

ORIGINAL RESEARCH OPEN ACCESS

Cyber-Resilient Distributed Secondary Control for Grid-Forming Inverters in AC Microgrids Using Short-Time Correlation Transform

Mohammadreza Saeidipour¹ | Bahador Fani¹ | Babak Keyvani-Boroujeni² | Iman Sadeghkhani^{3,4} 
¹Department of Electrical Engineering, Isf.C., Islamic Azad University, Isfahan, Iran | ²Department of Electrical Engineering, Bor.C., Islamic Azad University, Borojen, Iran | ³Department of Electrical Engineering, Na.C., Islamic Azad University, Najafabad, Iran | ⁴Smart Microgrid Research Center, Na.C., Islamic Azad University, Najafabad, Iran

Correspondence: Iman Sadeghkhani (sadeghkhani@iaui.ac.ir)

Received: 12 April 2025 | **Revised:** 17 February 2026 | **Accepted:** 4 March 2026

ABSTRACT

Ensuring the cybersecurity of secondary control in AC microgrids is crucial for maintaining system stability and operational resilience. Cyberattacks targeting the communication links of secondary controllers can lead to severe disruptions in frequency regulation, voltage control and power sharing mechanisms. This paper proposes a cybersecurity-resilient control strategy based on the short-time correlation transform (STCT) to enhance the robustness of distributed secondary control against cyber threats. The proposed strategy leverages the magnification properties of STCT to accurately identify compromised communication links, isolate them from the control network and reinforce the integrity of unaffected links for reliable data transmission. The STCT-based strategy is independent of attack type and location, making it highly adaptable to dynamic microgrid environments. The effectiveness of the proposed strategy is validated through extensive simulations on multiple microgrid topologies under various attack scenarios. Results demonstrate that the approach successfully mitigates cyberattacks, preserves system stability and restores microgrid frequency to its reference value with minimal delay. Furthermore, due to its lightweight computational requirements and compatibility with practical control implementations, the proposed strategy is well-suited for real-time applications. This study provides a significant advancement in microgrid cybersecurity by introducing a highly efficient, scalable and attack-agnostic protection mechanism for distributed secondary control.

1 | Introduction

1.1 | Background and Challenges

With the evolving dynamics of the global electricity market, ensuring the reliability, economic efficiency, resilience and sustainability of power distribution networks has become a critical priority for many nations. A pivotal strategy in achieving these objectives is the integration of distributed generation (DG) units into distribution systems. DG units encompass a variety of technologies, such as fuel cells, photovoltaic panels, wind

turbines and microturbines. Under normal operating conditions, consumers can sell excess electricity generated by DG units to distribution companies, whereas during grid outages, they rely on locally generated energy for their own needs—commonly referred to as islanding. The interconnection of DG units within a localized area, such as a neighbourhood, industrial park, or urban district, leads to the formation of microgrids, which play a vital role in modern energy systems. The increasing adoption of renewable energy sources has amplified the prominence of inverter-based microgrids. As microgrids incorporate renewable energy sources, power converters, energy storage devices, cyber

This is an open access article under the terms of the [Creative Commons Attribution-NonCommercial-NoDerivs](https://creativecommons.org/licenses/by-nc-nd/4.0/) License, which permits use and distribution in any medium, provided the original work is properly cited, the use is non-commercial and no modifications or adaptations are made.

© 2026 The Author(s). *IET Renewable Power Generation* published by John Wiley & Sons Ltd on behalf of The Institution of Engineering and Technology.

components and advanced communication networks, they are increasingly recognized as fundamental building blocks of smart grids [1, 2]. A hierarchical control framework is utilized to maintain the stability and reliability of microgrids, whether operating in grid-connected mode or in islanded conditions [3]. At the primary control level, local controllers regulate the real and reactive power of nearby DG units without inter-device coordination. In contrast, the secondary control level employs communication links to facilitate coordination among DGs, ensuring voltage magnitude and frequency regulation at nominal values while achieving proportional power sharing.

Based on their control and communication architectures, microgrids can be classified as either centralized or distributed [4, 5]. In centralized microgrids, a single controller aggregates system measurements and dispatches operational set points to DG units via a centralized energy management system. Although this approach offers optimized decision-making, it is highly susceptible to single points of failure, requiring high-bandwidth communication links and powerful computational resources [2, 6, 7]. Conversely, distributed control methodologies achieve operational objectives through peer-to-peer information exchange among neighbouring DGs, enhancing system flexibility and reliability [8–11]. Despite these advantages, distributed secondary control remains vulnerable to cyberattacks due to its extensive reliance on real-time data exchange [12–17]. If these vulnerabilities are not effectively addressed, they can pose severe threats to the stable operation of microgrids [18, 19]. Among the most prominent cyberattacks targeting microgrids are false data injection (FDI) [20] and denial of service (DoS) attacks [21]. These attacks, whether individually executed or in combination, can manipulate control signals, disrupt power generation, alter nominal voltage and frequency and even trigger protective relay operations—potentially leading to widespread outages. The 2015 cyberattack on Ukraine's power grid, orchestrated via spear-phishing campaigns and remote control of circuit breakers, led to a large-scale blackout affecting over 225,000 consumers. Between 2020 and 2022, cyberattacks on the power sector doubled, posing an increasing threat to energy infrastructure. In 2022, Europe suffered 48 successful cyber intrusions, underscoring the vulnerability of critical power systems [22]. Consequently, cybersecurity has become an essential cornerstone in ensuring the resilience and security of modern energy networks.

1.2 | Literature Review

Several studies have proposed different solutions to enhance cyber resilience in microgrids. Ref. [23] introduces a robust cooperative output regulation strategy for multi-agent systems (MASs), designed to withstand DoS attacks and unknown disturbances in exosystem dynamics. In [24], a robust event-triggered control strategy is introduced for DC microgrids, improving stability and system recoverability against disturbances. Ref. [25] proposes a resilient distributed control strategy to protect islanded microgrids against cyberattacks while maintaining system stability and security. Ref. [26] develops a resilient cooperative control strategy for DGs in distribution networks. Ref. [27] examines cyber-physical security challenges in smart grid infrastructures and presents protective solutions.

Previous strategies for preventing and mitigating the impact of cyberattacks on microgrids can be classified into four categories as follows [23, 28].

- i. **Prevention:** This strategy focuses on blocking cyberattacks from targeting the microgrid [24]. However, in practice, developing a universal structure capable of preventing all cyberattacks is nearly impossible, and such a system entails significant implementation and maintenance costs.
- ii. **Flexibility:** This strategy enables the microgrid to tolerate cyberattacks while maintaining normal operation [25]. Upon detecting an attack, communication link damages are categorized, and information transmission is rerouted through the least compromised channels to ensure stable system performance.
- iii. **Attack detection and isolation:** This strategy involves identifying the target of the attack, isolating the affected subsystem and efficiently restoring the system's normal behaviour [26, 28]. Controllers equipped with detection mechanisms can recognize and disconnect infected communication links upon an attack. However, well-designed attacks often evade detection, posing a significant challenge [24].
- iv. **Containment:** This strategy isolates compromised units from the system while enhancing the system's reactive flexibility. It employs a high-precision stimulus to determine the defence mechanism and reconstructs corrupted data through a secure communication channel. However, this strategy fails when all communication channels are under attack [24, 25].

Based on the discussed methodologies, previous research faces several limitations. Utilizing attack detectors introduces delays in control response, thereby slowing down controllers in suppressing attack vectors. Additionally, research on combined cyberattacks, particularly simultaneous DoS and FDI attacks, remains insufficient, leaving gaps in understanding their compounded effects on microgrid stability. Another significant challenge is that blocking attack channels disrupts system convergence, potentially leading to instability and degraded performance. Furthermore, the flexibility-based approach, while effective in mitigating cyber threats, imposes restrictions on certain compromised units, preventing them from functioning within the system and limiting overall operational resilience. These challenges highlight the need for a more adaptive and efficient cybersecurity strategy to ensure the robust protection of microgrid secondary control systems.

Several recent studies have further advanced cyber-resilient control strategies in AC microgrids and smart power systems. Distributed cooperative control has been widely adopted as a secondary control approach for frequency synchronization and voltage restoration due to its flexibility, scalability and computational efficiency. However, such systems remain vulnerable to cyberattacks, particularly FDI attacks. To address this, Chen et al. [29] propose a hidden-layer-based FDI-resilient distributed cooperative control algorithm for islanded microgrids. Similarly, the critical role of smart inverters in renewable-rich power systems has been highlighted, alongside their vulnerability to

TABLE 1 | Comparison of the proposed cybersecurity strategy with some existing approaches.

Reference	Attack type	Network type	Strategy	Advantages	Disadvantages
[18]	DoS, FDI	AC	Distributed robust control	Improved reliability	Implementation complexity
[19]	FDI	AC	Communication filtering	Reduced attack impact	Response latency
[23]	DoS	AC	Real-time network monitoring	High detection accuracy	Response latency
[24]	FDI	DC	Event-driven control	Reduced attack impact	Dependence on operational conditions
[25]	FDI	AC	Signal analysis and deep learning	High accuracy	Requires extensive training data
[26]	DoS	AC	Advanced data filtering	Optimized performance	High processing cost
[27]	DoS, FDI	AC/DC	Combining identification models	Reduced attack impact	Requires high computational resources
[34]	DoS	AC	Compensating for delays caused by DoS attacks using local dynamics	Reduced attack impact	Implementation complexity
[35]	FDI	AC & HVDC	Vulnerability analysis and impact of FDI attacks	Detecting and mitigating the effects of cyberattacks	Implementation complexity and possibility of errors in detection under noisy conditions
Proposed strategy	DoS, FDI	AC	Cyberattack detection, frequency restoration and proportional power sharing using STCT	Rapid attack detection independent of the topology, type, severity and location of the attack	Ineffective when the communication network remains disconnected for an extended period

cyber threats due to extensive information and communication technology (ICT) infrastructure; comprehensive reviews on this topic are provided in [30]. In demand response (DR) systems, deep cyber-physical coupling enhances performance but introduces risks of deception cyber-attacks, which may compromise power system stability. Yang et al. [31] develop a secure distributed control framework to mitigate deception cyber-attacks with arbitrary attack patterns. Event-triggered resilient strategies have also been explored; for example, Zhang et al. [32] propose an event-trigger-based resilient distributed energy management approach incorporating attack identification and compensation mechanisms to counter FDI and DoS attacks. Finally, distributed load frequency control (LFC) systems in microgrids are particularly sensitive to unobservable FDI attacks, and detection and defence methods have been presented to ensure frequency stability under such threats [33].

1.3 | Aims and Contributions

This paper aims to propose a flexible control strategy for AC microgrids that enhances resilience against cyberattacks. The approach is based on the short-time correlation transform (STCT), which, due to its magnification properties, effectively identifies compromised communication links, removes them from the network and strengthens the remaining secure links for reliable data transmission. Notably, this strategy is independent of the attack type and location, making it a robust solution for a wide range of cyber threats. The proposed strategy has been extensively tested on multiple common microgrid topologies under various attack scenarios, demonstrating its capability to mitigate attacks and restore microgrid frequency to its reference value. STCT is

computationally efficient, requiring minimal calculations and no complex operators, making it highly suitable for real-time implementation in practical systems. Table 1 compares the proposed strategy with some existing cyberattack mitigation strategies.

1.4 | Paper Organization

The remainder of this paper is organized as follows. Section 2 provides an overview of distributed secondary control in AC microgrids, explaining its role in frequency and voltage restoration as well as power sharing. In Section 3, various cybersecurity threats targeting the secondary control layer are discussed. The proposed cybersecurity-resilient control strategy based on STCT is introduced in Section 4, detailing its mechanism for detecting and mitigating cyberattacks in microgrid communication links. Section 5 presents simulation results to validate the effectiveness of the proposed strategy under different attack scenarios and microgrid topologies. Finally, Section 6 concludes the paper.

2 | Distributed Secondary Control

The droop control technique is the most widely adopted primary control strategy for DG units in a microgrid. Its core principle is to facilitate proportional power sharing among DG units [36]. In this approach, local controllers are positioned near DG units to adjust the output voltage magnitude and frequency, ensuring stable real and reactive power distribution among parallel-operated DG units. The control structure comprises three consecutive loops: power, voltage and current control loops.

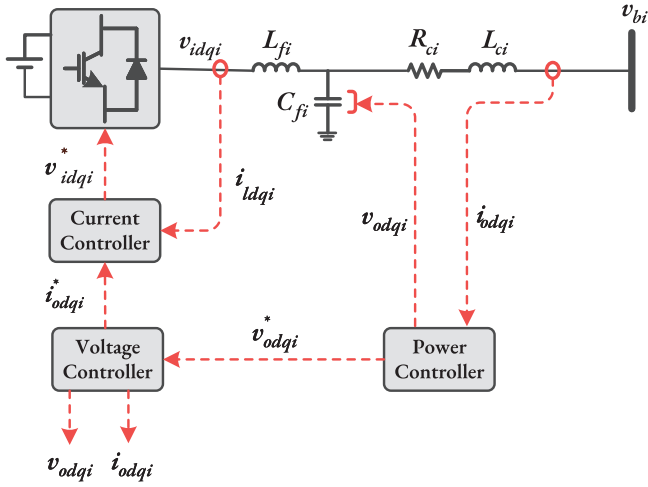


FIGURE 1 | Microgrid primary control level equipped with the droop technique.

The power controller operates based on droop coefficients. If the impedance of the microgrid is predominantly inductive, the general form of the droop control equations is given as

$$\omega = \omega_n - m_p P, \quad (1)$$

$$E = E_n - n_q Q, \quad (2)$$

where ω and E denote the reference frequency and voltage amplitude, respectively, while ω_n and E_n represent their no-load values, calculated by the secondary control level. The variables P and Q correspond to the measured real and reactive power of the DG unit and the coefficients m_p and n_q define the droop characteristics for real and reactive power, respectively.

The output frequency and voltage magnitude are adjusted in response to variations in real and reactive power, respectively, ensuring proportional power sharing among DG units within the microgrid. Figure 1 shows the control loops of a DG unit implementing droop control, comprising power, voltage and current controllers.

The application of droop control in DG units often leads to frequency deviations in the microgrid from its nominal value. To address this issue, a distributed secondary control layer is incorporated within the hierarchical control structure of islanded microgrids [28]. This secondary control mechanism adjusts the reference values in the primary control level to synchronize the frequency of DG units with the predefined nominal value. Figure 2 shows the fundamental operation of distributed secondary control in a sample microgrid consisting of four DG units. All DG units are interconnected through communication links, forming a directed graph, with at least one unit connected to the predefined reference value [6]. The communication topology between DG units depends on various factors, including the number of sources, their physical locations and associated costs, and can be either unidirectional or bidirectional. The main purpose of the secondary control layer is to correct frequency deviations, ensuring that $\omega \rightarrow \omega_{ref}$. To achieve this, an auxiliary control function u_ω is integrated into the secondary control layer, with its input for i th DG units derived from the derivative of Equation (2) as

$$\dot{\omega}_i = \dot{\omega}_{ni} - m_{pi} \dot{P}_i = u_{\omega i}. \quad (3)$$

The appropriate set point for the primary control level, ω_{ni} , is determined as

$$\omega_{ni} = \int (u_{\omega i} + m_{pi} \dot{P}_i) dt. \quad (4)$$

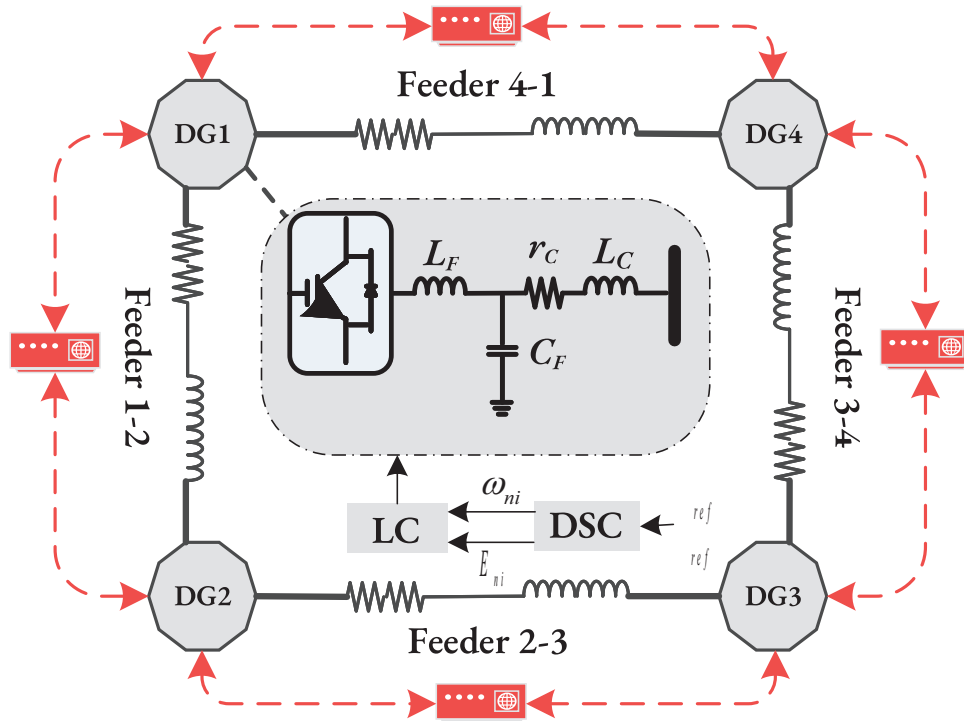


FIGURE 2 | Microgrid distributed secondary control level. DSC: distributed secondary control; LC: local controller.

The conventional secondary frequency control strategy relies on information exchange among neighbouring DG units and a reference node, following a predefined communication graph. The control update rule is expressed as [6]

$$u_{\omega i} = k_{\omega i} \left(\sum_{j=1}^N a_{ij} (\omega_j - \omega_i) + g_i (\omega_{\text{ref}} - \omega_i) \right), \quad (5)$$

where N denotes the total number of DG units in the microgrid. The adjacency matrix element a_{ij} is extracted from the communication graph, taking the value of zero if no link exists between DG units i and j , and $a_{ij} > 0$ if unit j receives information from unit i . The parameter g_i is set to one for the unit connected to the reference frequency and zero for all others. Additionally, ω_{ref} represents the system's reference frequency, while $k_{\omega i}$ is the control gain, determined based on system conditions.

Although Equation (5) enables frequency synchronization among DG units, this paper demonstrates that conventional distributed secondary control remains vulnerable to cyberattacks, particularly FDI and DoS attacks. Therefore, developing a robust control strategy to ensure reliable microgrid operation, regardless of network topology and attack type, is crucial.

3 | Cybersecurity Threats in Secondary Control of Microgrids

Although secondary control successfully restores the voltage magnitude and frequency of a microgrid to their reference values through a distributed communication network, the reliance on data transmission channels makes it vulnerable to various cyberattacks. These attacks, orchestrated by hackers, can destabilize the microgrid, necessitating robust countermeasures to ensure its resilience.

3.1 | Denial-of-Service Attack

DoS attacks, also known as service disruption attacks, flood the communication link with excessive data traffic, ultimately severing the data exchange between the sender and receiver units. This attack prevents the transmission of critical control signals within the system. In the context of a microgrid, such an attack results in the loss of connectivity between DG units, leading to fluctuations in output voltage magnitude, frequency instability and an imbalance in real power sharing among DG units. Consequently, the microgrid becomes unstable and may collapse. Figure 3 shows an example of a DoS attack disrupting the communication link between DG1 and DG2, effectively cutting off their data exchange.

3.2 | False Data Injection Attack

FDI, or false data injection attacks, are cyber threats designed to manipulate transmitted data rather than block communication. Hackers deploy phishing techniques, Trojan malware and other intrusion methods to access and alter data between the sender and receiver before forwarding the falsified information to the

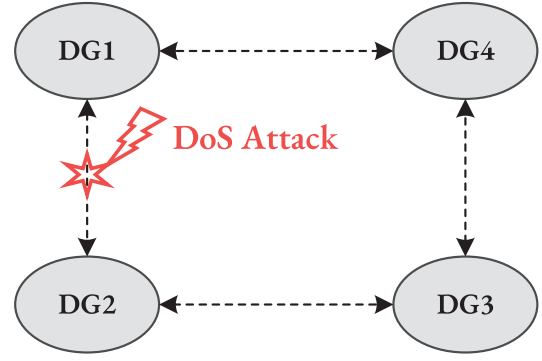


FIGURE 3 | A DoS attack on Line 1–2.

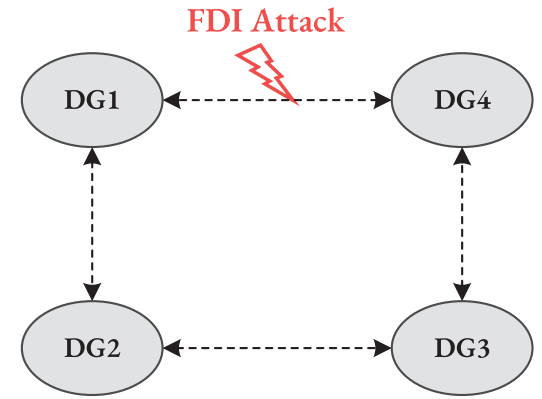


FIGURE 4 | An FDI attack on Line 1–4.

recipient. FDI is one of the most prevalent and disruptive cyberattacks in distributed control systems. By injecting erroneous data, it corrupts genuine control signals, thereby compromising system performance [26]. In microgrids, FDI leads to incorrect voltage magnitude and frequency data at the receiving DG unit. This results in an unbalanced real power distribution, causing excessive loading on certain DG units. As a result, protective relays may disconnect overloaded units, destabilizing and potentially leading to the failure of the entire microgrid. Figure 4 shows an FDI attack scenario where manipulated data is injected into the communication link between DG1 and DG4 while the data transmission remains active.

3.3 | Cyberattack Modeling

The distributed secondary control level heavily relies on frequency and power exchange among participating DG units. This dependency makes the system highly susceptible to cyberattacks. To enhance the resilience of control systems against such attacks, two primary strategies are commonly employed: (i) encrypting data transmitted over communication links [27] and (ii) implementing techniques to mitigate or eliminate the impact of cyberattacks.

To analyse their impact, first, two common types of cyberattacks are modelled and their effects on nominal frequency and power sharing within the microgrid are evaluated. Cyberattacks affecting frequency transmission between neighbouring DG units can

TABLE 2 | Identification of DoS and FDI attacks.

Attack type	Value of ξ_{aj}
Normal	0
DoS	1
FDI	$-0.1 < \xi_{aj} < +0.1, \xi_{aj} \neq 0$

be modelled as

$$\omega_{caj} = \omega_j(1 - \xi_{aj}), \quad (6)$$

where ω_{caj} represents the compromised frequency information received by the neighbouring DG unit due to a cyberattack, ω_j is the actual frequency of the j th neighbouring DG unit, and ξ_{aj} denotes the type and magnitude of the attack. The values of ξ_{aj} for different attack scenarios are provided in Table 2.

If $\xi_{aj} = 0$, no cyberattack has affected the communication link of the j th neighbouring DG unit. A value of $\xi_{aj} = 1$ indicates a DoS attack, which disrupts the communication link entirely. Unlike DoS attacks, FDI attacks are premeditated and strategically designed rather than occurring randomly [23]. To evade detection, FDI attacks maintain a controlled deviation within a limited range.

Considering the presence of cyberattacks, Equation (5) can be reformulated as

$$u_{\omega i} = k_{\omega i} \left(\sum_{j=1}^N a_{ij}(\omega_{caj} - \omega_i) + g_i(\omega_{\text{ref}} - \omega_i) \right). \quad (7)$$

4 | Proposed Methodology

In this section, a cyberattack detection and mitigation technique based on the STCT is proposed. This approach enables the suppression of cyberattacks without requiring prior knowledge of the attack's location, type or severity. The approach effectively restores the secondary control of the microgrid, ensuring its stable operation. A key advantage of STCT is its ability to amplify differences between input signals, making it an effective indicator for cyberattack detection. Due to the simplicity of STCT computations, the algorithm offers high processing speed, making it well-suited for practical applications that require fast computational performance. The correlation function measures the degree of similarity between two signals by analysing how one signal aligns with a time-shifted (k_d) version of another. This technique is extensively applied in signal processing to detect patterns and relationships within signals [37, 38].

In the proposed strategy, for two discrete-time frequency signals including the transmitted frequency between neighbouring sources $\omega_{ij}[k]$ and $\omega_{\text{ref}}[k]$, the cross-correlation function, $\Omega_{\omega}[k_d]$, is mathematically calculated as

$$\Omega_{\omega}[k_d] = \sum_{k=-\infty}^{\infty} \omega_{ij}[k] \omega_{\text{ref}}[k + k_d]. \quad (8)$$

In practical applications, signals are typically of finite duration, necessitating a modification of the summation limits as

$$\Omega_{\omega}[k_d] = \sum_{k=0}^{W-1} \omega_{ij}[k] \omega_{\text{ref}}[k + k_d], \quad (9)$$

where W represents the signal length.

STCT offers a time-frequency analysis of a signal by computing correlations within limited time intervals. This technique is particularly effective for analysing non-stationary signals with time-varying frequency characteristics. In discrete form, for two signals of length N , a window of length M and a window centre at k_0 , the STCT is computed as

$$\text{STCT}(\omega_j, \omega_{\text{ref}}) = \Omega_{\omega}[k_0, k_d] = \sum_{k=k_0-M/2}^{k_0+M/2-1} \omega_{ij}[k] \omega_{\text{ref}}[k + k_d]. \quad (10)$$

By setting $k_d = 1$, STCT simplifies as

$$[\text{STCT}[k]]_{N \times N} = \omega_{ij}[k] \omega_{\text{ref}}[k + 1] + \omega_{ij}[k] \omega_{\text{ref}}[k - 1]. \quad (11)$$

The STCT generates a matrix with dimensions equal to the adjacency matrix, where the reference frequency of the microgrid ω_{ref} is compared with the transmitted frequency between neighbouring sources ω_{ij} . If a discrepancy exists between the two frequency signals, the STCT amplifies the output frequency signal, indicating the presence of a cyberattack within the microgrid. The degree of amplification varies depending on the severity of the attack. Based on Equation (11), Equation (7) can thus be reformulated as

$$u_{\omega i} = k_{\omega i} \left(\sum_{j=1}^N \text{STCT}(\omega_j - \omega_i) + g_i(\omega_{\text{ref}} - \omega_i) \right). \quad (12)$$

The block diagram of the proposed STCT based cybersecurity strategy within the secondary control level of a microgrid is shown in Figure 5. The proposed approach utilizes incoming signals from neighbouring DG units to dynamically adjust the adjacency matrix coefficients, thereby restoring secondary control functionality. The approach is computationally lightweight and requires minimal processing time, making it highly suitable for real-time microgrid protection against cyber threats.

The proposed STCT-based mechanism does not counteract the malware directly. Instead, it isolates corrupted communication links, ensuring that the secondary control layer receives reliable frequency information. This allows the controller to maintain system frequency within allowable deviations and ride through the cyberattack. On the other hand, in this study, the consensus equations and the STCT-based detection mechanism are applied to frequency signals only. This choice reflects the increasing importance of frequency stability in low-inertia microgrids, where frequency excursions and rate of change of frequency (RoCoF) are the primary concerns. The proposed STCT-based strategy can, however, be extended to voltage-related consensus control in future work.

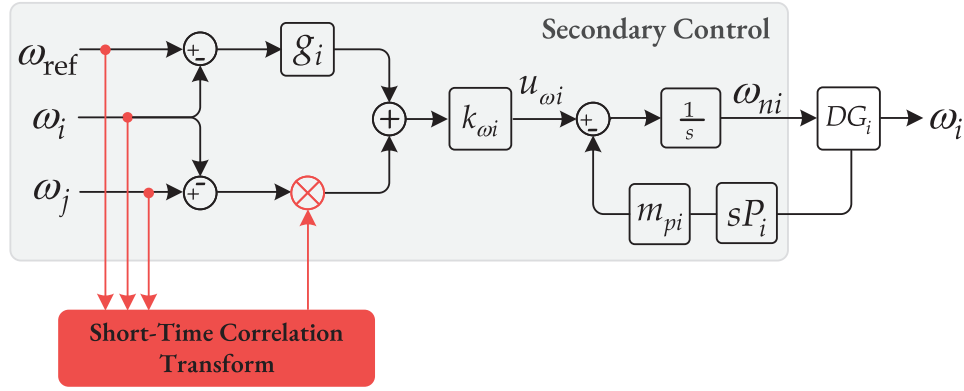


FIGURE 5 | Proposed cyberattack detection approach.

TABLE 3 | Parameters of the study microgrids.

Parameter	Value
Rated voltage	380 V
Rated frequency	50 Hz
Inverter filter	$C_f = 50\mu\text{F}$, $L_f = 1.35\text{mH}$, $R_f = 0.1\Omega$, $R_c = 0.03\Omega$, $L_c = 0.35\text{mH}$
Feeder impedance	Feeders 1–4&7: $0.23+j0.1$, Feeders 5–6: $0.44+j0.18$
Droop coefficients	$m_{p1} = m_{p2} = 9.4 \times 10^{-5}$, $m_{p3} = m_{p4} = 12.5 \times 10^{-5}$, $m_{p5} = 9.6 \times 10^{-5}$, $n_{q1} = n_{q2} = n_{q5} = 1.3 \times 10^{-3}$, $n_{q3} = n_{q4} = 1.5 \times 10^{-3}$
Load power	L1–L5: $20+j5.02$ kVA, L6&L12: $10+j2.5$ kVA, L7–L11: $40+j10.5$
Controller coefficients	$K_{pv} = 0.1$, $K_{iv} = 420$, $K_{pc} = 15$, $K_{ic} = 2 \times 10^4$
Cut-off frequency	$\omega_c = 31.4\text{rad/s}$

5 | Performance Evaluation

To evaluate the effectiveness of the proposed approach, simulations are conducted using MATLAB/Simulink environment under various topologies and attack scenarios to assess its robustness in different operating conditions. The parameters of the study systems are summarized in Table 3. The simulations analyse the impact of cyberattacks on the secondary control level and demonstrate how the STCT-based approach successfully mitigates their effects, restoring the microgrid's stability.

5.1 | Case I: Performance Assessment for Bus-Type Topology

5.1.1 | Load Switching

In this scenario, the bus-type microgrid of Figure 6 experiences a false frequency attack of 47 Hz on the communication link between DG2 and DG1. In this topology, all DG units and their nearby local loads are connected to a common bus, with one or more loads being supplied by the common bus. Figure 7a,b shows the microgrid's frequency and real power. For $t < 1$ s, the microgrid operates under primary control. At $t = 1$ s, the secondary control is activated. At $t = 2$ s, a cyberattack occurs that results in STCT increases significantly, as shown in Figure 7c. At $t = 2.5$ s, the proposed approach detects and mitigates the

attack. To further validate the effectiveness and stability of the proposed approach, at $t = 4$ s, a new load (L6) is integrated into the microgrid, and the variations in frequency and real power are observed. The proposed approach effectively maintains the stability of the microgrid under both the cyberattack and the high-power load switching event at the common bus. The nominal frequency and real power sharing are successfully restored by the secondary control level.

The study bus-type microgrid is investigated in the next scenario in the case of a DoS attack. The attack targets the communication link between DG4 and DG1, while all parameters and timing conditions remain the same as in the previous scenario. Figure 7c,d presents the microgrid control performance. At $t = 4$ s, Load 6 is connected to the microgrid. The proposed approach effectively mitigates DoS attacks in the common bus topology, maintaining system stability even after the occurrence of the attack and the integration of an additional load into the common bus.

5.1.2 | Change of R/X Ratio

In this scenario, the microgrid follows the same setup as the previous scenario, with the key difference being the variation in the R/X ratio where the line resistance is multiplied by 0.2. It changes the feeder impedance nature from resistive to inductive.

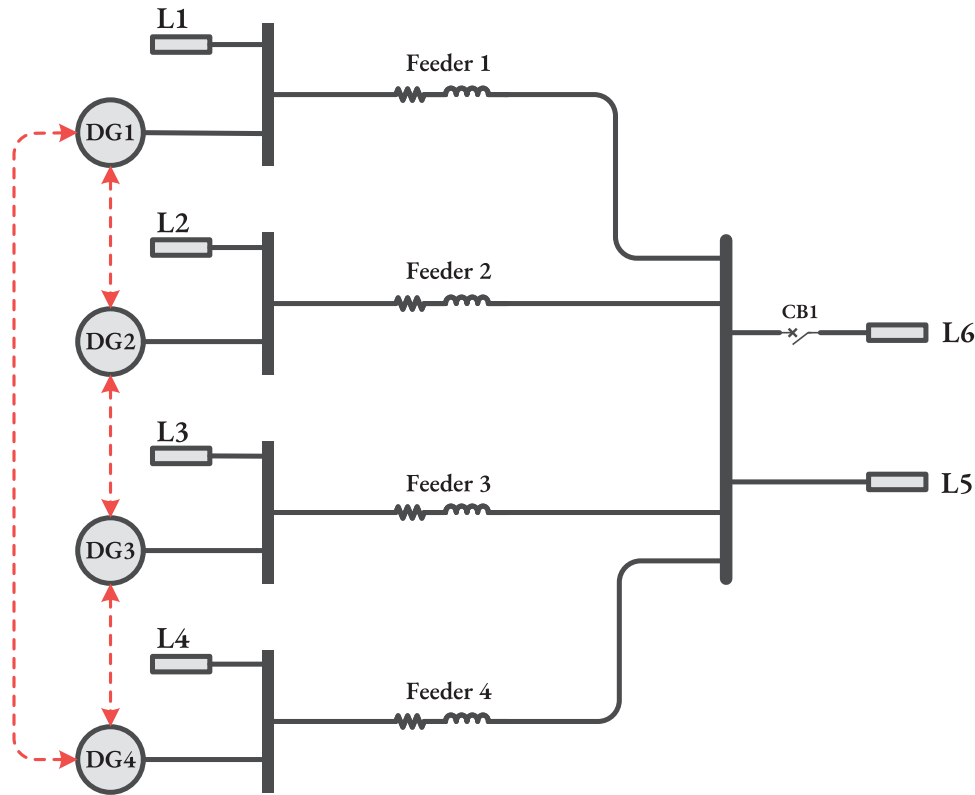


FIGURE 6 | Study bus-type microgrid.

Additionally, the cyberattack targets the communication link between DG4 and DG3. The simulation results are shown in Figure 8a,b. The proposed approach effectively preserves microgrid frequency stability and accurate real power sharing, even in the presence of impedance variations.

In the next scenario, the microgrid operates under the same conditions as the previous one, with multiplying the line resistance by 0.2, but this time subjected to a DoS attack. Figure 8c,d shows the frequency and real power of the microgrid under this condition. The DoS attack disrupts the communication link between DG4 and DG3, significantly impacting both microgrid frequency and real power. However, at $t = 2.5$ s, the proposed approach intervenes, successfully mitigating the attack and restoring the nominal values of the microgrid, demonstrating the effectiveness of the proposed strategy in this scenario.

5.1.3 | Change of Reference Bus

In this scenario, the microgrid operates under a resistive line impedance condition, where the R/X ratio is greater than one. Additionally, the secondary control reference bus is switched from Bus 1 to Bus 2. All other parameters and control timings remain unchanged compared to the previous scenario. Figure 9a,b presents the microgrid control performance under these conditions. At $t = 1$ s, the secondary control successfully synchronizes the microgrid frequency with the reference frequency, which is now connected to Bus 2. At $t = 2$ s, a cyberattack injects a false frequency of 44.5 Hz into the communication link between DG3 and DG2, disrupting system stability. However, at $t = 2.5$ s, the proposed strategy is activated, effectively

mitigating the attack. As a result, the nominal frequency and real power sharing are restored by the secondary control level, demonstrating the strong performance of the proposed strategy in this scenario.

All parameters, controller activation times and attack initiation and mitigation moments in the next scenario are identical to the previous one, with the only difference being the attack type. Instead of an FDI attack, this scenario considers a DoS attack targeting the same communication link. Figure 9c,d shows the microgrid frequency and real power sharing, respectively. The results confirm that the proposed strategy effectively mitigates the severe DoS attack, restoring the microgrid frequency to match Bus 2, which serves as the reference bus. Additionally, real power sharing among the DG units is successfully restored by the secondary control level, demonstrating the effectiveness of the proposed strategy.

5.2 | Case II: Performance Assessment for Looped-Type Topology

5.2.1 | Load Switching

In this scenario, a looped-type topology shown in Figure 10 with load switching is studied under an FDI attack. This topology is almost similar to the radial topology, with the difference that the last DG unit is connected to the first DG unit through a distribution feeder, forming a closed-loop structure. This configuration enhances network reliability, improves voltage stability and facilitates power distribution control. The reference bus is Bus 1, and a false 47 Hz frequency signal is injected into

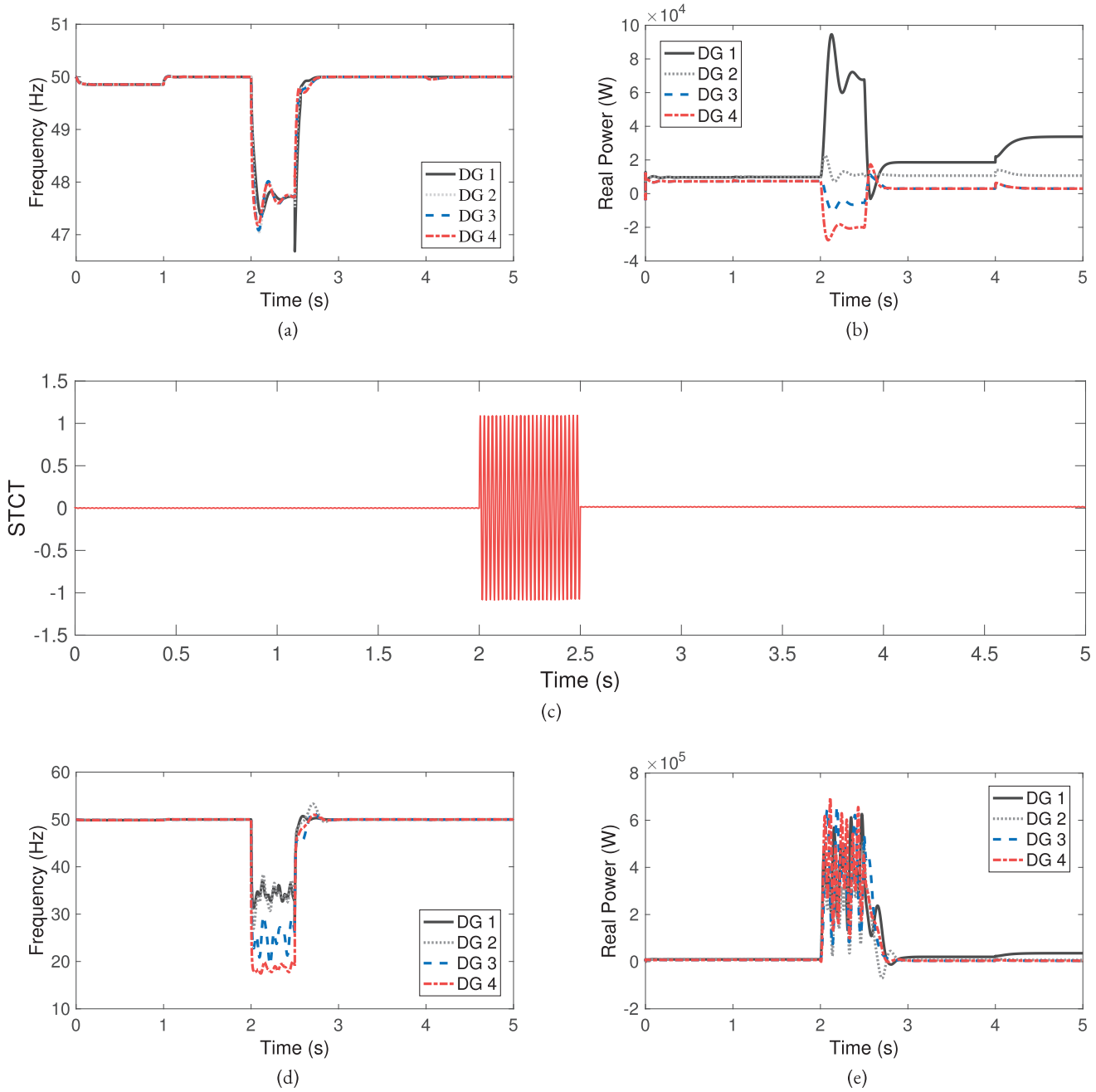


FIGURE 7 | Proposed cybersecurity strategy performance for the bus-type microgrid in the case of load switching. (a) Frequency under FDI attack, (b) real power under FDI attack, (c) STCT under FDI attack, (d) frequency under DoS attack and (e) real power under DoS attack.

the communication link between DG3 and DG4. The microgrid frequency and real power sharing are shown in Figure 11a,b. Initially, the microgrid operates under primary control ($t < 1$ s), followed by secondary control activation at $t = 1$ s. At $t = 2$ s, a cyberattack occurs, which is successfully mitigated by the proposed strategy at $t = 2.5$ s. At $t = 4$ s, load L6 is connected, and at $t = 5$ s, load L7 is switched on while L6 is disconnected. The proposed strategy not only mitigates the FDI attack but also maintains stability during load switching.

The next scenario replicates the previous one with a DoS attack instead of an FDI one. Figures 11c–e shows the simulation results under this attack. The results indicate that the proposed strategy successfully maintains microgrid stability following the attack

and during subsequent load variations, further demonstrating its robust performance.

5.2.2 | Change of R/X Ratio

In this scenario, by changing the R/X ratio of the lines, the impedance is converted from a resistive to an inductive state. To achieve this, the resistance of the lines is multiplied by 0.2, and the communication link between DG2 and DG3 is attacked. The fake frequency during the attack is 49.5 Hz. Figure 12a,b shows the simulation results. For $t < 1$ s, only the droop control is active. At $t = 1$ s, the secondary control enters the microgrid operation. At $t = 2$ s, a cyberattack occurs with a fake signal, and

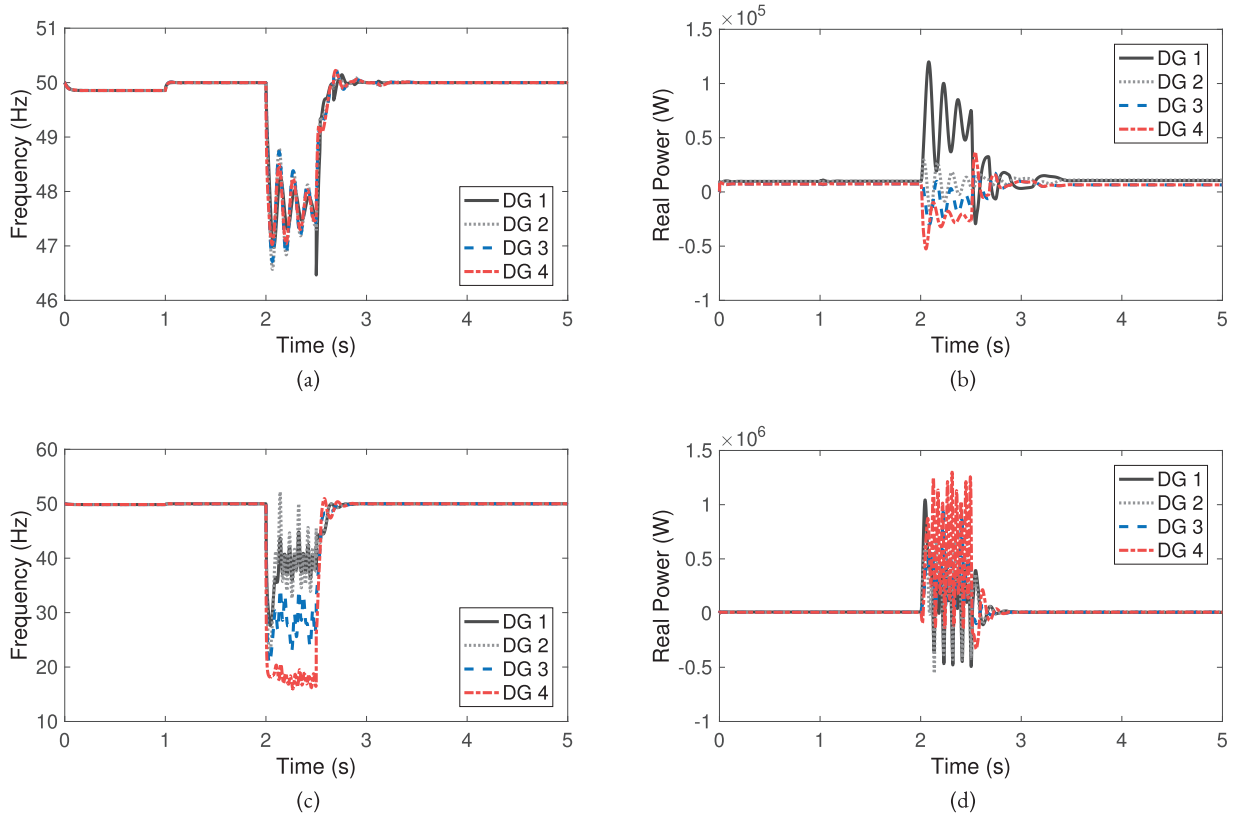


FIGURE 8 | Proposed cybersecurity strategy performance for the bus-type microgrid in the case of change of R/X ratio. (a) Frequency under FDI attack, (b) real power under FDI attack, (c) frequency under DoS attack and (d) real power under DoS attack.

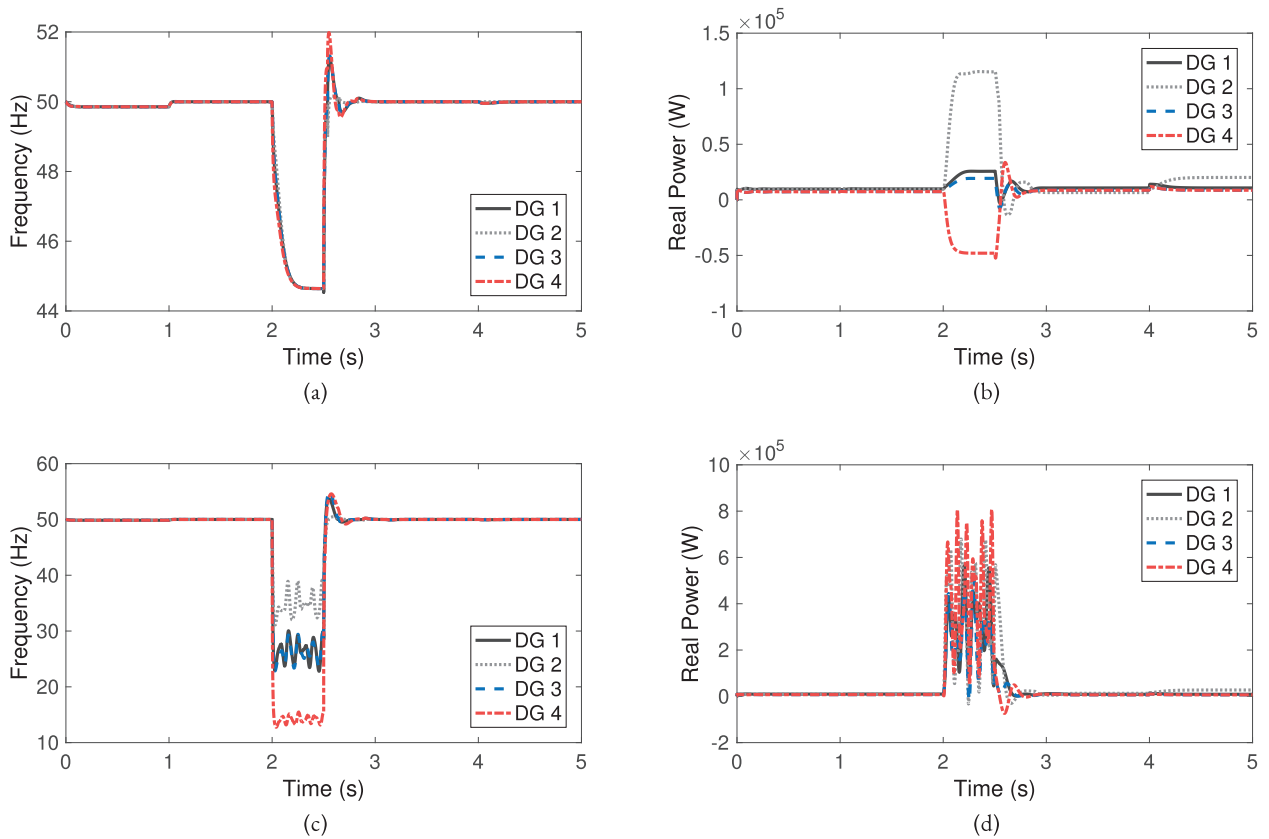


FIGURE 9 | Proposed cybersecurity strategy performance for the bus-type microgrid in the case of an FDI attack and change of reference bus. (a) Frequency under FDI attack, (b) real power under FDI attack, (c) frequency under DoS attack and (d) real power under DoS attack.

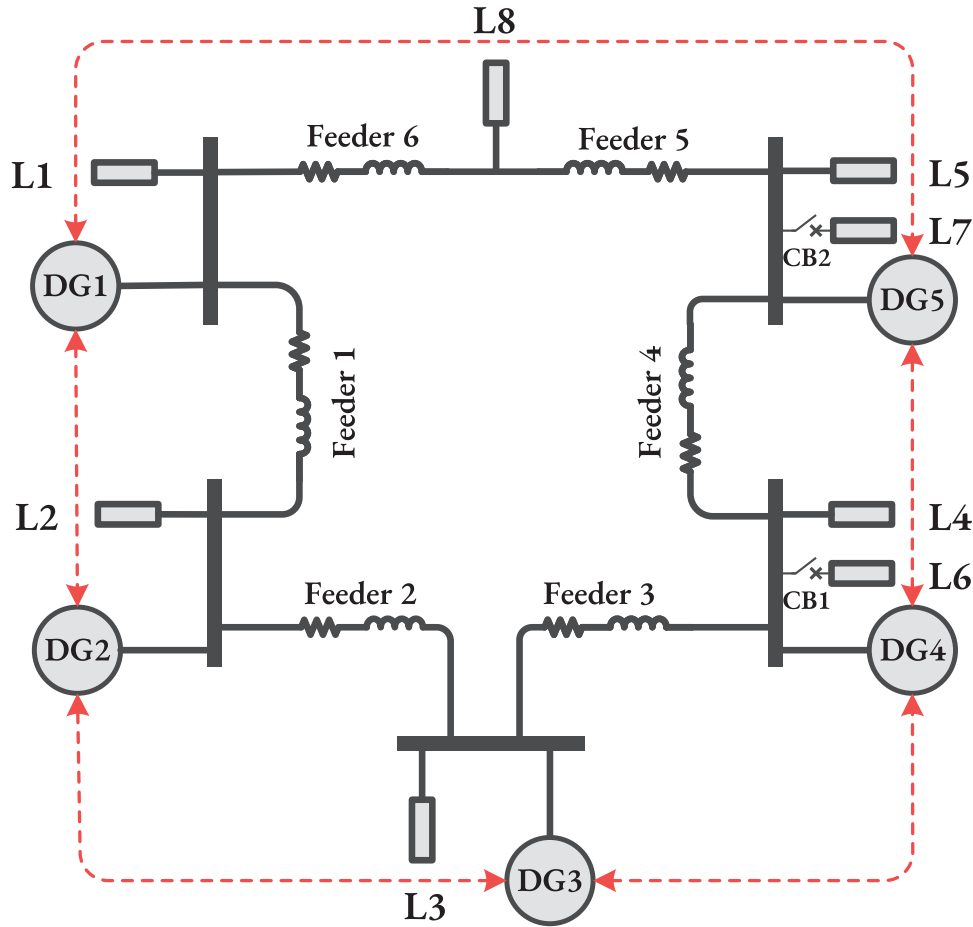


FIGURE 10 | Study looped-type microgrid.

at $t = 2.5$ s, the proposed strategy takes action and mitigates the attack. For $t < 1$ s, due to the inductive nature of the distribution lines, the primary control is unable to maintain the stability of the microgrid, causing fluctuations in frequency and real power. At $t = 1$ s, the secondary control operates and resolves this issue. At $t = 2$ s, a cyberattack occurs, disrupting the frequency of the sources and consequently the real power sharing. At $t = 3$ s, the proposed strategy restores the frequency to the reference value and properly redistributes the real power among the sources.

The only difference between the next scenario and the previous one is the type of attack. This time, a DoS attack is launched on the microgrid of the previous scenario, while all control parameters and timing remain unchanged. Figure 12c,d shows the frequency and real power of the DG units. The proposed strategy successfully mitigates the attacks in this scenario, restoring the frequency and real power of the microgrid by the secondary control level.

5.2.3 | Change of Reference Bus

In this scenario, a looped-type topology is considered with a reference bus shift from Bus 1 to Bus 4, subjected to an FDI attack injecting a false frequency of 53 Hz into the communication link between DG3 and DG4. Simulation results are shown in Figure 13a,b under primary control, secondary control, cyber-attack occurrence and the proposed mitigation strategy. Before

$t = 1$ s, the microgrid operates under primary control. At $t = 1$ s, secondary control is activated. At $t = 2$ s, the FDI attack disrupts system stability. However, at $t = 2.5$ s, the proposed strategy intervenes, successfully mitigating the attack and restoring the nominal frequency and real power sharing to the secondary control level, further validating the effectiveness of the proposed strategy in a looped-type topology with reference bus shifting.

The next scenario follows the same setup as the previous scenario, but with a DoS attack instead of an FDI attack. The DoS attack targets the communication link between DG2 and DG3. Figure 13c,d presents the microgrid frequency and real power sharing under this attack. The results confirm that the proposed strategy effectively mitigates the DoS attack while maintaining system stability in a looped-type topology with reference bus shifting.

5.3 | Case III: Performance Assessment for Meshed-Type Topology

5.3.1 | Load Switching

In this scenario, the communication link between DG1 and DG2 in a meshed topology shown in Figure 14 is attacked by an FDI attack with a fake frequency of 48 Hz. This type of topology consists of multiple buses that may or may not include DG

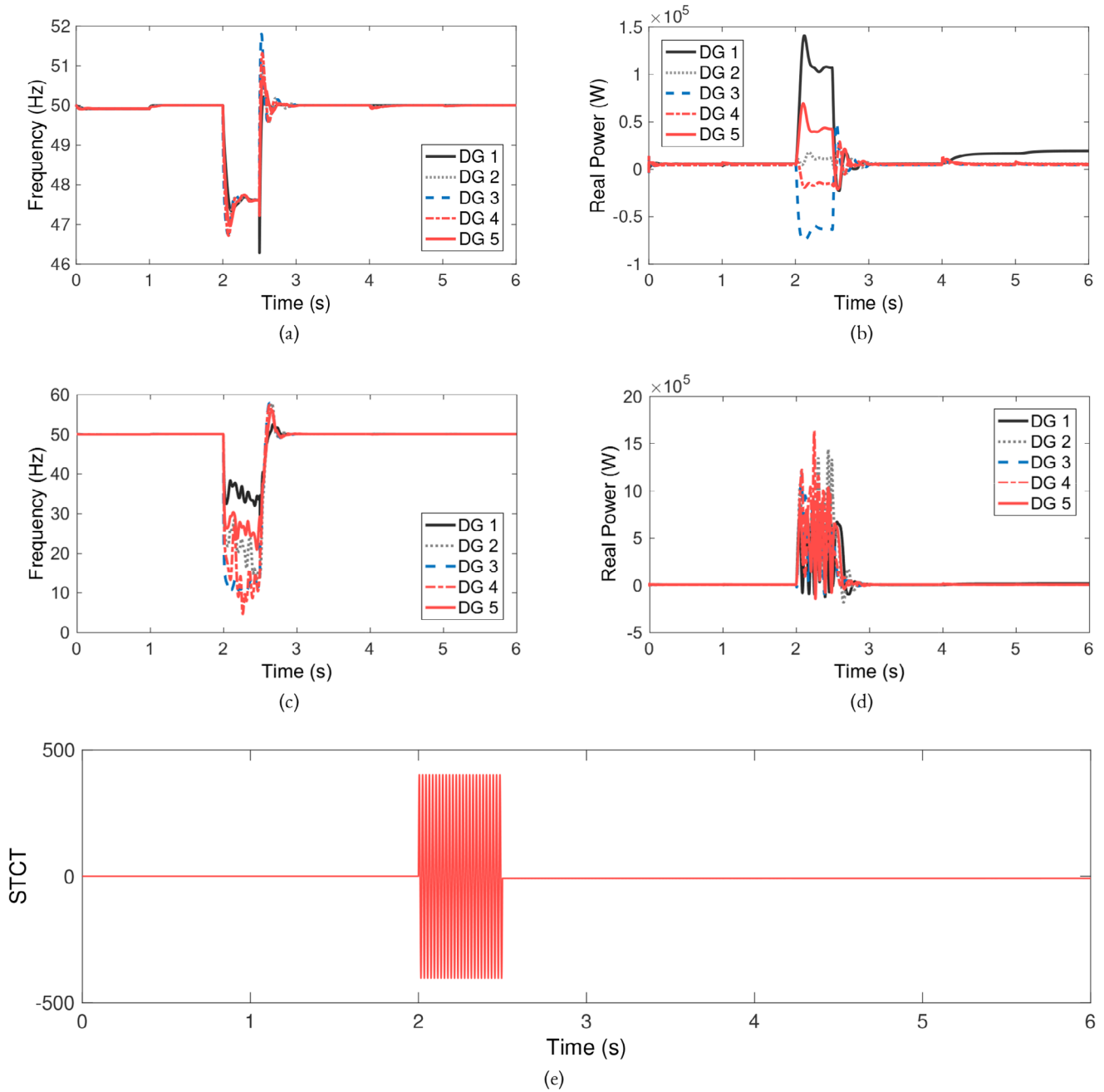


FIGURE 11 | Proposed cybersecurity strategy performance for the looped-type microgrid in the case of load switching. (a) Frequency under FDI attack, (b) real power under FDI attack, (c) frequency under DoS attack, (d) real power under DoS attack and (e) STCT under DoS attack.

units and are interconnected through distribution feeders. A series of load switching events also occur, and the stability of the microgrid is analysed under these conditions. The frequency and real power sharing as well as STCT output are shown in Figure 15a–c. For $t < 1$ s, the microgrid is controlled by primary control. At $t = 1$ s, the secondary control enters operation. At $t = 2$ s, a cyberattack occurs. At $t = 2.5$ s, the proposed strategy is activated, restoring the microgrid to the secondary control level. At $t = 4$ s, loads L2 and L9 are disconnected, while loads L7 and L11 are connected to the microgrid. The results confirm the effectiveness of the proposed strategy. It should be noted that in practice, both control layers operate simultaneously. The proposed STCT-based detection isolates compromised links in less than a quarter cycle (5 ms), preventing RoCoF relay operation and

allowing inverters to continue supplying power without a black-start.

All conditions in the next scenario are identical to the previous one, except the attack type has changed from FDI to DOS. Figure 15c,d shows the simulation results. The proposed strategy ensures accurate power sharing and effective frequency restoration.

5.3.2 | Change of R/X Ratio

In this scenario, the impedance ratio of the microgrid with a meshed topology is changed from resistive to inductive. To

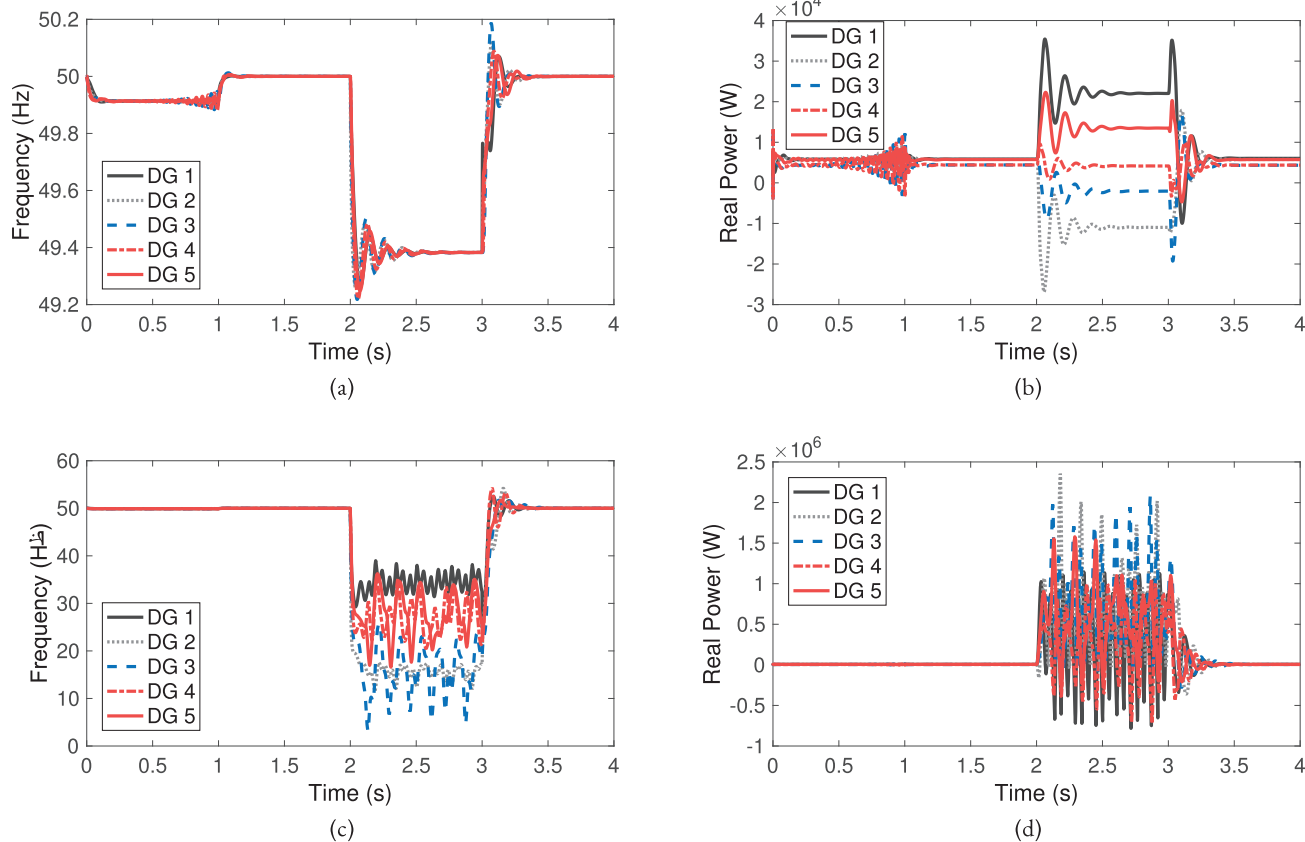


FIGURE 12 | Proposed cybersecurity strategy performance for the looped-type microgrid in the case of change of R/X ratio. (a) Frequency under FDI attack, (b) real power under FDI attack, (c) frequency under DoS attack and (d) real power under DoS attack.

achieve this, the resistance of the lines is set to 20% of its original value. The communication link between DG2 and DG3 is then subjected to an FDI attack with a fake frequency of 54 Hz, as shown in Figure 16a,b. The secondary control activates at $t = 1$ s. At $t = 2$ s, an FDI attack occurs, and at $t = 2.5$ s, the proposed strategy is activated, restoring the system to its previous state.

All conditions in the next scenario are identical to the previous one, except the type of attack is DoS. Figure 16c,d shows the performance of the proposed strategy for this scenario. It effectively mitigates this type of attack.

5.3.3 | Change of Reference Bus

In this scenario, a meshed topology is considered, with the reference bus changed from Bus 1 to Bus 5, while an FDI attack with a fake frequency of 46 Hz is launched. The results are shown in Figure 17a,b. A cyberattack occurs at $t = 2$ s, and at $t = 2.5$ s, the proposed strategy intervenes and mitigates the attack.

All conditions in the next scenario are identical to the previous one, except that the attack type is changed from FDI to DoS. Figure 17c,d shows the frequency and real power of the microgrid under this type of attack. The simulated DoS attack is properly mitigated by the proposed strategy.

5.4 | Case IV: Performance Assessment for Simultaneous Cyberattacks

In this section, the performance of the proposed strategy is evaluated for simultaneous FDI and DoS attacks. First, the microgrid operates under a bus-type topology. The communication link between DG2 and DG3 is subjected to a DoS attack, while the link between DG3 and DG4 is simultaneously compromised by an FDI attack with a falsified frequency of 49 Hz. The impact of these combined attacks on system performance is shown in Figure 18a,b. Then, a looped-type topology is considered. A DoS attack is launched on the communication link between DG3 and DG2, while an FDI attack with a forged frequency of 49.5 Hz is injected into the link between DG5 and DG1. The microgrid's frequency and real power responses under these conditions are shown in Figures 18c and 18d, respectively. Finally, the microgrid adopts a meshed-type topology. The communication link between DG3 and DG4 is targeted by a DoS attack, while an FDI attack with a forged frequency of 48.5 Hz is simultaneously applied to the link between DG4 and DG5. Figure 18e,f shows the system performance under these attacks. It can be concluded that, regardless of the microgrid topology, the combined effect of FDI and DoS attacks—primarily due to the dominant impact of the DoS attack—leads to system behaviour resembling that observed under standalone DoS conditions. However, the proposed strategy restores the frequency and share real power among DG units satisfactory.

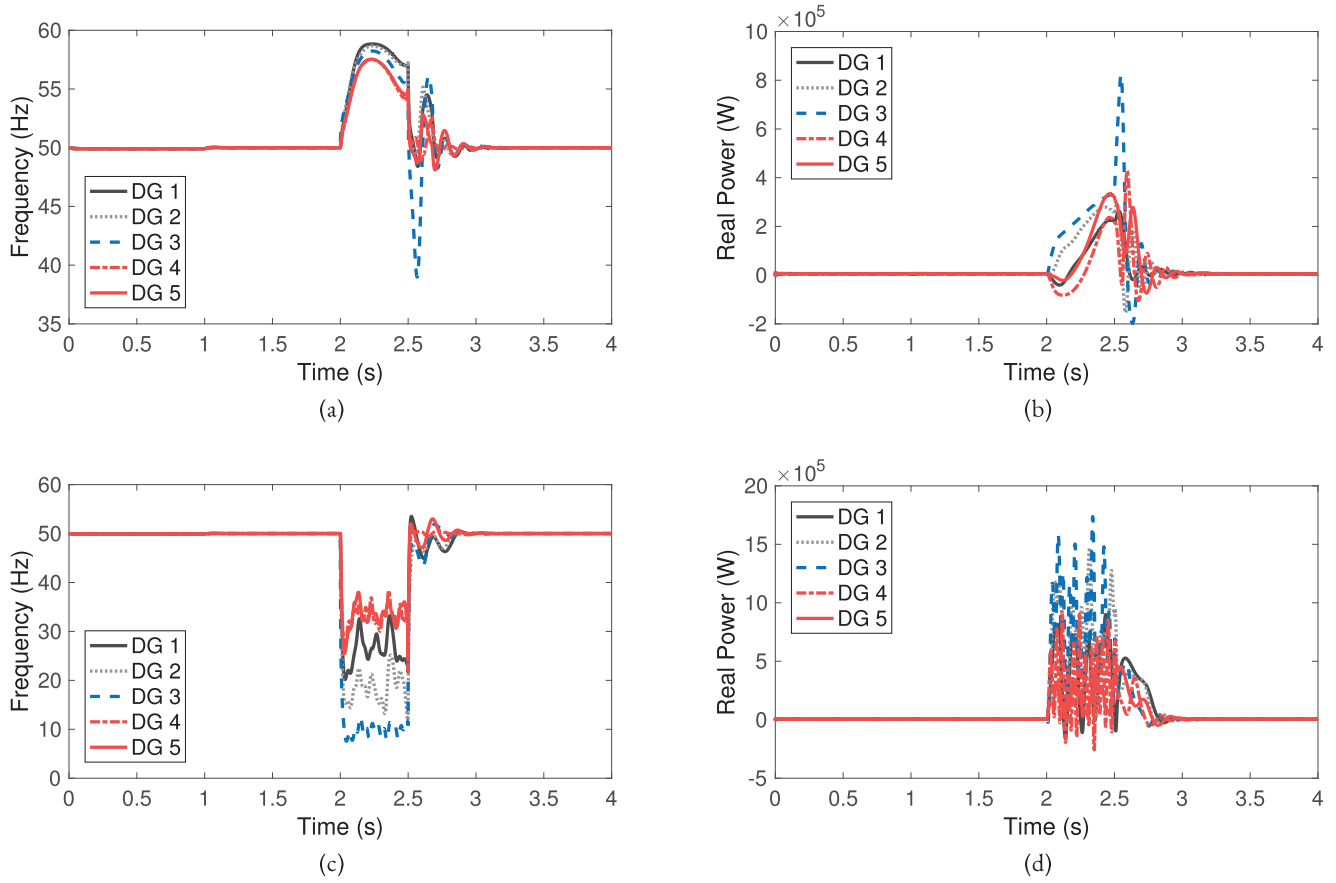


FIGURE 13 | Proposed cybersecurity strategy performance for the looped-type microgrid in the case of change of reference bus. (a) Frequency under FDI attack, (b) real power under FDI attack, (c) frequency under DoS attack and (d) real power under DoS attack.

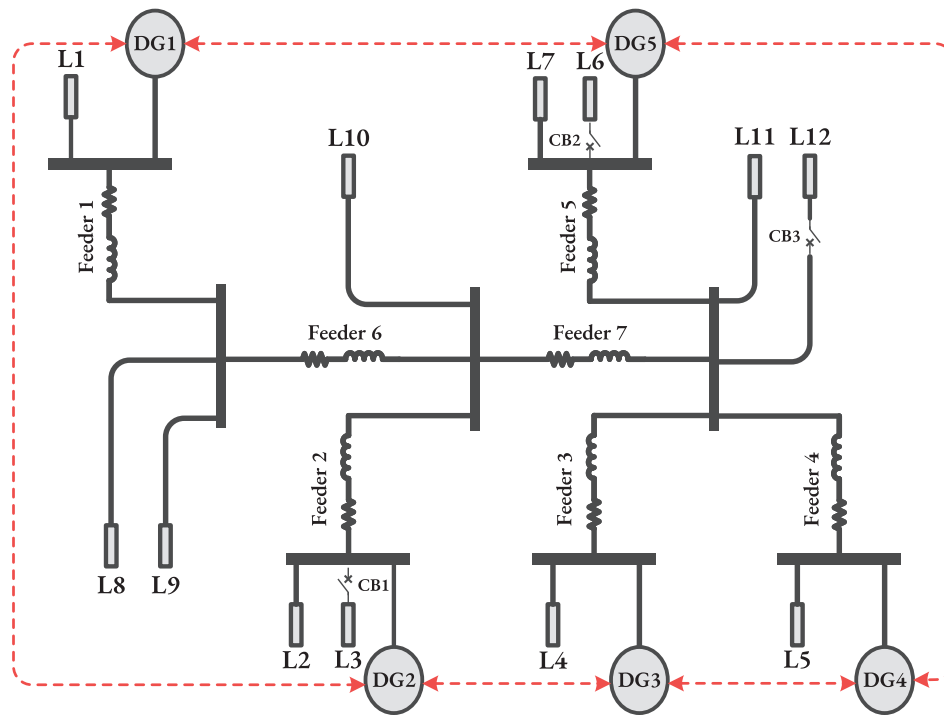


FIGURE 14 | Study meshed-type microgrid.

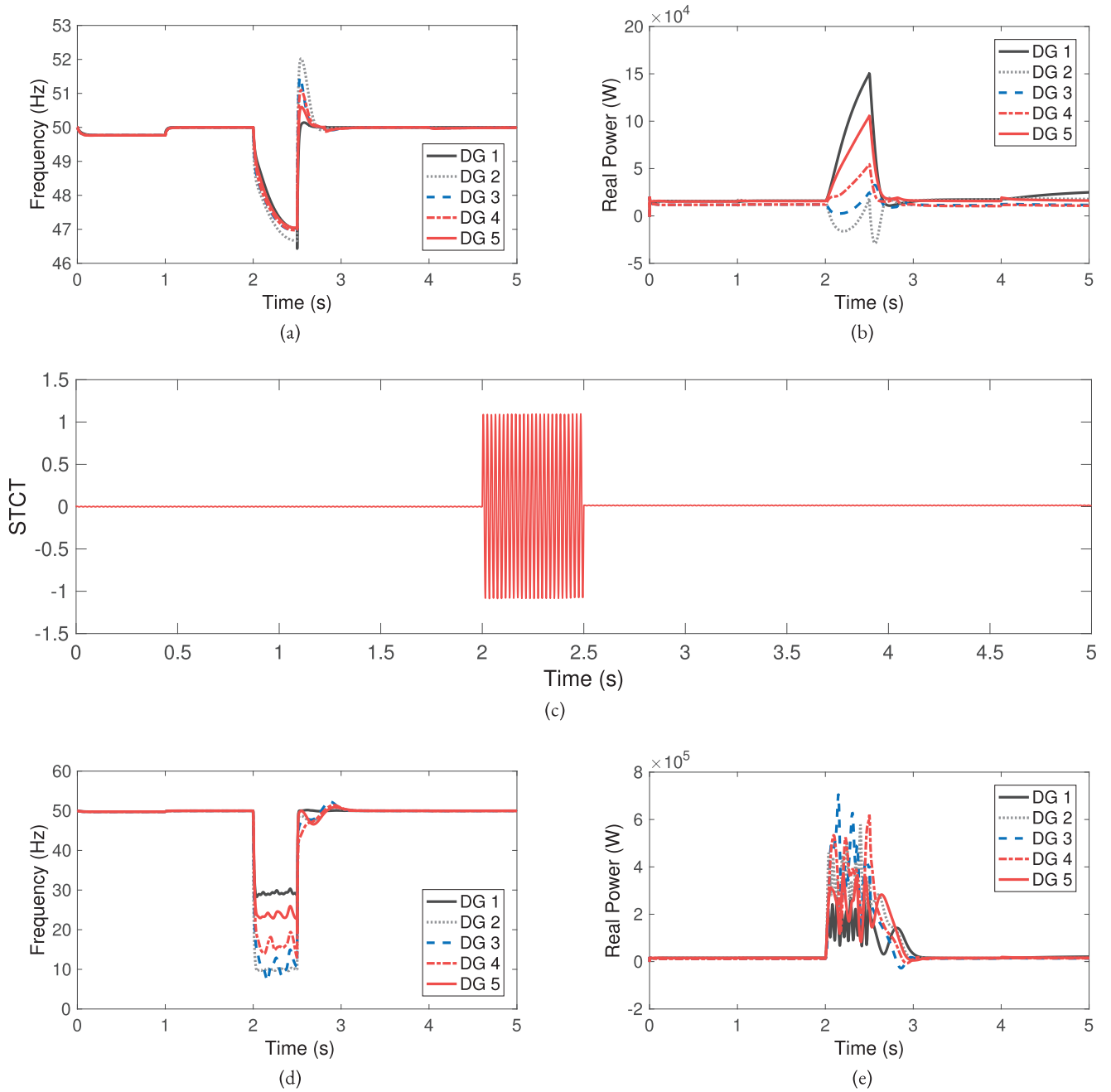


FIGURE 15 | Proposed cybersecurity strategy performance for the meshed-type microgrid in the case of load switching. (a) Frequency under FDI attack, (b) real power under FDI attack, (c) STCT under FDI attack, (d) frequency under DoS attack and (e) real power under DoS attack.

5.5 | Case V: Communication Link Delay

In this section, the performance of the proposed strategy is evaluated in the presence of communication link delay. Ideally, a communication network should transmit or receive data accurately and without delay. However, in practice, such behaviour is impossible. Time delay in data transmission is an inherent characteristic of any communication network and can affect the performance of controllers and the entire system. Time delay can particularly impact system behaviour in the initial moments of a change, such as a load variation, potentially causing instability. It is evident that time delay significantly influences the exchanged

parameter, leading to noticeable oscillations before reaching a steady state.

To determine system stability limits, the eigenvalues of the Laplacian matrix (L) must be obtained. The matrix eigenvalues (λ) are determined as

$$\det(L - \lambda I) = 0. \quad (13)$$

By finding the roots of the polynomial of this equation, the eigenvalues of the matrix can be determined. Once the eigenvalues are

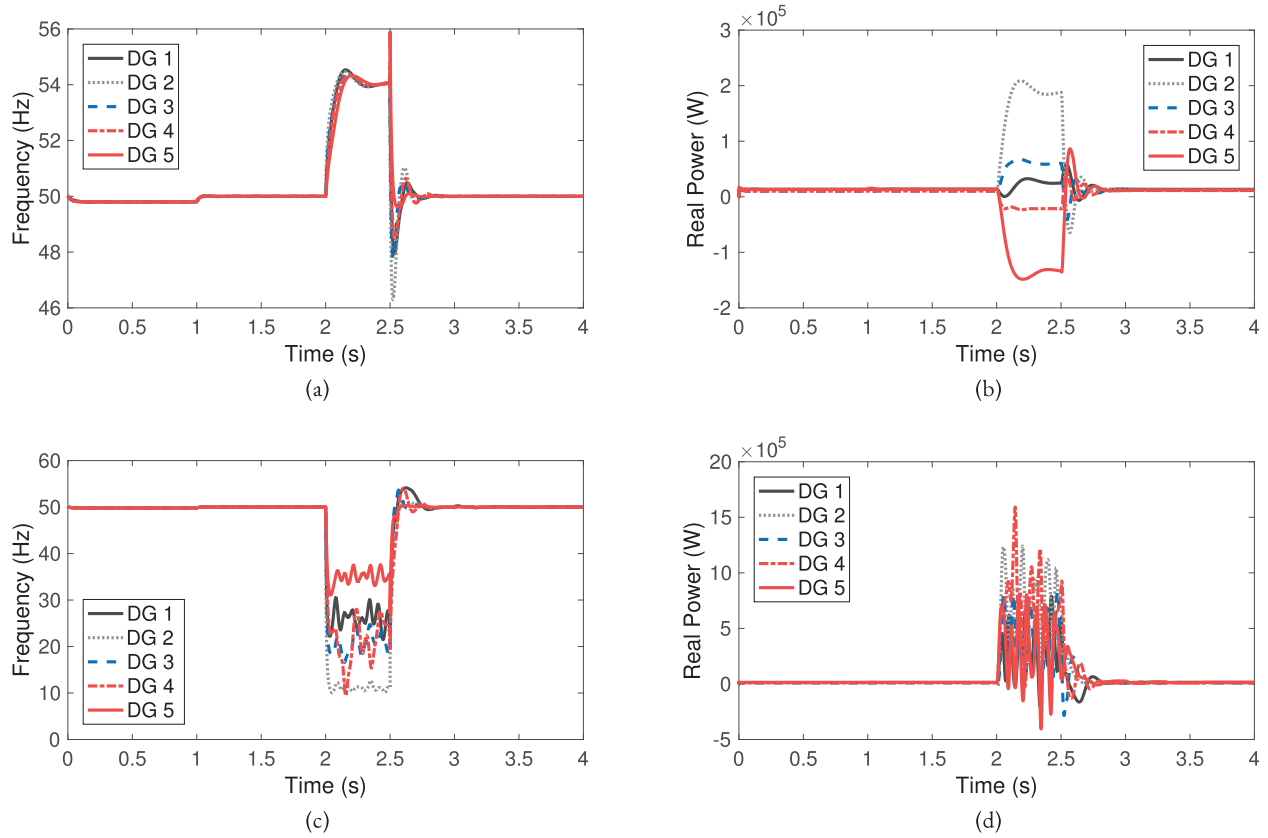


FIGURE 16 | Proposed cybersecurity strategy performance for the meshed-type microgrid in the case of change of R/X ratio. (a) Frequency under FDI attack, (b) real power under FDI attack, (c) frequency under DoS attack and (d) real power under DoS attack.

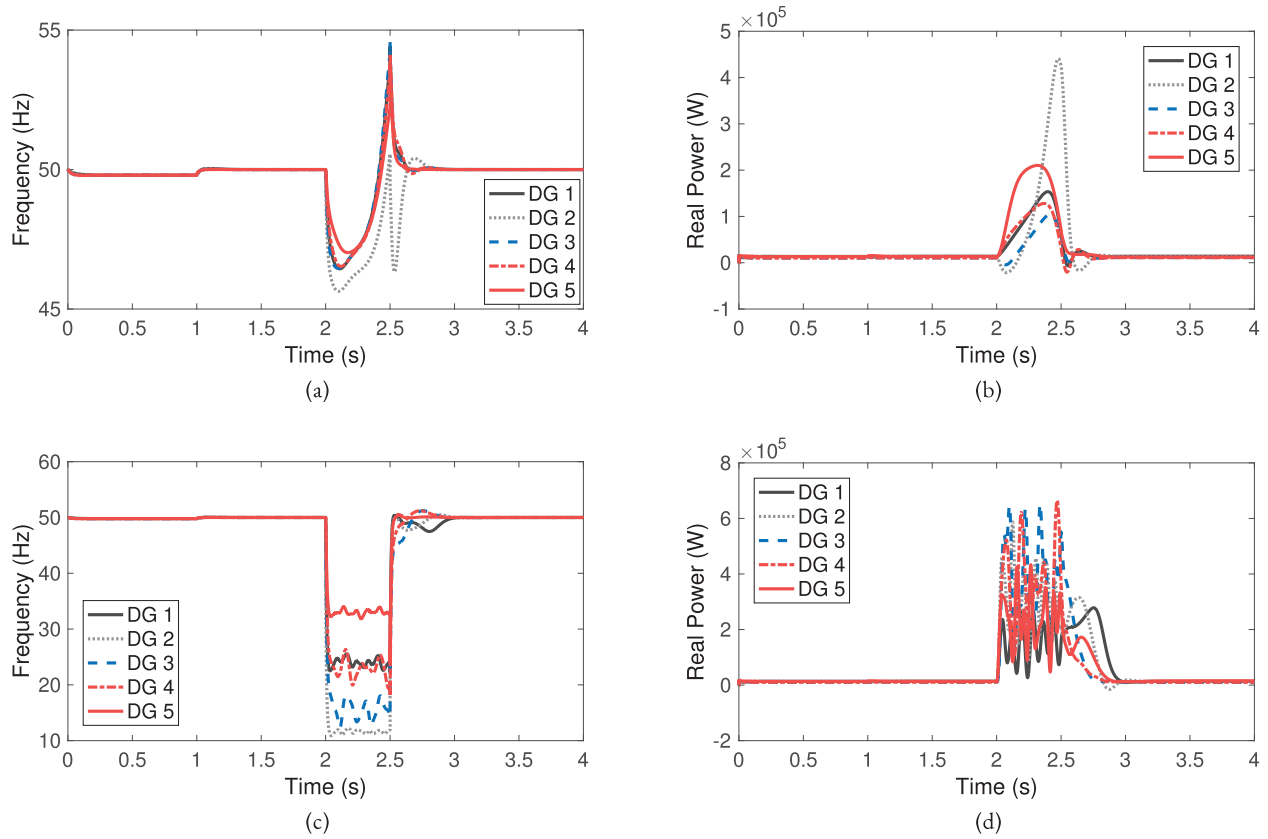


FIGURE 17 | Proposed cybersecurity strategy performance for the meshed-type microgrid in the case of change of reference bus. (a) Frequency under FDI attack, (b) real power under FDI attack, (c) frequency under DoS attack and (d) real power under DoS attack.

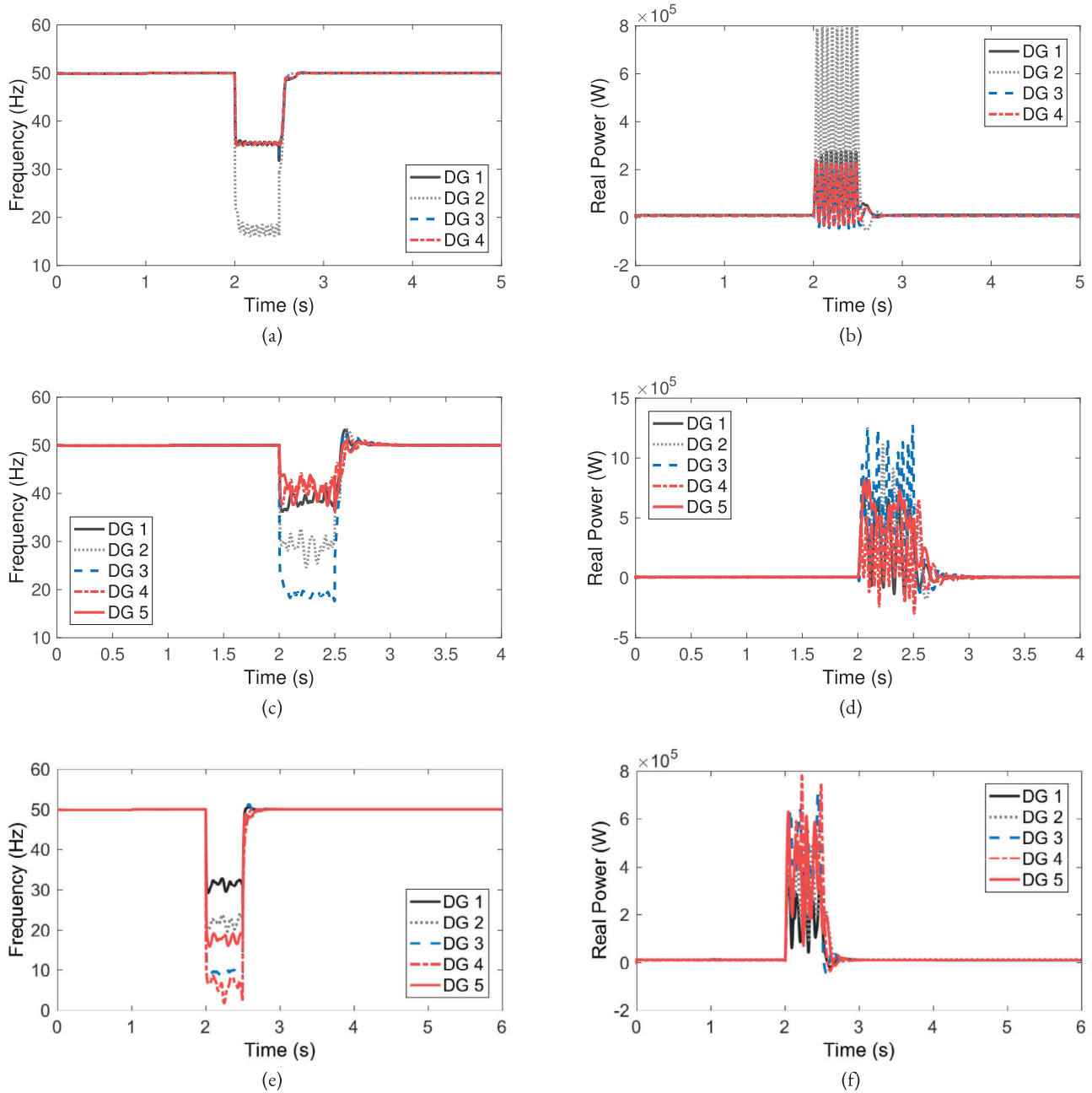


FIGURE 18 | Proposed cybersecurity strategy performance for the simultaneous cyberattacks. (a) Frequency in bus-type topology, (b) real power in bus-type topology, (c) frequency in looped-type topology, (d) real power in looped-type topology, (e) frequency in meshed-type topology and (f) real power in meshed-type topology.

obtained, the maximum allowable time delay can be computed as [39]

$$0 \leq \tau \leq \frac{\pi}{2\lambda_n}, \quad (14)$$

where τ represents the maximum time delay, and λ_n denotes the largest eigenvalue of the matrix. If the delay exceeds this value, the system becomes unstable.

In the study scenario of this section, based on Equation (13), the eigenvalues of the Laplacian matrix for a common bus

microgrid are calculated as $\lambda_1 = 0$, $\lambda_2 = 2$, $\lambda_3 = 2$ and $\lambda_4 = 4$. Using Equation (14), the maximum time delay is computed as $\tau = 392$ ms. Exceeding this value results in system instability. During $t < 1$ s, only the primary control operates. At $t = 1$ s, the secondary control is activated. To investigate the impact of communication delay on the microgrid performance, at $t = 1.5$ s, a communication delay of 500 ms—exceeding the system's maximum allowable threshold—is intentionally introduced into the microgrid links. This delay leads to instability in both frequency and real power within the system. To further evaluate the impact of cyberattacks on microgrid performance, a coordinated scenario is introduced at $t = 2$ s. Alongside the existing communication

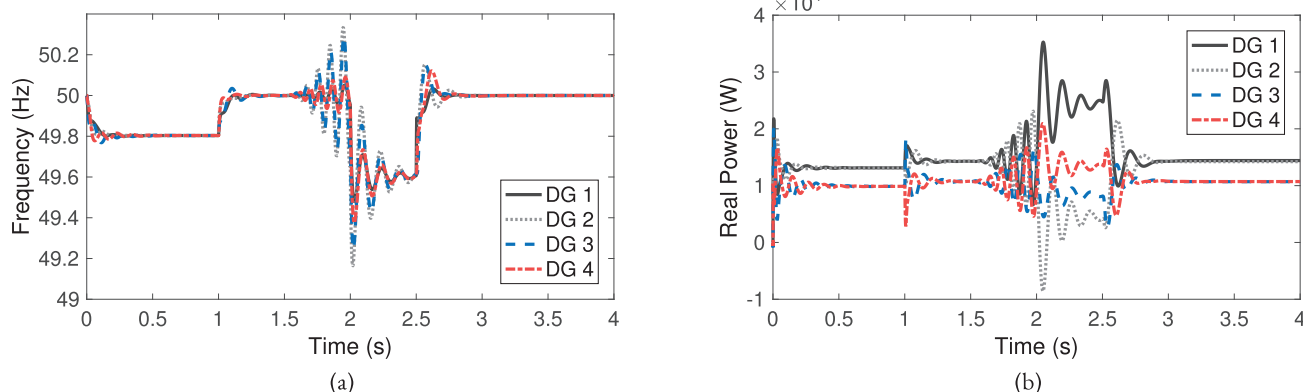


FIGURE 19 | Proposed cybersecurity strategy performance in the case of communication link delay and an FDI attack. (a) Frequency and (b) real power.

delay, an FDI attack is launched by injecting a falsified frequency signal of 49.5 Hz into the communication link between DG2 and DG3. Subsequently, at $t = 2.5$ s, the proposed strategy is activated to mitigate the attack's impact and restore system stability. Figure 19 shows the frequency and real power sharing for this scenario. The proposed strategy properly regulates the frequency and real power of the microgrid.

6 | Conclusion

This paper presented a robust cybersecurity strategy for distributed secondary control in AC microgrids, leveraging the STCT to mitigate the impact of cyberattacks on communication links. The proposed strategy effectively identifies and isolates compromised communication channels while reinforcing unaffected links to ensure reliable data transmission. The STCT-based strategy operates independently of attack characteristics, making it highly adaptable to diverse microgrid environments. Extensive simulations on bus-type, meshed-type and looped microgrid topologies under different attack scenarios verified the efficacy of the proposed strategy in preserving system stability and restoring frequency regulation with minimal deviation from reference values. Overall, this study contributes to the advancement of resilient microgrid operation by introducing a computationally efficient, attack-agnostic cybersecurity mechanism for distributed secondary control. From a technical perspective, the proposed STCT-based strategy offers several key advantages. It provides rapid and accurate detection of compromised communication links, independent of the microgrid topology, attack type, severity and location. Furthermore, the method relies on lightweight computations, making it suitable for real-time implementation. However, the approach also has limitations. The method assumes that at least part of the communication network remains functional; therefore, in scenarios where the communication layer remains fully disconnected for an extended duration, the controller cannot restore the correct consensus information. Addressing long-term communication outages is considered an important direction for future research. Additionally, future work will extend the proposed STCT-based cybersecurity mechanism to interconnected AC microgrid clusters, enabling evaluation under larger and more complex coordinated control architectures.

Author Contributions

Mohammadreza Saeidipour: investigation, software, visualization, writing – original draft. **Bahador Fani:** conceptualization, methodology, supervision, writing – original draft. **Babak Keyvani-Boroujeni:** investigation, methodology, supervision, writing – original draft. **Iman Sadeghkhani:** methodology, supervision, visualization, writing – review & editing.

Funding

The authors have nothing to report.

Conflicts of Interest

The authors declare no conflicts of interest.

Data Availability Statement

Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

References

1. L.-Y. Lu, S.-W. Lin, C.-C. Chu, and J.-H. Liu, "Generalized Deception Attack Detection of Consensus Control in Isolated AC Microgrids," in *2022 IEEE Industry Applications Society Annual Meeting (IAS)* (IEEE, 2022), 1–8.
2. J. M. Guerrero, J. C. Vasquez, J. Matas, L. G. de Vicuna, and M. Castilla, "Hierarchical Control of Droop-Controlled AC and DC Microgrids—A General Approach Toward Standardization," *IEEE Transactions on Industrial Electronics* 58, no. 1 (2011): 158–172.
3. A. Bidram, A. Davoudi, F. L. Lewis, and Z. Qu, "Secondary Control of Microgrids Based on Distributed Cooperative Control of Multi-Agent Systems," *IET Generation, Transmission & Distribution* 7, no. 8 (2013): 822–831.
4. M. Yazdani and A. Mehrizi-Sani, "Distributed Control Techniques in Microgrids," *IEEE Transactions on Smart Grid* 5, no. 6 (2014): 2901–2909.
5. Y. Han, K. Zhang, H. Li, E. A. A. Coelho, and J. M. Guerrero, "MAS-Based Distributed Coordinated Control and Optimization in Microgrid and Microgrid Clusters: A Comprehensive Overview," *IEEE Transactions on Power Electronics* 33, no. 8 (2018): 6488–6508.
6. S. Sahoo, T. Dragičević, and F. Blaabjerg, "Cyber Security in Control of Grid-Tied Power Electronic Converters—Challenges and Vulnerabilities," *IEEE Journal of Emerging and Selected Topics in Power Electronics* 9, no. 5 (2021): 5326–5340.

7. Z. Li, M. Shahidehpour, and F. Aminifar, "Cybersecurity in Distributed Power Systems," *Proceedings of the IEEE* 105, no. 7 (2017): 1367–1388.
8. J. Xiao, L. Wang, Z. Qin, and P. Bauer, "An Adaptive Cyber Security Scheme for AC Micro-Grids," in *IEEE Energy Conversion Congress and Exposition (ECCE)* (IEEE, 2022), 1–6.
9. B. Keyvani-Boroujeni, G. Shahgholian, and B. Fani, "A Distributed Secondary Control Approach for Inverter-Dominated Microgrids With Application to Avoiding Bifurcation-Triggered Instabilities," *IEEE Journal of Emerging and Selected Topics in Power Electronics* 8, no. 4 (2020): 3361–3371.
10. Q. Shafiee, J. M. Guerrero, and J. C. Vasquez, "Distributed Secondary Control for Islanded Microgrids—A Novel Approach," *IEEE Transactions on Power Electronics* 29, no. 2 (2014): 1018–1031.
11. Q. Shafiee, C. Stefanovic, T. Dragicevic, P. Popovski, J. C. Vasquez, and J. M. Guerrero, "Robust Networked Control Scheme for Distributed Secondary Control of Islanded Microgrids," *IEEE Transactions on Industrial Electronics* 61, no. 10 (2014): 5363–5374.
12. J. Choi, B. Roshanzadeh, M. Martínez-Ramón, and A. Bidram, "An Unsupervised Cyberattack Detection Scheme for AC Microgrids Using Gaussian Process Regression and One-Class Support Vector Machine Anomaly Detection," *IET Renewable Power Generation* 17, no. 8 (2023): 2113–2123.
13. S. Pazouki, E. Naderi, and A. Asrari, "A Remedial Action Framework Against Cyberattacks Targeting Energy Hubs Integrated With Distributed Energy Resources," *Applied Energy* 304 (2021): 117895.
14. Y. Qiao, D. Chen, Q. Z. Sun, G. Tian, and W. Wang, "Unveiling Stealthy Man-in-the-Middle Cyber-Attacks on Energy Performance in Grid-Interactive Smart Buildings," *Energy Conversion and Management* 319 (2024): 118949.
15. E. Naderi, S. Pazouki, and A. Asrari, "A Coordinated Cyberattack Targeting Load Centers and Renewable Distributed Energy Resources for Undervoltage/Overvoltage in the Most Vulnerable Regions of a Modern Distribution System," *Sustainable Cities and Society* 88 (2023): 104276.
16. S. H. Rouhani, C.-L. Su, S. Mobayen, N. Razmjoo, and M. Elsis, "Cyber Resilience in Renewable Microgrids: A Review of Standards, Challenges, and Solutions," *Energy* 309 (2024): 133081.
17. J. Chen, J. Yan, A. Kemmeugne, M. Kassouf, and M. Debbabi, "Cybersecurity of Distributed Energy Resource Systems in the Smart Grid: A Survey," *Applied Energy* 383 (2025): 125364.
18. C. Deng, Y. Wang, C. Wen, Y. Xu, and P. Lin, "Distributed Resilient Control for Energy Storage Systems in Cyber-Physical Microgrids," *IEEE Transactions on Industrial Informatics* 17, no. 2 (2021): 1331–1341.
19. S. Gholami and S. S. anzd Mohammad Aldeen, "Fault Tolerant Control of Electronically Coupled Distributed Energy Resources in Microgrid Systems," *International Journal of Electrical Power & Energy Systems* 95 (2018): 327–340.
20. O. A. Beg, T. T. Johnson, and A. Davoudi, "Detection of False-Data Injection Attacks in Cyber-Physical DC Microgrids," *IEEE Transactions on Industrial Informatics* 13, no. 5 (2017): 2693–2703.
21. S. Liu, Z. Hu, X. Wang, and L. Wu, "Stochastic Stability Analysis and Control of Secondary Frequency Regulation for Islanded Microgrids Under Random Denial of Service Attacks," *IEEE Transactions on Industrial Informatics* 15, no. 7 (2019): 4066–4075.
22. Eurelectric, "Cybersecurity in the Power Sector," accessed February 21, 2025, <https://www.eurelectric.org/in-detail/cybersecurity-in-the-power-sector> (2025).
23. C. Deng, D. Zhang, and G. Feng, "Resilient Practical Cooperative Output Regulation for MASs With Unknown Switching Exosystem Dynamics Under DoS Attacks," *Automatica* 139 (2022): 110172.
24. S. Sahoo, T. Dragicevic, and F. Blaabjerg, "An Event-Driven Resilient Control Strategy for DC Microgrids," *IEEE Transactions on Power Electronics* 35, no. 12 (2020): 13714–13724.
25. Q. Zhou, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, "A Cyber-Attack Resilient Distributed Control Strategy in Islanded Microgrids," *IEEE Transactions on Smart Grid* 11, no. 5 (2020): 3690–3701.
26. Y. Liu, H. Xin, Z. Qu, and D. Gan, "An Attack-Resilient Cooperative Control Strategy of Multiple Distributed Generators in Distribution Networks," *IEEE Transactions on Smart Grid* 7, no. 6 (2016): 2923–2932.
27. Y. Mo, T. H.-J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, "Cyber-Physical Security of a Smart Grid Infrastructure," *Proceedings of the IEEE* 100, no. 1 (2012): 195–209.
28. H. S. Sánchez, D. Rotondo, T. Escobet, V. Puig, and J. Quevedo, "Bibliographical Review on Cyber Attacks from a Control Oriented Perspective," *Annual Reviews in Control* 48 (2019): 103–128.
29. Y. Chen, D. Qi, H. Dong, C. Li, Z. Li, and J. Zhang, "A FDI Attack-Resilient Distributed Secondary Control Strategy for Islanded Microgrids," *IEEE Transactions on Smart Grid* 12, no. 3 (2021): 1929–1938.
30. N. D. Tuyen, N. S. Quan, V. B. Linh, V. Van Tuyen, and G. Fujita, "A Comprehensive Review of Cybersecurity in Inverter-Based Smart Power System Amid the Boom of Renewable Energy," *IEEE Access* 10 (2022): 35846–35875.
31. S. Yang, K.-W. Lao, H. Hui, and Y. Chen, "Secure Distributed Control for Demand Response in Power Systems Against Deception Cyber-Attacks With Arbitrary Patterns," *IEEE Transactions on Power Systems* 39, no. 6 (2024): 7277–7290.
32. H. Zhang, Z. Chen, C. Yu, D. Yue, X. Xie, and G. P. Hancke, "Event-Trigger-Based Resilient Distributed Energy Management Against FDI and DoS Attack of Cyber-Physical System of Smart Grid," *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 54, no. 5 (2024): 3220–3230.
33. Z. Zhang, J. Hu, J. Lu, J. Yu, J. Cao, and A. Kashkynbayev, "Detection and Defense Method Against False Data Injection Attacks for Distributed Load Frequency Control System in Microgrid," *Journal of Modern Power Systems and Clean Energy* 12, no. 3 (2024): 913–924.
34. M. D. Roig Greidanus, S. Sahoo, S. Mazumder, and F. Blaabjerg, "Novel Control Solutions for DoS Attack Delay Mitigation in Grid-Connected and Standalone Inverters," in *IEEE 12th International Symposium on Power Electronics for Distributed Generation Systems (PEDG)* (IEEE, 2021), 1–7.
35. K. Pan, E. Rakhshani, and P. Palensky, "False Data Injection Attacks on Hybrid AC/HVDC Interconnected Systems With Virtual Inertia—Vulnerability, Impact and Detection," *IEEE Access* 8 (2020): 141932–141945.
36. A. Bidram, A. Davoudi, and F. L. Lewis, "A Multiobjective Distributed Control Framework for Islanded AC Microgrids," *IEEE Transactions on Industrial Informatics* 10, no. 3 (2014): 1785–1798.
37. A. Mallahi and I. Sadeghkhani, "A Waveform Similarity Based Current-Only Differential Protection Technique for Inverter Interfaced Microgrids," *Electric Power Systems Research* 241 (2025): 111295.
38. K. Allahdadi, I. Sadeghkhani, and B. Fani, "Protection of Converter-Interfaced Microgrids Using Modified Short-Time Correlation Transform," *IEEE Systems Journal* 14, no. 4 (2020): 5172–5175.
39. R. Olfati-Saber, J. A. Fax, and R. M. Murray, "Consensus and Cooperation in Networked Multi-Agent Systems," *Proceedings of the IEEE* 95, no. 1 (2007): 215–233.