\} \in \mathbb{T}$. Considering the DC power flow model [21] for the transmission line $t \doteq \{i, j\}$, the power injection and power consumption equations are modeled by

$$P_i^I = \sum_{j \in \mathbb{G}} s_{ij}(\phi_i - \phi_j) + \sum_{j \in \mathbb{L}} s_{ij}(\phi_i - \theta_j), \quad \forall i \in \mathbb{G}, P_i^L = -\sum_{j \in \mathbb{G}} s_{ij}(\theta_i - \phi_j) - \sum_{j \in \mathbb{L}} s_{ij}(\theta_i - \theta_j), \quad \forall i \in \mathbb{L}, \tag{1}$$

where P_i^I is the power injection of the i^{th} generation bus, P_i^L is the power load of the i^{th} load bus, ϕ_i is the voltage phase angle of the i^{th} generator bus, θ_i is the voltage phase angle of the i^{th} load bus, and s_{ij} is susceptance (i.e., the reciprocal of the reactance) of branch t.

Considering the overall power transmission network, the power flow model according to (1) is described as follows:

$$\mathbf{P}^L = -\mathbf{S}^{\mathbb{L}\mathbb{L}}\boldsymbol{\theta} - \mathbf{S}^{\mathbb{L}\mathbb{G}}\boldsymbol{\phi}, \mathbf{P}^I = \mathbf{S}^{\mathbb{G}\mathbb{G}}\boldsymbol{\phi} + \mathbf{S}^{\mathbb{G}\mathbb{L}}\boldsymbol{\theta}, \tag{2}$$

where $\mathbf{P}^L \in \mathbb{R}^{N_1}$ and $\mathbf{P}^I \in \mathbb{R}^{N_2}$ are the vector of power loads and the vector of power injections, $\boldsymbol{\phi} = [\phi_1, \phi_2, \cdots, \phi_{N_1}]^T \in \mathbb{R}^{N_1}$ is a vector of voltage phase angles of generator buses, and $\boldsymbol{\theta} = [\theta_1, \theta_2, \cdots, \theta_{N_2}]^T \in \mathbb{R}^{N_2}$ is a vector of voltage phase angles of load buses. The matrices $\mathbf{S}^{\mathbb{G}\mathbb{G}}$, $\mathbf{S}^{\mathbb{G}\mathbb{L}}$, $\mathbf{S}^{\mathbb{L}\mathbb{L}}$, and $\mathbf{S}^{\mathbb{L}\mathbb{G}}$ are derived according to the network parameters and system topology given in (1).

Suppose the load buses are numbered with the first N_1 indices and the generation buses are numbered with the rest N_2 indices. The power system has $N = N_1 + N_2$ buses. The transmission lines that connect the generation and load buses are denoted by a set $\mathbb{T}^{\text{GG}}$. The susceptance matrix (in a diagonal form) corresponding to $\mathbb{T}^{\text{GG}}$ is $\mathbf{B}^{\mathbb{G}\mathbb{G}}$, which is constructed by setting the element at the position (t, t) as s_{ij} for the line t. By denoting the transmission lines that connect to only load buses (start and end at load buses), the corresponding diagonal matrix is $\mathbf{B}^{\mathbb{L}\mathbb{L}}$. To describe the system topology, the incident matrix $\mathbf{R}$ is given and is constructed as a sparse matrix, whose t^{th} row is a sparse vector with one at the i^{th} position and –1 at the j^{th} position, and otherwise are zeros. With the above matrices, we can derive that

$$\mathbf{S}^{GG} = \mathbf{B}^{GG}, \mathbf{S}^{GL} = \begin{bmatrix} -\mathbf{B}^{GG} & \mathbf{0} \end{bmatrix}, \mathbf{S}^{LL} = \mathbf{R}^T \begin{bmatrix} \mathbf{B}^{GG} & \mathbf{0} \\ \mathbf{0} & \mathbf{B}^{LL} \end{bmatrix} \mathbf{R}, \mathbf{S}^{LG} = \begin{bmatrix} -\mathbf{B}^{GG} \\ \mathbf{0} \end{bmatrix}, \tag{3}$$

where $\mathbf{0}$ is a matrix of appropriate size to form the larger matrix.

2.2 System Dynamic Model

Next, we introduce the system's dynamic model for maintaining the grid frequency. The swing equation for the generator is

$$\dot{\phi}_i = \nu_i, \nu_i \dot{\omega}_i = -d_i \nu_i + P_i^M - P_i^I, \tag{4}$$

where the roof mark $\cdot$ denotes the derivative operation, ν_i is the frequency deviation from the nominal frequency, $m_i > 0$ is the inertial factor, $d_i > 0$ is the damping ratio, and P_i^M is the mechanical power output. The grid frequency is maintained using a proportional-integral (PI) control strategy. The PI structure is $P_i^M = -(K_i^P \nu_i + K_i^I \phi_i)$, where $K_i^P > 0$ and $K_i^I > 0$ are control coefficients.

The input of the PI controller is the area control error (ACE) signal. The ACE is a reference to draw the deviations of the grid frequency and the power flow of the tie line to zero. The i^{th} generator outputs the mechanical power following the value $P_i^M = P_i^{\text{ref}} - \frac{1}{H_i}\omega_i$, where P_i^{ref} is the power reference and H_i is the regulation constant. For the i^{th} generator, the ACE signal is given by $\text{ACE}_i = \Delta P_i^{\text{tie}} + W_i \nu_i$, where ΔP_i^{tie} is the deviation of the power flow of the tie-line and W_i is a constant. The power reference is given by $P_i^{\text{ref}} = -K_i \int \text{ACE}_i dt$. Hence, the PI control strategy is obtained as $P_i^M = -(K_i^P \nu_i + K_i^I \phi_i)$, where $K_i^P = \frac{1}{H_i}$ and $K_i^I = K_i W_i$.

For each load, it can be categorized into two types: frequency-sensitive and constant. That is, the i^{th} load is constructed by $P_i^L = F_i \phi_i + P_i^0$, where $F_i > 0$ is the factor of the frequency-sensitive load and P_i^0 is the frequency-insensitive load. The following relationship holds for the angle transformation [10], that is, $\boldsymbol{\eta} = -\dot{\boldsymbol{\theta}}$, where $\boldsymbol{\eta} \in \mathbb{R}^{N_1}$ is a vector of frequency deviations of load buses and $\boldsymbol{\theta} \in \mathbb{R}^{N_1}$ is a vector of voltage phase angles of load buses.

Considering the overall power system, we obtain the following relationship:

$$\mathbf{P}^L = \mathbf{F}\boldsymbol{\eta} + \mathbf{P}^0, \tag{5}$$

where $\mathbf{F} \in \mathbb{R}^{N_1 \times N_1}$ is a diagonal matrix with the element at the position (i, i) is F_i and $\mathbf{P}^0 \in \mathbb{R}^{N_1}$ is a vector of frequency-insensitive loads. By eliminating $\boldsymbol{\eta}$, we have

$$\begin{bmatrix} \mathbf{I} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{I} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & -\mathbf{M} \end{bmatrix} \begin{bmatrix} \dot{\boldsymbol{\phi}} \\ \dot{\boldsymbol{\theta}} \\ \dot{\boldsymbol{\nu}} \end{bmatrix} = \begin{bmatrix} \mathbf{0} & \mathbf{0} & \mathbf{I} \\ \mathbf{F}^{-1}\mathbf{S}^{\mathbb{L}\mathbb{G}} & \mathbf{F}^{-1}\mathbf{S}^{\mathbb{L}\mathbb{L}} & \mathbf{0} \\ \mathbf{K}^I + \mathbf{S}^{\mathbb{G}\mathbb{G}} & \mathbf{S}^{\mathbb{G}\mathbb{L}} & \mathbf{K}^P + \mathbf{D} \end{bmatrix} \begin{bmatrix} \boldsymbol{\phi} \\ \boldsymbol{\theta} \\ \boldsymbol{\nu} \end{bmatrix} + \begin{bmatrix} \mathbf{0} \\ \mathbf{F}^{-1} \\ \mathbf{0} \end{bmatrix} \mathbf{P}^0, \tag{6}$$

where $\boldsymbol{\nu} \in \mathbb{R}^{N_2}$ is the frequency deviation vector, $\mathbf{M} \in \mathbb{R}^{N_2 \times N_2}$, $\mathbf{D} \in \mathbb{R}^{N_2 \times N_2}$, $\mathbf{K}^P \in \mathbb{R}^{N_2 \times N_2}$, and $\mathbf{K}^I \in \mathbb{R}^{N_2 \times N_2}$ are diagonal matrices corresponding to the inertial, damping ratio, proportional, and integral factors, respectively. The matrix $\mathbf{I}$ is an identity matrix of appropriate size. Suppose the state variable is $\mathbf{X} = \begin{bmatrix} \boldsymbol{\phi} & \boldsymbol{\theta} & \boldsymbol{\nu} \end{bmatrix}^T$ and $\mathbf{U} = \begin{bmatrix} \mathbf{0} \\ \mathbf{F}^{-1} \\ \mathbf{0} \end{bmatrix} \mathbf{P}^0$, we can derive that

$$\dot{\mathbf{X}} = \mathbf{A}\mathbf{X} + \mathbf{U}, \tag{7}$$

where, $\mathbf{A} = \begin{bmatrix} \mathbf{I} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{I} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & -\mathbf{M} \end{bmatrix}^{-1} \begin{bmatrix} \mathbf{0} & \mathbf{0} & \mathbf{I} \\ \mathbf{F}^{-1}\mathbf{S}^{\mathbb{L}\mathbb{G}} & \mathbf{F}^{-1}\mathbf{S}^{\mathbb{L}\mathbb{L}} & \mathbf{0} \\ \mathbf{K}^I + \mathbf{S}^{\mathbb{G}\mathbb{G}} & \mathbf{S}^{\mathbb{G}\mathbb{L}} & \mathbf{K}^P + \mathbf{D} \end{bmatrix}$.

Our use of a linearized second-order model is intentional and aligns with standard practices in power system stability analysis, especially for frequency stability studies in LFC contexts. This approximation is valid around the system's equilibrium operating point, where perturbations (such as those induced by dynamic load altering attacks, or DLAAs) are assumed to be small enough that higher-order terms can be neglected. The model enables us to analytically derive the impact of DLAA on system eigenvalues and the mitigating effects of network parameter regulation (NPR) using tools such as eigenvalue sensitivity and Lyapunov criteria, providing clear theoretical insights into stability margins. Similar linearizations are commonly employed in the LFC literature (e.g., [10,11,20]) to facilitate a tractable analysis without compromising essential dynamics for frequency regulation scenarios.

To validate the model's applicability, our extensive simulations in Section 4 incorporate more realistic system conditions, including time-domain responses to DLAA perturbations in multi-area power systems (e.g., IEEE 39-bus test case). These simulations demonstrate that the linear model's predictions hold well for the attack magnitudes and system stresses considered, where frequency deviations remain within ranges typical for LFC (e.g., ±0.5 Hz). However, we recognize that under extreme stress conditions—such as high renewable penetration leading to low inertia or cascading failures—the non-linear effects could become pronounced, potentially altering the DLAA's impact or NPR's effectiveness.

2.3 Dynamic Load Altering Attack

Recently, cyberattacks on power systems have increased due to the tense relationship between countries. The smart infrastructure introduces plenty of uncertainties into the power system operation [22,23]. Electric vehicles and distributed generators impact the security and safety of the smart grid. As a great economic system, targeting the power system is attractive to attackers. Especially, the smart and IP-enabled power load infrastructure is vulnerable to intrusions [24]. Smart home appliances have been proven vulnerable to botnet attacks [25]. Since the load is on the user's side, it can be easily altered by the attacker. Considering the adversarial loads, the dynamic load altering attack (DLAA) is constructed like $\tilde{P}_i^L = \pi_i F_i \phi + P^0$, where π_i is the attack coefficient against the i^{th} vulnerable load for DLAA. Thus, the attacker targets the frequency-sensitive load. Overall, the DLAA is constructed as

$$\tilde{\mathbf{P}}^L = \Pi \mathbf{F} \boldsymbol{\phi} + \mathbf{P}^0, \tag{8}$$

where $\Pi \in \mathbb{R}^{N_1 \times N_1}$ is a diagonal matrix with the diagonal element equal to π_i. If the i^{th} load is vulnerable, then $\pi_i \neq 0$; otherwise, $\pi_i = 0$.

According to the Lyapunov stability theory, the system is asymptotically stable if and only if all eigenvalues of the matrix $\mathbf{A}$ have negative real parts [26]. After DLAA, the system matrix becomes

$$\tilde{\mathbf{A}} = \begin{bmatrix} \mathbf{I} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{I} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & -\mathbf{M} \end{bmatrix}^{-1} \begin{bmatrix} \mathbf{0} & \mathbf{0} & \mathbf{I} \\ (\Pi \mathbf{F})^{-1} \mathbf{S}^{\mathbb{L}\mathbb{G}} & (\Pi \mathbf{F})^{-1} \mathbf{S}^{\mathbb{L}\mathbb{L}} & \mathbf{0} \\ \mathbf{K}^I + \mathbf{S}^{\mathbb{G}\mathbb{G}} & \mathbf{S}^{\mathbb{G}\mathbb{L}} & \mathbf{K}^P + \mathbf{D}. \end{bmatrix} \tag{9}$$

Therefore, once the matrix $\tilde{\mathbf{A}}$ has eigenvalues that have non-negative real parts, then the asymptotic stability of the system cannot be guaranteed.

3 Mitigating DLAA with NPR

To defend against the DLAA and maintain the stability of the grid frequency, we propose a network parameter regulation (NPR) approach by changing the line parameter (i.e., the susceptance). Hence, in the following, we first introduce the principle of NPR. Then, we model the system as a second-order dynamic system. Based on this model, we analyze the impact of DLAA and the mitigation effect of NPR.

3.1 Network Parameter Regulation

The implementation of NPR depends on the capacitor compensation device, which can actively change the line parameters, such as reactance. For example, the thyristor-controlled series capacitor device is remotely controlled and monitored by the supervisory control and data acquisition (SCADA) system. Therefore, the line parameter can be changed flexibly.

The modified susceptance is modelled as

$$s_{ij} = s_{ij}^{\text{ref}} + s_{ij}^{\text{fix}}, \tag{10}$$

where s_{ij} is the susceptance injected into the line, s_{ij}^{fix} is the initialized operating point, s_{ij}^{ref} is the targeted reference value. Therefore, if the reference value s_{ij}^{ref} is changed, then the matrices $\mathbf{S}^{\mathbb{LG}}$, $\mathbf{S}^{\mathbb{LL}}$, $\mathbf{S}^{\mathbb{GG}}$, and $\mathbf{S}^{\mathbb{GL}}$ are changed accordingly. Subsequently, the system matrix $\mathbf{A}$ is also changed. Therefore, the impact of DLAA can be alleviated and even eliminated with NPR.

3.2 Second-Order Description of the Dynamic System

To clearly describe the effect of NPR against DLAA, we transform the first-order dynamic model into a second-order dynamic model, which is given by

$$\begin{bmatrix} \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{M} \end{bmatrix} \begin{bmatrix} \ddot{\boldsymbol{\eta}} \\ \ddot{\boldsymbol{\nu}} \end{bmatrix} + \begin{bmatrix} -\mathbf{F} & \mathbf{0} \\ \mathbf{0} & \mathbf{K}^P + \mathbf{D} \end{bmatrix} \begin{bmatrix} \dot{\boldsymbol{\eta}} \\ \dot{\boldsymbol{\nu}} \end{bmatrix} + \begin{bmatrix} \mathbf{S}^{\mathbb{LL}} & -\mathbf{S}^{\mathbb{LG}} \\ -\mathbf{S}^{\mathbb{LL}} & \mathbf{K}^I + \mathbf{S}^{\mathbb{GG}} \end{bmatrix} \begin{bmatrix} \boldsymbol{\eta} \\ \boldsymbol{\nu} \end{bmatrix} = \mathbf{0} \tag{11}$$

To be concise, the transformed matrices are represented with

$$\mathcal{A} = \begin{bmatrix} \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{M} \end{bmatrix}, \mathcal{B} = \begin{bmatrix} -\mathbf{F} & \mathbf{0} \\ \mathbf{0} & \mathbf{K}^P + \mathbf{D} \end{bmatrix}, \mathcal{C} = \begin{bmatrix} \mathbf{S}^{\mathbb{LL}} & -\mathbf{S}^{\mathbb{LG}} \\ -\mathbf{S}^{\mathbb{LL}} & \mathbf{K}^I + \mathbf{S}^{\mathbb{GG}} \end{bmatrix}. \tag{12}$$

With the second-order dynamic model, the eigenvalues also represent the system's stability. The stability issue can be solved using the right and left eigenvalue problems, which are described with the following equations:

$$\beta_i^2 \mathcal{A}\mathbf{r}_i + \beta_i \mathcal{B}\mathbf{r}_i + \mathcal{C}\mathbf{r}_i = \mathbf{0}, \beta_i^2 \mathbf{l}_i^T \mathcal{A} + \beta_i \mathbf{l}_i^T \mathcal{B} + \mathbf{l}_i^T \mathcal{C} = \mathbf{0}, \tag{13}$$

where β_i is the i^{th} eigenvalue (i.e., latent root), $\vec{\mathbf{r}}_i$ and $\vec{\mathbf{l}}_i$ are the i^{th} right and left eigenvectors (i.e., latent vectors), respectively. By solving for the eigenvalues, we can determine the stability condition for the dynamic system based on the real parts of the eigenvalues. Next, we analyze the impact of DLAA and the effect of NPR on the eigenvalues.

3.3 Impact of the DLAA

First, we analyze the impact of DLAA on the eigenvalues. Under the adversarial case, the matrix $\mathcal{B}$ is changed to be $\tilde{\mathcal{B}} = \begin{bmatrix} -\Pi\mathbf{F} & \mathbf{O} \\ \mathbf{O} & \mathbf{K}^P + \mathbf{D} \end{bmatrix}$. From [27,28], we can derive the sensitivity of the eigenvalue against the DLAA. The first-order derivative of the i^{th} eigenvalue β_i is computed by

$$\frac{\partial \beta_i(\Pi)}{\partial \Pi} = -\frac{\mathbf{l}_i^T \left(\beta_i^2 \frac{\partial \mathcal{A}}{\partial \Pi} + \beta_i \frac{\partial \mathcal{B}}{\partial \Pi} + \frac{\partial \mathcal{C}}{\partial \Pi} \right) \mathbf{r}_i}{\mathbf{l}_i^T (2\beta_i \mathcal{A} + \mathcal{B}) \mathbf{r}_i}. \tag{14}$$

Since the matrices $\mathcal{A}$ and $\mathcal{C}$ are not affected by the DLAA, the derivatives of $\mathcal{A}$ and $\mathcal{C}$ with respect to the attack parameter Π are zero. Hence, we can derive that

$$\frac{\partial\beta_i(\Pi)}{\partial\Pi} = -\frac{\mathbf{l}_i^T\left(\beta_i\dfrac{\partial\mathcal{B}}{\partial\Pi}\right)\mathbf{r}_i}{\mathbf{l}_i^T(2\beta_i\mathcal{A}+\mathcal{B})\mathbf{r}_i}. \tag{15}$$

Suppose the set of vulnerable loads is $\mathbb{K}$, we have

$$\frac{\partial\beta_i(\Pi)}{\partial\Pi} = \sum_{j\in\mathbb{K}}\frac{\partial\beta_i(\pi_j)}{\partial\pi_j}, \frac{\partial\mathcal{B}}{\partial\Pi} = \sum_{j\in\mathbb{K}}\frac{\partial\mathcal{B}(\pi_j)}{\partial\pi_j}. \tag{16}$$

Therefore, under the DLAA, the i^{th} eigenvalue becomes

$$\tilde{\beta}_i = \beta_i + \sum_{j\in\mathbb{K}}\frac{\partial\beta_i(\pi_j)}{\partial\pi_j}\pi_j = \beta_i - \frac{\mathbf{l}_i^T\left(\beta_i\sum_{j\in\mathbb{K}}\dfrac{\partial\mathcal{B}(\pi_j)}{\partial\pi_j}\pi_j\right)\mathbf{r}_i}{\mathbf{l}_i^T(2\beta_i\mathcal{A}+\mathcal{B})\mathbf{r}_i}. \tag{17}$$

The second term is the impact of DLAA on the eigenvalue. By quantifying the impact of DLAA, the i^{th} eigenvalue is affected by

$$\Delta_i^{\text{DLAA}} = \text{Rel}(\beta_i) - \text{Rel}\left(\frac{\mathbf{l}_i^T\left(\beta_i\sum_{j\in\mathbb{K}}\dfrac{\partial\mathcal{B}(\pi_j)}{\partial\pi_j}\pi_j\right)\mathbf{r}_i}{\mathbf{l}_i^T(2\beta_i\mathcal{A}+\mathcal{B})\mathbf{r}_i}\right), \tag{18}$$

where $\text{Rel}(*)$ computes the real part of the complex value. Therefore, once $\Delta_i^{\text{DLAA}} > 0$, then the system is unstable. The grid frequency under the DLAA deviates from the nominal value (i.e., 50 or 60 Hz). To detail the attack process of the DLAA, we provide a flowchart in Fig. 1a. The attacker follows the flowchart to execute the attack and determine whether the attack is successful or not.

3.4 *Effect of NPR*

Next, we evaluate the effect of NPR on mitigating the impact of the DLAA. With NPR, by changing the line parameter s_{ij} into $\tilde{s}_{ij}$ (the line $\{i,j\}$ can be any line in the power transmission network), the matrices $\mathbf{S}^{\mathbb{LG}}$, $\mathbf{S}^{\mathbb{LL}}$, $\mathbf{S}^{\mathbb{GG}}$, and $\mathbf{S}^{\mathbb{GL}}$ are changed into $\tilde{\mathbf{S}}^{\mathbb{LG}}$, $\tilde{\mathbf{S}}^{\mathbb{LL}}$, $\tilde{\mathbf{S}}^{\mathbb{GG}}$, and $\tilde{\mathbf{S}}^{\mathbb{GL}}$. Thus, the matrix $\mathcal{C}$ is changed accordingly, that is, $\tilde{\mathcal{C}} = \begin{bmatrix}\tilde{\mathbf{S}}^{\mathbb{LL}} & -\tilde{\mathbf{S}}^{\mathbb{LG}}\\ -\tilde{\mathbf{S}}^{\mathbb{LL}} & \mathbf{K}^I + \tilde{\mathbf{S}}^{\mathbb{GG}}\end{bmatrix}$. Therefore, we can derive the effect of NPR as follows. For the i^{th} eigenvalue β_i, its sensitivity against the line parameter change is

$$\frac{\partial\beta_i(\tilde{s}_{ij})}{\partial\tilde{s}_{ij}} = -\frac{\mathbf{l}_i^T\left(\beta_i^2\dfrac{\partial\mathcal{A}}{\partial\tilde{s}_{ij}} + \beta_i\dfrac{\partial\mathcal{B}}{\partial\tilde{s}_{ij}} + \dfrac{\partial\tilde{\mathcal{C}}}{\partial\tilde{s}_{ij}}\right)\mathbf{r}_i}{\mathbf{l}_i^T(2\beta_i\mathcal{A}+\mathcal{B})\mathbf{r}_i}. \tag{19}$$

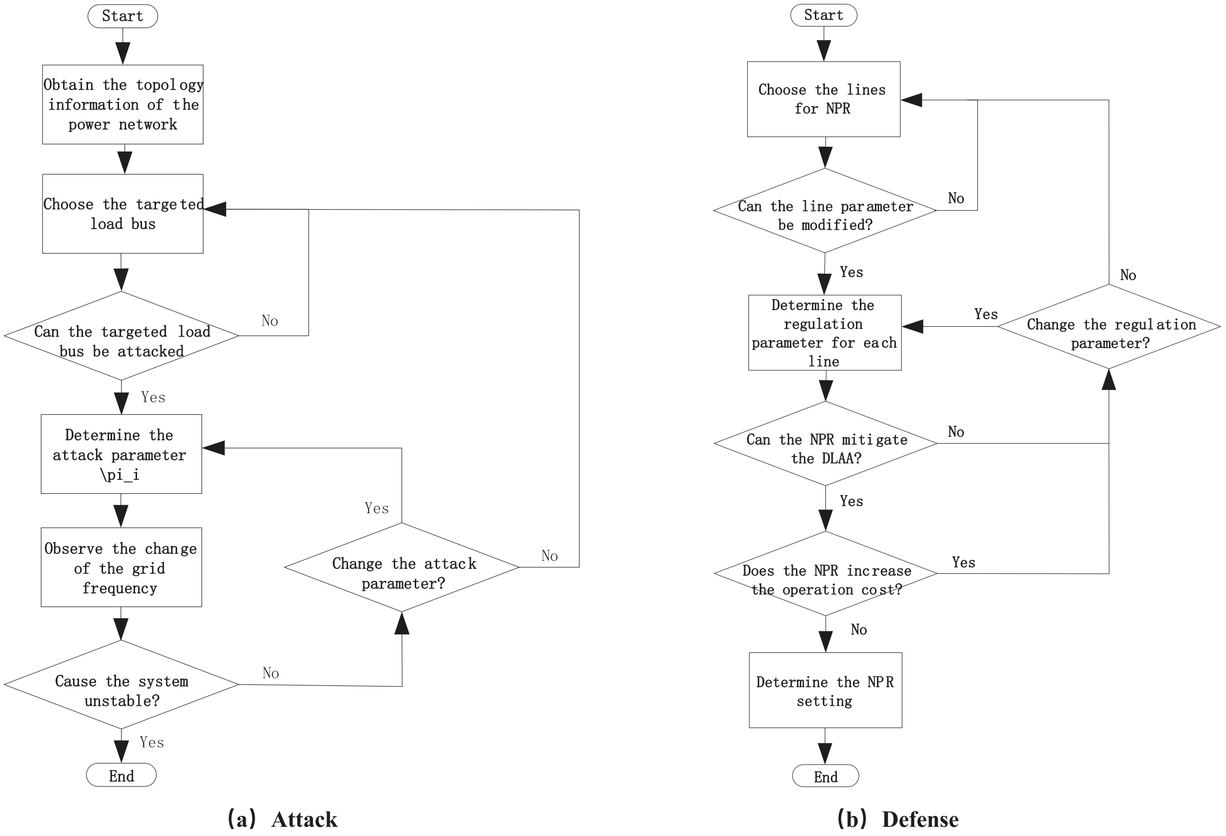

Start
Obtain the topology information of the power network
Choose the targeted load bus
Can the targeted load bus be attacked
No
Yes
Determine the attack parameter \pi_i
Observe the change of the grid frequency
Change the attack parameter?
Yes
No
Cause the system unstable?
No
Yes
End
(a) Attack
Start
Choose the lines for NPR
Can the line parameter be modified?
No
Yes
Determine the regulation parameter for each line
Change the regulation parameter?
Yes
No
Can the NPR mitigate the DLAA?
No
Yes
Does the NPR increase the operation cost?
Yes
No
Determine the NPR setting
End
(b) Defense

Figure 1: The flowcharts for the attack process of the DLAA and the defense process of the NPR

Since the matrices $\mathcal{A}$ and $\mathcal{B}$ are not changed by NPR, the derivatives of them against $\tilde{s}_{ij}$ are 0 s. Therefore, the effect of NPR can be described by

$$\frac{\partial \beta_i(\tilde{s}_{ij})}{\partial \tilde{s}_{ij}} = -\frac{\mathbf{l}_i^T \left(\dfrac{\partial \tilde{\mathcal{C}}}{\partial \tilde{s}_{ij}} \right) \mathbf{r}_i}{\mathbf{l}_i^T (2\beta_i \mathcal{A} + \mathcal{B}) \mathbf{r}_i}. \tag{20}$$

Therefore, the i^{th} eigenvalue after NPR is

$$\tilde{\beta}_i' = \beta_i - \frac{\mathbf{l}_i^T \left(\dfrac{\partial \tilde{\mathcal{C}}}{\partial \tilde{s}_{ij}} \right) \mathbf{r}_i}{\mathbf{l}_i^T (2\beta_i \mathcal{A} + \mathcal{B}) \mathbf{r}_i}. \tag{21}$$

If the NPR includes a set $\mathbb{M}$ of transmission lines, then we can quantify the effect of NPR on the i^{th} eigenvalue as

$$\Delta_i^{\text{NPR}} = \text{Rel}(\beta_i) - \text{Rel}\left(\frac{\mathbf{l}_i^T \left(\sum_{\{i,j\} \in \mathbb{M}} \dfrac{\partial \tilde{\mathcal{C}}}{\partial \tilde{s}_{ij}} \right) \mathbf{r}_i}{\mathbf{l}_i^T (2\beta_i \mathcal{A} + \mathcal{B}) \mathbf{r}_i} \right). \tag{22}$$

From the defender's perspective, $\Delta_i^{\mathrm{NPR}} < 0$ is the basic requirement. The NPR cannot affect the system's stability.

Next, if the NPR is used to mitigate the DLAA, then we have

$$\tilde{\beta}_i'' = \beta_i - \frac{\mathbf{l}_i^T \left(\beta_i \sum_{j \in \mathbb{K}} \frac{\partial \mathcal{B}(\pi_j)}{\partial \pi_j} \pi_j \right) \mathbf{r}_i}{\mathbf{l}_i^T (2\beta_i \mathcal{A} + \mathcal{B}) \mathbf{r}_i} - \frac{\mathbf{l}_i^T \left(\sum_{\{i,j\} \in \mathbb{M}} \frac{\partial \tilde{\mathcal{C}}}{\partial \tilde{s}_{ij}} \right) \mathbf{r}_i}{\mathbf{l}_i^T (2\beta_i \mathcal{A} + \mathcal{B}) \mathbf{r}_i}. \tag{23}$$

Therefore, the mitigation effect of the NPR for defending against the DLAA is given by

$$\begin{aligned} \Delta_i^{\mathrm{mit}} &= \mathrm{Rel}(\beta_i) - \mathrm{Rel}\left(\frac{\mathbf{l}_i^T \left(\beta_i \sum_{j \in \mathbb{K}} \frac{\partial \mathcal{B}(\pi_j)}{\partial \pi_j} \pi_j \right) \mathbf{r}_i}{\mathbf{l}_i^T (2\beta_i \mathcal{A} + \mathcal{B}) \mathbf{r}_i} \right) - \mathrm{Rel}\left(\frac{\mathbf{l}_i^T \left(\sum_{\{i,j\} \in \mathbb{M}} \frac{\partial \tilde{\mathcal{C}}}{\partial \tilde{s}_{ij}} \right) \mathbf{r}_i}{\mathbf{l}_i^T (2\beta_i \mathcal{A} + \mathcal{B}) \mathbf{r}_i} \right) \\ &= \Delta_i^{\mathrm{DLAA}} + \Delta_i^{\mathrm{NPR}} - \mathrm{Rel}(\beta_i). \end{aligned}$$

The goal of NPR is to make $\Delta_i^{\mathrm{mit}} < 0$. Therefore, the effectiveness of NPR is quantified by Δ_i^{mit}. The computation of (17) and (23) is given as follows. Since the matrix $\tilde{\mathcal{B}}$ is a diagonal matrix, the matrix $\sum_{j=1}^{N_1} \frac{\partial \beta_i(\pi_j)}{\partial \pi_j} \pi_j$ is sparse. Only the element corresponding to the vulnerable load (i.e., the frequency-sensitive load) is equal to π_i, and all other elements are 0. According to the model (3), the matrix $\tilde{\mathcal{C}}$ is also a sparse matrix. The derivative result $\sum_{j=1}^{N_1} \frac{\partial \mathcal{B}(\pi_j)}{\partial \pi_j} \pi_j$ is a constant matrix. As for the computation related to the right and left eigenvectors, the reference [27] provides an efficient approach. One way to speed up the computation is to normalize the term $\mathbf{l}_i^T (2\beta_i \mathcal{A} + \mathcal{B}) \mathbf{r}_i$ as 1 [28].

3.5 Cost-Effective NPR

From above, we have proved that the NPR can mitigate the impact of DLAA. However, a random NPR might introduce additional operational and infrastructure costs. Therefore, the NPR should be strategically designed to save on defense costs. As for NPR, the infrastructure cost can be defined by the difference of the reference susceptance injected into the capacitor compensation device, that is,

$$\Delta s_{ij}^{\mathrm{ref}} = |\tilde{s}_{ij}^{\mathrm{ref}} - s_{ij}^{\mathrm{ref}}|, \{i, j\} \in \mathbb{M} \tag{24}$$

where $\tilde{s}_{ij}^{\mathrm{ref}}$ is the susceptance reference after NPR and s_{ij}^{ref} is the original susceptance reference. Hence, the overall infrastructure cost is $\sum_{\{i,j\} \in \mathbb{M}} \Delta s_{ij}^{\mathrm{ref}}$. Since the change of the physical parameter affects the operating point, the generation cost might increase. The optimal power flow (OPF) is typically used to analyze changes in generation cost. Normally, the OPF is formulated and solved as a constrained optimization problem, that is,

$$C_0 = \min_{\mathbf{P^G}} \quad G(\mathbf{P^G}) \tag{25}$$

$$s.t. \quad \underline{\mathbf{P}}^{\mathbf{G}} \le \mathbf{P^G} \le \overline{\mathbf{P}}^{\mathbf{G}} \tag{26}$$

$$\sum \mathbf{P^G} = \sum \mathbf{P^L} \tag{27}$$

$$-\overline{\mathbf{F}} \le \mathbf{B R K}^{-1} \tilde{\mathbf{P}} \le \overline{\mathbf{F}}, \tag{28}$$

where $\mathbf{P^G}$ is a vector of power generations, $\underline{\mathbf{P}}^{\mathbf{G}}$ is a vector of the lower bound of the power generations, $\overline{\mathbf{P}}^{\mathbf{G}}$ is a vector of the upper bound of the power generations, $\overline{\mathbf{F}}$ is a vector of power flow limits, the matrix $\mathbf{B}$ is

$\mathbf{B} = \begin{bmatrix} \mathbf{B}^{GG} & \mathbf{0} \\ \mathbf{0} & \mathbf{B}^{LL} \end{bmatrix}$ and the matrix $\mathbf{K} = \mathbf{R}^T\mathbf{BR}$, $\tilde{\mathbf{P}}$ is a vector obtained by maintaining all but the first element of the vector $\mathbf{P^G} - \mathbf{P^L}$, and the power flow $\mathbf{F} = \mathbf{BRK}^{-1}\tilde{\mathbf{P}}$. The constraint (26) denotes the limits of the power generation. The constraint (27) represents the equality of the generation and consumption. The power flow limit is presented by (28). The cost function $G(\mathbf{P^G})$ is usually quadratic [29].

To reduce the operation cost, the optimization of NPR is formulated by

$$\Delta C^* = \min_{\mathbf{P^G}, \tilde{s}_{ij}, \{i,j\} \in \mathbb{M}} G(\mathbf{P^G}) - C_0 \tag{29}$$

$$s.t. \quad \underline{\mathbf{P}}^{\mathbf{G}} \leq \mathbf{P^G} \leq \overline{\mathbf{P}}^{\mathbf{G}} \tag{30}$$

$$\sum \mathbf{P^G} = \sum \mathbf{P^L} \tag{31}$$

$$-\overline{\mathbf{F}} \leq \mathbf{BRK}^{-1}\tilde{\mathbf{P}} \leq \overline{\mathbf{F}}, \tag{32}$$

$$|\mathbb{M}| \leq \zeta, \tag{33}$$

$$\sum_{\{i,j\} \in \mathbb{M}} \Delta s_{ij}^{\text{ref}} \leq \rho, \tag{34}$$

$$\Delta_i^{\text{mit}} < 0, \forall i, \tag{35}$$

$$0.5 \leq \frac{\tilde{s}_{ij}}{s_{ij}} \leq 1.5, \{i,j\} \in \mathbb{M}, \tag{36}$$

where ζ and ρ are positive constant, the first three constraints are the same as the normal OPF, the constraint (33) limits the number of transmission lines whose parameters are changed, the constraint (34) limits the magnitude of the susceptance injection, the constraint (36) guarantees that the stability of the grid frequency is not affected. The last constraint (36) limits the magnitude of the change of the line parameter for NPR. For the adversarial loads, they are determined during the defense period. Therefore, the optimization problem is in a combinatorial form. The set of transmission lines (whose parameters are changed) and the corresponding changed ratios can be solved using a Monte Carlo method. To clearly describe the defense process, we provide a flowchart in Fig. 1b for the system operator to carry out the NPR.

4 Simulation Results

Furthermore, we conduct extensive simulations to evaluate the impact of DLAA and the effect of NPR. The 39-bus power system is used as an example. The system parameters, configurations, and network structure are obtained from the New England test case [30]. The first 30 buses are load buses, while the rest are all generation buses. As shown in Fig. 2, it is a diagram of the 39-bus power system. The simulation is conducted on MATLAB R2019b. The code is written in the MATLAB script language. The computation platform is a Lenovo Thinkpad laptop with 11th Gen Intel(R) Core(TM) i7-1165 G7 2.80 GHz (2.80 GHz) and 32 G RAM.

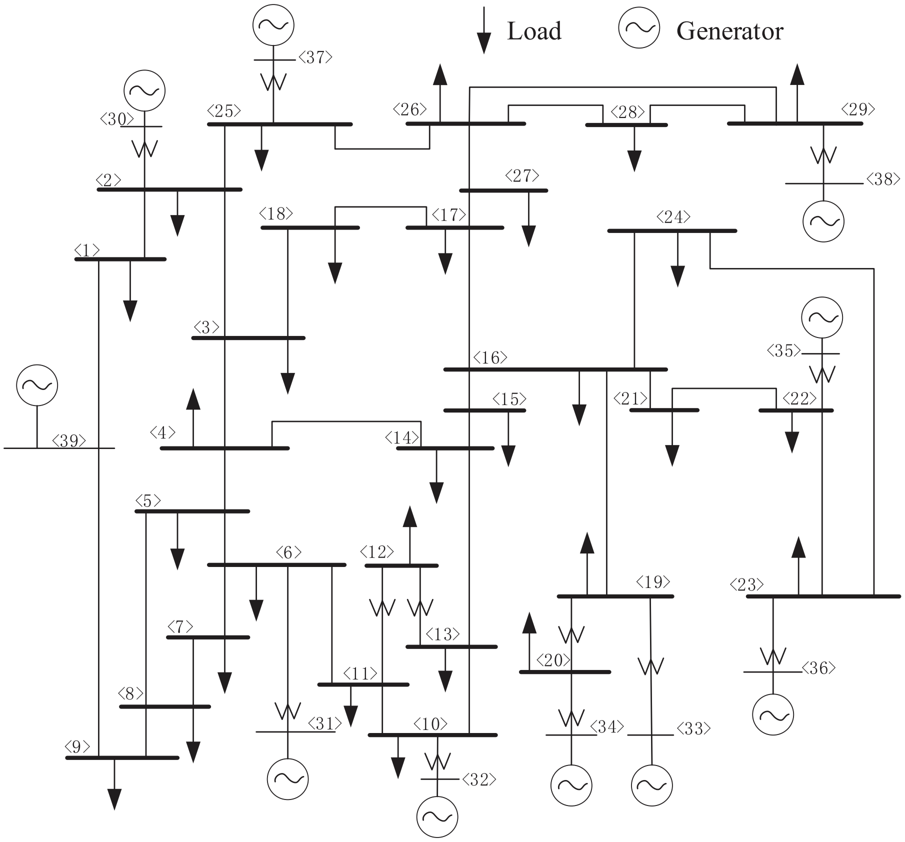


Figure 2: The IEEE 39-bus power system

4.1 Impact of the DLAA

First, we analyze the impact of DLAA on the stability of the grid frequency. We define the eigenvalue sensitivity of the i^{th} eigenvalue with respect to the j^{th} load as $\left|\mathrm{Rel}\left(\frac{\mathbf{l}_i^T\left(\beta_i\frac{\partial\mathcal{B}(\pi_j)}{\partial\pi_j}\right)\mathbf{r}_i}{\mathbf{l}_i^T(2\beta_i\mathcal{A}+\mathcal{B})\mathbf{r}_i}\right)\right|$. The relative eigenvalue sensitivity is defined as $\frac{\left|\mathrm{Rel}\left(\frac{\mathbf{l}_i^T\left(\beta_i\frac{\partial\mathcal{B}(\pi_j)}{\partial\pi_j}\right)\mathbf{r}_i}{\mathbf{l}_i^T(2\beta_i\mathcal{A}+\mathcal{B})\mathbf{r}_i}\right)\right|}{|\beta_i|}$. For each load and each eigenvalue, the sensitivity and relative sensitivity are shown in Figs. 3 and 4. We can see that the first 10 eigenvalues are more sensitive to the DLAA, as indicated by their absolute values. In comparison, the last 10 eigenvalues are more sensitive to the DLAA, considering the relative value. The results indicate that the DLAA has a different impact on the eigenvalues for various loads. Therefore, the targeted loads are crucial in designing the DLAA.

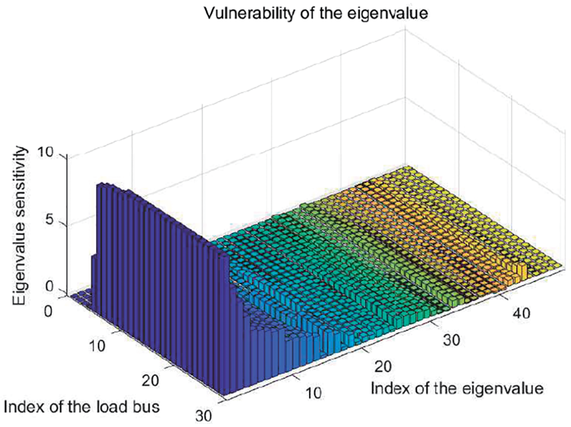


Figure 3: The eigenvalue sensitivity against the DLAA on each load

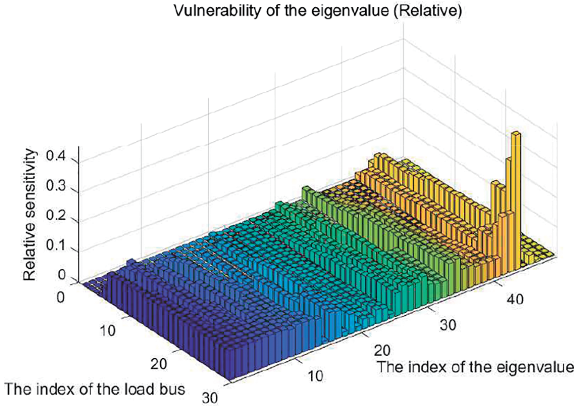
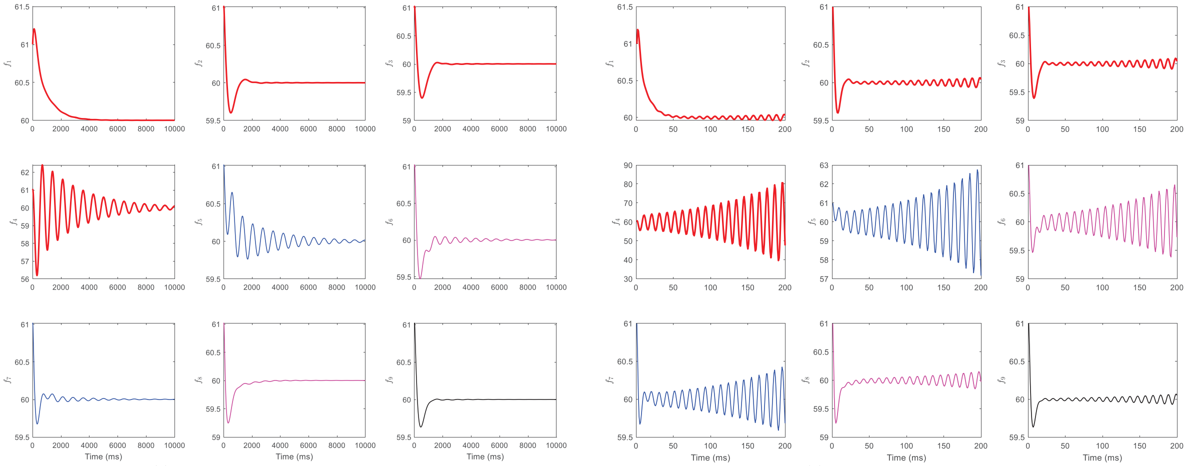


Figure 4: The eigenvalue sensitivity (the relative value) against the DLAA on each load

For the adversarial setting, the DLAA targets the 2nd, 19th, and 27th loads. That is, the frequency-sensitive loads contained in the 2nd, 19th, and 27th loads are maliciously modified. The attack parameters corresponding to them are set in two cases, as shown in Table 1. The DLAAs on the grid frequencies of the 9 generation buses are shown in Fig. 5. Fig. 6 shows the grid frequencies of the generations of buses without any attack. For the attack case 1, the grid frequencies of the 9 generation buses converge to 0s, although there are oscillations before the convergence. For the attack case 2, the grid frequencies of the 9 generation buses diverge from the nominal value (i.e., 60 Hz). The real parts of the eigenvalues given in Fig. 7 show that two eigenvalues have non-negative real parts in the attack case 2, which is the reason for the divergence of the grid. The results indicate that not all DLAAs are successful in destabilizing the grid frequencies. The DLAA should be carefully designed to affect the stability of the grid frequency.

Table 1: Two cases for constructing the DLAA

Attack parameter			
Cases	π_2	π_{19}	π_{27}
Attack Case 1	1.1	1.9	1.4
Attack Case 2	1.2	2.5	1.3



(a) Not be affected by the attack case 1 (b) Be affected by the attack case 2

Figure 5: The grid frequency under the DLAA

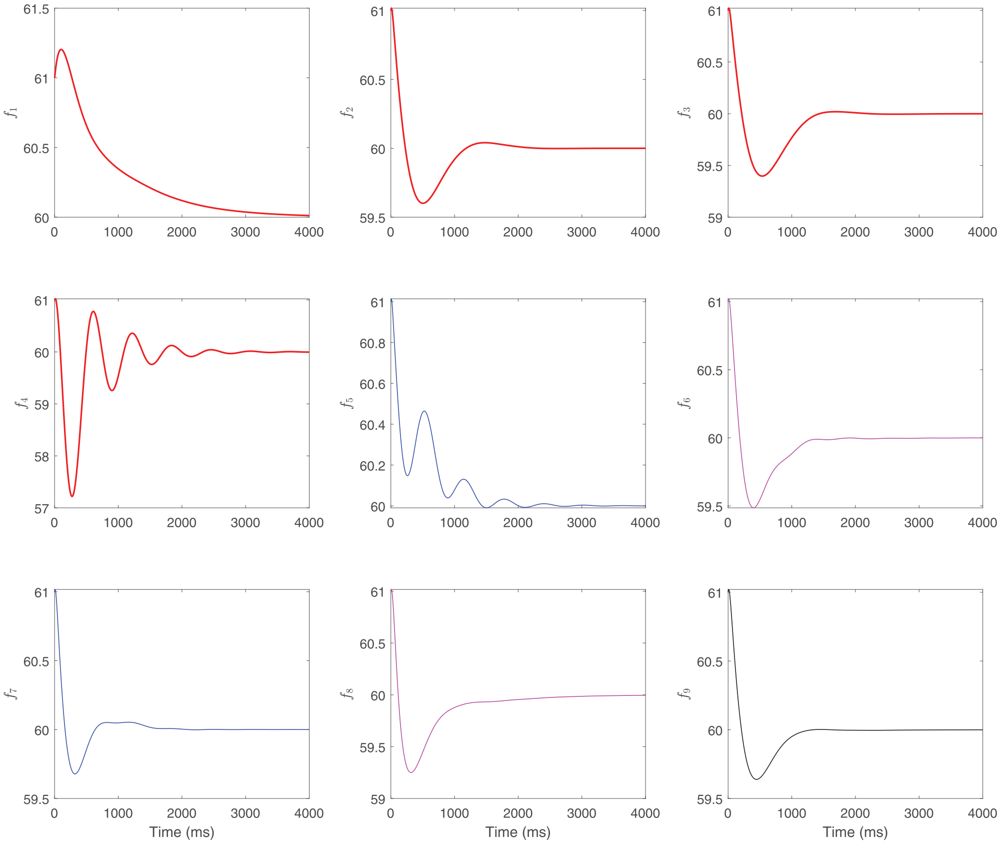


Figure 6: The grid frequency without the DLAA

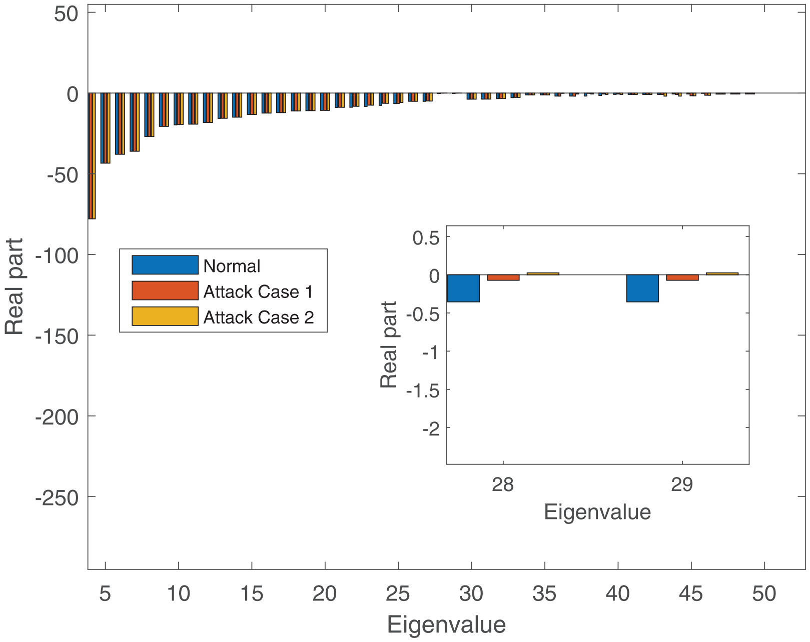


Figure 7: The real parts of the eigenvalues under different attack cases

4.2 Mitigating DLAA with MTD

Next, we evaluate the performance of MTD to mitigate the DLAA. The DLAA setting is like the attack case 2. The NPR parameters for the mitigation cases are given in Table 2. The set of transmission lines for NPR contains lines 9, 19, 26, 29, and 33. For the mitigation case 1 and mitigation case 2, the frequencies of the generation buses are shown in Fig. 8. We can see that the grid frequency still diverges from the nominal value in mitigation case 1, indicating that the NPR parameter does not effectively mitigate the DLAA. However, the grid frequency converges to the nominal value in mitigation case 2, indicating that the NPR is effective. The same effect can be obtained with the mitigation cases from 2 to 12. Therefore, the NPR parameters should be appropriately set to mitigate the impact of the DLAA.

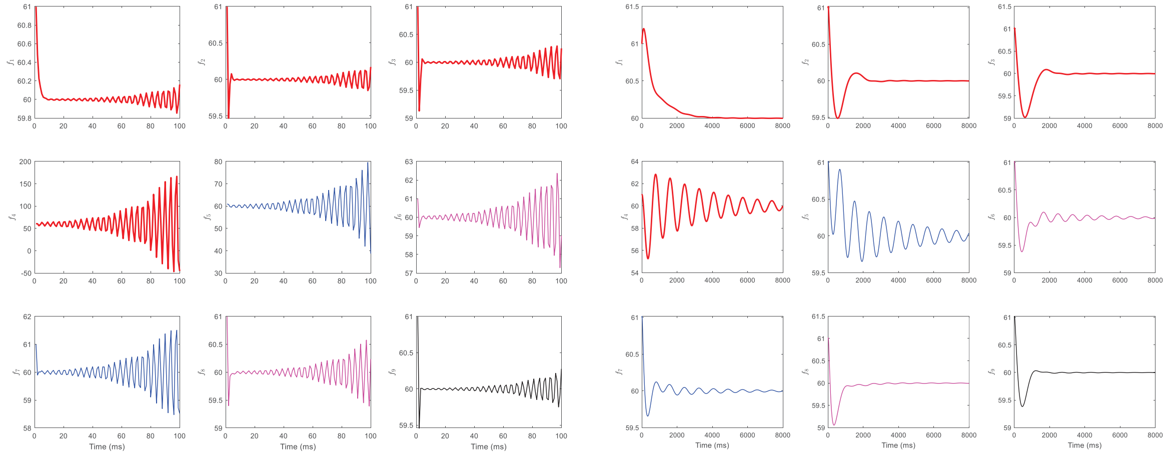
Table 2: The cases for constructing the MTD to mitigate the DLAA

	Parameter				
Cases	$\frac{\tilde{s}_9}{s_9}$	$\frac{\tilde{s}_{19}}{s_{19}}$	$\frac{\tilde{s}_{26}}{s_{26}}$	$\frac{\tilde{s}_{29}}{s_{29}}$	$\frac{\tilde{s}_{33}}{s_{33}}$
Mitigation Case 1	0.8	1.1	1.2	0.9	1.5
Mitigation Case 2	1.3	1.2	1.5	1.5	1.2
Mitigation Case 3	1.2	1.2	1.4	1.5	1.2
Mitigation Case 4	1.1	1.1	1.5	1.5	1.2
Mitigation Case 5	1.3	1.1	1.5	1.2	0.9
Mitigation Case 6	1.3	1.1	1.3	1.1	0.9
Mitigation Case 7	1.23	0.95	1.34	1.1	0.9
Mitigation Case 8	1.23	0.95	1.12	1.11	0.98
Mitigation Case 9	1.43	1.05	1.12	1.23	0.98

(Continued)

Table 2 (continued)

Cases	Parameter				
	$\frac{\tilde{s}_9}{s_9}$	$\frac{\tilde{s}_{19}}{s_{19}}$	$\frac{\tilde{s}_{26}}{s_{26}}$	$\frac{\tilde{s}_{29}}{s_{29}}$	$\frac{\tilde{s}_{33}}{s_{33}}$
Mitigation Case 10	1.43	0.75	1.32	1.03	1.38
Mitigation Case 11	1.33	0.95	1.22	1.13	1.08
Mitigation Case 12	1.33	0.95	1.02	1.34	1.16



(a) Not mitigate with the mitigation case 1

(b) Mitigate with the mitigation case 2

Figure 8: Mitigating the impact of the DLAA with NPR

To optimize the NPR, we test several cases to evaluate the cost change with different line change parameters. The attack is set as $\pi_2 = 1.2$, $\pi_{19} = 2.5$, and $\pi_{27} = 1.3$. The set of transmission lines chosen for NPR is $\{9, 19, 26, 29, 33\}$. The changes in line parameters are presented in Cases 2 to 12. The attack and defense settings guarantee that the constraint (36) is satisfied. Therefore, the optimization problem for NPR (29)–(36) can be solved using the *quadprog* package in MATLAB. To compute the OPF problem, the system parameters are given as follows. The cost function $G(\cdot)$ is in the quadratic form of $c_1x^2 + c_2x + c_0$, where c_1, c_2, and c_0 are coefficients. Among them, the coefficients c_1 and c_2 are critical for computing the optimal power flow problem. The generator parameters are given in Table 3. The generation limits are given in Table 4. The power flow limitation is set by $\overline{\mathbf{F}} = 1.5\mathbf{F}$. The parameters of the PI controller are: $K_1^p = 100$, $K_2^p = 45$, $K_3^p = 45$, $K_4^p = 10$, $K_5^p = 50$, $K_6^p = 40$, $K_7^p = 30$, $K_8^p = 20$, $K_9^p = 40$, $K_{10}^p = 50$, and $K_1^I = \cdots = K_{10}^I = 10$. The coefficient of the frequency-sensitive load for each load is 10.

Table 3: Parameters of the generators

Coefficients	Number of generators						
	1	2	3	4	5	6	7
c_1	0.04	0.25	0.01	0.01	0.01	0.01	0.01
c_2	10	15	20	25	30	30	30

Table 4: Generation limits

	Number of generators						
Limits	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Lower bound	0	0	0	0	0	0	0
Upper bound	100	100	100	150	100	100	100

The generation costs without NPR and with NPR are given in Table 5. Compared with the generation cost without NPR, the generation cost with NPR changes under different NPR parameters. The generation cost increases with the mitigation cases 2, 3, 4, 5, 6, 9, 10, and 12, while the generation cost is reduced with the mitigation cases 7, 8, and 11. The results indicate that in most cases, the NPR will introduce additional operational costs. The reason is that the NPR causes tight power flows for the system operation. Due to the nonlinear and non-convex properties of the optimization problem for OPF, the derivation of the essential implications of the additional cost caused by the NPR is out of the scope of this paper. From Fig. 9, with the mitigation case 8, the generation cost is 5764.24 $ MWh, which saves 41.18 $ MWh. Therefore, the NPR can be optimized to mitigate the DLAA. The cost-benefit NPR can be constructed to consider the defense effect and the operational cost simultaneously.

Table 5: Comparison of the generation costs with and without NPR

	Costs	
Cases	**Without NPR ($/MWh)**	**With NPR ($/MWh)**
Mitigation Case 2	5805.42	5852.11
Mitigation Case 3	5805.42	5843.30
Mitigation Case 4	5805.42	5825.03
Mitigation Case 5	5805.42	5813.97
Mitigation Case 6	5805.42	5807.01
Mitigation Case 7	5805.42	5803.11
Mitigation Case 8	5805.42	5764.24
Mitigation Case 9	5805.42	5821.27
Mitigation Case 10	5805.42	5807.14
Mitigation Case 11	5805.42	5786.34
Mitigation Case 12	5805.42	5845.17

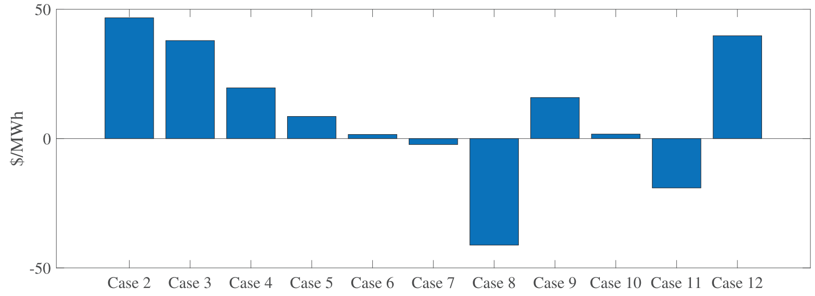


Figure 9: The cost-benefit using NPR to mitigate the DLAA

5 Conclusion

In this paper, we propose a network parameter regulation (NPR) strategy to defend against the dynamic load altering attack (DLAA) in the scenario of load frequency control. To begin with, we transformed the first-order dynamic model into a second-order dynamic model. By analyzing the eigenvalue sensitivity, the impact of the DLAA was modeled, and the effect of NPR was revealed. The deployment cost of NPR was optimized to realize a cost-effective defense strategy. Finally, the attack impact and defense performance were validated through extensive simulations. In future work, we can incorporate the prediction method as given in [31] to improve the performance of the mitigation approach in defending against the DLAA on the LFC. Besides, we will consider extending the analysis to non-linear models, such as full AC power flow simulations or hybrid automaton approaches for significant disturbances. This could involve tools like MATPOWER or PSAT for non-linear validation. We believe this addresses the concern while strengthening the paper's rigor.

Acknowledgement: We express our gratitude to the members of our research group, i.e., the Intelligent System Security Lab (ISSLab) of Guizhou University, and Guizhou Power Grid Co., Ltd. Electric Power Dispatching and Control Center, for their invaluable support and assistance in this investigation. We also extend our thanks to our university for providing essential facilities and environment.

Funding Statement: This paper is supported by the project Major Scientific and Technological Special Project of Guizhou Province ([2024]014).

Author Contributions: Conceptualization, Yunhao Yu, Boda Zhang, Meiling Dizha, Ruibin Wen, Fuhua Luo, Xiang Guo, Zhenyong Zhang; methodology, Yunhao Yu and Zhenyong Zhang; software, Yunhao Yu and Zhenyong Zhang; validation, Yunhao Yu and Zhenyong Zhang; formal analysis, Yunhao Yu and Zhenyong Zhang; investigation, Yunhao Yu and Zhenyong Zhang; resources, Yunhao Yu and Zhenyong Zhang; data curation,Yunhao Yu and Zhenyong Zhang; writing—original draft preparation, Yunhao Yu and Zhenyong Zhang; writing—review and editing, Yunhao Yu and Zhenyong Zhang; visualization, Yunhao Yu and Zhenyong Zhang; supervision, Zhenyong Zhang; project administration, Zhenyong Zhang; funding acquisition, Zhenyong Zhang. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Not applicable. This article does not involve data availability, and this section is not applicable.

Ethics Approval: Not applicable for studies not involving humans or animals.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

1. Jeong S, Choi D-H. Electric vehicle user data-induced cyber attack on electric vehicle charging station. IEEE Access. 2022;10:55856–67. doi:10.1109/access.2022.3177842.
2. Meserve J. Staged cyber attack reveals vulnerability in power grid [Internet]. [cited 2007 Sep 26]. Available from: http://edition.cnn.com/2007/US/09/26/power.at.risk/.
3. Zhang Z, Deng R, Tian Y, Cheng P, Ma J. SPMA: Stealthy physics-manipulated attack and countermeasures in cyber-physical smart grid. IEEE Trans Inf Forensics Secur. 2022;18:581–96. doi:10.1109/tifs.2022.3226868.
4. Amini S, Pasqualetti F, Mohsenian-Rad H. Dynamic load altering attacks against power system stability: attack models and protection schemes. IEEE Trans Smart Grid. 2018;9(4):2862–72. doi:10.1109/tsg.2016.2622686.
5. Yuan Y, Li Z, Ren K. Modeling load redistribution attacks in power systems. IEEE Trans Smart Grid. 2011;2(2):382–90. doi:10.1109/tsg.2011.2123925.
6. Zhang Z, Deng R, Yau D, Cheng P. Zero-parameter-information data integrity attacks and countermeasures in IoT-based smart grid. IEEE Internet Things J. 2021;8(8):6608–23. doi:10.1109/jiot.2021.3049818.

7. Alsharif G, Anagnostopoulos C, Marnerides A. Energy market manipulation via false-data injection attacks: a review. IEEE Access. 2025;13(2):42559–73. doi:10.1109/access.2025.3548914.
8. Yuan Y, Li Z, Ren K. Quantitative analysis of load redistribution attacks in power systems. IEEE Trans Parallel Distrib Syst. 2012;23(9):1731–8. doi:10.1109/tpds.2012.58.
9. Liu X, Song Y, Li Z. Dummy data attacks in power systems. IEEE Trans Smart Grid. 2019;10(2):1792–5. doi:10.1109/tsg.2019.2929702.
10. Lakshminarayana S, Adhikari S, Maple C. Analysis of IoT-based load altering attacks against power grids using the theory of second-order dynamical systems. IEEE Trans Smart Grid. 2021;12(5):4415–25. doi:10.1109/tsg.2021.3070313.
11. Zhang Z, Deng R, Yau D. Vulnerability of the load frequency control against the network parameter attack. IEEE Trans Smart Grid. 2021;10(1):921–33.
12. Meluccci C, Menon P, Edwards C, Ferrara A. Load alteration fault detection and reconstruction for power networks modeled with descriptor differential algebraic equation form. IEEE Trans Autom Control. 2021;66(2):489–503. doi:10.1109/acc.2015.7172254.
13. Su Q, Li S, Gao Y, Huang X, Li J. Observer-based detection and reconstruction of dynamic load altering attack in smart grid. J Franklin Inst. 2021;358(7):4013–27. doi:10.1016/j.jfranklin.2021.02.008.
14. Izbicki M, Amini S, Shelton CR, Mohsenian-Rad H. Identification of destabilizing attacks in power systems. In: 2017 American Control Conference (ACC); 2017 May 24–26; Seattle, WA, USA. p. 3424–9.
15. Lakshminarayana S, Sthapit S, Jahangir H, Maple C, Poor HV. Data-driven detection and identification of IoT-enabled load-altering attacks in power grids. IET Smart Grid. 2022;5(3):203–18. doi:10.1049/stg2.12066.
16. Amini S, Pasqualetti F, Mohsenian-Rad H. Detecting dynamic load altering attacks: a data-driven time-frequency analysis. In: 2015 IEEE International Conference on Smart Grid Communications (SmartGridComm); 2015 Nov 2–5; Miami, FL, USA. p. 503–8.
17. Lawal O, Teh J, Alharbi B, Lai C. Data-driven learning-based classification model for mitigating false data injection attacks on dynamic line rating systems. Sustain Energy Grids Netw. 2024;38:101347. doi:10.1016/j.segan.2024.101347.
18. Shrestha B, Lin H. Data-centric edge computing to defend power grids against IoT-based attacks. Computer. 2020;53(5):35–43. doi:10.1109/mc.2020.2972228.
19. Chu Z, Lakshminarayana S, Chaudhuri B, Teng F. Mitigating load-altering attacks against power grids using cyber-resilient economic dispatch. IEEE Trans Smart Grid. 2023;14(4):3164–75. doi:10.1109/tsg.2022.3231563.
20. Sayed MA, Ghafouri M, Atallah R, Debbabi M, Assi C. Protecting the future grid: an electric vehicle robust mitigation scheme against load altering attacks on power grids. Appl Energy. 2023;350:121769. doi:10.1016/j.apenergy.2023.121769.
21. Qi Y, Shi D, Tylavsky D. Impact of assumptions on DC power flow model accuracy. In: 2012 North American Power Symposium (NAPS); 2012 Sep 9–11; Champaign, IL, USA. p. 1–6.
22. Alhasnawi B, Zanker M, Bures V. A new smart charging electric vehicle and optimal DG placement in active distribution networks with optimal operation of batteries. Results Eng. 2025;25:104521. doi:10.1016/j.rineng.2025.104521.
23. Alhasnawi B, Hashim H, Zanker M, Bures V. The rising, applications, challenges, and future prospects of energy in smart grids and smart cities systems. Energy Convers Manag X. 2025;27:101162. doi:10.1016/j.ecmx.2025.101162.
24. Nasr T, Torabi S, Bou-Harb E, Fachkha C, Assi C. Power jacking your station: in-depth security analysis of electric vehicle charging station management systems. Comput Secur. 2022;112:102511. doi:10.1016/j.cose.2021.102511.
25. Chen Y, Luo B. S2A: secure smart household appliances. In: CODASPY ’12: Proceedings of the Second ACM Conference on Data and Application Security and Privacy; 2012 Feb 7–9; San Antonio, TX, USA. p. 217–28.
26. Khalil HK. Lyapunov stability. In: Control systems, robotics, and automation. Manchester, UK: EOLSS; 2009.
27. Nelson RB. Simplified calculation of eigenvector derivatives. AIAA J. 1976;14(9):1201–5.
28. Friswell MI, Adhikari S. Derivatives of complex eigenvectors using Nelson’s method. AIAA J. 2000;38(12):2355–6. doi:10.2514/2.907.
29. Monticelli A. Electric power system state estimation. Proc IEEE. 2000;88(2):262–82.

30. DESL-EPFL. IEEE 39-bus power system [Internet]. [cited 2025 Sep 2]. Available from: https://github.com/DESL-EPFL/IEEE-39-bus-power-system39busref.

31. Shi J, Teh J, Lai CM. Wind power prediction based on improved self-attention mechanism combined with bi-directional temporal convolutional network. Energy. 2025;322:135666. doi:10.1016/j.energy.2025.135666.