Linear Extended State Observer-Based Distributed Secondary Control of DC Microgrids Under False Data Injection Attacks

Yiwei FENG and Shuangshuang WANG

***Abstract*—To address the issue of unknown False Data Injection (FDI) attacks on controllers in DC microgrids, a distributed secondary controller for DC microgrids based on a linear extended state observer is presented to ensure that the system can achieve the control objectives of voltage regulation and current sharing even when subjected to FDI attacks. Firstly, the secondary control problem of multi-bus DC microgrids with FDI attacks is transformed into a first-order Multi-Agent System (MAS) fault-tolerant consistency problem, and the impact of FDI attacks on the microgrid system is analyzed. Then, a Linear Extended State Observer (LESO) is employed to detect the estimated injected FDI attack signals. Furthermore, a fault-tolerant secondary controller is designed to eliminate the adverse effects of FDI attacks on the system. The stability of the proposed method is verified using a Lyapunov function. Finally, the effectiveness and superiority of the proposed control method are experimentally demonstrated.**

***Index Terms*—DC microgrid, distributed fault-tolerant secondary control, false data injection (FDI) attack, linear extended state observer (LESO).**

I. Introduction

MICROGRIDS have emerged as a promising technology for integrating electronic interface-based renewable and non-renewable Distributed Generators (DGs), Energy Storage Systems (ESSs), and various loads, evolving into cyber-physical systems that incorporate communication, control, sensing, and computing capabilities [1], [2]. In recent years, research on DC and AC microgrids has been in full swing. Compared to AC microgrids, DC microgrids offer the following advantages: straightforward converter control, low power losses, and distributed control can be implemented more directly and efficiently without considering reactive power and harmonics [3]. DC microgrids have attracted widespread attention from researchers in recent years and have witnessed rapid development [4].

In earlier studies, droop control was used to restore DC bus voltages and achieve current sharing, which is the basic goal of DC microgrids [5]–[7]. However, due to the presence of line impedance, droop control alone often fails to achieve accurate current sharing and may also cause voltage drift. Therefore, it is necessary to introduce secondary control to compensate for droop control. Secondary control is mainly applied to centralized or distributed control methods [8]–[10]. Centralized control methods require system information from all DGs to achieve these control objectives over a global communication network, which can lead to high communication burden and operational errors in case of communication breakdowns [11]. Distributed secondary control has been widely studied due to the fact that it does not require global information, and the use of sparse communication networks can reduce the communication burden and make the system more robust [12]. However, this distributed cooperative control approach relies on local sensing and networked control over sparse communication networks, thus making these micro-networks highly vulnerable to malicious attacks and infiltration [13]–[15].

According to the current research on cyber attacks, cyber attacks are mainly categorized into the following types: False Data Injection (FDI) Attacks, Denial of Service Attacks (DoS) and Replay Attacks [16]–[18]. Among these attacks, FDI attacks have the greatest impact on DC microgrid systems, which can lead to problems such as misjudgment and misoperation of the system, thus affecting the stability and safety of the DC microgrid. To address FDI attacks in DC microgrid systems, detecting estimating and isolating the attack signals is one of the main methods to mitigate the impact of FDI attacks on control systems. In [19], a trust-based distributed secondary control method is proposed to detect and isolate the error mesdroopes in the system using a dynamic trust estimation mechanism to minimize the impact of FDI attacks in the communication link on the microgrid system. Literature [20] designed an attack detection method based on uncoordinated elements and proposed an evaluation theory to distinguish network attacks from system failures. However, these methods to suppress FDI attack signals by detecting estimating and isolating the attack signals tend to disrupt the

Manuscript received February 29, 2024; revised April 13, 2024, May 13, 2024 and June 8, 2024; accepted July 7, 2024. Date of publication September 30, 2024; date of current version July 16, 2024. This work was supported by Major Science and Technology Special Project of Gansu Province in China under Grant 23ZDGA007 and Industrial support plan project of Gansu Province in China under Grant 2024CYZC-18. *(Corresponding author: Yiwei Feng.)*

Both authors are with Electrical Engineering and Information Engineering, Lanzhou University of Technology, Lanzhou 730050, China (e-mail: ywfeng@yeah.net; 3180595559@qq.com).

Digital Object Identifier 10.24295/CPSSTPEA.2024.00013

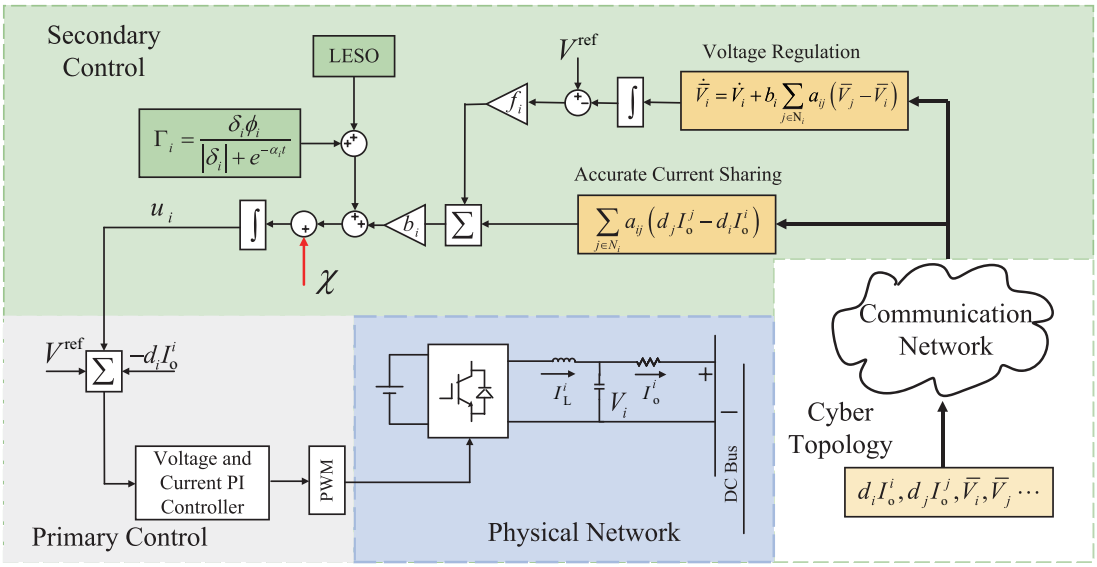

Fig. 1. Control block diagram of the given control scheme.

connectivity of the communication network and affect the consistency of the system, thus causing control bias [21]. The fault-tolerant control method, on the other hand, solves this problem. In recent years, many scholars have studied the FDI attack problem with fault-tolerant control methods. In [22], a novel distributed pulse adaptive fault-tolerant controller was constructed to address the challenges posed by spoofing attacks and actuator bias faults. In the literature [23], an adaptive fault-tolerant control scheme is proposed for a class of nonlinear strict feedback cyber-physical systems with spoofing attacks.

This paper presents a distributed fault-tolerant secondary control strategy for DC microgrids against FDI attacks. The main contributions of this paper are summarized as follows:

- A standard distributed secondary control method is reviewed, and then, by designing a new state variable, the secondary control problem of the multibus DC microgrid with attack signals is transformed into a first-order multi-intelligent body system (MAS) fault-tolerant consistency problem. The adverse effects of the attack signals on the microgrid system are also analyzed.
- A LESO is designed to detect various types of attack signals, state-space models are established, and the stability of the LESO method in DC microgrid systems is verified by pole configuration and frequency domain analysis.
- A fault-tolerant controller based on LESO is designed. The stability analysis of the global system is carried out, and the results show that the controller can enable the global system to achieve fault-tolerant consensus. Thus, it is theoretically demonstrated that the microgrid system can operate smoothly under the action of the designed controller.

The rest of the paper is structured as follows: Section II reviews distributed secondary control methods for DC microgrids and analyzes the impact of attack signals on the stability of microgrid systems. Section III presents a distributed fault-tolerant secondary control method based on LESO and proves its stability. Section IV verifies the effectiveness and superiority of the proposed control method in DC microgrids through simulation analysis of three cases. The experimental results are given in Section V. Finally, Section VI summarizes the paper.

II. Analysis of DC Microgrid System Based on FDI Attack

To facilitate the illustration of the proposed control method, this section first reviews a standard distributed secondary control method and then analyzes the impact of FDI attacks on DC microgrids.

A. Graph Theory and Symbols

The communication network of a DC microgrid system can be represented by a graph $G = (W, E, A)$ with a node set W, an edge set $E \subset W \times W$, and an adjacency matrix $\boldsymbol{A} = [a_{ij}]$. The graph edges represent the information flow from converter j to converter i, denoted by (w_j, w_i) and weighted by a_{ij}. If $(w_j, w_i) \in E$, then $a_{ij} = 1$; otherwise, $a_{ij} = 0$. If $(w_j, w_i) \in E$, then node j is considered to be a neighbor of node i. The set of neighbors of node i is denoted by $N_i = \{j \mid [(w_j, w_i) \in E]\}$. $\boldsymbol{D} = \text{diag}(d_i) \in R^{N\times N}$, with $d_i = \sum_{j\in N_i} a_{ij}$, is called the in-degree matrix. $\boldsymbol{L} = \boldsymbol{D} - \boldsymbol{A}$ denotes the Laplace matrix. G is assumed to be bidirectional, i.e., $a_{ij} = a_{ji}$. $\boldsymbol{L}$ is therefore symmetric. f_i is the pinning gain of the link from the pilot to the converter i. $f_i = 1$ if the pilot is connected to the i-converter; otherwise, $f_i = 0$. $\boldsymbol{F} = \text{diag}(f_i)$, $\forall i = 1, \cdots, N$, denotes a diagonal matrix consisting of pinning gains.

B. Secondary Control Method and System Analysis Under FDI Attack

The presented secondary control is based on a multi-bus DC microgrid system. Fig. 1 shows the overall cooperative control scheme of a DG unit in an isolated DC microgrid. In the primary control of isolated DC microgrids, droop control

is usually used to realize current sharing [24]. A local reference voltage V_i^* is generated and expressed as:

$$V_i^* = V_{\text{ref}} - d_i I_{\text{o}}^i \tag{1}$$

where V_{ref} is the output voltage reference, d_i is the i-th droop factor, and I_{o}^i is the output current of the i-th converter.

In order to compensate for the voltage deviation of the droop control, it is necessary to embed the secondary control signal in (1):

$$V_i^* = V_{\text{ref}} - d_i I_{\text{o}}^i + u_i \tag{2}$$

where u_i is the secondary control signal of the i-th converter, the time derivative of (2) is:

$$\dot{u}_i = \dot{V}_i^* + d_i \dot{I}_{\text{o}}^i = e_i \tag{3}$$

which e_i is the control input. The secondary control of DC microgrids is then transformed to a consensus problem for firstorder linear MAS. To achieve voltage regulation and accurate current sharing, the secondary control based on neighboring converter information is:

$$e_i = b_i \left[f_i (V_{\text{ref}} - \overline{V}_i) + \sum_{j \in N_i} a_{ij} (d_j I_{\text{o}}^j - d_i I_{\text{o}}^i) \right] \tag{4}$$

where b_i is the proportional gain. f_i is the i-th pinning gain. $\overline{V}_i$ is the global average voltage estimate for the i-th converter that satisfies the following conditions:

$$\dot{\overline{V}}_i = \dot{V}_i + b_i \sum_{j \in N_i} a_{ij} (\overline{V}_j - \overline{V}_i) \tag{5}$$

where V_i is the local output voltage.

As shown in Fig. 1, an unknown attack signal is injected to corrupt the control inputs. The dynamics of the attacked DC microgrid system can be given according to the following equation:

$$\dot{u}_i = e_i' = e_i + \chi_i \tag{6}$$

One of the control inputs that e_i' is damaged, χ_i is the attack signal, which can be modeled as a sum of finite step, ramp, or sinusoidal signals [25].

Assumption 1: For each converter, $\dot{\chi}_i$ is bounded.

Assumption 2: The attack injections considered in this paper satisfy: $\chi_i \leqslant \overline{\chi}_i$, where $\overline{\chi}_i$ is a positive constant.

The injected attack signals may destabilize the distributed system and thus damage the microgrid system. The effect of the attack signal on the system is analyzed theoretically below.

The local voltage controller regulates the output voltage of the converter to the reference voltage generated by the droop control with a voltage tracking error of $\varphi_i = V_i^* - V_i$, then $V_i^* = V_i + \varphi_i$, the time derivative of V_i^* can be derived as:

$$\dot{V}_i^* = \dot{V}_i + \dot{\varphi}_i \tag{7}$$

Substituting (6) and (7) into (3) yields:

$$\dot{V}_i + d_i \dot{I}_{\text{o}}^i + \dot{\varphi}_i = e_i + \chi_i \tag{8}$$

From (3)-(5) and (8), we can get:

$$\begin{aligned} \dot{\overline{V}}_i + d_i \dot{I}_{\text{o}}^i = b_i \sum_{j \in N_i} a_{ij} \left[\left(\overline{V}_j + d_j I_{\text{o}}^j \right) - \left(\overline{V}_i + d_i I_{\text{o}}^i \right) \right] + \\ b_i f_i \left[d_i \dot{I}_{\text{o}}^i - \left(\overline{V}_i + d_i I_{\text{o}}^i \right) \right] - \dot{\varphi}_i + \chi_i \end{aligned} \tag{9}$$

$d_i I_{\text{o}}^i$ converges to a constant I_{ss} in the steady state. Let $X_i = \overline{V}_i + d_i I_{\text{o}}^i$, $X_{\text{ref}} = I_{\text{ss}}$, then (10) can be rewritten as:

$$\dot{X}_i = b_i \left[\sum_{j \in N_i} a_{ij} (X_j - X_i) + f_i (X_{\text{ref}} - X_i) \right] - \dot{\varphi}_i + \chi_i \tag{10}$$

Remark 1: In this paper, we transform the distributed secondary control problem of a DC microgrid into a first-order MAS consistency problem. This is because in the secondary control, each DG unit needs to exchange its respective voltage and current information, of which $\overline{V}_i$ is easy to observe and $d_i I_{\text{o}}^i$ is hard to observe. In this paper, we design a new state variable X_i that converts the exchanged information ($\overline{V}_i$ and $d_i I_{\text{o}}^i$) into $\overline{V}_i$ and X_i, which allows us to derive the multi-bus DC microgrid model with FDI attack into a first-order MAS model. The MAS model is then used to analyze and design the controller.

Defining the state variable error as $\varepsilon_i = X_i - X_{\text{ref}}$, the time derivative of ε_i is:

$$\dot{\varepsilon}_i = -b_i \left[\sum_{j \in N_i} a_{ij} (\varepsilon_i - \varepsilon_j) - f_i \varepsilon_i \right] - \dot{\varphi}_i + \chi_i \tag{11}$$

Let $\boldsymbol{\varepsilon} = [\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n]^{\text{T}}$, then the global form of (11) can be expressed as:

$$\dot{\boldsymbol{\varepsilon}} = -\boldsymbol{B}(\boldsymbol{L} + \boldsymbol{F})\boldsymbol{\varepsilon} - \boldsymbol{\psi} + \boldsymbol{X} \tag{12}$$

where $\boldsymbol{B} = \text{diag}\,(b_i)$, $\boldsymbol{\psi} = [\dot{\varphi}_1, \dot{\varphi}_2, \cdots, \dot{\varphi}_n]^{\text{T}}$, $\boldsymbol{X} = [\chi_1, \chi_2, \cdots, \chi_n]^{\text{T}}$, $\boldsymbol{F} = \text{diag}\,(f_i)$. The dynamic expression can be derived:

$$\begin{aligned} \boldsymbol{\varepsilon}(t) = \exp\left[-\boldsymbol{B}(\boldsymbol{L} + \boldsymbol{F})t \right] \cdot \boldsymbol{\varepsilon}(t_0) + \\ \int_{t_0}^{t} \exp\left[-\boldsymbol{B}(\boldsymbol{L} + \boldsymbol{F})(t - \tau) \right] \cdot \left[\boldsymbol{X}(\tau) - \boldsymbol{\psi}(\tau) \right] \mathrm{d}\tau \end{aligned} \tag{13}$$

Without loss of generality, the attack signal is assumed to be positive, $\chi(\tau) > \chi_0 > 0$. It is assumed that the system can converge to the reference voltage, i.e., $\lim\limits_{t \to \infty} \varphi(t) = 0$, by means of a local voltage controller. Moreover, since $\boldsymbol{B}(\boldsymbol{L} + \boldsymbol{F})$ is a positive definite invertible matrix, $\exp[-\mathbf{B}(\boldsymbol{L} + \boldsymbol{F})t] \cdot \varepsilon(t_0)$ can converge to zero. Therefore, it is possible to obtain:

$$\begin{aligned} \lim_{t \to \infty} \boldsymbol{\varepsilon}(t) = \lim_{t \to \infty} \int_{t_0}^{t} \exp\left[-\boldsymbol{B}(\boldsymbol{L} + \boldsymbol{F})(t - \tau) \right] \cdot \boldsymbol{X}(\tau)\, \mathrm{d}\tau > \\ \exp\left[-\boldsymbol{B}(\boldsymbol{L} + \boldsymbol{F})t \right] \cdot \left\{ \exp\left[\boldsymbol{B}(\boldsymbol{L} + \boldsymbol{F})t \right] - \exp\left[\boldsymbol{B}(\boldsymbol{L} + \boldsymbol{F})t_0 \right] \right\} \cdot \\ \left[\boldsymbol{B}(\boldsymbol{L} + \boldsymbol{F}) \right]^{-1} \chi_0 = \left[\boldsymbol{B}(\boldsymbol{L} + \boldsymbol{F}) \right]^{-1} \chi_0 \geqslant 0 \end{aligned} \tag{14}$$

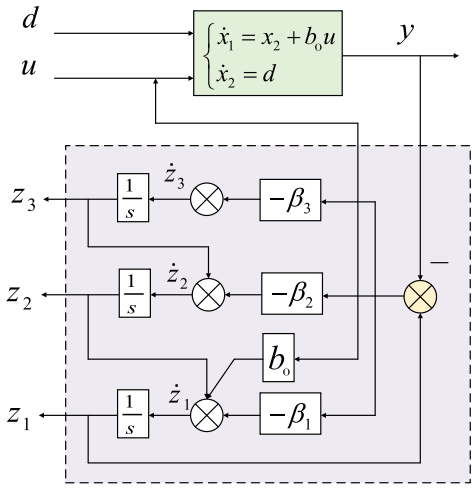

Fig. 2. Linear extended state observer.

From (14), the state error of the system fails to converge to zero under the influence of the FDI attack signal, i.e., it fails to achieve the desired goal of voltage regulation and current sharing.

III. A Distributed Fault-Tolerant Control Method Based on Leso is Given

This section details the given distributed fault-tolerant secondary control method based on LESO. Based on the system analysis, this paper transforms the control problem of DC microgrids into a first-order MAS fault-tolerant consistency problem. Firstly, LESO is designed to detect the estimated FDI attack signals. Then, a distributed fault-tolerant controller based on LESO is given to compensate and suppress the FDI attack. Finally, the stability of the designed LESO and fault-tolerant controller is verified.

A. Linear Extended State Observer

In order to detect and estimate FDI attack signals, the model of LESO is given in this part, as shown in Fig. 2.

From (6), considering u_i , χ as system state variables, the corresponding state space equation can be constructed as [26]:

$$\begin{cases} \dot{x}_1 = x_2 + b_o u \\ \dot{x}_2 = x_3 \\ \dot{x}_3 = h \\ y = x_1 \end{cases} \tag{15}$$

where $x_1 = u_i$, $x_2 = \chi$, $b_o = 1$, and e is the control input u. Extending the derivative term of the attack as a new state variable, that is $\dot{\chi} = x_3$, to increase bandwidth and reduce the number of communications. Then (15) is written in matrix form as:

$$\begin{cases} \dot{x} = \boldsymbol{A}x + \boldsymbol{B}u + \boldsymbol{E}h \\ y = \boldsymbol{C}x \end{cases} \tag{16}$$

where $\boldsymbol{A} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}$, $\boldsymbol{B} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$, $\boldsymbol{E} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$, $\boldsymbol{C} = [\,1\ 0\ 0\,]$.

By the introduction of the extended state, the original system is changed from the original second-order system to the thirdorder system, then the design of the extended state observer can be expressed as:

$$\begin{cases} \dot{z} = \boldsymbol{A}z + \boldsymbol{B}u - \boldsymbol{L}(z_1 - y) \\ y = \boldsymbol{C}z \end{cases} \tag{17}$$

where the observation matrix $\boldsymbol{L} = [\,\beta_1\ \beta_2\ \beta_3\,]^{\mathrm{T}}$, then the error matrix relationship can be expressed as:

$$\dot{e} = \boldsymbol{A}_e e - \boldsymbol{E}h \tag{18}$$

where $\boldsymbol{A}_e = \boldsymbol{A} - \boldsymbol{L}\boldsymbol{C} = \begin{bmatrix} -\beta_1 & 1 & 0 \\ -\beta_2 & 0 & 1 \\ -\beta_3 & 0 & 0 \end{bmatrix}$.

The system is stable if the chosen roots A_e are in the left half plane. To make the design process easy to implement, assuming that the observer poles are all located at $-\omega_o$, the characteristic polynomial can be designed as:

$$u(s) = \left|sI - \boldsymbol{A}_e\right| = s^3 + \beta_1 s^2 + \beta_2 s + \beta_3 = (s + \omega_o)^3 \tag{19}$$

where ω_o is the bandwidth of the LESO. $\beta_1 = 3\omega_o$, $\beta_2 = 3\omega_o^2$, $\beta_3 = \omega_o^3$.

B. Designed A Distributed Fault-Tolerant Controller

This section details the designed distributed fault-tolerant secondary controller and verifies the stability of the control system. Based on the derived MAS and the observed FDI attack signals, the distributed fault-tolerant secondary controller is designed to eliminate the adverse effects of the attack signals on the system.

For the sake of convenience, we denote:

$$\delta_i = b_i\left(\sum_{j \in N_i} a_{ij}(X_j - X_i) + f_i(X_{\mathrm{ref}} - X_i)\right) \tag{20}$$

To ensure voltage regulation and proportional load sharing under FDI attacks, we design the following distributed faulttolerant secondary controller [27]:

$$e_i = b_i\left[f_i\left(V_{\mathrm{ref}} - \overline{V}_i\right) + \sum_{j \in N_i} a_{ij}\left(d_j I_o^j - d_i I_o^i\right)\right] + \Gamma_i \tag{21}$$

$$\Gamma_i = \frac{\delta_i \phi_i}{\left|\delta_i\right| + \mathrm{e}^{-\alpha t}} \tag{22}$$

$$\dot{\phi}_i = u_i\left|\delta_i\right| \tag{23}$$

where Γ_i is the fault-tolerance compensation term, ϕ_i is the fault-tolerance parameter, α_i and μ_i are positive constants. For convenience, set $\mu_i \geqslant 1$. The consistent continuous function $\mathrm{e}^{-\alpha t}$ provides a smooth control method for practical implementation. Next, the stability of the designed controller is analyzed.

The time derivative of (20) can be obtained using (5), (6), and (21).

$$\begin{aligned}\dot{\delta}_i &= b_i\left[\sum_{j\in N_i} a_{ij}\left(\dot{X}_j - \dot{X}_i\right) + f_i\left(\dot{X}_{\text{ref}} - \dot{X}_i\right)\right] \\ &= -b_i(d_i + f_i)\dot{X}_i + b_i\sum_{j\in N_i} a_{ij}\dot{X}_j \\ &= -b_i(d_i + f_i)(\delta_i + \chi_i + \Gamma_i) + b_i\sum_{j\in N_i} a_{ij}(\delta_i + \chi_i + \Gamma_i)\end{aligned} \tag{24}$$

Denote $\Upsilon_i = \chi_i - \frac{1}{(d_i + f_i)}\sum_{j\in N_i} a_{ij}\ (\delta_j + \chi_j + \ \Gamma_j)$, then (24) can be rewritten as:

$$\dot{\delta}_i = -b_i(d_i + f_i)(\delta_i + \chi_i + \ \Gamma_i) \tag{25}$$

Consider the following Lyapunov candidate function:

$$V_i = \frac{1}{2}\left(|\delta_i| + \frac{\mathrm{d}|\Upsilon_i|}{\mathrm{d}t}\right)^2 \tag{26}$$

Its time derivative is given as:

$$\dot{V}_i = \left(|\delta_i| - \frac{\mathrm{d}|\Upsilon_i|}{\mathrm{d}t}\right)\left(\frac{\mathrm{d}|\delta_i|}{\mathrm{d}t} - \frac{\mathrm{d}^2|\Upsilon_i|}{\mathrm{d}t^2}\right) \tag{27}$$

where $\frac{\mathrm{d}|\Upsilon_i|}{\mathrm{d}t} = \frac{\Upsilon_i\dot{\Upsilon}_i}{|\Upsilon_i|} \leqslant \left|\dot{\Upsilon}_i\right|$, note that

$$\begin{aligned}\frac{\mathrm{d}|\delta_i|}{\mathrm{d}t} &= \frac{\delta_i\dot{\delta}_i}{|\delta_i|} = \frac{-b_i(d_i + f_i)\delta_i(\delta_i + \chi_i + \Gamma_i)}{|\delta_i|} \\ &= -b_i(d_i + f_i)\left(|\delta_i| + \frac{\delta_i\Upsilon_i}{|\delta_i|} + \frac{\delta_i\Gamma_i}{|\delta_i|}\right)\end{aligned} \tag{28}$$

Substituting (28) into (27) yields:

$$\begin{aligned}\dot{V}_i = &\left(|\delta_i| - \frac{\mathrm{d}|\Upsilon_i|}{\mathrm{d}t}\right)\times \\ &\left[-b_i(d_i + f_i)|\delta_i| - \frac{\mathrm{d}^2|\Upsilon_i|}{\mathrm{d}t^2} - b_i(d_i + f_i)\left(\frac{\delta_i\Upsilon_i}{|\delta_i|} + \frac{\delta_i\Gamma_i}{|\delta_i|}\right)\right]\end{aligned} \tag{29}$$

Use (22) to get:

$$\begin{aligned}&-b_i(d_i + f_i)\left(\frac{\delta_i\Upsilon_i}{|\delta_i|} + \frac{\delta_i\Gamma_i}{|\delta_i|}\right) = \\ &-b_i(d_i + f_i)\frac{\delta_i\Upsilon_i}{|\delta_i|} - b_i(d_i + f_i)\frac{|\delta_i|\phi_i}{|\delta_i| + \mathrm{e}^{-\alpha t}} \leqslant \\ &b_i(d_i + f_i)|\Upsilon_i| - b_i(d_i + f_i)\frac{|\delta_i|\phi_i}{|\delta_i| + \mathrm{e}^{-\alpha t}} \leqslant \\ &b_i(d_i + f_i)\frac{|\Upsilon_i||\delta_i| + \mathrm{e}^{-\alpha t}|\Upsilon_i| - |\delta_i|\phi_i}{|\delta_i| + \mathrm{e}^{-\alpha t}}\end{aligned} \tag{30}$$

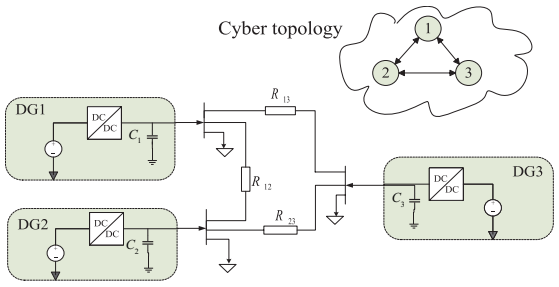

Fig. 3. DC microgrid system consisting of 3 DGs.

TABLE I
PARAMETER SETTING

Parameters	Value	Parameters	Value
V_{DC}	100 V	f_i	25
V_{ref}	48 V	b_i	20
f_s	100 KHz	d_i	1
L	1.8 mH	$k_{\text{vp}}/k_{\text{vi}}$	1/100
C	2.2 mF	$k_{\text{ip}}/k_{\text{ii}}$	0.5/10
T_{ij}	1 Ω	α_i	0.1
R	5 Ω	μ_i	5
W_o	200 rad/s		

Choosing $|\delta_i| > \frac{\mathrm{d}|\Upsilon_i|}{\mathrm{d}t}$ gets $\dot{\phi}_i > \frac{\mathrm{d}|\Upsilon_i|}{\mathrm{d}t}\cdot\mathrm{e}^{-\alpha t}|\Upsilon_i| \to 0$. Thus, $\exists\tau_1 > 0$, that makes for all $t > \tau_1$, we have:

$$|\Upsilon_i||\delta_i| + \mathrm{e}^{-\alpha t}|\Upsilon_i| - |\delta_i|\phi_i \leqslant 0 \tag{31}$$

Then, (30) and (31) are utilized to get:

$$-b_i(d_i + f_i)\left(\frac{\delta_i\Upsilon_i}{|\delta_i|} + \frac{\delta_i\Gamma_i}{|\delta_i|}\right) < 0\ ,\quad t > \tau_1 \tag{32}$$

Combining (29) and (32), the selection $|\delta_i| \geqslant -\frac{1}{b_i(d_i + f_i)}\frac{\mathrm{d}^2|\Upsilon_i|}{\mathrm{d}t^2}$ yields:

$$\begin{aligned}\dot{V}_i &\leqslant \left(|\delta_i| - \frac{\mathrm{d}|\Upsilon_i|}{\mathrm{d}t}\right)\left[-b_i(d_i + f_i)|\delta_i| - \frac{\mathrm{d}^2|\Upsilon_i|}{\mathrm{d}t^2}\right] \\ &\leqslant 0\ ,\quad \forall t > \tau_1\end{aligned} \tag{33}$$

$\dot{V}_i = 0$ if and only if $|\delta_i| = 0$. Therefore, the designed fault-tolerant controller can ensure the fault-tolerant consistency of the MAS, i.e., the DC microgrid system under FDI attack can maintain stable operation.

IV. Simulation Results

In order to verify the effectiveness of the given fault-tolerant control method, an islanded multi-bus DC microgrid system

TABLE II
ATTACK SIGNALS IN THE THREE CASES

Case	Attack note	Attack signal	t_{attack}
Case 1	DG1	10	t = 0.2–1 s
	DG3	10 sin(100 πt)	t = 0.4–1 s
Case 2	DG1	20 sin(200 πt) + 20	t = 0.2–1 s
	DG2	$-20t$	t = 0.4–1 s
Case 3	DG2	6	t = 0.2–1 s
	DG3	30 sin(300πt + π) + 30	t = 0.4–1 s

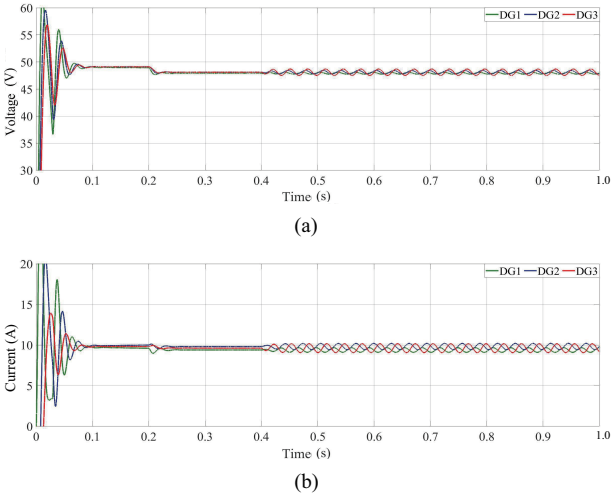

Fig. 4. The results of not configuring the fault-tolerant controller under the attack signal are: (a) output voltage, (b) output current.

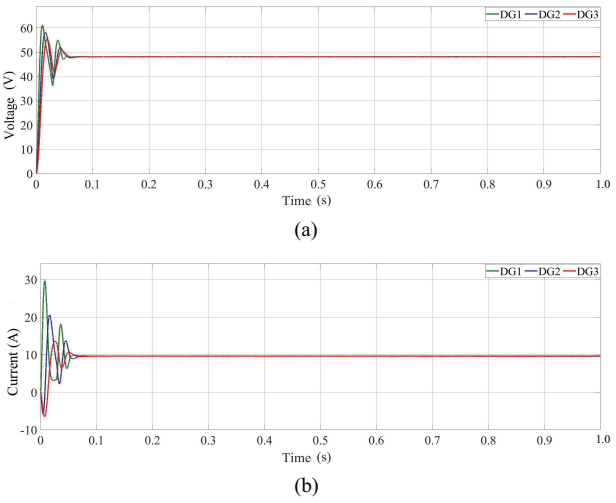

Fig. 5. The results of using fault tolerant controller under attack signal are: (a) output voltage, (b) output current.

with three DG units is constructed using MATLAB/Simulink as shown in Fig. 3. The parameters of the DGs and controllers are shown in Table I. The attack signals of each DG in different cases are shown in Table II [25], where tattack is the time interval of FDI attack.

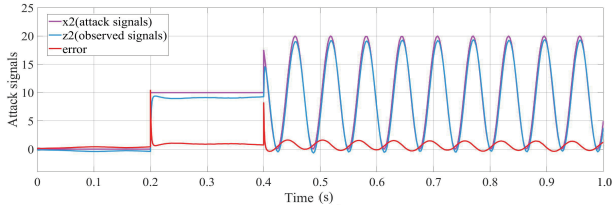

Fig. 6. Observed values of attack signals of case 1.

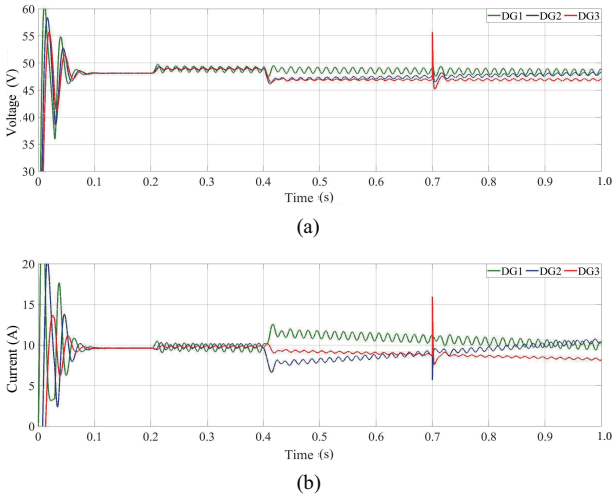

Fig. 7. The results of not configuring the fault-tolerant controller at t = 0.7 s communication interruption under attack signal are: (a) output voltage, (b) output current.

A. Case 1: Performance Comparison Under FDI Attack

In this section, the effectiveness of the given controller under network attack is simulated. The simulation process takes 1 s. A step attack signal χ_1 = 10 is injected into DG1 at t = 0.2 s and a sinusoidal attack signal χ_2 = 10 sin (100 πt) is injected into DG3 at t = 0.4 s. In this experiment, the given control strategies are compared with and without fault-tolerant controllers. The experimental results are shown in Figs. 4–6.

As shown in Fig. 4, injecting the attack signal into the control input channel at 0.2 s and 0.4 s, the DC microgrid system undergoes significant fluctuations. However, after adopting the fault-tolerant control method, as shown in Fig. 5, the system quickly converges to a steady-state value. Moreover, the output voltage of each converter is maintained at 48 V in the presence of the attack signal and the output current is accurately shared. The observed signals of the attack as well as the observation errors are shown in Fig. 6. It can be seen that the given LESO can track the attack signal quickly.

Therefore, the given fault tolerant control method is effective for general attack signals and ensures voltage regulation and current sharing.

B. Case 2: Communication Interruption

This section simulates and analyzes the performance of the designed fault-tolerant controller under communication interruption. In order to better analyze the performance of

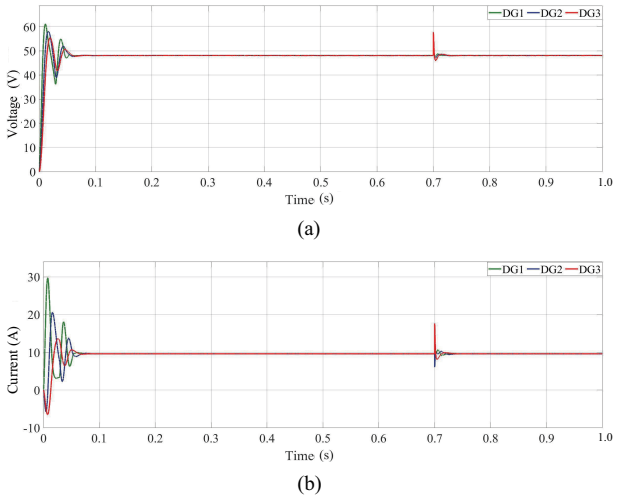

Fig. 8. The results of using fault-tolerant controller at $t = 0.7$ s communication interruption under attack signal are: (a) output voltage, (b) output current.

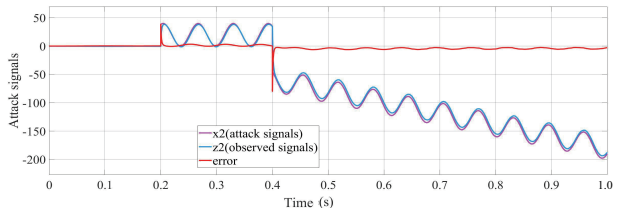

Fig. 9. Observed values of attack signals of case 2.

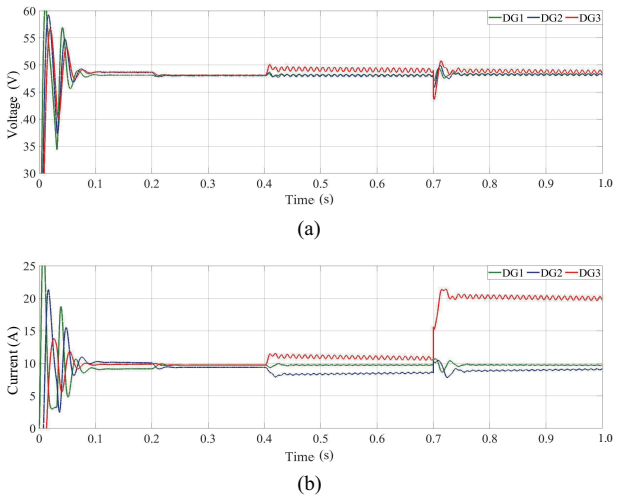

Fig. 10. The results of not configuring the fault-tolerant controller at $t = 0.7$ s load change under attack signal are: (a) output voltage, (b) output current.

the fault-tolerant controller in the case of communication interruption, a sinusoidal attack signal $\chi_1 = 20\sin(200\,\pi t) + 20$ is injected into DG1 at $t = 0.2$ s and a ramp attack signal $\chi_2 = -20t$ is injected into DG2 at $t = 0.4$ s. At $t = 0.7$ s, the communication between DG2 and DG3 is interrupted. The experimental results are shown in Figs. 7–9.

As can be seen in Figs. 7 and 8, the system stabilizes under the fault-tolerant controller at 0.2 s and 0.4 s injection attacks.

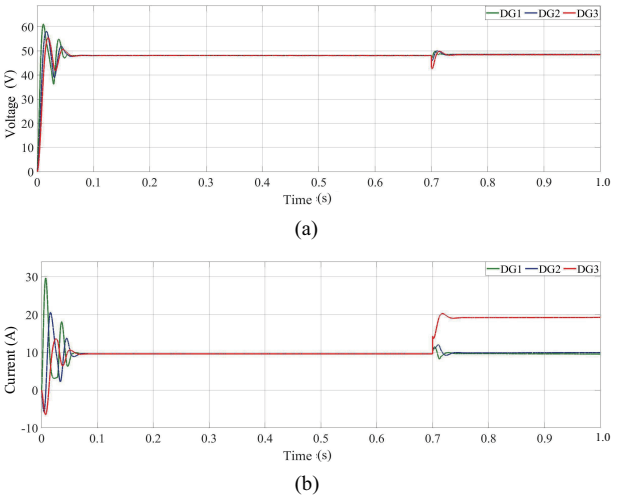

Fig. 11. The results of using fault-tolerant controller at $t = 0.7$ s load change under attack signal are: (a) output voltage, (b) output current.

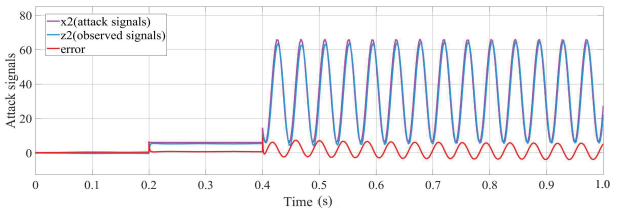

Fig. 12. Observed values of attack signals of case 3.

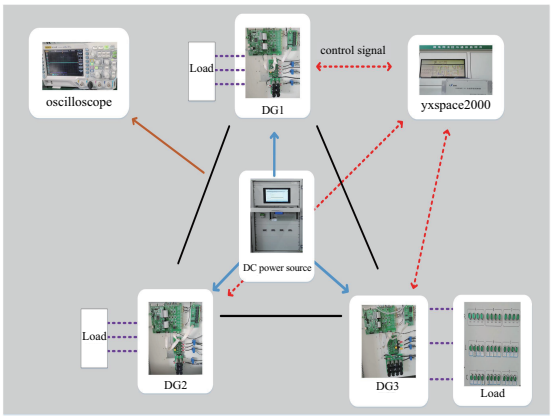

Fig. 13. Experimental setup.

Under the effect of 0.7 s communication interruption, both Fig. 7 and Fig. 8 have short fluctuations, indicating that the DC microgrid system without fault-tolerant controllers is inherently robust. In addition, it can be seen from Fig. 9 that the attack signal is successfully tracked.

C. Case 3: Load Variation

In this section, the system response of the given fault-tolerant secondary controller under load variation and network attack is simulated and analyzed. A step attack signal $\chi_1 = 6$ is injected into DG2 at $t = 0.2$ s and a sinusoidal attack signal

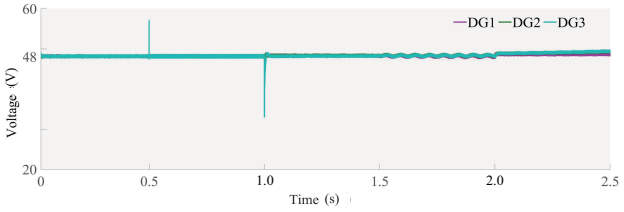

Fig. 14. Output voltage of experimental results.

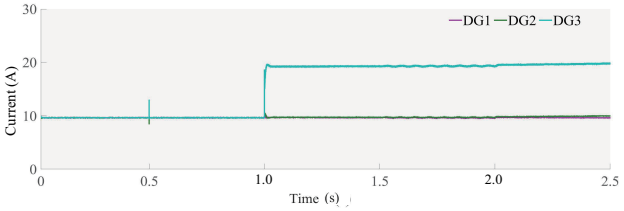

Fig. 15. Output current of experimental results.

$\chi_2 = 30\sin(300\pi t + \pi) + 30$ is injected into DG3 at $t = 0.4$ s. The load resistance of DG3 is reduced to 2.5 Ω at $t = 0.7$ s. The experimental results are shown in Figs. 10–12.

As can be observed from Fig. 10(a) and Fig. 11(a), it can be concluded that the system output voltage stabilizes under the fault-tolerant controller at 0.2 s and 0.4 s injection attacks; from Fig. 10(b) and Fig. 11(b), there is a sudden change in the output current of DG3 due to the load change. Under the effect of 0.7 s communication interruption, there is a short fluctuation in both Fig. 7 and Fig. 8, which also illustrates that the DC microgrid system without fault-tolerant controller is inherently robust. In addition, it can be seen from Fig. 12 that the tracking signal of the attack is good.

V. Experimental Results

The performance of the proposed fault-tolerant control scheme has been experimentally verified on a microgrid semiphysical platform consisting of 3 DGs and the YXSPACE2000 control platform, as shown in Fig. 13. The nominal voltage for the DC microgrid is 48 V. Besides, the line impedance of DGs are $r_{ij} = 5$ Ω. The control loop uses the scheme shown in Fig. 1 to regulate the voltage and current of each DG.

For convenience, all the results described above are represented in a single experiment via a microgrid semiphysical platform. In Figs. 14 and 15, the communication between DG2 and DG3 is interrupted at $t = 0.5$ s, at this time, the voltage and current fluctuate slightly. The load resistance of DG3 is reduced to 2.5 Ω at $t = 1$ s, there is a fluctuation in voltage and the current in DG3 doubles. At $t = 1.5$ s, a sinusoidal attack signal is injected into DG1, the system continues to fluctuate. At $t = 2$ s, the system incorporates the fault tolerant controller given in this paper, the system is restored to stability. It can be seen that system normal regulation signal do not continuously affect the system stability. When the attack signal is added, the system is dysregulated and external intervention is required to stabilize the system. Therefore, the fault-tolerance of the given scheme is verified.

VI. Conclusion

This paper presents a distributed LESO-based fault-tolerant secondary control method for DC microgrids, which enables voltage regulation and accurate current sharing in the presence of FDI attacks. LESO is utilized to estimate the attack signals in the DG, and a distributed fault-tolerant secondary controller is employed to compensate for the adverse effects of the attack signals on the system, with the capability to detect and suppress FDI attacks. A rigorous proof based on the Lyapunov function is provided. Moreover, the controller is robust against communication interruptions and load variations, further demonstrating the effectiveness and superiority of the method in DC microgrids. The controller designed in this paper primarily focuses on the attack signals in the actuators, and the attack signals in the sensors will be analyzed and investigated in the following step.

References

[1] X. Yu and Y. Xue, "Smart grids: A cyber–physical systems perspective," in *Proceedings of the IEEE*, vol. 104, no. 5, pp. 1058–1070, May 2016.

[2] J. Lai, X. Lu, X. Yu, and A. Monti, "Cluster-oriented distributed cooperative control for multiple AC microgrids," in *IEEE Transactions on Industrial Informatics*, vol. 15, no. 11, pp. 5906–5918, Nov. 2019.

[3] X. Lu, J. M. Guerrero, K. Sun, and J. C. Vasquez, "An improved droop control method for DC microgrids based on low bandwidth communication with DC bus voltage restoration and enhanced current sharing accuracy," in *IEEE Transactions on Power Electronics*, vol. 29, no. 4, pp. 1800–1812, Apr. 2014.

[4] F. Gao, R. Kang, J. Cao, and T. Yang, "Primary and secondary control in DC microgrids: A review," in *Journal of Modern Power Systems and Clean Energy*, vol. 7, no. 2, pp. 227–242, Mar. 2019.

[5] Z. Ma, X. Zhang, J. Huang, and B. Zhao, "Stability-constraining-dichotomy-solution-based model predictive control to improve the stability of power conversion system in the MEA," in *IEEE Transactions on Industrial Electronics*, vol. 66, no. 7, pp. 5696–5706, Jul. 2019.

[6] F. Guo, L. Wang, C. Wen, D. Zhang, and Q. Xu, "Distributed voltage restoration and current sharing control in islanded DC microgrid systems without continuous communication," in *IEEE Transactions on Industrial Electronics*, vol. 67, no. 4, pp. 3043–3053, Apr. 2020.

[7] J. M. Guerrero, J. C. Vasquez, J. Matas, L. G. de Vicuna, and M. Castilla, "Hierarchical control of droop-controlled AC and DC microgrids—A general approach toward standardization," in *IEEE Transactions on Industrial Electronics*, vol. 58, no. 1, pp. 158–172, Jan. 2011.

[8] Y. Li, Z. Zhang, T. Dragičević, and J. Rodriguez, "A unified distributed cooperative control of DC microgrids using consensus protocol," in *IEEE Transactions on Smart Grid*, vol. 12, no. 3, pp. 1880–1892, May 2021.

[9] L. Meng, T. Dragicevic, J. Roldán-Pérez, J. C. Vasquez, and J. M. Guerrero, "Modeling and sensitivity study of consensus algorithm-based distributed hierarchical control for DC microgrids," in *IEEE Transactions on Smart Grid*, vol. 7, no. 3, pp. 1504–1515, May 2016.

[10] Y. Fan, G. Hu, and M. Egerstedt, "Distributed reactive power sharing control for microgrids with event-triggered communication," in *IEEE Transactions on Control Systems Technology*, vol. 25, no. 1, pp. 118–128, Jan. 2017.

[11] T. Dragičević, J. M. Guerrero, and J. C. Vasquez, "A distributed control strategy for coordination of an autonomous LVDC microgrid based on power-line signaling," in *IEEE Transactions on Industrial Electronics*, vol. 61, no. 7, pp. 3313–3326, Jul. 2014.

[12] P. Prabhakaran, Y. Goyal, and V. Agarwal, "A novel communica-

tion-based average voltage regulation scheme for a droop controlled DC microgrid," in *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 1250–1258, Mar. 2019.

[13] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *ACM Transactions on Information and System Security*, vol. 14, no. 1, pp. 1–33, May 2011.

[14] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," in *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 645–658, Dec. 2011.

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

[16] M. R. Habibi, H. R. Baghaee, T. Dragičević, and F. Blaabjerg, "False data injection cyber-attacks mitigation in parallel DC/DC converters based on artificial neural networks," in *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 68, no. 2, pp. 717–721, Feb. 2021.

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

[18] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," in *IEEE Transactions on Automatic Control*, vol. 58, no. 11, pp. 2715–2729, Nov. 2013.

[19] S. Abhinav, H. Modares, F. L. Lewis, and A. Davoudi, "Resilient cooperative control of DC microgrids," in *IEEE Transactions on Smart Grid*, vol. 10, no. 1, pp. 1083–1085, Jan. 2019.

[20] S. Sahoo, J. C. -H. Peng, A. Devakumar, S. Mishra, and T. Dragičević, "On detection of false data in cooperative DC microgrids—A discordant element approach," in *IEEE Transactions on Industrial Electronics*, vol. 67, no. 8, pp. 6562–6571, Aug. 2020.

[21] Z. Tang, M. Kuijper, M. S. Chong, I. Mareels, and C. Leckie, "Linear system security—Detection and correction of adversarial sensor attacks in the noise-free case," in *Automatica*, vol. 101, pp. 53–59, Mar. 2019.

[22] L. Zhao and G. H. Yang, "Cooperative adaptive fault-tolerant control for multi-agent systems with deception attacks," in *Journal of the Franklin Institute*, vol. 357, no. 6, pp. 3419–3433, Apr. 2020.

[23] W. -D. Chen, Y. -X. Li, L. Liu, X. -D. Zhao, B. Niu, and L. -M. Han, "Nussbaum-based adaptive fault-tolerant control for nonlinear CPSs with deception attacks: A new coordinate transformation technology," in *IEEE Transactions on Cybernetics*, vol. 54, no. 2, pp. 1212–1222, Feb. 2024.

[24] J. Lu, X. Zhang, X. Hou, and P. Wang, "Generalized extended state observer-based distributed attack-resilient control for DC microgrids," in *IEEE Transactions on Sustainable Energy*, vol. 13, no. 3, pp. 1469–1480, Jul. 2022.

[25] Z. K. Xie and Z. Q. Wu, "Distributed fault-tolerant secondary control for DC microgrids against false data injection attacks," in *International Journal of Electrical Power & Energy Systems*, vol. 144, pp. 108599, Jan. 2023.

[26] B. Yu, A. Shen, B. Chen, X. Luo, Q. Tang, J. Xu, and M. Zhu, "A compensation strategy of flux linkage observer in SPMSM sensorless drives based on linear extended state observer," in *IEEE Transactions on Energy Conversion*, vol. 37, no. 2, pp. 824–831, Jun. 2022.

[27] S. Zuo, T. Altun, F. L. Lewis, and A. Davoudi, "Distributed resilient secondary control of DC microgrids against unbounded attacks," in *IEEE Transactions on Smart Grid*, vol. 11, no. 5, pp. 3850–3859, Sept. 2020.

Yiwei Feng, Professor in Lanzhou University of Technology(LUT), China; He was vice dean of college of Electrical and Information Engineering, LUT. He received the B.S. degree and the Master's degree from Lanzhou University of Technology, LanZhou, China, in1998 and 2007, respectively. He received his Ph.D degree from the Dalian Maritime University in 2011. His main research interests include distributed control and optimization, intelligent modeling, control and optimization of complex industrial processes, smart microgrid state evaluation and control.

Shuangshuang Wang received the B.E. degree from Panzhihua University, Sichuan, China, in 2022. She is currently pursuing a master's degree in control engineering at Lanzhou University of Technology in Gansu, China. Her main research interests are intelligent microgrids and network attacks.