mathematics

MDPI

Article

Distributed Resilient Control of DC Microgrid Subject to Time-Varying False Data Injection Attacks

Ziqi Xu, Zhenyu Gao *, Yongtao Wei and Feng Guo

School of Control Engineering, Northeastern University at Qinhuangdao, Qinhuangdao 066004, China
* Correspondence: 18840839109@163.com

Abstract

Focusing on the issue that false data injection (FDI) attacks on the secondary controllers of DC microgrids can affect the normal and stable operation of microgrids, a distributed resilient controller for DC microgrids is proposed to ensure that the two control objectives, voltage regulation and current sharing, can still be achieved under the action of time-varying bounded FDI attacks. First, the distributed secondary control problem of the microgrid is viewed as a leader–follower multi-agent consensus problem, and the impact of FDI attacks on the microgrid is analyzed. Second, a fully distributed resilient controller based on an adaptive compensation mechanism is designed to compensate for FDI attacks and mitigate their impact on the microgrid. Next, it is proven through Lyapunov stability theory that the microgrid can operate normally and stably under the designed distributed resilient controller, achieving the two control objectives. Finally, simulation analysis is used to verify the effectiveness of the proposed resilient control method.

Keywords: DC microgrid; false data injection attack; resilient control; voltage regulation; current distribution

MSC: 93B52

1. Introduction

In recent years, with the depletion of fossil energy and the deterioration of the ecological environment, new power systems have drawn widespread attention. As a key component of new power systems, microgrids have become a research focus for many scholars [1]. Microgrids can be classified into DC microgrids, AC microgrids, and hybrid AC/DC microgrids. Compared with AC microgrids, DC microgrids do not need to consider issues such as frequency and power, and distributed generators (DGs) like photovoltaic and wind power all possess DC characteristics, allowing them to be directly connected to form a DC microgrid through DC-DC converters, which is more conducive to energy utilization [2–4].

The operation of a DC microgrid involves two control objectives: voltage regulation and current sharing, i.e., regulating the average output voltage of all DGs to the nominal value and making the output currents of the DGs follow a fixed ratio [5]. Droop control is commonly used in the primary control of microgrids to achieve preliminary voltage regulation and current sharing. However, as a bottom-level control method, droop control often fails to achieve these two objectives simultaneously; therefore, secondary control is usually introduced to compensate for the shortcomings of droop control [6,7]. Secondary

Check for updates

Academic Editor: Luigi Fortuna

Received: 4 June 2026
Revised: 25 June 2026
Accepted: 29 June 2026
Published: 3 July 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

control generally includes centralized control and distributed control. Centralized control requires a central controller to regulate global information [8]. The central controller can collect global information for processing and decision making, offering high communication accuracy and making it more suitable for applications with stringent precision requirements [9]. However, the very presence of the central controller makes centralized control more dependent on the communication network, resulting in reduced reliability, especially in large-scale microgrids where single-point failures are prone to occur [10,11].

To avoid these drawbacks, distributed control is commonly employed in microgrids. In distributed control, there is no central controller, and communication links exist between neighboring units; each DG only needs to exchange information with its neighbors via these links. Due to the absence of a central controller, distributed control eliminates single-point failures, enables plug-and-play of DGs, and is more suitable for handling a large number of renewable energy sources such as photovoltaic and wind power [12,13]. Moreover, consensus algorithms can be introduced into distributed control, where a local control protocol is sought to bring all DGs to a consensus [14]. Therefore, distributed control is currently the most widely applied control method, and applying it to microgrids is one of the most effective approaches.

In recent years, information technology has continuously permeated production and daily life. Against this backdrop, the physical structure of a microgrid can be considered the physical layer, and its communication structure the cyber layer; that is, the microgrid can be viewed as a complex cyber-physical system [15]. However, this integration of information technology exposes microgrids to serious cybersecurity threats. In particular, for microgrids adopting distributed control, since there is no central controller, each DG needs to exchange information with neighboring DGs to infer global information. Consequently, when a single DG or communication link suffers a malicious cyber attack, the impact can easily propagate throughout the entire system, causing the microgrid's control objectives to fail or even leading to system collapse and severe economic losses. Microgrids with distributed control are therefore more vulnerable to malicious cyber attacks, which hinder their normal operation [16,17]. Cyber attacks that threaten microgrids can be divided into Denial-of-Service (DoS) attacks and false data injection (FDI) attacks [13]. DoS attacks mainly disrupt the information exchange between DGs, causing packet loss and preventing the microgrid from operating normally. FDI attacks inject malicious data into the microgrid's communication links, thereby masking the true data of the microgrid and affecting its stable operation. Compared with DoS attacks, FDI attacks are simpler, more efficient, and deceptive, and are not easily detected by the system, making the elimination of FDI attack impacts an important research topic [18,19].

Currently, methods to eliminate the impact of FDI attacks and maintain stable operation of microgrids can be classified into detection and isolation, and resilient control [20]. Detection and isolation are the primary methods for defending against FDI attacks. However, while isolating information related to the attack signals, this method inevitably also isolates some information that is useful to the microgrid, thereby affecting its normal operation to a certain extent [21]. Thus, detection and isolation methods cannot completely eliminate the impact of malicious cyber attacks. Resilient control, as a class of control methods with security protection features, can enable the system to restore normal operation after a malicious cyber attack, or maintain a stable working state that meets safety standards with only slight performance degradation. In response to malicious cyber attacks, resilient control methods strive to mitigate their negative impacts, allowing the microgrid to return to its normal operation mode within a short time. In recent years, resilient control methods have also attracted considerable attention from scholars [22,23].

Currently, most resilient control methods first require state observation of the microgrid and the design of a resilient controller to eliminate the impact of cyber attacks. However, observing the system state requires a large number of input signals, resulting in a heavy workload. For example, in [24], for the secondary control scenario of a microgrid under FDI attacks, the problem is modeled as a fault-tolerant consensus problem in a multi-agent system framework for analysis and research. A distributed extended state observer is constructed to observe the microgrid state, and a fault-tolerant controller is designed to counteract the interference caused by FDI attack signals. In [25], an intermittent control method is used to detect whether malicious cyber attack signals exist. Although this control method can effectively eliminate the impact of cyber attacks, the designed controller requires too many input signals, making the control method overly complex and causing a huge workload. Therefore, designing a resilient control method that does not require system state observation and further simplifies the control approach has become a research focus.

In view of this, this paper investigates the distributed secondary control problem for DC microgrids under the threat of time-varying false data injection attacks. First, the vulnerability of traditional distributed control strategies under attack conditions and their negative impact on system operation are analyzed. On this basis, a distributed resilient control scheme integrating an adaptive compensation mechanism is proposed. Simulations and analysis show that the proposed scheme can effectively resist attack disturbances and significantly improve the stability and reliability of microgrid operation. The main contributions of this paper are as follows:

(1) The proposed method does not require the establishment of complex detection mechanisms, does not need to observe the state of the microgrid, and does not require measuring too many input signals. It only uses an adaptive compensation mechanism to defend against FDI attacks, making the approach simple and easy to implement.
(2) The proposed resilient control method imposes no limit on the number of distributed generators and remains effective even when all DGs are under FDI attacks.
(3) The proposed control method can effectively mitigate the impact of bounded time-varying FDI attacks on the microgrid, ensuring that the two control objectives—voltage regulation and current sharing—are largely unaffected. Moreover, when there is no FDI attack, the proposed method does not interfere with the stable operation of the microgrid.

2. Preliminaries

2.1. Graph Theory

The communication network is a crucial component of a microgrid. In a distributed control architecture, each distributed generator can be regarded as an agent, and a DC microgrid equipped with multiple DGs can be equivalent to a multi-agent system. The DC microgrid can be abstracted as an undirected connected graph $G = \{E, V, A\}$ for modeling and analysis. DGs can be viewed as nodes in the undirected connected graph, and the set of all nodes can be expressed as $V = \{v_1, v_2, \ldots, v_N\}$. $E \subset V \times V$ denotes the set of communication edges, (v_i, v_j) represents the communication link between node i and node j, and $A = (a_{ij}) \in \mathbb{R}^{N \times N}$ denotes the adjacency matrix, where a_{ij} indicates the connection weight between node i and node j. If $(v_i, v_j) \in E$, then $a_{ij} = a_{ji} = 1$; otherwise $a_{ij} = a_{ji} = 0$, and a_{ii} is always 0. Node i can obtain information from its neighbors, and we define $N_i = \{v_j \in V \mid (v_i, v_j) \in E\}$ as the neighbor set of node i. The Laplacian matrix is defined as $L = D - A$, where $D = \mathrm{diag}\{d_1, d_2, \ldots, d_N\}$ denotes the degree matrix, and $d_i = \sum_{j \in N_i} a_{ij}$.

2.2. Distributed Cooperative Control of DC Microgrids

Primary control mainly includes droop control and voltage–current double closed-loop control, as shown in Figure 1. Under the action of primary control, the output reference voltage of the i-th distributed generator (DG_i), V_{refi} can be expressed as

$$V_{refi} = V^{ref} - k_i I_i \tag{1}$$

where V^{ref} denotes the nominal voltage, k_i denotes the droop gain, and I_i denotes the output current of DG_i.

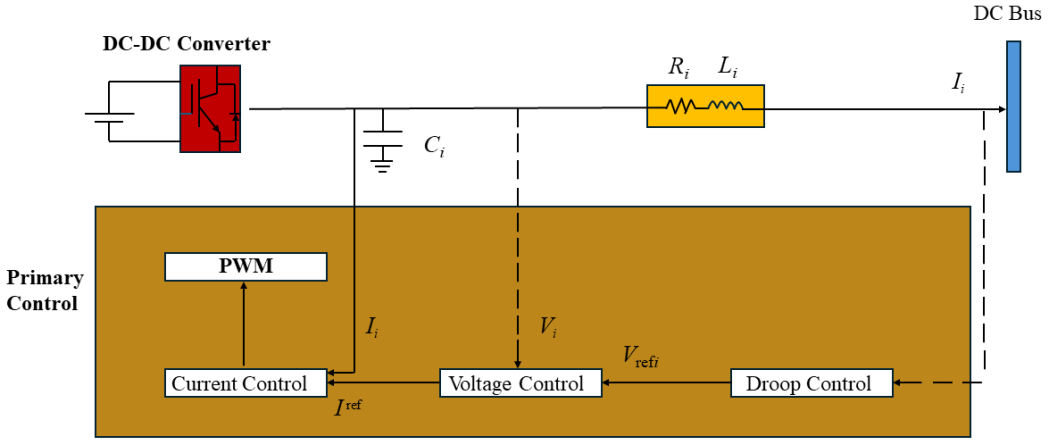


Figure 1. Primary control of DC microgrid.

If the parameters of the voltage loop and current loop are well designed, the output voltage V_i of DG_i can quickly track its reference voltage V_{refi}, i.e.,

$$V_i = V_{refi}. \tag{2}$$

Combining (1) and (2), one has:

$$V_i = V^{ref} - k_i I_i. \tag{3}$$

from which we can see that there exists a difference $k_i I_i$ between the output voltage of DG_i and the nominal voltage, and the larger the droop gain k_i, the larger this difference.

In this paper, the research object is a multi-bus DC microgrid containing N distributed generators, as shown in Figure 2, and the corresponding control objectives are presented in (4): regulating the average of all DGs' output voltages to the nominal value and making the output currents share according to a predetermined ratio. Generally, this ratio can be set as the inverse of the droop gains. Obviously, these two control objectives cannot be achieved through primary control alone.

Therefore, secondary control must be introduced on top of primary control to compensate for its shortcomings. A standard distributed secondary control is shown in Figure 3, from which we can see the multi-bus DC microgrid is composed of N distributed generators (DGs), each of which is connected to its corresponding bus through a DC-DC converter and an LC filter equipped with local resistors, and adjacent DGs are interconnected via transmission lines.

$$\begin{cases} \lim\limits_{t\to\infty} \frac{1}{N} \sum\limits_{i\in G} V_i = V^{ref} \\ \lim\limits_{t\to\infty} \frac{I_i}{I_j} = \frac{k_j}{k_i} \end{cases} \tag{4}$$

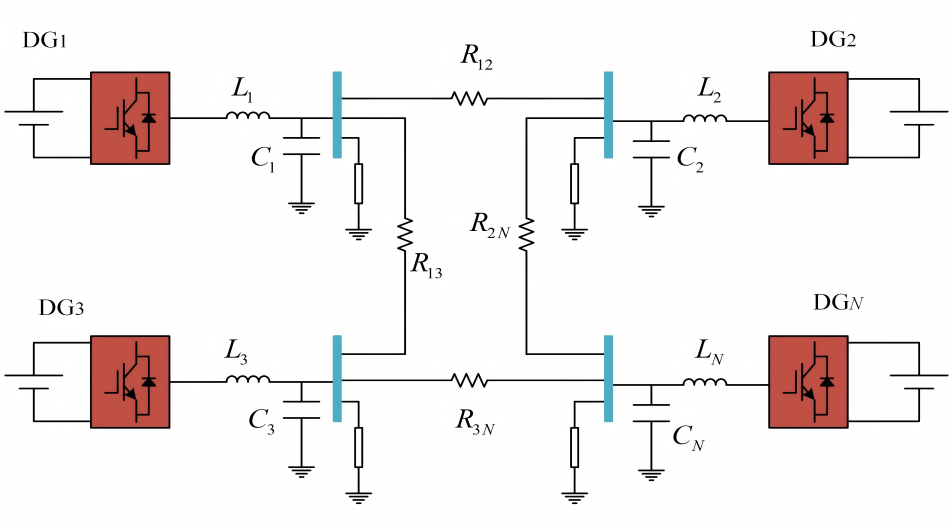


Figure 2. Multi-bus DC microgrid.

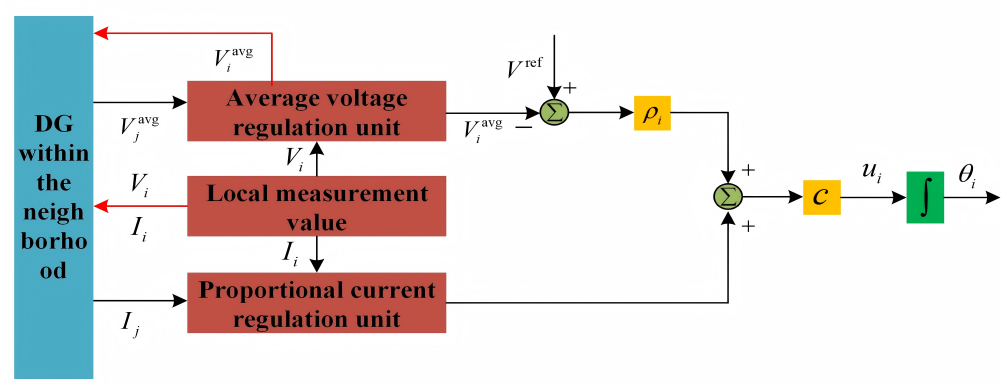


Figure 3. Standard distributed secondary control of DC microgrid.

The voltage regulation unit and current regulation unit in Figure 3 are respectively:

$$V_i^{\text{avg}} = V_i + c\int\left[\sum_{j\in N_i} a_{ij}\left(V_j^{\text{avg}} - V_i^{\text{avg}}\right)\right]\mathrm{d}t \tag{5}$$

$$v_i = \sum_{j\in N_i} a_{ij}\left(k_j I_j - k_i I_i\right) \tag{6}$$

where V_i^{avg} denotes the voltage estimate after the average voltage regulation unit, which can be used to estimate the average of all DGs' output voltages, and v_i denotes the output after the proportional current regulation unit. Under the distributed control shown in Figure 3, the control objectives in (4) can all be achieved; the detailed proof is provided in [5]. As shown in (5) and (6), DG$_i$ only needs to exchange information with neighboring DGs, without requiring global information or a central controller, so this control method is fully distributed. Furthermore, $c > 0$ in Figure 3 denotes the control gain, consistent with the c in (5). The value of ρ_i is either 0 or 1; when $\rho_i = 1$, DG$_i$ can receive the nominal voltage; otherwise it cannot. However, it is necessary to ensure that at least one distributed generator can receive the nominal voltage, i.e., at least one ρ_i equals 1.

By feeding the control output θ_i generated by the distributed secondary control into the primary control, the output voltage of DG$_i$ can be expressed as:

$$V_i = V^{\text{ref}} - k_i I_i + \theta_i. \tag{7}$$

Taking the first derivative of (7) yields:

$$\dot{V}_i + k_i \dot{I}_i = \dot{\theta}_i. \tag{8}$$

From Figure 3, one has $\dot{\theta}_i = u_i$, and further u_i can be expressed as:

$$u_i = c\left[\rho_i\left(V^{\mathrm{ref}} - V_i^{\mathrm{avg}}\right) + \sum_{j\in N_i} a_{ij}\left(k_j I_j - k_i I_i\right)\right]. \tag{9}$$

Combining (8) and (9), we can obtain:

$$\dot{V}_i + k_i \dot{I}_i = c\left[\rho_i\left(V^{\mathrm{ref}} - V_i^{\mathrm{avg}}\right) + \sum_{j\in N_i} a_{ij}\left(k_j I_j - k_i I_i\right)\right]. \tag{10}$$

Differentiating (5) yields:

$$\dot{V}_i^{\mathrm{avg}} = \dot{V}_i + c\sum_{j\in N_i} a_{ij}\left(V_j^{\mathrm{avg}} - V_i^{\mathrm{avg}}\right). \tag{11}$$

Together with (10) and (11), one has:

$$\begin{aligned} &\dot{V}_i^{\mathrm{avg}} + k_i \dot{I}_i \\ &= c\left[\rho_i\left(V^{\mathrm{ref}} - V_i^{\mathrm{avg}}\right) + \sum_{j\in N_i} a_{ij}\left(k_j I_j - k_i I_i\right)\right] \\ &\quad + c\sum_{j\in N_i} a_{ij}\left(V_j^{\mathrm{avg}} - V_i^{\mathrm{avg}}\right) \\ &= c\left\{\begin{array}{l}\rho_i\left[\left(V^{\mathrm{ref}} + k_i I_i\right) - \left(V_i^{\mathrm{avg}} + k_i I_i\right)\right] \\ + \sum_{j\in N_i} a_{ij}\left[\left(V_j^{\mathrm{avg}} + k_j I_j\right) - \left(V_i^{\mathrm{avg}} + k_i I_i\right)\right]\end{array}\right\}. \end{aligned} \tag{12}$$

Based on [26], under the distributed secondary control (as shown in Figure 3), the microgrid can reach the steady state quickly, and after stabilization the product of droop gain and output current $k_i I_i$ tends to a fixed value kI^{s}. Therefore, the expression (12) can be rewritten as:

$$\begin{aligned} &\dot{V}_i^{\mathrm{avg}} + k_i \dot{I}_i \\ &= c\left\{\begin{array}{l}\rho_i\left[\left(V^{\mathrm{ref}} + kI^{\mathrm{s}}\right) - \left(V_i^{\mathrm{avg}} + k_i I_i\right)\right] \\ + \sum_{j\in N_i} a_{ij}\left[\left(V_j^{\mathrm{avg}} + k_j I_j\right) - \left(V_i^{\mathrm{avg}} + k_i I_i\right)\right]\end{array}\right\}. \end{aligned} \tag{13}$$

For ease of expression, the following two new variables are introduced:

$$\begin{cases} \sigma_i = V_i^{\mathrm{avg}} + k_i I_i \\ \sigma^{\mathrm{ref}} = V^{\mathrm{ref}} + kI^{\mathrm{s}} \end{cases} \tag{14}$$

where σ_i denotes the sum of the average voltage of DG_i and the product of droop gain and output current, and σ^{ref} denotes the sum of the nominal voltage and the product of droop gain and output current at steady state, which is a constant value.

Therefore, based on (12), the expression (13) can be further rewritten as:

$$\dot{\sigma}_i = c\left[\sum_{j\in N_i} a_{ij}\left(\sigma_j - \sigma_i\right) + \rho_i\left(\sigma^{\mathrm{ref}} - \sigma_i\right)\right]. \tag{15}$$

When the DC microgrid is in steady state, the control objective can be transformed into $\sigma_i = \sigma_j = \sigma^{\text{ref}}$. Hence, under the distributed control strategy (see Figure 3), the control objective $\sigma_i = \sigma_j = \sigma^{\text{ref}}$ can be achieved.

3. Distributed Resilient Cooperative Control of DC Microgrid

Since distributed control lacks a central controller and cannot obtain global information, the system is unable to effectively detect whether an attack signal has been injected when an attack occurs, and its stability can be compromised.

3.1. Impact of FDI Attacks

During the communication process among DGs in the microgrid, an attacker may inject unknown malicious false data injection attacks to undermine the stability of the microgrid, preventing it from operating normally. Under the influence of FDI attacks, the average voltage of the distributed generators in the DC microgrid will deviate from the nominal value, and the output currents will fail to follow the predetermined ratio; i.e., the control objective $\sigma_i = \sigma_j = \sigma^{\text{ref}}$ cannot be achieved. Specifically, let u_i^a denote the secondary control input under a cyber attack, which can be expressed as

$$u_i^a = u_i + \zeta_i = c \left[\begin{array}{l} \rho_i \left(V^{\text{ref}} - V_i^{\text{avg}} \right) \\ + \sum\limits_{j \in N_i} a_{ij} \left(k_j I_j - k_i I_i \right) \end{array} \right] + \zeta_i \tag{16}$$

where ζ_i denotes the FDI attack suffered by DG_i.

Under the FDI attack, (15) can be rewritten as:

$$\dot{\sigma_i} = c \left[\rho_i \left(\sigma^{\text{ref}} - \sigma_i \right) + \sum_{j \in N_i} a_{ij} \left(\sigma_j - \sigma_i \right) \right] + \zeta_i. \tag{17}$$

Define $e_i = \sigma_i - \sigma^{\text{ref}}$ as the error between σ_i and σ^{ref}; then (17) becomes:

$$\dot{e}_i = -c \left[\sum_{j \in N_i} a_{ij} \left(e_i - e_j \right) + \rho_i e_i \right] + \zeta_i. \tag{18}$$

Define the vector $e = [e_1, e_2, \ldots, e_N]^{\text{T}}$ as the error vector. From (18), we have:

$$\dot{e} = -c(L + \rho)e + \zeta \tag{19}$$

where L denotes the Laplacian matrix of the microgrid, ρ is a diagonal matrix with diagonal elements ρ_i, and ζ is a column vector consisting of the attack signals ζ_i, defined respectively as:

$$\begin{cases} \rho = \text{diag}(\rho_i) \\ \zeta = [\zeta_1, \ldots, \zeta_N]^{\text{T}} \end{cases} \tag{20}$$

For convenience of subsequent analysis, let $B = L + \rho$, and then (20) can be written as:

$$\dot{e} = -cBe + \zeta. \tag{21}$$

According to (21), $e(t)$ becomes:

$$e(t) = \exp[-cB(t - t_0)]e(t_0) + \int_{t_0}^{t} \exp[-cB(t - \tau)]\zeta \, \text{d}\tau. \tag{22}$$

Based on [27], $L+\rho$ is a symmetric and positive definite matrix; therefore, the first term $\exp[-cB(t-t_0)]e(t_0)$ in (22) tends to zero. Hence,

$$\begin{aligned}\lim_{t\to\infty} e(t) &= \lim_{t\to\infty}\int_{t_0}^{t}\exp[-cB(t-\tau)]\zeta\,\mathrm{d}\tau \\ &= (cB)^{-1}\zeta\lim_{t\to\infty}\exp(-cBt) \\ &\quad\times\lim_{t\to\infty}[\exp(cBt)-\exp(cBt_0)] \\ &= \frac{1}{c}B^{-1}\zeta.\end{aligned} \tag{23}$$

From (23), it can be seen that as long as ζ is a non-zero FDI attack, the right-hand side of (22) will not equal zero, i.e., $\sigma_i=\sigma_j=\sigma^{\mathrm{ref}}$ does not hold. Therefore, the distributed secondary control strategy, shown in Figure 3, cannot achieve the two control objectives of the DC microgrid in the presence of FDI attacks. To this end, a novel resilient control strategy is proposed in this paper to eliminate the impact of FDI attacks and ensure the stable operation of the microgrid.

3.2. Distributed Resilient Control

To address the problem that FDI attacks can disrupt the stability of the microgrid, a resilient control strategy is designed on the basis of distributed secondary control. Typically, attackers may inject more complex time-varying FDI attacks to cause more severe damage to the microgrid. Therefore, the designed resilient control strategy is shown in Figure 4.

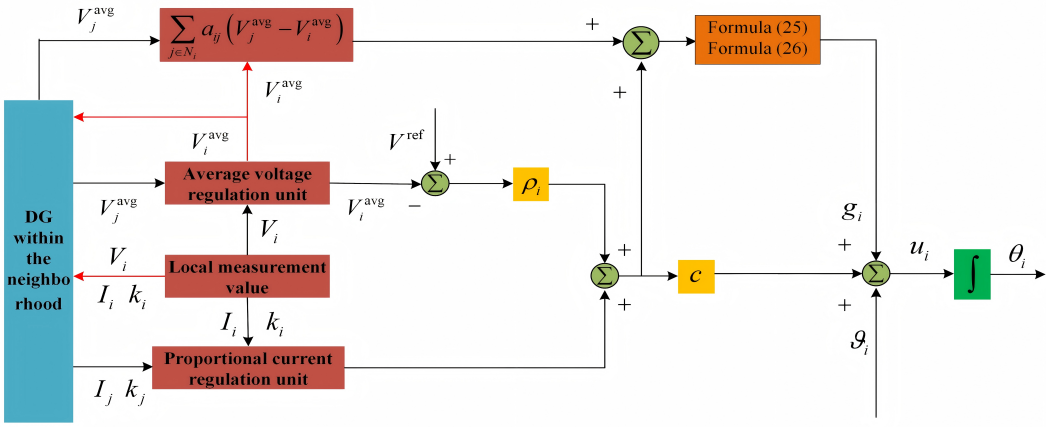


Figure 4. Distributed resilient control.

For the convenience of subsequent analysis, define a new variable z_i as:

$$z_i=\sum_{j\in N_i} a_{ij}(\sigma_j-\sigma_i)+\rho_i(\sigma^{\mathrm{ref}}-\sigma_i). \tag{24}$$

In Figure 4, ϑ_i denotes the time-varying FDI attack, $g_i(t)$ denotes the compensation term, and $g_i(t)$ is designed as:

$$g_i(t)=-\frac{z_i(t)}{\|z_i(t)\|}\hat{\vartheta}_i(t), \tag{25}$$

where $\hat{\vartheta}_i(t)$ denotes a dynamic term determined by the differential equation in (26):

$$\frac{\mathrm{d}}{\mathrm{d}t}\hat{\vartheta}_i(t)=\gamma_i\left[\|z_i(t)\|-\omega\hat{\vartheta}_i(t)\right], \tag{26}$$

in which γ_i and ω are both positive constants.

Under the joint action of the compensation term $g_i(t)$ and the time-varying FDI attack signal $\vartheta_i(t)$, u_i can be expressed as

$$\begin{aligned} u_i &= c\Big[\rho_i(V^{\text{ref}} - V_i^{\text{avg}}) + \sum_{j\in N_i} a_{ij}(k_j I_j - k_i I_i)\Big] + \vartheta_i(t) + g_i(t) \\ &= cz_i + \vartheta_i(t) + g_i(t). \end{aligned} \tag{27}$$

Considering the time-varying FDI attack, the error e_i can be expressed as

$$\dot{e}_i = -c\Big[\sum_{j\in N_i} a_{ij}(e_i - e_j) + \rho_i e_i\Big] + \vartheta_i. \tag{28}$$

By using the compensation term $g_i(t)$, (28) becomes

$$\dot{e}_i = -c\Big[\sum_{j\in N_i} a_{ij}(e_i - e_j) + \rho_i e_i\Big] + \vartheta_i + g_i. \tag{29}$$

Define vectors J and g as the vectors composed of the attack signal $\vartheta_i(t)$ and the compensation term g_i, respectively:

$$\begin{cases} J = [\vartheta_1, \vartheta_2, \ldots, \vartheta_N]^{\mathrm{T}}, \\ g = [g_1, g_2, \ldots, g_N]^{\mathrm{T}}. \end{cases} \tag{30}$$

Then (29) can be written as:

$$\dot{e} = -c(L + \rho)e + J + g = -cBe + J + g. \tag{31}$$

Assumption 1. *The time-varying FDI attack injected into the microgrid by the attacker is bounded, i.e.,*

$$|\vartheta_i(t)| \le \bar{\vartheta}_i, \tag{32}$$

where $\bar{\vartheta}_i$ denotes the upper bound of the time-varying FDI attack; that is, the absolute value of the FDI attack injected by the attacker into the microgrid is required to be less than this value.

Since the energy available for an attacker to inject FDI attacks is usually limited, this assumption is reasonable.

Remark 1. *The adaptive control scheme proposed in this paper requires that the injected false data injection attacks satisfy Assumption 1. If the injected attack signals are unbounded and may grow without bound, the presented control method may lose efficacy and fail to guarantee the achievement of the two control objectives as well as the stable operation of the microgrid.*

Theorem 1. *Assuming that the communication graph of the microgrid is undirected and connected, the compensation term shown in (25) can effectively mitigate the impact of bounded time-varying FDI attacks on the DC microgrid, and the two control objectives of voltage regulation and current sharing can be achieved.*

Proof. Choose the Lyapunov function as

$$W = e^{\mathrm{T}}Be + \sum_{i=1}^{N} \gamma_i^{-1}(\tilde{\vartheta}_i)^2, \tag{33}$$

where $\tilde{\vartheta}_i = \hat{\vartheta}_i - \bar{\vartheta}_i$.

Taking the derivative of (33) yields:

$$\begin{aligned} \dot{W} &= 2e^{\mathrm{T}}B\dot{e} + 2\sum_{i=1}^{N}\gamma_i^{-1}\tilde{\vartheta}_i\frac{\mathrm{d}}{\mathrm{d}t}(\tilde{\vartheta}_i) \\ &= -2c\, e^{\mathrm{T}}B\cdot Be + 2e^{\mathrm{T}}B(J+g) + 2\sum_{i=1}^{N}\gamma_i^{-1}\tilde{\vartheta}_i\frac{\mathrm{d}}{\mathrm{d}t}(\tilde{\vartheta}_i). \end{aligned} \tag{34}$$

Considering (25) and (26), we have

$$\begin{aligned} &2e^{\mathrm{T}}B(J+g) + 2\sum_{i=1}^{N}\gamma_i^{-1}\tilde{\vartheta}_i\frac{\mathrm{d}}{\mathrm{d}t}(\tilde{\vartheta}_i) \\ &\le 2\sum_{i=1}^{N}\Big[\|z_i\|\bar{\vartheta}_i + z_i g_i + \gamma_i^{-1}\tilde{\vartheta}_i\frac{\mathrm{d}}{\mathrm{d}t}(\tilde{\vartheta}_i)\Big] \\ &= 2\sum_{i=1}^{N}\Big(\|z_i\|\bar{\vartheta}_i - \|z_i\|\hat{\vartheta}_i + \tilde{\vartheta}_i\|z_i\| - \omega\tilde{\vartheta}_i\hat{\vartheta}_i\Big) \\ &\le \sum_{i=1}^{N}\Big[-\omega(\tilde{\vartheta}_i)^2 + \omega(\bar{\vartheta}_i)^2\Big]. \end{aligned} \tag{35}$$

Substituting (35) into (34), we obtain

$$\begin{aligned} \dot{W} &\le -2c\lambda_{\min}\, e^{\mathrm{T}}Be - \omega\sum_{i=1}^{N}(\tilde{\vartheta}_i)^2 + \omega\sum_{i=1}^{N}(\bar{\vartheta}_i)^2 \\ &\le -\alpha W + \beta, \end{aligned} \tag{36}$$

where $\alpha = \min\{2c\lambda_{\min}, \omega\gamma_i\}$, $\beta = \omega\sum_{i=1}^{N}(\bar{\vartheta}_i)^2$, and $\lambda_{\min}$ denotes the smallest eigenvalue of matrix B.

From (36) we have

$$W \le e^{-\alpha t}W(0) + \frac{\beta}{\alpha}(1 - e^{-\alpha t}). \tag{37}$$

Combining (33) and (37) gives

$$e^{\mathrm{T}}Be \le e^{-\alpha t}W(0) + \frac{\beta}{\alpha}(1 - e^{-\alpha t}). \tag{38}$$

Since $W(0) > 0$, $\alpha > 0$, and $\beta > 0$, we obtain

$$\|e\| \le \frac{1}{\lambda_{\min}}\Big[e^{-\alpha t}W(0) + \frac{\beta}{\alpha}(1 - e^{-\alpha t})\Big]^{1/2}. \tag{39}$$

Therefore, by appropriately choosing parameters α and β, $\|e\|$ can be made sufficiently small, i.e., e is uniformly bounded, so the difference between σ_i and σ^{ref} is sufficiently small. According to [27], if e is uniformly bounded, the microgrid can operate normally and stably under FDI attacks, and the two control objectives of voltage regulation and current sharing are not affected. □

Remark 2. *It can be observed from (39) that α appears in the denominator and β lies in the numerator, thus to make $\|e\|$ smaller, the controller gain c can be adjusted to be large enough such that $\alpha = \min\{2c\lambda_{\min}, \omega\gamma_i\}$ takes the value of $\omega\gamma_i$, and γ_i should be made as large as possible to minimize the ratio $\frac{\beta}{\alpha}$. In conclusion, it is required that the controller gain c be large enough, the adaptive parameter γ_i be as large as possible, and there are no special requirements for ω.*

Remark 3. *Based on the above analysis, it can be concluded that the resilient controller designed in this paper can effectively resist bounded time-varying false data injection attacks. Notably, Assumption 1 only imposes a boundedness constraint on the amplitude of FDIAs without any restriction on their frequency, whereby the controller remains effective in the presence of fast-varying FDI attacks.*

4. Simulation Analysis

In this section, MATLAB/Simulink (MATLAB R2022a) is used to verify the effectiveness of the proposed resilient control method. A multi-bus DC microgrid containing three distributed generators (DG1, DG2, DG3) is built in Simulink. The communication graph among the three DGs is shown in Figure 5, and the microgrid simulation parameters (same with [28]) are listed in Table 1. DG1 is set as the DG that can receive the nominal voltage, i.e., $\rho_1 = 1$, while the other two DGs cannot receive the nominal voltage. As illustrated in Figure 5, the three distributed generators (DGs) in the microgrid are interconnected to enable information interaction among neighboring agents, and when modeling their communication topology as a graph, the corresponding adjacency matrix, degree matrix, and Laplacian matrix are expressed as follows:

$$A = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}, D = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix}, L = \begin{bmatrix} 2 & -1 & -1 \\ -1 & 2 & -1 \\ -1 & -1 & 2 \end{bmatrix} \tag{40}$$

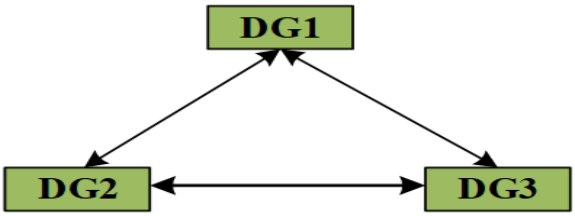


Figure 5. Communication diagram among DGs.

Table 1. Microgrid simulation parameters.

Parameter	Meaning	Unit	Value	Function
V_{in}	Input voltage	V	100	Provide step-down conversion for the base voltage
V^{ref}	Nominal voltage	V	48	Maintain stable electrical performance
f_{s}	Switching frequency	kHz	10	Govern the turn-on and turn-off of switching tubes
C_{f}	Filter capacitor	μF	2200	Filter out high-frequency noise
L_{f}	Filter inductor	mH	1.8	Smooth current and realize energy storage
$K_{\text{pv}}/K_{\text{ic}}$	Voltage loop PI coefficients	–	1/50	Detect and regulate current magnitude
$K_{\text{pc}}/K_{\text{ic}}$	Current loop PI coefficients	–	0.5/10	Guarantee stable and accurate output voltage
R_{i}	Line impedance	Ω	0.01	Serve circuit protection
R_{L1}	Load resistance	Ω	5	
k_i	Droop gain	–	3	

To verify the effectiveness of the distributed resilient control, two scenarios are tested in this paper: a single DG under FDI attack and all DGs under FDI attacks. First, it is verified that when there is no FDI attack, the resilient control does not affect the stable operation of the microgrid. The simulation lasts 8 s in total. Distributed secondary control is activated at $t = 0$ s. After the microgrid reaches steady state, the resilient control is activated at $t = 4$ s. Figure 6 shows the average voltage and output currents of the DGs. As shown in Figure 6, at the moment the resilient control is activated, the average voltage of the DGs experiences

a small fluctuation but quickly recovers to the nominal value. Since the droop gains of the three DGs are identical, the output currents should be equal, and indeed the output currents remain normal and stable under the resilient control. Therefore, the proposed resilient control does not interfere with the normal operation of the microgrid.

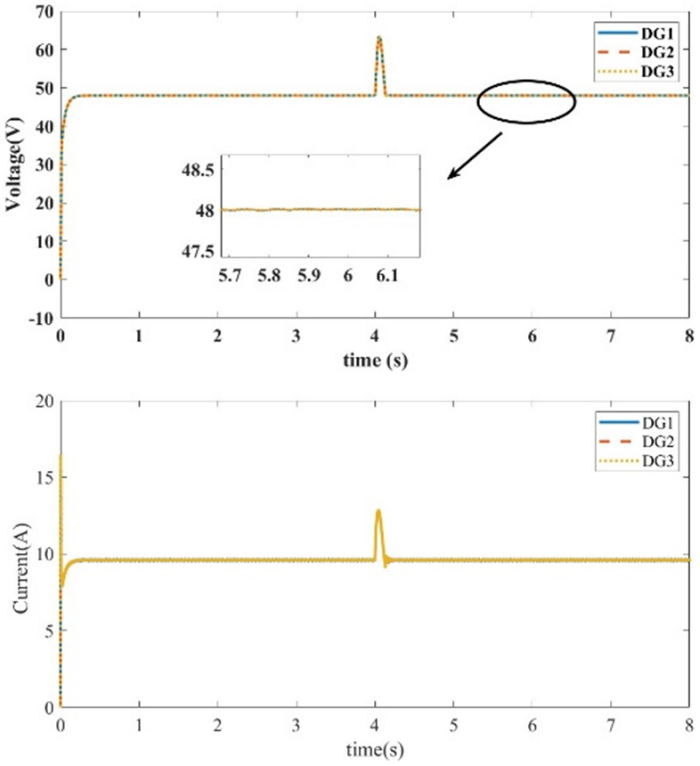


Figure 6. Average voltage and output current of DGs.

Next, the effectiveness of the resilient control is verified when a single DG is subjected to an FDI attack. DG1 is set as the target of the FDI attack. An arbitrary periodic function can be expanded into a sum of sinusoidal functions of different frequencies through Fourier series, so the simulated time-varying FDI attack signal is set as a sinusoidal signal. The simulation lasts 16 s. Distributed secondary control starts at $t = 0$ s. After the microgrid stabilizes, the resilient control is activated at $t = 4$ s. At $t = 8$ s, an FDI attack $20\sin(20\pi t)$ is injected; at $t = 12$ s, an FDI attack $50\sin(30\pi t)$ is injected. Figure 7 shows the average voltage and output currents of the DGs without resilient control. As can be seen, without resilient control, when FDI attacks are injected, the average voltage of the DGs deviates from the nominal value, and the output currents fluctuate more drastically. Figure 8 shows the average voltage and output currents when resilient control is present under a single DG FDI attack. As shown in Figure 8, under the action of resilient control, the deviation of the average voltage from the nominal value is greatly reduced, and the output currents are barely affected. Therefore, when a single DG is under FDI attack, the proposed resilient control can effectively mitigate its impact on the microgrid.

Finally, the effectiveness of the resilient control is verified when all DGs are under FDI attacks. The simulation lasts 16 s. Distributed secondary control starts at $t = 0$ s, resilient control is activated at $t = 4$ s. At $t = 8$ s, time-varying FDI attacks $20\sin(20\pi t)$, $100\sin(50\pi t)$, and $50\sin(30\pi t)$ are injected into the three DGs, respectively. At $t = 12$ s, time-varying FDI attacks $50\sin(30\pi t)$, $150\sin(20\pi t)$, and $100\sin(50\pi t)$ are injected into the three DGs, respectively. Figure 9 shows the average voltage and output currents without resilient control, and Figure 10 shows the results with resilient control. As shown in Figure 9, under FDI attacks, the output currents of the DGs cannot follow the predetermined ratio,

and the average voltage deviates from the nominal value by more than 0.5 V at $t = 8$ s and by more than 1 V at $t = 12$ s. As shown in Figure 10, with resilient control, the impact of FDI attacks is effectively mitigated; at $t = 8$ s and $t = 12$ s, the deviation of the average voltage from the nominal value is less than 0.5 V, the output currents are almost unaffected, and they can be shared according to the original ratio. Therefore, when all DGs are subjected to time-varying FDI attacks, the proposed resilient control can effectively mitigate their impact on the microgrid.

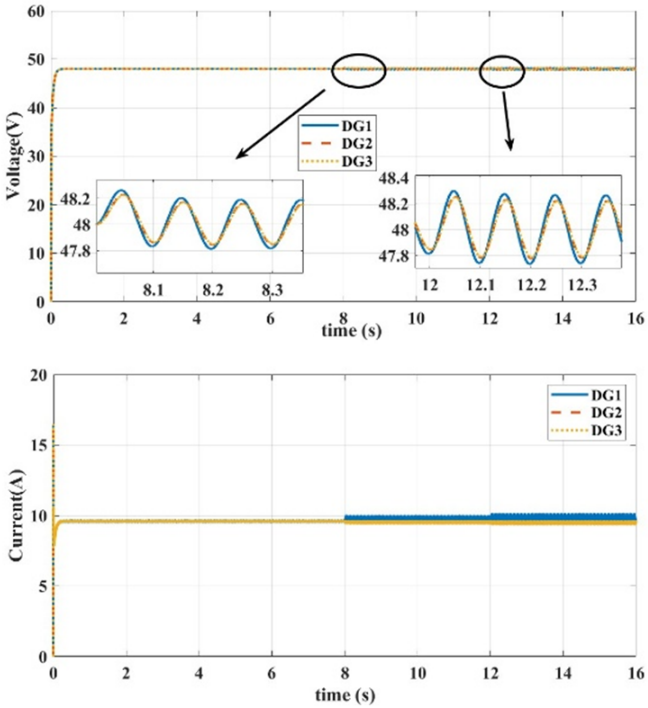


Figure 7. Average voltage and output current of DGs.

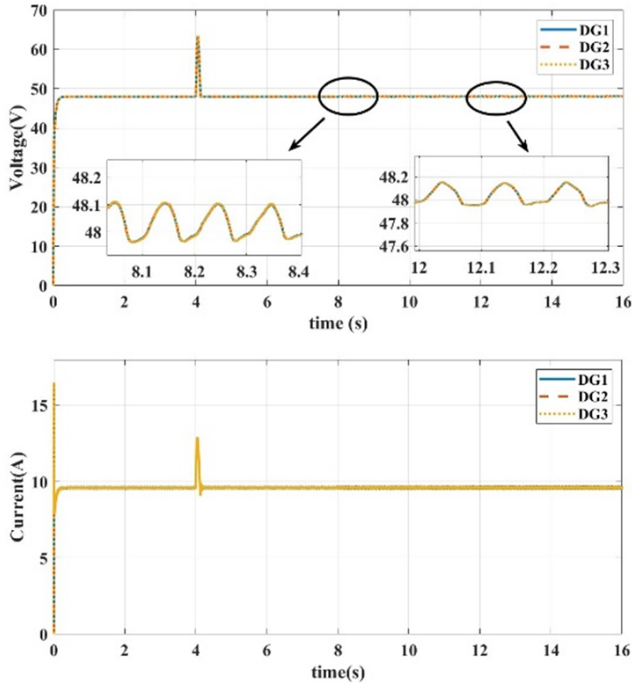


Figure 8. Average voltage and output current of DGs under resilient control.

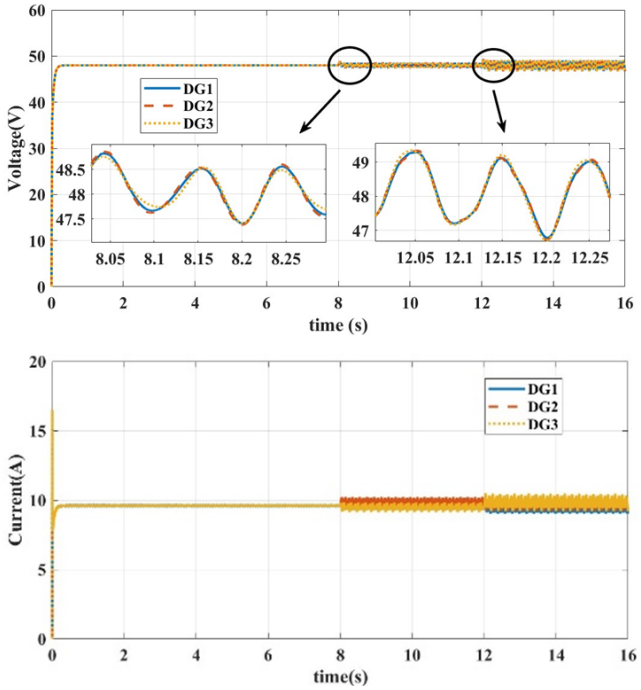


Figure 9. Average voltage and output current of DGs under distributed secondary control.

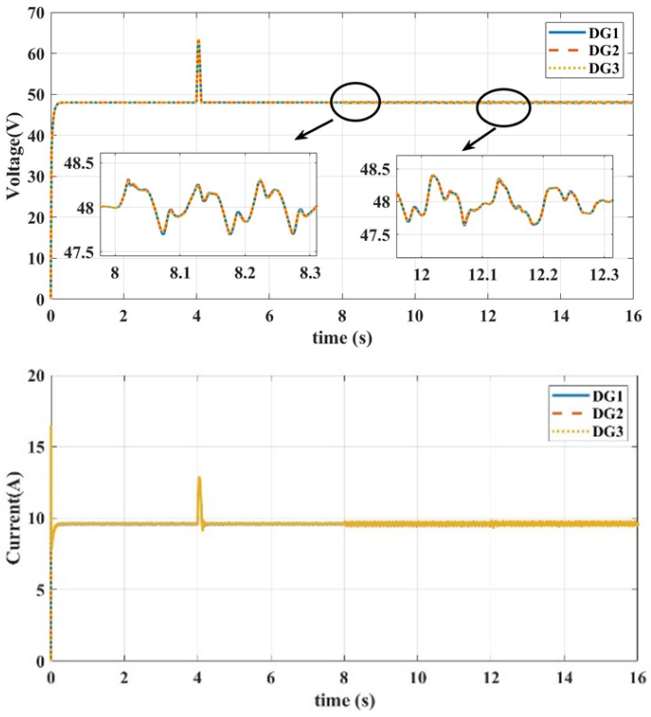


Figure 10. Average voltage and output current of DGs under resilient control.

5. Conclusions

This paper takes the multi-bus DC microgrid as the research object and proposes a resilient control method to resist time-varying FDI attacks. The resilient control method is introduced on the basis of distributed secondary control to mitigate the impact of time-varying FDI attacks on the microgrid. The feasibility of the proposed resilient control method is proved via Lyapunov stability theory, and its effectiveness is verified using MATLAB/Simulink. Simulation results show that the proposed resilient control method does not affect the normal operation of the microgrid system when there is no FDI attack.

When a single DG or all DGs are subjected to FDI attacks, the method effectively mitigates their impact on the microgrid, reduces the deviation of the average voltage from the nominal value, and keeps the output current sharing ratio essentially unchanged.

Author Contributions: Methodology, Z.X.; Software, Y.W.; Validation, Y.W.; Formal analysis, F.G.; Writing—original draft, Z.X.; Writing—review & editing, Z.G.; Funding acquisition, Z.G. and F.G. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the National Natural Science Foundation of China (62303101 and 62303100), the Natural Science Foundation of Hebei Province (F2023501001 and F2024501001), the Fundamental Research Funds for the Central Universities (2025GFYD005), and the Science and Technology Cooperation Special Project between Northeastern University and Shijiazhuang City (NEUS2025-01-005) (Corresponding author: Zhenyu Gao).

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Wang, Z.; Chen, Y.; Li, X. Coordinated control strategy for frequency deviation-free regulation of multiple VSGs in an island microgrid. *Power Syst. Prot. Control* **2024**, *52*, 12–23.
2. Chai, J.; Wang, M.; Xu, Z. A distributed event-triggered fixed-time secondary control for DC microgrids without continuous signal transmission. *IEEE J. Emerg. Sel. Top. Power Electron.* **2024**, *12*, 5123–5138.
3. Song, X.; Xu, Y.; Yuan, C.; Chen, Y.; Sun, S. Multi-storage SOC stabilization and equalization control strategy for islanded DC microgrids. *Power Syst. Prot. Control* **2024**, *52*, 49–59.
4. Avon, G.; Bucolo, M.; Buscarino, A.; Fortuna, L. Sensing frequency drifts: A lookup table approach. *IEEE Access* **2022**, *10*, 96249–96259. [CrossRef]
5. Nasirian, V.; Moayedi, S.; Davoudi, A.; Lewis, F.L. Distributed cooperative control of DC microgrids. *IEEE Trans. Power Electron.* **2015**, *30*, 2288–2303.
6. Jiang, Y.; Yang, Y.; Tan, S.; Hui, S.Y.R. Power loss minimization of parallel-connected distributed energy resources in DC microgrids using a distributed gradient algorithm-based hierarchical control. *IEEE Trans. Smart Grid* **2022**, *13*, 4538–4550.
7. Augustine, S.; Mishra, M.K.; Lakshminarasamma, N. Adaptive droop control strategy for load sharing and circulating current minimization in low-voltage standalone DC microgrid. *IEEE Trans. Sustain. Energy* **2015**, *6*, 132–141.
8. Cao, X.; Li, Z.; Cui, G. Distributed robust fixed-time secondary control of islanded microgrids. *Power Syst. Prot. Control* **2024**, *52*, 143–153.
9. Cucuzzella, M.; Trip, S.; Persis, C.D.; Cheng, X.; Ferrara, A.; van der Schaft, A. A robust consensus algorithm for current sharing and voltage regulation in DC microgrids. *IEEE Trans. Control Syst. Technol.* **2019**, *27*, 1583–1595.
10. Jiang, Y.; Yang, Y.; Tan, S.; Hui, S.Y.R. Distribution power loss mitigation of parallel-connected distributed energy resources in low-voltage DC microgrids using a Lagrange multiplier-based adaptive droop control. *IEEE Trans. Power Electron.* **2021**, *36*, 9105–9118.
11. Zhou, J.; Kim, S.; Zhang, H.; Sun, Q.; Han, R.R. Consensus-based distributed control for accurate reactive, harmonic, and imbalance power sharing in microgrids. *IEEE Trans. Smart Grid* **2018**, *9*, 2453–2467.
12. Khayat, Y.; Shafiee, Q.; Heydari, R.; Naderi, M.; Dragičević, T.; Simpson-Porco, J.W.; Dörfler, F.; Fathi, M.; Blaabjerg, F.; Guerrero, J.M.; et al. On the secondary control architectures of AC microgrid: An overview. *IEEE Trans. Power Electron.* **2020**, *35*, 6482–6500.
13. Liu, X.; Wang, S.; Chi, M.; Liu, Z.W.; Wang, Y.W. Resilient secondary control and stability analysis for DC microgrids under mixed cyber attacks. *IEEE Trans. Ind. Electron.* **2024**, *71*, 1938–1947.
14. Zhang, H.; Meng, W.C.; Qi, J.J.; Wang, X.; Zheng, W.X. Distributed load sharing under false data injection attack in an inverter-based microgrid. *IEEE Trans. Ind. Electron.* **2019**, *66*, 1543–1551.
15. Xie, X.-P.; Yang, F.-Y.; Wei, C. Joint design of FDI estimation and fuzzy control for DC microgrid under hybrid attacks. *Control Decis.* **2023**, *38*, 2335–2345.
16. Deng, C.; Guo, F.; Wen, C.; Yue, D.; Wang, Y. Distributed resilient secondary control for DC microgrids against heterogeneous communication delays and DoS attacks. *IEEE Trans. Ind. Electron.* **2022**, *69*, 11560–11568.
17. Yang, H.; Li, T.; Long, Y.; Xiao, Y. Event-triggered distributed secondary control with model-free predictive compensation in AC/DC networked microgrids under DoS attacks. *IEEE Trans. Cybern.* **2024**, *54*, 298–307. [PubMed]

18. Chen, Y.; Qi, D.; Dong, H.; Li, C.; Li, Z.; Zhang, J. A FDI attack-resilient distributed secondary control strategy for islanded microgrid. *IEEE Trans. Smart Grid* **2021**, *12*, 1929–1938.
19. Lian, Z.; Guo, F.; Wen, C.; Deng, C.; Lin, P. Distributed resilient optimal current sharing for an islanded DC microgrid under DoS attacks. *IEEE Trans. Smart Grid* **2021**, *12*, 4494–4505.
20. Sahoo, S.; Mishra, S.; Peng, J.; Dragičević, T. A stealth cyber-attack detection strategy for DC microgrid. *IEEE Trans. Power Electron.* **2019**, *34*, 8162–8174.
21. Tang, Z.; Kuijper, M.; Chong, M.S.; Mareels, I.; Leckie, C. Linear system security—Detection and correction of adversarial sensor attacks in the noise-free case. *Automatica* **2019**, *101*, 53–59.
22. Jin, X.; Haddad, W.M.; Yucelen, T. An adaptive control architecture for mitigating sensor and actuator attacks in cyber-physical systems. *IEEE Trans. Autom. Control* **2017**, *62*, 6058–6064. [CrossRef]
23. Liu, X.; Wen, C.; Xu, Q.; Wang, Y.W. Resilient control and analysis for DC microgrid system under DoS and impulsive FDI attacks. *IEEE Trans. Smart Grid* **2021**, *12*, 3742–3752.
24. Xie, Z.; Wu, Z. Distributed fault-tolerant secondary control for DC microgrids against false data injection attacks. *Int. J. Electr. Power Energy Syst.* **2023**, *144*, 108599.
25. Zhou, Q.; Shahidehpour, M.; Alabdulwahab, A.; Abusorrah, A. A cyber-attack resilient distributed control strategy in islanded microgrids. *IEEE Trans. Smart Grid* **2020**, *11*, 3690–3701. [CrossRef]
26. Zuo, S.; Altun, T.; Lewis, F.L.; Davoudi, A. Distributed resilient secondary control of DC microgrids against unbounded attacks. *IEEE Trans. Smart Grid* **2020**, *11*, 3850–3859. [CrossRef]
27. Zuo, S.; Davoudi, A.; Song, Y.; Lewis, F.L. Distributed finite-time voltage and frequency restoration in islanded AC microgrids. *IEEE Trans. Ind. Electron.* **2016**, *63*, 5988–5997. [CrossRef]
28. Guo, F.; Xu, Q.; Wen, C.; Wang, L.; Wang, P. Distributed secondary control for power allocation and voltage restoration in islanded DC microgrids. *IEEE Trans. Sustain. Energy* **2018**, *9*, 1857–1869. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.