2023 IEEE IAS Global Conference on Renewable Energy and Hydrogen Technologies (GlobConHT)
The Maldives National University, Male City (Maldives). Mar 11-12, 2023

2023 IEEE IAS Global Conference on Renewable Energy and Hydrogen Technologies (GlobConHT) | 979-8-3503-3211-7/23/$31.00 ©2023 IEEE | DOI: 10.1109/GLOBCONHT56829.2023.10087633

A Resilient Controller for Frequency Regulation of Power Grids against Cyber Attacks

Shaohua Yang
State Key Laboratory of Internet of Things for Smart City; *Department of Electrical and Computer Engineering, University of Macau*
Macao, China
yc17436@um.edu.mo

Keng-Weng Lao
State Key Laboratory of Internet of Things for Smart City; *Department of Electrical and Computer Engineering, University of Macau*
Macao, China
johnnylao@um.edu.mo

Hongxun Hui
State Key Laboratory of Internet of Things for Smart City; *Department of Electrical and Computer Engineering, University of Macau*
Macao, China
hongxunhui@um.edu.mo

Yulin Chen
Hainan Institute of Zhejiang University
Sanya, China
chenyl2017@zju.edu.cn

***Abstract*—Maintaining system frequency at a rated value is a fundamental requirement to ensure the stability and security of power grids. However, the advanced frequency regulation process is more cyber-dependent, and raises a cyber-security issue for the power system. Traditional methods cannot avoid the adverse impacts of cyber attacks, which may lead to frequency deviations and, in severe cases, even blackouts. To address this issue, we propose an attack-resilient control algorithm for the smart grid's frequency regulation to defend the system frequency against cyber attacks. The stability of the system with the proposed controller can be guaranteed, which is strictly proved by Lyapunov theorem. Furthermore, the effectiveness of the proposed resilient controller is validated by case studies. The results show that in comparison with the existing methods, the proposed controller can make the system frequency achieve faster recovery with a minor frequency deviation. Specifically, using the proposed method, the maximum frequency deviation can be reduced from 0.17 Hz to approximately 0 Hz even under a cyber attack, which means that the adverse effects of a cyber attack can be almost eliminated. Therefore, the proposed controller can well counter potential cyber attacks, which helps improve the stability of the system frequency.**

***Index Terms*—Power grid, frequency regulation, cyber attack, resilient control, Lyapunov theorem**

I. Introduction

FOR the stable and secure operation of the power grid, the system frequency must be controlled at the rated value [1]. However, the load consumption and the renewable generation in power grids are often changing [2], [3]. For example, according to real loading data reported by the Electric Reliability Council of Texas (ERCOT), the actual hourly load of an electric grid varies within the range of 35,993MWh to 45,056MWh in Texas, USA, on Jan 11, 2016 [4], [5]. These fluctuations in power consumption or generation cause deviations in the power grid frequency [6]. Therefore, stabilizing the system frequency becomes a challenge in practice.

This work was partly Funded by The Science and Technology Development Fund, Macau SAR (File/Project no. FDCT/0022/2020/A1, SKL-IOTSC-2021-2023, 0003/2020/AKP). (Corresponding author: *Keng-Weng Lao*.)

To improve the stability of system frequency, frequency regulation of power grids has received attention, and several studies have been performed recently. For example, based on a consensus control algorithm, the renewable generators are dispatched fairly to maintain the frequency stability [7]. In addition, considering limited communication bandwidth, a new load frequency control method is presented for smart grids [8]. Considering both the supply and demand sides, a coordinated control framework is proposed for distributed generators and virtual power plants to achieve better frequency performance of microgrids [9]. A control approach to suppress fluctuations is adopted by central air conditioners to provide regulation services for power grids and guarantee regulation accuracy [10]. As an emergency control strategy, bang-bang control is proposed for frequency regulation based on the Lyapunov method [11]. It is worth noting that in different frequency regulation control methods, proportional integral (PI) controllers are the most widely utilized in practical engineering [12]. Moreover, an improved PI controller is presented for frequency regulation affected by delays [13]. As mentioned above, much work has been done in the area of frequency regulation, and constructive progress has been made in these efforts.

However, one of the critical factors in the modern power grid, i.e., the potential cyber-attack, needs to be taken into account and addressed. In fact, modern smart grids rely on information, communication, and control technologies, which makes the power grid vulnerable to cyber attacks with potentially disastrous consequences [14]. For instance, in 2003, in the USA, cyber attacks resulted in the Davis-Besse nuclear power station being compromised [15]. In addition, in 2015, in Ukraine, malicious false data injection (FDI) attacks led to the compromise of the Ukrainian electric power system, which resulted in power outages lasting several hours [16]. Among different types of cyber attacks (e.g., the resonance attack, the FDI attack, and the denial of service (DoS) attack, and so on), the FDI attack is considered the most dangerous threat to

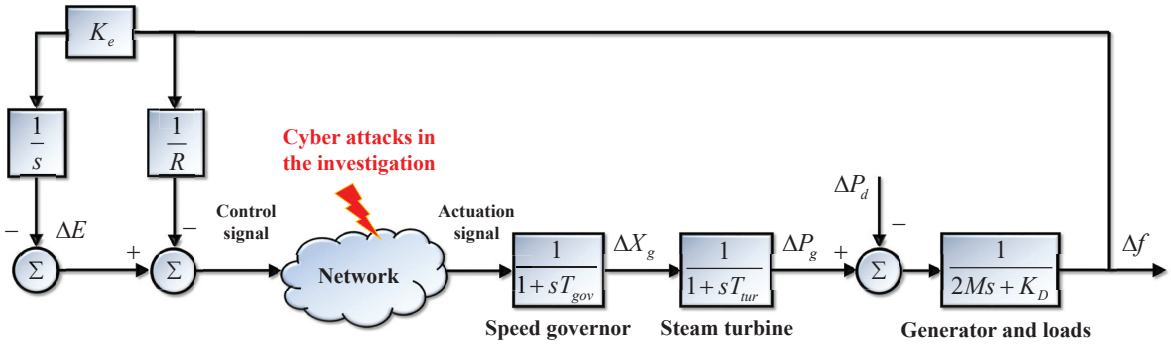

Fig. 1. Control block diagram of the frequency regulation system for power grids under cyber attacks.

modern smart grids' frequency regulation [17].

The threat of FDI attacks has been validated in many studies. For instance, Liu et al. [18] show that power system state estimation can be destroyed by FDI attacks. Moreover, the conclusion in [19] indicates that the FDI attacks may result in the control failure of power systems. In addition, literature [20] shows that an FDI attack may result in reduced power generation efficiency, drive-train overload, shutdowns, and even possibly equipment damage to wind turbines. It is known from these existing efforts that FDI attacks raise new security challenges to power grids. However, considering the frequency regulation of power grids, the FDI attack problem still needs to be fully addressed.

To address the problem, a novel attack-resilient controller is proposed for frequency regulation to defend the system frequency against cyber attacks. Using the proposed controller, the system frequency can be controlled at the rated value even under cyber attacks. Moreover, the system with the proposed controller can be stable by theoretical proof of Lyapunov theorem. The attack-resilient controller proposed for frequency regulation contributes to the stable and secure operation of power grids.

The remainder of this article is organized as follows. In Section II, the frequency regulation system is modeled considering cyber attacks. In Section III, a novel attack-resilient control algorithm is proposed. Case studies and verification can be found in Section IV, and then, this paper is concluded in Section V.

II. Frequency Regulation System Considering Cyber Attacks

In this section, the frequency regulation system of the power grid is modeled at first. Then, the model of the FDI attack is described. Finally, the dynamics of this system are developed considering cyber attacks.

A. Model of Frequency Regulation System for Power Grids

Fig. 1. presents the control block diagram of the frequency regulation system for power grids. This system consists of a governor, a turbine, a generator, and a controller. Here, variable states ΔX_g, ΔP_g, Δf, $\Delta E(t)$, and ΔP_d present the deviation of governor valve position, the deviation of turbine output, the deviation of system frequency of the frequency regulation system, the deviation of integral control and the power disturbance of load applied to the power grid, respectively. Denote M, R, K_D, K_e, s, T_{gov}, and T_{tur} as the equivalent inertia constant, the speed drooping coefficient, the equivalent damping coefficient, the integral control gain, the Laplace operator, the speed governor time constant, and the steam turbine time constant. The function of this frequency regulation system is to accommodate deviations in the system frequency. If system frequency deviation exceeds the threshold, e.g., over frequency threshold or under frequency threshold, the deviation will be sent back to the controller as a feedback signal. Then, the frequency regulation process starts, i.e., based on this feedback signal, the controller can yield control signals to mitigate the deviations of the system frequency. As described in [21], the most common controller utilized in frequency regulation systems is the PI controller, which can be described as follows:

$$PI(t) = -K_P \cdot \Delta f(t) - K_I \cdot \int \Delta f(t)\mathrm{d}t, \tag{1}$$

where $PI(t)$ is the control input of the PI controller, which is utilized to regulate the frequency deviation; K_P and K_I denote the controller gains.

According to the transfer function given in the control block diagram as Fig. 1 [22], [23], the dynamics is formulated as below:

$$\Delta\dot{f}(t) = -\frac{K_D}{2M}\Delta f(t) + \frac{1}{2M}\Delta P_g(t) - \frac{1}{2M}\Delta P_d(t) \tag{2}$$

$$\Delta\dot{P}_g(t) = -\frac{1}{T_{tur}}\Delta P_g(t) + \frac{1}{T_{tur}}\Delta X_g(t), \tag{3}$$

$$\Delta\dot{X}_g(t) = -\frac{1}{RT_{gov}}\Delta f(t) - \frac{1}{T_{gov}}\Delta E(t) + \frac{1}{T_{gov}}u(t) - \frac{1}{T_{gov}}\Delta X_g(t), \tag{4}$$

$$\Delta\dot{E}(t) = K_e\Delta f(t). \tag{5}$$

where u is the auxiliary control input for secondary control.

The dynamic characteristics described in (2)-(5) can be reformulated into a matrix form, and in this way, the state space equation can be established as follows:

$$\dot{\boldsymbol{x}}(t) = \boldsymbol{A}\boldsymbol{x}(t) + \boldsymbol{B}\boldsymbol{u}(t) + \boldsymbol{D}\Delta P_d(t), \tag{6}$$

where

$$\boldsymbol{x}(t) = \begin{bmatrix}\Delta f(t) & \Delta P_g(t) & \Delta X_g(t) & \Delta E(t)\end{bmatrix}^{\mathrm{T}},$$

$$\boldsymbol{A} = \begin{bmatrix} -\frac{K_D}{2M} & \frac{1}{2M} & 0 & 0 \\ 0 & -\frac{1}{T_{tur}} & \frac{1}{T_{tur}} & 0 \\ -\frac{1}{RT_{gov}} & 0 & -\frac{1}{T_{gov}} & -\frac{1}{T_{gov}} \\ K_e & 0 & 0 & 0 \end{bmatrix},$$

$$\boldsymbol{B} = \begin{bmatrix}0 & 0 & \frac{1}{T_{gov}} & 0\end{bmatrix}^{\mathrm{T}},$$

$$\boldsymbol{D} = \begin{bmatrix}-\frac{1}{2M} & 0 & 0 & 0\end{bmatrix}^{\mathrm{T}}.$$

B. False Data Injection Attacks

As reported in the literature review, cyber attacks have become a critical threat to industrial power grids [14], [16], [19]. In fact, the frequency regulation system is a cyber-physical system, whose processes involve a large number of information exchange and communication links. As a result, the frequency regulation system is indeed vulnerable to FDI attacks.

In addition, as an important function for the secure and stable operation of power grids, the frequency regulation system under FDI attacks can lead to severe problems and even blackouts. Attacking control signals is the most direct and powerful way of attack that affects the system's working, which is what this paper focuses on. When the control signal is hacked by an FDI attack, the corrupted control signal of the frequency regulation will include injected data [18], which can be represented as follows:

$$\widetilde{v}(t) = v(t) + \gamma(t)\psi(t), \tag{7}$$

where $v(t)$ is an original control signal of the frequency regulation at the time t; $\widetilde{v}(t)$ is the corrupted control signal under the FDI attack; and $\gamma(t)$ is a binary function where $\gamma(t) = 1$ implies that the FDI attack is launched at time t, and conversely, $\gamma(t) = 0$ implies no attack presence; $\psi(t)$ is the injected false data of attack.

In practice, it is impossible for a hacker to inject an unlimited variable as an attack signal. Hence, the malicious fault data ψ injected by hackers need to be constrained, which could be more realistic. Specifically, the attack data under consideration has a boundary, which can be stated as follows:

$$||\psi(t)|| < \delta. \tag{8}$$

where δ is a positive constant, which denotes the boundary of attack data.

C. Frequency Regulation System with Attack

Under the FDI attacks, the final control input implemented by the actuator is altered. As a result, the system described in (6) with the FDI attack is reformulated as follows:

$$\dot{\boldsymbol{x}}(t) = \boldsymbol{A}\boldsymbol{x}(t) + \boldsymbol{B}(\boldsymbol{u}(t) + \boldsymbol{\gamma}(t)\boldsymbol{\psi}(t)) + \boldsymbol{D}\Delta P_d(t), \tag{9}$$

where $\boldsymbol{\psi}(t) = [\psi_1(t)\ \psi_2(t)\ \cdots\ \psi_n(t)]^{\mathrm{T}}$ is the vector of injected false data; $\boldsymbol{\gamma}(t) = \mathrm{diag}\,[\psi_1(t)\ \psi_2(t)\ \cdots\ \psi_n(t)]^{\mathrm{T}}$ is the diagonal matrix to describe the presence of the FDI attack at this moment.

Therefore, under the FDI attack, the actuators cannot accurately receive the original control signals sent from the controller. On the contrary, the received actuator signals of the frequency regulation system are interrupted and maliciously injected with additional information by the hackers. As a result, the dynamics of the control system are modified differently, and the grid's system frequency is hard to control at the original control target, i.e., maintained at the rated value.

III. Proposed Attack-resilient Control Algorithm

To counter against FDI attacks, we propose a resilient control algorithm based on the sliding mode control, which can protect frequency regulation systems and maintain power grids' frequency. First, a surface is designed by using Lyapunov theorem to eliminate the attack impact. And then, a control algorithm is developed to execute and thus avoid possible deviations or even instabilities caused by FDI attacks.

A. Surface Design to Eliminate Attack Impacts

In this subsection, the first step of the attack-resilient control algorithm is developed. We design a surface by using Lyapunov theorem to provide a reference guide for the control. On this Basis, the studied system can be stale even under the FDI attack.

The designed surface is presented below:

$$\boldsymbol{B}^T\boldsymbol{P}\boldsymbol{x} = 0, \tag{10}$$

where $\boldsymbol{P}$ is a positive definite matrix. This matrix $\boldsymbol{P}$ is obtained from the Lyapunov equation, which is shown below:

$$\boldsymbol{A}_s^T\boldsymbol{P} + \boldsymbol{P}\boldsymbol{A}_s = -\boldsymbol{Q}, \tag{11}$$

where $\boldsymbol{A}_s$ denotes a stable matrix; $\boldsymbol{Q}$ is an arbitrary symmetric positive definite matrix.

According to the state feedback control, if the system pair (A, B) is controllable, then the system can be controlled by state feedback $\boldsymbol{u} = -\boldsymbol{K}\boldsymbol{x} + \boldsymbol{\nu}$. It is noted that to let $\boldsymbol{A} - \boldsymbol{B}\boldsymbol{K}$ possess n stable eigenvalues, the matrix $\boldsymbol{K}$ can be determined by the pole-placement method. Therefore, to guarantee the matrix $\boldsymbol{A}_s$ is stable, the feedback matrix $\boldsymbol{K}$ is introduced below.

The matrix $\boldsymbol{K}$ is designed through pole assignment such that the eigenvalues of matrix $\boldsymbol{A}_s = \boldsymbol{A} - \boldsymbol{B}\boldsymbol{K}$ are less than zero to obtain the positive definite matrix $\boldsymbol{P}$.

On this basis, the designed surface function can be shown as follows:

$$s(t) = \boldsymbol{B}^T\boldsymbol{P}\boldsymbol{x}, \tag{12}$$

The surface function given in (12) is a function of $\boldsymbol{x}$, and hence it changes with the system's variables. When variables

reach the designed surface, the surface function meets the following property:

$$s(t) = 0. \tag{13}$$

Theorem 1: The system dynamic performance can be stable even under FDI attacks when $\boldsymbol{s}(t) = 0$, i.e., the state variables reach the surface designed in (10)-(11).

Proof 1: Since we focus on the cyber attack problem, the FDI attack is present, and the load disturbances are not present in this case.

According to the feedback control $\boldsymbol{u} = -\boldsymbol{B}\boldsymbol{x} + \boldsymbol{\nu}$, the system in (9) can be reformulated as follows:

$$\dot{\boldsymbol{x}} = \boldsymbol{A}_s\boldsymbol{x} + \boldsymbol{B}\boldsymbol{\nu} + \boldsymbol{B}\boldsymbol{\psi}, \tag{14}$$

Constructing a Lyapunov function as follows:

$$V(\boldsymbol{x}) = \boldsymbol{x}^{\mathrm{T}}\boldsymbol{P}\boldsymbol{x}. \tag{15}$$

The derivative of the constructed Lyapunov function in (22) is derived below:

$$\begin{aligned}\dot{V}(\boldsymbol{x}) &= \dot{\boldsymbol{x}}^{\mathrm{T}}\boldsymbol{P}\boldsymbol{x} + \boldsymbol{x}^{\mathrm{T}}\boldsymbol{P}\dot{\boldsymbol{x}} \\ &= \left(\boldsymbol{A}_s\boldsymbol{x} + \boldsymbol{B}\boldsymbol{\nu} + \boldsymbol{B}\boldsymbol{\psi}\right)^{\mathrm{T}}\boldsymbol{P}\boldsymbol{x} \\ &+ \boldsymbol{x}^{\mathrm{T}}\boldsymbol{P}\left(\boldsymbol{A}_s\boldsymbol{x} + \boldsymbol{B}\boldsymbol{\nu} + \boldsymbol{B}\boldsymbol{\psi}\right) \\ &= \boldsymbol{x}^{\mathrm{T}}\boldsymbol{A}_s^{\mathrm{T}}\boldsymbol{P}\boldsymbol{x} + \boldsymbol{x}^{\mathrm{T}}\boldsymbol{P}\boldsymbol{A}_s\boldsymbol{x} + \left(\boldsymbol{B}\boldsymbol{\nu} + \boldsymbol{B}\boldsymbol{\psi}\right)^{\mathrm{T}}\boldsymbol{P}\boldsymbol{x} \\ &+ \boldsymbol{x}^{\mathrm{T}}\boldsymbol{P}\left(\boldsymbol{B}\boldsymbol{\nu} + \boldsymbol{B}\boldsymbol{\psi}\right) \\ &= -\boldsymbol{x}^{\mathrm{T}}\boldsymbol{Q}\boldsymbol{x} + 2\boldsymbol{\nu}^{\mathrm{T}}\boldsymbol{B}^{\mathrm{T}}\boldsymbol{P}\boldsymbol{x} + 2\boldsymbol{\psi}^{\mathrm{T}}\boldsymbol{B}^{\mathrm{T}}\boldsymbol{P}\boldsymbol{x}. \end{aligned} \tag{16}$$

Because the state variables reach the surface designed, i.e., $s(t) = 0$, we have:

$$s(t) = \boldsymbol{B}^{\mathrm{T}}\boldsymbol{P}\boldsymbol{x} = 0. \tag{17}$$

Then the derivative of the Lyapunov function can be reformulated as follows:

$$\begin{aligned}\dot{V}(\boldsymbol{x}) &= -\boldsymbol{x}^{\mathrm{T}}\boldsymbol{Q}\boldsymbol{x} + 2\boldsymbol{\nu}^{\mathrm{T}}\boldsymbol{B}^{\mathrm{T}}\boldsymbol{P}\boldsymbol{x} + 2\boldsymbol{\psi}^{\mathrm{T}}\boldsymbol{B}^{\mathrm{T}}\boldsymbol{P}\boldsymbol{x} \\ &= -\boldsymbol{x}^{\mathrm{T}}\boldsymbol{Q}\boldsymbol{x} + 0 + 0 \\ &= -\boldsymbol{x}^{\mathrm{T}}\boldsymbol{Q}\boldsymbol{x} < 0. \end{aligned} \tag{18}$$

According to (18), then the deviation of Lyapunov function $V(t)$ is always less than zero, which means this function is stable from the point of view of energy in Lyapunov theorem. In addition, the Lyapunov function designed in (15) implies that $V(t)$ is always larger than zero. As a result, the Lyapunov function $V(t)$ will tend to zero with time. At the same time, the state variables of the system $\boldsymbol{x}(t)$, which are variables of the Lyapunov function $V(t)$, will also converge to zero. This means the dynamic performance of the studied system is stable, even under FDI attacks.

The proof is complete. ■

Theorem 1 illustrates the effectiveness of the designed surface, because through the surface, the states of the power grid are stable even under cyber attacks.

B. Control Algorithm Development

Above, a surface is designed to provide stability, while the issue of how to get the trajectory to reach the surface hasn't been resolved. To this end, a control algorithm is designed to solve this issue by enabling the system's trajectory to be driven to and maintained on the designed surface. To design this control algorithm, a constant rate reaching law is employed, which can be shown below:

$$\dot{s}(t) = -m \cdot \operatorname{sgn}\left(s(t)\right), \tag{19}$$

where m is a positive constant; $\operatorname{sgn}(\cdot)$ denotes a mathematical function that extracts the sign of a real number, which can be shown as follows:

$$\operatorname{sgn}\left(s(t)\right) = \begin{cases} -1, & \text{if } s(t) < 0. \\ 0, & \text{if } s(t) = 0 \\ 1, & \text{if } s(t) > 0 \end{cases} \tag{20}$$

The control algorithm can be shown as follows:

$$\begin{aligned}\boldsymbol{u}(t) = &-m \cdot \left(\boldsymbol{B}^T\boldsymbol{P}\boldsymbol{B}\right)^{-1} \cdot \operatorname{sgn}\left(s(t)\right) \\ &- \delta \cdot \operatorname{sgn}\left(s(t)\right) - \left(\boldsymbol{B}^T\boldsymbol{P}\boldsymbol{B}\right)^{-1}\boldsymbol{B}^T\boldsymbol{P}\boldsymbol{A}\boldsymbol{x}, \end{aligned} \tag{21}$$

where $\boldsymbol{P}$ is a positive definite matrix obtained from (11), δ is a positive constant, which is the boundary of attack data.

Theorem 2: The analyzed system's track will always reach the surface designed in (10) when the controller in (21) is utilized, i.e., ensuring the designed surface's functionality.

Proof 2: According to (12) and (21), the surface function's derivative is derived as below:

$$\begin{aligned}\dot{s}(t) &= \boldsymbol{B}^T\boldsymbol{P}\dot{\boldsymbol{x}} \\ &= \boldsymbol{B}^T\boldsymbol{P}[\boldsymbol{A}\boldsymbol{x} + \boldsymbol{B}\boldsymbol{u} + \boldsymbol{B}\boldsymbol{\psi}] \\ &= \boldsymbol{B}^{\mathrm{T}}\boldsymbol{P}\boldsymbol{B}[\boldsymbol{\psi} - \operatorname{sgn}\left(s(t)\right) \cdot \delta] - m \cdot \operatorname{sgn}\left(s(t)\right). \end{aligned} \tag{22}$$

From (22), it can be known that $s(t)\dot{s}(t) < 0$, which means that the system's track can always be met to reach the surface.

The proof is complete. ■

The general procedure of the proposed resilient controller consists of setting the parameters, designing a surface (10), and formulating the control law (21). Through **Theorem 1** and **Theorem 2**, it is known that the track of the system can always reach the designed surface and eventually ensure the system's stability, i.e., the system frequency can be controlled at the rated value even under FDI attacks.

IV. Case Study and Verification

A. Test System

In this section, a frequency regulation system of the power grid (shown in Fig. 1) is established in MATLAB/Simulink environment to validate the effectiveness and advantages of the proposed resilient controller. The basic parameters settings of this tested system are provided in Table I; some of them refer to [22] and [23]. The rated frequency of the power system is 50 Hz, which is the control objective of the system frequency.

TABLE I
PARAMETERS OF FREQUENCY REGULATION SYSTEM FOR POWER GRID

Symbols	Parameters	Values	Units
T_{gov}	Speed governor time constant	0.2	s
T_{tur}	Steam turbine time constant	0.35	s
R	Speed drooping coefficient	0.05	–
K_e	Integral control gain	21.8	–
M	Equivalent inertia constant	12	–
K_D	Equivalent damping coefficient	1.8	–
S_n	Generation capacity	800	MW
f_r	Rated frequency	50	Hz

There are two different types of FDI attacks, which are the static FDI attack and the dynamic FDI attack. The static attack is a common FDI attack, whose advantage is that the injected data can be without further changes. Hence, the static attack is a low-cost attack method that is easy to launch successfully. Dynamic attacks are more difficult for attackers to implement since they require more resources to change the injected data in real time. However, they are also more challenging to detect, track, and defend. Therefore, both of these two types of attacks deserve attention.

The proposed resilient controller is validated under these two types of FDI attacks. On this basis, there are two scenarios, i.e., (1) the frequency regulation with the static attack, and (2) the frequency regulation with the dynamic attack. For comparison with the resilient controller, the traditional control method (PI control) is also implemented in the case studies.

The simulation process is presented as follows. At $t = 0$ s, the initial system frequency has a deviation of 0.1 Hz; after $t = 20$ s, the hacker maliciously launches a cyber attack against the controller of the tested system by injecting false data (i.e., FDI attack), and this round of attacks lasts one minute; at $t = 40$ s, a sudden load disturbance occurs in the tested power grid; at $t = 60$ s, this load disturbance is recovered; at $t = 80$ s, the cyber attack launched by the hacker is stopped. The total simulation time is 100 s. All the scenarios are illustrated as follows.

B. Verification of System Frequency Under a Static Attack

In the first scenario, it is assumed that the hacker launches a static FDI attack to compromise the control process of frequency regulation. Specifically, assume that the value of injected data is 0.1, which is not varying with time, shown as follows:

$$\psi(t) = 0.1. \tag{23}$$

The grid frequency is shown in Fig. 2. As illustrated in Fig. 2, during 0-20 s, the system frequency cannot be fully stabilized to the rated frequency by the traditional method. However, by the proposed method, the frequency deviation controlled can be controlled from the initial value of 0.1 Hz to a steady-state value of almost zero, i.e., the system frequency can converge to the rated frequency of 50 Hz.

At 20 s, the static FDI attack is launched by a hacker. During 20-40 s, the system frequency controlled by the traditional method fluctuates drastically by the interference due to the cyber attack, and the maximum frequency deviation reaches about 0.17 Hz. However, using the proposed method, the frequency deviation remains stable at almost zero, which implies that the proposed method is resistant to cyber attacks.

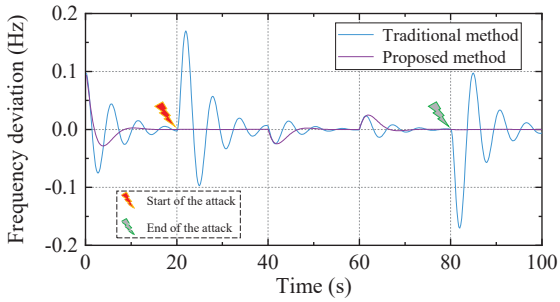

Fig. 2. The frequency of the power grid under a static FDI attack (starts at 20 s and ends at 80 s).

At 40 s, a sudden load disturbance occurs in the tested power grid. During 40-60 s, the system frequency controlled by the traditional method cannot be recovered to the rated frequency due to the load disturbance. However, using the proposed method, the frequency is rapidly recovered to 50 Hz, which implies that the proposed method also performs well in dealing with events such as load fluctuations.

At 60 s, this load disturbance is recovered. During 60-80 s, the system frequency controlled by the traditional method is similar to the previous 20 seconds since the recovered load disturbance is a load disturbance in the opposite direction. In addition, using the proposed method, the system frequency can rapidly recover to 50 Hz, which is similar to the previous 20 seconds.

At 80 s, this static FDI attack launched by the hacker is stopped. During 80-100 s, the system frequency controlled by the traditional method fluctuates due to the cessation of the attack, with frequency deviations reaching -0.17 Hz at the worst. However, using the proposed method, the system frequency remains stable at 50 Hz.

C. Verification of System Frequency Under a Dynamic Attack

In the second scenario, a dynamic FDI attack is launched by the hacker to compromise the control process of frequency regulation. In particular, assume that the value of injected data varies with time, which can be expressed as follows:

$$\psi(t) = 0.1 \cdot \sin(2\pi \cdot t). \tag{24}$$

Under this dynamic FDI attack, the power grid frequency is shown in Fig. 3. As illustrated in Fig. 3, during 0-20 s, the performance of system frequency controlled by the proposed method is better than that controlled by the traditional method, which means that the proposed method performs well in dealing with the initial frequency deviation.

At 20 s, a hacker launches the dynamic FDI attack shown in (24). During 20-40 s, the system frequency controlled by the traditional method is severely oscillated due to the dynamic

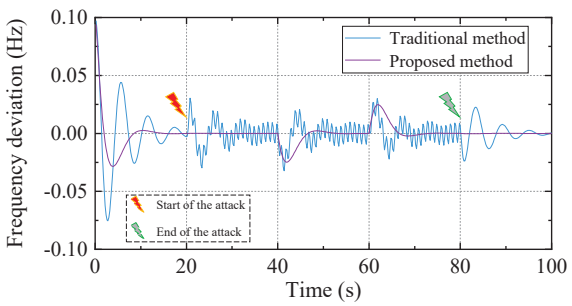

Fig. 3. The frequency of the power grid under a dynamic FDI attack (starts at 20 s and ends at 80 s).

FDI attack. However, with our proposed method, the system frequency can still be stable, which implies that our proposed method is effective even under a dynamic attack.

During 40-60 s and 60-80 s, due to the additional load disturbances, the system frequency controlled by the traditional method oscillates but with additional fluctuations. However, the system frequency can be recovered to 50 Hz rapidly with our proposed method.

During 80-100 s, dealing with the cessation of the cyber attack, the frequency characteristics with our method still outperform the traditional method, which validates the superiority of the proposed method.

V. Conclusion

Cyber-security issues are research hotspots in the frequency regulation of modern power systems. To this end, we propose a novel attack-resilient controller for the frequency regulation system against cyber attacks. Theoretically, the system with the proposed controller is stable by the proof of Lyapunov theorem. The adverse impacts caused by cyber attacks can be almost eliminated by using our proposed method, which is better than other methods. The results indicate that, under the cyber attack, the maximum frequency deviation reaches about 0.17 Hz with the traditional method. However, with the proposed method, the system frequency can be stabilized at the rated value, and the maximum frequency deviation can be mitigated to almost zero. The proposed method helps improve the system frequency's stability and security.

References

[1] H. Hui, P. Siano, Y. Ding, P. Yu, Y. Song, H. Zhang, and N. Dai, "A transactive energy framework for inverter-based hvac loads in a real-time local electricity market considering distributed energy resources," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 12, pp. 8409–8421, 2022.

[2] S. Yang, K.-W. Lao, H. Hui, Y. Chen, and N. Dai, "Real-time harmonic contribution evaluation considering multiple dynamic customers," *CSEE Journal of Power and Energy Systems*, Early Access, 2023.

[3] S. Wang, J. Zhai, and H. Hui, "Optimal energy flow in integrated electricity and gas systems with injection of alternative gas," *IEEE Transactions on Sustainable Energy*, Early Access, 2023.

[4] "Hourly real-time load vs. actual report," tech. rep., Jan. 11, 2016. [Online]. Available: http://www.ercot.com/mktinfo/rtm/index.html.

[5] Y. Wu, Z. Wei, J. Weng, X. Li, and R. H. Deng, "Resonance attacks on load frequency control of smart grids," *IEEE Transactions on Smart Grid*, vol. 9, no. 5, pp. 4490–4502, 2018.

[6] Q. Shi, F. Li, G. Liu, D. Shi, Z. Yi, and Z. Wang, "Thermostatic load control for system frequency regulation considering daily demand profile and progressive recovery," *IEEE Transactions on Smart Grid*, vol. 10, no. 6, pp. 6259–6270, Feb. 2019.

[7] Y. Chen, D. Qi, Z. Li, Z. Wang, X. Yang, and J. Zhang, "Distributed event-triggered control for frequency restoration in islanded microgrids with reduced trigger condition checking," *CSEE Journal of Power and Energy Systems*, Early Access. 2022.

[8] S. Liu and P. X. Liu, "Distributed model-based control and scheduling for load frequency regulation of smart grids over limited bandwidth networks," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 5, pp. 1814–1823, 2018.

[9] H. Hui, Y. Chen, S. Yang, H. Zhang, and T. Jiang, "Coordination control of distributed generators and load resources for frequency restoration in isolated urban microgrids," *Applied Energy*, vol. 327, p. 120116, 2022.

[10] K. Xie, H. Hui, Y. Ding, Y. Song, C. Ye, W. Zheng, and S. Ye, "Modeling and control of central air conditionings for providing regulation services for power systems," *Applied Energy*, vol. 315, p. 119035, 2022.

[11] G. Shirai, "Load frequency control using Lyapunov's second method: Bang-Bang control of speed changer position," *Proceedings of the IEEE*, vol. 67, no. 10, pp. 1458–1459, 1979.

[12] S. Yang, Z. Shao, W. Zheng, and F. Chen, "Mitigation of background harmonics effect on mmc controller based on a novel coordinate transformation technique," *IEEE Access*, vol. 7, pp. 167113–167126, 2019.

[13] L. Jiang, W. Yao, Q. H. Wu, J. Y. Wen, and S. J. Cheng, "Delay-dependent stability for load frequency control with constant and time-varying delays," *IEEE Transactions on Power Systems*, vol. 27, no. 2, pp. 932–941, 2012.

[14] C. Peng, J. Li, and M. Fei, "Resilient event-triggering H_∞ load frequency control for multi-area power systems with energy-limited dos attacks," *IEEE Transactions on Power Systems*, vol. 32, no. 5, pp. 4110–4118, 2017.

[15] W. Ahn, M. Chung, B.-G. Min, and J. Seo, "Development of cyber-attack scenarios for nuclear power plants using scenario graphs," *International Journal of Distributed Sensor Networks*, vol. 11, no. 9, p. 836258, Sep. 2015.

[16] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 ukraine blackout: Implications for false data injection attacks," *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3317–3318, 2017.

[17] Y. Chen, D. Qi, H. Dong, C. Li, Z. Li, and J. Zhang, "A fdi attack-resilient distributed secondary control strategy for islanded microgrids," *IEEE Transactions on Smart Grid*, vol. 12, no. 3, pp. 1929–1938, 2021.

[18] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, pp. 1–33, 2011.

[19] M. Li and Y. Chen, "Wide-area robust sliding mode controller for power systems with false data injection attacks," *IEEE Transactions on Smart Grid*, vol. 11, no. 2, pp. 922–930, 2020.

[20] S. Zhao, Q. Yang, P. Cheng, R. Deng, and J. Xia, "Adaptive resilient control for variable-speed wind turbines against false data injection attacks," *IEEE Transactions on Sustainable Energy*, vol. 13, no. 2, pp. 971–985, 2022.

[21] K.-D. Lu, G.-Q. Zeng, X. Luo, J. Weng, Y. Zhang, and M. Li, "An adaptive resilient load frequency controller for smart grids with dos attacks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 5, pp. 4689–4699, 2020.

[22] J. Liu, Y. Gu, L. Zha, Y. Liu, and J. Cao, "Event-triggered H_∞ load frequency control for multiarea power systems under hybrid cyber attacks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 8, pp. 1665–1678, 2019.

[23] H. Hui, Y. Ding, Y. Song, and S. Rahman, "Modeling and control of flexible loads for frequency regulation services considering compensation of communication latency and detection error," *Appl. Energy*, vol. 250, no. PT.1, pp. 161–174, Sep. 2019.