

A redundant secondary control scheme to resist FDI attacks in AC microgrids

Xueyang Wu^{1,2}, Yinghao Shan^{1,2,*}, and Xiaowu Lin^{1,2}

¹ Department of Electrical Engineering, College of Information Science and Technology, Donghua University, Shanghai, 201620, PR China

² Engineering Research Center of Digitized Textile and Apparel Technology, Ministry of Education, Donghua University, Shanghai, 201620, PR China

Received: 12 June 2024 / Accepted: 11 August 2024

Abstract. Hierarchical control of AC microgrids, despite providing stable voltage, frequency, and optimal power distribution, is susceptible to false data injection (FDI) attacks on its secondary control. Electric power systems in countries such as the United States and Venezuela have suffered cyberattacks. This paper proposes a redundant secondary control method to resist FDI attacks. This method uses distributed generators (DGs) on-line as redundant units on standby, generating dynamic corrections to the attacked DGs, thus eliminating the attack impact. It effectively addresses the numerical tampering and addition brought by FDI to the frequency and voltage setting values of the secondary control, ensuring the microgrid can still output stable frequency and voltage. The principle of this control method is direct and practical; it does not require complex controllers and can respond quickly to FDI attacks. Then, focusing on a microgrid system containing six DGs, the setting values of the microgrid system are tampered with by multiple values in different time periods, the simulation results confirm that the proposed method can effectively resist FDI attacks under various scenarios. Finally, field programmable gate array (FPGA)-in-the-loop experiments further verify the effectiveness of the proposed method.

Keywords: FDI attacks, Redundant secondary control method, AC microgrids, FPGA-in-the-loop.

1 Introduction

The electricity system is an indispensable infrastructure in social development. Microgrids, as a clean power supply system, have attracted extensive attention and research [1]. Microgrids are small power generation and distribution systems consisting of distributed generators (DGs), loads, and energy storage equipment [2, 3]. Conventional power systems appear to be increasingly inadequate to meet the needs of contemporary society in the face of increasing power demand and environmental issues [4]. Because of their distributed, flexible, and controllable characteristics, microgrids are considered an innovative solution to energy problems and have been widely studied [5, 6]. In microgrids, the integration of distributed energy, energy storage technology, and smart grid systems into local areas is conducive to better power supply [7]. Microgrids usually adopt a hierarchical control structure, and the primary control mainly realizes stable output through droop control. Secondary control is used to accomplish frequency recovery and voltage amplitude recovery [8, 9]; Power scheduling is carried

out by tertiary control for optimal operation control of the microgrid [10, 11].

However, microgrids are largely subject to cyber attacks during operations [12–15]. False data injection (FDI) attack is a common cyber attack method used by attackers, which is more flexible and oriented than other forms of attacks [16–18]. FDI attacks cause the output of microgrids to deviate from the expected value by modifying the internal parameters of the microgrids, which can cause damage to the power equipment [19]. Therefore, a series of anti-attack methods have been developed. Literature [20] proposed a resilient distributed secondary frequency control strategy for shipboard microgrids against FDI attacks. Literature [21] investigated the frequency and voltage regulation of AC microgrids under FDI attacks at the secondary control. Literature [22] proposed a network fault-tolerant resilient nonlinear frequency controller for microgrid testbed frequency regulation. A harmonic nonlinear perturbation observer is utilised for the initial identification and estimation of unknown object uncertainty and hidden FDI network attacks. Literature [23] proposed a real-time centralised monitoring scheme for detecting and mitigating FDI attacks. Literature [24] proposed a method to detect

* Corresponding author: shanyh@dhu.edu.cn

FDI attacks on microgrids using transient information. Literature [25] introduced the utilisation level of coordinated generators and evaluated their changes during FDI attacks with a particular injection strategy.

The existing literature has designed various controllers and observers to defend against FDI attacks. However, current research lacks a focus on expanding the structure of secondary control in microgrids to resist FDI attacks. From another perspective, if secondary control can correct frequency and voltage offsets caused by primary droop control, can it also correct deviations caused by FDI? Therefore, first, consider the premise that the likelihood of all DGs being attacked simultaneously is low and the redundancy characteristics of DGs within the microgrid. It is worth conducting in-depth research to determine whether the unattacked redundant DG and its secondary control can eliminate the impact of the attacked DGs. In this study, the above questions will be addressed to fully explore the defensive performance of the proposed redundant secondary control method. This control method is direct, practical, and quickly responds to FDI attacks without complex controllers. The main contributions of this study are as follows:

1. Setting a comparator at the microgrid's output, checks frequency and voltage amplitude against desired values. Anti-attack control activates when differences exceed a threshold, and deactivates when desired values are reached, ensuring normal operation and effective FDI attack resistance.
2. In a microgrid composed of six DGs, a nested secondary control structure is designed, selecting the secondary control of DG5 and DG6 as the standard. Then, in case of FDI attacks frequency on DG1-DG4, the secondary control output of either DG5 or DG6 is added to the secondary control of the attacked DG to resist FDI attacks.
3. A redundant secondary frequency controller is designed to control the secondary control of DG5 and DG6. When DG5 or DG6 is attacked by FDI, the redundant controller acts on it to resist FDI attacks. Redundant controllers are also designed for secondary voltage control to resist FDI attacks.

2 Structure of microgrids and false data injection attacks

The control structure of microgrids mainly adopts hierarchical control, and this study utilizes a hierarchical control framework with two control layers, as shown in Figure 1. The DG first passes through inverters and filters. Then the voltage and frequency are regulated by droop control in the primary control. The on-and-off time of the inverter in a period is controlled by pulse width modulation (PWM), which regulates the output of the microgrid. The secondary control first calculates the difference between the reference values of the frequency and voltage amplitude of the microgrid (*i.e.*, ω^* and E^*) and its actual output values (*i.e.*, ω and E), and then compensates the difference

between them through the proportional-integral (PI) controllers. The secondary control's output acts on the droop control ultimately modifies the PWM signal generator and adjusts the inverter of each DG unit within the microgrid to make it output the desired current and voltage.

2.1 Primary control

The primary control chiefly controls the power converter and mainly achieves a stable output of voltage and frequency. Droop control is typically used in primary control, and it simulates the principle of traditional generator primary frequency regulation. The control principle is that when the active power and reactive power of the microgrid changes the microgrid regulates the frequency and amplitude of the output voltage according to the P - ω and Q - E droop curves, and its regulation formula is as follows [26–28]:

$$\omega_i = \omega_{ri} - m_{P_i}(P_i - P_{ri}) \quad (1)$$

$$E_i = E_{ri} - n_{Q_i}(Q_i - Q_{ri}) \quad (2)$$

where ω_i and E_i represent the output frequency and voltage amplitude of DG_{*i*}, correspondingly; ω_{ri} and E_{ri} denote the rated frequency and rated voltage amplitude of the microgrid, respectively; m_{P_i} is the active droop control factor, n_{Q_i} is the reactive droop control factor; P_i and Q_i are the active and reactive power of the microgrid, respectively; P_{ri} and Q_{ri} are the rated active and rated reactive power of the microgrid, respectively.

2.2 Secondary control

The secondary control serves to correct for the drop in the frequency and amplitude of the microgrid output voltage caused by the droop control. As shown in Figure 1, the secondary controller first receives the instantaneous voltage amplitude and frequency of the output voltage through the phase-locked loop and compares the measured values with the reference values, and their deviation is corrected by the PI controllers in the secondary control. In the end, the frequency and magnitude of the microgrid output voltage are approximated to the predetermined reference values [29]. The mathematical equations are [30–32]

$$\delta\omega_i = k_{p\omega}(\omega_{ri} - \omega_i) + k_{i\omega} \int (\omega_{ri} - \omega_i) dt \quad (3)$$

$$\delta E_i = k_{pE}(E_{ri} - E_i) + k_{iE} \int (E_{ri} - E_i) dt \quad (4)$$

where $\delta\omega_i$ and δE_i represent the regulated values of the frequency and voltage amplitude of the controller's output, respectively, $k_{p\omega}$ and $k_{i\omega}$ represent the proportional and integral coefficients of the PI controller used for frequency correction within the secondary control [26]. Furthermore, k_{pE} and k_{iE} express the proportional and integral coefficients of the PI controller for voltage amplitude correction within the secondary control.

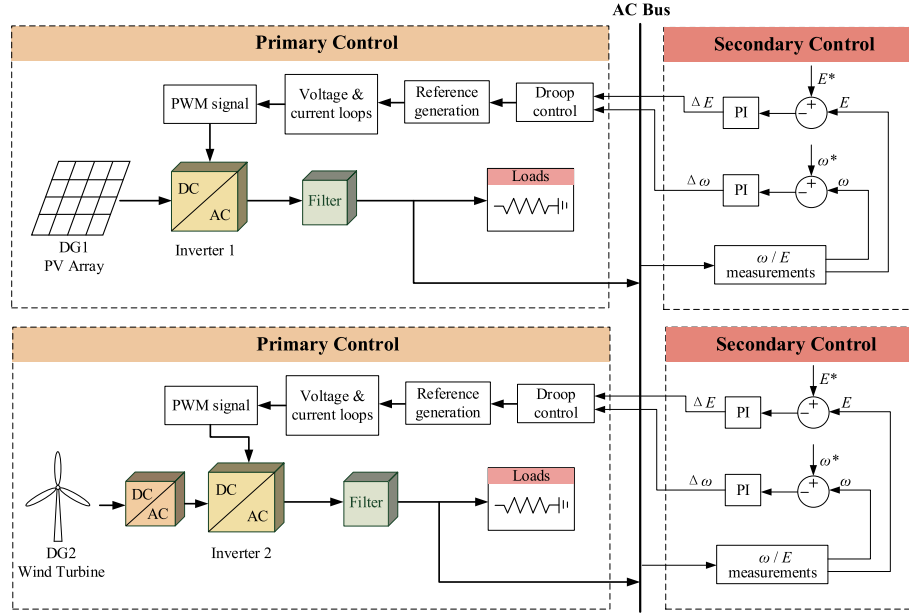


Fig. 1. Hierarchical control topology of microgrids.

2.3 False data injection attacks

In microgrids with multiple DGs, frequency stabilisation at the desired value is critical for the system when the microgrid works in an island state [33]. The secondary control can coordinate all DGs to correct voltage amplitude and frequency offsets caused by droop control only through local communication. However, security issues are also considered significant for the microgrid's secondary control. Due to the distributed dissemination of information, its control is vulnerable to FDI attacks, which cause its output to deviate from the desired value by modifying the fixed parameters set within the microgrid, which can cause damage to the electrical equipment, microgrid systems, etc. The attack on the American power grid in 2009 demonstrates how harmful cyberattacks can be to the power system.

And FDI can attack any position of the microgrid. Due to the secondary control being located in the outer loop of the entire control system, as soon as the microgrid's secondary control is attacked, the main circuit and the droop control within the system will be affected. In addition, the secondary control system sets some important reference values, resulting in vulnerabilities and insufficient safety measures in the traditional secondary control. Moreover, secondary control is a critical part of the microgrid control system, which can affect the overall operation of the whole microgrid or even lead to the collapse of the microgrid system once it is attacked. As shown in Figure 2, when FDI attacks the frequency of the secondary control, the frequency set value 50 is modified or increase the amount of attack is based on 50, which will result in the frequency of the microgrid's output voltage close to the modified value, which will have an impact on the system's loads and stability.

The same is valid for voltage attacks in secondary control, FDI attacks tamper with the voltage reference

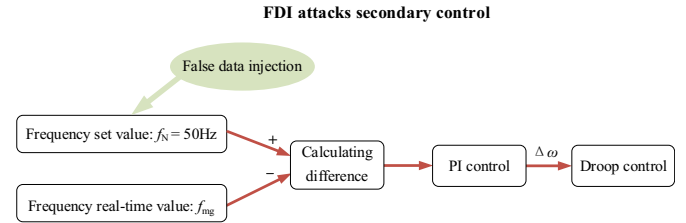


Fig. 2. Schematic of secondary control attacked by FDI.

value and in turn, play havoc with the output of the microgrid. The equations regarding the FDI attacks on frequency and voltage magnitude are as follows:

$$\omega_i^a = \omega_i + a_{\omega i} \quad (5)$$

$$E_i^a = E_i + a_{E i} \quad (6)$$

where ω_i^a and E_i^a are the frequency and voltage amplitude of the inputs to the controllers under FDI attacks, $a_{\omega i}$ and $a_{E i}$ are the FDI attacks on the i th DG controller, which are assumed to be constant in this research.

3 Redundant secondary control to resist FDI attacks

As mentioned before, while many defences against FDI attacks focus on controllers and observers, this study explores redundant secondary control in microgrids. We investigate whether secondary control, which corrects frequency and voltage deviations, can mitigate FDI-induced deviations. Assuming that redundancy prevents simultaneous attacks on all DGs, we examine whether unattacked

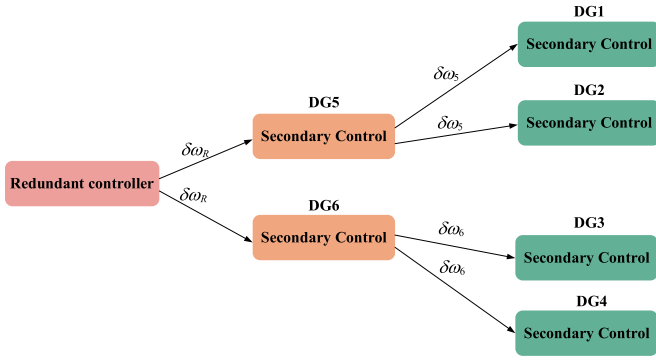


Fig. 3. The proposed redundant secondary control method.

DGs can lessen the impact of those that were attacked. In the following section, a practical solution that quickly responds to FDI attacks without relying on complex controllers will be detailed.

The secondary control structure designed in this study is shown in [Figure 3](#), where DG5 and DG6 are selected as the reference object, and the secondary frequency control of this reference DG then controls the secondary frequency control of other DGs, *i.e.*, the adjusted value of the output of the secondary frequency control of this DG will be applied to the secondary control of other DGs. The secondary control of each DG then outputs the regulation value to control the primary control.

However, the secondary control selected as the standard cannot act on other DGs at all times to avoid control disruption. To this end, a conditional function is designed to first compare the difference between the output value and the desired value of the frequency within each DG. When the difference exceeds the threshold value of 0.1 Hz, the secondary control output of the standard DG is activated. The expression of the designed function is as follows:

$$\delta\omega_{\text{FDI}i} = \begin{cases} \delta\omega, & \text{when } (\omega_i - \omega_{\text{ref}}) \in (-\infty, 0.1) \cup (0.1, +\infty) \\ 0 & \text{when } (\omega_i - \omega_{\text{ref}}) \in [-0.1, 0.1] \end{cases} \quad (7)$$

where $\delta\omega_{\text{FDI}i}$ is the output regulation of the secondary control of the reference DG (*i.e.*, DG5 and DG6 in [Fig. 3](#)).

However, when the DG selected as the reference object in the above mechanism is attacked, its control structure cannot resist FDI attacks, which will cause the frequency of the microgrid system to be disturbed and deviate from the desired value. For this reason, a redundant controller is designed, which outputs the regulation to resist the FDI attacks when the secondary control is DG5 or DG6. Similarly, the model of (7) is also equipped inside the DG5 and DG6. In this way, when the redundant controller is attacked, it will not affect other DGs.

From the above structure and principle, we can obtain the following expression for the secondary frequency control of other DGs under this secondary control method:

$$\delta\omega_i^* = k_{p\omega}(\omega_{ri} - \omega_i) + k_{i\omega} \int (\omega_{ri} - \omega_i) dt + \delta\omega_r \quad (8)$$

where $\delta\omega_i^*$ is the regulation value of the output of the secondary controllers in each DG when the redundant controller is triggered, $\delta\omega_r$ is the regulated value of the output of the redundant secondary frequency controller.

Different from the control method of resisting FDI frequency attacks, the principle of resisting FDI attacks in voltage is to set a redundant controller for the secondary voltage control of each DG. Following the same concept, if a DG secondary voltage control is identified as being attacked, the redundant controllers will activate to counter the FDI attack.

$$\delta E_{\text{FDI}i} = \begin{cases} \delta E, & \text{when } (E_i - E_{\text{ref}}) \in (-\infty, 0.2) \cup (0.2, +\infty) \\ 0 & \text{when } (E_i - E_{\text{ref}}) \in [-0.2, 0.2] \end{cases} \quad (9)$$

where $\delta E_{\text{FDI}i}$ is the output of the redundant secondary controller, and the threshold of voltage amplitude deviation is set to 0.2 V.

Similarly, we can obtain equation (10) for the secondary voltage control of other DGs under the proposed secondary control methods:

$$\delta E_i^* = k_{pE}(E_{ri} - E_i) + k_{iE} \int (E_{ri} - E_i) dt + \delta E_r \quad (10)$$

where δE_i^* is the regulation value of the output of the secondary controllers in each DG when the redundant controller is triggered, δE_i is the regulated value of the output of the redundant secondary voltage controller.

4 Simulation results under multiple attack scenarios

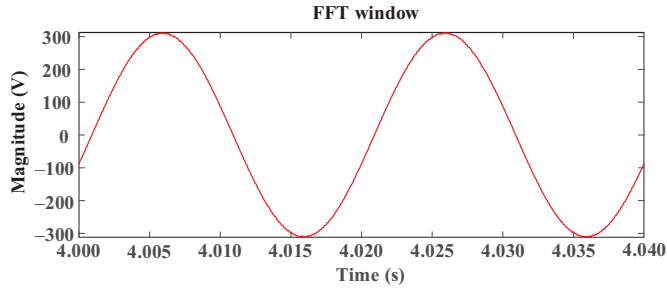
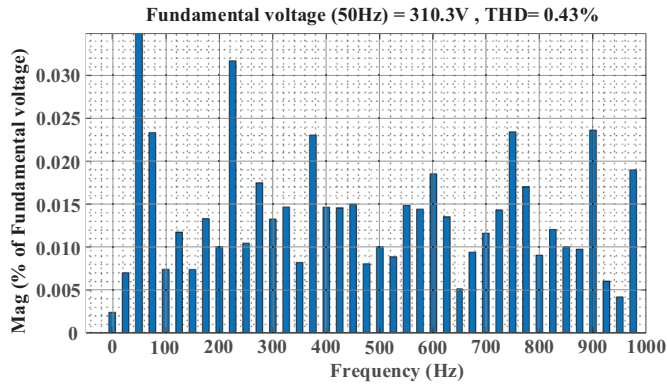
To evaluate the performance of the proposed methodology to resist FDI attacks, the proposed microgrid redundant secondary control method is simulated in MATLAB/Simulink. The parameter settings of the system are shown in [Table 1](#). The microgrid system contains six DGs whose output buses converge together to form a common bus. Each DG has an inverter and filter inside, and each DG carries a local load inside and a common load on the common bus. A primary and a secondary controller are included with each DG. In [Table 1](#), i is 1, 2, ..., 6.

According to the parameters in [Table 1](#), the microgrid model is constructed in MATLAB, and the output voltage of the DG1 at a certain moment is randomly intercepted. For example, [Figure 4](#) is the fast Fourier transform (FFT) window in MATLAB, which shows the microgrid's output voltage for two cycles after 4 s, which can be found to be standard sine. The Simulink microgrid model established in MATLAB is debugged for the parameters and eventually generates a microgrid model with a relatively good output of power quality.

In [Figure 5](#), the frequency of the microgrid is set to 50 Hz, and the fundamental amplitude of its output voltage in the period from 4.000 to 4.040 s is 310.3 V. [Figure 5](#) shows the total harmonic distortion (THD) rate of the voltage based on the waveform in [Figure 4](#) from the Fourier

Table 1. System setting and control parameters.

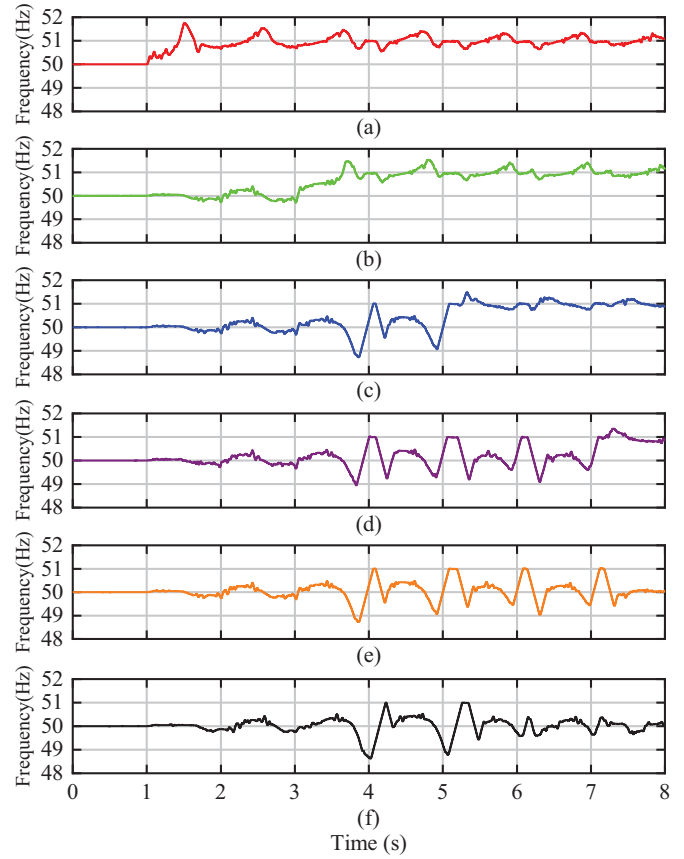
Description	Value
Bus voltage	DC: 1000 V; AC: 380 V (V_{rms} , phase-phase), ($f = 50$ Hz)
AC-side filter	$L = 0.9$ mH, $C = 250$ μ F;
Default loads	Local loads: $P_{DGi} = 10$ kW; Common loads: $P_C = 40$ kW
Droop control	$m_{Pi} = 3/70000$, $n_{Qi} = 4/11000$; $P_{ri} = Q_{ri} = 0$
Primary control PI parameters	Outer voltage loop: $k_p = 8$, $k_i = 12$
Secondary control PI parameters	Inner current loop: $k_p = 0.24$, $k_i = 0.01$ $k_{p\omega} = 0.5$, $k_{i\omega} = 1.2$; $k_{pE} = 0.5$, $k_{iE} = 1.6$

**Fig. 4.** The output voltage of DG1 of the microgrid from 4.000 s to 4.040 s.**Fig. 5.** The total harmonic distortion of the output voltage of DG1 from 4.000 s to 4.040 s.

transform, and the THD is 0.43%, and the vertical coordinate is the percentage of the harmonic to the fundamental waveform for different sampling frequencies. Finally, it can be concluded that the output of this microgrid model is very stable.

4.1 Case 1: Frequency regulation under traditional secondary control

In this case, the traditional secondary control was activated at the initial time, and the timing started after the system was stable. The frequency of the microgrid's output voltage with traditional secondary control is illustrated in Figure 6.

**Fig. 6.** The frequency of each DG with traditional secondary control under FDI attacks: Frequency of (a) DG1, (b) DG2, (c) DG3, (d) DG4, (e) DG5 and (f) DG6.

From 1 to 2 s, the reference value 50 of the secondary frequency control of DG1 tampers with 50.5; from 3 to 4 s, the reference value 50 of the secondary frequency control setting of DG2 tampers with 50.6; and from 5 to 6 s, the reference value 50 of the secondary frequency control setting of DG3 tampers with 50.7; from 7 to 8 s, the reference value 50 of the secondary frequency control setting of DG4 tampers with 50.8.

It can be concluded from Figure 6 that when the frequency of the microgrid with conventional secondary

control is attacked by FDI, its frequency will be disordered, which leads to a serious deviation from the desired frequency value and when the attack stops, the system is still not able to recover to the desired frequency.

4.2 Case 2: Frequency regulation under proposed redundant secondary control

In this scenario, the microgrid adopts the proposed redundant secondary control method, frequency variations of each DG in the microgrid attacked by FDI are shown in Figure 7. From 0 to 8 s, the FDI attack settings are the same as in *Case 1*. However, from 9 to 10 s, the reference value 50 of the secondary frequency control setting of DG5 is tampered with 51; and from 10 to 11 s, the reference value 50 of the redundant controller is tampered with 51.

In Figure 7, the proposed secondary control method is utilized in the microgrid, when the frequency is attacked by FDI, its frequency will deviate from the desired frequency at the beginning of the attack, but it can be restored to the desired frequency of 50, immediately.

4.3 Case 3: Voltage regulation under traditional secondary control

In this scenario, the amplitude of the voltage measured by the secondary voltage control is different from that of the frequency. Here the amplitude of the voltage at the output of each DG is measured, not the voltage amplitude at the busbar. The traditional secondary control has been activated at the initial time, and the timing starts after the system is stable. The amplitude of the output voltage of the microgrid with traditional secondary control is shown in Figure 8.

From 1 to 2 s, the reference value 311 of the secondary voltage control setting of DG1 is tampered with 312; from 3 to 4 s, the reference value 311 of the secondary voltage control setting of DG2 is tampered with 313; and from 5 to 6 s, the reference value of the secondary voltage control setting of DG3 is tampered with 313; from 7 to 8 s, the reference value of the secondary voltage control setting of DG4 is tampered with 313. The voltage references for DG5 and DG6 have never been attacked.

It can be concluded that when the microgrid adopts the conventional secondary control, when FDI attacks the voltage reference value of the secondary control of one of the DGs of the microgrid, it causes the output voltage to deviate from the desired value and follows the injected false data.

4.4 Case 4: Voltage regulation under proposed redundant secondary control

In this scenario, the microgrid adopts the proposed redundant secondary control. The settings of FDI attacks are the same as in *Case 3*, voltage variations of each DG in the microgrid attacked by FDI are illustrated in Figure 9. It can be concluded from Figure 9 that when the microgrid is controlled with redundant secondary voltage control, the voltage amplitude deviates from the desired value at the beginning of the attack by FDI, the scale of its change at

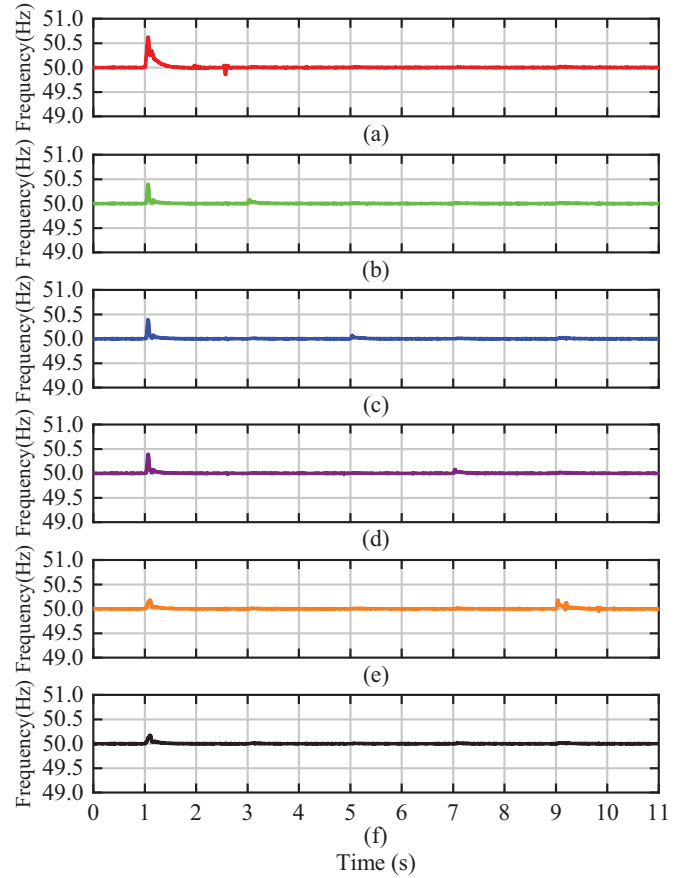


Fig. 7. The frequency of each DG with redundant secondary control under FDI attacks: Frequency of (a) DG1, (b) DG2, (c) DG3, (d) DG4, (e) DG5 and (f) DG6.

the beginning is smaller than that of the conventional secondary control, and immediately returns to the desired value 311. So the proposed method is successful in resisting FDI attacking the voltage.

5 FPGA-in-the-loop experiments

In this study, the hardware-in-the-loop simulation framework is used to verify the performance of the designed secondary control method in resisting FDI attacks. Hardware-in-the-loop is a semi-physical real-time simulation technique. With this principle, field programmable gate array (FPGA) and MATLAB are united, and the personal computer is physically connected to the FPGA. In this study, the joint test action group method is used to realize the communication between the FPGA and MATLAB on the personal computer side. The principle of this connection is similar to the Signaltap of Quartus II, which generates the module in the FPGA that takes charge of the transmission of information.

The principle of the experiment is shown in Figure 10. Firstly, the model connected to the FPGA is created in Simulink, through which the signal is generated and transmitted to the FPGA. Then the FPGA reads the signal and

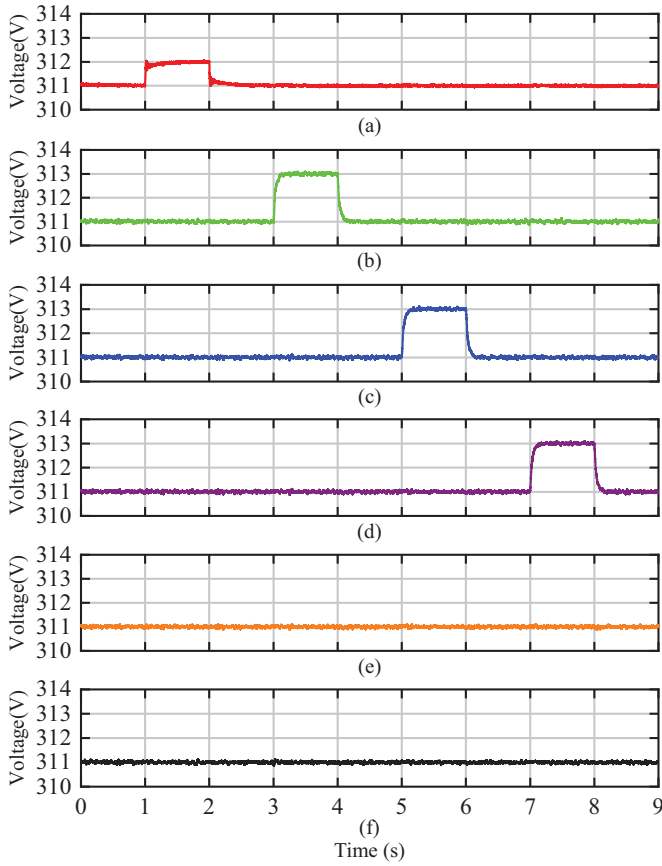


Fig. 8. The voltage of each DG with traditional secondary control under FDI attacks: Voltage amplitude of (a) DG1, (b) DG2, (c) DG3, (d) DG4, (e) DG5 and (f) DG6.

transfers it to Simulink for display. And the FPGA can be used to simulate the FDI attacks in this study, the false data is output through the “key” on the FPGA, which is transmitted to the computer side of the Simulink model, and then this false data is injected into the frequency reference and voltage reference of the secondary control of the microgrid for FDI attacks. Then the performance of the proposed method to resist FDI attacks is tested through the experimental results.

5.1 FPGA-in-the-loop experiments for FDI attacks frequency

The settings of the hardware-in-the-loop experiments are similar to the FDI attack settings simulated in *Case 1*. **Figure 11** is the output of the FPGA, which will be used as FDI attacks on the secondary frequency control after being multiplied by the corresponding coefficients (0.5 and 0.6 in DG1 and DG2, respectively).

Figure 12 presents the frequency of the output voltage of DG1 and DG2 of the conventional secondary-controlled microgrid under FDI attacks. It can be summarized that once the microgrid is attacked by the false data outputted by FPGA, the frequency of the microgrid deviates from the desired value and becomes disordered. In **Figure 13**,

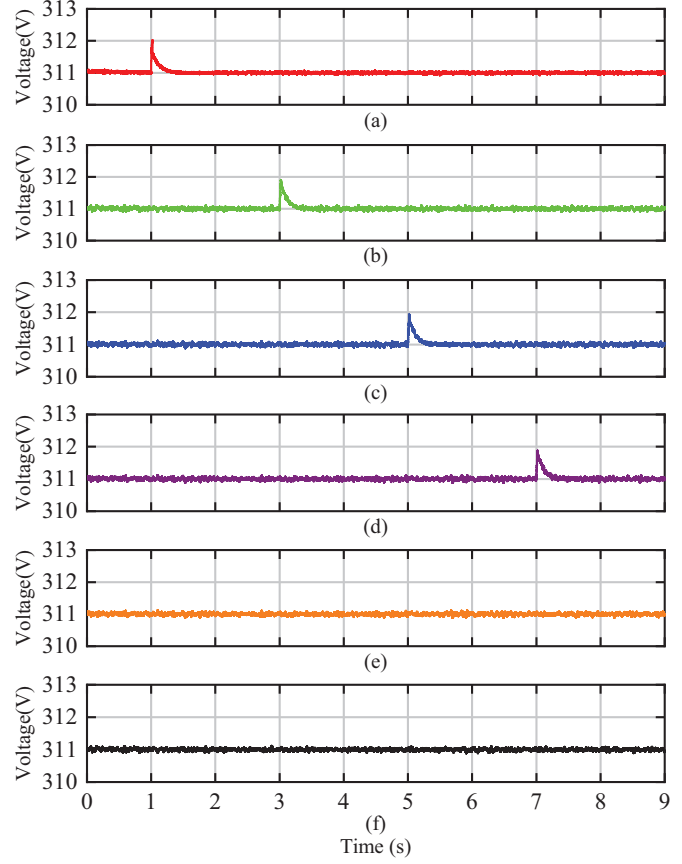


Fig. 9. The voltage of each DG with redundant secondary control under FDI attacks: Voltage amplitude of (a) DG1, (b) DG2, (c) DG3, (d) DG4, (e) DG5 and (f) DG6.

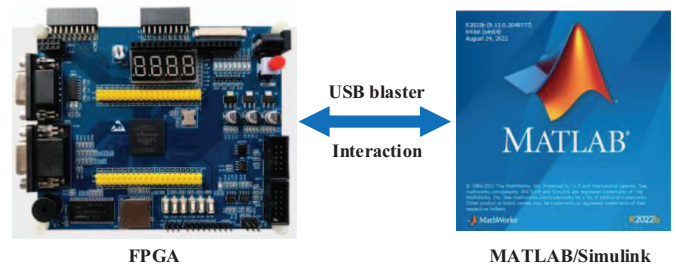


Fig. 10. Hardware-in-the-loop experiment structure.

the frequency of the microgrid with redundant secondary control is attacked by FDI. It can be summarized that when the microgrid is attacked by the false data output from FPGA, the frequency of the microgrid deviates from the desired value in the beginning period, but immediately returns to the desired value.

5.2 FPGA-in-the-loop experiments for FDI attacks voltage

The settings of the hardware-in-the-loop simulation are similar to the FDI attack settings simulated in *Case 3*. **Figure 14** is the output of the FPGA, which will be used

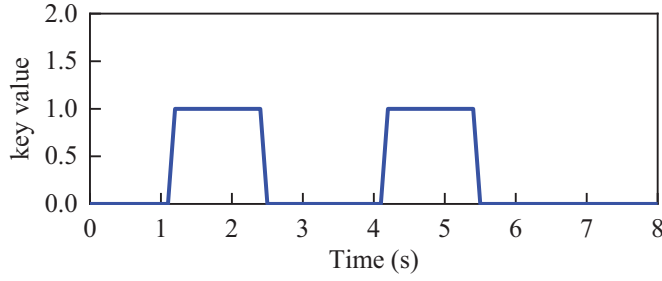


Fig. 11. The output from FPGA to the secondary frequency control in MATLAB.

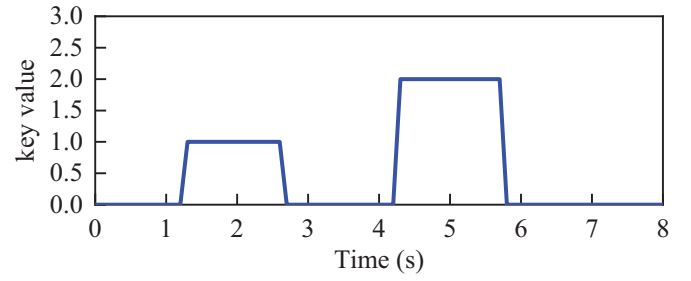


Fig. 14. The output from FPGA to the secondary voltage control in MATLAB.

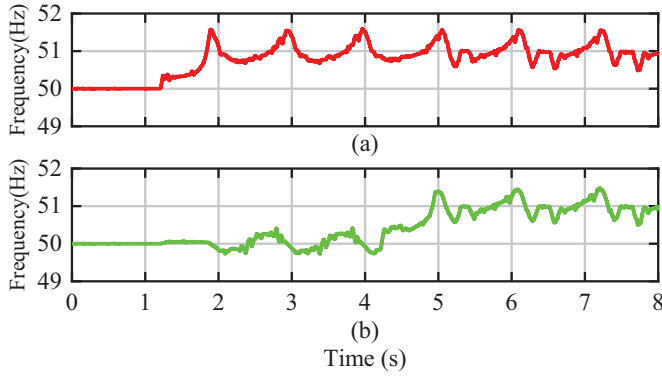


Fig. 12. The frequency of the microgrid under the conventional secondary control attacked by the output of FPGA: Frequency of (a) DG1 and (b) DG2.

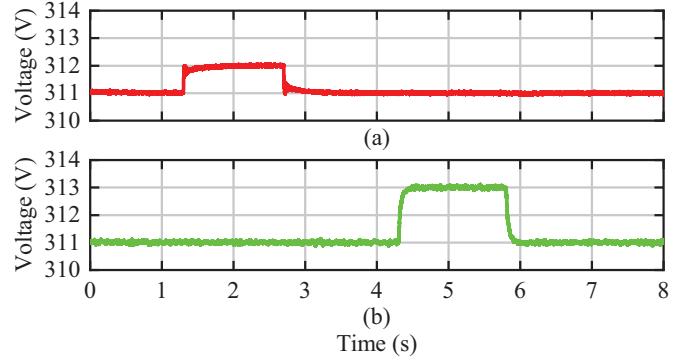


Fig. 15. The voltage amplitude of the microgrid under the conventional secondary control attacked by the output of FPGA: Voltage amplitude of (a) DG1 and (b) DG2.

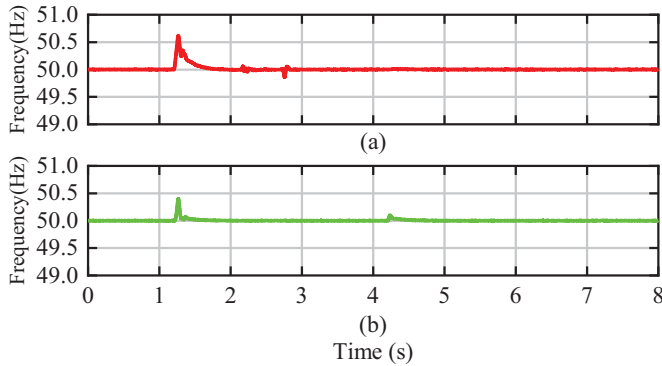


Fig. 13. The frequency of the microgrid under the proposed secondary control attacked by the output of FPGA: Frequency of (a) DG1 and (b) DG2.

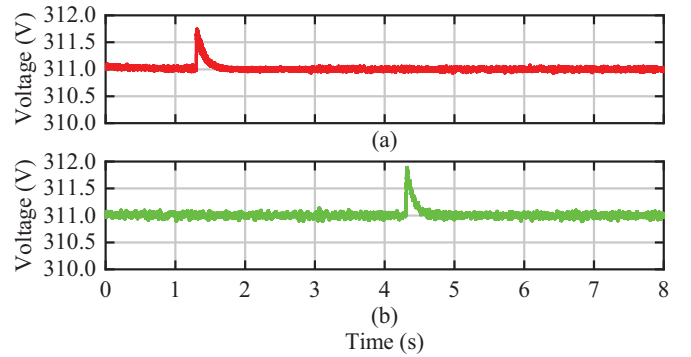


Fig. 16. The voltage amplitude of the microgrid under the proposed secondary control attacked by the output of FPGA: Voltage amplitude of (a) DG1 and (b) DG2.

as the FDI attacks on the secondary voltage control. Figure 15 shows the amplitude of the output voltage of DG1 and DG2 after the microgrid is attacked by FDI. It can be concluded that once the voltage of the microgrid is attacked by the false data output from the FPGA, the voltage amplitude of the microgrid follows the reference value of the injected false voltage amplitude. Similarly, in Figure 16, when the voltage of the microgrid with redundant secondary control is attacked by the false data output from FPGA, the voltage of the microgrid deviates from the desired value during the initiation period, but promptly comes to the desired value.

6 Limitations of the study

To realize the stable operation of microgrids, this study proposes a redundant secondary control scheme to resist FDI attacks, but the study still has some defects and limitations as follows:

1. This study only simulated FDI attacks on microgrids, there are a variety of attacks in practice, and our team will also study microgrids facing a variety of attack scenarios next.

2. In this study, redundant secondary control is equipped for microgrids to resist FDI attacks, but the effect of the redundant modules on the economic operation of the microgrid, energy management, etc. is not considered.
3. The scheme proposed in this study to resist FDI attacks is only validated by using FPGA, and it remains to be verified whether it can achieve the above effects in actual microgrid operation, and there is still a gap with practical applications.

7 Conclusion

In response to FDI attacks on microgrids, this study resists the FDI attacks on microgrids with voltage and frequency, respectively, through the proposed redundant control. We verify that the method can successfully resist FDI attacks by using the FPGA-in-the-loop experiments. The contributions of this study are as follows:

1. A redundant secondary control method is proposed in this paper to address the problem of FDI attacking the frequency and voltage of AC microgrids.
2. A comparator is set within each DG, so that when FDI attacks the frequency or voltage setpoint of its secondary control, *i.e.*, the difference between the output frequency value of the microgrid and the desired value exceeds the set threshold value of 0.1 Hz, and the difference between the output voltage value of the microgrid and the desired value exceeds the set threshold value of 0.2 V, the output of the redundant controller is activated to respond to the frequency or voltage change caused by FDI attacks.
3. Six DGs are tested for their frequency and voltage change after being attacked by FDI, and the results indicate that the proposed redundant secondary control method can resist FDI attacks on the frequency and voltage of AC microgrids.

Funding

This work was supported by the National Natural Science Foundation of China (62303107), Shanghai Sailing Program (21YF1400100) and Fundamental Research Funds for the Central Universities (2232021D-38, 2232022G-09).

References

- 1 Peng Y., Jolfaei A., Yu K. (2021) A novel real-time deterministic scheduling mechanism in industrial cyber-physical systems for energy Internet, *IEEE Trans. Ind. Inform.* **18**, 8, 5670–5680. <https://doi.org/10.1109/TII.2021.3139357>.
- 2 Lu X., Yu X., Lai J., Wang Y., Guerrero J.M. (2016) A novel distributed secondary coordination control approach for islanded microgrids, *IEEE Trans. on Smart Grid* **9**, 4, 2726–2740. <https://doi.org/10.1109/TSG.2016.2618120>.
- 3 Qing H., Zhang C., Xu J., Zeng S., Guo X. (2023) A nonlinear multimode controller for seamless off-grid of energy storage inverter under unintentional islanding, *IEEE Trans. Ind. Electron.* **70**, 12, 12354–12364. <https://doi.org/10.1109/TIE.2022.3232639>.
- 4 Xu F., Qiu P., Ding C., Lu Y. (2023) Flexible combined heat and power dispatch based on probabilistic prediction of wind power, in: 2023 5th Asia Energy and Electrical Engineering Symposium (AEEES), Chengdu, China, 23–26 March, IEEE, pp. 1491–1495. <https://doi.org/10.1109/AEEES56888.2023.10114217>.
- 5 Zhou J., Sun H., Xu Y., Han R., Yi Z., Wang L., Guerrero J. M. (2021) Distributed power sharing control for islanded single-/three-phase microgrids with admissible voltage and energy storage constraints, *IEEE Trans. Smart Grid* **12**, 4, 2760–2775. <https://doi.org/10.1109/TSG.2021.3057899>.
- 6 An R., Liu J., Liu Z., Song Z. (2022) Flexible transfer converters enabling autonomous control and power dispatch of microgrids, *IEEE Trans. Ind. Electron.* **37**, 11, 13767–13781. <https://doi.org/10.1109/TPEL.2022.3180562>.
- 7 Shuai H., Li F., Pulgar-Painemal H., Xue Y. (2021) Branching dueling Q-network-based online scheduling of a microgrid with distributed energy storage systems, *IEEE Trans. Smart Grid* **12**, 6, 5479–5482. <https://doi.org/10.1109/TSG.2021.3103405>.
- 8 Ling Y., Li Y., Yang Z., Xiang J. (2020) A dispatchable droop control method for distributed generators in islanded AC microgrids, *IEEE Trans. Ind. Electron.* **68**, 9, 8356–8366. <https://doi.org/10.1109/TIE.2020.3013547>.
- 9 Shan Y., Hu J., Guerrero J.M. (2019) A model predictive power control method for PV and energy storage systems with voltage support capability, *IEEE Trans. Smart Grid* **11**, 2, 1018–1029. <https://doi.org/10.1109/TSG.2019.2929751>.
- 10 Qiu H., Zhao B., Gu W., Bo R. (2018) Bi-level two-stage robust optimal scheduling for AC/DC hybrid multi-microgrids, *IEEE Trans. Smart Grid* **9**, 5, 5455–5466. <https://doi.org/10.1109/TSG.2018.2806973>.
- 11 Zhang C., Xu Y., Dong Z.Y., Yang L.F. (2019) Multitimescale coordinated adaptive robust operation for industrial multienergy microgrids with load allocation, *IEEE Trans. Ind. Inform.* **16**, 5, 3051–3063. <https://doi.org/10.1109/TII.2019.2907710>.
- 12 Wan Y., Dragičević T. (2022) Data-driven cyber-attack detection of intelligent attacks in islanded DC microgrids, *IEEE Trans. Ind. Electron.* **70**, 4, 4293–4299. <https://doi.org/10.1109/TIE.2022.3176301>.
- 13 Tadeipalli P.S., Pullaguram D. (2022) Distributed control microgrids: cyber-attack models, impacts and remedial strategies, *IEEE Trans. Signal Inf. Proc. Netw.* **8**, 1008–1023. <https://doi.org/10.1109/TSIPN.2022.3230562>.
- 14 Kerdphol T., Ngamroo I., Surinkaew T. (2024) Enhanced robust frequency stabilization of a microgrid against simultaneous cyber-attacks, *Electr. Power Syst. Res.* **228**, 110006. <https://doi.org/10.1016/j.epsr.2023.110006>.
- 15 Mahvash H., Taher S.A., Guerrero J.M. (2024) Modified backstepping control for cyber security enhancement of a wind farm based DFIG against false data injection, hijack and denial of service cyber attacks, *Electr. Power Syst. Res.* **231**, 110357. <https://doi.org/10.1016/j.epsr.2024.110357>.
- 16 Habibi M.R., Baghaee H.R., Dragičević T., Blaabjerg F. (2020) False data injection cyber-attacks mitigation in parallel DC/DC converters based on artificial neural networks, *IEEE Trans. Circuits Syst. II – Express Briefs* **68**, 2, 717–721. <https://doi.org/10.1109/TCSII.2020.3011324>.

- 17 Weng S., Weng P., Chen B., Liu S., Yu L. (2022) Distributed secure estimation against unknown FDI attacks and load deviation in multi-area power systems, *IEEE Trans. Circuits Syst. II – Express Briefs* **69**, 6, 3007–3011. <https://doi.org/10.1109/TCSII.2022.3162239>.
- 18 Lin W., Chen G., Zhou X. (2024) Privacy-preserving federated learning for detecting false data injection attacks on power system, *Electr. Power Syst. Res.* **229**, 110150. <https://doi.org/10.1016/j.epsr.2024.110150>.
- 19 Su Q., Fan H., Li J. (2023) Distributed adaptive secondary control of AC microgrid under false data injection attack, *Electr. Power Syst. Res.* **223**, 109521. <https://doi.org/10.1016/j.epsr.2023.109521>.
- 20 Wang L., Yu R., Lv J., Zhang B., Wang F., Teng F. (2023) Resilient distributed secondary control strategy for new energy shipboard microgrid against bounded FDI attacks, in: 2023 IEEE 12th Data Driven Control and Learning Systems Conference (DDCLS), Xiangtan, China, 12–14 May, IEEE, 2023, pp. 1761–1766. <https://doi.org/10.1109/DDCLS58216.2023.10165958>.
- 21 Yang H., Deng C., Xie X., Ding L. (2023) Distributed resilient secondary control for AC microgrid under FDI attacks, *IEEE Trans. Circuits Syst. II-Express Briefs* **70**, 7, 2570–2574. <https://doi.org/10.1109/TCSII.2023.3245282>.
- 22 Guha D. (2023) Cyber-Tolerant resilient frequency control for microgrid with mismatched uncertainties and stealthy FDI-attack, in: 2023 IEEE 3rd International Conference on Sustainable Energy and Future Electric Transportation (SEFET), Bhubaneswar, India, 9–12 August, IEEE, pp. 1–6. <https://doi.org/10.1109/SeFeT57834.2023.10245888>.
- 23 Karanfil M., Youssef E.-N.S., Kassouf M., Debbabi M., Ghafouri M., Hanna A., Real-time protection against microgrid false data injection attacks using passive monitoring, in: (2023) Real-time protection against microgrid false data injection attacks using passive monitoring, in: IEEE Power & Energy Society General Meeting (PESGM), Orlando, FL, USA, 16–20 July, IEEE, pp. 1–5. <https://doi.org/10.1109/PESGM52003.2023.10252928>.
- 24 James Ranjith K.R., Kundur D., Sikdar B. (2019) Transient model-based detection scheme for false data injection attacks in microgrids, in: 2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), Beijing, China, 21–23 October, IEEE, pp. 1–6. <https://doi.org/10.1109/SmartGridComm.2019.8909780>.
- 25 Zhang H., Meng W., Qi J., Wang X., Zheng W.X. (2018) Distributed load sharing under false data injection attack in an inverter-based microgrid, *IEEE Trans. Ind. Electron.* **66**, 2, 1543–1551. <https://doi.org/10.1109/TIE.2018.2793241>.
- 26 Guerrero J.M., Vasquez J.C., Matas J., de Vicuna L.G., Castilla M. (2011) Hierarchical control of droop-controlled AC and DC microgrids – a general approach toward standardization, *IEEE Trans. Ind. Electron.* **58**, 1, 158–172. <https://doi.org/10.1109/TIE.2010.2066534>.
- 27 Han Y., Li H., Shen P., Coelho E.A.A., Guerrero J.M. (2017) Review of active and reactive power sharing strategies in hierarchical controlled microgrids, *IEEE Trans. Power Electron.* **32**, 3, 2427–2451. <https://doi.org/10.1109/TPEL.2016.2569597>.
- 28 Qian T., Liu Y., Zhang W., Tang W., Shahidehpour M. (2020) Event-triggered updating method in centralized and distributed secondary controls for islanded microgrid restoration, *IEEE Trans. Smart Grid* **11**, 2, 1387–1395. <https://doi.org/10.1109/TSG.2019.2937366>.
- 29 Wu X., Shan Y., Fan K. (2024) A Modified particle swarm algorithm for the multi-objective optimization of wind/photovoltaic/diesel/storage microgrids, *Sustainability* **16**, 3, 1065. <https://doi.org/10.3390/su16031065>.
- 30 Simpson-Porco J.W., Shafiee Q., Dörfler F., Vasquez J.C., Guerrero J.M., Bullo F. (2015) Secondary frequency and voltage control of islanded microgrids via distributed averaging, *IEEE Trans. Ind. Electron.* **62**, 11, 7025–7038. <https://doi.org/10.1109/TIE.2015.2436879>.
- 31 Chen M., Xiao X., Guerrero J.M. (2018) Secondary restoration control of islanded microgrids with a decentralized event-triggered strategy, *IEEE Trans. Ind. Inform.* **14**, 9, 3870–3880. <https://doi.org/10.1109/TII.2017.2784561>.
- 32 Ning B., Han Q.-L., Ding L. (2021) Distributed finite-time secondary frequency and voltage control for islanded microgrids with communication delays and switching topologies, *IEEE T. Cybern.* **51**, 8, 3988–3999. <https://doi.org/10.1109/TCYB.2020.3003690>.
- 33 Chen Y., Qi D., Dong H., Li C., Li Z., Zhang J. (2020) A FDI Attack-resilient distributed secondary control strategy for islanded microgrids, *IEEE Trans. Smart Grid* **12**, 3, 1929–1938. <https://doi.org/10.1109/TSG.2020.3047949>.