scientific reports

Check for updates

OPEN

Resilient oscillator-based cyberattack detection for distributed secondary control of inverter-interfaced Islanded microgrids

Fahimeh Zargarzadeh-Esfahani[1], Bahador Fani[1]✉, Babak Keyvani-Boroujeni[2], Iman Sadeghkhani[3,4] & Mahdi Sajadieh[1]

With the increasing integration of Distributed Generation (DG) units and advanced control systems, microgrids have become more vulnerable to cyberattacks, particularly those targeting secondary control mechanisms. False Data Injection (FDI) and Denial-of-Service (DoS) attacks can significantly disrupt the stability and performance of microgrids by manipulating communication links and control signals. This paper proposes a robust cyber-resilient strategy to mitigate the impact of cyberattacks on secondary control in islanded AC microgrids. The proposed approach enhances the resilience of frequency regulation and real power sharing by integrating adaptive anomaly detection and hierarchical control mechanisms. The approach's effectiveness is evaluated through comprehensive simulations in MATLAB/Simulink, considering various cyberattack scenarios, including FDI and DoS attacks on critical communication links. Results demonstrate that, under normal conditions, the primary and secondary controllers ensure frequency stability and balanced power distribution. However, in the presence of cyberattacks, the conventional control strategy fails to maintain stability, leading to frequency deviations and power imbalances. The proposed approach successfully detects and mitigates these attacks, restoring system stability and ensuring robust operation. Furthermore, the effectiveness of the proposed approach is validated across different microgrid topologies, including networked, looped-type, and bus-type configurations, demonstrating its adaptability and effectiveness in diverse network structures.

Keywords Cyberattack, Cybersecurity, Microgrids, Oscillator, Secondary control

Background and challenges

With the increasing penetration of inverter-interfaced Distributed Generation (DG) units in distribution networks, the concept of microgrids has emerged as a promising solution for managing smart grids [1–3]. Microgrids are small-scale power systems that integrate various DG units, energy storage systems, and loads efficiently [4]. One distinguishing characteristic of microgrids is their flexibility to function in both grid-connected and islanded modes, allowing them to disconnect from the main grid due to planned or unplanned events. The control strategies for power management differ significantly between these two operational modes [5]. To ensure reliable operation in islanded mode, inverter-based microgrids typically employ a hierarchical control structure consisting of a local primary control and a centralized or distributed secondary control [6]. Primary control regulates voltage and frequency while sharing power among DGs using the droop control technique, which relies solely on local measurements [7]. However, conventional droop control suffers from poor power-sharing accuracy due to line impedance mismatches and voltage and frequency deviations from nominal values [5]. To address these issues, secondary control is implemented to restore voltage and frequency to their nominal values by adjusting the setpoints of the primary droop controllers. This control level enables data exchange among

[1]Department of Electrical Engineering, Isf.C., Islamic Azad University, Isfahan, Iran. [2]Department of Electrical Engineering, Bor.C., Islamic Azad University, Borojen, Iran. [3]Smart Microgrid Research Center, Na.C., Islamic Azad University, Najafabad, Iran. [4]Department of Electrical Engineering, Na.C., Islamic Azad University, Najafabad, Iran. ✉email: b.fani@iau.ac.ir

DGs via communication networks, enhancing system coordination [8,9]. It is typically implemented in either a centralized or distributed cooperative manner. In the centralized approach, a central controller collects data from all DGs and sends corrective commands. However, this structure has scalability limitations, requires a robust communication network, and is highly vulnerable to single-point failures [10]. To enhance reliability, scalability, and flexibility, distributed cooperative control has gained popularity. In this approach, each DG communicates only with its immediate neighbors based on a directed communication graph, enabling plug-and-play operation and improved fault tolerance [10–12].

Despite its operational advantages, distributed secondary control is highly vulnerable to cybersecurity threats. Unlike centralized control, where a central entity oversees the entire system, distributed microgrids lack global observability, making it difficult to detect malicious activities in communication links. The presence of communication links introduces cybersecurity challenges [13–17], noise, uncertainties, and data accessibility issues. As a result, limited information exchange makes distributed control structures more susceptible to cyberattacks, potentially affecting system stability and control accuracy [18]. In distributed secondary control architectures, both DG units and communication links serve as potential targets for cyberattacks. These attacks threaten data confidentiality, integrity, and availability, ultimately disrupting control objectives such as voltage and frequency regulation. Among various cyber threats, False Data Injection (FDI) and Denial-of-Service (DoS) attacks are the most critical, widely discussed in the literature [19,20].

- *False Data Injection Attacks* These attacks compromise the integrity of control and decision-making processes by injecting falsified measurement data into communication links [21]. As a result, incorrect control commands are issued, leading to voltage and frequency instability [22]. FDI attacks are particularly dangerous because they often remain stealthy and deceptive, making detection extremely challenging [23]. The major consequences of FDI attacks include: (i) Instability in power-sharing and load-generation balance in microgrids, (ii) incorrect operational decisions, leading to blackouts, (iii) increased operational and maintenance costs due to incorrect control actions, and (iv) reduced trust in smart grid technologies, raising security concerns.
- *Denial-of-Service Attacks* In DoS attacks, hackers flood the communication network with unnecessary traffic, disrupting data transmission. This results in severe degradation of communication performance and, in extreme cases, complete failure of data exchange [23]. Consequently, the inability to transmit control signals jeopardizes system stability and microgrid operation [6].

Literature review

In recent years, extensive research has been conducted on cybersecurity challenges in microgrids [24,25]. Based on these studies, existing cyberattack detection and isolation mechanisms in islanded microgrids can be broadly categorized into two main groups [19,20]: (1) Data-driven and (2) signal processing-based approaches. Data-driven approaches primarily utilize machine learning techniques and statistical analysis to derive a system model based on historical data and real-time measurement signals [26–28]. While these methods have shown promising results, a major challenge remains: the difficulty in gathering complete and accurate datasets; In real-world scenarios, obtaining comprehensive datasets for training and validation is often impractical, limiting the effectiveness of purely data-driven approaches. In contrast, signal processing-based approaches enable real-time monitoring of system states, allowing for more effective identification of cyber threats. These approaches can be further divided into two main categories: (i) Model-free and (ii) model-based methods.

Most research on cybersecurity in inverter-based microgrids has focused on either detecting cyberattacks or analyzing their impact [23,29]. A transient model-based technique for detecting FDI attacks on centralized microgrid controllers is proposed in [30]. Ref. [31] investigates the vulnerabilities and challenges of DC microgrids when exposed to FDI attacks. In [32], an extended state observer (ESO)-based approach is introduced to estimate disturbance signals, including FDI attacks in microgrids. However, this approach operates under the assumption that the derivative of disturbance signals remains zero in the steady state., and it does not account for the possibility that the ESO itself could be compromised by adversaries. The concept of a stability region is introduced in [33], discussing the impact of FDI attacks on microgrid utilization levels, but no countermeasures are provided. Ref. [34] proposes an attack detection approach based on signal temporal logic that estimates upper and lower voltage and current limits to indicate potential attacks. However, the presence of false states within these predefined limits can still lead to substantial disruptions in system performance. Ref. [35] examines how cyberattacks infiltrate and affect microgrid systems, while [36,37] provide a detailed classification of different cyberattack strategies.

In [38,39], an active synchronous detection approach is employed to identify cyberattacks targeting controllers. This approach involves generating small probing signals from the microgrid control center and transmitting them to controllers. The output coefficients of the received signals are then compared with predefined values to detect potential cyber threats. However, since the injection of probing signals can introduce minor fluctuations in output parameters, this approach may not be suitable for practical applications. A resilient control strategy against cyberattacks on communication links is proposed in [40]. In this approach, if only one received link is compromised, the faulty unit's data is disregarded to prevent its influence on the system. However, a single compromised link can still affect others. A multi-layer resilient control approach against man-in-the-middle attacks is presented in [41]; it considered attacks on communication links and not sensor attacks.

A resilient control approach for mitigating FDI attacks in DC microgrids is introduced in [42], utilizing a proportional-integral (PI) controller with adjustable gains. A similar noise-reduction technique is employed in [43]. To prevent cyberattacks from spreading to controllers,[44] proposes a mechanism that disables the communication link of compromised units, effectively isolating the affected component. Ref. [45] introduces a resilient control approach capable of reconstructing corrupted data from healthy communication links; however, this approach fails when all links are under attack. A robust synchronization protocol against sensor and actuator attacks is proposed in [33]. Additionally, a trust-based distributed control mechanism is designed to mitigate the effects of

communication link breaches and controller hijacking. However, if more than half of the communication links are compromised, the defense mechanism becomes ineffective.

The impact of DoS attacks on microgrid frequency in the secondary control level, considering active power reference, is analyzed in [46]. A distributed control strategy to mitigate DoS attacks is introduced in [47], where the controller uses the average of outputs as a reference to counteract the attack's effect. However, while this approach neutralizes the attack, it may cause the outputs to drift toward the average rather than the desired reference value. Ref. [46] also employs a decentralized control approach, leveraging Multi-Agent Systems (MASs) to counteract DoS attacks in microgrids. A distributed secondary control approach for AC microgrids using the weighted mean subsequence reduce technique is proposed in [48]. It utilizes a time-varying virtual communication graph, where each DG unit calculates communication link quality based on its own power angle and that of neighboring DERs. Ref. [33] examines FDI attacks targeting distributed load-sharing in microgrids. However, it only analyzes the stability region under such attacks and does not propose any mitigation strategies.

Aims and contributions

Hackers attempting to compromise the operation of inverter-based microgrids with distributed secondary control can lead to severe consequences, including blackouts, equipment damage, and system instability. To mitigate these risks, this paper presents a cyberattack detection and mitigation approach based on the DG frequency, designed to counter both DoS and FDI attacks. In this approach, each energy source's connected bus is equipped with an Intelligent Electronic Device (IED) to extract its frequency, which is then processed by an oscillator. The core advantage of the proposed oscillator-based fault detection mechanism lies in its ability to identify cyberattacks by analyzing the oscillator's state variables. Specifically, cyber-induced disturbances in microgrid communication links during islanded operation alter the oscillator system's phase trajectory, shifting it from a stable oscillatory state to an unstable one. Under such conditions, the state variables of the oscillator increase indefinitely, signaling the presence of an attack. Once a cyberattack is detected, the proposed approach works to restore frequency stability and ensure proper power sharing among inverters in AC microgrids. This is achieved by adjusting and strengthening the weights of healthy communication links within the network graph using oscillator-based equations. A key feature of this approach is its independence from both the microgrid's structural configuration and the specific nature of the cyberattack, enabling a rapid and adaptive response to potential threats. Table 1 compares the features of the proposed strategy with various studied approaches for detecting and mitigating cyberattacks in microgrids.

The main contribution of this paper can be summarized as follows:

- The proposed approach does not rely on identifying the specific type of attack, enhancing the system's flexibility against a wide range of threats. This characteristic, enabled by distributed algorithms and a system dynamics-based model, allows for rapid responses to unexpected disturbances and changes.
- The proposed approach can simultaneously counteract both DoS and FDI attacks due to its decentralized control structure based on oscillators, which reduces direct communication between nodes and strengthens local

Reference	Distributed Secondary Control	Control Goals	Attack Type	Attack on Operators	Attack on Communication Links	Model-Based/Free	Network Type	Detection Approach	Topology Independent
[4]	✓	Detection and mitigation	FDI	X	✓	Model-based	AC	Robust control and machine learning	X
[8]	✓	Increasing stability	Delay and data loss attack	X	✓	Model-based	AC	Machine learning and artificial neural network	X
[23]	✓	Detection	Stealth attack	X	✓	Model-based	DC	Machine learning	X
[26]	✓	Detection	Intelligent data attack	X	✓	Model-free	DC	Data-driven	✓
[27]	✓	Detection and mitigation	Destabilizing attacks	X	✓	Model-free	AC	Deep reinforcement learning	✓
[28]	✓	Defence	FDI	X	✓	Model-free	AC	Distributed deep reinforcement learning	✓
[31]	✓	Detection and mitigation	FDI	X	✓	Hybrid	DC	Nonlinear autoregressive exogenous input-based observers	X
[33]	✓	Robust control	FDI	X	✓	Model-based	DC	Kalman filter and machine learning	X
[34]	X	Detection	FDI	✓	✓	Model-based	DC	Graph neural networks	X
[42]	✓	Robust control	FDI	✓	✓	Hybrid	DC	Robust control and machine learning	X
[46]	✓	Robust secondary control	DoS	X	✓	Model-free	AC	Multi-agent reinforcement learning	✓
Proposed Approach	✓	Detection, frequency restoration, optimal power sharing	FDI, DoS	✓	✓	Model-based	AC	Oscillator	✓

Table 1. Comparison of Proposed Cyberattack Detection Approach with Some Existing Ones.

control at each node. As a result, even when DoS attacks disrupt communication and FDI attacks introduce false sensor readings, the system maintains stable operation.

- Another key feature of the proposed approach is the use of oscillator-based dynamic models to detect anomalies caused by cyberattacks. These models can identify disturbances in key system variables such as voltage, real power, and reactive power. By leveraging this approach, the system can detect abnormal behavior and mitigate the impact of cyberattacks by reinforcing and adjusting the weights of communication links between healthy nodes in the adjacency matrix, thereby reducing the influence of compromised nodes. Consequently, the proposed approach not only detects cyberattacks but also ensures the system's recovery to a stable operating condition.
- This study introduces the use of oscillator-based dynamic models for cyberattack detection in AC microgrids-offering a novel approach that leverages real-time system dynamics rather than relying on historical datasets or predefined attack signatures.

Paper organization

The remainder of this paper is structured as follows. Section 2 provides an overview of the hierarchical control structure of inverter-based islanded microgrids and discusses the role of different control levels in maintaining system stability. The proposed oscillator-based approach for detecting and mitigating cyberattacks is presented in Sect. 3, explaining its operational principles and advantages. Section 4 presents simulation results to assess the effectiveness of the proposed approach under various attack scenarios. Section 5 outlines the main limitations of the proposed approach and discusses directions for future work. Finally, Sect. 6 concludes the paper.

Hierarchical control structure of microgrids

For the proper operation of a microgrid in islanded mode, an effective power management strategy is essential. This necessity arises from the fact that DG units within the microgrid typically have limited power capacity and diverse generation characteristics, and there is often no dominant energy source to regulate frequency under islanded operation. Consequently, the power management strategy must not only ensure appropriate load sharing among DG units but also regulate the system's voltage and frequency. To achieve these objectives, a hierarchical control structure, comprising primary and secondary control levels, is widely employed in islanded microgrids [49], as shown in Fig. 1. The primary control level regulates frequency, output voltage, and power sharing among sources using conventional local droop control technique. The secondary control level, utilizing a distributed communication network, compensates for the errors introduced by the primary control [10].

Primary control

The primary control is typically implemented as a local controller within each DG unit. This controller operates independently and is responsible for maintaining the optimal operating conditions of each DG. To ensure proper coordination among controllers and overall system stability, inter-controller relationships within the microgrid

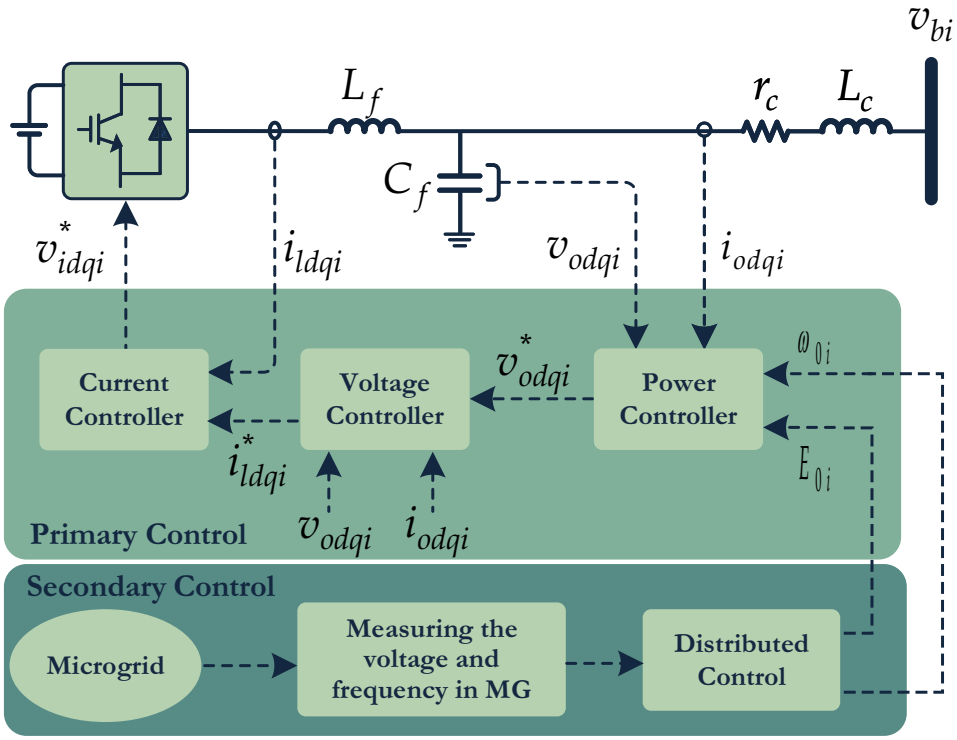

Figure 1. Hierarchical control of inverter-interfaced microgrids.

Attack Type	α_j	$F(\xi_j, t)$
Normal	1	–
DoS	0	0
FDI	$0 < \alpha_j < 1$	$F(\xi_j, t) \neq 0$
DoS & FDI	0	$F(\xi_j, t) \neq 0$

Table 2. Identification of FDI and DoS Attacks.

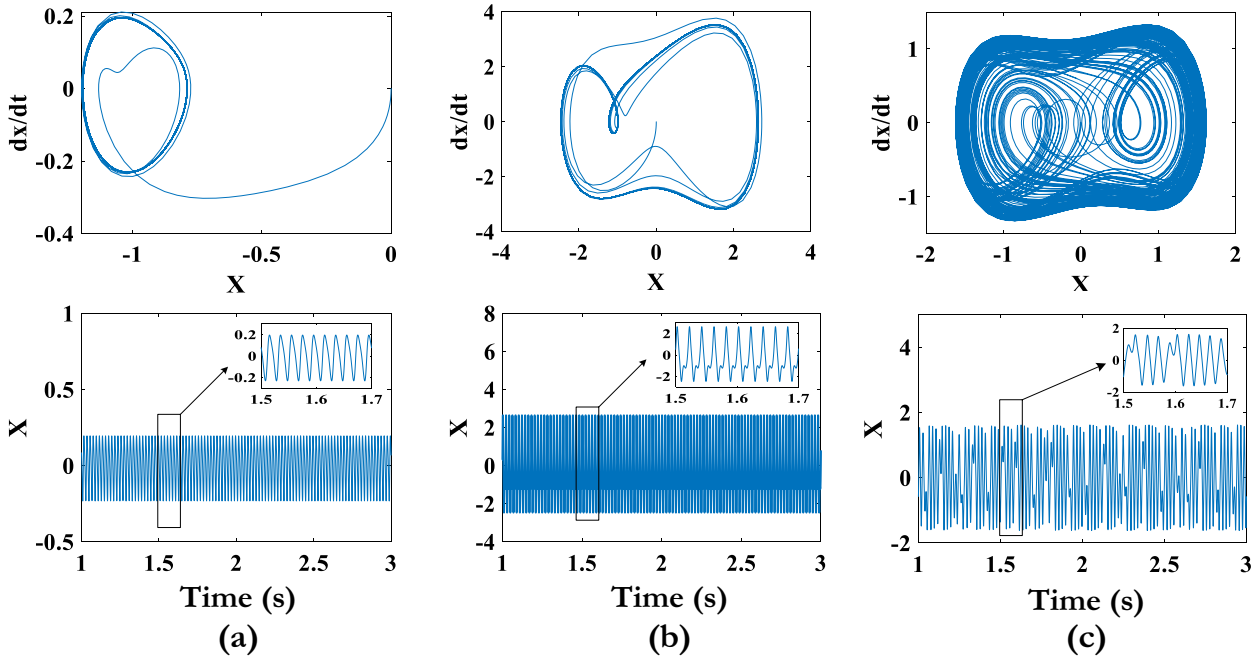

Figure 2. Oscillator in the phase plane and $x - t$ diagram in the (**a**) Stable, (**b**) Oscillatory, and (**c**) Chaotic states of the system.

must be well-defined and managed. This coordination is primarily achieved through the real power-frequency ($P - f$) and reactive power-voltage ($Q - V$) droop control technique. The droop control equations facilitate adaptive control for enhancing system stability and response time [44] as

$$\omega = \omega_0 - m_p P, \tag{1}$$

$$E = E_0 - n_q Q, \tag{2}$$

where ω and E are the frequency and amplitude of voltage reference, and ω_0 and E_0 are these values at no-load, respectively. P and Q represent the measured real and reactive power of the DG unit, and the coefficients m_p and n_q are the real and reactive power droop coefficients, respectively.

Distributed cooperative secondary control

Although the droop-based primary control technique prevents voltage and frequency instability in microgrids, its decentralized nature cannot guarantee the restoration of voltage and frequency to their nominal values. To mitigate deviations from nominal voltage and frequency in the primary control stage, a distributed secondary control approach leveraging a sparse communication network is employed [10]. The secondary control adjusts the reference values of primary control ω_0 and E_0 to drive frequency and voltage deviations to zero. In this technique, each DG unit requires only local information and data from its immediate neighbors within the communication graph.

Frequency control

The distributed secondary control for frequency restoration in microgrids can be formulated as a consensus-based synchronization problem in MASs. The objective is for all DG units to synchronize their terminal voltage magnitudes and frequencies with predefined nominal values, ensuring:

$$\lim_{t \to \infty} (\omega_i - \omega_{\text{ref}}) = 0 \tag{3}$$

$$\lim_{t\to\infty}(E_i - E_{\text{ref}}) = 0, \tag{4}$$

By differentiating the frequency droop characteristic in (1) for *i*th DG unit, the distributed secondary frequency control problem can be expressed as a tracking synchronization problem in the first-order linear MAS as

$$\dot{\omega}_i = \dot{\omega}_{0i} - m_{pi}\dot{P}_i = u_{\omega i} \rightarrow \omega_{0i} = \int (u_{\omega i} + m_{pi}\dot{P}_i)dt, \tag{5}$$

where $u_{\omega i}$ is an auxiliary control variable used to adjust the frequency reference in the primary control loop. When secondary frequency control is applied, the output power of DG units should be allocated following the same pattern established in the primary control, maintaining [50]:

$$m_{p1}P_1 = m_{p1}P_1 = \ldots = m_{pN}P_N. \tag{6}$$

To achieve proportional load sharing among DG units based on their capacities, additional cooperative control is introduced as

$$m_{P_i}\dot{P}_i = u_{pi}. \tag{7}$$

The auxiliary controls u_{pi} and $u_{\omega i}$ can be formulated using the information from their source (DG_i) and their neighboring units through the directed communication graph [10] as

$$u_{\omega i} = -c_{\omega i}\Big(\sum_{j\in N_i} a_{ij}(\omega_i - \omega_j) + g_i(\omega_i - \omega_{\text{ref}})\Big), \tag{8}$$

$$u_{pi} = -c_{pi}\sum_{j\in N_i} a_{ij}(m_{pi}P_i - m_{pj}P_j), \tag{9}$$

where $c_{\omega i}$ and c_{pi} are positive control gains that determine the rate at which the secondary frequency control converges to its desired state. The gain $g_i \geq 0$ represents the edge weight of the directed communication graph, which is nonzero for at least one source connected to the reference node.

By substituting (8) and (9) into (5), the reference frequency in the primary control level is computed as

$$\begin{aligned}\omega_{0i} &= \int (u_{\omega i} + m_{pi}\dot{P}_i)dt \\ &= \int \Big(- c_{\omega i}\Big(\sum_{j\in N_i} a_{ij}(\omega_i - \omega_j) + g_i(\omega_i - \omega_{\text{ref}})\Big) - c_{pi}\sum_{j\in N_i} a_{ij}(m_{pi}P_i - m_{pj}P_j)\Big)dt.\end{aligned} \tag{10}$$

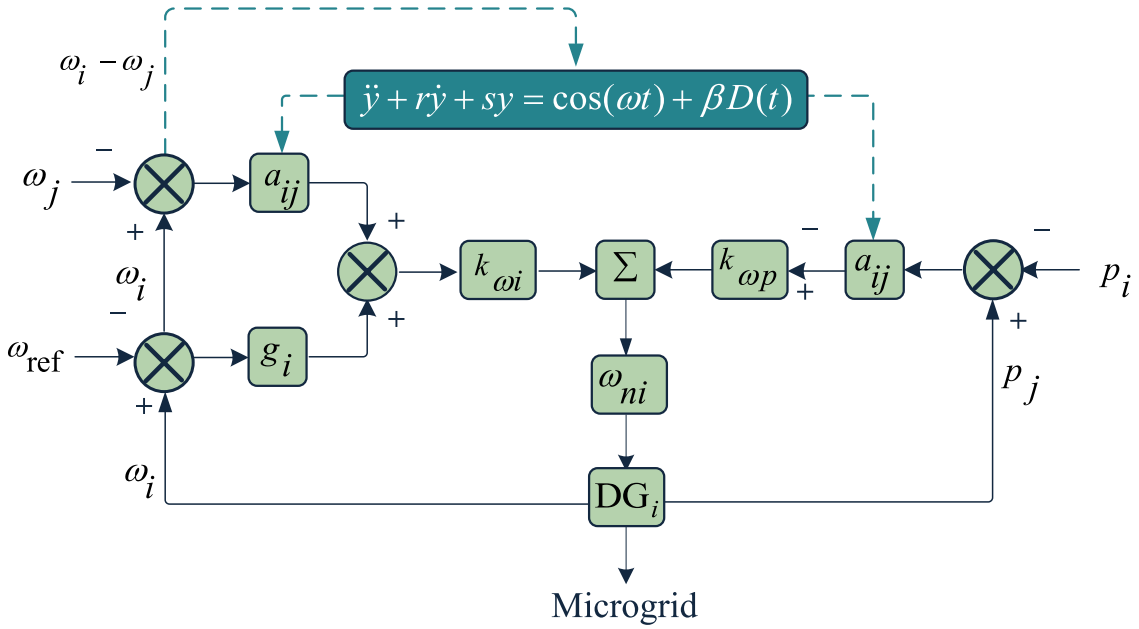

Figure 3. Block diagram of the proposed cyberattack detection approach.

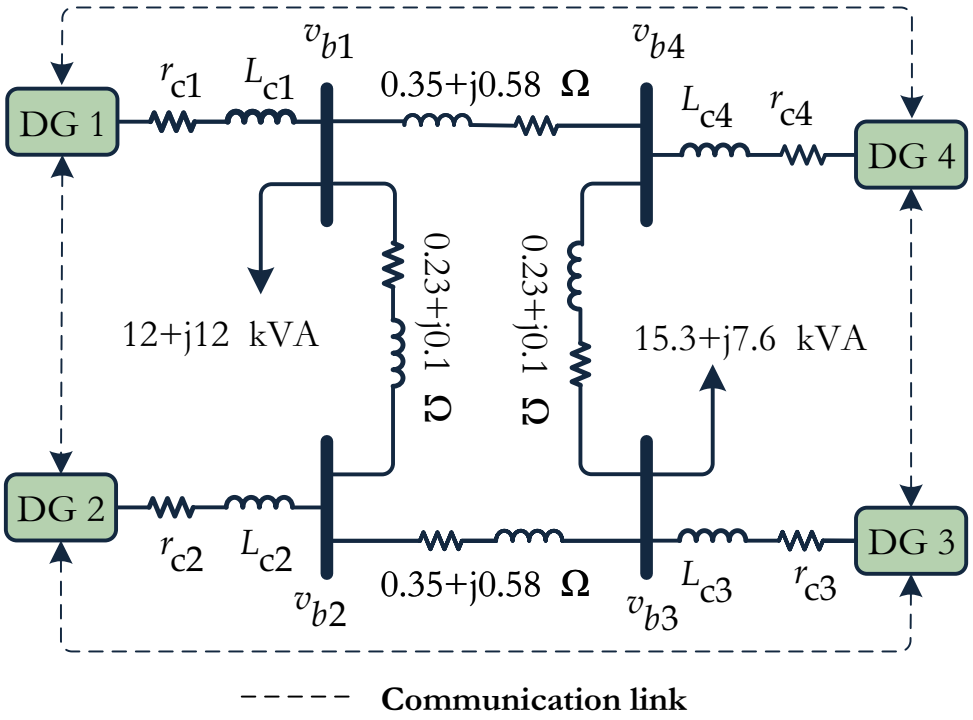

Figure 4. Single-line diagram of the study test microgrid.

Parameter	Value
Inverter filter	$C_f = 50\,\mu$F, $L_f = 1.35$ mH, $r_f = 0.1\Omega$
DG interface cable impedance	$r_c = 0.03\Omega$, $L_c = 0.35$ mH
Droop coefficients	$m_{p1} = m_{p2} = 9.4 \times 10^{-5}$
	$m_{p3} = m_{p4} = 12.5 \times 10^{-5}$
	$n_{q1} = n_{q2} = 1.3 \times 10^{-3}$
	$n_{q3} = n_{q4} = 1.5 \times 10^{-3}$
Controller coefficients	$k_pv1 = k_pv2 = 0.1,\ k_iv1 = k_iv2 = 420$
	$k_{pv3} = k_{pv4} = 0.05,\ k_{iv3} = k_{iv4} = 390$
	$k_{pc1} = k_{pc2} = 15,\ k_{ic1} = k_{ic2} = 20000$
	$k_{pc3} = k_{pc4} = 10.5,\ k_{ic3} = k_{ic4} = 16000$
Cut-off frequency of controller	$\omega_c = 31.41$ rad/s
Oscillator threshold	$y_{\text{th}} = 1.5$

Table 3. Parameters of the Study Test Microgrid.

Despite the capability of the distributed secondary control technique to restore the terminal voltage magnitude and frequency of microgrid sources to their nominal values, the lack of complete information in distributed communication structures increases the vulnerability of the microgrid to cyber attacks such as FDI and DoS attacks.

Oscillator-based cyberattack detection and mitigation

Cyberattacks on secondary control

Due to the heavy reliance of the distributed secondary control structure on information exchange between DGs, cyberattacks can significantly impact the stability of AC microgrids. The severity and extent of this impact depend on the type and scale of cyberattacks, which can range from minor adjustments in system settings to widespread disruptions in the overall operation of the microgrid. This section examines and models two common types of cyber attacks: FDI attacks, which involve injecting incorrect data into communication links between agents, and DoS attacks, which prevent an agent from receiving information from its neighboring agent.

To analyze the effects of both types of cyberattacks on the communication links between neighboring agents in the communication graph, attacks can be modeled as follows:

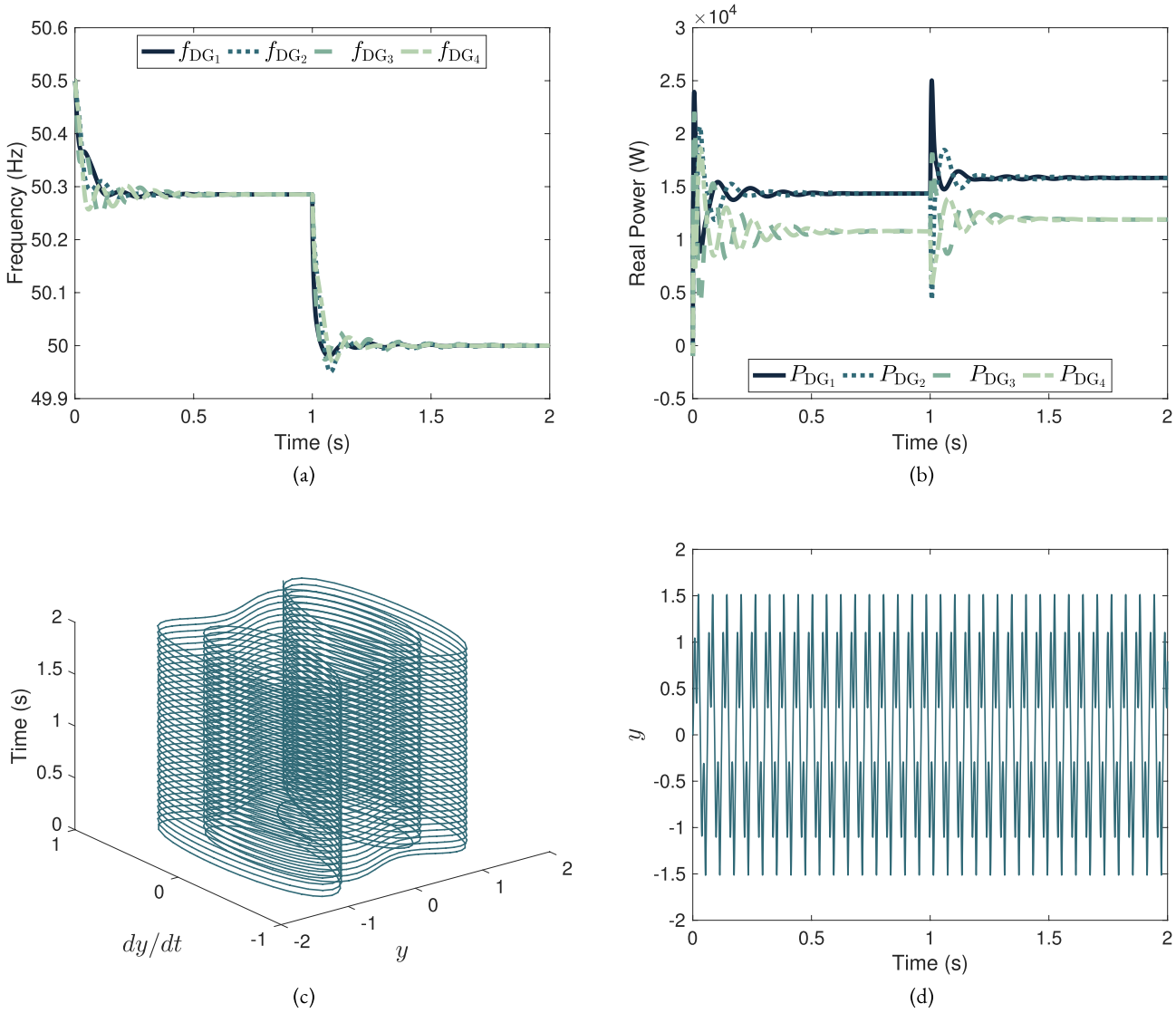

Figure 5. Performance of microgrid control in the absence of a cyberattack. (**a**) Frequency, (**b**) Real power, (**c**) Oscillator output and (**d**) 3D oscillator response.

$$\omega_j^{\text{att}} = \alpha_j \omega_j^{\text{nom}} + \Big(1 - \alpha_j F(\xi_j, t)\Big) \tag{11}$$

This equation simulates the impact of cyber attacks on key system parameters such as frequency, power, and communications, providing a foundation for designing countermeasures. ω_j^{att} represents the compromised frequency data, ω_j^{nom} is the nominal frequency in the absence of an attack, and the coefficient α_j, which varies between 0 and 1, indicates the extent to which the signal is affected by the attack. The function $F(\xi_j, t)$ models the changes caused by the attack, which can include random noise, false data, or any other frequency alteration. The presence or absence of different types of cyber attacks in the microgrid is defined in Table 2.

If $\alpha_j = 1$), the system operates normally with no attack. A value of $\alpha_j = 0$ along with $F(\xi_j, t) = 0$) indicates a DoS attack, which disrupts communication. In an FDI attack, $0 < \alpha_j < 1$, and false data $F(\xi_j, t) \neq 0$ is injected into the system. In the combined FDI & DoS attack, $\alpha_j = 0$ and $F(\xi_j, t) \neq 0$, meaning that communication is disrupted while simultaneously injecting false data.

By replacing the compromised frequency data of source *j*, ω_j^{att}, into (10), this equation can be rewritten as

$$\omega_{0i} = \int \left(- c_{\omega i} \Big(\sum_{j \in N_i} a_{ij} (\omega_i - \omega_j^{\text{att}}) + g_i (\omega_i - \omega_{\text{ref}}) \Big) - c_{pi} \sum_{j \in N_i} a_{ij} (m_{pi} P_i - m_{pj} P_j) \right) dt. \tag{12}$$

The error between *i*th inverter frequency and the nominal frequency is denoted as $\Delta\omega_i = \omega_i^{\text{att}} - \omega_i^{\text{nom}}$. The frequency dynamics under attack can be expressed as $\Delta(t) = -\alpha k(L+G)\Delta\omega(t) + BF(\xi, t)$, where $\alpha k(L+G)$

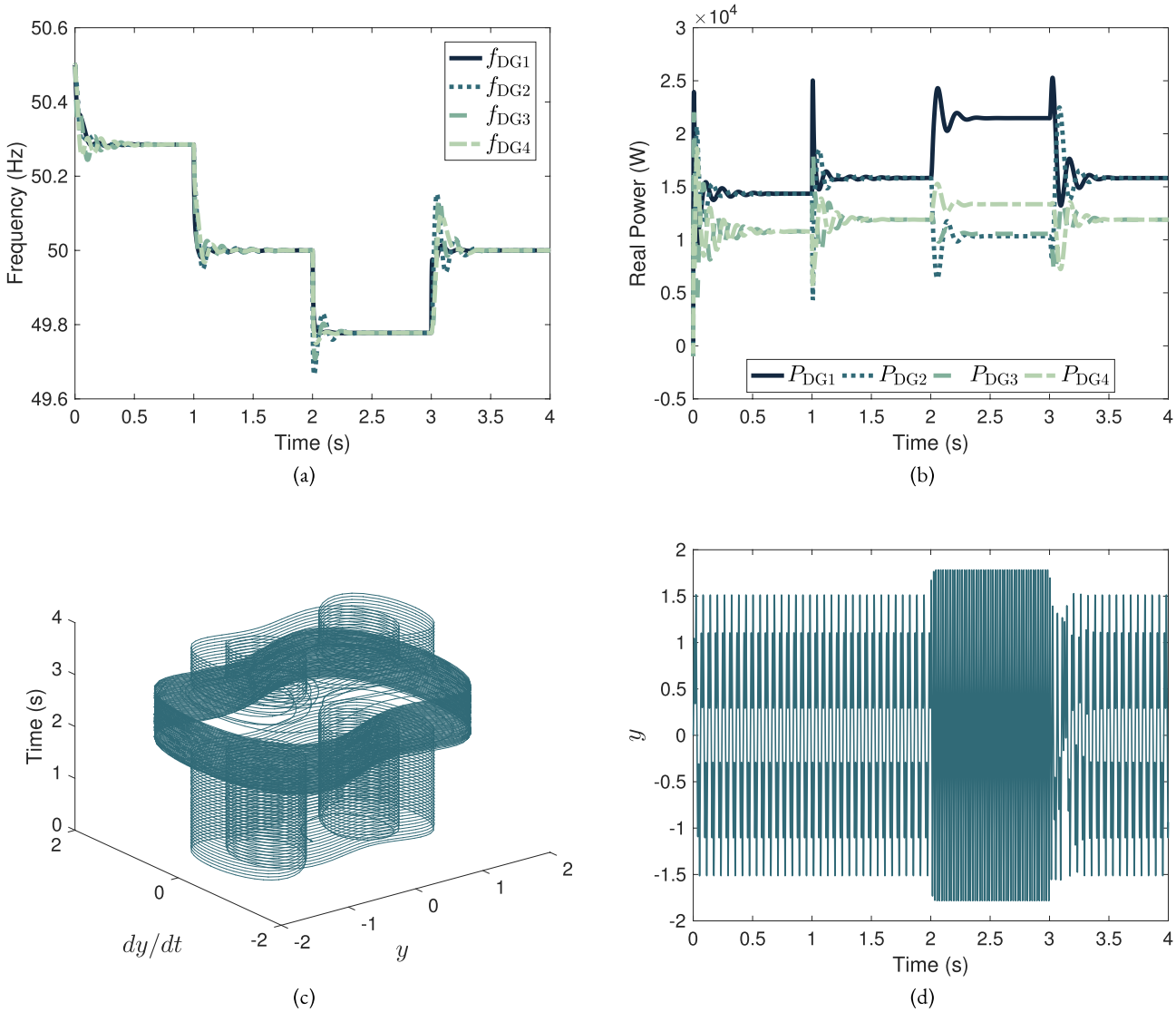

Figure 6. Performance of microgrid control equipped with the proposed approach under an FDI attack. (**a**) Frequency, (**b**) Real power, (**c**) Oscillator output and (**d**) 3D oscillator response.

represents the characteristics of the communication network links. A higher value of this term indicates an increased rate of information exchange between inverters in the microgrid. The matrix L acts as the Laplacian of the communication network, while G represents the secondary control layer. The convergence gain of the secondary control is determined by k, which directly affects the frequency synchronization speed of the microgrid.

Since $\alpha k(L+G)$ is a negative and invertible term, in normal conditions without an attack, $\Delta\omega_i$ gradually decreases and converges to zero. However, in the presence of a cyberattack, $\Delta\omega_i$ converges to a nonzero value, leading to a disturbance in frequency synchronization across the microgrid. Given the direct relationship between frequency and real power, this disturbance disrupts the proportional real power sharing in the microgrid and ultimately affects system stability.

Basic principle

Nonlinear dynamic systems exhibit three stability conditions: (i) stable, (ii) oscillatory, and (iii) chaotic. As a nonlinear dynamic system, islanded microgrids are highly vulnerable to cyberattacks due to their heavy reliance on information exchange through communication networks for generation-load coordination and frequency regulation. Some cyberattacks, such as FDI and DoS attacks, are designed to remain undetectable in their early stages, gradually altering measured values. Although these changes may initially appear insignificant, they can lead to long-term frequency deviations and improper power sharing within the microgrid.

To address this issue, this paper proposes the use of an oscillator that is sensitive to minor frequency variations and can detect and mitigate cyberattacks before they cause severe instability in the network. The standard dynamic equation of the oscillator is expressed as [51]

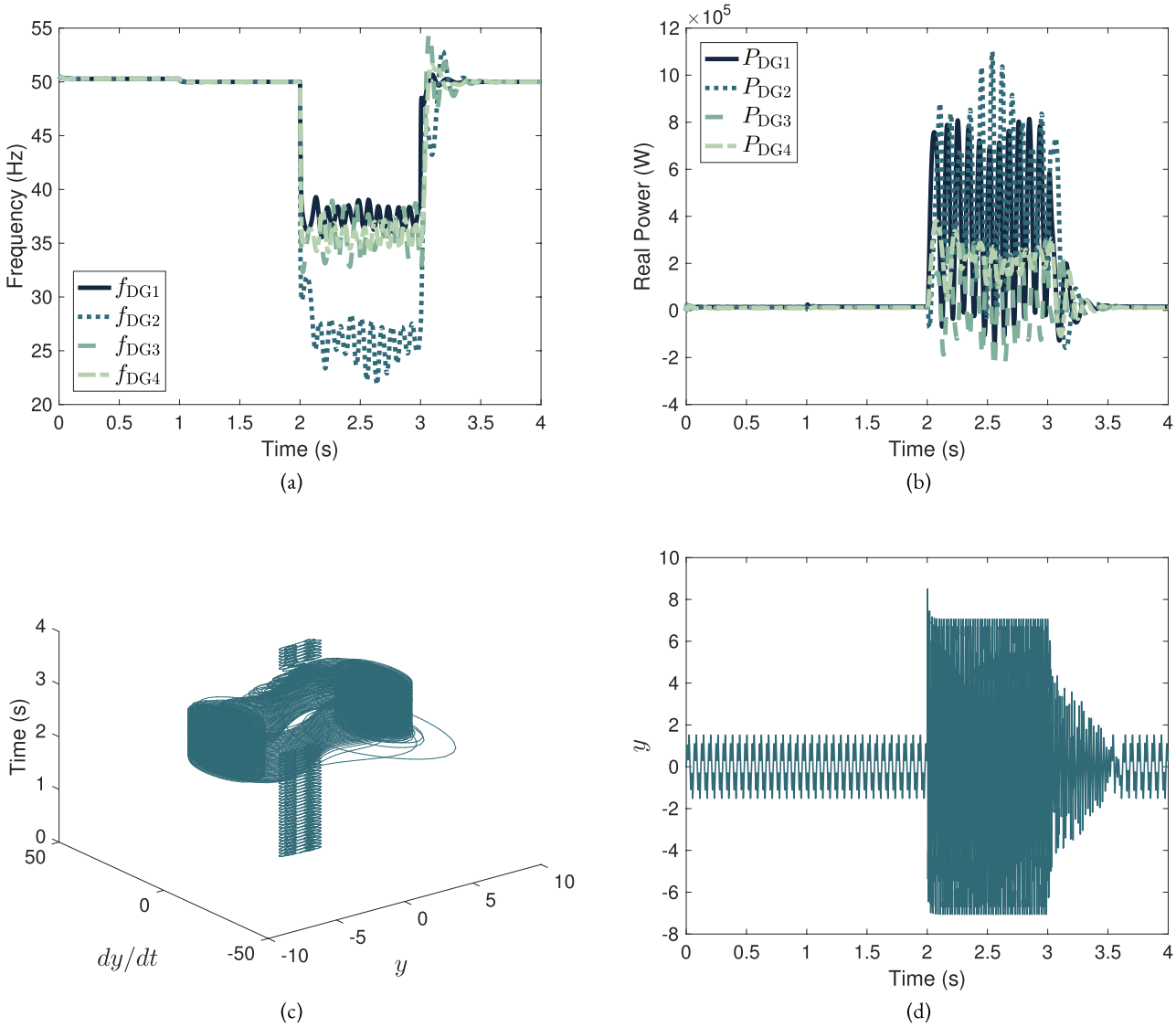

Figure 7. Performance of microgrid control equipped with the proposed approach under a DoS attack. (**a**) Frequency, (**b**) Real power, (**c**) Oscillator output and (**d**) 3D oscillator response.

$$\ddot{y} + r\dot{y} + sy = \cos(\omega t) + \beta D(t), \tag{13}$$

where r and s are the equation coefficients, ω represents the angular frequency of excitation, $D(t)$ denotes the disturbance caused by cyberattacks, and β determines the impact of these attacks on the system. In this technique, under normal conditions where no frequency deviations occur in the network, the oscillator's input remains constant, and its response stays within a predefined range as

$$y(t) = c_1 e^{\lambda_1 t} + c_2 e^{\lambda_2 t}, \tag{14}$$

where λ_1 and λ_2 are the system's eigenvalues (Fig. 2a).

When a cyberattack begins, the network frequency undergoes slight and gradual variations. This change causes the oscillator to slowly deviate from its stable state and move toward instability. The oscillator's response in this case is given by

$$y(t) \approx e^{\gamma t} \sin(\omega t), \tag{15}$$

where γ represents the degree of variation in the network, which, if it increases gradually, indicates the occurrence of a cyberattack. In this state, the system continues to oscillate, but its amplitude gradually increases (Fig. 2b). However, if the variation exceeds a certain threshold, the network experiences severe instability, and the oscillator's state variable diverges toward an unbounded value, as expressed in (16). This condition signifies the onset of chaos in the system, necessitating an immediate response (Fig. 2c).

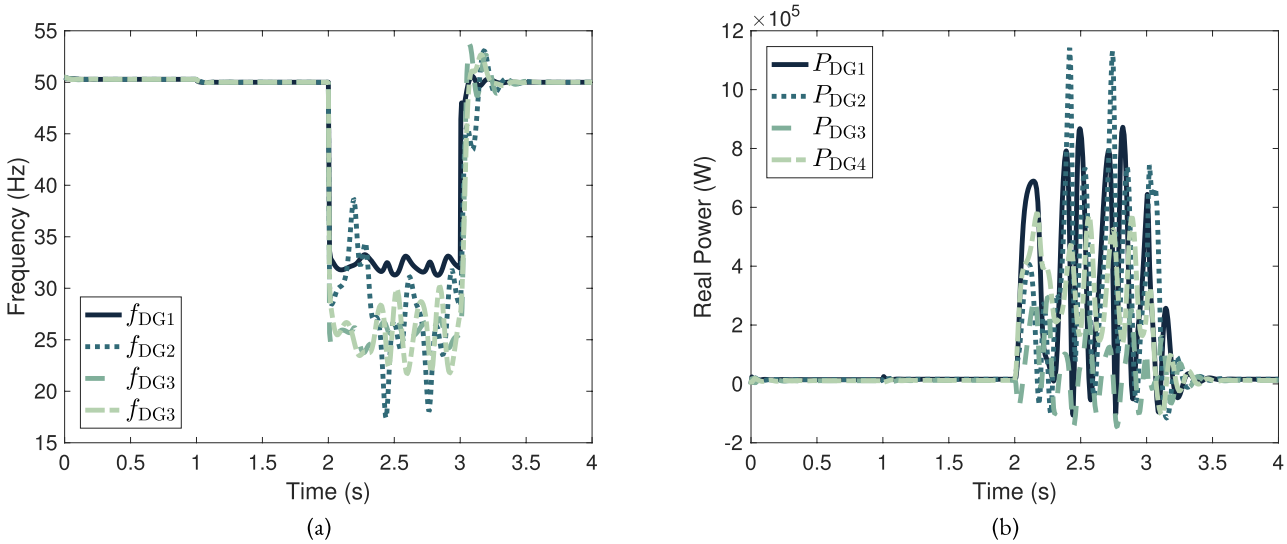

Figure 8. Performance of microgrid control equipped with the proposed approach under simultaneous FDI and DoS attacks. (**a**) Frequency and (**b**) Real power.

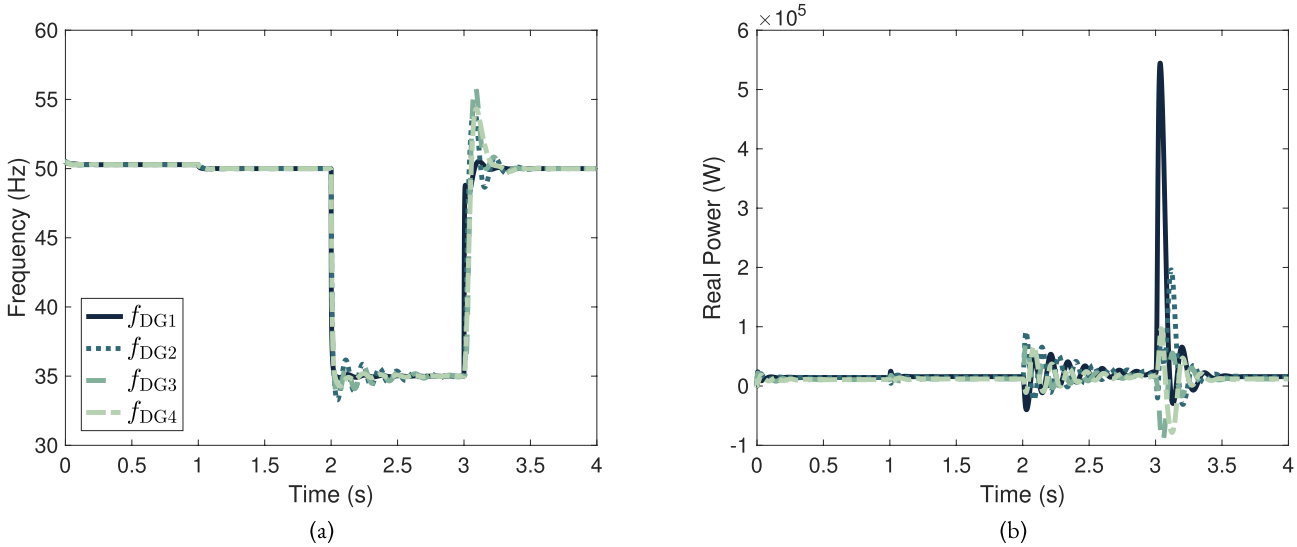

Figure 9. Performance of microgrid control equipped with the proposed approach under an FDI attack and communication delay. (**a**) Frequency and (**b**) Real power.

$$\lim_{t\to\infty} y(t) = \infty. \tag{16}$$

Proposed approach

To detect an attack, the oscillator's output is monitored. If the output remains within the standard range, the network is in a normal state. However, if the output exceeds a predefined threshold y_{th}, an attack is detected, as expressed in (17), and necessary actions must be taken to mitigate its impact.

$$D = \begin{cases} 0, & \text{if } y < y_{\text{th}} \rightarrow \text{ Normal operation }, \\ 1, & \text{if } y \geq y_{\text{th}} \rightarrow \text{ Attack detected }. \end{cases} \tag{17}$$

At this stage, the status of communication links is analyzed, and those experiencing the most significant changes are identified as compromised links. Links with severely altered data are excluded from the data transmission process, and healthier communication paths are selected and reinforced. After identifying the compromised links, as shown in Fig. 3, the weighting coefficient a_{ij} in the healthy links is adjusted in (12) to reconfigure the frequency across different network points, effectively mitigating the impact of the attack. By selecting more stable links, the system can restore its nominal frequency and prevent instability. This process is continuously

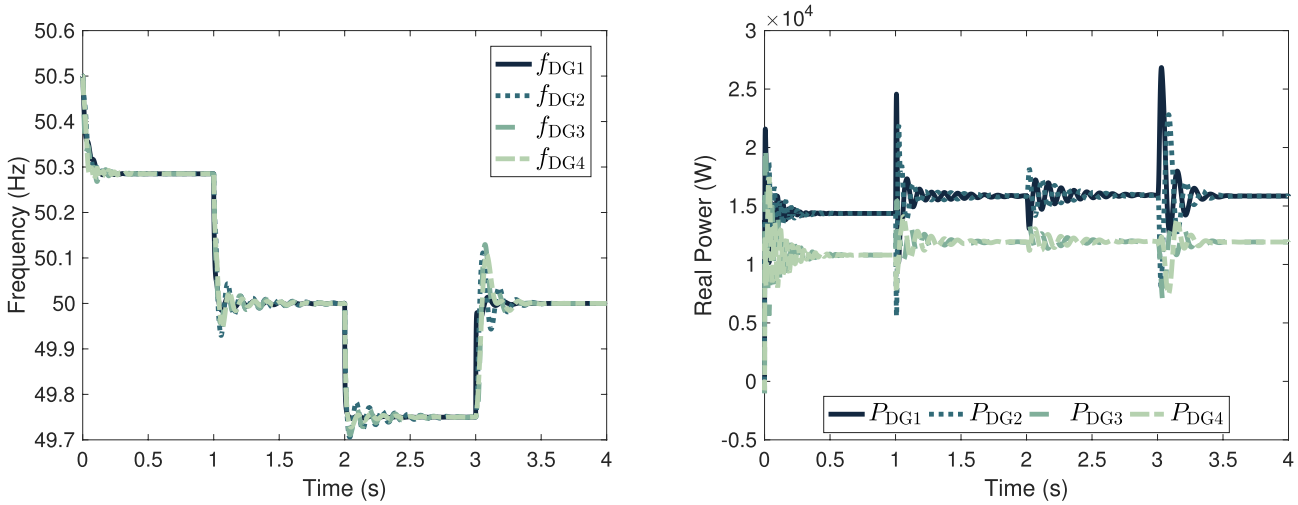

Figure 10. Performance of microgrid control equipped with the proposed approach under an FDI attack and change of R/X ratio. (**a**) Frequency and (**b**) Real power.

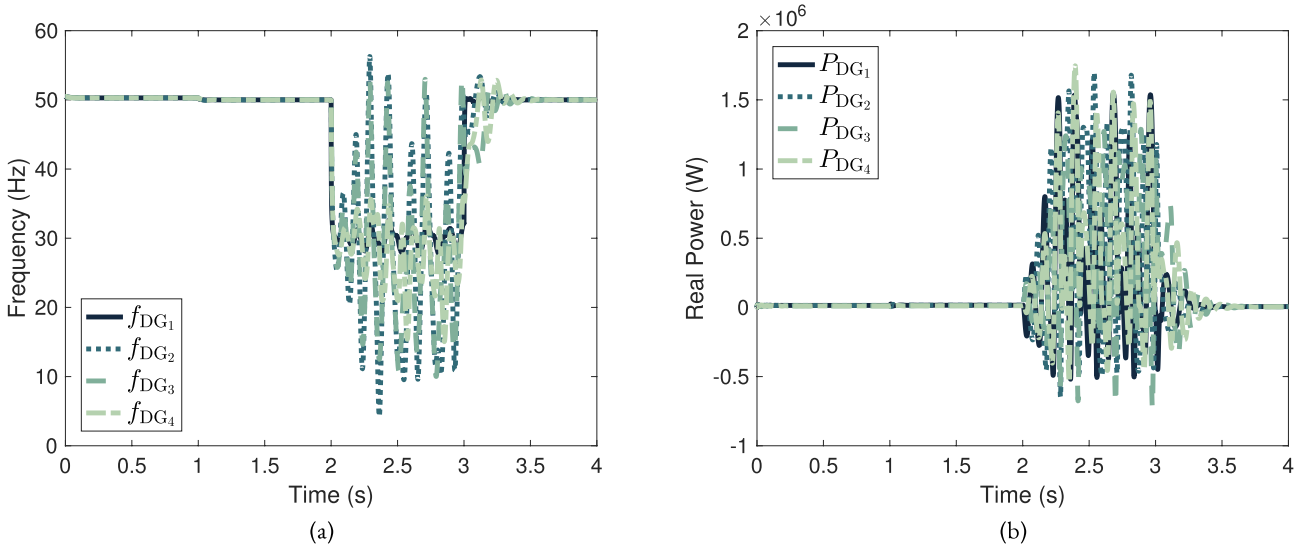

Figure 11. Performance of microgrid control equipped with the proposed approach under a Dos attack and change of R/X ratio. (**a**) Frequency and (**b**) Real power.

performed, with the network status being monitored based on the oscillator's output at all times. If a new attack occurs, the system can respond quickly and effectively. The key advantage of this approach is its independence from the type of attack and the topology of the microgrid. Algorithm 1 presents the execution procedure of the proposed approach.

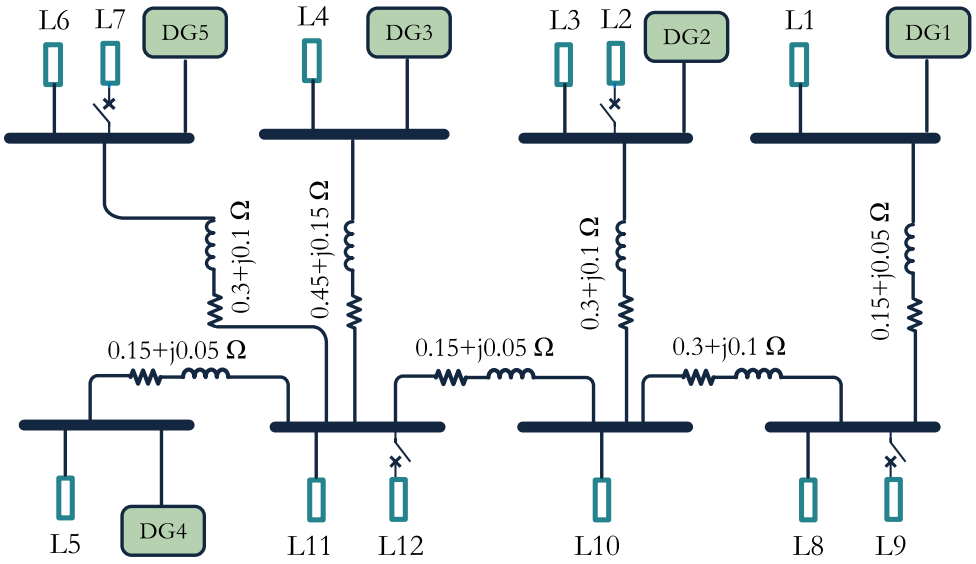

Figure 12. Study networked microgrid.

Input: Adjacent unit frequency data ω_j^{att}
Output: Updated communication weights a_{ij}
Determine local frequency using conventional droop control (Equations (1) and (2));
Receive frequency input ω_j^{att} from neighboring DG units;
Compute anomaly index y;
if $y < y_{th}$ **then**
    No anomaly detected;
    Set $a_{ij} \leftarrow 1$ for all adjacent units;
else
    Cyberattack detected;
    Recalculate a_{ij} using Equation (13);
end
Update communication weights a_{ij} in the distributed secondary control (Equation 12);
Repeat the process continuously in real-time;

Algorithm 1. Execution Procedure of the Proposed Cyber-Resilient Mechanism

Performance assessment

In this section, the effectiveness of the proposed approach is evaluated on a three-phase islanded microgrid shown in Fig. 4 by conducting multiple simulation scenarios in the MATLAB/Simulink environment. The test system comprises four DG units and two loads, interconnected via bidirectional communication links to facilitate information exchange. The nominal operating frequency and voltage of the microgrid are 50 Hz and 400 V, respectively. The detailed parameters of the test system and controllers are provided in Table 3. The detection logic triggers an attack alarm when the oscillator output exceeds a threshold value y_{th}. In this work, the threshold is set to 1.5, determined through extensive simulation studies encompassing both normal operation and various FDI and DoS attack scenarios. The selected value effectively avoids false alarms while ensuring timely detection of cyberattacks.

Scenario 1: controller performance under normal operation

In this section, the performance of the study microgrid under normal operating conditions, without cyberattacks, is analyzed. Fig. 5 shows the performance of the microgrid control system including frequency and output power as well as oscillator output. For $t < 1$ s, the primary control (droop control) effectively regulates power sharing and mitigates frequency oscillations. However, secondary control is essential to eliminate steady-state errors. At

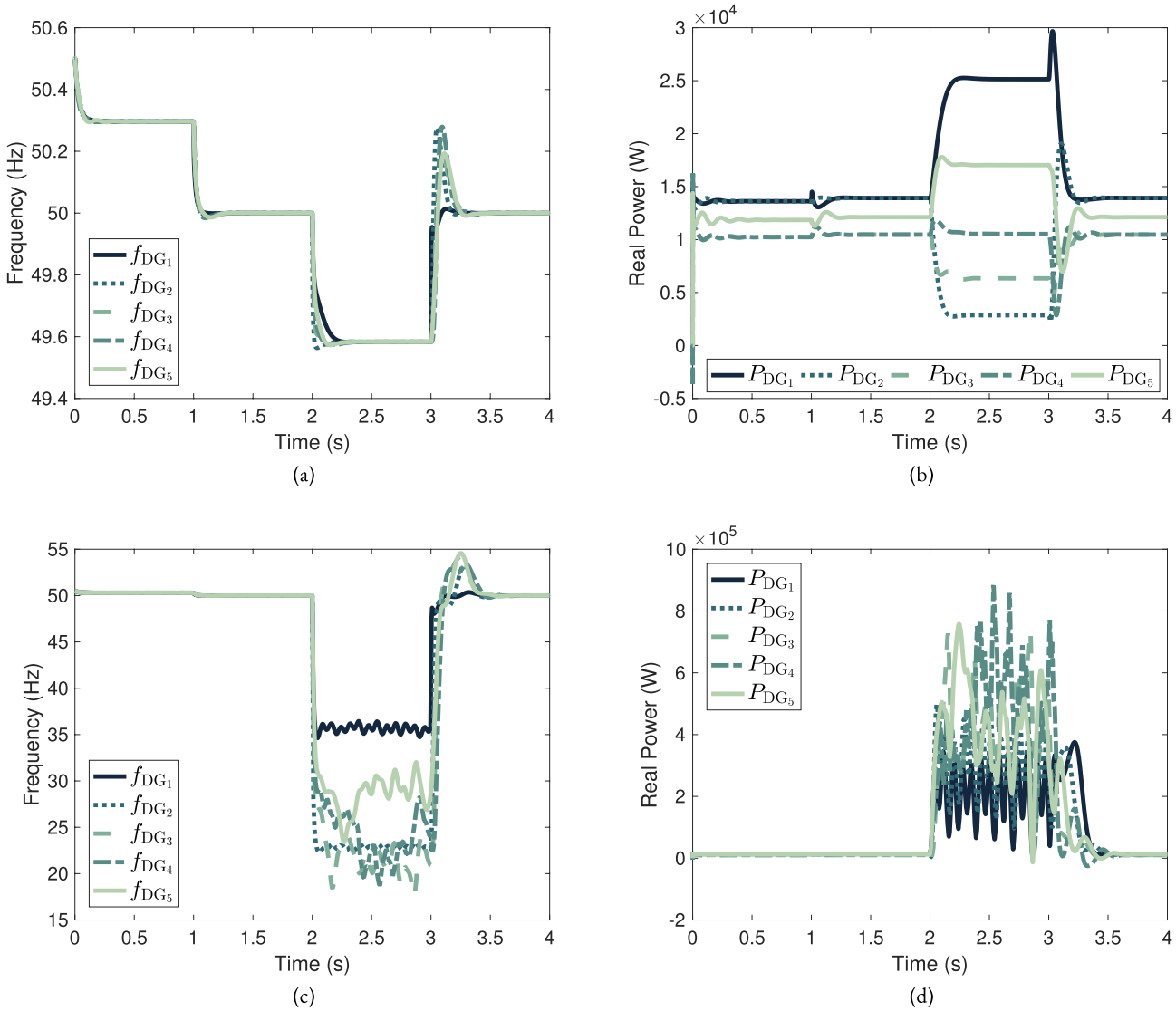

Figure 13. Performance of microgrid control equipped with the proposed approach in the study networked microgrid. (**a**) Frequency response under FDI attack, (**b**) Real power response under FDI attack, (**c**) Frequency response under DoS attack, and (**d**) Real power response under DoS attack.

$t = 1$ s, the activation of secondary control leads to a more balanced power distribution among DG units and restores the system frequency to its nominal value of 50 Hz. These results highlight the critical role of integrating both primary and secondary control mechanisms in enhancing microgrid performance and stability. The motion trajectories follow a consistent and repetitive pattern, reflecting system stability and proper operation. No disturbances, abnormal oscillations, or sudden changes are observed in these plots, confirming the absence of faults or disruptions in system performance during this period.

Scenario 2: controller performance under FDI attack

In this scenario, the communication link between nodes 2 and 3 is subjected to an FDI attack with a frequency of 4905 Hz. This attack disrupts frequency stability and coordination among DG units. The variations in frequency and real power of the DG units and oscillator response are shown in Fig. 6. For $t < 1$ s, the system operates under droop control, where real power and frequency exhibit initial oscillations before gradually stabilizing. At $t = 1$ s, secondary control is activated, compensating for frequency deviations and restoring the frequency closer to 50 Hz while stabilizing real power. Also, the oscillator functions normally in an oscillatory state. However, at $t = 2$ s, the FDI attack induces sudden fluctuations in real power and causes the frequency to drop below 49.8 Hz. Also, the oscillator exceeds its threshold value, leading to increased oscillation amplitude and transitioning into a chaotic state. At $t = 3$ s, the proposed approach is activated, effectively mitigating oscillations and gradually restoring system stability.

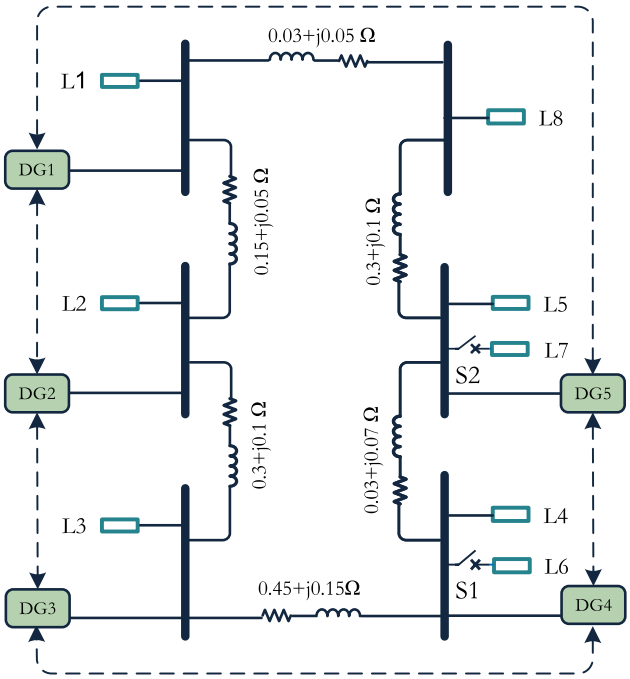

Figure 14. Study looped-type microgrid.

Scenario 3: controller performance under DoS attack

In this scenario, a DoS attack disrupts the communication link between nodes 2 and 3. The impact of this attack on the frequency and real power of the DG units is shown in Fig. 7, highlighting the effectiveness of the proposed approach in counteracting its effects. During the time interval $0 \leq t < 2$ s, both primary and secondary control techniques are in operation, maintaining the system's stability and keeping the frequency at its nominal value of 50 Hz. The system operates in a stable and fault-free condition, with the oscillator maintaining its regular oscillatory behavior. However, at $t = 2$ s, the occurrence of the DoS attack leads to a sharp frequency drop and significant oscillations in output real power, causing system instability. The system surpasses its threshold, resulting in sudden oscillations and significant disturbances in the oscillator graph. These fluctuations indicate the impact of the DoS attack on the system, causing instability and shifting its behavior from a controlled oscillatory state to a chaotic condition. Subsequently, at $t = 3$ s, the proposed approach is activated, gradually restoring frequency and power balance, thereby re-establishing system stability.

Scenario 4: controller performance under simultaneous FDI and DoS attacks

This section analyzes the simultaneous impact of an FDI attack on link 1-2 and a DoS attack on link 3-1, evaluating their effects on the microgrid's frequency and power stability. Additionally, the effectiveness of the proposed approach in enhancing system stability and mitigating the consequences of these cyberattacks is assessed. The results of this scenario are presented in Fig. 8. The system initially maintains its nominal frequency of 50 Hz. However, at $t = 2$ s, the occurrence of these attacks causes a severe frequency drop below 25 Hz, leading to microgrid instability. The FDI attack disrupts power regulation by injecting false data, thereby affecting the control system's performance, while the DoS attack severely degrades or nearly disables the communication link, disrupting coordination between control components. Despite these challenges, the proposed approach effectively enhances the system's response time and compensates for communication disturbances, successfully reducing frequency oscillations and restoring power stability. These findings highlight that cyberattacks pose a significant threat to microgrids. However, implementing the proposed approach can mitigate their impact and ensure system stability.

Scenario 5: controller performance under FDI attack in the presence of communication delay

In this scenario, the variations in frequency and output power under the influence of an FDI attack on link 1-2 and communication delays on links 2-3 and 3-2 are shown in Fig. 9. During the time interval $0 < t < 2$ s, both primary and secondary control mechanisms are active, ensuring precise regulation of frequency and output power within the nominal range and maintaining system stability. However, at $t = 2$ s, the simultaneous occurrence of an FDI attack on link 1-2 and severe disruptions on links 2-3 and 3-2 leads to the transmission of incorrect data, power imbalance, a significant frequency drop, and extensive power oscillations. At $t = 3$ s, the proposed approach is activated, effectively restoring frequency and output power to their nominal values. Ultimately, the system achieves a new equilibrium through the implementation of multi-layer controls.

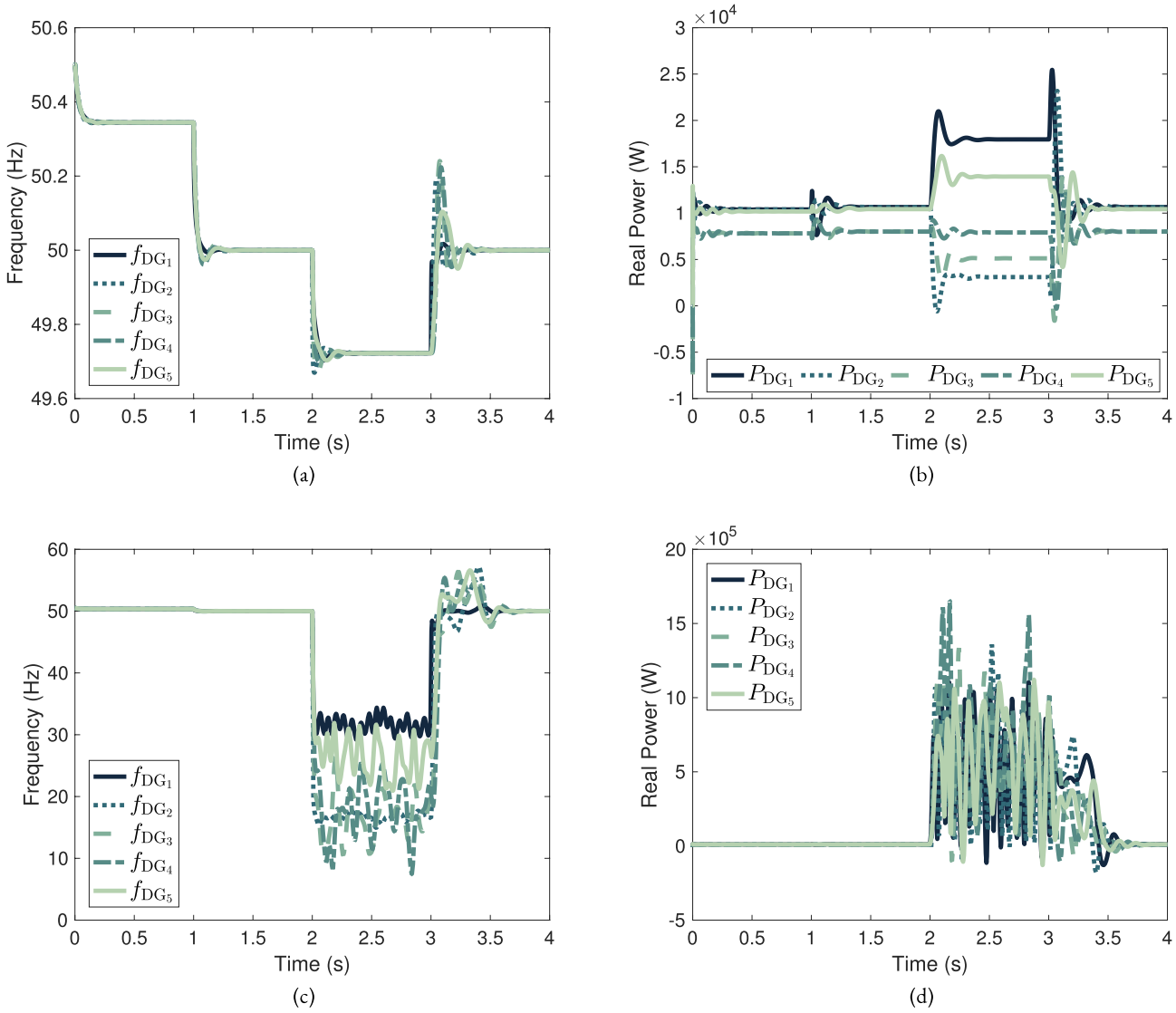

Figure 15. Performance of microgrid control equipped with the proposed approach in the study looped-type microgrid. (**a**) Frequency response under FDI attack, (**b**) Real power response under FDI attack, (**c**) Frequency response under DoS attack, and (**d**) Real power response under DoS attack.

Scenario 6: controller performance under FDI attack in the case of changing *R*/*X* Ratio

In this scenario, the resistances of microgrid lines are multiplied by 0.3 to change R/X ratio of the network lines, and the impact of an FDI attack on link 1-2 is analyzed in terms of system stability. The corresponding results, depicting frequency and output power variations, are presented in Fig. 10. Initially, droop control gradually reduces frequency and power oscillations, maintaining a relative system balance. With the activation of secondary control, the frequency stabilizes, and power fluctuations diminish. However, at $t = 2$ s, the FDI attack induces a sharp frequency drop and significant power oscillations. The proposed approach, by intervening rapidly at $t = 3$ s, successfully restores the frequency to its nominal value and stabilizes the generated power. These results highlight the effectiveness of the proposed approach in preserving network stability and mitigating the impact of cyberattacks.

Scenario 7: controller performance under DoS attack in the case of changing *R*/*X* Ratio

In the proposed framework, the impact of a DoS attack on link 1-2 is analyzed, considering a R/X ratio change by multiplying the line resistances by 0.3. The results illustrating frequency and output power variations are presented in Fig. 11. The primary and secondary control mechanisms initially maintain power balance and system stability. However, when the attack occurs at $t = 2$ s, the system experiences severe frequency fluctuations and output power instability. Upon applying the proposed approach at $t = 3$ s, oscillations are mitigated, and the system returns to its nominal state. These findings confirm that the proposed approach effectively mitigates the impact of cyberattacks and optimizes system performance.

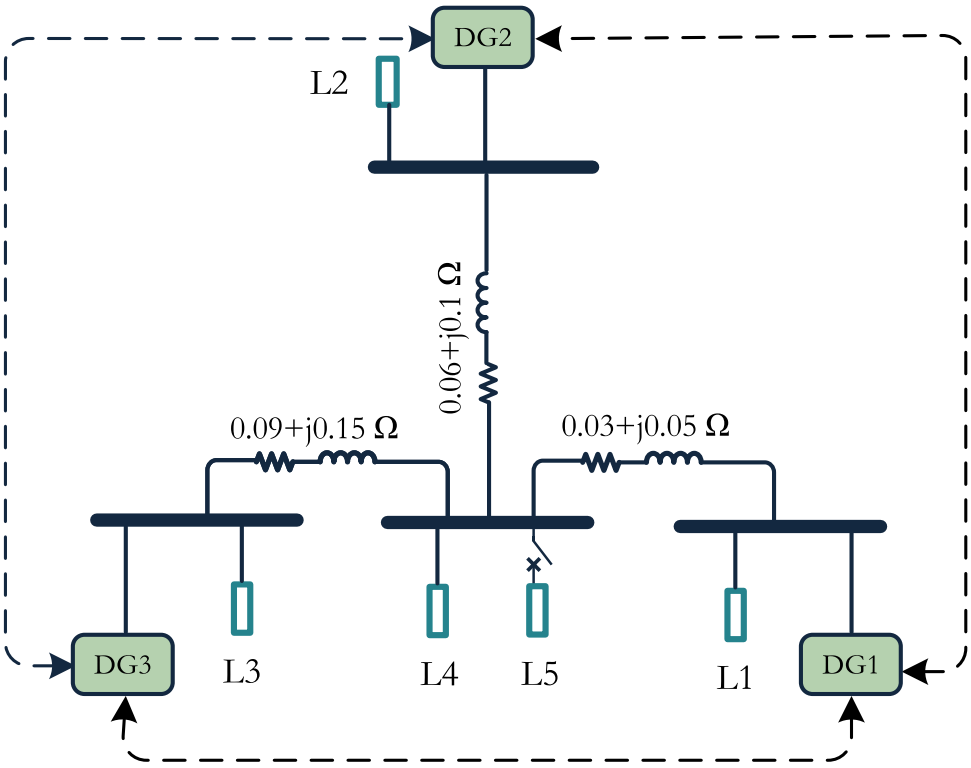

Figure 16. Study bus-type microgrid.

Scenario 8: Controller performance under cyberattacks in networked microgrids

To evaluate the proposed approach across different topologies, three single-phase microgrids have been analyzed to assess the independence of the proposed approach from network topology. The first study system is a networked microgrid, consisting of DG units and loads that can be connected to various nodes. The resistive nature of the feeder lines in this microgrid increases the coupling between real and reactive power, leading to reduced system stability. The second microgrid features a looped topology, which is suitable for systems with short transmission lines. In this configuration, the electrical distance of each inverter from the reference bus varies. The third microgrid adopts a common-bus structure, where three parallel inverters are connected to a central bus. This topology has been selected for its simplicity and high controllability.

In this section, the networked topology, shown in Fig. 12, is analyzed. In this configuration, each DG unit transfers power to connected loads via feeders. A key characteristic of this topology is the clearly defined power supply path for each load, which simplifies network management and control. The presence of multiple DG units enhances reliability, while the multiple feeders contribute to a more balanced load distribution and reduced energy losses across the network. Fig. 13 shows the variations in network frequency and power in response to FDI and DoS cyberattacks targeting link 2-1. The results indicate that under normal operating conditions, the primary and secondary control mechanisms effectively regulate network performance. However, upon the occurrence of a cyberattack, system instability emerges. By implementing the proposed approach, oscillations are mitigated, and both frequency and power are restored to their standard operating range.

Scenario 9: controller performance under cyberattacks in looped-type microgrids

The looped-type topology in microgrids enhances network flexibility, stability, and reliability by establishing bidirectional connections between DG units. In this configuration, the last DG unit is connected to the first one, forming a closed-loop structure. This design facilitates better load distribution and ensures more stable network performance under various operating conditions. The schematic representation of this topology is shown in Fig. 14. Fig. 15 presents the frequency and power variations in the looped-type microgrid when subjected to FDI and DoS cyberattacks on link 2-3. The results indicate that the system remains stable initially, with primary and secondary control mechanisms effectively maintaining frequency and power balance. However, FDI and DoS cyberattacks introduce severe oscillations and instability. By implementing the proposed approach, system equilibrium is restored, frequency and power return to nominal values, and the adverse effects of the attacks are mitigated, ensuring network stability.

Scenario 10: controller performance under cyberattacks in bus-type microgrids

The bus-type topology is shown in Fig. 16. In this structure, all generation sources and local loads are connected to a central bus. Due to its simplicity, reduced control complexity, and ease of energy management, this topology is extensively utilized in microgrids. The DG units inject their power into the common bus, while the connected

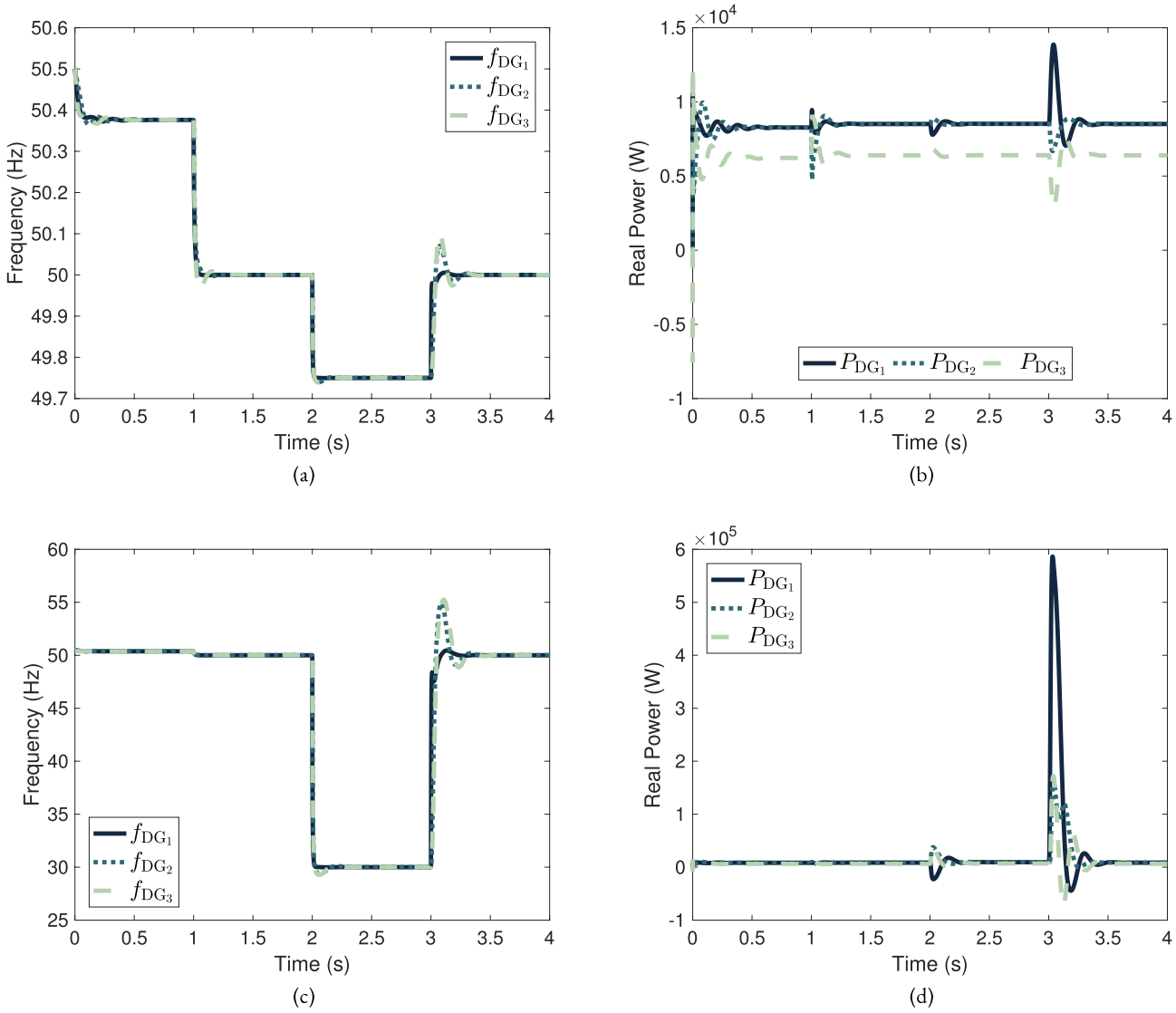

Figure 17. Performance of microgrid control equipped with the proposed approach in the study bus-type microgrid. (**a**) Frequency response under FDI attack, (**b**) Real power response under FDI attack, (**c**) Frequency response under DoS attack, and (**d**) Real power response under DoS attack.

loads draw the required energy. Fig. 17 shows the impact of FDI and DoS cyberattacks on the frequency and power of a four-bus network with three DG units. This analysis evaluates system performance under cyberattacks and the implementation of the proposed approach. The network maintains frequency stability and ensures proper power sharing through primary and secondary control mechanisms. In response to FDI and DoS attacks, which disrupt system stability, the proposed approach effectively enhances network performance and mitigates oscillations, preventing instability.

Limitations and future work

While the proposed oscillator-based detection and mitigation approach demonstrates strong performance against a range of cyber threats in islanded AC microgrids, a few limitations should be acknowledged:

- *Dependency on System Modeling* As a model-based technique, the approach relies on accurate estimation of system parameters. Inaccuracies due to measurement noise, component aging, or dynamic changes in the system configuration may affect detection reliability.
- *Communication Delay Sensitivity* Although the proposed detection mechanism itself does not introduce intrinsic delay, communication latency in the cyber layer can impact the responsiveness of control decisions. Scenario 5 explores the effect of communication delay on the control strategy's performance.
- *Model Update Complexity* Adapting the model to reflect system evolution (e.g., load variation, topology changes) may require significant computational resources, which could affect real-time performance in large-scale deployments.

- *Scalability and Resource Constraints* The decentralized nature of the approach enhances resilience, but practical implementation in microgrids with constrained hardware (e.g., limited memory or processing power in IEDs) may require optimization.
- *Multi-vector Attack Coordination* While Scenario 4 validates the system's capability to detect and respond to simultaneous FDI and DoS attacks, further evaluation under more complex, coordinated multi-vector scenarios would be beneficial.
- *Future Work* Future efforts may aim to hybridize the proposed model-based approach with lightweight data-driven techniques, thereby improving resilience under parameter uncertainty. Moreover, adaptive thresholding strategies can be developed to extend the applicability of the approach across diverse microgrid topologies and operational conditions.

Conclusion

This paper investigates the effect of cyberattacks on the secondary control level of islanded AC microgrids and proposes a cyber-resilient approach to mitigate their effects. The proposed approach is specifically designed to detect and counteract FDI and DoS attacks targeting critical communication links within the microgrid. The approach is based on an oscillator-based secondary control mechanism, which provides a dynamic and adaptive response to system disturbances caused by cyberattacks. Through extensive simulations conducted on a benchmark microgrid under various attack scenarios, the paper highlights the vulnerabilities of microgrids to such cyber threats. The simulations cover different system setups, including networked, looped-type, and bus-type topologies, to ensure the robustness and adaptability of the proposed approach under diverse operating conditions. The quantitative results show that when FDI and DoS attacks are present, the system experiences substantial frequency deviations and power oscillations, leading to network instability. Without the implementation of the proposed approach, the frequency drops below 49.8 Hz during FDI attacks and below 25 Hz when both FDI and DoS attacks occur simultaneously, severely impacting the microgrid's performance. However, when the cyber-resilient approach is applied, the system successfully restores the frequency to its nominal value of 50 Hz and stabilizes the power flow within approximately one second after activation. This study demonstrates that the integration of cyber-resilient control can significantly enhance the robustness and stability of microgrids against cyberattacks, providing a reliable solution for securing critical infrastructure in modern power systems.

Data Availability Statement

The datasets generated during and/or analyzed during the current study are available from the corresponding author on reasonable request.

Received: 1 April 2025; Accepted: 3 June 2025
Published online: 01 July 2025

References

1. Zandi, F., Fani, B., Sadeghkhani, I. & Orakzadeh, A. Adaptive complex virtual impedance control scheme for accurate reactive power sharing of inverter interfaced autonomous microgrids. *IET Gener, Transm Distrib* **12**(22), 6021–6032 (2018).
2. Pushkarna, M., Ashfaq, H., Singh, R. & Kumar, R. A new analytical method for optimal sizing and sitting of type-IV DG in an unbalanced distribution system considering power loss minimization. *J Electr Eng Technol* **17**(5), 2579–2590 (2022).
3. Pushkarna, M., Ashfaq, H., Singh, R. & Kumar, R. An optimal placement and sizing of type-IV DG with reactive power support using UPQC in an unbalanced distribution system using particle swarm optimization. *Energy Syst* **15**(1), 353–370 (2022).
4. Ahmadi, A. & Shafiee, Q. An estimation based detection method for deception cyber attack in AC microgrids, in *11th Smart Grid Conference (SGC)*, (2021).
5. Carpintero-Rentería, M., Santos-Martín, D. & Guerrero, J. M. Microgrids literature review through a layers structure. *Energies* **12**(22), 4381 (2019).
6. Shi, M., Chen, X., Shahidehpour, M., Zhou, Q. & Wen, J. Observer-based resilient integrated distributed control against cyberattacks on sensors and actuators in islanded AC microgrids. *IEEE Trans Smart Grid* **12**(3), 1953–1963 (2021).
7. Tran, Q. T. T., Luisa Di Silvestre, M., Riva Sanseverino, E., Zizzo, G. & Pham, T. N. Driven primary regulation for minimum power losses operation in islanded microgrids. *Energies* **11**(11), 2890 (2018).
8. Lu, X., Yu, X., Lai, J., Guerrero, J. M. & Zhou, H. Distributed secondary voltage and frequency control for islanded microgrids with uncertain communication links. *IEEE Trans. Ind. Inf.* **13**(2), 448–460 (2017).
9. Xu, Y., Sun, H., Gu, W., Xu, Y. & Li, Z. Optimal distributed control for secondary frequency and voltage regulation in an islanded microgrid. *IEEE Trans. Ind. Inf.* **15**(1), 225–235 (2019).
10. Keyvani-Boroujeni, B., Shahgholian, G. & Fani, B. A distributed secondary control approach for inverter-dominated microgrids with application to avoiding bifurcation-triggered instabilities. *IEEE J Emerg Sel Top Power Electron* **8**(4), 3361–3371 (2020).
11. Huang, X. et al. Distributed secondary control for islanded microgrids considering communication delays. *IEEE Access* **12**, 64 335-64 350 (2024).
12. Zhang, C. et al. Containment-based distributed cooperative control of microgrid clusters: Accurately constraining the bus states of loads and microgrids. *IEEE Trans. Power Syst.* **39**(4), 5741–5754 (2024).
13. Fakhrooeian, M. et al. An artificial insurance framework for a hydrogen-based microgrid to detect the advanced cyberattack model. *Sci. Rep.* **15**(1), 3762 (2025).
14. Pazouki, S., Naderi, E. & Asrari, A. A remedial action framework against cyberattacks targeting energy hubs integrated with distributed energy resources. *Appl. Energy* **304**, 117895 (2021).
15. Ragab, M. et al. Advanced artificial intelligence with federated learning framework for privacy-preserving cyberthreat detection in IoT-assisted sustainable smart cities. *Sci. Rep.* **15**(1), 4470 (2025).
16. Qiao, Y., Chen, D., Sun, Q. Z., Tian, G. & Wang, W. Unveiling stealthy man-in-the-middle cyber-attacks on energy performance in grid-interactive smart buildings. *Energy Convers. Manage.* **319**, 118949 (2024).
17. Rouhani, S. H., Su, C.-L., Mobayen, S., Razmjooy, N. & Elsisi, M. Cyber resilience in renewable microgrids: A review of standards, challenges, and solutions. *Energy* **309**, 133081 (2024).
18. Xie, Z. et al. Distributed control for DC microgrids with cyber attacks and constraints: A fault-tolerant model predictive controller. *Sustain Energy, Grids Netw* **39**, 101487 (2024).

19. Dibaji, S. M. et al. A systems and control perspective of CPS security. *Annu. Rev. Control.* **47**, 394–411 (2019).
20. Sánchez, H. S., Rotondo, D., Escobet, T., Puig, V. & Quevedo, J. Bibliographical review on cyber attacks from a control oriented perspective. *Annu. Rev. Control.* **48**, 103–128 (2019).
21. Bakeer, M., Bakeer, A., Magdy, G. & Aly, M. M. A new cyber-security approach for load frequency control of hybrid interconnected renewable power systems. *J. Clean. Prod.* **425**, 138866 (2023).
22. Li, Z., Shahidehpour, M. & Aminifar, F. Cybersecurity in distributed power systems. *Proc. IEEE* **105**(7), 1367–1388 (2017).
23. Sahoo, S., Mishra, S., Peng, J.C.-H. & Dragičević, T. A stealth cyber-attack detection strategy for DC microgrids. *IEEE Trans. Power Electron.* **34**(8), 8162–8174 (2019).
24. Sahoo, S., Blaabjerg, F. & Dragicevic, T. *Cyber Security for Microgrids*. Institution of Engineering and Technology, (2022).
25. Meng, W., Wang, X. & Liu, S. *Distributed control methods and cyber security issues in microgrids* (Academic Press, Cambridge, 2020).
26. Wan, Y. & Dragičević, T. Data-driven cyber-attack detection of intelligent attacks in islanded DC microgrids. *IEEE Trans. Ind. Electron.* **70**(4), 4293–4299 (2023).
27. Wang, Y. & Pal, B. C. Destabilizing attack and robust defense for inverter-based microgrids by adversarial deep reinforcement learning. *IEEE Trans Smart Grid* **14**(6), 4839–4850 (2023).
28. Zhang, H., Yue, D., Dou, C. & Hancke, G. P. Resilient optimal defensive strategy of micro-grids system via distributed deep reinforcement learning approach against FDI attack. *IEEE Trans Neural Netw Learn Syst* **35**(1), 598–608 (2024).
29. Liu, S., Liu, P. X. & Wang, X. Effects of cyber attacks on islanded microgrid frequency control, In *IEEE 20th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, 461–464, (2016).
30. James Ranjith, K. R., Kundur, D. & Sikdar, B. Transient model-based detection scheme for false data injection attacks in microgrids, in *IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, (2019).
31. Taher, M. A., Behnamfar, M., Sarwat, A. I. & Tariq, M. False data injection attack detection and mitigation using nonlinear autoregressive exogenous input-based observers in distributed control for DC microgrid. *IEEE Open J Ind Electron Soc* **5**, 441–457 (2024).
32. Chen, L. et al. Resilient active power sharing in autonomous microgrids using pinning-consensus-based distributed control. *IEEE Trans Smart Grid* **10**(6), 6802–6811 (2019).
33. Zhang, H., Meng, W., Qi, J., Wang, X. & Zheng, W. X. Distributed load sharing under false data injection attack in an inverter-based microgrid. *IEEE Trans. Ind. Electron.* **66**(2), 1543–1551 (2019).
34. Beg, O. A., Nguyen, L. V., Johnson, T. T. & Davoudi, A. Signal temporal logic-based attack detection in DC microgrids. *IEEE Trans Smart Grid* **10**(4), 3585–3595 (2019).
35. Mahmoud, M. S., Hamdan, M. M. & Baroudi, U. A. Modeling and control of cyber-physical systems subject to cyber attacks: A survey of recent advances and challenges. *Neurocomputing* **338**, 101–115 (2019).
36. Yan, H., Wang, J., Zhang, H., Shen, H. & Zhan, X. Event-based security control for stochastic networked systems subject to attacks. *IEEE Trans Syst, Man, Cybern: Syst* **50**(11), 4643–4654 (2020).
37. Yuan, Y., Yuan, H., Guo, L., Yang, H. & Sun, S. Resilient control of networked control system under DoS attacks: A unified game approach. *IEEE Trans. Ind. Inf.* **12**(5), 1786–1794 (2016).
38. Li, Y., Zhang, P., Zhang, L. & Wang, B. Active synchronous detection of deception attacks in microgrid control systems. *IEEE Trans Smart Grid* **8**(1), 373–375 (2017).
39. Lu, L.-Y., Liu, H. J., Zhu, H. & Chu, C.-C. Intrusion detection in distributed frequency control of isolated microgrids. *IEEE Trans Smart Grid* **10**(6), 6502–6515 (2019).
40. Sahoo, S., Dragičević, T. & Blaabjerg, F. Resilient operation of heterogeneous sources in cooperative DC microgrids. *IEEE Trans. Power Electron.* **35**(12), 12 601-12 605 (2020).
41. Sahoo, S., Dragičević, T. & Blaabjerg, F. Multilayer resilience paradigm against cyber attacks in DC microgrids. *IEEE Trans. Power Electron.* **36**(3), 2522–2532 (2021).
42. Karimi, A., Ahmadi, A., Shahbazi, Z., Shafiee, Q. & Bevrani, H. A resilient control method against false data injection attack in DC microgrids, In *7th International Conference on Control, Instrumentation and Automation (ICCIA)*, (2021).
43. Nasirian, V., Moayedi, S., Davoudi, A. & Lewis, F. L. Distributed cooperative control of DC microgrids. *IEEE Trans. Power Electron.* **30**(4), 2288–2303 (2015).
44. Deng, C., Wang, Y., Wen, C., Xu, Y. & Lin, P. Distributed resilient control for energy storage systems in cyber–physical microgrids. *IEEE Trans. Ind. Inf.* **17**(2), 1331–1341 (2021).
45. Xiao, J., Wang, L., Qin, Z. & Bauer, P. An adaptive cyber security scheme for AC micro-grids, in *IEEE Energy Conversion Congress and Exposition (ECCE)*, (2022).
46. Chen, P., Liu, S., Chen, B. & Yu, L. Multi-agent reinforcement learning for decentralized resilient secondary control of energy storage systems against DoS attacks. *IEEE Trans Smart Grid* **13**(3), 1739–1750 (2022).
47. Chen, X., Zhou, J., Shi, M., Chen, Y. & Wen, J. Distributed resilient control against denial of service attacks in DC microgrids with constant power load. *Renew. Sustain. Energy Rev.* **153**, 111792 (2022).
48. Bidram, A., Poudel, B., Damodaran, L., Fierro, R. & Guerrero, J. M. Resilient and cybersecure distributed control of inverter-based islanded microgrids. *IEEE Trans. Ind. Inf.* **16**(6), 3881–3894 (2020).
49. Guerrero, J. M., Vasquez, J. C., Matas, J., de Vicuna, L. G. & Castilla, M. Hierarchical control of droop-controlled AC and DC microgrids-A general approach toward standardization. *IEEE Trans. Ind. Electron.* **58**(1), 158–172 (2011).
50. Pogaku, N., Prodanovic, M. & Green, T. C. Modeling, analysis and testing of autonomous operation of an inverter-based microgrid. *IEEE Trans. Power Electron.* **22**(2), 613–625 (2007).
51. Ahmadi, S., Sadeghkhani, I., Shahgholian, G., Fani, B. & Guerrero, J. M. Protection of LVDC microgrids in grid-connected and islanded modes using bifurcation theory. *IEEE J Emerging Sel Top Power Electron* **9**(3), 2597–2604 (2021).

Additional information

Correspondence and requests for materials should be addressed to B.F.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.