IET Generation, Transmission & Distribution

WILEY

The Institution of Engineering and Technology

ORIGINAL RESEARCH OPEN ACCESS

A Novel Model-Free Defense Scheme for Power Systems Stability Under Cyber Attacks

Soroush Oshnoei[1] | Rasool Peykarporsan[2] | Jalal Heidari[3,4] | Esmaeil Mahboubi-Moghaddam[5] | Tek Tjing Lie[2] | Mohammad-Hassan Khooban[1]

[1]Department of Electrical and Computer Engineering, Aarhus University, Aarhus, Denmark | [2]Department of Electrical and Electronic Engineering, Auckland University of Technology, Auckland, New Zealand | [3]Department of Electromechanical, Systems and Metal Engineering, Ghent University, Ghent, Belgium | [4]FlandersMake UGent-Corelab MIRO, Lommel, Belgium | [5]Department of Electrical Engineering, Faculty of Electrical and Computer Engineering, Quchan University of Technology, Quchan, Iran

Correspondence: Esmaeil Mahboubi-Moghaddam (mahboubi@qiet.ac.ir)

Received: 27 June 2025 | **Revised:** 4 November 2025 | **Accepted:** 11 December 2025

ABSTRACT

The load frequency control (LFC) scheme, as a vital application in power systems' stability, makes the power system susceptible to cyber-attacks due to its dependence on information technologies and communication networks. This paper studies the LFC performance of Kundur's 4-unit-12-bus power system under false data injection (FDI) attacks. The available defence schemes are either based on the system's model or data-driven. The effectiveness of these schemes depends on the precise mathematical modelling or the extensive historical data of the power system. Therefore, it is necessary to design a defence strategy without depending on the mathematical model and the historical data of the system. To this end, this paper proposes a model-free resilient defence strategy, comprising a model-free detection scheme and an event-triggered mechanism. The presented detection scheme accomplishes the manipulated signal estimation using the measurement and control signals and compares the difference between the estimated and observed signals with a predefined threshold value. When the difference exceeds the threshold value, the detection scheme announces that an attack has occurred on the system. After detecting an attack, the event-triggered mechanism is activated to mitigate the attack's effect on the system frequency response. Accordingly, the event-triggered mechanism blocks the falsified signal and submits the estimated signal to the LFC controller. The presented scheme is independent of the system's mathematical model and historical data and can be employed in any cyber-physical power system. The design process of this strategy is simple and independent of the size and complexity of the power system. A deep reinforcement learning algorithm is also employed to tune the adjustable parameters of the proposed method. The real-time results obtained by the OPAL-RT simulator show that the developed scheme can timely identify FDI attacks and completely mitigate the attack's effect on the system's dynamic performance.

1 | Introduction

Several advances in information technologies and communication networks (ITCNs), computer science and control theory have led to extensive research on cyber-physical systems (CPSs) in recent years [1]. A CPS can be defined as a system that is monitored or controlled by a computer-based algorithm and combined with a network and a user interface [2]. There are several subsystems and control systems in the power system, making it a complex CPS. One of these systems is load frequency control (LFC), which has an essential role in the power grid, since minimizing frequency fluctuations in the network is incredibly critical [3]. The ITCNs have a key function in the LFC's efficiency and the system's dynamic stability. Using the area control error

(ACE) obtained through distributed sensors, the LFC system regulates generator outputs to maintain the frequency at the nominal value [4]. Physical and cyber layers in the LFC system are closely interconnected, creating a vulnerability where attacks on one layer compromise both grid stability and security [5]. Hackers can target this vulnerability and apply cyber-attacks, which if not defended against, can greatly threaten the power network [6].

One of the most serious cyber-attacks in the power system is false data injection (FDI) attacks which can target measurement and control signals in the LFC system [7]. The attacker exploits weaknesses in the information exchange process to deceive control centres, causing the generating units to be controlled incorrectly [8]. The FDI attack in the LFC application has been approached using several strategies in the literature. In general, they can be classified into two categories: model-based and model-free techniques. Model-based techniques rely on building an explicit model of the environment, allowing accurate predictions and planning. On the other hand, model-free techniques learn directly from experience, making them more flexible and suitable for problems with unknown dynamics or complex environments.

In [9], the defence performance of a model-based technique based on a reduced-order H_∞ filter as the secondary frequency controller in a power system has been evaluated under cyber-attacks. In addition, a model predictive control technique integrated with H_2/H_∞ algorithm as well as an event-triggered mechanism, has been developed in [10] for addressing FDI attacks targeting the LFC system. The authors in [11] developed a dynamic event-triggered H_∞ technique in a multi-area power system to mitigate FDI and hybrid attacks. In [12], FDI attacks on networked control systems were mitigated through dynamic watermarking. A multiplicative watermarking technique is introduced in [13] for a networked control system when the LFC system is under cyber-attacks. In [14], a model-based observer is investigated for estimating the system's state variables, and a model-free observer to estimate the disruption applied to a two-area linearized power system. A two-step cyber-resilient control strategy, comprised of an auxiliary trajectory control and a safety surface, has been presented in [15] to cope with FDI and denial-of-service (DoS) attacks in an interconnected LFC system. An adaptive-memory event-triggered mechanism has been introduced in [16] to enhance the frequency stability of a multi-area power system under FDI attacks. The authors in [17] have focused on an informer-based FDI attack recovery model to regulate the control input signals for reconfiguration in a two-area LFC system. The sliding mode control strategy using an adaptive event-triggered scheme has been addressed in [18] to improve frequency regulation in a two-area LFC network under FDI attacks and time delays.

Among model-free techniques, machine learning algorithms are widely used in the literature to protect against cyber-attacks in the LFC systems. The authors in [19] proposed a self-learning approach that follows a specific coordination pattern for mitigating ACE signals compromised by FDI attacks. For the prevention of FDI attacks on the multi-area power system, Ref. [20] reported the development of a deep learning technique based on a two-stage long-short term memory framework. The authors in [21] presented a modified cascaded dual-loop linear active disturbance rejection-based tilted secondary controller to reduce effects of cyber-attacks on the frequency response of a multi-area power system. A reinforcement active disturbance rejection control strategy, combined with a parallel attack detection system based on a regression tree, has been proposed in [22] to mitigate cyber-attacks in an interconnected LFC system. The authors in [23] developed an technique based on artificial intelligence to detect and counter FDI attacks on LFC systems within integrated energy systems. A deep-learning algorithm-based attack detection system for hybrid power systems was presented in [24]. In [25], an ultra-local model-free control strategy has been presented as the secondary frequency controller to improve the LFC efficiency of a two-area power system affected by FDI attacks. The authors in [26] proposed a cascade FOPIDN-(1+TD) controller using the quasi opposition arithmetic optimization algorithm to improve the LFC performance of power systems under cyber-attacks. A modified fuzzy logic-based FOPI-TD controller was presented in [27] to regulate the frequency response of a two-area power system. A 3-DOF FOPI-FOPD controller optimized by a modified volleyball premier league algorithm was presented in [28] to improve the frequency response of an interconnected power system. In [29], the authors reported the effectiveness of a fuzzy logic-based fractional-order cascade control method as a secondary controller of a multi-area power system to enhance its frequency stability. A resilient event-triggered LFC approach for power systems with an additional control loop under DoS attacks was developed in [30].

Taking into account the literature review, the research gaps in the previous works are presented as follows:

- Prior studies have investigated the impact of FDI attacks on the frequency response of linearized power systems.
- The model-based defence methods heavily rely on accurate and up-to-date models of the system being analysed. The effectiveness of these methods significantly reduces in power systems with a complex dynamic nature.
- The data-driven methods are highly dependent on the network's historical data and may struggle with the lack of sufficient and high-quality training data, leading to unreliable predictions. Such algorithms require high computational power and might not be feasible for real-world applications.

Building on the aforementioned gaps, the major contributions of this study are specified as follows:

- A model-free resilient defence approach based on a deep reinforcement learning (DRL) algorithm, composed of a model-free detection scheme and an event-triggered mechanism, is developed to deal with FDI attacks affecting the measurement signals in Kundur's 4-unit-12-bus realistic power system.
- The proposed defence method estimates the manipulated signal, computes the residual signal and compares it with a predefined threshold value. Exceeding the residual signal from the threshold value indicates an attack has occurred. After identifying an attack, the event-triggered mechanism sends the estimated signal to the secondary PI controller to mitigate the attack's effect.
- The developed defence strategy is independent of the mathematical model and the historical data of the system. Therefore, this strategy can be used in any cyber-physical power system.

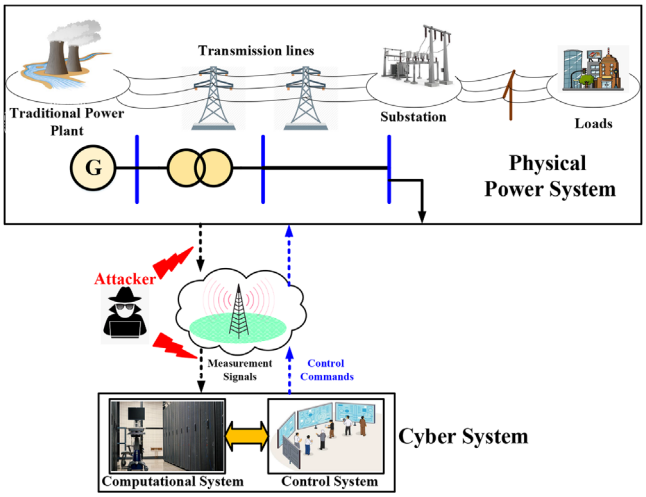

FIGURE 1 | Schematic diagram of a cyber-physical power system under cyber threats.

- The real-time applicability of the proposed defence method is assessed using the OPAL-RT simulator under different scenarios.

The reminder of the presented work is as follows: The power system model under study is described in Section 2. In Section 3, modelling FDI attacks on the system measurement signal is provided. Section 4 describes the design of the presented defence method. Section 5 represents the simulation results relevant to the proposed defence method. Finally, the current work is concluded in Section 6.

2 | Studied Power System

Figure 1 demonstrates the schematic diagram of a cyber-physical power system under cyber threats. As shown, the measurement signal associated with the physical power system is transferred to the cyber system over communication networks. The computational part of the cyber system processes the incoming measurement data. After processing the measurement data, the cyber system control part receives this data and generates the required control actions to balance the load and generation. Then, the generated control actions are transmitted to the physical power system via communication networks to respond to load changes. The cyber-physical power system's vulnerability points are depicted in Figure 1. According to this figure, the attacker can penetrate communication networks between the cyber and physical systems to manipulate the transmitted data using false data. As a result of receiving false data, the cyber system generates destructive control actions that can compromise power system stability. Figure 2 depicts the schematic of Kundur's 4-unit-12-bus power system considered in this research. The power system under study is divided into two areas. Only area 1 is assumed to be equipped with the AGC control loop. Secondary frequency control is performed by a PI controller, while the nominal frequency is set to 60 Hz. The nominal capacity and voltage of the system's generators are 900 MVA and 20 kV, respectively. A 230 kV nominal voltage is used in the transmission system. Also, the power flow exchanged between areas is a constant value of 400

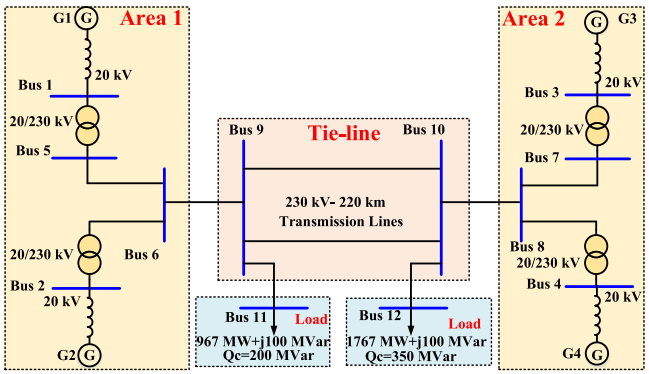

FIGURE 2 | Schematic of Kundur's 4-unit-12-bus power system.

MW. Therefore, the AGC loop in area 1 only controls the system frequency. Whenever the frequency fluctuates from the nominal value due to the load changes, the generation units in each area participate in the frequency control using the primary control loop or droop control. If the ACE signal in the area 1 remains non-zero, the area 1 AGC control loop sends control signals for area 1 generation units to change their generation powers and regulate the ACE signal into zero. The control signal generated by the AGC service (u_{AGC}) is as follows:

$$u_{\mathrm{AGC}} = K_{\mathrm{P}}\Delta f_1(t) + K_{\mathrm{I}}\int_0^{\tau}\Delta f_1(t) \tag{1}$$

where $\Delta f_1(t)$ is the frequency deviation of area 1, K_{P} and K_{I} represent the proportional and integral gains of the PI controller, respectively. The AGC correction is allocated to participating generators in area 1 by fixed participation factors $\{\alpha_i\}$ as follows:

$$\Delta P_i(t) = \alpha_i u_{\mathrm{AGC}}, \quad \sum_{i=1}^{2}\alpha_i = 1. \tag{2}$$

where $\Delta P_i(t)$ is the output power of generation unit ith. More details about the power system model under study are available in [31]. The proposed defence framework is model-free and can be used for any cyber-physical power system. Therefore, its performance does not depend on the detailed AGC configuration of the system. However, the dynamic equations of the model under study are represented to recreate the environment to tune the observer's coefficients using a DRL algorithm.

It is common to assess frequency responses and design relevant controllers based on the system frequency response. Although simple, the system cannot fully represent the dynamic properties of real-life systems. Hence, for this study, more detailed models, which present actual system responses more than the frequency response model, are built. Multiple auxiliary control systems and complex generating units, as well as the communication network are present in reality, so the final implemented power system should have many inputs and outputs and have a high order of nonlinearity.

1) Electromechanical unit model: In this study, the classic 7-order system consisting of both excitation and governor control systems

is implemented as follows:

$$\begin{cases} \dot{E}'_{di} = \dfrac{1}{T_{q0i}}\left[-E'_{di} + \left(x_{qi} - x'_{qi}\right) I_{qi}\right] \\ \dot{E}'_{qi} = \dfrac{1}{T_{d0i}}\left[-E'_{qi} + \left(x_{di} - x'_{di}\right) I_{di} + E_{fi}\right] \\ \dot{P}_{mi} = \dfrac{1}{T_{ti}}(P_{gi} - P_{mi}) \\ \dot{P}_{gi} = \dfrac{1}{T_{gi}}\left(-P_{gi} - \dfrac{\omega_i - \omega_0}{R_i} + u_{gi}\right) \\ \dot{E}_{fi} = -\dfrac{E_{fi}}{T_{ei}} + \dfrac{K_{ei}}{T_{ei}}(V^{\mathrm{r}}_{ti} - V_{ti}) \\ \dot{\delta}_i = \omega_i - \omega_0 = \Delta\omega_i \\ \dot{\omega}_i = \dfrac{\omega_0}{H_i}\left[P_{mi} + \left(x'_{di} - x'_{qi}\right) I_{di} I_{qi} - E'_{qi} I_{qi} - E'_{di} I_{di}\right] \end{cases} \tag{3}$$

In this model, I_{di} and I_{qi} are related to d-axis and q-axis components of the current, respectively; E'_{di} and E'_{qi} correspond to the d-axis and q-axis part of the voltage behind transient reactance x'_{di} and x'_{qi}, respectively; T_{d0i} and T_{q0i} represent the open circuit time constants for d-axis and q-axis. In addition, δ_i, ω_i and ω_0 correspond to the machine angle, machine speed and the nominal machine speed. Also, $\omega_i = 2\pi f$, which f is the system frequency. Moreover, P_{mi} denotes the mechanical power, P_{gi} represents the governor power, R_i corresponds to the droop coefficient, H_i is the inertia constant and u_{gi} is the control action by the governor. Furthermore, T_{ei} and K_{ei} are control parameters of the excitation system, V^{r}_{ti} is the reference voltage for the terminal, V_{ti} is the terminal voltage and E_{fi} is the excitation voltage.

2) Interface model: The interface model consists of the power equation, stator voltage and dq/xy transformation. Combined, they represent the interface relation between the external transmission network and the internal unit. For the stator, voltage can be expressed as follows:

$$\begin{cases} U_{di} = x_{qi} I_{qi} - r_{ai} I_{di} \\ U_{qi} = E'_{qi} - x'_{di} I_{di} - r_{ai} I_{qi} \end{cases} \tag{4}$$

where U_{di} and U_{qi} correspond to d-axes and q-axes components of the terminal voltage, respectively. The terminal voltage can be computed as $V_{ti} = \sqrt{U_{di}^2 + U_{qi}^2}$.

Using the $xy - dq$ transformation, the relationship between xy and the dq axis for voltage is as follows:

$$\begin{bmatrix} U_{xi} \\ U_{yi} \end{bmatrix} = \begin{bmatrix} \cos\delta_i & \sin\delta_i \\ \sin\delta_i & -\cos\delta_i \end{bmatrix} \begin{bmatrix} U_{qi} \\ U_{di} \end{bmatrix} \tag{5}$$

where U_{xi} and U_{yi} are the terminal voltage for x-axis and y-axis. Similarly, for the current, we can have:

$$\begin{bmatrix} I_{xi} \\ I_{yi} \end{bmatrix} = \begin{bmatrix} \cos\delta_i & \sin\delta_i \\ \sin\delta_i & -\cos\delta_i \end{bmatrix} \begin{bmatrix} I_{qi} \\ I_{di} \end{bmatrix} \tag{6}$$

where I_{xi} and I_{yi} are the terminal voltage for x-axis and y-axis. Using Equations (5) and (6), the output power can be calculated by:

$$\begin{cases} P_i = U_{xi} I_{xi} - U_{yi} I_{yi} \\ Q_i = U_{xi} I_{yi} + U_{yi} I_{xi} \end{cases} \tag{7}$$

here, Q_i is the reactive power and P_i is the active power.

3) Network model: The network can be modelled with equations for active and reactive power injection at each node:

$$P_i + jQ_i = \sum_k V_i V_k Y_{ik} e^{j(\theta_i - \theta_k - \phi_{ik})} \tag{8}$$

In this model, V_i corresponds to the voltage magnitude for bus i, θ_i corresponds to the voltage angle for bus i, and Y_{ik} corresponds to the admittance between bus i and k. The final nonlinear model of power system under study can be obtained by integrating Equations (3) to (8):

$$\begin{cases} \dot{x} = f(x, u, z) \\ 0 = g(x, u, z) \end{cases} \tag{9}$$

In this model, x, u, z corresponds to the states, control inputs and the auxiliary variables, respectively. It should be noted that the ramp rate limitations are not included in the AGC service modelling of the power system under study.

3 | Modelling FDI Attacks

This section describes the modelling of FDI attacks on the frequency signal, which may threaten the stability of the power system under study. An FDI attack falsifies the measurement signals transmitted during communication networks using false data, leading to the signals getting impacted and the control signals distorted. To design FDI attacks, it is presumed that the adversary possesses comprehensive knowledge about the system architecture and access to the frequency signal transmitted during the communication network. The AGC loop is the automated control loop between the cyber and physical layers; it is extremely vulnerable to cyber-attacks. Since the area 1 of the system under study is equipped with the AGC control loop, this control area is vulnerable to FDI attacks. It is necessary to mention that the communication protocols used in the AGC service are often Modbus, IEC61850, DNP3 and ICCP, which are not made with adequate security mechanisms by default. Therefore, the adversary can falsify the frequency signal transmitted during the insecure communication network by injecting a malicious data to into it. The ACE signal in area 1 can be described as:

$$\mathrm{ACE}_1 = \omega_1 - \omega_0 = \Delta\omega_1 \tag{10}$$

where ACE_1 and $\Delta\omega_1$ are the ACE signal and the frequency deviations in area 1, respectively. FDI attacks are classified to formats of exogenous and scaling attacks [14]. In exogenous FDI attacks, the d_{e} disruption is added to the real signal transmitted

during the communication network as follows:

$$\begin{cases} Y_a = Y_r & ,t < t_s \\ Y_a = Y_r + d_e & ,t \geq t_s \end{cases} \tag{11}$$

where Y_a and Y_r show the attacked and real signals, respectively, t_s is the time that the FDI attack imposes on the system. In scaling FDI attacks, the targeted signal is modified regarding the scaling parameter d_s as follows:

$$\begin{cases} Y_a = Y_r & ,t < t_s \\ Y_a = d_s \times Y_r & ,t \geq t_s \end{cases} \tag{12}$$

The scaling parameter d_s causes three states negative compensation ($d_s < 0$), under-compensation ($d_s < 1$) and over-compensation ($d_s > 1$). In the current work, the FDI attack targeting the frequency signal is modelled as follows:

$$\begin{cases} Y_a = Y_r & ,t < t_s \\ Y_a = d_s \times Y_r + d_e & ,t \geq t_s \end{cases} \tag{13}$$

In this equation, d_s and d_e are time-dependent disruptions.

4 | Design of the Presented Defence Method

This section describes the design of the presented defence method to cope with FDI attacks in the studied power system. The presented defence method comprises a model-free observer, a detector and an event-trigger strategy. The presented observer estimates the targeted frequency signal and sends it to the detector. The parameters of the designed observer are tuned by a DRL algorithm. The detector calculates the difference between the observed and estimated frequency signals and compares it with a predefined threshold value. When the evaluated difference crosses the threshold value, the event-based triggering strategy replaces the observed frequency signal with the estimated signal for the secondary controller.

The presented model-free observer is described using the single-input and single-output equation as follows:

$$\begin{cases} x^{(n)} = f(x^{(n-1)}(t), x^{(n-2)}(t), \ldots, x(t), d(t), t) + bu(t), \\ y = x(t) \end{cases} \tag{14}$$

In this equation, n represents the plant order, u represents the plant input, y denotes the plant output, $d(t)$ is the external disturbance, b is considered as a constant and the unknown function $f(.)$ is the total uncertainty or disturbance in the system, both external and internal. Consider $h = df/dt$. In the case of a non-smooth function f, h corresponds to the generalized derivative of $f(.)$. Considering the uncertainty f as a state of the system (14), we can write Equation (14) as follows [32]:

$$\begin{cases} \dot{x}_1 = x_2(t), \\ \vdots \\ \dot{x}_{n-1}(t) = x_n(t), \\ \dot{x}_n(t) = x_{n+1}(t) + bu, \\ \dot{x}_{n+1}(t) = h(.) \end{cases} \tag{15}$$

where $X = [x_1, \ldots, x_{n+1}]^\tau \in \mathbb{R}^{n+1}$ is the system's state. For the uncertain system (14), the observer for calculating both the states and extended states is as follows:

$$\begin{cases} \dot{z}_1 = z_2 - \beta_1 fal(e_1, \alpha_1, \gamma), \\ \vdots \\ \dot{z}_{n-1} = z_n - \beta_{n-1} fal(e_1, \alpha_{n-1}, \gamma), \\ \dot{z}_n = z_{n+1} - \beta_n fal(e_1, \alpha_n, \gamma) + bu, \\ \dot{z}_{n+1} = -\beta_{n+1} fal(e_1, \alpha_{n+1}, \gamma), \end{cases} \tag{16}$$

where $\beta_i (i \in n+1)$, $e_1 = z_1 - x_1$ and $X = [z_1, \ldots, z_{n+1}]^\tau \in \mathbb{R}^{n+1}$ represent the observer's gains, the observed error and the observer's state variable, respectively. Moreover, $fal(e, \alpha, \gamma)$ can be defined as [32]:

$$fal(e, \alpha, \gamma) = \begin{cases} |e|^\alpha sgn(e), & |e| > \gamma \\ \frac{e}{\gamma^{1-\alpha}}, & otherwise \end{cases} \tag{17}$$

where $0 \leq \alpha \leq 1$, $\gamma > 0$. It should be noted that the observer is intended to include the following feature $z_i(t) \to x_i(t) (i \in n+1)$. Moreover, when $\alpha_i = 1 (i \in n+1)$, Equation (16) describes a Luenberger observer in classical form. However, when $\alpha_i = 0 (i \in n+1)$, Equation (16) follows the form of the sliding mode observer.

The observer (16) can be linearized with $\alpha_i = 1 (i \in n+1)$ which is defined as follows:

$$\begin{cases} \dot{z}_1 = z_2 - \beta_1 e_1, \\ \vdots \\ \dot{z}_{n-1} = z_n - \beta_{n-1} e_1, \\ \dot{z}_n = z_{n+1} - \beta_n e_1 + bu, \\ \dot{z}_{n+1} = -\beta_{n+1} e_1, \end{cases} \tag{18}$$

The variables are selected in a specific way as $s^{n+1} + \beta_1^n + \cdots + \beta_{n+1} = (s + \omega_0)^{n+1}$, where ω_0 corresponds to the linearized observer bandwidth (18). It should be noted that the observer is designed using Equations (16) and (17) when no attack has occurred in the system. The proposed method does not require a detailed model of the studied system and extensive historical data. This method is robust against disturbances and system uncertainties. The proposed observer is inherently a model-free and low-order estimator. The structure of this observer requires only basic algebraic and differential operations and does not depend on heavy computations in real time. No online optimization algorithm is necessary during real-time operation. This ensures that the proposed method can be applied to any real power system with the least computational complexity. Since the presented

method does not depend on a detailed system model, it decreases its sensitivity to parameter uncertainties and modelling errors. Moreover, the method operates in parallel with the AGC loop without depending on the detailed AGC configuration. Therefore, even in the case of a malfunction in the proposed method, the AGC loop-based frequency regulation remains unchanged, ensuring that system stability is not compromised.

4.1 | Stability Analysis

This subsection provides the stability analysis of the proposed defence method.

Theorem 1. *Assume that the observer's gains satisfy* $\beta_i \geq \beta_{\min} > 0$ *for all* $i = 1, \ldots, n+1$, *and the disturbance* $d(t)$ *satisfies* $|d(t)| \leq \bar{d} < \infty$. *Therefore, the* $e_1(t)$ *is exponentially stable in the case without any disturbance and input-to-state for bounded disturbances, that is, there exist constants* $c, \rho > 0$ *such that:*

$$|e_1(t)| \leq |e_1(0)|e^{-ct} + \rho\,\bar{d}. \tag{19}$$

Proof. Consider the following vector:

$$\zeta = \begin{bmatrix} z_1 & z_2 & \cdots & z_{n+1} \end{bmatrix}^\top, \tag{20}$$

and the following Lyapunov function:

$$V(\zeta) = \tfrac{1}{2}\|\zeta\|^2. \tag{21}$$

By substituting Equation (18) into the derivative V ($\dot{V}$) and considering the disturbance $d(t)$, we have:

$$\dot{V} \leq -c_1\|\zeta\|^2 + c_2|e_1|\,|d(t)|, \tag{22}$$

Since e_1 is a linear function of ζ, there exists $k_e > 0$ such that:

$$|e_1| \leq k_e\|\zeta\|. \tag{23}$$

Substituting Equation (23) into Equation (22) and applying Young's inequality yields:

$$\dot{V} \leq -\tfrac{c_1}{2}\|\zeta\|^2 + \frac{c_2^2 k_e^2}{2c_1}d^2(t). \tag{24}$$

Since $\|\zeta\|^2 = 2V$, inequality (24) becomes

$$\dot{V} \leq -\alpha V + \beta d^2(t), \qquad \alpha = \tfrac{c_1}{1},\ \beta = \tfrac{c_2^2 k_e^2}{2c_1}. \tag{25}$$

Solving Equation (25) gives:

$$V(t) \leq V(0)e^{-\alpha t} + \tfrac{\beta}{\alpha}\bar{d}^2(1 - e^{-\alpha t}). \tag{26}$$

Hence,

$$\|\zeta(t)\| \leq \|\zeta(0)\|e^{-\alpha t/2} + \sqrt{\tfrac{\beta}{\alpha}}\bar{d}, \tag{27}$$

By Equation (23), the bound (19) for $e_1(t)$ obtains with $c = \alpha/2$ and $\rho = k_e\sqrt{\beta/\alpha}$. □

This shows that the $e_1(t)$ converges exponentially to zero in the absence of disturbances, while in their presence it remains proportionally bounded to $\bar{d}$. Therefore, the proof is completed.

The observer's parameters are tuned by a DRL algorithm. By employing a trained agent, a DRL algorithm allows a machine to adapt and learn a targeted task in a dynamic and unknown environment. The agent transmits actions according to observations and rewards from the environment. The success of an action is assessed by how well it achieves its purpose. Regarding a state-action mapping policy s_t, agents select the most effective action (a_t) in the action space (A) for the current state of the environment ($\pi(a_t|s_t)$). After every action, the agent obtains a reward r_t and the environment varies to a new state s_{t+1}. For all states, this procedure is performed again to maximize agents' expectations regarding discount rewards $R_t = \sum_{k=0}^{\infty}\gamma^k r_{t+k}$, where γ represents a discount factor between 0 and 1 [6].

Typically, an agent comprises a policy and a learning algorithm. In the policy, actions are specified according to observations. Also, the learning algorithm's policy parameters are progressively tuned regarding observations, actions and rewards. This paper uses a deep deterministic policy gradient (DDPG) algorithm, considered an off-policy alternative among RL algorithms. Utilizing DDPG to determine the optimal policy focuses on maximizing the forecasted cumulative reward across the long term. This algorithm applies two actor–critic deep neural networks, characterized by continuous state and action spaces, to facilitate stable and resilient learning. By mapping an environment state to a certain action, the actor–network of weight θ^μ sets the current policy $\mu(s_t|\theta^\mu)$. The critic network is $Q(s_t, a_t|\theta^\mu)$, having a weight of θ^Q. To minimize the loss function, the critic network parameters are adjusted through stochastic gradient descent [6]:

$$L(\theta^Q) = E_{(s,a)}[(y_t - Q(s_t, a_t|\theta^\mu))^2] \tag{28}$$

where y_t can be computed as follows:

$$y_t = r_t(s_t, a_t) + \gamma Q(s_{t+1}, \mu(s_t|\theta^\mu)|\theta^Q) \tag{29}$$

Moreover, the actor–network parameters are tuned by Equation (30):

$$\nabla_{\theta^\mu}J^{\theta^\mu} \approx \mathbb{E}_{s_t\sim\rho^\beta}[\nabla_a Q(s, a|\theta^Q)|_{a=\mu^\theta(s)}\nabla_{\theta^\mu}\mu(s|\theta^\mu)] \tag{30}$$

In this equation, β shows a specific policy to the current policy of π and ρ is the state distribution discount.

After estimating the frequency signal by the observer, the detector $\mathcal{D}$ receives the estimated and observed frequency signals. The $\mathcal{D}$ calculates the residual signal of the system output as follows:

$$r_f = f - \hat{f} \tag{31}$$

where r_f and $\hat{f}$ are the residual and estimated frequency signals, respectively. After calculating the residual signal, the $\mathcal{D}$ compares the absolute of r_f with a predetermined value to identify the attack as follows:

$$\mathcal{D} = \begin{cases} |r_f| \geq \mathrm{Th_v}, \text{ Attack has been occurred} \\ |r_f| < \mathrm{Th_v}, \text{ No attack} \end{cases} \tag{32}$$

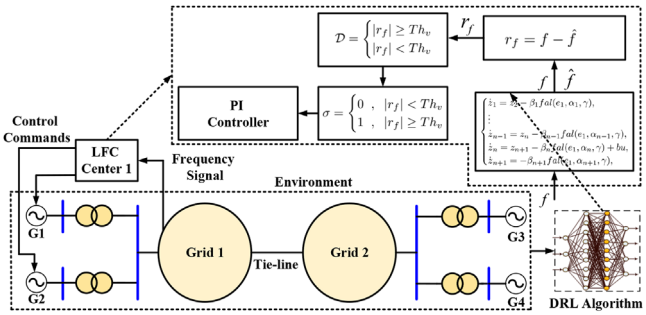

FIGURE 3 | Power system structure equipped with the proposed defence method.

where $\mathrm{Th_v}$ is the threshold value. When an attack is identified, the event-trigger strategy is applied to minimize the effect of the attack on the frequency response of the system. To this end, the event-trigger strategy blocks the observed frequency signal and forwards the estimated frequency signal to the secondary frequency controller. In this regard, the event-trigger strategy output (σ) is represented as follows:

$$\sigma = \begin{cases} 0, & |r_{\mathrm{f}}| < \mathrm{Th_v} \\ 1, & |r_{\mathrm{f}}| \geq \mathrm{Th_v} \end{cases} \tag{33}$$

According to Equation (33), when no attack occurs in the system ($|r_{\mathrm{f}}| < \mathrm{Th_v}$), the event-trigger strategy output is equal to 0 and the observed frequency signal is transmitted to the secondary controller. When an attack is identified ($|r_{\mathrm{f}}| \geq \mathrm{Th_v}$), the event-trigger strategy output represents the value of 1 and submits the estimated frequency signal to the secondary controller. Figure 3 depicts the power system structure equipped with the proposed defence approach. Also, Figure 4 illustrates the flowchart of the developed defence mechanism. The proposed defence method is model-free and depends only on measurable outputs of the system. The method is used for the signals vulnerable to cyber-attacks and independent of the precise modelling of AGC participant units. Therefore, an increase in the number of AGC participant units does not increase the computational burden of the developed method.

5 | Real-Time Results

This section evaluates the effectiveness of the implemented defence structure in identifying and mitigating FDI attacks imposed on the frequency signal of the Kundur's 4-unit-12-bus power system under different scenarios. The frequency response of the power system under study is obtained without any defence method and with the proposed defence method in MATLAB/Simulink software. Moreover, the proposed defence method's effectiveness is compared with the FOPID controller-based defence method presented in [33]. The values associated with the power system characteristics are available in [31]. The threshold value $\mathrm{Th_v}$ is considered to be 0.03. The OPAL-RT real-time simulator illustrated in Figure 5 is used to validate the implementation of the developed defence approach on real-time applications.

A. Scenario 1

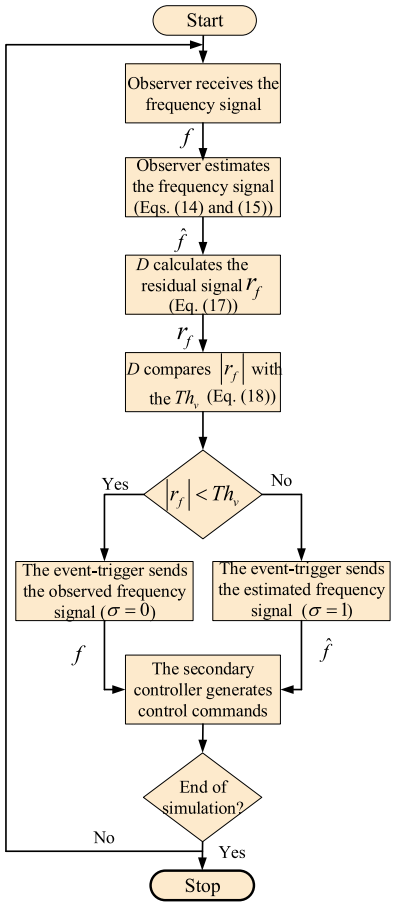

FIGURE 4 | Flowchart of the implemented defence method.

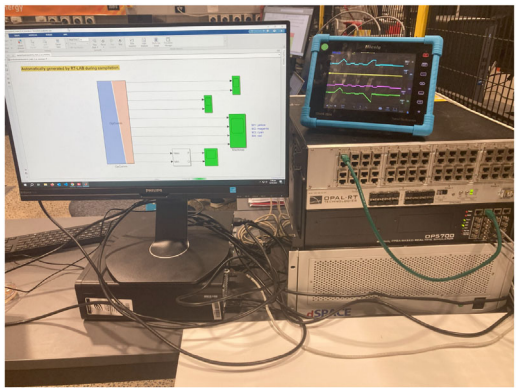

FIGURE 5 | OPAL-RT real-time simulator.

The frequency signal is attacked by an exogenous FDI attack in this scenario. First, a ramp disruption with a slope of 1 Hz is injected into the frequency signal at $100 < t \leq 108$ s. Then, the frequency signal is subjected to pulse disruptions at amplitudes of 0.6 Hz and 0.8 Hz within the time windows $112 < t \leq 116$ and $120 < t \leq 124$ s, respectively. After that, a ramp disruption with a slope of −1 Hz is applied to the frequency signal at $128 < t \leq 136$ s. Finally, a sinusoidal disturbance in the format of "$0.3\sin(t) + 0.4$" is imposed on the frequency signal at $140 < t \leq 152$ s.

Figure 6 demonstrates the frequency response of the system without defence method, FOPID controller-based defence method

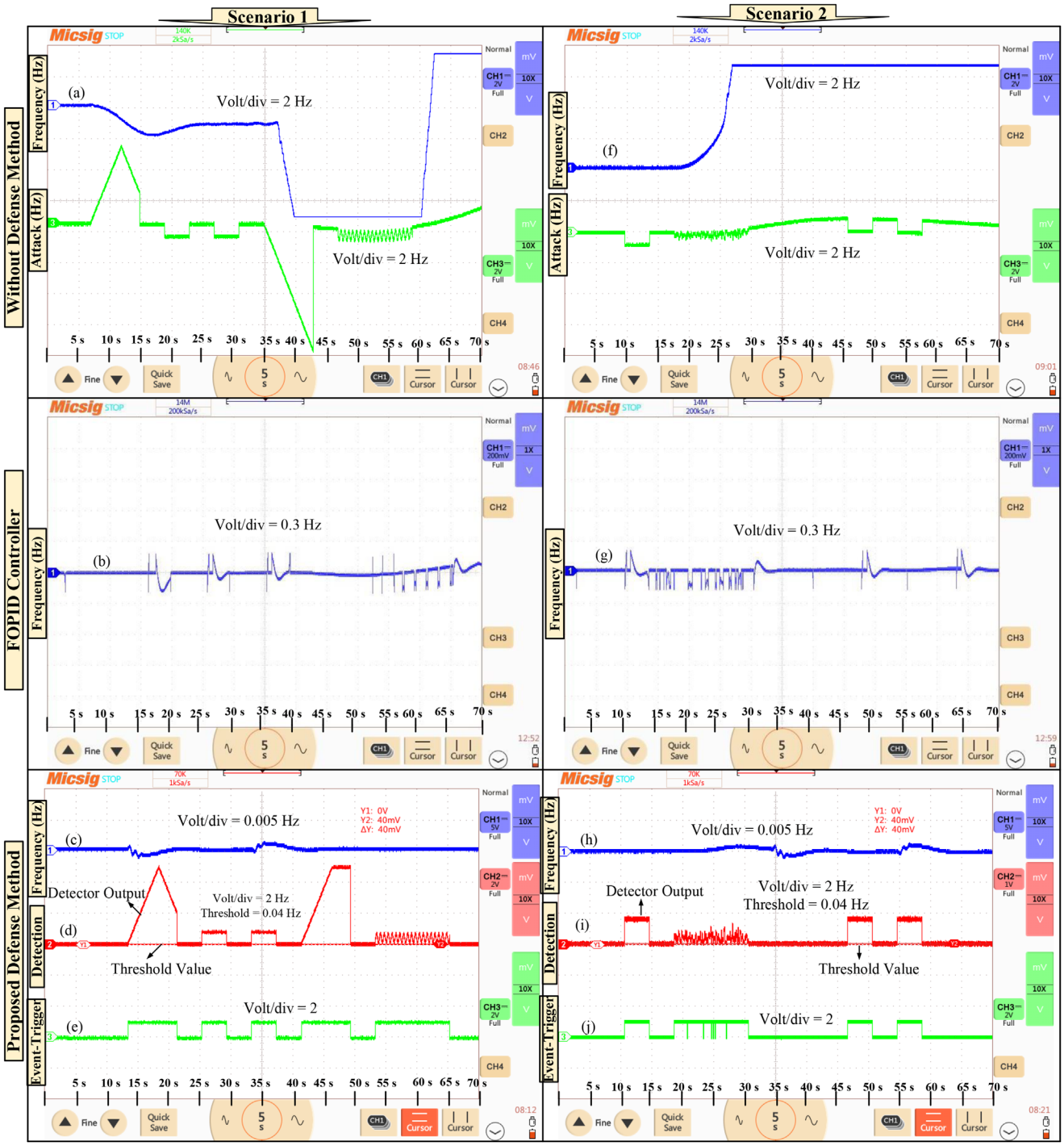

FIGURE 6 | Real-time results of the considered defence methods under different scenarios.

and the proposed defence method under different scenarios. According to Figure 6a, the system frequency response (blue curve) without a defence method greatly varies from the nominal value when the power system is targeted with FDI attacks and the system stability is seriously compromised. As a result, it is important to design an efficient defence strategy to mitigate effects of attacks on the system frequency performance. Figure 6b shows the system frequency response using the FOPID controller-based defence method under Scenario 1. As shown, employing a defence method provides a much better response compared to the "without defence method" case and the frequency oscillations are mitigated. The frequency signal attained by the proposed defence method is illustrated in Figure 6c. It is evident that the system frequency response remains at the nominal value even though the frequency measurement is falsified by FDI attacks. As shown, the proposed method can significantly enhance the system frequency response than the FOPID controller-based defence method under FDI attacks. Figure 6d illustrates the performance of the developed defence method in identifying FDI cyber-attacks under Scenario 1. According to this figure, the detector output (red curve) exceeds the threshold of 0.03 (red line) when the power system is targeted by FDI attacks. Regarding Equation (32),

exceeding the $|r_f|$ form the Th_v clears that an attack has occurred. Hence, it can be said that the developed defence approach can identify FDI attacks on time. After an attack is detected, the event trigger strategy blocks the falsified frequency signal and sends the estimated frequency signal to the secondary controller. In this case, $\sigma = 1$ as depicted in Figure 6e. Accordingly, the proposed defence method has completely mitigated the effects of attacks on the system frequency performance.

B. Scenario 2

The frequency signal is targeted by the scaling and exogenous FDI attacks in this scenario. In this regard, the combination of the exogenous and scaling FDI cyber-attacks in the format of "$1.05f + 0.45$" are injected into the frequency signal at $100 < t \leq 104$. After that, a random FDI attack having a mean of 0.02 and variance of 0.05 is added to the frequency signal at $108 < t \leq 120$. At $136 < t \leq 140$, the frequency signal is manipulated by the "$1.03f + 0.55$" disruption. Eventually, the pulse disruption with the amplitude of 0.5 Hz is injected into the frequency signal at $144 < t \leq 148$.

Figure 6f shows the system frequency response without the proposed defence method for Scenario 2. According to this figure, the secondary and the primary frequency control loops are not capable of coping with FDI attacks applied to the power system. Hence, the frequency signal experiences a significant deviation and the system frequency stability is seriously threatened. Accordingly, an appropriate defence strategy should be employed in the secondary control loop. The system frequency signal using the FOPID controller-based defence method is depicted in Figure 6g. It is clear that employing a defence method can improve the system frequency response under cyber-attacks and presents a suitable dynamic signal than the "without defence method" case. The frequency response of the power system equipped with the proposed defence strategy is shown in Figure 6h. As shown in this figure, employing the developed defence method in the power system maintains the frequency at the nominal value when FDI attacks are present. Moreover, the proposed defence method provides a much better frequency response than the FOPID controller-based defence method. Therefore, the developed method is able to compensate for attacks' effects on the system frequency response. Figure 6i demonstrates the detection performance of the proposed defence strategy under Scenario 2. As shown, the red curve related to the detector output is above the threshold value of 0.03 (red line) when FDI attacks are applied to the power system in the mentioned time ranges. As a result, the designed FDI attacks are detected on time. In the developed defence strategy structure, the falsified frequency signal is blocked by the event-trigger mechanism and the estimated frequency signal is submitted to the PI controller. Hence, $\sigma = 1$ as depicted in Figure 6j. Accordingly, the presented defence strategy completely mitigates the impact of FDI attacks on the frequency response of the system, as demonstrated in Figure 6g.

6 | Conclusion

This paper investigated the LFC performance of a realistic power system under the frequency signal falsified by FDI attacks. Accordingly, a model-free resilient defence scheme, comprising a model-free detection scheme and an event-triggered mechanism, was proposed to deal with FDI attacks in Kundur's 4-unit-12-bus power system. Unlike available methods, the proposed strategy is independent of the system's mathematical model and historical data and can be employed in any power system. Moreover, the design process of this strategy is simple and independent of the size and complexity of the power system. In the proposed defence scheme structure, a model-free observer estimated the targeted frequency signal and the detector calculated the residual frequency signal without requiring the state-space equations and historical data. The parameters of the presented model-free observer were tuned by a DRL algorithm. After calculating the residual signal, the detector compared it with a predetermined threshold value. When the residual signal exceeded the threshold value, the attack was detected. Then, an event-trigger strategy was employed to reduce the attacks' effects on the system frequency response. To do that, the event-trigger mechanism blocked the manipulated frequency signal and submitted the estimated frequency signal when the FDI attack was detected. The real-time experimental results obtained by the OPAL-RT simulator indicated that the proposed scheme timely detected FDI attacks and completely mitigated FDI attacks on the system frequency response under different scenarios.

In future work, the defence performance of the proposed scheme will be evaluated under replay and DoS attacks in Kundur's 4-unit-12-bus power system.

Author Contributions

Soroush Oshnoei: investigation, methodology, software. **Rasool Peykarporsan:** investigation, validation, visualization. **Jalal Heidari:** investigation, visualization, writing – original draft, writing – review & editing. **Esmaeil Mahboubi-Moghaddam:** data curation, formal analysis, validation. **Tek Tjing Lie:** supervision, validation, writing – review & editing. **Mohammad-Hassan Khooban:** supervision, visualization, writing – review & editing.

Funding

The authors have nothing to report.

Conflicts of Interest

The authors declare no conflicts of interest.

Data Availability Statement

Research data are confidential.

References

1. Y. Cui, T. Wu, and Y. Zhang, "Load Frequency Control of Smart Grid Based on Data-Driven FDI Attacks Detection and Data Repair,"*IEEE Transactions on Smart Grid* (2025).

2. S. Oshnoei, J. Heidari, E. Mahboubi-Moghaddam, M. Gheisarnejad, and M.-H. Khooban, "Identification and Mitigation of Data Integrity Stealth Attacks in Frequency Regulation of Power Systems," *IEEE Transactions on Information Forensics and Security* 20 (2025): 6133–6148.

3. Z. Hu, S. Liu, W. Luo, and L. Wu, "Credibility-Based Secure Distributed Load Frequency Control for Power Systems Under False Data Injection

Attacks," *IET Generation, Transmission & Distribution* 14, no. 17 (2020): 3498–3507.

4. A. Oshnoei, M. Kheradmandi, R. Khezri, et al., "Intelligent Coordination of Traditional Power Plants and Inverters Air Conditioners Controlled With Feedback-Corrected MPC in LFC," *IEEE Transactions on Circuits and Systems I: Regular Papers* 71, no. 1 (2023): 473–484.

5. S. Oshnoei, E. Mahboubi-Moghaddam, and M. H. Khooban, "Advanced Defense Strategy for Cyber-Resilient Frequency Control in Real Power Grids," *IEEE Transactions on Automation Science and Engineering* 22 (2025): 19366–19376.

6. S. Oshnoei, M. R. Aghamohammadi, J. Heidary, and M. H. Khooban, "Watermarking-Based Defense Mechanism in LFC of Electricity Grids Compromised by Covert Attacks," *IEEE Transactions on Circuits and Systems II: Express Briefs* 71, no. 10 (2024): 4576–4580.

7. S. Oshnoei and M. Aghamohammadi, "Detection and Mitigation of Coordinate False Datainjection Attacks in Frequency Control of Power Grids," in *2021 11th Smart Grid Conference (SGC)* (IEEE, 2021), 1–5.

8. S. R. Jelodar, J. Heidary, R. Rahmani, B. Vahidi, and H. Askarian-Abyaneh, "Frequency Control Using Fuzzy Active Disturbance Rejection Control and Machine Learning in a Two-Area Microgrid Under Cyber-attacks," *IET Generation, Transmission & Distribution* 18, no. 15 (2024): 2521–2542.

9. S. Beura and B. P. Padhy, "Implementation of Novel Reduced-Order H Filter for Simultaneous Detection and Mitigation of FDI-Attacks in AGC Systems," *IEEE Transactions on Instrumentation and Measurement* 72 (2022): 1–12.

10. Y. Liu, Y. Chen, and M. Li, "Dynamic Event-Based Model Predictive Load Frequency Control for Power Systems Under Cyber Attacks," *IEEE Transactions on Smart Grid* 12, no. 1 (2020): 715–725.

11. J. Wang, D. Wang, L. Su, J. H. Park, and H. Shen, "Dynamic Event-Triggered H Load Frequency Control for Multi-Area Power Systems Subject to Hybrid Cyber Attacks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 52, no. 12 (2022): 7787–7798.

12. D. Du, C. Zhang, X. Li, M. Fei, T. Yang, and H. Zhou, "Secure Control of Networked Control Systems Using Dynamic Watermarking," *IEEE Transactions on Cybernetics* 52, no. 12 (2021): 13609–13622.

13. R. M. Ferrari and A. M. Teixeira, "A Switching Multiplicative Watermarking Scheme for Detection of Stealthy Cyber-Attacks," *IEEE Transactions on Automatic Control* 66, no. 6 (2020): 2558–2573.

14. S. Oshnoei, M. R. Aghamohammadi, and M. H. Khooban, "Smart Frequency Control of Cyber-Physical Power System Under False Data Injection Attacks," *IEEE Transactions on Circuits and Systems I: Regular Papers* 71, no. 12 (2024): 5582–5595.

15. S. Yang, K.-W. Lao, H. Hui, J. Su, and S. Wang, "Secure Frequency Regulation in Power System: A Comprehensive Defense Strategy Against FDI, DOS, and Latency Cyber-Attacks," *Applied Energy* 379 (2025): 124772.

16. Z. Wang and H. Zhang, "Adaptive-Memory Event-Triggered Load Frequency Control for Multi-Input-Delay Power Systems Against FDI Attacks and Sensor Faults," *IEEE Transactions on Circuits and Systems II: Express Briefs* 71, no. 12 (2024): 4919–4923.

17. X. He, R. Zhang, and P. Wang, "A New Attack Recovery Approach and H Performance Analysis for LFC Systems With FDI Attacks and Uncertainties," *IEEE Access* 13 (2025): 23399–23411.

18. W. Guo, F. Liu, Y. Wang, D. Sidorov, and J. Wu, "Adaptive Event-Triggered Sliding Mode Load Frequency Control for Cyber-Physical Power Systems Under False Data Injection Attacks," *IEEE Transactions on Industrial Informatics* 21, no. 4 (2024): 2947–2956.

19. X. He, X. Liu, and P. Li, "Coordinated False Data Injection Attacks in AGC System and its Countermeasure," *IEEE Access* 8 (2020): 194640–194651.

20. A. Ayad, M. Khalaf, M. Salama, and E. F. El-Saadany, "Mitigation of False Data Injection Attacks on Automatic Generation Control Considering Nonlinearities," *Electric Power Systems Research* 209 (2022): 107958.

21. P. P. Singh, R. Shankar, and S. Singh, "Chaos Quasi-Opposition Crayfish Based Modified New Controller Designed for Hybrid Deregulated Power Environment Considering Cyber-Attack," *Chaos, Solitons & Fractals* 187 (2024): 115444.

22. J. Heidary, S. Oshnoei, M. Gheisarnejad, M. R. Khalghani, and M. H. Khooban, "Shipboard Microgrid Frequency Control Based on Machine Learning Under Hybrid Cyberattacks," *IEEE Transactions on Industrial Electronics* 71, no. 7 (2023): 7136–7146.

23. Z. Zhang, J. Hu, J. Lu, J. Cao, and J. Yu, "False Data Injection Attacks on LFC Systems: An AI-Based Detection and Countermeasure Strategy," *IEEE Transactions on Circuits and Systems I: Regular Papers* 71, no. 5 (2023): 1969–1977.

24. A. Saxena, R. Shankar, C. Kumar, and S. Parida, "A Resilient Frequency Regulation for Enhancing Power System Security Against Hybrid Cyber-Attacks," *IEEE Transactions on Industry Applications* 60, no. 3 (2024): 4583–4597.

25. S. Oshnoei, M. R. Aghamohammadi, and M.-H. Khooban, "Model-Free Predictive Frequency Control Under Sensor and Actuator FDI Attacks," *IEEE Transactions on Circuits and Systems II: Express Briefs* 71, no. 4 (2023): 2434–2438.

26. M. Ranjan, R. Shankar, U. Raj, S. Kumar, and J. Kumar, "Cyber-Attack and Defense Method for Load Frequency Control in Smart Grid Systems With Electric Vehicles," *Optimal Control Applications and Methods* 45, no. 6 (2024): 2722–2747.

27. A. Saxena and R. Shankar, "An Interactive Operating Demand Response Approach for Hybrid Power Systems Integrating Renewable Energy Sources," *Protection and Control of Modern Power Systems* 9, no. 3 (2024): 174–194.

28. S. Murali, P. Saini, K. Abhinav, R. Shankar, and S. Parida, "Improved LSTM-Based Load Forecasting Embedded 3DOF (FOPI)-FOPD Controller for Proactive Frequency Regulation in Power System," *IEEE Transactions on Industry Applications* 60, no. 6 (2024): 8213–8227.

29. S. Murali, R. Shankar, P. Sharma, and S. Singh, "Assessment of Power System Resiliency With New Intelligent Controller and Energy Storage Systems," *Electric Power Components and Systems* 52, no. 8 (2024): 1414–1436.

30. K.-D. Lu and Z.-G. Wu, "Resilient Event-Triggered Load Frequency Control for Cyber-Physical Power Systems Under DOS Attacks," *IEEE Transactions on Power Systems* 38, no. 6 (2022): 5302–5313.

31. P. Kundur, "Power System Stability," *Power system stability and control* 10, no. 1 (2007): 7–11.

32. S. K. Panda and B. Subudhi, "An Extended State Observer Based Adaptive Backstepping Controller for Microgrid," *IEEE Transactions on Smart Grid* 15, no. 1 (2023): 171–178.

33. R. C. Khamari, P. K. Ray, M. K. Senapati, and S. Padmanaban, "Resilient Microgrid Frequency Control Under Cyber Threats With Experimental Validation Using MIWO-FOPID Controller," *IEEE Transactions on Consumer Electronics* 71, no. 3 (2025): 7920–7932.