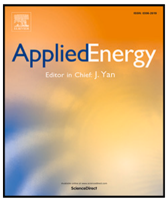
Contents lists available at ScienceDirect

Applied Energy

journal homepage: www.elsevier.com/locate/apenergy



Secure frequency regulation in power system: A comprehensive defense strategy against FDI, DoS, and latency cyber-attacks

Shaohua Yang [a,b], Keng-Weng Lao [a,b,*], Hongxun Hui [a,b], Jinshuo Su [c], Sheng Wang [d]

[a] *State Key Laboratory of Internet of Things for Smart City, University of Macau, 999078, Macao Special Administrative Region of China*
[b] *Department of Electrical and Computer Engineering, University of Macau, 999078, Macao Special Administrative Region of China*
[c] *School of Electrical Engineering, Guangxi University, Nanning, 530004, China*
[d] *School of Engineering, Newcastle University, Newcastle, United Kingdom*

ARTICLE INFO

Keywords:
Power system security
Frequency regulation
Multiple types of cyber-attacks
Resilient control
Lyapunov theorem

ABSTRACT

Maintaining frequency is crucial for the security of power systems, while deep cyber–physical interactions make frequency regulation susceptible to cyber-attack risks. False data injection (FDI) attacks, denial-of-service (DoS) attacks, and latency attacks are typical types of cyber-attacks prevalent in power systems, each capable of deteriorating system frequency through distinct mechanisms and posing serious security risks. However, existing studies on frequency regulation lack security aspects that can comprehensively address all these attack types. To fill this gap, this paper investigates a security strategy to safeguard power system frequency regulation. First, considering all these attacks, the system frequency regulation system is modeled to reveal the severity of cyber-security problems, specifically the failure to maintain frequency due to cyber-attacks. Moreover, a cyber-resilient control (CRC) strategy is developed to counter FDI, DoS, and latency attacks comprehensively. The CRC strategy involves a two-step process, including a safety surface and auxiliary trajectory control. The safety surface serves as a defensive barrier against multiple cyber-attacks, while the auxiliary trajectory control activates the safety surface's defense capability, thereby ensuring the security of system frequency. Furthermore, rigorous proofs are given based on Lyapunov theorem, demonstrating that system stability can be guaranteed by the developed CRC strategy, even under multiple types of cyber-attacks. Finally, test results confirm the efficacy of the CRC strategy. For instance, it prevents pre-existing frequency oscillations and destabilization, and also reduces the maximum frequency deviation by approximately 96.61% under multiple cyber-attacks. Therefore, the developed CRC strategy can comprehensively defend against FDI, DoS, and latency cyber-attacks, significantly contributing to the power system security.

1. Introduction

The frequency is an essential indicator for assessing the power system performance [1]. Frequency deterioration can result in severe damage and even lead to system collapse. For example, according to the Federal Government, on September 14, 2023, at 00:41 a.m., in Nigeria, the system frequency dropped to 48.41 Hz due to the line fire, which eventually led to the system collapse of the grid [2]. Similarly, on August 9, 2019, at 4:52 p.m., in the United Kingdom, the system frequency dropped from an initial 50 Hz to 48.8 Hz due to a lightning strike that caused the loss of two large generating units and amounts of distributed generation [3]. This frequency deterioration triggered the system operator's under-frequency load-shedding scheme, which affected critical facilities, including a hospital and an airport, and also resulted in the interruption of electricity supply to approximately 1.1 million customers [3]. Therefore, maintaining the system frequency at the nominal frequency[1] is crucial for ensuring the safety and stability of the power system [4].

The frequency regulation system is an integral component of the power system, which intends to maintain the nominal value by adjusting power generation or consumption in response to frequency deviations[2] [5]. To date, sorts of research have been conducted to deal with the frequency regulation problem [6]. For example, to regulate the frequency in microgrids, a self-triggered strategy is proposed to fully utilize distributed renewable generators while maintaining low communication and computation burdens, as well as preserving privacy [7].

* Corresponding author.
E-mail address: johnnylao@um.edu.mo (K.-W. Lao).

[1] Across the globe, the nominal frequency in most regions is typically either 50 Hz or 60 Hz. For example, 50 Hz in China and most of Europe, and 60 Hz in North America.

[2] The frequency deviation denotes the deviation between the actual frequency value and the nominal frequency value.

https://doi.org/10.1016/j.apenergy.2024.124772
Received 8 July 2024; Received in revised form 12 October 2024; Accepted 18 October 2024
Available online 25 November 2024
0306-2619/© 2024 Published by Elsevier Ltd.

Nomenclature

Abbreviation

CRC	Cyber-resilient control
DoS	Denial-of-service
FDI	False data injection
FSF	Full state feedback
Hz	Hertz
IoT	Internet of Things
MFD	Maximum frequency deviation
MW	Megawatt
RToF	Recovery time of frequency
WAN	Wide area network

Set

$\mathcal{T}$	The set of time during the frequency regulation process
$S_{n,1}$	The set of time when the blocking attack signal remains inactive during the nth DoS attack period's DoS-free part
$S_{n,2}$	The set of time when the blocking attack signal is active during the nth DoS attack period's DoS part
S_n	The set of time during the whole nth DoS attack period ($S_n = S_{n,1} \cup S_{n,2}$)

Parameter

$\boldsymbol{\Theta}$	Safety surface matrix
δ	Boundary of the control deviation caused by multiple hybrid cyber-attacks.
$D_{\text{off},n}$	Duration of the nth DoS-free interval
$D_{\text{on},n}$	Duration of the nth DoS interval
D_n	Total length of the nth DoS attack period ($D_n = D_{\text{off},n} + D_{\text{on},n}$)
f_{N}	Nominal frequency value

Variable

$\boldsymbol{\epsilon}$	Cyber-attack vector
$\boldsymbol{x}$	State variable vector of the state-space model
γ	Function of the designed safety surface
$\widetilde{U}_{\text{Atts}}$	Control signal under multiple hybrid cyber-attacks
Ξ	Deviation of control signal due to multiple hybrid cyber-attacks
$\xi^{\text{DoS}}_{\text{dvt}}$	Control deviation caused by DoS attacks
$\xi^{\text{FDI}}_{\text{dvt}}$	Control deviation caused by FDI attacks
$\xi^{\text{LA}}_{\text{dvt}}$	Control deviation caused by latency attacks
ζ_{FO}	Frequency oscillation under cyber-attacks
ζ_{MFD}	Maximum frequency deviation under cyber-attacks
ζ_{RToF}	Recover time of frequency under cyber-attacks
Δf	Deviation of system frequency
U	Original control input for the frequency regulation
u_{aux}	Auxiliary trajectory control signal
U_{exc}	Actual execution control signal including the original control input, the multiple cyber-attacks, and the auxiliary trajectory control input

Moreover, based on a distributed model, a novel load frequency control method is proposed for the frequency regulation, which also considers the finiteness of communication bandwidth [8]. Besides, a membership-function-based frequency regulation scheme is given to compensate for communication delays in distributed generators [9]. In addition to these efforts from supply-side, there are also efforts from demand-side to improve the frequency performance of power systems [10,11]. For instance, a control strategy is proposed for thermostatic loads based on daily demand profile to achieve frequency regulation of power systems, while also considering customer comfort requirements [12]. A confidence interval-based optimal strategy is given to manage electric vehicle loads and simultaneously guarantee frequency stability [13]. A model predictive control-based scheme is introduced to capitalize on the inherent flexibility of buildings to offer frequency reserves for the power system [14]. Furthermore, considering both distributed generators on supply-side and load resources on demand-side, a coordination control scheme is designed to increase the regulation capacities and thus maintain the frequency stability of microgrids [15]. Numerous aspects, such as the communication resource constraints [16], diverse flexible resources on the demand side [17,18], and supply–demand coordination [19,20], have been taken into account in the power system frequency regulation field. Constructive progress has been realized through these existing efforts.

However, a critical factor in the frequency regulation of modern power systems, i.e., cyber-security, has not been adequately considered and resolved in previous literature [21]. With the deep cyber–physical coupling, the communication, computation, and control components are integrated with physical entities to realize real-time monitoring

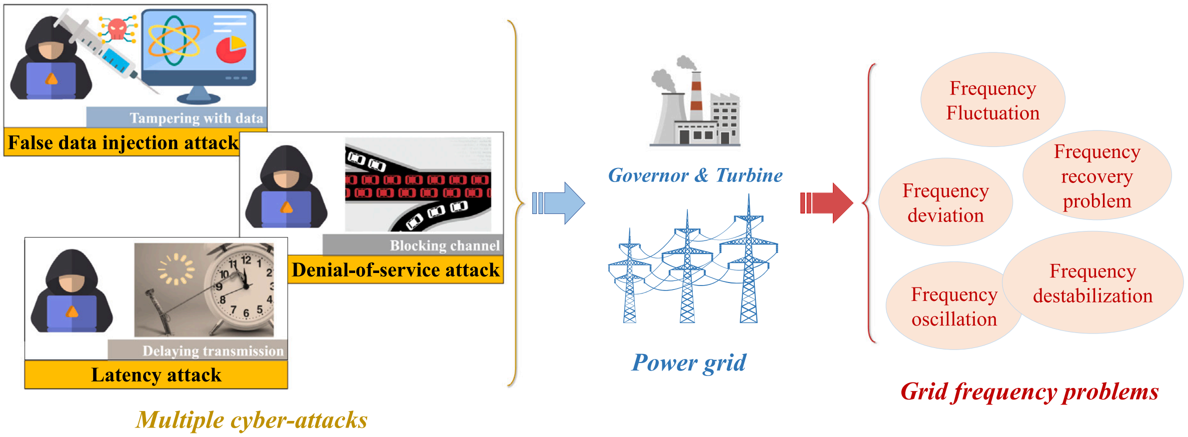


Fig. 1. Multiple cyber-attacks leading to frequency problems of the power system.

and dynamic control [22,23]. For this reason, the frequency regulation system of the modern power system has evolved into an open system, making it susceptible to the potential risk of cyber-attacks [24]. Actually, cyber-security has emerged as an essential problem in the frequency regulation field [25], as illustrated in Fig. 1. For example, false data injection (FDI) attack is a typical threat that can degrade the frequency performance of power systems [26]. Specifically, the FDI attack tampers with control signals by introducing false data, resulting in inaccurate control within frequency regulation systems [27]. Due to this inaccurate control, frequency deviations and fluctuations will occur, leading to serious damage to the power system that must be addressed [28]. Therefore, considering the FDI attack is crucial when investigating the cyber-security aspects of frequency regulation. In addition, denial-of-service (DoS) attack is a typical cyber-attack deserving of attention as well [29]. The DoS attack can interrupt the transmission of data packets by overloading the communication channel with blocking signals, which in turn leads to consequences such as data packet dropout [30]. In frequency regulation systems, a DoS attack can block control signals in communication channel, leading to actuator failure to receive control signals and resulting in serious frequency deviations, which threaten the security of power systems [31]. Furthermore, latency attack has also become a cyber threat for power systems. Unlike the FDI and DoS attacks, the latency attack does not involve tampering with or denying data packets. Instead, it alters the dynamic characteristics of a control system by maliciously delaying the data packet transmission [32]. To be specific, the latency attack postpones the time for actuators to receive control signals, affecting the characteristics of the frequency regulation system [33]. This implies that actuators may respond oppositely to actual requirements, thereby causing frequency oscillations and, in severe cases, leading to frequency destabilization in power systems.

It is worth noting that FDI attack, DoS attack, and latency attack each have distinct features, leading to varied adverse consequences on frequency regulation systems, such as frequency oscillations, frequency deviations, frequency destabilization, etc. [34]. Each of these adverse consequences can further threaten the power system security and deserve further investigation. However, existing studies on frequency regulation lack security aspects that can comprehensively consider all these types of cyber-attacks. Therefore, developing a comprehensive strategy to defend against various types of cyber-attacks, including FDI, DoS, and latency attacks, is essential for ensuring frequency stability and power system security.

To this end, this paper focuses on frequency regulation considering the cyber-security problem described above. The major contributions are fourfold:

- To comprehensively safeguard power system frequency regulation against FDI, DoS, and latency attacks, a cyber-resilient control (CRC) strategy is developed, which involves a two-step process, i.e., a safety surface and auxiliary trajectory control. This strategy can directly counter cyber-attacks without relying on attack detection or state estimation.
- A safety surface is designed in the state space based on Lyapunov equation and full state feedback (FSF) method. Once activated, this surface can serve as a defensive barrier, comprehensively countering multiple types of cyber-attacks. Moreover, the efficacy of the safety surface is rigorously proved by using Lyapunov theorem.
- An auxiliary trajectory control is proposed to drive the system state trajectory to the designed safety surface, thereby activating the safety surface's defense capability and comprehensively ensuring frequency security of power systems. Similarly, a rigorous proof is presented from a mathematical perspective, theoretically demonstrating the efficacy of the auxiliary trajectory control.
- The efficacy of the developed defense strategy is thoroughly validated from various perspectives, including different attack types, multiple hybrid attacks, diverse attack locations, and different system configurations, etc. Therefore, this work can help address cyber-security problems well and provide valuable insights for frequency regulation in power systems.

For the rest, the modeling of the frequency regulation system with multiple types of cyber-attacks is presented in Section 2. In addition, a CRC strategy is developed for system frequency security in Section 3. Specifically, a safety surface and an auxiliary trajectory control are given to comprehensively counter the negative consequences of multiple cyber-attacks. Moreover, rigorous proof of stability is also provided in this part. In Section 4, the efficacy of the developed CRC strategy is validated by various case studies, and finally, the whole article is concluded by Section 5.

2. Modeling of power system frequency regulation considering multiple cyber-attacks

In this part, we first model the power system frequency regulation. Moreover, the modeling of FDI attacks, DoS attacks, and Latency attacks are given, respectively. Based on this, the cyber-security problem of frequency regulation system is formulated considering multiple types of cyber-attacks.

2.1. Modeling of frequency regulation system for power systems

The control block diagram of the frequency regulation system is illustrated in Fig. 2. As observed, the power system's frequency regulation system comprises the control part, communication network, speed

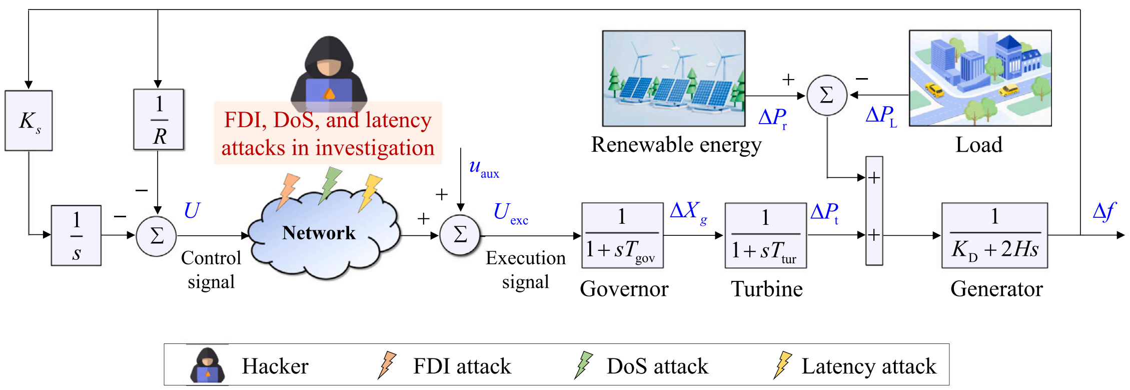


Fig. 2. Block diagram of frequency regulation system considering FDI attacks, DoS attacks, and latency attacks, comprehensively.

governor, steam turbine, and power system generator. Symbols U, ΔX_g, ΔP_t, and Δf denote the control input for the frequency regulation, deviation of speed governor valve position, steam turbine output, and system frequency, respectively. All of them are variable states of this dynamic system [35,36]. Symbols u_{aux} and U_{exc} stand for the auxiliary trajectory control signal to be designed, as well as the actual execution signal taking into account the original control input, the multiple cyber-attacks, and the auxiliary control input, respectively. Moreover, symbol ΔP_r and ΔP_L are the power perturbations to the power system from supply-side renewable energies and demand-side loads, respectively [37,38]. In addition, R, s, and K_s represent the speed drooping coefficient, Laplace operator, and integral control gain, respectively. Symbols T_{gov} and T_{tur} denote time constants of the speed governor and the steam turbine, respectively. And symbols K_D and H represent the equivalent damping coefficient and equivalent system inertia coefficient, respectively.

The dynamics of the control block diagram in Fig. 2 can be formulated as [39]:

$$\Delta \dot{f}(t) = -\frac{K_D}{2H}\Delta f(t) + \frac{1}{2H}\Delta P_t(t) + \frac{1}{2H}\Delta P_r(t) - \frac{1}{2H}\Delta P_L(t), \tag{1}$$

$$\Delta \dot{P}_t(t) = -\frac{1}{T_{\text{tur}}}\Delta P_t(t) + \frac{1}{T_{\text{tur}}}\Delta X_g(t), \tag{2}$$

$$\Delta \dot{X}_g(t) = -\frac{1}{T_{\text{gov}}}\Delta X_g(t) + \frac{1}{T_{\text{gov}}}U(t), \tag{3}$$

$$\dot{U}(t) = (\frac{K_D}{2HR} - K_s)\Delta f(t) - \frac{1}{2HR}\Delta P_t(t) - \frac{1}{2HR}\Delta P_r(t) + \frac{1}{2HR}\Delta P_L(t). \tag{4}$$

The function of this dynamic frequency regulation system is to eliminate the frequency deviations, which are inevitable in the power system, possibly due to the customer's dynamic behavior, the stochastic nature of renewable energies, or other power perturbations. As depicted in the left part of Fig. 2, the controller is the main component of the frequency regulation system. During the frequency regulation process, the actual system frequency deviation serves as a feedback signal transmitted to the controller. The controller then accumulates these frequency deviations and combines the integral result with the proportional feedback value to convert them into control signals. These control signals are sent to the actuator to adjust the output power of the steam turbine, thereby alleviating the system frequency deviation. Even when the power system experiences power perturbations, the controller can continuously adjust the system frequency to maintain its stability [8]. In addition, as illustrated in Fig. 2, potential different types of cyber-attacks, i.e., FDI attacks, DoS attacks, and latency attacks, are comprehensively considered in the frequency regulation to investigate the cyber-security of the system frequency. However, it is worth noting that the original controller does not contribute to the stability of the system against cyber-attacks. This is because, unlike power disturbances, cyber-attacks can directly interfere with the transmitted control signals from the original controller. As a result, the actuator cannot execute the correct control signals to accurately adjust the steam turbine's output power, rendering the controller ineffective. Therefore, the original controller in the frequency regulation system cannot maintain the system frequency at its nominal value under cyber-attacks, which requires further investigation.

2.2. Modeling of FDI attacks

The FDI attack is a crucial cyber-attack on power systems that can deteriorate the system's performance by injecting malicious data into original data packets. As illustrated in Fig. 3, FDI attacks can lead to inaccurate control in the frequency regulation system, since the control signals are tampered with by the injected false data as they are transmitted over the communication channel. Consequently, the frequency performance of the power system may deteriorate significantly, which is harmful to the stable operation of the power system. Hence, it is essential to consider the potential FDI attacks when defending the power system against cyber threats. When the control signal is subjected to FDI attacks, the corrupted control signal will contain the original frequency regulation control signal and malicious injected data from the hackers. On this basis, the FDI attack can be modeled as follows [27]:

$$\widetilde{U}_{\text{FDI}} = U + \kappa\phi, \tag{5}$$

where U denotes the original control signal of the frequency regulation system; $\widetilde{U}_{\text{FDI}}$ is the corrupted control signal under the FDI attack; and κ is a binary variable where $\kappa = 1$ and $\kappa = 0$ represent the presence and absence of FDI attacks, respectively; ϕ denotes the malicious injected data of FDI attack.

Assumption 1. A boundary exists on the injected data of FDI attacks.

In practice, due to physical constraints, it is impossible to inject unlimited data into the control signal of the frequency regulation system. Hence, the injected data ϕ launched by the hacker has to be constrained. To be specific, the amplitude of FDI attack injected data has a boundary that can be expressed as follows:

$$\|\phi(t)\| \leq \overline{\phi}, \tag{6}$$

where $\overline{\phi} > 0$ represents the boundary of the FDI attack data.

2.3. Modeling of DoS attacks

The DoS attack is a typical cyber-attack that can make a communication channel unavailable by temporarily blocking signals. During DoS attacks, the transmission of legitimate data packets is disrupted, since the communication channel becomes overloaded due to blocking

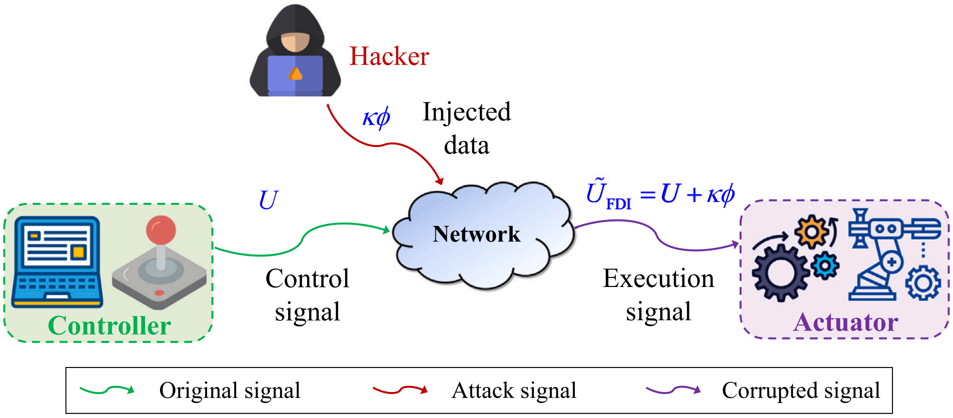


Fig. 3. Illustration of FDI attacks.

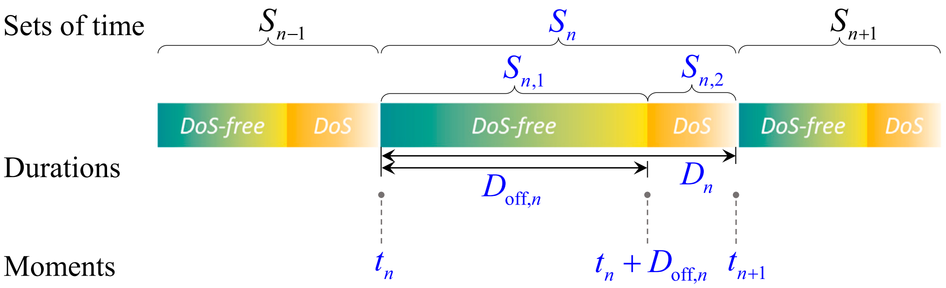


Fig. 4. Schematic diagram of blocking signals of DoS attacks.

signals. Hence, DoS attacks usually lead to consequences such as data packet dropout.

In the frequency regulation system, the DoS attack can cause a blockage of the communication channel that transmits control signals, resulting in the actuator failing to receive control signals. Consequently, serious frequency deviations can occur, threatening the safety of the power system. Therefore, the DoS attack should be considered when investigating the cyber-security of frequency regulation systems. The blocking signal of a DoS attack can be modeled as follows [39]:

$$b(t) = \begin{cases} 0, t \in S_{n,1} = [t_n, t_n + D_{\mathrm{off},n}), \\ 1, t \in S_{n,2} = [t_n + D_{\mathrm{off},n}, t_{n+1}), \end{cases} \tag{7}$$

where $n \in \mathbb{N}$ is a period number of blocking signal of DoS attack; $S_{n,1}$ represents a DoS-free interval where the blocking attack signal remains inactive, allowing the control information transmission through the communication channel; $S_{n,2}$ denotes the nth DoS interval, during which the blocking signal of DoS attack is active, resulting in failure to transmit control information; t_n and t_{n+1} are the beginning and ending moments of the nth DoS attack period; $D_{\mathrm{off},n}$ indicates the duration of the nth DoS-free interval. To illustrate it clearly, a schematic of DoS attacks is shown in Fig. 4. Symbol $D_n = D_{\mathrm{off},n} + D_{\mathrm{on},n}$ denotes the total length of the nth DoS attack period; $D_{\mathrm{on},n}$ denotes the duration of the nth DoS interval; and $S_n = S_{n,1} \cup S_{n,2}$ is the set of time in the whole nth DoS attack period. Moreover, the OFF/ON transition instants of DoS attacks can be represented as follows:

$$t_{n,i} = \begin{cases} t_n, & i = \mathrm{OFF}, \\ t_n + D_{\mathrm{off},n}, & i = \mathrm{ON}. \end{cases} \tag{8}$$

Assumption 2. There is a limitation on the duration of each DoS and each DoS-free interval.

That implies the duration of DoS interval $D_{\mathrm{on},n}$ satisfying $D_{\mathrm{on},n}^{\min} \leq D_{\mathrm{on},n} \leq D_{\mathrm{on},n}^{\max}$, $\forall n \in \mathbb{N}$, where $D_{\mathrm{on},n}^{\min}$ and $D_{\mathrm{on},n}^{\max}$ are the lower and upper boundaries of $D_{\mathrm{on},n}$, respectively. Similarly, the duration of DoS-free interval $D_{\mathrm{off},n}$ satisfying $D_{\mathrm{off},n}^{\min} \leq D_{\mathrm{off},n} \leq D_{\mathrm{off},n}^{\max}$, $\forall n \in \mathbb{N}$, where $D_{\mathrm{off},n}^{\min}$ and $D_{\mathrm{off},n}^{\max}$ are the lower and upper boundaries of $D_{\mathrm{off},n}$, respectively. From a practical perspective, the sleep duration of a DoS attack cannot always last since a DoS attack will happen eventually. In addition, the duration of a DoS attack cannot be sustained indefinitely due to energy limitations. Therefore, the assumption is reasonable.

2.4. Modeling of latency attacks

The latency attack has emerged as a new cyber-security threat with the widespread use of Internet of Things (IoT) and wireless wide area network (WAN) technologies. Unlike FDI and DoS attacks, the latency attack does not involve denying or tampering with data packets. Instead, it operates by delaying the transmission of data packets, thereby altering the dynamic characteristics of a control system and even affecting system stability. As illustrated in Fig. 5, a latency attack can postpone the reception time of control signals by an actuator in the frequency regulation system. This implies that the actuator may respond in a contrary manner to the actual requirements. For example, in an under-frequency case, the actuator may execute outdated and erroneous control signals, leading to a further decrease in the system frequency. In severe cases, the latency attack could even threaten the frequency stability of the power system. Under a latency attack, there will be a control error for the frequency regulation system:

$$U_{\mathrm{err}} = \tilde{U}_{\mathrm{LA}} - U, \tag{9}$$

where U_{err} is the control error between the original control signal and the actual executed control signal due to a latency attack; $U = U(t_{\mathrm{up}})$ is the original control signal transmitted by the controller, which can be regarded as the real-time and effective control signal; t_{up} is the actual uploading time of the control signal to the communication channel; $\tilde{U}_{\mathrm{LA}} = U(t_{\mathrm{rc}})$ is the control signal executed by the actuator, which is

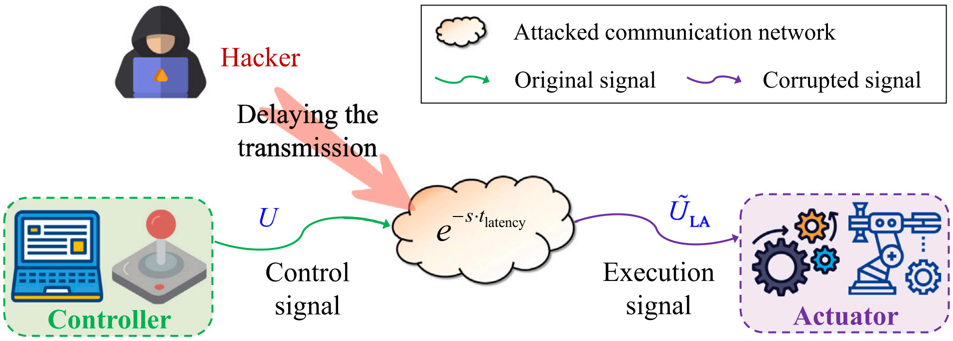


Fig. 5. Illustration of latency attacks.

affected by the latency attack; t_{rc} is the uploading time of the control signal that the actuator receives and executes, which can be represented as follows:

$$t_{\text{rc}} = t_{\text{up}} - t_{\text{latency}}, \tag{10}$$

where t_{latency} is the latency time caused by the latency attack.

It is also worth noting that, in addition to cyber-attacks, various other factors can also introduce latency, such as natural communication delays. In this case, (10) can be represented as $t_{\text{rc}} = t_{\text{up}} - \sum_{i=1}^{\text{N}} t_{\text{latency},i}$, where $t_{\text{latency},i}$ represents the latency caused by factor i, with a total of N factors. To address the latency caused by various factors, the strategy proposed in this work takes the above equation into account.

2.5. *Cyber-security problem statement considering multiple types of cyber-attacks*

Considering the multiple types of cyber-attacks comprehensively, i.e., FDI, DoS, and latency attacks, the control signal executed by the actuator of frequency regulation system is modified as follows:

$$\widetilde{U}_{\text{Atts}}(t) = U(t) + \Xi(t), \tag{11}$$

where $\Xi(t)$ is the deviation of control signal due to multiple hybrid cyber-attacks, which can be further expressed as follows:

$$\Xi(t) = \xi_{\text{dvt}}^{\text{FDI}}(t) + \xi_{\text{dvt}}^{\text{DoS}}(t) + \xi_{\text{dvt}}^{\text{LA}}(t), \tag{12}$$

where $\xi_{\text{dvt}}^{\text{FDI}}(t)$, $\xi_{\text{dvt}}^{\text{DoS}}(t)$, and $\xi_{\text{dvt}}^{\text{LA}}(t)$ are control deviation caused by FDI, DoS, and latency attacks, respectively.

Assumption 3. There exists a boundary on the control deviation $\Xi(t)$ caused by these multiple hybrid cyber-attacks.

This is because the control deviation $\Xi(t)$ consists of three parts, i.e., (i) the FDI attack deviation $\xi_{\text{dvt}}^{\text{FDI}}(t)$, (ii) the DoS attack deviation $\xi_{\text{dvt}}^{\text{DoS}}(t)$, and (iii) the latency attack deviation $\xi_{\text{dvt}}^{\text{LA}}(t)$. The FDI attack deviation $\xi_{\text{dvt}}^{\text{FDI}}(t)$ depends on the injected data of the FDI attack, which is inherently bounded, as previously mentioned in *Assumption* 1 in Section 2.2. In addition, the control deviation caused by DoS attack is equal to the difference between the original control signal and zero, since the control signal is blocked. The latency attack deviation denotes the difference between the actual executed control signal and the original control signal. Meanwhile, combined with the fact that the control signal is limited in any case due to the physical constraints, the DoS attack deviation $\xi_{\text{dvt}}^{\text{DoS}}(t)$ and the latency attack deviation $\xi_{\text{dvt}}^{\text{LA}}(t)$ are also bounded in any case, respectively. Therefore, it is reasonable that the total control deviation $\Xi(t)$ has a boundary, which can be presented as follows:

$$\|\Xi(t)\| \le \delta, \tag{13}$$

where $\delta > 0$ represents the boundary of the control deviation caused by multiple hybrid cyber-attacks.

Cyber-Security Problem Statement: Since the control deviation is associated with FDI, DoS, and latency attacks, the control signals of frequency regulation are affected in a complex and unpredictable way. This implies the system's dynamic characteristic is altered, and the frequency regulation objective, i.e., to maintain the nominal value, cannot be achieved again. In severe cases, this can even cause frequency destabilization. As a result, the system frequency cannot be guaranteed, and the power system security is threatened. Therefore, multiple cyber-attack types pose a critical challenge for the frequency regulation system and must be addressed.

3. Developed cyber-resilient control strategy for power system frequency regulation

To counter against these multiple types of cyber-attacks, a cyber-resilient control (CRC) strategy is developed to safeguard the frequency regulation system and maintain the power system's frequency. This section begins with an overview of the CRC strategy. The CRC strategy is based on sliding mode control theory and, for ease of explanation, comprises two essential parts, i.e., a safety surface and an auxiliary trajectory control. Subsequently, the design of the safety surface and the development of the auxiliary trajectory control are detailed. Furthermore, rigorous proof is presented, demonstrating that the proposed CRC strategy can effectively stabilize the system frequency, despite multiple types of cyber-attacks.

3.1. *Overview of developed cyber-resilient control strategy*

The CRC strategy is a two-step process. The first step is to design a safety surface, which can function as a defensive barrier to counter against multiple types of cyber-attacks comprehensively once activated. And the second step involves utilizing auxiliary trajectory control to drive the system's dynamic trajectory onto this surface, so as to activate the safety surface's defense capability. In this way, the frequency regulation system can be defended against multiple types of cyber-attacks. Therefore, slight deviations and rapid convergence in system frequency can be achieved, and potential frequency oscillation and destabilization caused by cyber-attacks can be avoided. Meanwhile, under the CRC strategy, the control input for the frequency regulation system is composite, which is co-formed by the superimposition of the original control and the auxiliary trajectory control, as follows:

$$u_{\text{rsl}}(t) = U(t) + u_{\text{aux}}(t), \tag{14}$$

where $u_{\text{rsl}}(t)$ is the resilient control signal at time t taking into account the original control signal $U(t)$ and the auxiliary trajectory control signal $u_{\text{aux}}(t)$ to be designed. Moreover, the original control signal can be incorporated into the state-space equation and regarded as a state variable.

Furthermore, considering the multiple types of cyber-attacks and the introduced auxiliary trajectory control, the dynamic characteristic described in (1)–(4) can be reformulated into a matrix form. In this way, the state-space model is established as:

$$\dot{\boldsymbol{x}}(t) = \boldsymbol{A}\boldsymbol{x}(t) + \boldsymbol{B}(u_{\text{aux}}(t) + \Xi(t)) + \boldsymbol{D}(\Delta P_{\text{L}}(t) - \Delta P_{\text{r}}(t)) \tag{15}$$

$$= \boldsymbol{A}\boldsymbol{x}(t) + \boldsymbol{B}u_{\text{aux}}(t) + \boldsymbol{D}(\Delta P_{\text{d}}(t) - \Delta P_{\text{r}}(t)) + \epsilon(t), \tag{16}$$

where $\boldsymbol{x}(t) = \begin{bmatrix}\Delta f(t) & \Delta P_{\text{t}}(t) & \Delta X_{\text{g}}(t) & U(t)\end{bmatrix}^{\text{T}}$ is the state variable vector of the state-space model; the matrix $\boldsymbol{A}$ denotes the state-transition matrix, as follows:

$$\boldsymbol{A} = \begin{bmatrix} -\frac{K_{\text{D}}}{2H} & \frac{1}{2H} & 0 & 0 \\ 0 & -\frac{1}{T_{\text{tur}}} & \frac{1}{T_{\text{tur}}} & 0 \\ 0 & 0 & -\frac{1}{T_{\text{gov}}} & +\frac{1}{T_{\text{gov}}} \\ \frac{K_{\text{D}}-2HRK_s}{2HR} & -\frac{1}{2HR} & 0 & 0 \end{bmatrix}, \tag{17}$$

and $\boldsymbol{B} = \begin{bmatrix}0 & 0 & \frac{1}{T_{\text{gov}}} & 0\end{bmatrix}^{\text{T}}$ represents the control matrix, indicating how the introduced auxiliary control regulates the frequency regulation system; $\boldsymbol{D} = \begin{bmatrix}-\frac{1}{2H} & 0 & 0 & \frac{1}{2HR}\end{bmatrix}^{\text{T}}$ denotes the influence matrix, indicating how power perturbations influence the system; and $\boldsymbol{\epsilon} = \begin{bmatrix}0 & 0 & \frac{1}{T_{\text{gov}}}\Xi(t) & 0\end{bmatrix}^{\text{T}}$ is the cyber-attack vector describing the dynamic error caused by multiple types of cyber-attacks, e.g., FDI attacks, DoS attacks, and latency attacks.

On this basis, our objective is to design a safety surface and develop auxiliary trajectory control to guarantee the stability of this modeled system considering multiple cyber-attacks.

3.2. Designing a safety surface to counter against multiple types of cyber-attacks

This part presents the CRC strategy's first step in detail. Specifically, an effective and precise safety surface is constructed based on Lyapunov theorem. This safety surface functions as a secure barrier, and when the system trajectory is located on the safety surface, the negative consequences (e.g., frequency oscillations and frequency destabilization) caused by multiple types of cyber-attacks will be eliminated. In other words, the safety surface is a pivotal defensive technique that can aid the frequency regulation system in countering various cyber-attacks.

The safety surface can be designed as follows:

$$\boldsymbol{B}^{\text{T}}\boldsymbol{\Theta}\boldsymbol{x} = 0, \tag{18}$$

where $\boldsymbol{\Theta}$ is the safety surface matrix. This matrix $\boldsymbol{\Theta}$ must be positive definite and to be designed. To obtain this positive definite matrix $\boldsymbol{\Theta}$, the Lyapunov equation is introduced, as below:

$$\boldsymbol{A}_{\text{s}}^{\text{T}}\boldsymbol{\Theta} + \boldsymbol{\Theta}\boldsymbol{A}_{\text{s}} = -\boldsymbol{Q}, \tag{19}$$

where $\boldsymbol{Q}$ can be an arbitrary matrix satisfying the symmetry and the positive definiteness; and $\boldsymbol{A}_{\text{s}}$ represents a stable matrix that needs to be determined.

In order to determine this stable matrix $\boldsymbol{A}_{\text{s}}$, the full state feedback (FSF) method is introduced. Namely, if a system pair ($\boldsymbol{A}$, $\boldsymbol{B}$) is considered controllable, the system can be controlled by the state feedback:

$$u = -\boldsymbol{K}\boldsymbol{x} + v, \tag{20}$$

where u refers to the control input of this controllable system; $\boldsymbol{K}$ denotes the feedback matrix; and v represents an introduced new intermediate variable. On this basis, the FSF method can become applicable for placing the closed-loop poles at predetermined locations in the s-plane [40]. This placement of poles is advantageous since the pole locations directly correlate with the eigenvalues of the system, and these eigenvalues influence the system's response characteristics [41].

Therefore, to obtain a stable matrix $\boldsymbol{A}_{\text{s}}$, the eigenvalues can be set to satisfy the following inequality:

$$\text{Re}(\lambda_i[\boldsymbol{A}_{\text{s}} = \boldsymbol{A} - \boldsymbol{B}\boldsymbol{K}]) < 0, \text{for } i = 1, 2, \ldots, n, \tag{21}$$

where $\lambda_i[\cdot]$ denotes the ith eigenvalue; Re(λ_i) stands for the ith eigenvalue's real part. Based on the specified eigenvalues satisfying (21), the feedback matrix $\boldsymbol{K}$ can be determined, and the matrix $\boldsymbol{A}_{\text{s}}$ can be guaranteed to be stable.

Combining the settled eigenvalues satisfying (21), the FSF method, and the Lyapunov equation in (19) yields the desired safety surface matrix $\boldsymbol{\Theta}$. Based on this, the function of the designed safety surface can be expressed as follows:

$$\gamma(t) = \boldsymbol{B}^{\text{T}}\boldsymbol{\Theta}\boldsymbol{x}. \tag{22}$$

Note that the safety surface function presented in (22) is a function of the state variable vector $\boldsymbol{x}$. Hence, the value of this safety surface function varies with changes in the system state variables. When the trajectory of the system state variables approaches the safety surface, the defense capability of this surface is activated, and at this point, the function in (22) can satisfy the following property:

$$\gamma(t) = 0. \tag{23}$$

With the designed safety surface in (18), the following main outcome can be derived for the frequency regulation system when subjected to multiple types of cyber-attacks.

Theorem 1. *As the system trajectory approaches the designed safety surface in (18)–(21), i.e., $\gamma(t) = 0$, the stability of the frequency regulation system can be guaranteed, even under multiple types of cyber-attacks.*

Proof. The main focus of our problem is on cyber-attacks, and traditional power perturbations can be left out of the analysis process. This is because the frequency regulation system can inherently handle power perturbations in the physical layer. However, in assessing the efficacy of the safety surface, we have to consider multiple types of cyber-attacks. Therefore, FDI attacks, DoS attacks, and latency attacks must be taken into account in the analytical model.

Combining the FSF control in (20)–(21), the dynamics of frequency regulation (16) under multiple types of cyber-attacks can be given as follows:

$$\dot{\boldsymbol{x}} = \boldsymbol{A}_s\boldsymbol{x} + \boldsymbol{B}v + \boldsymbol{B}\Xi. \tag{24}$$

To prove its stability, a Lyapunov function candidate is provided below:

$$V(\boldsymbol{x}) = \boldsymbol{x}^{\text{T}}\boldsymbol{\Theta}\boldsymbol{x}. \tag{25}$$

The derivative of Lyapunov function in (25) can be derived below:

$$\begin{aligned}\dot{V}(\boldsymbol{x}) &= \left(\boldsymbol{A}_s\boldsymbol{x} + \boldsymbol{B}v + \boldsymbol{B}\Xi\right)^{\text{T}}\boldsymbol{\Theta}\boldsymbol{x} + \boldsymbol{x}^{\text{T}}\boldsymbol{\Theta}\left(\boldsymbol{A}_s\boldsymbol{x} + \boldsymbol{B}v + \boldsymbol{B}\Xi\right) \\ &= \boldsymbol{x}^{\text{T}}\boldsymbol{A}_s^{\text{T}}\boldsymbol{\Theta}\boldsymbol{x} + \boldsymbol{x}^{\text{T}}\boldsymbol{\Theta}\boldsymbol{A}_s\boldsymbol{x} + (\boldsymbol{B}v + \boldsymbol{B}\Xi)^{\text{T}}\boldsymbol{\Theta}\boldsymbol{x} + \boldsymbol{x}^{\text{T}}\boldsymbol{\Theta}(\boldsymbol{B}v + \boldsymbol{B}\Xi) \\ &= -\boldsymbol{x}^{\text{T}}\boldsymbol{Q}\boldsymbol{x} + 2v^{\text{T}}\boldsymbol{B}^{\text{T}}\boldsymbol{\Theta}\boldsymbol{x} + 2\Xi^{\text{T}}\boldsymbol{B}^{\text{T}}\boldsymbol{\Theta}\boldsymbol{x}.\end{aligned} \tag{26}$$

Since the trajectory of the system state variables approaches the safety surface, the property described in (23) is possessed,i.e., $\gamma(t) = 0$. On this basis, we obtain:

$$\gamma(t) = \boldsymbol{B}^{\text{T}}\boldsymbol{\Theta}\boldsymbol{x} = 0. \tag{27}$$

Combining (26) and (27), it can be further deduced that the derivative of the Lyapunov function satisfies the following inequality:

$$\begin{aligned}\dot{V}(\boldsymbol{x}) &= -\boldsymbol{x}^{\text{T}}\boldsymbol{Q}\boldsymbol{x} + 2v^{\text{T}}\boldsymbol{B}^{\text{T}}\boldsymbol{\Theta}\boldsymbol{x} + 2\Xi^{\text{T}}\boldsymbol{B}^{\text{T}}\boldsymbol{\Theta}\boldsymbol{x} \\ &= -\boldsymbol{x}^{\text{T}}\boldsymbol{Q}\boldsymbol{x} + 0 + 0 \\ &= -\boldsymbol{x}^{\text{T}}\boldsymbol{Q}\boldsymbol{x} < 0.\end{aligned} \tag{28}$$

It can be seen from (28) that the derivative of the Lyapunov function $V(t)$ is always less than zero, which implies the function's energy will be continuously decreasing from the energy's perspective in the Lyapunov Theorem [42]. Moreover, the analyzed Lyapunov function candidate $V(t)$ in (25) is always larger than or equal to zero, implying that the Lyapunov function's initial value is non-negative. Therefore, its energy decreases over time, indicating that the value of $V(t)$ will gradually decrease from a non-negative number to converge to zero at last.

Furthermore, the variables of the function $V(t)$, i.e., the state variable vector $\boldsymbol{x}(t)$ of the system, will similarly converge to zero along with $V(t)$, since the Lyapunov function $V(t)$ is a quadratic form. Therefore, our designed safety surface can guarantee the system's stability, despite multiple types of cyber-attacks.

The proof is complete. ■

Remark. Theorem 1 demonstrates the designed safety surface is effective. Upon activation, this safety surface ensures the stability of the system's state variables, including the system frequency deviation, even in the presence of simultaneous FDI, DoS, and latency attacks.

3.3. Developing auxiliary trajectory control to activate safety surface's defense capability

In the previous section we designed a safety surface and proved its efficacy to counter against multiple types of cyber-attacks. However, it is necessary to drive the trajectory of system state variables to approach the safety surface to activate the defense capability. Therefore, in this section, we develop an auxiliary trajectory control to activate the designed safety surface, protecting the power system from cyber-attacks.

To develop the auxiliary trajectory control, the constant rate approaching law is employed as follows:

$$\dot{\gamma}(t) = -\omega \cdot \operatorname{sgn}(\gamma(t)), \tag{29}$$

where ω denotes the approaching gain, which is a positive constant; symbol $\operatorname{sgn}(\cdot)$ represents the sign function, which can return the sign of a real number, as follows:

$$\operatorname{sgn}(\gamma(t)) = \begin{cases} -1, & \text{if } \gamma(t) < 0, \\ 0, & \text{if } \gamma(t) = 0, \\ 1, & \text{if } \gamma(t) > 0. \end{cases} \tag{30}$$

On this basis, the auxiliary trajectory control is developed as follows:

$$u_{\text{aux}}(t) = -(\boldsymbol{B}^{\mathrm{T}}\boldsymbol{\Theta}\boldsymbol{B})^{-1} \cdot \omega \cdot \operatorname{sgn}(\gamma(t)) \\ - \delta \cdot \operatorname{sgn}(\gamma(t)) - (\boldsymbol{B}^{\mathrm{T}}\boldsymbol{\Theta}\boldsymbol{B})^{-1}\boldsymbol{B}^{T}\boldsymbol{\Theta}\boldsymbol{A}\boldsymbol{x}, \tag{31}$$

where $\boldsymbol{\Theta}$ is a positive definite matrix determined from the Lyapunov equation in (19), δ is a positive constant representing the boundary of control deviations caused by multiple hybrid cyber-attacks. On this basis, the following main outcome can be given.

Theorem 2. *With the auxiliary trajectory control in (31), the trajectory of system state variables $\boldsymbol{x}(t)$ can always approach the safety surface designed in (18).*

Remark. Theorem 2 implies the safety surface's defense capability can be activated by the developed auxiliary trajectory control.

Proof. According to (22), the derivative of the safety surface function can be obtained as follows:

$$\dot{\gamma}(t) = \boldsymbol{B}^{\mathrm{T}}\boldsymbol{\Theta}\dot{\boldsymbol{x}} = \boldsymbol{B}^{\mathrm{T}}\boldsymbol{\Theta}[\boldsymbol{A}\boldsymbol{x} + \boldsymbol{B}\boldsymbol{u} + \boldsymbol{B}\boldsymbol{\Xi}]. \tag{32}$$

Combining (31) and (32), this derivative can be further derived as follows:

$$\dot{\gamma}(t) = \boldsymbol{B}^{\mathrm{T}}\boldsymbol{\Theta}\boldsymbol{B}[\boldsymbol{\Xi} - \operatorname{sgn}(\gamma(t)) \cdot \delta] - \omega \cdot \operatorname{sgn}(\gamma(t)), \tag{33}$$

where the first part is positive definite since $\boldsymbol{B}$ is non-zero vector, i.e., $\boldsymbol{B}^{\mathrm{T}}\boldsymbol{\Theta}\boldsymbol{B} > 0$.

Furthermore, based on (33), one has a inequality as below:

$$\gamma(t)\dot{\gamma}(t) < 0. \tag{34}$$

Based on the phase portrait analysis for this conclusion $\gamma(t)\dot{\gamma}(t) < 0$, it can be revealed that the safety surface function $\gamma(t)$ will always converge to zero. This implies the trajectory of system state variables can always approach the safety surface.

The proof is complete. ■

Remark. Theorem 2 demonstrates that with the developed auxiliary trajectory control in (31), the system trajectory can approach the safety surface in (18). This implies the defense capability of the safety surface can be activated successfully. In addition, Theorem 1 shows that when the defense capability is activated, system frequency stability can be ensured, despite the presence of multiple types of cyber-attacks. Therefore, by employing the developed CRC strategy consisting of the designed safety surface and the proposed auxiliary trajectory control, the system frequency stability can be comprehensively guaranteed against multiple types of cyber-attacks.

In addition, it is noteworthy that, unlike existing detection-based methods, our control-based method does not rely on attack detection or state estimation, thus avoiding the requirements for historical data and additional detection monitors [43,44]. Therefore, our method can be simpler, more efficient, and more practical to implement.

4. Case study and verification

4.1. System setup

Table 1
Parameters of frequency regulation system for power system.

Symbols	Parameters	Values	Units
T_{tur}	Steam turbine time constant	0.35	s
T_{gov}	Speed governor time constant	0.2	s
H	Equivalent system inertia coefficient	12	–
K_{D}	Equivalent damping coefficient	1.8	–
K_s	Integral control gain	21.8	–
R	Speed drooping coefficient	0.05	–
S_{N}	Generation capacity	800	MW
f_{N}	Nominal frequency value	50	Hz

The efficacy of the developed CRC strategy against multiple types of cyber-attacks is verified using a frequency regulation system of the power system shown in Fig. 2. The parameter settings for the test system are detailed in Table 1 [5,39]. The control objective is to regulate the power system frequency to the nominal frequency, i.e., 50 Hz.

Various types of cyber-attacks, namely, FDI attack, DoS attack, and latency attack are taken into account for the verification process. FDI attacks can be further categorized into the FDI with static attack pattern and the FDI with dynamic attack pattern [45]. Among them, the static FDI attack has the advantage of the injected data requiring no further modification. This feature makes static FDI attack an easily executable method. Moreover, the dynamic FDI attack requires more resources to modify the injected data in real time, posing challenges for attackers to implement. At the same time, the dynamic attack also presents more challenges for detection, tracking, and defense [46]. Therefore, both static and dynamic types of FDI attack deserve careful consideration. Moreover, combining the aforementioned DoS attack and latency attack, while taking into account diverse attack locations, sensitivity analyses, and different system configurations, the developed CRC strategy is validated in the following 8 distinct scenarios, as detailed below:

[S-1]: Frequency regulation performance under FDI attacks with static attack pattern;

[S-2]: Frequency regulation performance under FDI attacks with dynamic attack pattern;

[S-3] Frequency regulation performance under DoS attacks;

[S-4] Frequency regulation performance under different levels of latency attacks;

[S-5] Frequency regulation performance under multiple hybrid cyber-attacks simultaneously.

[S-6] Comparative case considering cyber-attacks targeting different locations;

[S-7] Sensitive analysis to varying attack levels;

[S-8] Comparative case with different system configurations.

It is noteworthy that the concept of power system frequency resilience refers to the ability of the power system to maintain frequency stability while responding to various types of cyber-attacks or other external interference. In cases involving cyber-attacks, malicious activities can lead to significant frequency fluctuations or even frequency oscillations, posing a threat to the stability of the power system. Therefore, quantifying system frequency resilience is crucial to ensure that the power system can effectively withstand various cyber-attacks and maintain stable operation. To this end, we employ three key indicators to quantify system frequency resilience under cyber-attacks, which are the recover time of frequency (RToF), the maximum frequency deviation (MFD), and the frequency oscillation (FO), as follows:

- RToF under cyber-attacks, denoted as ζ_{RToF}, stands for the duration from the occurrence of a cyber-attack to the completion of the frequency recovery. On this basis, the RToF under cyber-attacks can be represented by the following equation:

$$\zeta_{\mathrm{RToF}} = t_{\mathrm{rec}} - t_{\mathrm{ons}}, \tag{35}$$

  where t_{ons} represents the time of onset of the cyber-attack, and t_{rec} represents the time of frequency recovery. A shorter RToF indicates stronger resilience to external interference and faster recovery, thereby contributing to the power system's frequency stability.
- MFD under cyber-attacks, denoted as ζ_{MFD}, stands for the maximum deviation of the power system frequency from the nominal frequency value (e.g., 50 Hz). It serves as an essential indicator to quantify system frequency resilience. The MFD indicator ζ_{MFD} can be represented as below:

$$\zeta_{\mathrm{MFD}} = \max[\Delta f(t)] - f_{\mathrm{N}}, \ \forall t \in \mathcal{T}, \tag{36}$$

  where the function $\max[\cdot]$ represents the operation of obtaining the maximum value; and $\mathcal{T}$ denotes the set of time during the frequency regulation process. In general, a smaller MFD indicates a faster recovery to the nominal frequency after a cyber-attack.
- FO under cyber-attacks, denoted as ζ_{FO}, refers to the repetitive or periodic fluctuations of the system frequency around the nominal frequency, typically without significant decay over time. The FO indicator ζ_{FO} is a binary variable where $\zeta_{\mathrm{FO}} = 1$ (Yes) and $\zeta_{\mathrm{FO}} = 0$ (No) represent the presence and absence of FO phenomenon, respectively. FO serves as a critical indicator for determining the frequency resilience of the power system. The absence of oscillations signifies better stability, while significant frequency oscillations indicate severe instability, potentially damaging to the power system.

4.2. Frequency regulation performance under FDI attacks with static attack pattern

In this first scenario, the hacker launches FDI attacks with the static attack pattern to disrupt the control process of power system frequency regulation. To be specific, the value of injected false data is set at −0.2, which is a constant value and is injected continuously, as depicted below:

$$\phi(t) = -0.2. \tag{37}$$

Without loss of generality, both over-frequency and under-frequency cases are considered in this scenario. The system frequency performance is illustrated in Fig. 6.

According to Fig. 6, we can observe that under the influence of static FDI attack, severe frequency deviation occurs during the frequency regulation process, and a long time of accommodation is required to complete the frequency recovery. However, using the developed CRC strategy, the power system frequency performance is significantly improved, achieving rapid frequency recovery and slight frequency deviation.

To be specific, due to the influence of static FDI attack, the MFD deteriorates to about 0.32599 Hz and 0.40734 Hz in the over-frequency case in Fig. 6(a) and under-frequency case in Fig. 6(b), respectively. However, with the CRC strategy, the values of this evaluating indicator can be reduced to about 0.00777 Hz and 0.01551 Hz, respectively. In other words, the MFD of the power system (a negative indicator, lower is better) is reduced by about 97.62% and 96.19% in the over-frequency case and under-frequency case, respectively, which means the developed CRC strategy dramatically improves this MFD indicator.

In addition, affected by the static FDI attack, the RToF gets worse to about 20.3835 s and 20.7597 s in the over-frequency and under-frequency cases, respectively. However, with the CRC strategy, the RToF indicator can achieve only about 2.0891 s and 5.2828 s, which saves nearly 89.75% and 74.55% of the time, respectively. This implies that compared to the original, the system frequency can be recovered quickly.

The results of this scenario show that the CRC strategy performs well under static FDI attacks, which not only achieves rapid frequency recovery effectively, but also reduces the frequency deviation significantly during the frequency regulation process. Therefore, the developed CRC strategy contributes to the power system's security when facing static FDI attacks.

4.3. Frequency regulation performance under FDI attacks with dynamic attack pattern

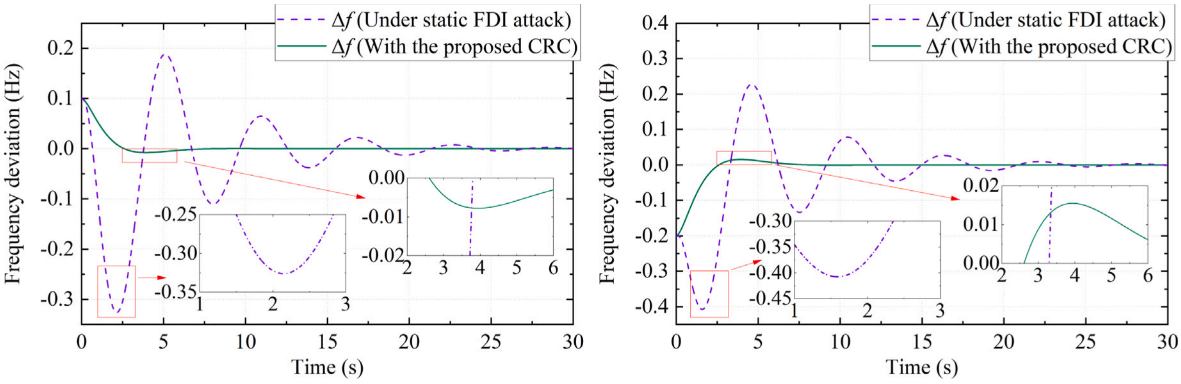
In the second scenario, it is assumed that the hacker launches FDI attacks with dynamic attack pattern to disrupt the control process of power system frequency regulation. The value of injected false data changes over time and can be expressed below:

$$\phi(t) = -0.2 \cdot \sin(2\pi \cdot t). \tag{38}$$

Likewise, both over-frequency and under-frequency cases are considered in this scenario. Under dynamic FDI attacks, the power system frequency test results are illustrated in Fig. 7.

From Fig. 7, it can be seen that the power system frequency fluctuates drastically and fails to converge to the nominal frequency due to the dynamic FDI attack. This is reasonable since the control signal of the frequency regulation system varies with the dynamic attack data. However, under the protection of the developed CRC strategy, the impact of the dynamic FDI attack is negligible, with the system frequency recovering rapidly and the original frequency fluctuations being eliminated effectively.

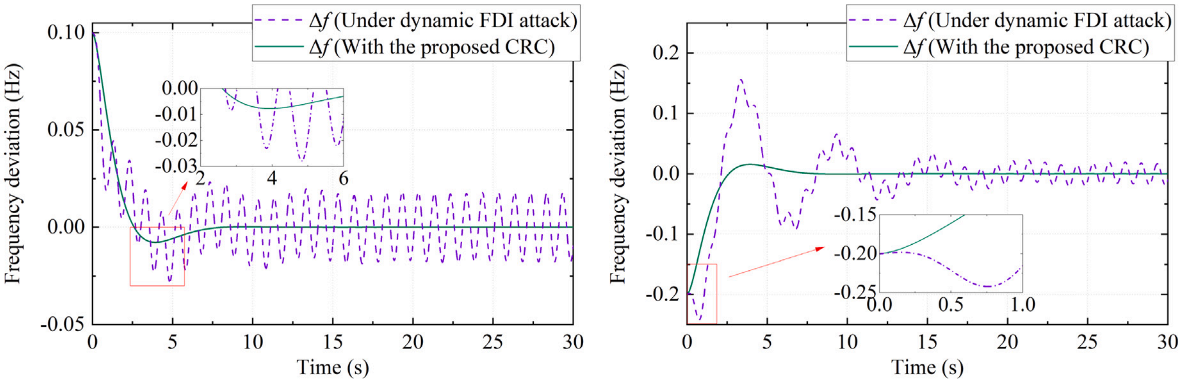
Taking the over-frequency case as an example, from the enlarged view in Fig. 7(a), it can be seen that the MFD deteriorates to about 0.02795 Hz due to the dynamic FDI attack. However, the value of this indicator can be decreased to about 0.00776 Hz with the help of the CRC strategy, which is a remarkable reduction of 72.24%. Moreover, as can be seen from the enlarged view in Fig. 7(b), the frequency is even regulated in the opposite direction at the beginning in the



(a) The over-frequency case.

(b) The under-frequency case.

Fig. 6. Power system frequency performance under FDI attacks with a static attack pattern: (a) over-frequency case; (b) under-frequency case.



(a) The over-frequency case.

(b) The under-frequency case.

Fig. 7. Power system frequency performance under FDI attacks with a dynamic attack pattern: (a) over-frequency case; (b) under-frequency case.

under-frequency case. The CRC strategy can also avoid such undesirable impacts as well.

In addition, affected by the dynamic FDI attack, the system frequency continuously fluctuates and cannot be recovered to the nominal frequency. However, after adopting the CRC strategy, the original system frequency fluctuation is eliminated, and the RToF can achieve only about 2.0906 s. This implies the CRC strategy contributes to a qualitative change in a positive direction from the perspective of frequency recovery.

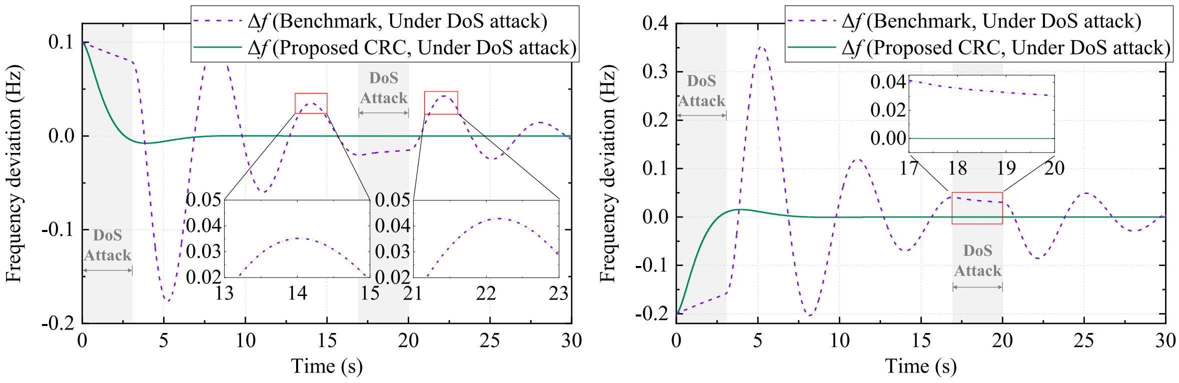
It is worth noting that the static FDI attack in case [S-1] and the dynamic FDI attack in case [S-2] share the same amplitude. In the static FDI attack, the injected false data remains constant throughout. However, in the dynamic FDI attack, the injected data only reaches this constant value at peak moments. During other periods, when the dynamic function is not at its peak, the injected data is lower than this constant value. Therefore, while the injected data during the peak of the dynamic FDI attack matches that of the static FDI attack, it is generally smaller at most other times. This explains why, despite having the same amplitude, the frequency deviation caused by the dynamic FDI attack is smaller compared to the static FDI attack.

Regardless, in this scenario, the results demonstrate that the developed CRC strategy remains highly effective against dynamic FDI attack. It successfully reduces the MDF during the frequency regulation process and facilitates the rapid convergence of the initially fluctuating frequency. Therefore, this strategy proves to be advantageous for power systems in mitigating the impact of dynamic FDI attacks.

4.4. *Frequency regulation performance under DoS attacks*

In the third scenario, DoS attacks are launched by the hacker to interrupt the control process of power system frequency regulation. Specifically, the blocking signal intervals of DoS attacks are 0 s to 3 s, and 17 s to 20 s. During these intervals, the transmission of legitimate data packets is interrupted due to blocking signal overload. Likewise, both over-frequency and under-frequency cases are considered in this DoS attack scenario. The frequency performance under the DoS attacks is illustrated in Fig. 8. To improve the readability of the test results, gray shading is used to represent the duration of the DoS attacks.

As shown in Fig. 8(a) and (b), whether it is the over-frequency case or the under-frequency case, during the first stage (0 s–3 s), the normal regulation cannot be implemented due to the blocking signals of DoS attack, and the initial frequency deviation can only be slowly degraded by the inertia of the power system. For the second stage (3 s–17 s), frequency regulation resumed, and the system frequency gradually converged to the nominal frequency. During this stage, the MFD occurs during the whole frequency regulation process, exemplified by the over-frequency case, i.e., about 0.17667 Hz. For the third stage (17–20 s), the second blocking signal of the DoS attack arrives, again interrupting the frequency regulation process, as seen in the enlarged view of Fig. 8(b). Finally, for the fourth stage (20 s–30 s), the blocking signal of the DoS attack ends, and normal frequency regulation resumes again. It is noteworthy that, observing the enlarged view of Fig. 8(a), the frequency deviation value of the first positive wave peak in the fourth stage reaches about 0.04293 Hz. In contrast, this value of the



(a) The over-frequency case.
(b) The under-frequency case.

Fig. 8. Power system frequency performance under DoS attacks (blocking signal intervals of DoS attacks: 0 s–3 s and 17 s–20 s): (a) over-frequency case; (b) under-frequency case.

second positive wave peak in the second stage of 3–17 s has recovered to only about 0.03518 Hz. This indicates that a DoS attack not only blocks the frequency regulation process, but also worsens the system frequency performance. Even if the normal frequency regulation process is resumed after the end of the DoS attack, the frequency deviation will be worse than before the DoS attack. Therefore, a DoS attack is a serious cyber-attack with disruptive and damaging characteristics.

However, with the implementation of our CRC strategy, the adverse impact of DoS attacks on the frequency performance is significantly mitigated. Specifically, our CRC strategy can reduce the MFD from the original 0.17667 Hz to about 0.00776 Hz. Note that MFD is a negative indicator, with lower being better, and it is reduced by 95.61%, which means the MFD indicator is improved dramatically. In addition, due to multi-stage DoS attacks, the system frequency is difficult to recover to the nominal frequency. However, with our CRC strategy, the system frequency can stabilize at the nominal frequency with the RToF of only approximately 2.0904 s. This signifies a qualitative improvement in terms of frequency recovery.

Therefore, the developed CRC strategy can also effectively address DoS attacks, reducing frequency deviations and assisting in the rapid and accurate system frequency convergence.

4.5. Frequency regulation performance under different levels of latency attacks

In the fourth scenario, different latency attacks are launched by hackers in the frequency regulation process to validate that our proposed CRC method can be equally effective with different levels of attacks. Four different levels of latency attacks are implemented to verify the efficacy of the CRC strategy, introducing time latency of 50 ms, 100 ms, 200 ms, and 300 ms, respectively. The test results under these latency attacks are depicted in Fig. 9.

It can be observed from Fig. 9 that the frequency performance is degraded under different levels of latency attack, as manifested by the large MFD and the long CToF. In addition, frequency oscillations and even frequency destabilization occur when the degree of latency attack is serious. However, with our CRC strategy, all these adverse effects are well countered and eliminated, and the system frequency performance improves dramatically, converging rapidly with very slight frequency deviations.

Specifically, as shown in the enlarged views in Fig. 9(a), (b), and (c), the MFD reaches about 0.05177 Hz, 0.05714 Hz, and 0.06936 Hz due to 50 ms, 100 ms, and 200 ms latency attacks, respectively. In addition, the CToF in the first and second cases are about 13.0477 s and 18.5591 s, respectively. Moreover, the third case exhibits frequency oscillations and fails to converge during the test. The fourth case is the most critical one, the frequency destabilization of the power system occurs, and the frequency deviation continues to increase due to the 300 ms latency attack. This implies the power system is damaged at a severe level. Therefore, latency attacks are undoubtedly destructive to the power system frequency and deserve focused attention.

However, any degree of latency attack can be well defended against when adopting our CRC strategy. For example, the MFD can be reduced to only about 0.00776 Hz in these cases, and in case 3, for instance, this MFD indicator is improved by 88.81%. Moreover, the frequency oscillations and the frequency destabilization in cases 3 and 4 can be well addressed, and the frequency can rapidly converge to the nominal frequency with the CToF of only about 2.0903 s. This indicates a qualitative improvement from the point of view of frequency recovery.

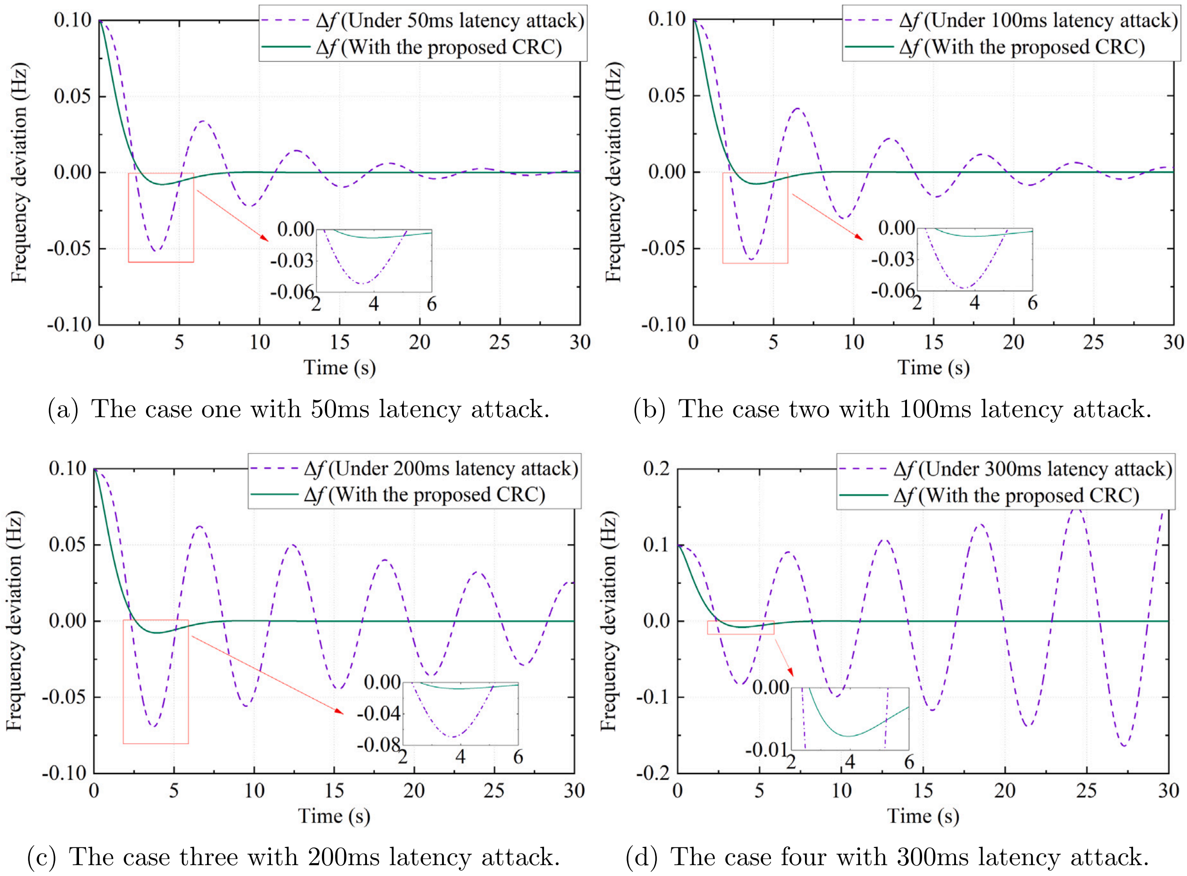
Therefore, the developed CRC strategy can effectively counter different levels of latency attacks. It can help the original destabilized system frequency converge rapidly and accurately, even during communication latency or malicious latency attack scenarios.

4.6. Frequency regulation performance under multiple hybrid cyber-attacks simultaneously

In order to validate the efficacy of the CRC strategy in a complicated situation with multiple hybrid cyber-attacks. This scenario considers FDI, DoS, and latency attacks simultaneously. The FDI attack employs a dynamic false data signal that is more difficult to detect and defend; the DoS attack employs a multi-stage blocking signal, which is launched during 0 s–3 s and 17 s–20 s, respectively; and the latency attack employs a 200 ms time latency. The test results under these multiple hybrid attacks are shown in Fig. 10.

From Fig. 10, it can be observed that the hybrid attack heavily deteriorates the frequency performance of the power system, including large frequency deviations, trouble in convergence, frequency fluctuations, and frequency oscillations. However, these adverse impacts are suppressed, and the frequency performance is significantly improved by employing our developed CRC strategy.

Specifically, frequency oscillations exist under the multiple hybrid attacks that cause four wave peaks throughout the whole test. This is reasonable since the latency attack creates this characteristic. Moreover, power fluctuations and frequency oscillations exist, which make frequency performance even worse and further enhance the destructive capability of cyber-attacks. In addition, the progress of the system frequency regulation is interrupted when the blocking signals of the DoS attack are launched (0 s–3 s and 17 s–20 s). As seen in the enlarged view in Fig. 10, the DoS attack also deteriorates the system frequency performance besides interrupting the regulation process. For example, the original MFD has initially recovered to approximately 0.16064 Hz



(a) The case one with 50ms latency attack.

(b) The case two with 100ms latency attack.

(c) The case three with 200ms latency attack.

(d) The case four with 300ms latency attack.

Fig. 9. Power system frequency performance under different levels of latency attacks: (a) under 50 ms latency attack; (b) under 100 ms latency attack; (c) under 200 ms latency attack; (d) under 300 ms latency attack.

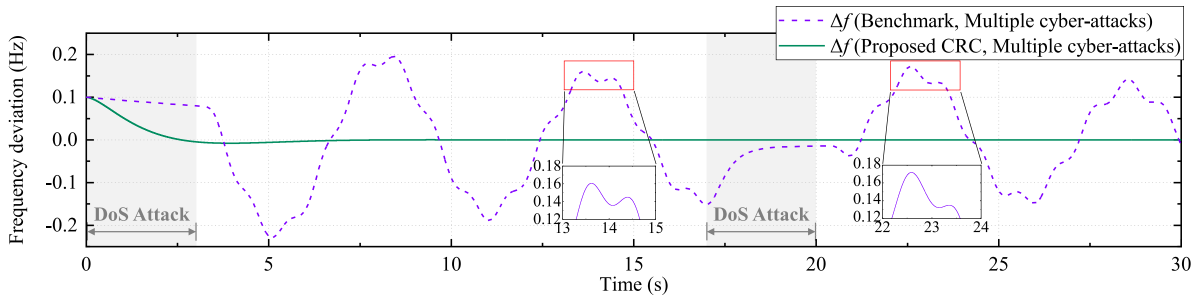


Fig. 10. Power system frequency performance under multiple hybrid cyber-attacks, simultaneously including dynamic FDI attack, DoS attack (blocking signal intervals: 0 s–3 s, 17 s–20 s) and 200 ms latency attack.

(the first enlarged view), but deteriorates to around 0.17185 Hz again after a DoS attack (the second enlarged view). In summary, the test results demonstrate that different types of cyber-attacks can all cause undesirable consequences on the system frequency. This means the damage to system frequency from multiple hybrid attacks is multidimensional, and the adverse consequences of each dimension deserve attention and resolution.

However, using the CRC strategy, the MFD can be reduced from the original 0.2293 Hz to about 0.00777 Hz, an improvement of 96.61%. And the original frequency oscillations are improved to converge with the CToF of only about 2.0904 s. With the help of our strategy, all these adverse characteristics mentioned above are eliminated, and the system frequency is rapidly and accurately recovered to the nominal frequency, despite multiple hybrid attacks. This suggests that the developed CRC strategy can counter against FDI attacks, DoS attacks, and latency attacks comprehensively, and guarantee the power system security even in tough cyber environments.

4.7. Comparative case considering cyber-attacks targeting different locations

This section explores the effectiveness of the CRC method against cyber-attacks targeting different locations through comparative case studies. In these cases, hackers launch a 250 ms latency attack on both the controller and the sensor, targeting different locations. The frequency performance can be illustrated in Fig. 11.

As depicted in Fig. 11(a), a cyber-attack targeting the controller can result in the MFD of 0.07617 Hz. Moreover, this attack can trigger

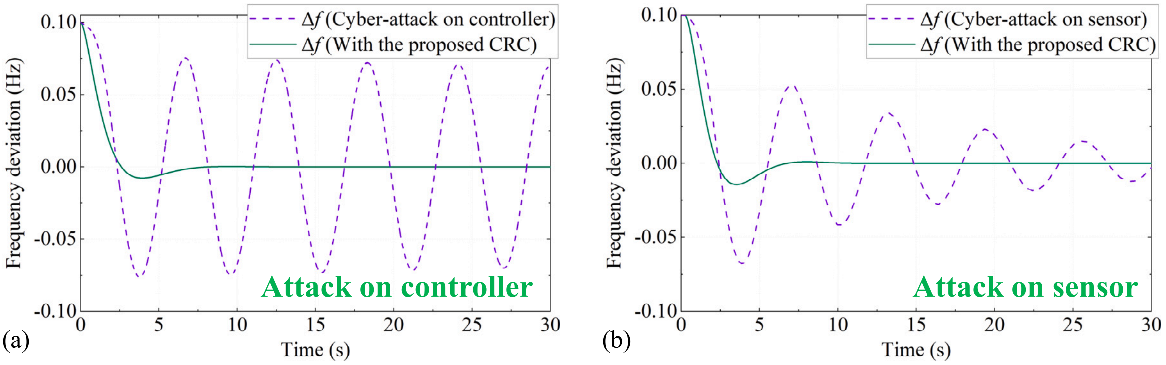


Fig. 11. Comparative cases of power system frequency performance under cyber-attacks in different locations: (a) case of cyber-attack on controller, the frequency oscillation can be eliminated and the attack can be countered; (b) case of cyber-attack on sensor, i.e., another position, the frequency deviation can be mitigated and the recovery time of frequency is shortened significantly.

frequency oscillations, posing a severe threat to the power system's stable operation. However, benefiting from our CRC method, even in the event of an attack on the controller, the MFD is reduced to only 0.00776 Hz, representing an approximately 89.81% reduction. Additionally, frequency oscillations in the power system can be effectively countered.

Furthermore, the frequency performance under the cyber-attack on the sensor (i.e., a different location) can be observed in Fig. 11(b). It is evident that when the sensor is targeted by the cyber-attack, the power system frequency undergoes drastic fluctuations, with the MFD reaching 0.06757 Hz. Moreover, it is challenging for the frequency to recover to its nominal value and the frequency always exhibits deviations. However, benefiting from the CRC method, even under the attack on the sensor (i.e., a different location), the MFD is reduced to only about 0.01434 Hz, representing a reduction of about 78.78% compared to before. In addition, the RToF is significantly shortened. Specifically, it takes only about 4.6608 s for the frequency deviation to recover to within 0.01 Hz. This indicates that the proposed CRC method can enhance power system frequency performance even in the presence of cyber-attacks targeting different locations.

4.8. Sensitive analysis to varying attack levels

Sensitivity analysis involves determining how variations in the output of a model can be attributed to different variations in its input parameters. It helps identify the model's robustness to changes in these parameters. In this part, we consider varying levels of latency attacks with latency times of 50 ms, 100 ms, 200 ms, and 300 ms to a specific system configuration, so as to analyze the sensitivity of the power system frequency to the latency time caused by cyber-attacks, as illustrated in Fig. 12.

From Fig. 12, it can be observed that as the latency time increases, the amplitude of frequency deviation becomes larger, and the time required to recover to the nominated frequency also increases. When the attack latency time reaches 300 ms, frequency oscillations and frequency destabilization even occur. The greater the latency time caused by cyber-attacks, the worse the frequency performance of the power system. Furthermore, for a more intuitive understanding, detailed indicators can be found in Table 2.

From the data in Table 2, it is evident that as the latency time caused by cyber-attacks increases, the frequency performance of the power system deteriorates, such as larger MFD and RToF, and even the FO beginning to occur. This implies that the frequency performance is highly sensitive to the latency time caused by cyber-attacks. However, with our CRC method, even under these varying levels of latency attacks with latency times of 50 ms, 100 ms, 200 ms, and 300 ms, the MFD consistently remains around 0.00776 Hz and the RToF around 2.0903 s. This implies that, with the help of our CRC method, the system frequency is significantly improved and becomes less sensitive to the latency time caused by cyber-attacks. Therefore, the system's robustness against cyber-attacks can be significantly enhanced by our developed CRC method.

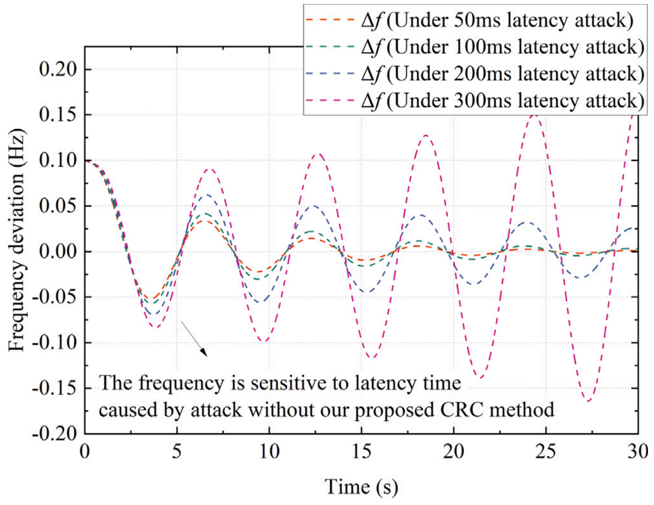


Fig. 12. Sensitivity analysis of the system frequency to the latency time caused by cyber-attacks.

Table 2
Typical indicators for power system frequency considering varying levels of latency attacks.

Scenarios	Typical indicators		
	MFD (Hz)	FO (Y/N)	RToF (s)
Under 50 ms latency attack	0.05177	No	13.0477
Under 100 ms latency attack	0.05714	No	18.5591
Under 200 ms latency attack	0.06936	No	NA
Under 300 ms latency attack	NA	Yes	NA
With CRC method under these attack	0.00776	No	2.0903

Note: NA denotes not applicable.

4.9. Comparative case with different system configurations

To validate that our developed CRC method is equally effective for real-time applications with different configurations, we conduct comparative studies on two different system configurations. The detailed

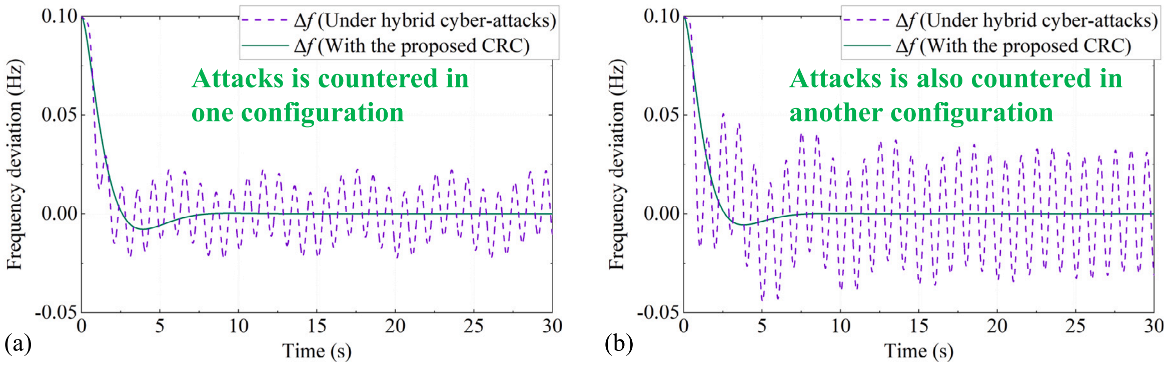


Fig. 13. Comparative cases of power system frequency performance under cyber-attacks with different system configurations: (a) case with the first system configuration described in Table 1, the frequency fluctuations can be eliminated and the adverse attack impact can be countered; (b) case with the second system configuration described in Table 3, the frequency fluctuations can also be eliminated and the adverse attack impact can also be countered.

Table 3
Parameters of Frequency Regulation System for Another Configuration.

Symbols	Parameters	Values	Units
T_{tur}	Steam turbine time constant	0.3	s
T_{gov}	Speed governor time constant	0.1	s
H	Equivalent system inertia coefficient	10	–
K_{D}	Equivalent damping coefficient	1.0	–
K_s	Integral control gain	21.0	–
R	Speed drooping coefficient	0.05	–

parameters for the first system configuration and the second system configuration are shown in Table 1 and Table 3, respectively [5], [39]. In the comparative cases, the same latency attack and dynamic FDI attack are launched simultaneously, but different system configurations are considered. The frequency performance can be illustrated in Fig. 13 below.

Fig. 13(a) illustrates the frequency performance under the first system configuration described in Table 1. As shown in Fig. 13(a), the system experiences serious and sustained frequency fluctuations when subjected to cyber-attacks, failing to recover to the nominal frequency. However, employing our proposed CRC method can eliminate these frequency fluctuations and restore the system frequency to the nominal frequency rapidly, despite cyber-attacks.

Fig. 13(b) depicts the frequency performance under the second system configuration described in Table 3. As shown in Fig. 13(b), the system also experiences sustained frequency fluctuations when subjected to cyber-attacks, failing to recover to the nominal frequency. Moreover, due to the change in system configuration, the impact of cyber-attacks is even more severe in this case. It is worth noting that, as indicated by the green curve in Fig. 13(b), the proposed CRC method can still eliminate the frequency fluctuations and rapidly restore and stabilize the system frequency at the nominal frequency, even in the presence of cyber-attacks, across different system configurations.

Therefore, this comparative case demonstrates that the proposed CRC method is always effective even with different system configurations.

5. Conclusion

It is a critical concern in power systems to safeguard the cybersecurity of the frequency regulation in tough cyber environments. In this paper, FDI, DoS, and latency attacks are all involved, in which FDI attacks aim at tampering with data packets, DoS attacks aim at blocking the communication channel, and latency attacks aim at postponing the transmission of data packets in the frequency regulation system. All these types of cyber-attacks can threaten the frequency security of power systems. To guarantee the security of power systems, the CRC strategy is developed to counter against static FDI attacks, dynamic FDI attacks, multi-stage DoS attacks, and different levels of latency attacks comprehensively. First, a safety surface is designed to function as a secure barrier. Once the system trajectory is located on the safety surface, the adverse impacts of multiple types of cyber-attacks can be countered. Moreover, an auxiliary trajectory control is proposed to drive the system trajectory to approach the safety surface, so as to activate the designed safety surface's defense capability. Furthermore, rigorous proofs theoretically confirm that stability can be guaranteed by the developed CRC strategy, despite multiple types of cyber-attacks.

The test results demonstrate that benefiting from the developed CRC strategy, the frequency performance can be significantly improved even under the tough situation of multiple hybrid cyber-attacks. For example, adopting the developed CRC strategy can reduce the MFD (negative indicator) by about 96.61%, which is a remarkable improvement. In addition, in serious cyber-attack situations, frequency oscillations and frequency destabilization can occur, resulting in the failure of the system frequency to converge to the nominal frequency. However, utilizing our proposed strategy, the system frequency can still realize convergence in only about 2.0904 s, even under multiple hybrid cyber-attacks simultaneously. Therefore, the efficacy of the proposed CRC strategy is validated, which can defend against multiple types of cyber-attacks at the same time, thus making an essential contribution to power system security.

CRediT authorship contribution statement

Shaohua Yang: Writing – review & editing, Writing – original draft, Investigation, Conceptualization. **Keng-Weng Lao:** Supervision, Project administration, Funding acquisition, Investigation, Resources. **Hongxun Hui:** Writing – review & editing, Validation, Data curation, Supervision. **Jinshuo Su:** Validation, Writing – review & editing. **Sheng Wang:** Validation, Writing – review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This work was partly funded by University of Macau Research Committee, Macao SAR (MYRG2022-00168-FST); Science and Technology Innovation Bureau, Zhuhai, China (EF2023-00092-IOTSC).

Data availability

The authors do not have permission to share data.

References

[1] Su J, Zhang H, Liu H, Liu D. Lyapunov-based distributed secondary frequency and voltage control for distributed energy resources in islanded microgrids with expected dynamic performance improvement. Appl Energy 2025;377:124539.

[2] Izuaka M. Why national grid collapsed – Minister. Tech. rep., 2023, [Online]. Available: https://www.premiumtimesng.com/news/top-news/625516-why-national-grid-collapsed-minister.html.

[3] MacIver C, Bell K, Nedd M. An analysis of the August 9th 2019 GB transmission system frequency incident. Electr Power Syst Res 2021;199:107444.

[4] Yang L, Li H, Zhang H, Wu Q, Cao X. Stochastic-distributionally robust frequency-constrained optimal planning for an isolated microgrid. IEEE Trans Sustain Energy 2024. http://dx.doi.org/10.1109/TSTE.2024.3404434.

[5] Yang S, Lao KW, Hui H, Chen Y. A robustness-enhanced frequency regulation scheme for power system against multiple cyber and physical emergency events. Appl Energy 2023;350:121725.

[6] Su J, Zhang H, Wong CK, Yu L, Tan Z. Hierarchical control of inverter air conditioners for frequency regulation service of islanded microgrids with fair power participation. IEEE Trans Smart Grid 2024;15(5):4602–17.

[7] Huang X, Qi D, Chen Y, Yan Y, Yang S, Wang Y, et al. Distributed self-triggered privacy-preserving secondary control of VSG-based AC microgrids. IEEE Trans Smart Grid 2024. http://dx.doi.org/10.1109/TSG.2024.3467392.

[8] Liu S, Liu PX. Distributed model-based control and scheduling for load frequency regulation of smart grids over limited bandwidth networks. IEEE Trans Ind Inf 2018;14(5):1814–23.

[9] Su J, Zhang H, Liu H, Yu L, Tan Z. Membership-function-based secondary frequency regulation for distributed energy resources in islanded microgrids with communication delay compensation. IEEE Trans Sustain Energy 2023;14(4):2274–93.

[10] Hui H, Ding Y, Luan K, Chen T, Song Y, Rahman S. Coupon-based demand response for consumers facing flat-rate retail pricing. CSEE J Power Energy Syst 2024;10(5):1887–900.

[11] Wang S, Zhai J, Hui H, Ding Y, Song Y. Operational reliability of integrated energy systems considering gas flow dynamics and demand-side flexibilities. IEEE Trans Ind Inf 2024;20(2):1360–73.

[12] Shi Q, Li F, Liu G, Shi D, Yi Z, Wang Z. Thermostatic load control for system frequency regulation considering daily demand profile and progressive recovery. IEEE Trans Smart Grid 2019;10(6):6259–70.

[13] Liu H, Pan H, Wang N, Yousaf MZ, Goh HH, Rahman S. Robust under-frequency load shedding with electric vehicles under wind power and commute uncertainties. IEEE Trans Smart Grid 2022;13(5):3676–87.

[14] Bünning F, Heer P, Smith RS, Lygeros J. Increasing electrical reserve provision in districts by exploiting energy flexibility of buildings with robust model predictive control. Adv Appl Energy 2023;10:100130.

[15] Hui H, Chen Y, Yang S, Zhang H, Jiang T. Coordination control of distributed generators and load resources for frequency restoration in isolated urban microgrids. Appl Energy 2022;327:120116.

[16] Ma L, Hui H, Song Y. Data valuation-aware coordinated optimization of power-communication coupled networks considering hybrid ancillary services. IEEE Trans Smart Grid 2024. http://dx.doi.org/10.1109/TSG.2024.3409814.

[17] Yang Z, Li H, Zhang H. Dynamic collaborative pricing for managing refueling demand of hydrogen fuel cell vehicles. IEEE Trans Transp Electrification 2024. http://dx.doi.org/10.1109/TTE.2024.3381236.

[18] Wang S, Hui H, Zhai J, Siano P. Carbon-embedded nodal energy price in hydrogen-blended integrated electricity and gas systems with heterogeneous gas compositions. IEEE Trans Sustain Energy 2024;15(3):1729–42.

[19] Liu X, Lin X, Qiu H, Li Y, Huang T. Optimal aggregation and disaggregation for coordinated operation of virtual power plant with distribution network operator. Appl Energy 2024;376:124142.

[20] Lin X, Huang T, Liu X, Bompard EF, Wang B. A long-term congestion management framework through market zone configuration considering collusive bidding in joint spot markets. IEEE Trans Power Syst 2024. http://dx.doi.org/10.1109/TPWRS.2024.3392934.

[21] Zhou Q, Shahidehpour M, Alabdulwahab A, Abusorrah A, Che L, Liu X. Cross-layer distributed control strategy for cyber resilient microgrids. IEEE Trans Smart Grid 2021;12(5):3705–17.

[22] Hou Q, Dai N, Huang Y. Voltage regulation enhanced hierarchical coordinated volt/var and volt/watt control for active distribution networks with soft open points. IEEE Trans Sustain Energy 2024;15(3):2021–37.

[23] Yang S, Lao KW, Hui H, Chen Y, Dai N. Real-time harmonic contribution evaluation considering multiple dynamic customers. CSEE J Power Energy Syst 2023. http://dx.doi.org/10.17775/CSEEJPES.2022.06570.

[24] Krayem A, Thorin E, Wallin F. Experiences from developing an open urban data portal for collaborative research and innovation. Appl Energy 2024;355:122270.

[25] Chen C, Cui M, Fang X, Ren B, Chen Y. Load altering attack-tolerant defense strategy for load frequency control system. Appl Energy 2020;280:116015.

[26] Hussain S, Hussain SMS, Hemmati M, Iqbal A, Alammari R, Zanero S, et al. A novel hybrid cybersecurity scheme against false data injection attacks in automated power systems. Prot Control Mod Power Syst 2023;8(3):1–15.

[27] Yang S, Lao KW, Chen Y, Hui H. Resilient distributed control against false data injection attacks for demand response. IEEE Trans Power Syst 2024;39(2):2837–53.

[28] Feng G, Lao KW, Chen G. Out-of-distribution detection of unknown false data injection attack with logit-normalized Bayesian ResNet. IEEE Trans Smart Grid 2024. http://dx.doi.org/10.1109/TSG.2024.3416164.

[29] Biswas R, Wu J. Optimal filter assignment policy against distributed denial-of-service attack. IEEE Trans Dependable Secure Comput 2022;19(1):339–52.

[30] Amma NGB, Selvakumar S, Velusamy RL. A statistical approach for detection of denial of service attacks in computer networks. IEEE Trans Netw Serv Manag 2020;17(4):2511–22.

[31] Peng C, Li J, Fei M. Resilient event-triggering H_∞ load frequency control for multi-area power systems with energy-limited DoS attacks. IEEE Trans Power Syst 2017;32(5):4110–8.

[32] Xiahou K, Xu X, Huang D, Du W, Li M. Sliding-mode perturbation observer-based delay-independent active mitigation for AGC systems against false data injection and random time-delay attacks. IEEE Trans Ind Cyber-Phys Syst 2024;2:446–58.

[33] Hosseini SA, Toulabi M, Dobakhshari AS, Ashouri-Zadeh A, Ranjbar AM. Delay compensation of demand response and adaptive disturbance rejection applied to power system frequency control. IEEE Trans Power Syst 2020;35(3):2037–46.

[34] Latif A, Hussain SS, Das DC, Ustun TS. State-of-the-art of controllers and soft computing techniques for regulated load frequency management of single/multi-area traditional and renewable energy based power systems. Appl Energy 2020;266:114858.

[35] Yao L, Wang Y, Xiao X. Concentrated solar power plant modeling for power system studies. IEEE Trans Power Syst 2024;39(2):4252–63.

[36] Wang P, Zhang Z, Dai N, Huang Q, Lee WJ. Robust dynamic equivalent modeling of active distribution network with time-varying parameters. IEEE Trans Power Syst 2024. http://dx.doi.org/10.1109/TPWRS.2024.3471811.

[37] Yao L, Guan Z, Wang Y, Hui H, Luo S, Jia C, et al. Evaluating the feasibility of concentrated solar power as a replacement for coal-fired power in China: A comprehensive comparative analysis. Appl Energy 2025;377:124396.

[38] Chen L, Hui H. Model predictive control-based active/reactive power regulation of inverter air conditioners for improving voltage quality of distribution systems. IEEE Trans Ind Inf 2024. http://dx.doi.org/10.1109/TII.2024.3468475.

[39] Liu J, Gu Y, Zha L, Liu Y, Cao J. Event-triggered H_∞ load frequency control for multiarea power systems under hybrid cyber attacks. IEEE Trans Syst Man Cybern: Syst 2019;49(8):1665–78.

[40] Sontag ED. Mathematical control theory: Deterministic finite dimensional systems, vol. 6, Springer Science & Business Media; 2013.

[41] Friedland B. Control system design: An introduction to state-space methods. Courier Corporation; 2012.

[42] Lyapunov AM. General problem of the stability of motion, vol. 55, (3). CRC Press; 1992.

[43] Yu P, Wang Z, Zhang H, Song Y. Safe reinforcement learning for power system control: A review. 2024, http://dx.doi.org/10.48550/arXiv.2407.00681, arXiv preprint arXiv:2407.00681.

[44] Feng G, Lao KW. Wasserstein adversarial learning for identification of power quality disturbances with incomplete data. IEEE Trans Ind Inf 2023;19(10):10401–11.

[45] Yang S, Lao KW, Hui H, Chen Y. Secure distributed control for demand response in power systems against deception cyber-attacks with arbitrary patterns. IEEE Trans Power Syst 2024. http://dx.doi.org/10.1109/TPWRS.2024.3381231.

[46] Chen B, Wu Q, Li M, Xiahou K. Detection of false data injection attacks on power systems using graph edge-conditioned convolutional networks. Prot Control Mod Power Syst 2023;8(2):1–12.