Dynamic Defense Method Against Malicious Attacks for DC Microgrids

Zhixun Zhang, Jianqiang Hu, *Member, IEEE*, Jianquan Lu, *Senior Member, IEEE*, Josep M. Guerrero, *Fellow, IEEE*, and Jinde Cao, *Fellow, IEEE*

***Abstract*—DC microgrids can significantly benefit from the implementation of distributed communication and control, but these advancements also increase susceptibility to malicious attacks. To address these concerns, this article proposes a defense method to resist malicious attacks, including false data injection attacks (FDIAs) and denial-of-service (DoS) attacks. The proposed method includes two key strategies. To resist FDIAs, a strategy is employed that involves dynamically removing security data-assisted equivalence relations. The equivalence relations can detect FDIAs and compute mitigation vectors to eliminate their adverse effects. In addition, the dynamic removal of security data strategy reduces the computational burden and improves the computational efficiency of the dc microgrid. In response to DoS attacks, a weighted average estimation method is proposed. Subsequently, the estimated current values are transmitted to the controller to ensure the stability of the dc microgrid. Finally, simulation results on dc microgrid clusters demonstrate the validity of the proposed defense method.**

***Index Terms*—DC microgrids, denial-of-service (DoS) attacks, dynamic defense, false data injection attacks (FDIAs).**

NOMENCLATURE

A. Parameters of the DC Microgrids Model

T	Sampling time.
C_i	Capacitance of the buck converter.
L_i	Inductance of the buck converter.
R_i	Resistance of the buck converter.
$V_i(k)$	Output value of the voltage.
$I_i(k)$	Output value of the current.
R_{ij}	Resistance of the contact line of dc microgrids i and j.
L_{ij}	Inductance of the contact line of dc microgrids i and j.
$V_{ci}(k)$	Voltage command.
R_{Li}	Resistance load.
I_{Li}	Current load.
$\mathcal{N}_i$	Neighbor set of the ith dc microgrid.
I_{Ci}	Current sharing ratio of the ith dc microgrid.
V_i^{ref}	Reference voltage value of ith dc microgrid.
ν	Coefficient of the dc microgrid cluster.

B. Parameters of the Malicious Attacks and Defense Method

$\bar{f}$	Upper bound of the false data vector.
Φ_1	Sampling time of DoS attacks.
Φ_2	Normal sampling time.
Φ	Whole sampling time.
α, τ_D	Constant of DoS attacks.
r	Residual matrix.
H	Jacobian matrix of the dc microgrid.
L	Nominal values of the inductance.
C	Nominal values of the capacitance.
δ	Percentage deviation.
r_t^A	Residual threshold.
σ_r	Standard deviation of residual terms.
ζ_σ	Adjustment parameters of the confidence interval.
d	Upper limit of residual test data capacity.
$C_{\text{mem}}^{\max}$	Computational cost.
$C_{\text{mem}}^{\max}$	Memory usage.
μ, η	Weighting factors of dynamic data removal method.
ω	Weighting factor of CPSO algorithm.
n	Total number of weighting factor in the swarm.
c_1, c_2	Acceleration coefficients.
w	Inertia coefficient.
γ_1, γ_2	Uniformly distributed random numbers.

C. Abbreviation

DC	Direct current.
MG	Microgrid.
FDIAs	False data injection attacks.
DoS	Denial-of-service.
AC	Alternating current.
CPS	Cyber-physical systems.
MTD	Moving target defense.
CPSO	Cooperative particle swarm optimization.
RES	Renewable energy source.
ESS	Energy storage system.
PCC	Point of common coupling.

Received 18 November 2024; revised 25 January 2025; accepted 5 March 2025. Date of publication 11 March 2025; date of current version 14 April 2025. This work was supported in part by the Natural Science Foundation of Jiangsu Province under Grant BK20231416 and Grant BK20240009, in part by the National Natural Science Foundation of China under Grant 62373105, in part by the Jiangsu Provincial Scientific Research Center of Applied Mathematics under Grant BK20233002, and in part by the SEU Innovation Capability Enhancement Plan for Doctoral Students under Grant CXJH_SEU 24240. Recommended for publication by Associate Editor G.-S. Seo. *(Corresponding author: Jianqiang Hu.)*

Zhixun Zhang is with the School of Cyber Science and Engineering, Southeast University, Nanjing 210096, China (e-mail: zxzhangmw@seu.edu.cn).

Jianqiang Hu, Jianquan Lu, and Jinde Cao are with the School of Mathematics, Southeast University, Nanjing 211189, China (e-mail: jqhu@seu.edu.cn; jqluma@seu.edu.cn; jdcao@seu.edu.cn).

Josep M. Guerrero is with the Department of Energy Technology, Aalborg University, 9220 Aalborg, Denmark (e-mail: joz@et.aau.dk).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TPEL.2025.3550178.

Digital Object Identifier 10.1109/TPEL.2025.3550178

I. Introduction

UNDER the trend of vigorous development of renewable energy, microgrids have become a critical component of intelligent power systems due to their ability to effectively consume renewable energy sources [1]. Moreover, the large-scale distributed energy in microgrids can provide economic benefits and a reliable source of energy for load supply. There are two main types of microgrids: dc and ac. In a dc microgrid, the internal components, such as distributed energy, energy storage devices, and loads are connected to a dc bus, which makes the structure of a dc microgrid more efficient and concise compared to an ac microgrid where the internal components are connected to the bus through power electronics. Furthermore, in comparison to ac microgrids, dc microgrids operate with a unidirectional flow of power, eliminating the necessity for frequency and reactive power management, thus significantly streamlining reactive power management. This mode of operation simplifies the entire system, lowers operational expenses, and boosts overall efficiency and reliability [2], [3]. Therefore, the development of microgrids, especially dc microgrids, can contribute to the efficient and sustainable use of renewable energy sources.

Microgrids are modern CPS that heavily rely on advanced information and communication technologies to control and communicate with each other. However, this increased reliance on technology also elevates the risk of cyber attacks. For instance, in December 2015, the Ukrainian national power grid suffered from FDIAs, leading to extensive power outages throughout the country. Then, in March 2019, hackers exploited known vulnerabilities in Cisco firewalls to execute DoS attacks on an American renewable energy power company. These attacks inflicted considerable damage on the nation, including production interruptions, halted commercial activities, service disruptions, and significant economic losses [5], [6]. FDIAs are primarily utilized to inject false data into the microgrid to cause unstable deviations in voltage and proportional current sharing. Attackers target the link between sensors and the controller, as it is often the most vulnerable area with weak defense [7], [8]. On the other hand, DoS attacks disrupt the transmission of information, hindering the timely exchange of critical data between microgrid neighbors or sensors. This disruption can prevent the controller from making appropriate adjustments based on the corresponding information, leading to a significant impact on the stability of microgrid. DoS attacks often occur on the communication line between neighbors and can cause cascading failures of microgrid clusters [9]. Given the severe impact of FDIAs and DoS attacks on microgrids, it is crucial to address their security. By implementing appropriate security measures, microgrids can continue to provide reliable and efficient energy services while protecting against potential malicious attacks.

Considering the destructive nature of FDIAs and DoS attacks, as well as the reliability and efficiency of dc microgrids, extensive research has been dedicated to exploring protection measures for dc microgrids. First, countermeasures against FDIAs can be classified into the following four types.

1) Signal-based: The signal-based approach focuses on combating FDIAs by detecting signal characteristics and changes within the system [10], [11], [12].
2) Model-based: The model-based approaches are mainly defended by system modeling and parameter information, including static state estimation[13], dynamic state estimation [14], [15], observer-based [16], [17], [18], matrix separation [19], [20], and parity-based [21].
3) Data-driven: The data-driven approach is based on historical data and measurement data to develop protection strategies, including machine learning [22], [23], [24], [25] and reinforcement learning [26], [27].
4) MTD: The approach of MTD increases the difficulty and uncertainty of the attack mainly by adding controlled offsets and variations to the system [28], [29], [30].

Second, research on dc microgrids against DoS attacks, including resilient control based on new sampling period and communication mechanism [31], [32], [33], resilient controller based on consensus algorithms [34], controller based on control laws and attack parameters [35], event-triggered control [36], [37], [38], [39], an enhanced state estimation algorithm [40], and software defined network [41].

All the above studies are only for FDIAs or DoS attacks, but FDIAs combined with DoS attacks can cause vigorous serious impacts on microgrids. Considering the malicious attacks consisting of FDIAs and DoS attacks, some detection and countermeasures are proposed. In [42], a signal temporal logic-based method was proposed to detect and locate FDIAs and DoS attacks, and the damage level of the attacked part of the system was also determined. Hu et al. [43] proposed a segmented observer to estimate the system state under DoS attacks and the unknown FDIAs. In [44], a switching secondary controller based on current and voltage error was developed to recover the uniform current and voltage under FDIAs and DoS attacks. A parallel control network layer was suggested in [45], which can collaborate with the control network layer to resist FDIAs and DoS attacks. Chen et al. [46] proposed a resilient controller with compensation method, furthermore, the method can cope with unbounded FDIAs and DoS attacks without frequency information. In [47], a distributed event-triggered communication policy based on bandwidth allocation was proposed, which can maintain the normal allocation of bandwidth under FDIAs and DoS attacks. In [48], a three-stage defense framework is proposed where the resilient controller guarantees the communication of the system in the first stage. Then, the network partitioning problem caused by hybrid attacks is solved in the second stage based on software-defined networking, and the third stage based on local control.

However, most existing works on FDIAs focus only on detecting FDIAs and fail to provide corresponding protective measures. FDIAs can be easily concealed in hybrid attacks, rendering both signal-based detection and observer-based approaches insufficiently robust against stealthy FDIAs. Moreover, research on malicious attacks involving FDIAs and DoS attacks is still limited. Some of these methods may involve complex computations and algorithms, such as signal temporal logic [42]

or distributed event-triggered communication strategies [47]. This could result in high computational costs and delays in practical systems, particularly for large-scale microgrid systems. Furthermore, the literature mentions certain network-level strategies, such as parallel control network layers [45], [48], to counter attacks. However, these methods may require further research to ensure the resilience of the network. Specifically, for the network partitioning issues caused by FDIAs and DoS attacks, more comprehensive solutions are needed to ensure that the system can maintain normal communication and control after the attacks. For this reason, simpler and more efficient detection and countermeasures are preferable for addressing malicious attacks that include FDIAs and DoS attacks.

Motivated by the above discussions, this article proposes a lightweight countermeasure against malicious attacks that combine FDIAs and DoS attacks. First, this article utilizes an equivalence relation-based detection strategy, combined with a dynamic security data removal approach, to detect the presence of FDIAs in dc microgrids. This approach is designed to be robust against FDIAs, regardless of unknown system membership and parameter changes. In addition, if the amount of data in the equivalence relation exceeds the computational capacity of the dc microgrids, the dynamic security data removal approach removes the normal data from the previous m steps. This action alleviates the computational load on the dc microgrid, thereby enhancing detection efficiency. Once FDIAs are detected, mitigation vectors are computed using equivalence relations and then injected into the dc microgrids to counteract the negative impact of FDIAs. Second, a weighted average estimation method is proposed to estimate the current value that cannot be transmitted during the DoS attack period. The weighting factor is obtained using the CPSO algorithm. The historical data of the past k steps are combined with the optimized weighting factor to estimate the optimal current value, and then the optimal voltage value is calculated and transmitted to the controller based on the current sharing error. This ensures the safe operation of the dc microgrid. Finally, this article verifies the effectiveness of the counteracting malicious attacks method in the dc microgrid cluster. The main contributions of this article are as follows.

1) An equivalence relation-based strategy is employed to against FDIAs, which is robust to false data and can avoid the interference of other data and parameters. In addition, the proposed method calculates mitigation vectors based on the equivalence relation, which effectively counteracts the negative effects of FDIAs.
2) A dynamic security data removal approach is proposed to alleviate the computational and memory burden of the dc microgrid. By selectively removing security data from the equivalence relation based on the system-set threshold, this approach significantly improves the efficiency of the countermeasure against FDIAs.
3) A weighted average estimation method is developed to compensate for the missing control information during the DoS attack period. The weighting factor is optimized through the CPSO method, ensuring that the final estimated control value is optimal.

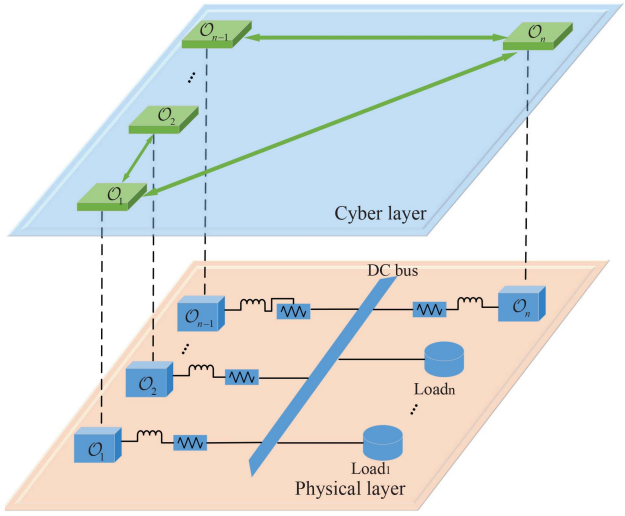


Fig. 1. DC microgrid cluster.

The rest of this article is organized as follows. Section II illustrates the dc microgrid and its control objects. Section III introduces the malicious attacks and the countermeasure strategy. Section IV presents the simulation results of the proposed strategy. Discussions on the proposed countermeasure strategy is provided in Section V. Finally, Section VI concludes this article.

II. DC Microgrids Model

A. Graph Theory

The dc microgrid forms a cluster with other dc microgrids through interconnection lines that include the resistance and inductance. Suppose there is a microgrid cluster consisting of N dc microgrids, and the dc microgrid in the microgrid cluster communicates with their neighbors through a communication network, which can be defined as an undirected graph $G = \{\mathcal{O}, \varepsilon, A\}$, where $\mathcal{O} = \{1, 2, \ldots, N\}$ is the set of dc microgrids, $\varepsilon = \mathcal{O} \times \mathcal{O}$ is the set of communication links, and $A = [a_{ij}] \in R^{n\times n}$ is the adjacency matrix of the undirected graph. If dc microgrids i and j are connected, then $a_{ij} > 0$. Otherwise, $a_{ij} = 0$. The Laplacian matrix $L_{\mathrm{DC}} = [l_{ij}] \in R^{n\times n}$ is composed of $l_{ij} = -a_{ij}, i \neq j$, and $l_{ij} = \Sigma_{j=1}^{N} a_{ij}, i = j$. The illustration of the microgrid cluster is shown in Fig. 1.

B. Electrical Model of DC Microgrids

In this section, the dc microgrid's energy is primarily supplied by a combination of a RES system and an ESS. These systems are connected to the PCC bus via a buck converter. The PCC bus has a ZIP load, which includes a constant impedance load (Z), a constant current load (I), and a constant power load (P). The constant power load includes a constant negative impedance and a current load. To linearize the constant power load, the ZIP load can be modeled as an impedance load and a current load [49].

The model of the ith dc microgrid is shown in Fig. 2. The neighbor set of the ith dc microgrid can be defined as

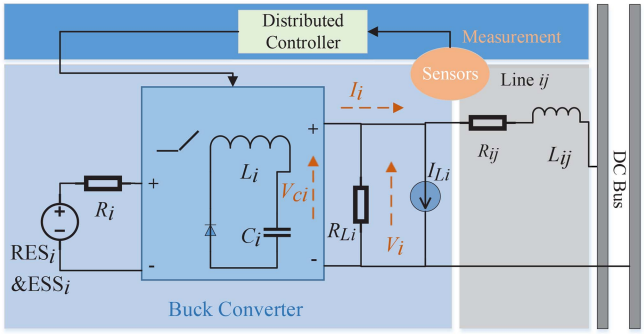


Fig. 2. DC microgrid model.

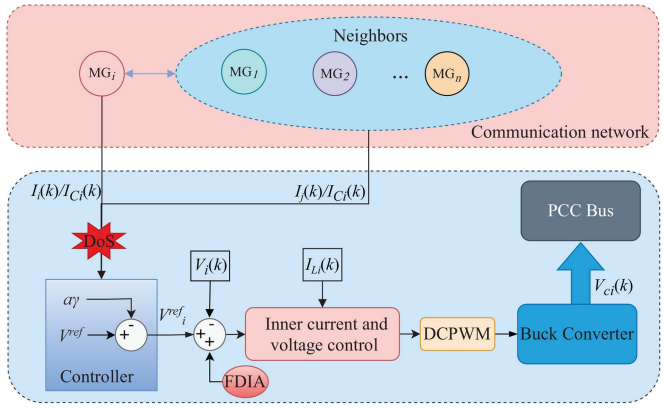


Fig. 3. Control model of dc microgrid.

$\mathcal{N}_i = \{j \in \mathcal{O} | i, j \in \varepsilon\}$. Since the local controller is implemented by a digital controller, the dynamic of the ith microgrid can be expressed as

$$\begin{cases} V_i(k+1) &= \left(1 - \frac{\lambda_1}{R_{Li}}\right) V_i(k) + \sum_{j \in N_i} \lambda_1 \left(\frac{V_j(k) - V_i(k)}{R_{ij}}\right) \\ &\quad + \lambda_1 I_i(k) - \lambda_1 I_{Li}(k) \\ I_i(k+1) &= \lambda_2 V_{ci}(k) + (1 - \lambda_2 R_i) I_i(k) - \lambda_2 V_i(k) \end{cases} \tag{1}$$

where $\lambda_1 = T/C_i, \lambda_2 = T/L_i$, T is the sampling time and C_i, L_i, and R_i are the capacitance, inductance, and the resistance of the buck converter; $V_i(k)$ and $I_i(k)$ are the output value of the voltage and current; R_{ij} and L_{ij} are the resistance and inductance of the contact line of dc microgrids i and j; $V_{ci}(k), R_{Li}$, and I_{Li} represent the voltage command, the resistance load, and the current load, respectively; $\mathcal{N}_i$ is the neighbor set of the ith dc microgrid.

C. System Model

According to the dynamic (1), the state space equation of the ith dc microgrid can be expressed as

$$\begin{cases} x_i(k+1) = A_i x_i(k) + B_i u_i(k) + M_i d_i(k) \\ y_i(k) = C_i x_i(k) \end{cases} \tag{2}$$

where $x_i(k) = [V_i(k), I_i(k)]^T$ is the state of the ith MG; $u_i(k) = [V_{ci}(k)]$ is the control input; $d_i(k) = [\sum_{j \in N_i}(V_j(k) - V_i(k))/R_{ij} - I_{Li}(k)]$ is the external disturbance including the coupling with the adjacent MG and the external input. According to the (1), the coefficient matrix of the ith MG can be shown:

$$\begin{aligned} A_i &= \begin{bmatrix} 1 - \frac{\lambda_1}{R_{Li}} & \lambda_1 \\ -\lambda_2 & 1 - \lambda_2 R_i \end{bmatrix}, \quad B_i = \begin{bmatrix} 0 \\ \lambda_2 \end{bmatrix}, \\ M_i &= \begin{bmatrix} \lambda_1, \\ 0 \end{bmatrix}, \quad C_i = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}. \end{aligned} \tag{3}$$

D. Control Model of DC Microgrids

In a dc microgrid cluster, two key performance indicators are accomplished to ensure its stability. First, the energy distribution within the dc microgrid is based on the rated power of the ZIP load. This measure prevents overloading of the local ZIP load and mitigates large-scale failures within the dc microgrid. Second, the bus voltage is kept consistent with the local busbar reference voltage to prevent voltage deviations that could lead to system instability. These two indicators can be expressed as

$$\begin{aligned} \frac{I_i(k)}{I_{Ci}} &= \frac{I_j(k)}{I_{Cj}}, \text{ for } \forall i, j \in \mathcal{O} \\ V_i(k+1) &= V_i^{\text{ref}}(k+1) \end{aligned} \tag{4}$$

where I_{Ci} is assigned according to the rated power of the ith dc microgrid and the load of each dc microgrid is proportional to the energy; V_i^{ref} is the reference voltage value of ith dc microgrid.

The control model of dc microgrid is shown in Fig. 3. A dc microgrid is a decentralized electricity group that can communicate with its neighboring grids through a communication network. This unique feature of the microgrid allows it to function autonomously in island mode while also working with the macro grid. By changing the modes, the microgrid provides security to the supply, and can transfer power between island and connected modes. Consider the ith dc microgrid as an illustration, it can transmit $I_i(k)/I_{Ci}$ to the neighboring jth dc microgrid while simultaneously receiving information $I_j(k)/I_{Cj}$ from the jth dc microgrid. According to the received information, the current proportional deviation of the dc microgrid is shown as follows:

$$\gamma_i(k) = \sum_{j \in N_i} a_{ij} \left(\frac{I_i(k)}{I_{Ci}} - \frac{I_j(k)}{I_{Cj}}\right). \tag{5}$$

Based on (4) and (5), the control algorithm for the ith dc microgrid can be expressed as

$$V_i(k+1) = V_i(k) - \nu \gamma_i(k) \tag{6}$$

where $\nu > 0$ is the coefficient of the dc microgrid cluster. With the adjustment of the controller and inner voltage and current controller, the voltage of the ith dc microgrid is equal to the reference voltage, and the current proportion deviation $\gamma_i(k)$ is finally restored to the normal value, which satisfies $\gamma_i(k) = 0$.

III. Malicious Attacks and Defense Method

In this section, FDIAs and DoS attacks are first introduced. Then, the corresponding defense strategies are developed for malicious attacks including FDIAs and DoS attacks in dc microgrids.

A. FDIAs and DoS Attacks

In this article, it is assumed that an attacker can access the communication network of the MG and then launch FDIAs or DoS attacks. As shown in Fig. 3, the value of $V_i(k)$ from the sensors may carry false data or fail to transmit after being attacked by the attacker.

FDIAs: Here, the false data vector injected by the FDIAs is defined as

$$V_i^{\text{FDI}}(k) = V_i(k) + F_i(k). \tag{7}$$

Then, the state space equations of the ith dc microgrid can be expressed as

$$\begin{cases} x_i(k+1) = A_i x_i(k) + B_i u_i(k) + M_i d_i(k) \\ y_i(k) = C_i x_i(k) + C_{ai} x_i^{\text{FDI}}(k) \end{cases} \tag{8}$$

where $C_{ai} = [1, 0]^T$ is the FDIA matrix and $x_i^{\text{FDI}}(k) = [F_i(k), 0]^T$ is the FDIA vector.

Assumption 1: The false data vector of FDIAs is upper bounded. If the false data vector $F_i(k) = [f_1, f_2, \ldots, f_n]^T$, then $\|f_i(k)\|_{\max} \leq \bar{f}$, which $\bar{f}$ is the upper bound of the false data vector.

DoS attacks: As shown in Fig. 3, the next sampling moment control output of the microgrid requires information from the previous sampling moment, which is transmitted over the communication network through the sensors. Under the DoS attacks, the communication channel is blocked during the sampling time, causing the information collected by the sensors about $I_i(k)/I_{Ci}$ and $I_j(k)/I_{Cj}$ to be untransmitted. The microgrid is unable to make the next instruction because of the missing information. The set of DoS attacks can be defined as

$$\Lambda_{\text{DoS}}(k) = \begin{cases} 1, \ k \in \Phi_1 \triangleq [k_{d1}, k_{d2}, \ldots, k_{dn}] \\ 0, \ k \in \Phi_2 \triangleq [k_{n1}, k_{n2}, \ldots, k_{nn}] \end{cases} \tag{9}$$

where Φ_1 represents the sampling time of DoS attacks; Φ_2 represents the normal sampling time. $\Phi = \Phi_1 \bigcup \Phi_2$ represents all the sampling time of the MG.

Assumption 2: DoS attacks are bounded in time and number.

1) The duration of DoS attacks are defined as T_D, which is less than the sampling time T of the dc microgrid, and can be represented as $T_D < T$.
2) The number of DoS attacks condition satisfy

$$|n(k)| \leq \alpha + \frac{T_D}{\tau_D} \tag{10}$$

where $|n(k)|$ represents the number of DoS attacks in the sampling time, the constants $\alpha \geq 0, \tau_D > 0$.

Remark 1: In practice, from an attacker's standpoint, the constraints on energy and resources make it impractical to sustain a continuous barrage of attacks. Conversely, from the viewpoint of a system controller, if there were no limits on the duration and frequency of attacks, perpetual assaults would make achieving control unattainable and threaten the system's stability. Therefore, it is essential to implement limits on the duration and number of DoS attacks. Assumption 2 gives limits on the duration and number of DoS attacks, which below T and $\alpha + T_D/\tau_D$. These limits are also easy to implement, such as existing low-pass filtering and diffusion techniques. It is important to note that these limits may vary based on the workload and severity of the DoS attacks.

B. Strategy to Resist FDIAs

In the defense strategy against FDIAs. First, an equivalence relationship between dc microgrid inputs and outputs in the past m steps is established to detect and defend against FDIAs. Then, residual terms are generated based on the relationship between outputs and inputs, and the sensitivity of the residual terms to the attack vector is increased through optimization to ensure that the detection attack is not affected by perturbation terms. Second, the mitigation vectors are calculated to counteract the false data vector when FDIA is detected, and the negative impact of FDIA is eliminated. Finally, a dynamic security data removal strategy is proposed to improve the computational efficiency of the equivalence relation and reduce the burden of the dc Microgrids.

The output $y(k)$ of the dc microgrid in the past m steps is expressed as

$$\begin{aligned} k = 0 : y(0) &= cx(0) + cx^{\text{FDI}}(0) \\ k = 1 : y(1) &= C[Ax(0) + Bu(0) + Md(0)] + Cx^{\text{FDI}}(1) \\ k = 2 : y(2) &= C[Ax(1) + Bu(1) + Md(1)] + Cx^{\text{FDI}}(2) \\ &= CA^2x(0) + CABu(0) + CAMd(0) \\ &\quad + CBu(1) + CMd(1) + Cx^{\text{FDI}}(2) \\ &\ldots \\ k = m : y(m) &= CA^m x(0) + \sum_{i=0}^{m-1} CA^{m-1-i}[Bu(i) + Md(i)] \\ &\quad + Cx^{FDI}(m). \end{aligned} \tag{11}$$

The output of the system at the last m steps can be written in the form of a vector matrix, which can be shown as

$$Y(m) = Nx(0) + PU(m) + RD(m) + SX^{\text{FDI}}(m) \tag{12}$$

where $Y(m), U(m), D(m),$ and $X^{\text{FDI}}(m)$ are the data for the last m steps. The coefficient matrices N, P, R, S are presented in Appendix.

Remark 2: The dc microgrid system proposed in this article is completely observable, and the initial state value $x(0)$ of the system can be determined from the corresponding output value $y(m)$ of the system within a finite iteration step. In addition, the dc microgrid of nonsublinear equations determined by (12) has a unique solution satisfying $rank(N) = 2(m+1)$.

According to (12), the residual utilized to detect FDIAs can be defined as

$$\begin{aligned} r(m) &= r^T \left(Y(m) - HU(m)\right) \\ &= r^T (Nx(0) + (P - H)\, U(m) \\ &\quad + RD(m) + SX^{\text{FDI}}(m)) \\ &= r^T \left(VQ(m) + SX^{\text{FDI}}(m)\right) \end{aligned} \tag{13}$$

where r is the residual matrix; H is the Jacobian matrix of the dc microgrid; $V, Q(m)$ are as follows:

$$V = [N, P - H, R] \in \mathbb{R}^{[2(m+1)]\times[2(m+2)]}$$
$$Q(m) = [x(0), U(m), D(m)].$$

In order to make the residual term sensitive only to the attack vector, The residual matrix r^T should be designed to be insensitive to noise or disturbances in the system, meaning it should satisfy $r^T V Q(m) = 0$. However, the reality is that it is difficult to make the $r^T V Q(m) = 0$, so the optimization problem can be described as

$$\begin{aligned} &\min \left(r^T V Q(m)\right) \\ \text{s.t.}\quad &L - \delta L \le L_i \le L + \delta L \\ &C - \delta C \le C_i \le C + \delta C \end{aligned} \tag{14}$$

where L and C are the nominal values of the inductance and capacitance of the dc buck converter, and δ is the percentage deviation.

Remark 3: In the dc microgrid, the parameters of the LC filter in the dc buck converter may change in a small range. Considering the impact of the unknown variation on the residual term, the deviation value δ is set to $\pm 5\%$, and the residual matrix that minimizes the unknown perturbation is obtained by taking different values in this parameter range to achieve the optimization goal.

To more accurately detect FDIAs in dc microgrids, the residual threshold is established based on residual terms $r^T V Q(m)$ under no attack. First, collect the past N sets of residual terms $r_r = \{r_{r1}, r_{r2}, \ldots, r_{rn}\}$. The residual threshold can be calculated using the average of historical states and a bias term, which can be expressed

$$r_t^A = \frac{1}{N}\sum_{k=1}^{N}(r_{rk}) + \sigma_r \zeta_\sigma \tag{15}$$

where σ_r is the standard deviation and ζ_σ is the adjustment parameters of the confidence interval. By adjusting the confidence interval using the standard deviation σ_r and adjust parameter ζ_σ, the method gains better adaptability, allowing it to flexibly address various dc microgrid environments or monitoring requirements. This enhances the reliability and robustness of detection.

When the residual value exceeds the threshold r_t^A set by the dc microgrid, the mitigation vector is computed to offset the false data vectors. The mitigation vector can be expressed as

$$Z(m) = S^{-1}\left(Nx(0) + PU(m) + RD(m) - Y(m)\right) \tag{16}$$

where $Z(m) = [z(0), z(1), z(2), \ldots, z(m)]^T$ is the mitigation vector. By injecting the mitigation vector into the dc microgrid, the output state $y_i(k)$ can be expressed as

$$y_i(k) = C_i x_i(k) + C_{ai}\left(x_i^{FDI}(k) + z_i(k)\right). \tag{17}$$

The mitigation vector can make $x_i^{\text{FDI}}(k) + z_i(k) = 0$. Therefore, the negative impact from the false data is eliminated, and the mitigation and resistance to the FDIAs can be achieved by the residual test and the mitigation vector.

In addition, considering the memory capacity and the computational burden of the dc microgrid, a dynamic security data removal strategy is proposed by setting an upper limit of residual test data capacity d. If $m > d$, the residual terms that do not exceed the residual threshold in the past m steps will be defined as safety data, while the safe data will not be utilized for the computation of the residual test. By the dynamic data removal method, not only the storage and computational burden of the dc microgrid can be relieved, but also the FDIAs can be accurately detected. Define the set of safety data $s = [1, 2, \ldots, s]$, $r(c)$ is the residuals after removing the safety data, and $r(c) \cup r(s) = r(m)$. The residuals with dynamically removed data can be expressed as

$$r(c) = r^T\left(VQ(c) + SX^{\text{FDI}}(c)\right), c \le d. \tag{18}$$

Finally, we rigorously analyze the selection of historical data steps m and dynamic data removal threshold d to balance detection accuracy, computational efficiency, and memory usage in microgrid anomaly detection systems. The historical data steps m is optimized by maximizing detection performance $A(m)$, subject to constraints on computational cost $C_{\text{comp}}(m) \le C_{\text{comp}}^{\max}$ and memory usage $C_{\text{mem}}(m) \le C_{\text{mem}}^{\max}$, which can be expressed

$$\begin{aligned} &\max\left[A(m)\right] \\ \text{s.t.}\quad &C_{\text{comp}}(m) \le C_{\text{comp}}^{\max} \\ &C_{\text{mem}}(m) \le C_{\text{mem}}^{\max} \end{aligned} \tag{19}$$

where $C_{\text{comp}}^{\max}$ and $C_{\text{mem}}^{\max}$ are the maximum computational and memory capacities the microgrid's controller can handle without jeopardizing its real-time performance.

Similarly, the dynamic data removal threshold d defines the upper limit of retained safe data, balancing algorithm efficiency $Q(d)$ and the dc microgrid robustness $R(d)$ through a multiobjective optimization problem

$$\begin{aligned} &\max\left[\mu Q(d) + \eta R(d)\right] \\ \text{s.t.}\quad &d \ge m \end{aligned} \tag{20}$$

where μ and η are weights that prioritize either memory efficiency $Q(d)$ or the dc microgrid robustness $R(d)$, respectively. $Q(d) = 1/T_m(d)$ measures the execution efficiency in countering FDIAs when the dc microgrid is allowed to retain up to d safe data points in its secure data pool, where $T_m(d)$ represents the time required to mitigate FDIAs. Meanwhile, Robustness $R(d)$ is quantified as the detection performance $A(d)$, which captures the system's ability to withstand FDIAs.

Remark 4: The larger the value of m, the more historical data are required, which improves estimation accuracy. However, excessive historical data can burden the microgrid's computing and storage capabilities. Therefore, m should be selected based on the scale of the microgrid. The most suitable value of m is the one that ensures the highest accuracy in detecting FDIAs while maintaining the necessary computing and storage capabilities for the microgrid's normal operation. The value of d is the critical threshold that affects the normal operation of the microgrid. If the chosen step size is $d + 1$, the operation of the microgrid will be impacted. In summary, the selection of m and d should be

Algorithm 1: Detection and Mitigation Method for FDIAs.

Input: System output $Y(m)$ and input $u(m)$ in the past m steps.
Create residual term:
$r(m) = r^T(VQ(m) + SX^{FDI}(m))$.
Minimize the vectors in the residual term unrelated to FDIA by optimizing problem (14).
Determine the presence of FDIAs by the residual term.
if FDIAs are detected
Calculate the mitigation vector $z(k)$ to offset the false data vector.
end if
if $m > d$
Adopt dynamic data removal method to remove the safety data from the residuals.
end if
Output: FDIAs are detected and mitigated.

determined based on the scale of the microgrid. The appropriate values should be chosen to ensure the highest accuracy in detecting FDIAs while maintaining the normal operation of the microgrid.

In this section, a methodology to detect and mitigate FDIAs in the dc microgrid is proposed. Initially, a residual test is used to detect the presence of FDIAs in the microgrid. If an attack is detected, mitigation vectors are employed to offset the presence of false data vectors and protect the dc microgrid from FDIAs. Furthermore, to enhance the computational efficiency of the residual test, we propose a dynamic security data removal strategy that reduces the computational and memory burden of the dc microgrid. The detection and mitigation method for FDIAs are summarized in an algorithm provided as follows.

C. Strategy Against DoS Attacks

In this article, the transmission lines of current proportional sharing cannot transmitted to the controller due to DoS attacks, which affects the regulation signal of the controller, therefore, a strategy based on weighted average estimated current is proposed to resist DoS attacks in this section.

Consider the ith dc microgrid, which is assumed to be subject to a DoS attack at step k, the DoS attacks in this article primarily target the proportional current sharing channels within the dc microgrid. Attackers exploit by sending a large number of invalid or malicious requests to consume the resources of the target dc microgrid, resulting in the blocking of the proportional current sharing channels. Consequently, the controller is unable to receive proportional current sharing information from both local and neighboring dc microgrids. First, the current history data for the past $k-m$ sampling periods are selected. Then, weights are assigned to the current of each period worth to the weighted average estimated current. Finally, the current of the ith dc microgrid at k sampling periods can be expressed as

$$\bar{I}_i(k) = \omega_{k-m} I_i(k-m) + \omega_{k-m+1} I_i(k-m+1) + \cdots + \omega_{k-1} I_i(k-1) \tag{21}$$

where ω is the weighting factor, which satisfies $\omega_{k-m} + \omega_{k-m+1} + \cdots + \omega_{k-1} = 1$. Based on the estimated current values, the estimated current proportional deviation can be obtained as

$$\bar{\gamma}_i(k) = \sum_{j \in N_i} a_{ij} \left(\frac{\bar{I}_i(k)}{I_{Ci}} - \frac{\bar{I}_j(k)}{I_{Cj}} \right). \tag{22}$$

Based on (21) and (22), the control algorithm for the ith dc microgrid under DoS attacks can be expressed as

$$\bar{V}_i(k+1) = V_i(k) - a\bar{\gamma}_i(k). \tag{23}$$

In order to make the estimated control input more accurate, the weighting factors need to be optimized to minimize the error between the estimated voltage values and the reference voltage values of the dc microgrid, the optimization problem can be expressed as

$$\begin{aligned} &\min ||V_i^{\text{ref}}(k+1) - \bar{V}_i(k+1)|| \\ &\text{s.t.} \quad 0 < \omega_{k-m}, \omega_{k-m+1}, \ldots, \omega_{k-1} < 1. \end{aligned} \tag{24}$$

Inspired by [50], a CPSO algorithm can be utilized to solve the optimization problem (24), where each microgrid is considered as a cluster. The optimization objective of all microgrids is achieved by the optimization of each cluster. Defining the swarms $P_i, i = 1, 2, \ldots, n$, where i is the total number of swarms

$$P_i = \{\omega_1, \omega_2, \ldots, \omega_n\} \tag{25}$$

where n is the total number of weighting factor in the swarm P_i, and the velocity and position of the particle updates are as follows:

$$\begin{aligned} v_i(t+1) &= w \times v_i(t) + c_1 \times \gamma_1 \times \left[p_i^b(t) - p_i(t)\right] \\ &\quad + c_2 \times \gamma_2 \times \left[p_i^{gb}(t) - p_i(t)\right] \\ p_i(t+1) &= p_i(t) + v_i(t+1) \end{aligned} \tag{26}$$

where c_1 and c_2 are acceleration coefficients and w are inertia coefficient; $\gamma_1, \gamma_2 \in [0, 1]$ are uniformly distributed random numbers; $p_i^b(t)$ and $p_i^{gb}(t)$ denote the best personal position and the global best position of particle i at iteration t. The schematic diagram of the CPSO algorithm are shown in Fig. 4. First, initialize particles for all swarms at random positions, calculate their fitness, and set the global bests for each swarm. Then, the iteration loop and the swarm loop are started. Particles are reset and the stagnation criterion for the ith swarm is checked. The global best for the swarm is updated, followed by updating the velocity and position of s particles within the swarm. The optimization problem (24) is solved during the iteration loop, and finally, the control output is obtained.

The CPSO algorithm can minimize the error of the optimization problem and obtain the optimal estimated voltage value, which can be utilized to fill the voltage value of the dc microgrid subject to DoS attacks that cannot be calculated by the estimated voltage value $\bar{V}_i(k+1)$. In addition, CPSO algorithm can reduce the computational burden on the dc microgrids by calculating the weight values offline. This method can be a good

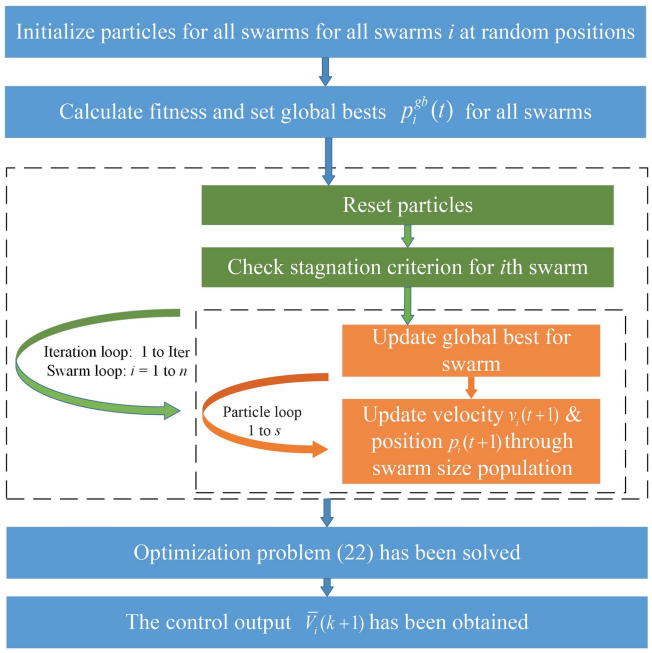


Fig. 4. Schematic diagram of the CPSO algorithm.

Algorithm 2: Strategy against DoS attacks.

1: **Input**: current $I_i(k)$ and $I_j(k)$ in the past $k-m$ steps.
2: Estimate the current $\bar{I}_i(k)$ and $\bar{I}_j(k)$ by (21).
3: Estimate the current proportional deviation $\bar{\gamma}_i(k)$ by (22).
4: Calculate the control output $\bar{V}_i(k+1)$ based on (21) and (22).
5: Improve the accuracy of the estimated voltage values through optimization problem (24).
6: Determine the presence of DoS attacks based on whether the proportional current sharing channels are maliciously blocked.
7: **if** DoS attacks are detected
8: Utilize estimated control output $\bar{V}_i(k+1)$ to issue commands to the DC microgrid.
9: **end if**
10: **Output**: DoS attacks are mitigated.

way to stabilize the dc microgrid and enhance the robustness of the dc microgrid against DoS attacks.

Fig. 5 presents a flowchart outlining a methodology for detecting and defending against malicious attacks in dc microgrids. The methodology utilizes equivalence relations to calculate optimal residuals, which can detect FDIAs by comparing them to predefined thresholds. The equivalence relations can also generate mitigation vectors that counteract the effects of FDIAs. To improve the effectiveness of this approach, a strategy based on dynamic removal of secure data are used to assist in removing the presence of FDIAs. On the other hand, the control information obtained through current estimation calculations and CPSO algorithm is leveraged to resist DoS attacks. Furthermore, by

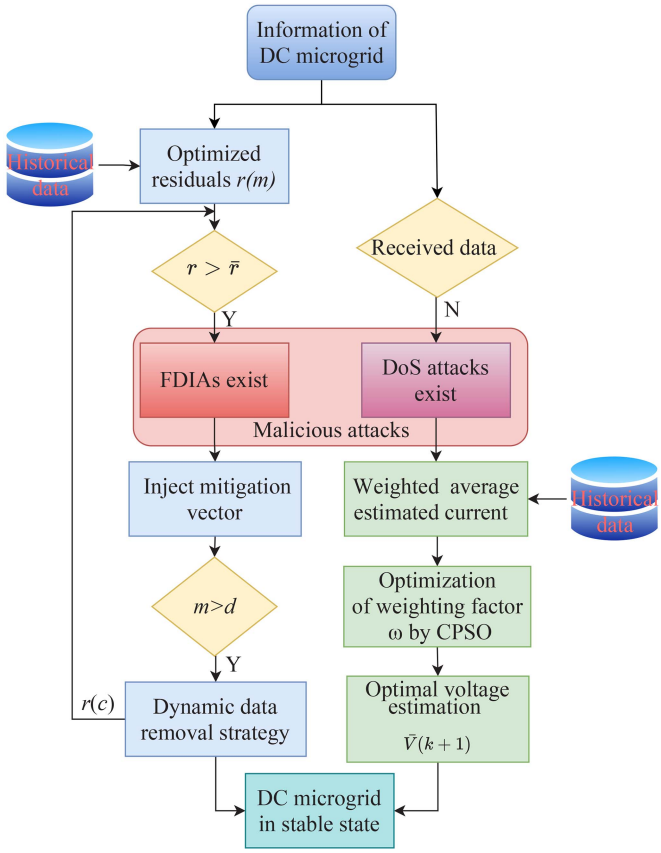


Fig. 5. Countermeasures against malicious attacks in dc microgrid.

utilizing the CPSO algorithm and the dynamic removal of security data, the computational demands placed on dc microgrids can be significantly decreased. This approach provides fast and effective detection and defense against malicious attacks, while maintaining computational efficiency.

IV. Validation Studies

A. *Effectiveness of the Dynamic Defense Method Against Malicious Attacks*

In this section, a dc microgrid cluster formed by four interconnected dc microgrids is utilized to verify our proposed defense method. This dc microgrid cluster is implemented in the Simpower System toolbox in Matlab/Simulink, and the simulation model is shown in Fig. 6. The parameter information of the dc microgrid cluster is shown in Table I. The RES is modeled as a photovoltaic panel with maximum power point tracking functionality. This photovoltaic panel consists of 12 series-connected solar cells, each with an open-circuit voltage of approximately 0.6 V. The photovoltaic panel is designed to supply power at a low voltage suitable for the system, specifically matching the reference voltage of 6 V used in the interconnected microgrid cluster.

Fig. 7 illustrates the injection time and data volume of FDIAs. In this article, the FDIAs occurs at the point where the controller sends instructions. The first attack injects a false data vector of

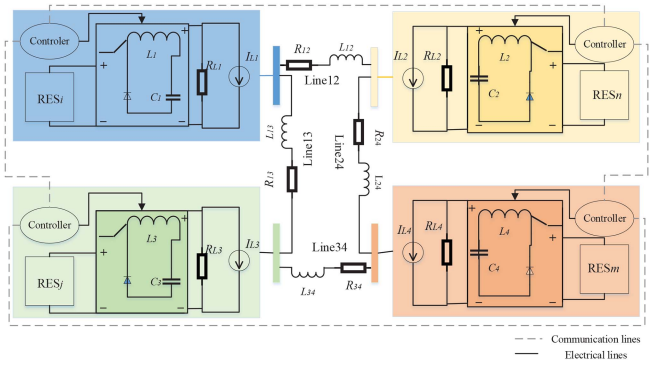


Fig. 6. Simulation model.

TABLE I
PARAMETERS CONFIGURATION

	Parameters	Value
Nominal voltage(V)	V^{ref}	6
The buck Converter	R_i, C_i, L_i	0.1 Ω, 1 mH, 100 μF
Rated Powers(A)	$I_{c1}, I_{c2}, I_{c3}, I_{c4}$	1/14, 1/14, 1/6, 1/6
Line resistance(Ω)	$R_{12}, R_{13}, R_{24}, R_{34}$	1,1,1,1
Line inductance(H)	$L_{12}, L_{13}, L_{24}, L_{34}$	0.1, 0.1, 0.05, 0.05
Impedance load(Ω)	$R_{L1}, R_{L2}, R_{L3}, R_{L4}$	0.1, 0.1, 0.05, 0.05
Current load(A)	$I_{L1}, I_{L2}, I_{L3}, I_{L4}$	0.1, 0.1, 0.05, 0.05
The Control Model	ν, T	0.05, 5×10^{-6}
The dynamic security data removal approach	d, m	15, 6
The weighted average estimation method	n, Iter, s	20, 30, 20
Communication Network	$a_{12}, a_{13}, a_{24}, a_{34}$	1, 1, 1, 1
The CPSO algorithm	n, Iter, s, c_1, c_2	50, 100, 25, 1.2, 1.2
Performance parameters	$C_{\text{comp}}^{\max}, C_{\text{mem}}^{\max}, \mu, \eta$	4ms, 100 kB, 0.5, 0.5

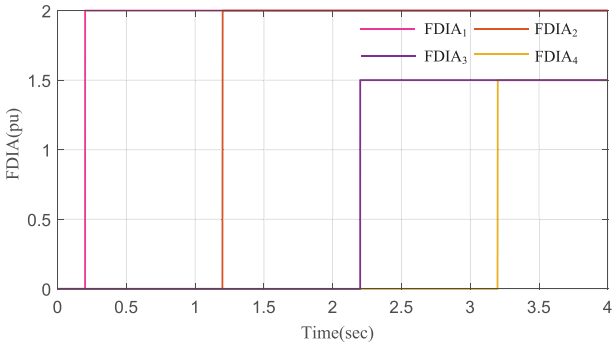


Fig. 7. FDIA vector.

2 p.u. into dc microgrid 1 at 0.2 s, and 2 p.u. of false data vector is injected into DC microgrid 2 at 1.2 s. At 2.2 s and 3.2 s, false data vectors of 1.5 p.u. are injected into dc microgrid 3 and dc microgrid 4, respectively. Fig. 8 shows the time and attack area of the DoS attacks. In this simulation, the communication channel of the first dc microgrid is occupied by the DoS attacks, and the duration and quantity of the DoS attacks satisfy the setting of Assumption 2.

Fig. 9 presents the results of the residual test in this article. Initially, random noise with a magnitude of $\sin(0.5t)$ p.u. was applied at 0.35 s, load changes were introduced at 0.5 and 1.5 s, and a small-scale false vector of 0.5 p.u. was injected at 2.02 s to assess the robustness of the residual test against other vector changes. The introduction of load variations and random noise

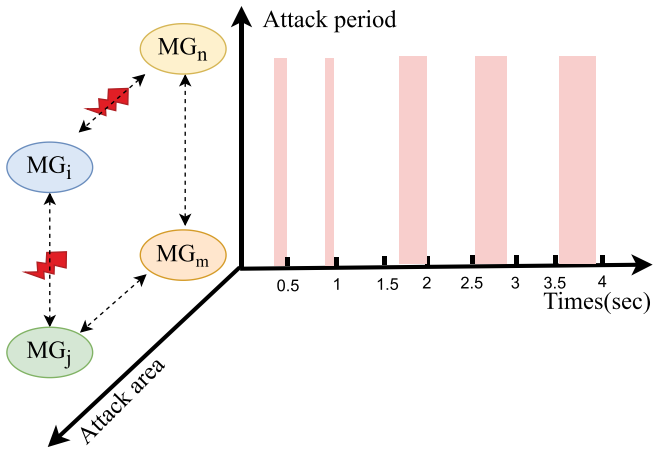


Fig. 8. Periods and areas of DoS attacks.

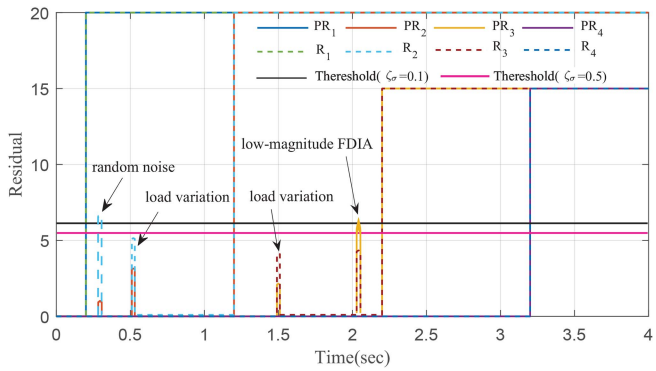


Fig. 9. Residual test. (PR_1, PR_2, PR_3, PR_4 are the proposed residual, R_1, R_2, R_3, R_4 are the traditional residual.).

is primarily intended to verify whether the proposed defense strategy might mistakenly classify normal system fluctuations as FDIAs. It can be observed that the proposed residual test in this article exhibits high sensitivity to FDIAs. In the presence of random noise and load changes, the residuals remain below the threshold, while the test is also capable of detecting low-magnitude FDIAs. In contrast, the traditional residual test falsely detects FDIAs in the presence of random noise, and load changes have a greater impact on it, with residuals approaching the threshold during the load changes at 0.5 and 1.5 s, while failing to detect small-scale FDIAs. Therefore, compared to the traditional residual test, the residual test proposed in this article has stronger robustness and is more sensitive in detecting FDIAs. Meanwhile, the adjustment parameter ζ_σ of the residual threshold is set to 0.5 and 1. As the adjustment parameter decreases, the confidence interval narrows. Therefore, the residual threshold with an adjustment parameter of 0.5 will be more stringent, leading to an increased probability of detecting FDIAs.

As shown in Fig. 10, without the defensive measures proposed in this article, the bus voltage values oscillate accordingly under both DoS attacks and FDIAs, and the voltage values of all four dc microgrids do not reach the rated voltage values at the end. The output current values are shown in Fig. 11, the current ratio is also affected by the malicious attacks, and finally the current ratio

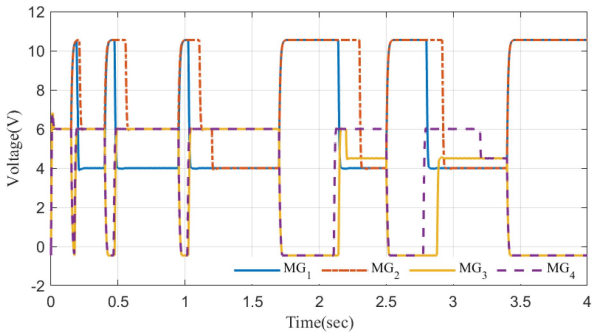


Fig. 10. Voltages of dc microgrid cluster under malicious attacks.

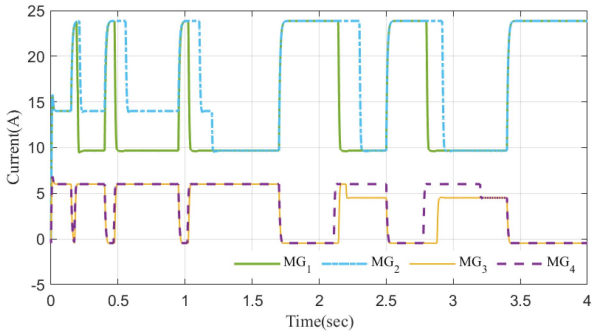


Fig. 11. Current outputs of dc microgrid cluster under malicious attacks.

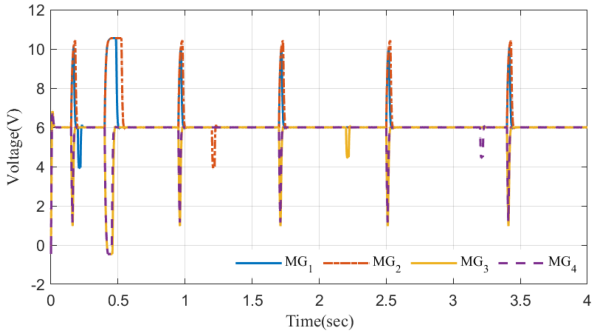


Fig. 12. Voltages of dc microgrid cluster with proposed countermeasures. The voltage in the normal state is 6 V.

does not reach the rated current value. Therefore, the malicious attacks cause large oscillations in the voltage and current of the microgrid, which has a great impact on the stability of the microgrid.

Figs. 12 and 13 show the output voltage and current values under the method proposed in this articke. During the FDIAs, the strategy based on equivalence relations and dynamic removal of security data reacts quickly to detect FDIAs and calculates mitigation vectors to eliminate their impact, with dynamic removal of security data parameters shown in Table I. When a DoS attack exists, a weighted average estimation method was utilized to obtain optimal voltage estimation using the CPSO optimization algorithm. This approach quickly compensated for the lack of voltage information during the attack. The statistical results for

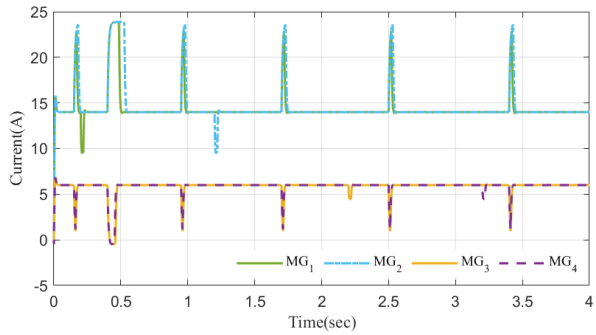


Fig. 13. Current outputs of dc microgrid cluster with proposed countermeasures. In the steady state, the current in $MG_{1/2}$ is 14 A, and the current in $MG_{3/4}$ is 6 A.

TABLE II
STATISTICAL RESULTS FOR VOLTAGE OBJECTIVE

	CPSO	RPCPSO	PSO	DPSO
Objective value average	0.5001	0.8214	0.9648	1.2853
Objective value standard deviation	0.0412	0.1623	0.2301	0.4962
Best objective value	0.4241	0.6453	0.7182	1.0639
Average function evaluations	4920	4810	5020	6140
Average Convergence Iterations	98	120	150	200
Estimated Accuracy	0.0050	0.0080	0.0100	0.0150

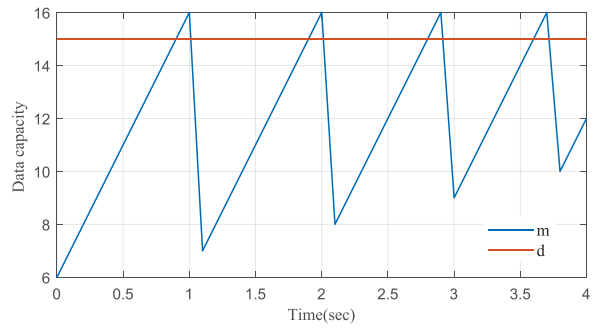


Fig. 14. Dynamic security data removal strategy.

voltage objective are presented in Table II, which depicts the mean, standard deviation, and optimal value of the objective function for 25 experiments, along with the average number of function estimates for four different methods, including CPSO, randomly partitioned CPSO (RPCPSO), PSO, and decentralized PSO (DPSO). From the table, it can be seen that CPSO performs better in several aspects. Its average objective value is 0.5001, significantly lower than RPCPSO, PSO, and DPSO, with reductions of 39%, 48%, and 61%, respectively, demonstrating its advantage in optimizing the objective. In addition, CPSO has the smallest standard deviation of the objective value, indicating more stable results. The average function evaluations and convergence iterations of CPSO are also relatively low, suggesting better computational load and convergence speed. Finally, CPSO shows the best performance in estimated accuracy, with a mean squared error of only 0.0050, further proving its accuracy advantage. Overall, CPSO has better performance and efficiency compared to the other methods.

Fig. 14 illustrates the effectiveness of the dynamic security data removal strategy. When $m > d$, the strategy quickly

TABLE III
MITIGATION PERFORMANCE OF THE PROPOSED FRAMEWORK

	Mitigation time(s)			Performance metrics		
	Min	Avg	Max	$Q(d)$	$R(d)$	A(m)
Without a dynamic security data removal strategy	0.0471	0.0632	0.0907	–	–	–
$\star$ With a dynamic security data removal strategy($m = 6, d = 15$)	0.0257	0.0336	0.0652	59.5	99.3%	97.6%
With a dynamic security data removal strategy($m = 10, d = 20$)	0.0352	0.0485	0.0811	41.2	99.6%	97.8%
With a dynamic security data removal strategy($m = 2, d = 11$)	0.0439	0.0572	0.0896	35.0	98.1%	96.2%

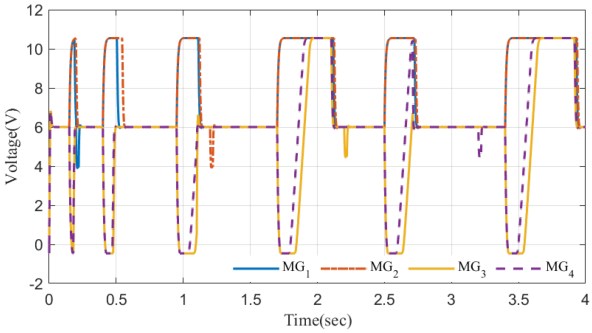


Fig. 15. Voltages of dc microgrid cluster with latest input method [51].

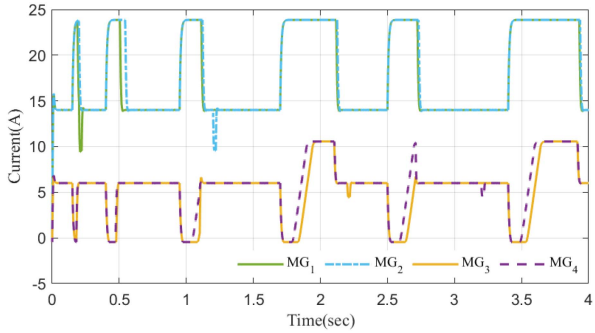


Fig. 16. Current outputs of dc microgrid cluster with latest input method [51].

removes the safety data, restoring the state to $m < d$ in the next step. This approach reduces the computational and storage burden on DC microgrids while ensuring the accuracy of FDIA detection. Table III illustrates the mitigation performance for the proposed framework when addressing both FDIAs and DoS attacks. The data indicates that the strategy effectively mitigates these attacks. With the assistance of the dynamic removal of security data strategy, the recovery time of dc microgrids under different parameter selections was tested. In the experiment with the initial values of $m = 6$ and $d = 15$, the shortest time for the dc microgrids to return to normal is 0.0257 s, with an average time of 0.0336 s and a maximum time of 0.0652 s, while achieving $Q(d) = 59.5s^{-1}$, $R(d) = 99.3\%$, and $A(m) = 97.6\%$. Without this strategy, the shortest recovery time is 0.0471 s, with an average time of 0.0632 s and a maximum time of 0.0907 s. These results show that the dynamic removal of security data strategy can reduce the microgrid's computational burden and accelerate the microgrid's recovery time. In addition, given that m remains within the dynamic data removal threshold d, it is progressively increased to enhance the detection performance $A(m)$. the values of $R(d)$ and $Q(d)$ enable the optimization problem (20) to reach its optimum. It provides an optimal solution that achieves a practical balance between execution efficiency and defense robustness, while staying within the system's computational cost and memory usage, ensuring optimal detection performance. Furthermore, the framework is capable of promptly responding to and mitigating the negative impacts of malicious attacks, thereby maintaining the stability of microgrids.

Figs 15 and 16 give the voltage and current outputs under the latest input method, to ensure a fair comparison, the method for countering FDIAs is the same as that proposed in this article. To ensure a fair comparison, the method for countering FDIAs is the same as that proposed in this article. It is evident that the utilization of the latest input method may lead to a temporary instability in voltage and current outputs, characterized by significant oscillations in both voltage and current. These oscillations cannot be swiftly corrected due to the diminished accuracy of voltage estimation during DoS attacks. This is a direct threat to the normal operation of the microgrid. On the contrary, the proposed weighted average estimation method combined with the CPSO optimisation algorithm can mitigate the oscillations caused by DoS attacks in a short period of time and guarantee the safe operation of the microgrid.

From the above, the effectiveness of the proposed method is verified as it can maintain the stability of dc microgrid clusters under DoS attacks and FDIAs, and both control objectives of the dc microgrid can be achieved under malicious attacks. When the proposed method detects FDIAs using the residual test, the corresponding mitigation vector value is calculated using the residual amount to offset the false data injection vector value. On the other hand, in the presence of DoS attacks, the voltage value can be estimated based on the estimated current proportional deviation to be used as the actual voltage value when the information cannot be transmitted, thus maintaining the stability of the dc microgrid cluster.

B. Scalability Test of the Proposed Dynamic Defense Method

To further demonstrate the scalability of our proposed dynamic defense method, a simulation model of ten interconnected microgrids is presented, as shown in Fig. 17. This simulation model operates at a rated voltage of 48 V, and the current sharing ratio $I_{C1} : I_{C2} : I_{C3} : I_{C4} : I_{C5} : I_{C6} : I_{C7} : I_{C8} : I_{C9} : I_{C10} = 4 : 3 : 2 : 1 : 4 : 3 : 2 : 1 : 1 : 1$. The attacker launches malicious attacks at 0.8 and 4 s, with a DoS attack blocking the communication links between microgrid 1 and its neighboring

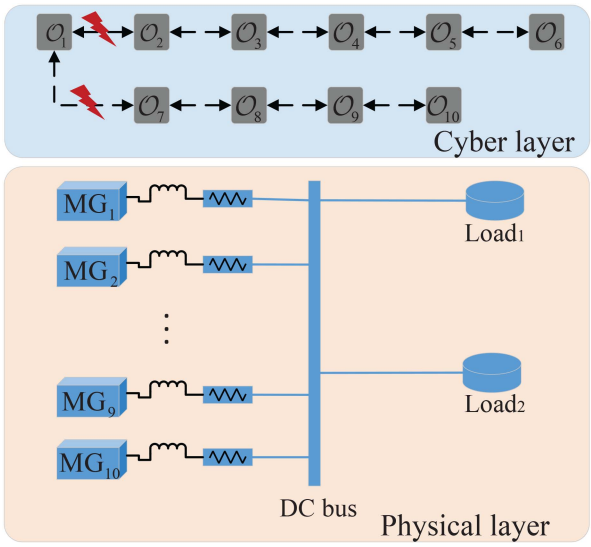


Fig. 17. Simulation model of ten interconnected MGs.

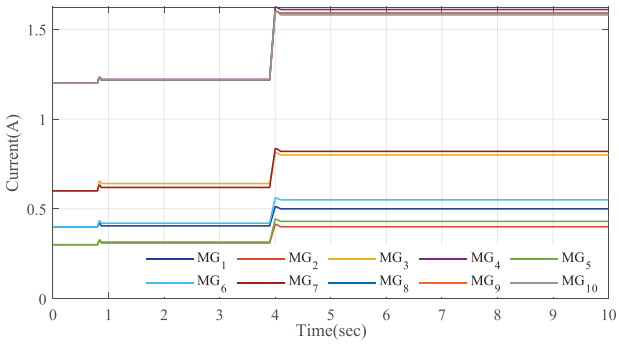


Fig. 18. Current outputs of dc microgrid cluster with the proposed countermeasures.

microgrids 2 and 7. At 0.8 s, the FDIA targets microgrids 1, 2, 8, and 10, injecting a false data vector of $\sin 2t$. At 4 s, the attacker injects a false data vector of $\sin 4t$ into microgrids 4, 5, 6, and 9. Each microgrid is powered by a photovoltaic array composed of multiple series-connected solar cells to achieve the desired voltage levels. Specifically, the photovoltaic panels consist of 72 series-connected cells, each with an open-circuit voltage of approximately 0.6 V, resulting in a total open-circuit voltage of about 43.2 V per panel. To reach the 48 V system voltage, the photovoltaic arrays are configured with two such panels connected in series.

Figs. 18 and 19 show the current and voltage outputs of a dc microgrid cluster with the proposed countermeasures. At 0.8 s, the current and voltage outputs become unstable due to malicious attacks. However, within 0.05 s, the defense method proposed in this article stabilizes the current output ratios to approximately $I_1 : I_2 : I_3 : I_4 : I_5 : I_6 : I_7 : I_8 : I_9 : I_{10} = 0.31 : 0.405 : 0.641 : 1.221 : 0.315 : 0.42 : 0.619 : 1.217 : 1.219 : 1.219$ and restores the voltage to the rated 48 V. At 4 s, as the attacker intensifies the attack, both current and voltage outputs experience more severe instability. Nevertheless, within 0.04 s, the proposed method stabilizes the current output ratios to approximately $I_1 : I_2 : I_3 : I_4 : I_5 : I_6 : I_7 : I_8 : I_9 : I_{10} = 0.4 : 0.5 : 0.8 : 1.61 : 0.43 : 0.55 : 0.82 : 1.59 : 1.59 : 1.58$ while also restoring the voltage output to the rated 48 V. This demonstrates that the proposed method can effectively counter malicious attacks even in more complex and large-scale models, ensuring the stability and security of microgrids.

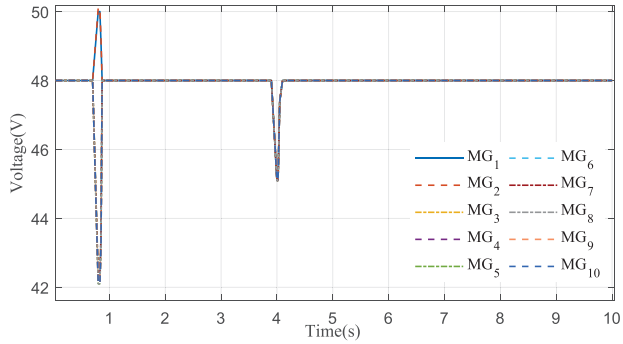


Fig. 19. Voltage outputs of dc microgrid cluster with the proposed countermeasures.

TABLE IV
WORST-CASE RESILIENCY PERFORMACE OF THE PROPOSED METHOD

Simulation model	Average	Best	Worse
4-MGs	99%	100%	75%
10-MGs	99.8%	100%	90%

C. Worst-Case Resiliency Test of the Proposed Dynamic Defense Method

To validate the worst-case resiliency of the proposed method, we calculated the total percentage of the dc microgrid cluster compromise that can be handled at any single instance. The total compromise percentage refers to the maximum proportion of malicious attacks that the microgrid can endure at a specific time without causing the overall system to fail or collapse. Assuming that all four microgrids are subjected to both FDIAs and DoS attacks, we conducted 50 experiments to obtain a more comprehensive and robust estimate of the average total compromise percentage. The total compromise percentage can be expressed as

$$P_i = \frac{N_{\text{compromised},i}}{N_{\text{total}}} \times 100\% \tag{27}$$

where $N_{\text{compromised},i}$ represents the number of compromised microgrids in the ith experiment, N_{total} represents the total number of microgrids. The average total compromise percentage is as follows:

$$\bar{P} = \frac{1}{N}\sum_{i=1}^{N} P_i \tag{28}$$

where N represents the total number of experiments and P_i represents the total compromise percentage in the ith experiment.

As shown in Table IV, the worst-case resiliency of the proposed method indicates that, within a model of four interconnected dc microgrids, the average total compromise rate is 99%, with the best rate being 100% and the worst being 75%. In 50

experiments, there was only one instance where the microgrid cluster collapsed when three microgrids simultaneously suffered from FDIAs and DoS attacks. In a model of ten interconnected dc microgrids, the proposed method achieved an average total compromise rate of 99.8%, with the best rate being 100% and the worst being 90%. This demonstrates that the proposed method can effectively handle mixed network attacks and maintain high stability and security for microgrids in most cases.

V. Discussion

The implementation of distributed communication and control in dc microgrids has brought significant benefits to their performance, but at the same time, it has also increased their susceptibility to cyber attacks. Considering the above problems, this article proposes a method to mitigate malicious attacks, including FDIAs and DoS attacks, which are common in dc microgrids.

Implementation: In dc microgrids, a defense method is needed to target malicious attacks. The proposed method combines two strategies to combat FDIAs and DoS attacks. For FDIAs, the method utilizes equivalence relations and dynamic removal of security data. To efficiently detect and mitigate FDIAs, this method computes mitigation vectors, undertakes residual tests, and sets optimization parameters depending on microgrid parameters. The second strategy employs a weighted average estimation method to defend against DoS attacks. The method optimizes the weights using the CPSO algorithm to calculate the optimal voltage estimates.

Application: Real-world microgrids face challenges such as increasing matrix dimensions, communication overhead, and the need for robust coordination within hierarchical control architectures. In addition, the risk of false positives caused by actual faults, such as short circuits, must be effectively mitigated. The proposed framework addresses these challenges by relying primarily on software updates, requiring minimal hardware modifications, and thus making it highly compatible with existing controllers. Moreover, through optimized parameter configurations and parallelized or edge-based deployment, the framework can scale efficiently with system size while maintaining real-time performance. Within multilevel control structures, the algorithm demonstrates strong integration capabilities with local control, scheduling, and upper-layer market modules, providing an accurate, secure, and flexible defense mechanism for large-scale microgrids or active distribution networks.

Drawbacks: The proposed method assumes that the dc microgrid is already under attack. A more comprehensive approach should also consider proactive measures to prevent cyber attacks.

In conclusion, the proposed defense method is a promising step toward improving the security of dc microgrids against malicious attacks.

VI. Conclusion

In this article, a novel approach for detecting and mitigating malicious attacks was presented in the dc microgrid. The method combines two strategies to address FDIAs and DoS attacks, respectively. The first strategy involves dynamically removing security data-assisted equivalence relations to resist FDIAs. This approach sets optimization parameters based on microgrid parameters, conducts residual tests, and computes mitigation vectors to detect and mitigate FDIAs effectively. The dynamic removal of security data can improve the computational efficiency of the equivalence relation and reduce the burden of the dc microgrids. Meanwhile, the second strategy introduces a weighted average estimation method to defend against DoS attacks. The method optimizes the weights using the CPSO algorithm to calculate the optimal voltage estimates. Finally, the effectiveness of the proposed method is verified based on a microgrid cluster model. In practical deployments, additional field tests will be necessary to accommodate heterogeneous microgrid conditions and ensure compliance with established cybersecurity standards. Future work will focus on developing universal approaches to counter malicious attacks in various operating environments of real-world LFC systems.

Appendix

The coefficient matrices in (12)

$$Y(m)=\begin{bmatrix} y(0) \\ y(1) \\ \vdots \\ y(m) \end{bmatrix}, \quad U(m)=\begin{bmatrix} u(0) \\ u(1) \\ \vdots \\ u(m), \end{bmatrix}, \quad D(m)=\begin{bmatrix} d(0) \\ d(1) \\ \vdots \\ d(m) \end{bmatrix}$$

$$x^{FD1}(m)=\begin{bmatrix} x^{FDI}(0) \\ x^{FDI}(1) \\ \vdots \\ x^{FDI}(m) \end{bmatrix}, \quad N=\begin{bmatrix} C \\ CA \\ \vdots \\ CA^m \end{bmatrix}_{2(m+1)\times 2}$$

$$P=\begin{bmatrix} 0 & 0 & \cdots & 0 \\ CB & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ CA^{m-1}B & CA^{m-2}B & \cdots & 0 \end{bmatrix}_{2(m+1)\times(m+1)}$$

$$R=\begin{bmatrix} 0 & 0 & \cdots & 0 \\ CM & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ CA^{m-1}M & CA^{m-2}M & \cdots & 0 \end{bmatrix}_{2(m+1)\times(m+1)}$$

$$S=\begin{bmatrix} I & 0 & \cdots & 0 \\ 0 & I & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & I \end{bmatrix}_{2(m+1)\times 2(m+1).}$$

References

[1] T. Dragičević, X. Lu, J. C. Vasquez, and J. M. Guerrero, "DC microgrids—Part II: A review of power architectures, applications, and standardization issues," *IEEE Trans. Power Electron.*, vol. 31, no. 5, pp. 3528–3549, May 2016.

[2] X. Liu, P. Wang, and P. C. Loh, "A hybrid AC/DC microgrid and its coordination control," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 278–286, Jun. 2011.

[3] J. J. Justo, F. Mwasilu, J. Lee, and J.-W. Jung, "AC-microgrids versus DC-microgrids with distributed energy resources: A review," *Renewable Sustain. Energy Rev.*, vol. 24, pp. 387–405, 2013.

[4] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 Ukraine blackout: Implications for false data injection attacks," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 3317–3318, Jul. 2017.

[5] C. Avraam, L. Ceferino, and Y. Dvorkin, "Operational and economy-wide impacts of compound cyber-attacks and extreme weather events on electric power networks," *Appl. Energy*, vol. 349, 2023, Art. no. 121577.

[6] A. V. Kayem, S. D. Wolthusen, and C. Meinel, *Smart Micro-Grid Systems Security and Privacy*. Berlin, Germany: Springer, 2018.

[7] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1630–1638, Jul. 2017.

[8] Z. Zhang, J. Hu, J. Lu, J. Cao, and F. E. Alsaadi, "Preventing false data injection attacks in LFC system via the attack-detection evolutionary game model and KF algorithm," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 6, pp. 4349–4362, Nov./Dec. 2022.

[9] S. Madichetty and S. Mishra, "Cyber attack detection and correction mechanisms in a distributed DC microgrid," *IEEE Trans. Power Electron.*, vol. 37, no. 2, pp. 1476–1485, Feb. 2022.

[10] O. A. Beg, T. T. Johnson, and A. Davoudi, "Detection of false-data injection attacks in cyber-physical DC microgrids," *IEEE Trans. Ind. Inform.*, vol. 13, no. 5, pp. 2693–2703, Oct. 2017.

[11] M. A. Jarrahi, H. Samet, and T. Ghanbari, "Fault detection in DC microgrid: A transient monitoring function-based method," *IEEE Trans. Ind. Electron.*, vol. 70, no. 6, pp. 6284–6294, Jun. 2022.

[12] Q. Zhou, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, "A cyber-attack resilient distributed control strategy in islanded microgrids," *IEEE Trans. Smart Grid*, vol. 11, no. 5, pp. 3690–3701, Sep. 2020.

[13] A. Abur and A. G. Exposito, *Power System State Estimation: Theory and Implementation*. Boca Raton, FL, USA: CRC Press, 2004.

[14] K. Manandhar, X. Cao, F. Hu, and Y. Liu, "Detection of faults and attacks including false data injection attack in smart grid using Kalman filter," *IEEE Trans. Control Netw. Syst.*, vol. 1, no. 4, pp. 370–379, Dec. 2014.

[15] M. N. Kurt, Y. Yilmaz, and X. Wang, "Real-time detection of hybrid and stealthy cyber-attacks in smart grid," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 2, pp. 498–513, Feb. 2019.

[16] S. Tan, P. Xie, J. M. Guerrero, J. C. Vasquez, and R. Han, "Cyberattack detection for converter-based distributed DC microgrids: Observer-based approaches," *IEEE Ind. Electron. Mag.*, vol. 16, no. 3, pp. 67–77, Sep. 2022.

[17] M. Shi, X. Chen, M. Shahidehpour, Q. Zhou, and J. Wen, "Observer-based resilient integrated distributed control against cyberattacks on sensors and actuators in islanded AC microgrids," *IEEE Trans. Smart Grid*, vol. 12, no. 3, pp. 1953–1963, May 2021.

[18] A. J. Gallo, M. S. Turan, F. Boem, T. Parisini, and G. Ferrari-Trecate, "A distributed cyber-attack detection scheme with application to DC microgrids," *IEEE Trans. Autom. Control*, vol. 65, no. 9, pp. 3800–3815, Sep. 2020.

[19] B. Li, T. Ding, C. Huang, J. Zhao, Y. Yang, and Y. Chen, "Detecting false data injection attacks against power system state estimation with fast go-decomposition approach," *IEEE Trans. Ind. Inform.*, vol. 15, no. 5, pp. 2892–2904, May 2019.

[20] K. Huang, Z. Xiang, W. Deng, C. Yang, and Z. Wang, "False data injection attacks detection in smart grid: A structural sparse matrix separation method," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 3, pp. 2545–2558, Jul.–Sep. 2021.

[21] S. Tan, P. Xie, J. M. Guerrero, and J. C. Vasquez, "False data injection cyber-attacks detection for multiple DC microgrid clusters," *Appl. Energy*, vol. 310, 2022, Art. no. 118425.

[22] Y. Zhang, J. Wang, and B. Chen, "Detecting false data injection attacks in smart grids: A semi-supervised deep learning approach," *IEEE Trans. Smart Grid*, vol. 12, no. 1, pp. 623–634, Jan. 2021.

[23] Z. Zhang, J. Hu, J. Lu, J. Cao, and J. Yu, "False data injection attacks on LFC systems: An AI-Based detection and countermeasure strategy," *IEEE Trans. Circuits Syst. I: Reg. Papers*, vol. 71, no. 5, pp. 1969–1977, May 2024.

[24] M. R. Habibi, H. R. Baghaee, T. Dragičević, and F. Blaabjerg, "Detection of false data injection cyber-attacks in DC microgrids based on recurrent neural networks," *IEEE Trans. Emerg. Sel. Topics Power Electron.*, vol. 9, no. 5, pp. 5294–5310, Oct. 2021.

[25] Z. Zhang, J. Hu, J. Lu, J. Cao, and A. Kashkynbayev, "Detection and defense of false data injection attacks in distributed load frequency control system in microgrid," *J. Modern Power Syst. Clean Energy*, vol. 12, no. 3, pp. 913–924, 2023.

[26] M. N. Kurt, O. Ogundijo, C. Li, and X. Wang, "Online cyber-attack detection in smart grid: A reinforcement learning approach," *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 5174–5185, Sep. 2019.

[27] H. Zhang, D. Yue, C. Dou, and G. P. Hancke, "Resilient optimal defensive strategy of micro-grids system via distributed deep reinforcement learning approach against FDI attack," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 35, no. 1, pp. 598–608, Jan. 2024.

[28] Z. Zhang, R. Deng, P. Cheng, and M.-Y. Chow, "Strategic protection against FDI attacks with moving target defense in power grids," *IEEE Trans. Control Netw. Syst.*, vol. 9, no. 1, pp. 245–256, Mar. 2022.

[29] M. Liu, C. Zhao, Z. Zhang, R. Deng, P. Cheng, and J. Chen, "Converter-based moving target defense against deception attacks in DC microgrids," *IEEE Trans. Smart Grid*, vol. 13, no. 5, pp. 3984–3996, Sep. 2022.

[30] J. Giraldo, M. El Hariri, and M. Parvania, "Decentralized moving target defense for microgrid protection against false-data injection attacks," *IEEE Trans. Smart Grid*, vol. 13, no. 5, pp. 3700–3710, Sep. 2022.

[31] Z. Lian, F. Guo, C. Wen, C. Deng, and P. Lin, "Distributed resilient optimal current sharing control for an islanded DC microgrid under DoS attacks," *IEEE Trans. Smart Grid*, vol. 12, no. 5, pp. 4494–4505, Sep. 2021.

[32] C. Deng, F. Guo, C. Wen, D. Yue, and Y. Wang, "Distributed resilient secondary control for DC microgrids against heterogeneous communication delays and DoS attacks," *IEEE Trans. Ind. Electron.*, vol. 69, no. 11, pp. 11560–11568, Nov. 2022.

[33] Y. Li, W. Meng, B. Fan, S. Zhao, and Q. Yang, "Distributed aperiodic control of multibus DC microgrids with DoS-attack resilience," *IEEE Trans. Smart Grid*, vol. 13, no. 6, pp. 4815–4827, Nov. 2022.

[34] X. Chen, J. Zhou, M. Shi, Y. Chen, and J. Wen, "Distributed resilient control against denial of service attacks in DC microgrids with constant power load," *Renewable Sustain. Energy Rev.*, vol. 153, 2022, Art. no. 111792.

[35] S. Hu, F. Yang, S. Gorbachev, D. Yue, V. Kuzin, and C. Deng, "Resilient control design for networked DC microgrids under time-constrained DoS attacks," *ISA Trans.*, vol. 127, pp. 197–205, 2022.

[36] S. Hu, P. Yuan, D. Yue, C. Dou, Z. Cheng, and Y. Zhang, "Attack-resilient event-triggered controller design of DC microgrids under DoS attacks," *IEEE Trans. Circuits Syst. I: Reg. Papers*, vol. 67, no. 2, pp. 699–710, Feb. 2020.

[37] H. Yang, T. Li, Y. Long, and Y. Xiao, "Event-triggered distributed secondary control with model-free predictive compensation in AC/DC networked microgrids under DoS attacks," *IEEE Trans. Cybern.*, vol. 54, no. 1, pp. 298–307, Jan. 2024.

[38] J. Lu, H. Jiang, X. Hou, and P. Wang, "Distributed edge-based event-triggered control for voltage restoration and current sharing in DC microgrids under DoS attacks," *IEEE Trans. Ind. Electron.*, vol. 70, no. 8, pp. 8053–8063, Aug. 2023.

[39] X.-Y. Liu and W.-W. Che, "Event-based distributed secondary voltage tracking control of microgrids under DoS attacks," *Inf. Sci.*, vol. 608, pp. 1572–1590, 2022.

[40] X. Li, C. Jiang, D. Du, W. Li, M. Fei, and L. Wu, "A novel state estimation method for smart grid under consecutive denial of service attacks," *IEEE Syst. J.*, vol. 17, no. 1, pp. 513–524, Mar. 2023.

[41] P. Danzi, M. Angjelichinoski, Č. Stefanović, T. Dragičević, and P. Popovski, "Software-defined microgrid control for resilience against denial-of-service attacks," *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 5258–5268, Sep. 2019.

[42] O. A. Beg, L. V. Nguyen, T. T. Johnson, and A. Davoudi, "Signal temporal logic-based attack detection in DC microgrids," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 3585–3595, Jul. 2019.

[43] S. Hu, X. Ge, X. Chen, and D. Yue, "Resilient load frequency control of islanded AC microgrids under concurrent false data injection and denial-of-service attacks," *IEEE Trans. Smart Grid*, vol. 14, no. 1, pp. 690–700, Jan. 2023.

[44] X.-K. Liu, C. Wen, Q. Xu, and Y.-W. Wang, "Resilient control and analysis for DC microgrid system under DoS and impulsive FDI attacks," *IEEE Trans. Smart Grid*, vol. 12, no. 5, pp. 3742–3754, Sep. 2021.

[45] Q. Zhou, M. Shahidehpour, A. Alabdulwahab, A. Abusorrah, L. Che, and X. Liu, "Cross-layer distributed control strategy for cyber resilient microgrids," *IEEE Trans. Smart Grid*, vol. 12, no. 5, pp. 3705–3717, Sep. 2021.

[46] X. Chen, S. Hu, Y. Li, D. Yue, C. Dou, and L. Ding, "Co-estimation of state and FDI attacks and attack compensation control for multi-area load frequency control systems under FDI and DoS attacks," *IEEE Trans. Smart Grid*, vol. 13, no. 3, pp. 2357–2368, May 2022.

[47] M. M. Hossain, C. Peng, H.-T. Sun, and S. Xie, "Bandwidth allocation-based distributed event-triggered LFC for smart grids under hybrid attacks," *IEEE Trans. Smart Grid*, vol. 13, no. 1, pp. 820–830, Jan. 2022.

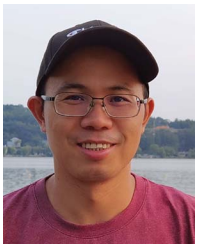
[48] X. Xiao, Q. Zhou, F. Wang, and W. Huang, "Three-stage defensive framework for distributed microgrid control against cyberattacks," *J. Modern Power Syst. Clean Energy*, vol. 10, no. 6, pp. 1669–1678, 2022.
[49] R. Han, M. Tucci, A. Martinelli, J. M. Guerrero, and G. Ferrari-Trecate, "Stability analysis of primary plug-and-play and secondary leader-based controllers for DC microgrid clusters," *IEEE Trans. Power Syst.*, vol. 34, no. 3, pp. 1780–1800, May 2019.
[50] M. Papadimitrakis, A. Kapnopoulos, S. Tsavartzidis, and A. Alexandridis, "A cooperative PSO algorithm for VOLT-VAR optimization in smart distribution grids," *Elect. Power Syst. Res.*, vol. 212, 2022, Art. no. 108618.
[51] W. Xu, D. W. Ho, J. Zhong, and B. Chen, "Event/self-triggered control for leader-following consensus over unreliable network with DoS attacks," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 30, no. 10, pp. 3137–3149, Oct. 2019.

Zhixun Zhang is currently pursuing a Ph.D. degree in Cyber Science and Engineering at Southeast University, Nanjing, China.

His research interests include the security of cyber-physical systems, cyber-attacks, and anomaly detection.

Jianqiang Hu (Member, IEEE) received the B.S. degree in mathematics and applied mathematics from the North China University of Water Resources and Electric Power, Zhengzhou, China, in 2010, the M.S. degree in applied mathematics and the Ph.D. degree in control theory and control engineering from Southeast University, Nanjing, China, in 2013 and 2016, respectively.

He is currently an Associate Professor with the Jiangsu Provincial Key Laboratory of Networked Collective Intelligence and the Department of System Science, School of Mathematics, Southeast University. His current research interests include the distributed optimization and control of multiagent systems, and demand-side control in smart grids.



Jianquan Lu (Senior Member, IEEE) received the B.S. degree in mathematics from Zhejiang Normal University, Zhejiang, China, in 2003, the M.S. degree in mathematics from Southeast University, Nanjing, China, in 2006, and the Ph.D. degree in applied mathematics from the City University of Hong Kong, Hong Kong, in 2009.

From 2010 to 2012, he was an Alexander von Humboldt Research Fellow with PIK, Germany. He is currently a Full Professor with Southeast University. He has authored or coauthored more than 100 IEEE Transactions journal articles. His current research interests include collective behavior in complex dynamical networks and multiagent systems, logical networks, and hybrid systems.

Dr. Lu was named as a Highly Cited Researcher by Clarivate Analytics. He was elected as a most Cited Chinese Researcher by Elsevier. He is an Associate Editor of *Neural Processing Letters, Journal of The Franklin Institute*, and *Neural Computing and Applications*, and a Guest Editor of *Science China: Information Sciences* and *IET Control Theory and Applications*.

Josep M. Guerrero (Fellow, IEEE) received the B.S. degree in telecommunications engineering, the M.S. degree in electronics engineering, and the Ph.D. degree in power electronics from the Technical University of Catalonia, Barcelona, Spain, in 1997, 2000 and 2003, respectively.

Since 2011, he has been a Full Professor with AAU Energy, Aalborg University, Aalborg, Denmark, where he is responsible for the Microgrid Research Program. From 2019, he became a Villum Investigator by the Villum Fonden, which supports the Center for Research on Microgrids at Aalborg University, being the Founder and the Director of the same center. In 2023, he joined the Technical University of Catalonia as an ICREA Research Professor. He has authored or coauthored more than 1000 journal papers in the fields of microgrids and renewable energy systems, which are cited more than 100 000 times. His research interests different microgrid frameworks like energy microgrids, hydrogen and biomass, water micronets, biological systems, seaport microgrids and electrical ships, airport microgrids and more electrical aircrafts, space microgrids, and smart medical systems.

Dr. Guerrero was the recipient of the Clarivate Analytics as Highly Cited Researcher for ten consecutive years, from 2014 to 2023.

Jinde Cao (Fellow, IEEE) received the B.S. degree in mathematics from Anhui Normal University, Wuhu, China in 1986, the M.S. degree from Yunnan University, Kunming, China, and the Ph.D. degree from Sichuan University, Chengdu, China, both in applied mathematics, 1989, and 1998, respectively. He was a Postdoctoral Research Fellow at the Department of Automation and Computer-Aided Engineering, Chinese University of Hong Kong, Hong Kong, China from 2001 to 2002.

Professor Cao is an Endowed Chair Professor, the Dean of Science Department and the Director of the Research Center for Complex Systems and Network Sciences at Southeast University (SEU). He is also the Director of the National Center for Applied Mathematics at SEU-Jiangsu of China and the Director of the Jiangsu Provincial Key Laboratory of Networked Collective Intelligence of China. He is also Honorable Professor of Institute of Mathematics and Mathematical Modeling, Almaty, Kazakhstan.

Prof. Cao was a recipient of the National Innovation Award of China, IETI Annual Scientific Award, Obada Prize and the Highly Cited Researcher Award in Engineering, Computer Science, and Mathematics by Clarivate Analytics. He is elected as a member of Russian Academy of Sciences, a member of the Academia Europaea (Academy of Europe), a member of Russian Academy of Engineering, a member of the European Academy of Sciences and Arts, a member of the Lithuanian Academy of Sciences, a fellow of African Academy of Sciences, and a fellow of Pakistan Academy of Sciences.