mathematics

MDPI

Article

Energy-Management Strategy of Battery Energy Storage Systems in DC Microgrids: A Distributed Fuzzy Output Consensus Control Considering Multiple Cyber Attacks

Xu Tian [1], Weisheng Wang [1], Liang Zou [2], Shuo Zhai [1], Bin Hai [1] and Rui Wang [1,3,*]

[1] College of Information Science and Engineering, Northeastern University, Shenyang 110819, China; 2300782@stu.neu.edu.cn (X.T.); 2271026@stu.neu.edu.cn (W.W.); 2270989@stu.neu.edu.cn (S.Z.); 20205532@stu.neu.edu.cn (B.H.)
[2] School of Electrical Engineering, Shandong University, Jinan 250061, China; zouliang@sdu.edu.cn
[3] Foshan Graduate School of Innovation, Northeastern University, Foshan 528311, China
* Correspondence: wangrui@ise.neu.edu.cn

Abstract: Distributed renewable sources are one of the most promising contributors for DC microgrids to reduce carbon emission and fuel consumption. Although the battery energy storage system (BESS) is widely applied to compensate the power imbalance between distributed generators (DGs) and loads, the impacts of disturbances, DGs, constant power loads (CPLs) and cyber attacks on this system are not simultaneously considered. Based on this, a distributed fuzzy output consensus control strategy is proposed to realize accurate current sharing and operate normally in the presence of denial of service (DoS) attacks and false data injection (FDI) attacks. Firstly, the whole model of the BESS in DC microgrids embedded into disturbance items, DGs, CPLs and resistive loads, is firstly built. This model could be further transformed into standard linear heterogeneous multi-agent systems with disturbance, which lays the foundation for the following control strategy. Then the model of FDI and DoS attacks are built. Meanwhile, the fuzzy logic controller (FLC) is applied to reduce the burden of communication among batteries. Based on these, a distributed output consensus fuzzy control is proposed to realize accurate current sharing among batteries. Moreover, the system under the proposed control in different cases is analyzed. Finally, the feasibility of the proposed control strategy is verified by numerical simulation results and experiment results.

Keywords: battery energy storage system; output consensus control; fuzzy control; cyber attacks

MSC: 93D20

Citation: Tian, X.; Wang, W.; Zou, L.; Zhai, S.; Hai, B.; Wang, R. Energy-Management Strategy of Battery Energy Storage Systems in DC Microgrids: A Distributed Fuzzy Output Consensus Control Considering Multiple Cyber Attacks. *Mathematics* **2024**, *12*, 887. https://doi.org/10.3390/math12060887

Academic Editor: Fausto Sargeni

Received: 19 February 2024
Revised: 7 March 2024
Accepted: 13 March 2024
Published: 18 March 2024

1. Introduction

Distributed renewable sources have become one of the most effective contributors for DC microgrids to reduce carbon emission and fossil energy consumption [1,2]. The battery energy storage system (BESS) has been widely studied to solve the power imbalance between distributed generators (DGs) and loads [3]. However, loads in the BESS are always connected to the tightly controlled power electronic converters, and they are considered as constant power loads (CPLs), which have negative impedance characteristics [4,5]. This will cause the instability of the system. Meanwhile, the current among batteries should be shared based on the real time of state of charge (SoC) and the remaining capacity of battery for this system [6]. According to the literature [7], the multilevel control strategy including primary control and secondary control has been widely applied to solve current sharing control with CPLs.

Primary control has been widely applied to realize energy management in microgrids. Decentralized control strategies were proposed, which included the V-I droop controller and the current controller. Therein, battery inverters operated as voltage source converters

(VSCs) and renewable energy source converters operated as current sources converters (CSCs) in this system [8,9]. To this end, CSCs could realize the maximum power point tracking (MPPT) in normal operating conditions [8]. And the voltage regulation was realized in the V-I droop controller. However, the accurate current sharing control among batteries was not realized due to the line impedance differences, which reduced battery utilization and caused overcharge/overdischarge for some batteries. Furthermore, these problems resulted in reduced battery lifetime and even fires [10].

In order to solve above problems, various secondary control strategies have been proposed, which can be separated into centralized control and distributed control. For centralized control, a quick communication system between the central controller and other controllers was required. The central controller collected the information from the entire system and sends control commands to other controllers, and it easily resulted in single-point failure and system errors with the increasing scale of power systems [11]. In order to solve these problems, distributed control was proposed, which only required a sparse communication link. Furthermore, SoC balance among batteries in the islanded microgrid could be realized. A distributed control strategy was proposed to achieve the balance of the energy state for the specific batteries system [12]. In [13], the distributed control strategy was improved to protect the batteries based on the SoC measurements. The accurate current sharing control considering the SoC among batteries was realized in [14]. However, the aforementioned studies all focused on the distributed control strategy under free communication. Cyber attacks on communication links among batteries were ignored, which resulted in the failure of control strategy. Thus, accurate current sharing control considering cyber attacks was necessary for the BESS in DC microgrids.

Cyber attacks on power systems include false data injection (FDI) attacks, denial of service (DoS) attacks, time-delay attacks, and resonance attacks [15]. Therein, FDI and DoS attacks are two typical cyber attacks in microgrids. FDI attacks are a kind of deception attack that manipulate information by injecting the false information into controller/sensor, and DoS attacks are a kind of disruption attack that destroy data availability by blocking the communication link. These attacks can lead to the performance degradation of the system and even cause the instability of systems [15]. Note that FDI attacks can be designed to target sensor, controller and energy markets [16]. The focus of this paper is on current sharing among batteries in secondary control. Thus, the FDI attacks are designed to inject the secondary controller in this paper.

On issues related to FDI attacks, numerous studies have focused on the detection and mitigation for DC microgrids in the secondary control [17–20]. In the study [17], a framework to carry out the detection by identifying a change in sets of inferred candidate invariant in DC microgrids was proposed. In order to solve the bi-level optimization problem, some new computationally efficient algorithms were proposed in the large-scale power systems [16]. A game algorithm based on the socially rational multi-agent system and fictitious play was proposed [21]. A method to signal temporal logic detection by monitoring the output voltages and currents of DC microgrids against the defined bounds was proposed [18]. In the study [19], a fully distributed control strategy based on detection strategy was proposed for DC microgrids in the presence of the two variants of false data injection into current sensor. Meanwhile, some scholars also designed resilient control strategies to eliminate the impact of FDI attacks on systems. In the study [22], a trust-based cooperative controller which only required local and neighbor information was proposed to mitigate the effects of attacks on communication links and controller hijacking. According to [23], a control strategy based on the neural network was proposed to compensate for a kind of unknown FDI attack signal. The event-driven resilient control based on a detection strategy was proposed to mitigate unknown boundary FDI attacks by designing a local authentication signal [24]. The output consensus control for the linear heterogeneous multi-agent against continuous FDI attacks was proposed by designing an auxiliary controller in [25].

Meanwhile, there were seldom works focused on the issues of DC microgrids related to DoS attacks [26]. A control strategy with event-based sampling under DoS attacks was proposed for linear multi-agent systems in [27]. Furthermore, a sample-data fully distributed consistency algorithm under DoS attacks was proposed in [28]. Different from the study in [27], it could be applied in linear heterogeneous multi-agent systems and the global information was not necessary. Furthermore, the event-trigged resilient control for DC microgrids under DoS attacks was proposed and the stability condition based on DoS frequency and DoS duration was established [29]; However, the control strategy for the BESS considering DoS and continuous FDI attacks was rarely studied.

Meanwhile, although the burden of communication can be reduced, calculations will increase, which could increase the burden of the controller and even system faults.

To sum up, this paper proposes a distributed output consensus control for the BESS considering disturbance items, DGs, CPLs, DoS, and FDI attacks. In order to further reduce the burden of communication, a fuzzy logic controller (FLC) is introduced in this paper.

The detailed contributions of this paper are shown as follows:

1. The model of the BESS in DC microgrids embedded with disturbance items, DGs, CPLs and resistive loads, is built in this paper. And it can be further transformed into linear heterogeneous multi-agent systems, which lays the foundation for the following control strategy.
2. The model of DoS and FDI attacks are built for this system. Different from previous literatures, the FDI is a kind of continuous attack in this paper. Based on this, the state-space function model of the BESS considering DoS and FDI attacks is further proposed.
3. To further reduce the burden of communication among batteries, the FLC is applied in this system.
4. Based on the proposed system model and the FLC, a new distributed fuzzy output consensus control strategy is proposed to realize accurate current sharing control among batteries in the presence of DoS and FDI attacks, which can extend the lifetime of the batteries and eliminate security risks.

The rest of this paper is organized as follows. The model of the BESS in DC microgrids embedded with disturbance items, DGs, CPLs and resistive loads, is built in Section 2. Furthermore, the models of DoS, FDI attacks, and the FLC are built in Section 3. Based on these, a new distributed fuzzy output consensus control strategy is proposed to realize accurate current sharing control among batteries in the presence of DoS and FDI attacks. Meanwhile, the system under the proposed control in different cases is analyzed. Then numerical simulation examples are provided to verify the feasibility of the proposed control strategy in Section 4. Meanwhile, the experiment results are described in Section 5. Finally, this paper is concluded in Section 6. The flowchat of the methodology is shown in Figure 1.

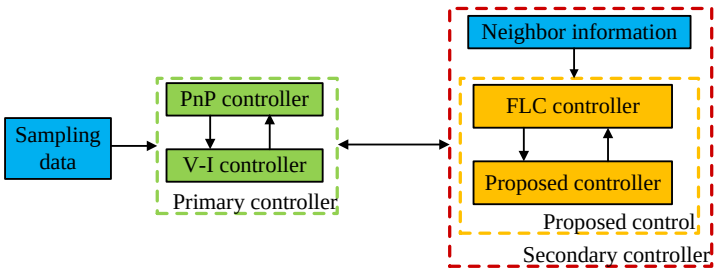

Figure 1. The flow of the methodology in this paper.

2. The Model of Battery Energy Storage Systems in DC Microgrids

As shown in Figure 2, the structure of the ith battery in DC microgrids is given. There are many DGs and CPLs in microgrids, and they can cause the fluctuation of bus voltage and even instability of system [30]. CPLs and DGs can be linearized at the voltage stable operation point $V_{\infty,i}$ by the Taylor series expansion method [31].

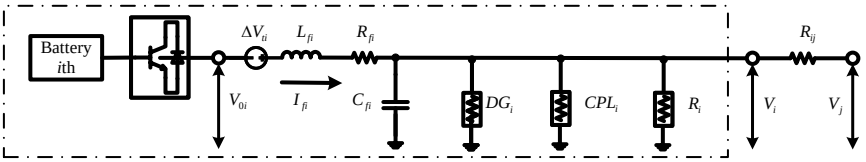

Figure 2. The structure of the BESS in DC microgrids with one DG and one CPL.

And they are shown as follows:

$$I_{CPL,i} = \frac{P_{CPL,i}}{v_{CPL,i}} \approx \frac{P_{CPL,i}}{V_{\infty,i}} - \frac{P_{CPL,i}}{V_{\infty,i}^2}\left(v_{CPL,i} - V_{\infty,i}\right) = I_{cpl,i} + \frac{v_{CPL,i}}{R_{CPL,i}} \tag{1}$$

$$I_{DG,i} = \frac{P_{DG,i}}{v_{DG,i}} \approx -\frac{P_{DG,i}}{V_{\infty,i}} + \frac{P_{DG,i}}{V_{\infty,i}^2}\left(v_{DG,i} - V_{\infty,i}\right) = I_{dg,i} + \frac{v_{DG,i}}{R_{DG,i}} \tag{2}$$

where $I_{cpl,i} = 2P_{CPL,i}/V_{\infty,i}$ and $I_{dg,i} = -2P_{DG,i}/V_{\infty,i}$ represent the equivalent constant current loads regarding the DG_i and the CPL_i, respectively. $R_{CPL,i} = -V_{\infty,i}^2/P_{CPL,i}$ and $R_{DG,i} = V_{\infty,i}^2/P_{DG,i}$ represent the equivalent resistances which can undermine the stability of the system. The constant power value for the CPL_i and the $DG_i$are represented as $P_{CPL,i}$ and $P_{DG,i}$, respectively. $v_{DG,i}$ and $v_{CPL,i}$ are the input voltages. And there is $v = v_{DG,i} = v_{CPL,i}$. Note that the CPLs refer to the power electronic load under the tightly control in this paper. Meanwhile, the disturbances from DGs are considered in this paper. And these disturbances are denoted as ΔV_{ti}. R_{Li} represents the common resistive load in this system. By applying Kirchhoff's current law and voltage law, the model of the ith battery is built and given by (3).

$$\begin{cases} C_{fi}\frac{dV_i}{dt} = I_{fi} + \sum_{j\in N_i}\frac{V_j - V_i}{R_{ij}} - \frac{V_i}{R_i} - I_{eq.i} \\ L_{fi}\frac{dI_{fi}}{dt} = V_{0i} + \Delta V_{ti} - R_{fi}I_{fi} - V_i \end{cases} \tag{3}$$

where V_{0i} and I_{fi} are the output voltage and current of the ith battery, respectively. R_{fi}, L_{fi}, C_{fi} are the RLC filter of the ith battery. V_i is the point voltage of the ith battery. And V_j is the point voltage of the jth battery. R_{ij} is the power-line load between the ith battery and the jth battery. $R_i = R_{CPL,i} + R_{DG,i} + R_{Li}$ represents the total resistive load in this system. $I_{eq,i} = I_{cpl,i} + I_{dg,i}$ represents the equivalent current load in this system.

Then let $\bar{x}_i(t) = \left(V_i, I_{fi}\right)^T$, $\bar{u}_i(t) = V_{0i}$, $\bar{\omega}_i(t) = \left(I_{eq,i}, \Delta V_{ti}\right)^T$, $\bar{y}_i(t) = n_i I_{fi}$ where $n_i = n_{0i}I_{fi}/\mathrm{SoC}$. Therein, n_{0i} is the droop gain. In light of Equation (3), the state-space function of the ith battery in DC microgrids can be obtained as follows:

$$\begin{cases} \dot{\bar{x}}_i(t) = & \bar{A}_i\bar{x}_i(t) + \sum \bar{A}_{ij}(\bar{x}_i(t) - \bar{x}_j(t)) \\ & +\bar{B}_i\bar{u}_i(t) + \bar{D}_{1i}\bar{\omega}_i(t) \\ y_i(t) = & \bar{C}_i\bar{x}_i(t) \end{cases} \tag{4}$$

where $\bar{A}_i = \begin{bmatrix} -\frac{1}{C_{fi}R_i} & \frac{1}{C_{fi}} \\ -\frac{1}{L_{fi}} & -\frac{R_{fi}}{L_{fi}} \end{bmatrix}$, $\bar{A}_{ij} = \begin{bmatrix} -\frac{1}{R_{ij}C_{fi}} & 0 \\ 0 & 0 \end{bmatrix}$, $\bar{B}_i = \begin{bmatrix} 0 \\ \frac{1}{L_{fi}} \end{bmatrix}$, $\bar{C}_i = \begin{bmatrix} 0 \\ n_i \end{bmatrix}^T$, $\bar{D}_i = \begin{bmatrix} -\frac{1}{C_{fi}} & 0 \\ 0 & \frac{1}{L_{fi}} \end{bmatrix}$.

In order to provide stable output voltage and current, the plug and play (PnP) controller is applied as the zero controller, which is beneficial for the features of PnP regarding DGs and loads. And the detailed design of the PnP controller is shown as follows:

$$\bar{u}_i(t) = p_{i,1}V_i + p_{i,2}I_{fi} + p_{i,3}\int_0^t (V_{r,i} - V_i)dt \tag{5}$$

where $p_{i,1}$, $p_{i,2}$, $p_{i,3}$ are the control parameters of the PnP controller, and $V_{r,i}$ is the rate voltage. The system is asympototically stable, if the control parameters of the PnP controller meet the following conditions [32]:

$$p_{i,1} < \left(\sum_{j\in N_i}\frac{1}{R_{ij}} + \frac{1}{R_{Li}} + \frac{1}{R_{CPL,i}} + \frac{1}{R_{DG,i}}\right)(R_{fi} - n_{i,2}) + 1 \tag{6}$$

$$p_{i,2} < \frac{L_{fi}}{C_{fi}}\left(\sum_{j\in N_i}\frac{1}{R_{ij}} + \frac{1}{R_{Li}} + \frac{1}{R_{CPL,i}} + \frac{1}{R_{DG,i}}\right) + R_{fi} \tag{7}$$

$$p_{i,3} \in \left(0, \frac{(n_{i,1}-1)\left(n_{i,2} - R_{fi}\right)}{L_{fi}}\right) \tag{8}$$

The V-I droop controller is applied as the primary controller to realize voltage regulation and preliminary current sharing among batteries, and it is shown as follows:

$$V_{r,i} = V_{nl} - n_i I_{fi} + \Delta V_i(t) \tag{9}$$

where V_{nl} is the no-load voltage of the ith battery in DC microgrids, $\Delta V_i(t)$ is the PI controller which is used to realize accurate current sharing among batteries in secondary control. The design of $\Delta V_i(t)$ is shown as follows:

$$\Delta V_i(t) = k_P u_i(t) + k_I \int_0^t u_i(t)dt \tag{10}$$

where k_P and k_I are coefficients of this PI controller, $u_i(t)$ is the feedback controller to be designed in next section.

To sum up, the overall model of the BESS in DC microgrids can be obtained. In light of Equations (5), (9) and (10), there are:

$$\bar{u}_i(t) = P_i^1\bar{x}_i(t) + P_i^2 z_i(t) \tag{11}$$

$$\dot{z}_i(t) = P_i^3\bar{x}_i(t) + V_{ul} + \Delta V_i(t) \tag{12}$$

$$\dot{\rho}_i(t) = k_I u_i(t) \tag{13}$$

$$\Delta V_i(t) = k_P u_i(t) + \rho_i(t) \tag{14}$$

where $z_i(t) = \int_0^t (V_{r,i} - V_i)dt$, $\rho_i(t) = k_I\int_0^t u_i(t)dt$, $P_i^1 = [p_{i,1}, p_{i,2}]$, $P_i^2 = p_{i,3}$, $P_i^3 = [-1, -n_i]$. Then set $x_i(t) = [\bar{x}_i^T(t), z_i(t)^T, \rho_i(t)^T]^T$. Combining Equation (4), the overall space-state model of the BESS in DC microgrids is provided:

$$\begin{cases} x_i(t) = & A_i x_i(t) + \sum_{j\in N_i} A_{ij}(x_i(t) - x_j(t)) \\ & + B_i u_i(t) + D_i\omega_i(t) \\ y_i(t) = & C_i x_i(t) \end{cases} \tag{15}$$

where $A_i = \begin{bmatrix} \bar{A}_i + \bar{B}_i P_i^1 & \bar{B}_i P_i^2 & 0_{2\times 1} \\ P_i^3 & 0 & 1 \\ 0_{1\times 2} & 0 & 0 \end{bmatrix}$, $\omega_i(t) = \begin{bmatrix} \bar{\omega}_i(t) \\ V^* \end{bmatrix}$, $B_i = \begin{bmatrix} 0_{2\times 1} \\ k_P \\ k_I \end{bmatrix}$, $C_i = \begin{bmatrix} \bar{C}_i^T \\ 0 \\ 0 \end{bmatrix}^T$, $A_{ij} = \begin{bmatrix} \bar{A}_{ij} & 0_{2\times 1} & 0_{2\times 1} \\ 0_{1\times 2} & 0 & 0 \\ 0_{1\times 2} & 0 & 0 \end{bmatrix}$, $D_i = \begin{bmatrix} \bar{D}_{1i} & 0_{2\times 1} \\ 0_{1\times 2} & 1 \\ 0_{1\times 2} & 0 \end{bmatrix}$.

Meanwhile, the 0th battery is design as a leader for the secondary control. And the space-state function model of the 0th battery is provided as follows:

$$\begin{cases} \dot{x}_0(t) = A_0 x_0(t) + D_0 \omega_0(t) \\ y_0(t) = C_0 x_0(t) \end{cases} \tag{16}$$

Note that the A_0 can be set by the Equation (16). And this equation have been described in detail in [11]. In addition, the interaction $\sum_{j\in N_i} A_{ij}(x_i(t) - x_j(t))$ can be incorporated into disturbance items according to [11]. Thus, the final space-state model of the BESS in DC microgrids is shown as follows:

$$\begin{cases} \dot{x}_i(t) = A_i x_i(t) + B_i u_i(t) + D_i \omega_i(t) \\ y_i(t) = C_i x_i(t) \\ \dot{x}_0(t) = A_0 x_0(t) + D_0 \omega_0(t) \\ y_0(t) = C_0 x_0(t) \end{cases} \tag{17}$$

Note that the Equation (17) is a standard linear heterogeneous multi-agent system with disturbance. For the linear heterogeneous multi-agent system (17), a common strategy is introduced, which lays the foundation for the following strategy [33]. And the common strategy is shown as follows:

$$\begin{cases} \dot{\eta}_{c,i}(t) = A_0 \eta_{c,i}(t) + F_i[\sum_{j\in N_i} a_{ij}(\eta_{c,i}(t) - \eta_{c,j}(t) + b_i(\eta_{c,i}(t) - x_0(t))] \\ u_{c,i}(t) = K_i(y_i(t) - C_i \Pi_i \eta_{c,i}(t)) + \Gamma_i \eta_{c,i}(t) \end{cases} \tag{18}$$

where K_i and F_i are the control gains in the system. And $\eta_{c,i}(t)$ is a compensator for ith battery that mainly transforms the information among batteries. $u_{c,i}(t)$ is the output feedback controller, and there is $u_i(t) = u_{c,i}(t)$ for this common strategy.

The communication among N batteries is represented by a directed graph $\mathcal{G} = (\mathcal{A}, \bar{\mathcal{V}}, \mathcal{E})$. $\bar{\mathcal{V}} = \mathcal{V} \cup \{v_0\}$ with $\mathcal{V} = \{v_1, v_2, v_3, ...v_N\}$ represents N battery and 0th battery. $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ with $(v_i, v_j) \in \mathcal{E}$ represents that there is a path from the ith battery to the jth battery. In the adjacency matrix $\mathcal{A} = [a_{ij}] \in R^{N\times N}$ for the graph, $a_{ij} > 0$ if $(v_i, v_j) \in \mathcal{E}$, otherwise $a_{ij} = 0$. $L = \{l_{ij}\} \in R^{N\times N}$ represents the Laplace matrix and if $i = j$ there is $l_{ij} = \sum_{j\in N_i} a_{ij}$, otherwise $l_{ij} = -a_{ij}$. The adjacency matrix $B = diag\{b_1, b_2, b_3...b_N\}$ between the leader and followers is defined as $b_i = 1$ if the ith battery can receive information from the leader, $b_i = 0$ otherwise. Finally, let $H = L + B$.

From the above analysis, the accurate current sharing is realized if and only if $p_0 I_{f0} = p_1 I_{f1} = \cdots = p_N I_{fN}$, that is $y_0 = y_1 = \cdots = y_N$. Note that it has been transformed into the output consensus control. Thus, the purpose of the proposed control strategy is essentially to realize $\lim_{t\to\infty} \|y_i(t) - y_0(t)\| = 0, i = 1, 2, \ldots, N$. Before that, these conditions should be met in order to realize the output consensus control:

(1) The communication system has at least one directed spanning tree path from the leader to each follower;
(2) The following equations have at least one solution:

$$\begin{cases} \Pi_i A_0 = A_i \Pi_i + B_i \Gamma_i \\ 0 = C_i \Pi_i - C_0, i = 1, 2, 3, \ldots, N \end{cases} \tag{19}$$

where $\Pi_i \in R^{4\times4}$, $\Gamma_i \in R^{1\times4}$;

(3) The disturbances $\omega_i(t)$, $\omega_0(t)$ should meet the following conditions:

$$\begin{cases} \lim\limits_{T\to\infty}\left(\frac{1}{T}\int_0^T \|\omega_i(t)\|^2 dt\right) < \infty \\ \lim\limits_{T\to\infty}\left(\frac{1}{T}\int_0^T \|\omega_0(t)\|^2 dt\right) < \infty \end{cases} \tag{20}$$

3. Current Sharing Fuzzy Control Strategy Considering Multiple Network Attacks

In this section, the models of DoS and FDI attacks are introduced, respectively. Then the FLC is applied to further reduce the burden of communication among batteries. Based on these, the space-state function of the BESS considering DoS and FDI attacks is built. Furthermore, a distributed fuzzy control strategy considering multiple cyber attacks is proposed in this section. And the system under the proposed control law is analyzed in different cases.

3.1. The Model of FDI Attacks

FDI attacks are a kind of deception attack that inject false data into controllers and/or sensors to prevent realizing the control goal [25,34]. Meanwhile, these false data are injected continuously into controllers in this paper.

The model of controller considering FDI attacks is shown as follows:

$$u_i^a = u_i + \mu_i^a \tag{21}$$

where μ_i^a is the injected data, u_i^a is the damaged controller for the ith battery.

Note that the information is only changed in the corresponding controller. The output feedback controller is applied in this paper. Thus, the output of the system considering FDI attacks is given as:

$$y_i^a = y_i + s_i^a \tag{22}$$

where s_i^a is the injected data, y_i^a is the damaged output information for the ith battery.

Meanwhile, the following assumptions should be met for FDI attacks:

(a) The injected false data are bounded.

(b) The FDI attacks are mainly compound attacks consisting of bias attacks and harmonic attacks.

Based on this, the space-state function of the BESS in DC microgrids under the DoS and FDI attacks is further built:

$$\begin{cases} \dot{x}_i(t) = A_i x_i(t) + B_i u_i^a(t) + D_i \omega_i(t) \\ y_i(t) = C_i x_i(t) \\ \dot{x}_0(t) = A_0 x_0(t) + D_0 \omega_0(t) \\ y_0(t) = C_0 x_0(t) \end{cases} \tag{23}$$

Remark 1. *Actually, the attack emitters often operate with a limited supply of energy. Thus, the injected false data are bounded due to limited energy of attacks. Based on Equation (23), the bias attacks or the harmonic attacks could be regarded as disturbances because the space function of this system contains disturbance items. Therefore, the control goal could still be realized in the presence of this FDI attack. However, compound attacks could easily cause the failure of control goal according to [25]. For attackers, the compound attacks are the most effective means. Thus, the FDI attacks are mainly compound attacks.*

3.2. Modeling of DoS Attacks

For this system, each battery exchanges information with its neighbors through the communication link so as to realize the control goal. However, the communication link is often attacked by certain cyber attacks due to the open setting [34]. Therein, DoS attacks are a kind of prevalent attack in cyber attacks. DoS attacks mainly prevent the exchange information among batteries by blocking the communication link, and this causes the failure of the control strategy. Meanwhile, in order to ensure the universality of the model, DoS attacks are aperiodic in this paper.

And the attack moment and the duration of DoS attacks are represented as the $\{t_d\}(d = 1, 2, \ldots)$ and Δ_d, respectively. Thus, the time period during DoS attacks is represented as $(t_d, t_d + \Delta_d)$, and the next time period should meet $t_{d+1} > t_d + \Delta_d$. The sum time of DoS attacks in $[0, t]$ is $\Xi_d(0, t) = \mathsf{U}_{d=1,2\ldots}(t_d, t_d + \Delta_d) \cap [0, t]$. Moreover, the successful probability of DoS attacks is given as follows [35]:

$$\begin{cases} \text{Prob}\{\vartheta(t) = 0\} = \text{E}\{\vartheta(t)\} = 1 - d \\ \text{Prob}\{\vartheta(t) = 1\} = 1 - \text{E}\{\vartheta(t)\} = d \end{cases} \tag{24}$$

where $d \in [0, 1]$. $\vartheta(t)$ is a detector of DoS attacks with $\vartheta(t) = 0$ if $t \in \Xi(0, t)$ and with $\vartheta(t) = 1$ if $t \in \Xi_d(0, t)$. The communication time among batteries is $\Xi(0, t) = [0, t]/\Xi_d(0, t)$. The total number of DoS attacks is M, and the frequency of DoS attacks can be defined as:

$$f = \frac{M}{t} \tag{25}$$

$|\Xi_d(0, t)|$ is the total length of DoS attacks, the attacks ratio in $[0, t]$ can be defined as

$$\alpha = \frac{|\Xi_d(0, t)|}{t} \tag{26}$$

Meanwhile, the following assumptions should be met for DoS attacks:

(i) The number of DoS attacks is limited, and the duration of each DoS has the upper limit.
(ii) The controllers and state values are no longer updated in the presence of DoS attacks.
(iii) Every DoS attack can be detected.

Remark 2. *As a kind of cyber attack, DoS attacks need the carrier to provide the energy. Moreover, the carriers have the limit of this energy supply. Thus, the condition (i) is reasonable.*

Remark 3. *Although the ith battery has the ability to communicate during DoS attacks, the availability of data is violated [28]. Based on this, the controllers and state values are no longer updated in order to make data reliable.*

Remark 4. *Note that the detection of DoS attacks have been widely studied [36]. Thus, condition (iii) is satisfied.*

3.3. Design of the Fuzzy Logic Controller

Next, an FLC is designed to improve the dynamic performance and reduce the burden of communication among batteries by minimizing unnecessary information exchange.

The FLC transforms logic judgment strategies based on human rich experience into applicable control strategies to controllers. And since there is no need to know the detailed mathematical description of the system, it has been widely studied [37]. Thus, the FLC is applied in this paper.

The processing of the FLC can be divided into three parts: fuzzification, regularization of logic inference, and defuzzification. In fuzzification, the main task is to collect and transform the input data into a fuzzy set by fuzzy linguistic terms and membership functions. A set of fuzzy rules for logical reasoning is introduced in second part, where the fuzzy

rules can be described by simple IF–THEN. In the third part, the fuzzy output is mapped to a clear output by the membership function. And the common methods are the center of gravity method and maximum membership method. Herein, the center of gravity method is applied in this paper.

Based on above analysis, the FLC is introduced to reduce the burden of communication among batteries by judging whether the system needs to update or not based on the $\Delta y_i(t)$ and d. Note that $\Delta y_i(t) = |C_i \dot{x}_i(t)|$ represents the variation of output. Therein, there is $\Delta y_i(t) \in [0, h_i]$, where h_i is the upper limited. The FLC is shown in Figure 3.

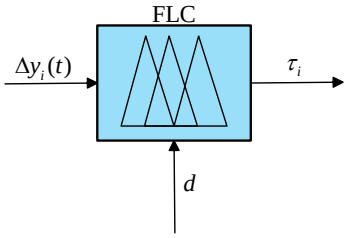

Figure 3. The fuzzy logic controller.

The FLC has three input membership functions for $\Delta y_i(t)$: small (S), medium (M), big (B). For d, there are two membership functions: small (S), big (B). The output has three membership functions: positive small (PS), positive medium (PM), positive big (PB). And the fuzzy rules are shown in Table 1.

Table 1. Fuzzy rules.

τ_i	d	
$\Delta y_i(t)$	S	B
S	PS	PS
M	PM	PB
B	PM	PB

3.4. Current Sharing Fuzzy Control Strategy in the Presence of FDI and DoS Attacks

Next, a current sharing fuzzy control strategy considering FDI and DoS attacks is proposed in this section. And the system under the proposed control strategy is analyzed in different cases. Before that, the current sharing control without FLC is proposed:

$$\begin{cases} \dot{\eta}_i(t) = A_0\eta_i(t) + F_i\left[\sum_{j\in N_i} a_{ij}\hat{\eta}_{ij}(t) + b_i\hat{\eta}_{i0}\right] \\ u_i(t) = K_i\hat{y}_i^a(t) + \Gamma_i\eta_i(t) + z_i(t) \\ \dot{z}_i(t) = -\iota_i K_i(y_i^d - y_{ref,i}) - \iota_i z_i(t) \end{cases} \tag{27}$$

where $\hat{\eta}_{ij} = (1-\vartheta(t))\big(\eta_i(t) - \eta_j(t)\big) + \vartheta(t)\big(\eta_i(t_d) - \eta_j(t_d)\big)$, $\hat{\eta}_{i0} = (1-\vartheta(t))\big(\eta_i(t) - x_0(t)\big) + \vartheta(t)\big(\eta_i(t_d) - x_0(t)\big)$, $\hat{y}_i^a(t) = (1-\vartheta(t))\big(y_i^a(t) - C_i\Pi_i\eta_i(t)\big) + \vartheta(t)\big(y_i^a(t) - C_i\Pi_i\eta_i(t_d)\big)$. Therein, $z_i(t)$ is a proposed auxiliary controller which is designed to mitigate the impact of FDI attacks, and ι_i is a given parameter.

Meanwhile, a reference model for each battery is introduced without FDI attacks. And it is shown as follows:

$$\begin{cases} \dot{x}_{ref,i}(t) = A_i x_{ref,i}(t) + B_i\hat{u}_{ref,i}(t) + D_i\omega_i(t) \\ y_{ref,i}(t) = C_i x_{ref,i}(t) \\ \hat{u}_{ref,i}(t) = K_i\big(\hat{y}_{ref,i}(t) - C_i\Pi_i\eta_i(t)\big) + \Gamma_i\eta_i(t) \end{cases} \tag{28}$$

where $\hat{y}_{ref,i}(t) = (1-\vartheta(t))\big(y_{ref,i}(t) - C_i\Pi_i\eta_i(t)\big) + \vartheta(t)\big(y_{ref,i}(t) - C_i\Pi_i\eta_i(t_d)\big)$.

From the above descriptions, the rules for this system can be obtained as follows. Rule 1: if $\Delta y_i(t)$ is S then τ_i is PS. Rule 2: if $\Delta y_i(t)$ is M, B, and d is B then τ_i is PB. Rule 3: if

$\Delta y_i(t)$ is M, B, and d is S then τ_i is PM. Note that the output of the FLC is represented by τ_i, whose value ranges between 0 and (1+h_i). The control law is proposed as follows, and τ_i can be incorporated into the control law (27):

$$\begin{cases} u_i(t) = \frac{1}{2}\left(\beta_{i,1}\hat{u}_i(t) + \beta_{i,2}\hat{u}_i(t^-)\right) \\ \dot{\eta}_i(t) = \frac{1}{2}\left(\beta_{i,1}\dot{\hat{\eta}}_i(t) + \beta_{i,2}\dot{\hat{\eta}}_i(t^-)\right) \\ \hat{u}_i(t) = K_i\hat{y}_i^a(t) + \Gamma_i\hat{\eta}_i(t) + z_i(t) \\ \dot{\hat{\eta}}_i(t) = A_0\hat{\eta}_i(t) + F_i\left[\sum_{j\in N_i} a_{ij}\hat{\eta}_{ij}(t) + b_i\hat{\eta}_{i0}\right] \\ \dot{z}_i(t) = -\iota_i K_i(y_i^d - y_{ref,i}) - \iota_i z_i(t) \end{cases} \tag{29}$$

where m_i is the dividing value of the FLC between PS and PM, $\beta_{i,1} = \text{sign}(\tau_i - m_i) + 1$ and $\beta_{i,2} = \text{sign}(m_i - \tau_i) + 1$. Note that sign$(\cdot)$ is the symbolic function. Finally, the current sharing fuzzy control strategy (29) is proposed.

Based on this, the following cases could be defined: case 1 if the $(\tau_i - m_i)$ is negative, and case 2 if the $(\tau_i - m_i)$ is positive. Therein, case 1 includes Rule 1, and case 2 includes Rule 2 and Rule 3.

3.4.1. Case 1

In case 1, there are $\beta_{i,2} = 2$ and $\beta_{i,1} = 0$. The control law (29) is rewritten as:

$$\begin{cases} u_i(t) = \hat{u}_i(t^-) \\ \dot{\eta}_i(t) = \dot{\hat{\eta}}_i(t^-) \end{cases} \tag{30}$$

The system is not updated in this case since $\Delta y_i(t)$ is S. If the output of ith battery changes very little, it will not affect the output consensus of the system even if controllers is not updated. It is regarded as the unnecessary information in this case. Thus, the burden of communication is reduced by minimizing unnecessary information exchange.

3.4.2. Case 2

In this case, $\beta_{i,2} = 0$, $\beta_{i,1} = 2$, the control law (29) is rewritten as:

$$\begin{cases} u_i(t) = \hat{u}_i(t) \\ \dot{\eta}_i(t) = \dot{\hat{\eta}}_i(t) \end{cases} \tag{31}$$

If the d is B, it represents the higher successful probability of DoS attacks, and it can be regarded that the DoS attack occurs in this situation. Thus, $\vartheta(t)$ should be reset to $\vartheta(t) = 0$ if the d is S, and $\vartheta(t) = 1$ if the d is B in this case. Meanwhile, the system needs to update so as to realize the current sharing control when $\Delta y_i(t)$ is M, B. In other words, the accurate current sharing control among batteries in this case is transformed into the current sharing control of the system (23) considering FDI and DoS attacks under the control law (31). Note that the continuous updating of information is also unnecessary if $\Delta y_i(t)$ is between PS and PM. And it can be solved by adjusting m_i. Then, the detail of choosing K_i and F_i is shown as follows.

The F_i can be chosen by the following algebraic Riccati equation [25,38]:

$$A_i^T M_i + M_i A_i + X_i - M_i T_i^{-1} M_i = 0 \tag{32}$$

where M_i is the symmetric positive matrix, $F_i = -\gamma_i T_i^{-1} M_i$, $X_i > 0$ and $T_i > 0$. Note that $\gamma_i \geq 1/2\overline{\lambda}_{min}$ and $\overline{\lambda}$=min(ReH). Next, the solution of K_i is given. Meanwhile, it is proved that the BESS in DC microgrids could realized the output consensus under the control law (31).

Before that, the current sharing among batteries is defined:

Definition 1. *For the performance metric γ_i, if the system (23) meets the following conditions, it can be said that the system realizes the H_∞ consensus, i.e., accurate current sharing control under the corresponding controller [33]:*

(i) If $\|\omega_{1i}(t)\| = \|\omega_0(t)\| \equiv 0, i = 1, 2, 3, ..., N$; then this is true for any initial value

$$\lim_{t\to\infty} \|x_i(t) - \Pi_i \eta_i(t)\| = 0$$
$$\lim_{t\to\infty} \|\eta_i(t) - x_0(t)\| = 0$$

combine Equation (19), we can obtain

$$\lim_{t\to\infty} \|y_i(t) - y_0(t)\| = 0 \tag{33}$$

(ii) If the initial values of the state variables for the leader, followers and compensators are 0, and the disturbance are limited, then the following holds:

$$\frac{1}{T} Y(t) < \frac{1}{T} \gamma^2 W(t), \forall T > 0 \tag{34}$$

where

$$Y(t) = \int_0^T \sum_{t=1}^{N} \|y_i(t) - y_0(t)\| dt$$
$$W(t) = \int_0^T \left(\sum_{i=1}^{N} \|\omega_i(t)\| + \|\omega_0(t)\| \right) dt$$

Theorem 1. *The conditions for the system (23) to realize the output consensus under the control law (31) with ι_i, are shown as follows: Given some symmetric positive matrices P_i and R_i, and scalar ι_i>0 satisfy the following conditions:*

$$\begin{pmatrix} (A_i^*)^T P_i + P_i A_i^* + C_i^T C_i & P_i & P_i B_i \\ P_i & -\iota_i I & 0 \\ B_i^T P_i & 0 & -R_i \end{pmatrix} < 0 \tag{35}$$

where $A_i^* = A_i + B_i K_i C_i$ and $K_i C_i = R_i^{-1} B_i^T P_i$.

Proof. Let $x_{\Delta i} = x_i - x_{ref,i}$. Then, combining Equations (23), (27) and (28), there is

$$\begin{aligned} \dot{x}_{\Delta i} &= \dot{x}_i - \dot{x}_{ref,i} \\ &= A_i x_i + B_i u_i^a + D_i \omega_i - (A_i x_{ref,i} + B_i u_{ref,i} + D_i \omega_i) \\ &= (A_i + B_i K_i C_i) x_{\Delta i} + B_i (z_i + f_i^0) \\ &= A_i^* x_{\Delta i} + B_i \bar{z}_i \end{aligned} \tag{36}$$

where $f_i^0 = K_i s_i^a + \mu_i^a$ and $\bar{z}_i = z_i + f_i^0$, and the z_i is rewritten as

$$\begin{aligned} \dot{z}_i &= -\iota_i K_i (y_i^d - y_{ref,i}) - \iota_i z_i(t) \\ &= -\iota_i K_i (y_i - y_{ref,i} + s_i^a) - \iota_i z_i(t) \\ &= -\iota_i K_i (C_i x_i - C_i x_{ref,i} + s_i^a) - \iota_i z_i(t) \\ &= -\iota_i K_i C_i x_{\Delta i} - \iota_i (z_i(t) + K_i s_i^a) \end{aligned} \tag{37}$$

where $f_i^1 = K_i s_i^a - f_i^0$. Define the Lyapunov function candidate

$$V_i = x_{\Delta i}^T P_i x_{\Delta i} + \iota_i^{-1} \bar{z}_i^T R_i \bar{z}_i \tag{38}$$

Combining $K_iC_i = R_i^{-1}B_i^TP_i$, Equations (36) and (37), the derivative of V_i is shown as follows:

$$\begin{aligned}\dot{V}_i =&\dot{x}_{\Delta i}^T P_i x_{\Delta i} + x_{\Delta i}^T P_i \dot{x}_{\Delta i} + \iota_i^{-1}\dot{\bar{z}}_i^T R_i \bar{z}_i + \iota_i^{-1}\bar{z}_i^T R_i \dot{\bar{z}}_i \\ =&(A_i^* x_{\Delta i} + B_i\bar{z}_i)^T P_i x_{\Delta i} + x_{\Delta i}^T P_i (A_i^* x_{\Delta i} + B_i\bar{z}_i) + \iota_i^{-1}(-\iota_i K_i C_i x_{\Delta i} - \iota_i \bar{z}_i(t) - \iota_i f_i^1 + + f_i^0)^T R_i \bar{z}_i \\ &+ \iota_i^{-1}\bar{z}_i^T R_i(-\iota_i K_i C_i x_{\Delta i} - \iota_i \bar{z}_i(t) - \iota_i f_i^1 + f_i^0) \\ =&x_{\Delta i}^T((A_i^*)^T P_i + P_i A_i^*)x_{\Delta i} - 2\bar{z}_i^T R_i \bar{z}_i - 2\bar{z}_i^T R_i(f_i^1 - \iota_i^{-1} f_i^0) \\ \leq&x_{\Delta i}^T((A_i^*)^T P_i + P_i A_i^* + \frac{P_i^T P_i}{\iota_i})x_{\Delta i} - 2\bar{z}_i^T R_i \bar{z}_i - 2\bar{z}_i^T R_i(f_i^1 - \iota_i^{-1} f_i^0)\end{aligned}$$

From Equation (35), there is

$$\begin{aligned}\dot{V}_i \leq&x_{\Delta i}^T((A_i^*)^T P_i + P_i A_i^* + \frac{P_i^T P_i}{\iota_i})x_{\Delta i} - 2\bar{z}_i^T R_i \bar{z}_i - 2\bar{z}_i^T R_i(f_i^1 - \iota_i^{-1} f_i^0) \\ \leq& - x_{\Delta i}^T(C_i^T C_i + P_i B_i R_i^{-1} B_i^T P_i)x_{\Delta i} - 2\bar{z}_i^T R_i \bar{z}_i - 2\bar{z}_i^T R_i(f_i^1 - \iota_i^{-1} f_i^0) \\ \leq& - x_{\Delta i}^T(C_i^T C_i)x_{\Delta i} - x_{\Delta i}^T(P_i B_i R_i^{-1}(B_i P_i)^T)x_{\Delta i} - 2\bar{z}_i^T R_i \bar{z}_i - 2\bar{z}_i^T R_i(f_i^1 - \iota_i^{-1} f_i^0)\end{aligned} \quad (39)$$

And, it can have

$$\dot{V}_i \leq -x_{\Delta i}^T(C_i^T C_i)x_{\Delta i} - 2\bar{z}_i^T R_i \bar{z}_i - 2\bar{z}_i^T R_i(f_i^1 - \iota_i^{-1} f_i^0) \quad (40)$$

Then, using Young inequality, the following equality can be obtained:

$$\dot{V} \leq -x_{\Delta i}^T(C_i^T C_i)x_{\Delta i} + (f_i^1 - \iota_i^{-1} f_i^0)^T R_i(f_i^1 - \iota_i^{-1} f_i^0) \quad (41)$$

Thus, according to [25], there is $\dot{V}_i < 0$ if

$$||x_{\Delta i}||_2 > \frac{\lambda_{max}(R_i)}{\lambda_{min}(C_i^T C_i)}||f_i^1 - \iota_i^{-1} f_i^0||_2 \quad (42)$$

Hence, there is a small parameter δ_i that makes $\lim_{t\to\infty}||x_{\Delta i}||_2 \leq \delta_i$. And δ_i could be chosen by adjusting R_i and ι_i. According to [28,39], it can obtain that $\lim\limits_{t\to\infty}\|x_{ref,i}(t) - \Pi_i\eta_i(t)\| = 0$ and $\lim\limits_{t\to\infty}\|\eta_i(t) - x_0(t)\| = 0$. Furthermore, there are $\lim\limits_{t\to\infty}\|x_i(t) - \Pi_i\eta_i(t)\| \leq \delta_i$ and $\lim\limits_{t\to\infty}\|\eta_i(t) - x_0(t)\| = 0$, i.e., $\lim\limits_{t\to\infty}\|y_i(t) - y_0(t)\| \leq \delta_i$. Thus, the output consensus can be realized by adjusting δ_i. Note that the (35) can be solved by the LMI toobox in a MATLAB software environment.

This completes the proof. □

Remark 5. *The control strategy considering DoS attacks has been widely studied [28,39]. Note that the system (23) is almost same as the system (17) by desiging the $z_i(t)$ [25]. According to the [28], the state information of controllers among batteries is replaced with the most recent available data based on the common strategy (18).*

4. Simulation

In order to verify the feasibility of the proposed strategy in the presence of DoS and FDI attacks, simulation examples are provided in MATLAB environment, where four batteries systems and one leader system are considered in the BESS.

And the relevant communication topology is shown in Figure 4. The detailed parameters are shown as follows. The line parameters among batteries are selected: $R_{14} = 0.20\ \Omega$, $R_{41} = 0.20\ \Omega$, $R_{12} = 0.40\ \Omega$, $R_{21} = 0.40\ \Omega$, $R_{32} = 0.20\ \Omega$, $R_{23} = 0.20\ \Omega$, $R_{34} = 0.50\ \Omega$, $R_{43} = 0.50\ \Omega$, $R_{01} = 1.00\ \Omega$, $R_{10} = 1.00\ \Omega$. And the resistive loads are selected:

$R_{L0} = 2.00\ \Omega$, $R_{L1} = 1.30\ \Omega$, $R_{L2} = 2.30\ \Omega$, $R_{L3} = 1.30\ \Omega$, $R_{L4} = 2.30\ \Omega$. For the parameters of the RLC filter, they are shown as follows:

$$\begin{cases} R_{f0} = 0.50\ \Omega, L_{f0} = 2\ \text{mH}, C_{f0} = 1.00\ \text{mF} \\ R_{f1} = 0.50\ \Omega, L_{f1} = 1\ \text{mH}, C_{f1} = 0.66\ \text{mF} \\ R_{f2} = 0.40\ \Omega, L_{f2} = 2\ \text{mH}, C_{f2} = 0.33\ \text{mF} \\ R_{f3} = 0.50\ \Omega, L_{f3} = 1\ \text{mH}, C_{f3} = 0.66\ \text{mF} \\ R_{f4} = 0.25\ \Omega, L_{f3} = 3\ \text{mH}, C_{f4} = 0.33\ \text{mF} \end{cases}$$

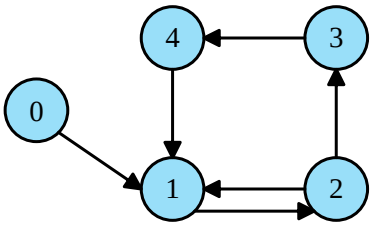

Figure 4. Communication topology structure.

The relevant parameters of the V-I droop controller are $k_P = -1.5$ and $k_I = -3$. The capacities of the DGs and CPLs are $P_{DG,i} = P_{CPL,i} = 200W, i = 1, 2, 3, 4$. The rated voltage of the DC microgrid is 50 V, and the disturbance from DGs can be selected 10% DC voltage fluctuation. At the beginning, the SoC of each battery is 90%, and the ratio of rated capacities of these five batteries included one leader and four batteries is chosen as 2:1:2:1:2. The parameters of the PnP controller are shown as follows:

$$\begin{cases} p_{0,1} = -1.00, p_{0,2} = -3.50, p_{0,3} = 2.00 \\ p_{1,1} = -3.00, p_{1,2} = -2.00, p_{1,3} = 2.00 \\ p_{2,1} = -3.00, p_{2,2} = -5.60, p_{2,3} = 2.00 \\ p_{3,1} = -1.00, p_{3,2} = -1.25, p_{3,3} = 1.00 \\ p_{4,1} = -2.00, p_{4,2} = -5.00, p_{4,3} = 1.50 \end{cases}$$

Meanwhile, the Equation (32) is a algebraic Riccati equation, it can be solved in the MATLAB. Thus, based on Equation (32), the controller gain F_i = [−6.0,−6.0,−6.0,−6.0;−6.0, −6.0,−6.0,−6.0;−6.0,−6.0,−6.0,−6.0;−6.0,−6.0,−6.0,−6.0] can be obtained. Then the output feedback controller gain can be obtained from Equation (35) by the LMI toolbox in MATLAB. Therein, $K_1 = 2.83$, $K_2 = 2.75$, $K_3 = 1.74$ and $K_4 = 1.70$.

As for network attacks, there are t_d = 1 s, 3 s, 5 s, α = 20%, f = 0.2 Hz, Δ_d = 0.5 s, 1 s, 1.5 s for DoS attacks. Meanwhile, FDI attacks are selected as follows: $s_1^a = 2 + \sin(0.1t)$, $s_2^a = -2 + \sin(0.1t)$, $s_3^a = \sin(2t)$ and $s_4^a = 0$. For the parameters of the auxiliary controller, there are $\iota_1 = 25$, $\iota_2 = 35$, $\iota_3 = 35$ and $\iota_4 = 0$.

The output of the system under the control law (18) in the idea environment is shown in Figure 5. From it, it can be found that the system could realize the accurate current sharing control among batteries under the control law (18) without cyber attacks. However, the outputs of the system in the presence of cyber attacks such as DoS attacks, FDI attacks, or a mixture of the two, are shown in Figure 5b–d. It is clear that FDI attacks prevent the output consensus of 1st battery and 2nd battery. Therein, FDI attacks for 3rd battery are the harmonic attacks, and this system still can realize output consensus. For 1st and 2nd battery, FDI attacks are the compound attacks, and they cannot realize the output consensus. Meanwhile, it can be found that DoS attacks make the system no update. These are consistent with the assumptions of cyber attacks. Based on this, the auxiliary controller is introduced in equation (27). The output of this system considering DoS and FDI attacks under the control law (27) is shown in Figure 6. As can be seen from the Figure 6a,b, this system realizes the output consensus, i.e., accurate current sharing among batteries, even

if there are multiple cyber attacks in this system. The feasibility of this control law (27) is proved.

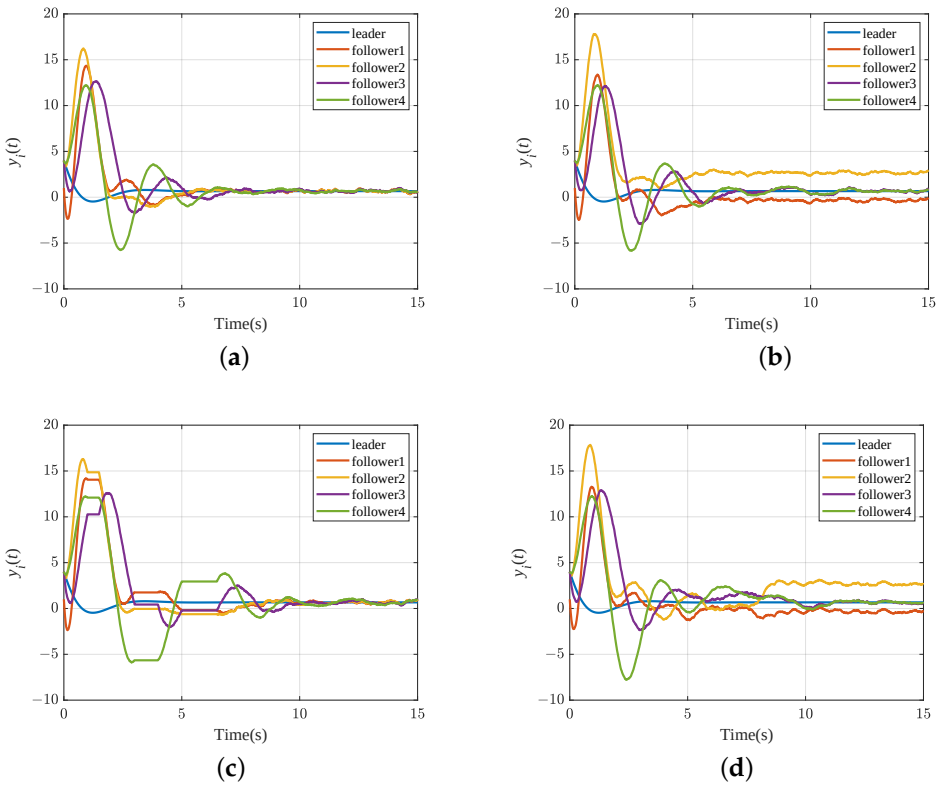

Figure 5. The output of system (17) under the control law (18): (**a**) no network attacks; (**b**) FDI attacks; (**c**) DoS attacks; (**d**) FDI and DoS attacks.

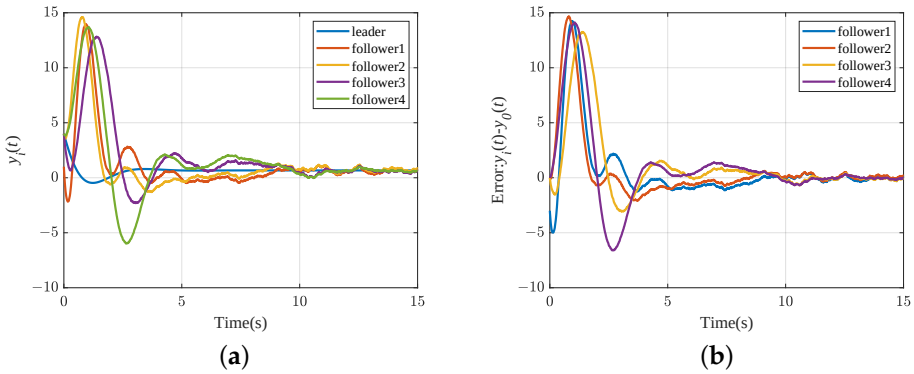

Figure 6. The output of the system (23) under the proposed control law (27): (**a**) outputs of this system; (**b**) output errors of this system.

However, this control law (27) does not take into account the burden of communication among batteries. In order to reduce the burden of communication among batteries, the FLC is applied in the BESS.

For the FLC, the parameters of membership functions are shown as follows. Note that the main task is to verify the feasibility, so the membership can be simply set in Figure 7. Therein, $h_i = 1$ and $m_1 = m_2 = 0.48$, $m_3 = m_4 = 1.33$. Based on Equation (24), the memberships of the d could be set as triangular membership functions. For the membership function of $\Delta y_i(t)$ in PS, it can be considered as an unnecessary update if $\Delta y_i(t) < 0.02$. The influence of updates on the system becomes increasingly significant with increasing

values of $\Delta y_i(t)$. Based on this, the membership of $\Delta y_i(t)$ is set as a trapezoidal function. Similarly, the other membership functions can be set as trapezoidal functions.

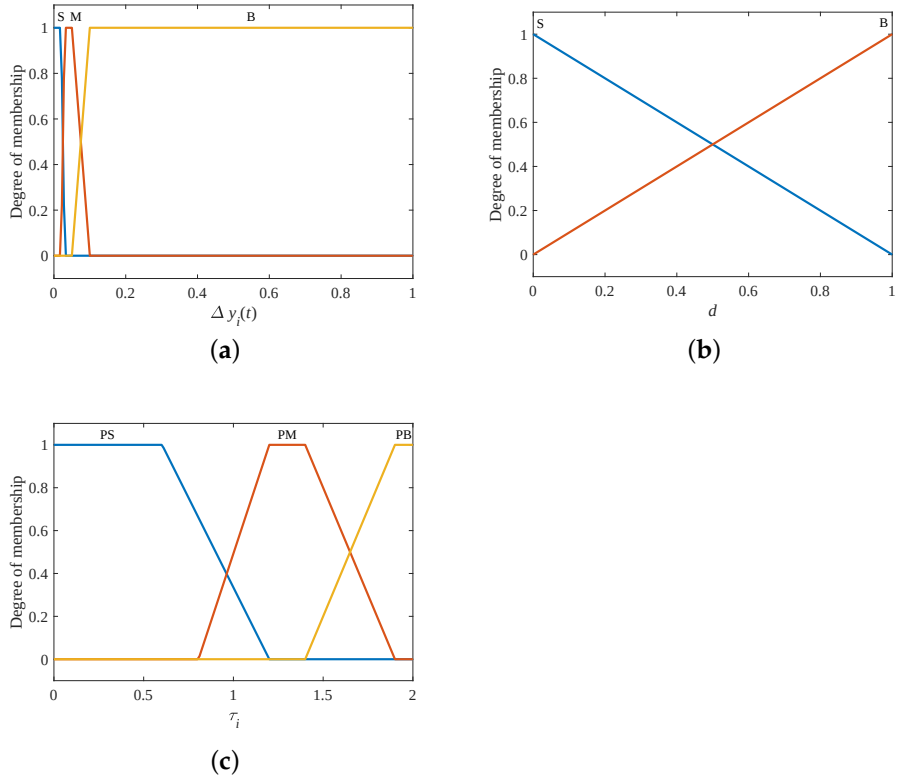

Figure 7. The membership functions of fuzzy logic controller: (**a**) the membership function of $\Delta y_i(t)$; (**b**) the membership function of d; (**c**) the membership function of ι_i.

The output of the system under the control law (29) is shown in Figure 8a. Meanwhile, the events are shown in Figure 8b, which represent the update of the controller.

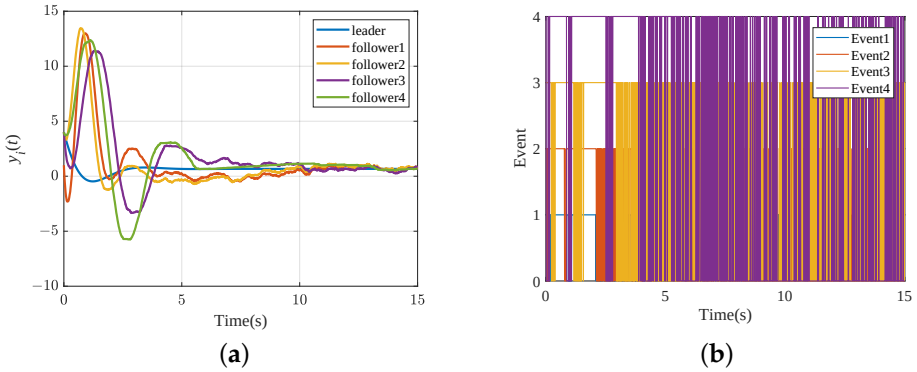

Figure 8. The output of the system under the control law (29): (**a**) the output of this system; (**b**) the update of the controller.

Furthermore, in order to highlight the advantages of the proposed control strategy (29), the comparison simulation results are shown in Table 2. Different from the common output consensus strategy in [33], the proposed control strategy is a kind of resilient control against the cyber attacks. Meanwhile, compared with [28] and [25], this control strategy could realize the output consensus control for the system under DoS and FDI attacks. Moreover, the burden of communication among batteries is reduced by applying the FLC, which is beneficial to the increasing scale of the BESS. Meanwhile, compared with event-triggered

control, the proposed control strategy only needs to set the FLC without complex arithmetic. To sum up, the feasibility of the proposed control strategy is proved.

Table 2. Performance comparison.

Scheme	Resilient Control Type	Need Continuous Information	Average Controller Update	Mean Sample Time
Condition [28]	DoS	Yes	1500	0.010
Condition [25]	FDI	Yes	1500	0.010
Condition (29)	Both	No	835	0.018

5. Experiment Results

In this section, the controller hardware-in-the-loop (CHIL) experiment is carried out to further verify the accurate current sharing for the BESS under the proposed control strategy via the StarSim HIL real-time simulator. In this experiment, the control strategy for four inverters are considered in the DSP (TMS320F28335) controller when the other parts of the system are simulated in the StarSim HIL real-time simulator. This is shown in Figure 9. The line parameters are selected as $R_{01} = 1.00\ \Omega$, $R_{12} = 0.40\ \Omega$, $R_{23} = 0.20\ \Omega$, $R_{30} = 0.50\ \Omega$. The resistive loads are shown as $R_{L0} = 1.30\ \Omega$, $R_{L1} = 2.30\ \Omega$, $R_{L2} = 1.30\ \Omega$, $R_{L3} = 2.30\ \Omega$. For the PnP controller, the relevant parameters are shown as $p_{0,1} = p_{2,1} = -1.00$, $p_{1,1} = p_{3,1} = -3.00$, $p_{0,2} = p_{2,2} = -3.50$, $p_{1,2} = p_{3,2} = -5.60$, $p_{0,3} = p_{1,3} = p_{2,3} = p_{3,3} = 2.00$. The parameters of PI controller are shown as $k^P = -1.5, k^I = -3$. At the beginning, the SoC of each battery is 90%, and the ratio of rated capacities of these four batteries is chosen as 2:2:1:1. The droop gains of each agent are shown as $n_0 = n_1 = 0.03$, $n_2 = n_3 = 0.06$. And the other parameters are the same as the part of simulations in Section 4.

Based on this, the experiment is texted via the StarSim HIL simulator. Meanwhile, in order to better show the performance of proposed strategy, the time of this system is selected as [0 s, 25 s]. And the control strategy in [28] and proposed control strategy (29) are applied, separately. Before t = 10 s, this system applies the control strategy in [28]. After that, the proposed control strategy is applied. The output current is shown in Figure 10. Before 10 s, the output current sharing is not realized due to the cyber attacks. After that, the output current sharing is achieved by applying the proposed control strategy. Moreover, according to $\overline{y_i}(t) = n_i I_{fi}$ where $n_i = n_{0i}/SoC$, there is $I_{fi} = \frac{1}{n_i}$ when the outputs of each agent achieve the output consensus, i.e., the current sharing among batteries. Thus, the output current of each agent should meet $2:2:1:1$. As shown in Figure 10, the output currents are $24A, 24A, 12A$, and $12A$, separately. The performance of the proposed strategy is verified.

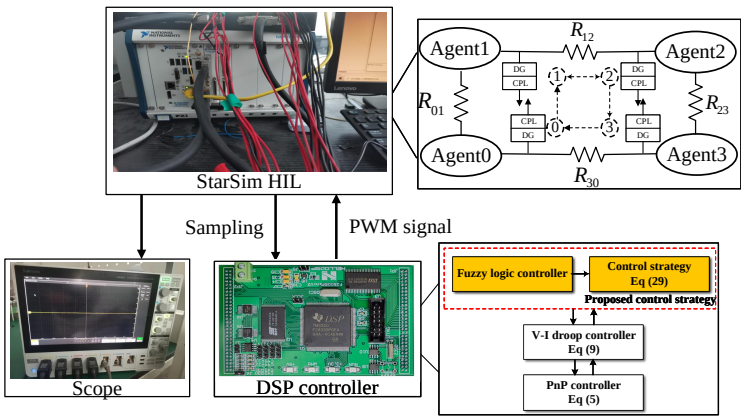

Figure 9. The StarSim HIL experiment system.

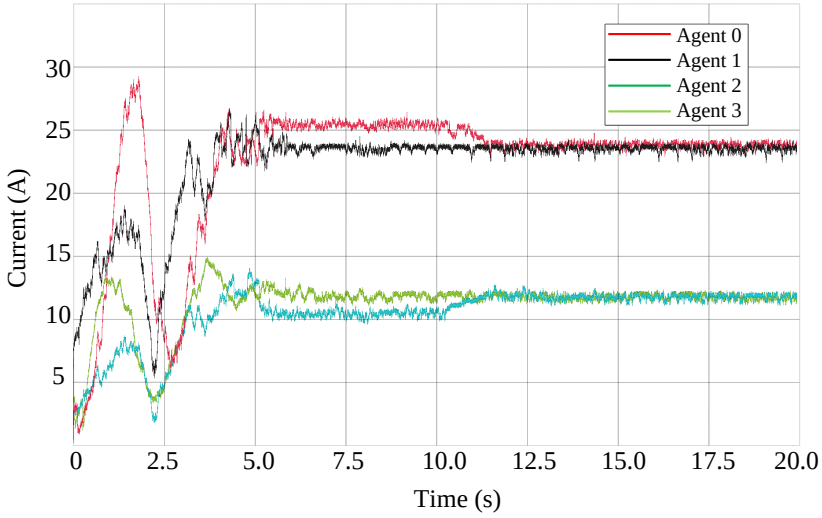

Figure 10. The output current of the system.

6. Conclusions

Sine DGs have been widely applied in DC microgrids, the BESS have been widely applied to compensate the power imbalance between DGs and loads. However, the impact of disturbance, DGs, CPLs and cyber attacks on this system have not been simultaneously considered. Thus, a distributed control strategy is proposed in this paper, which could realize the accurate current sharing and operate normally in the presence of multiple cyber attacks. Compared with the previous literature, this paper has the following contributions:

1. The whole model of the BESS in DC microgrids embedded into disturbance items, DGs, CPLs, and resistive loads, has been built in this paper. Furthermore, it can be further transformed into the linear heterogeneous multi-agent system, which lays the foundation for the following control strategy.
2. The model of DoS and FDI attacks for this system have been built. Different from previous literatures, the FDI attacks are a kind of continuous attack in this paper. Based on this, the state-space function model considering DoS and FDI attacks has been built.
3. To further reduce the burden of communication among batteries, the FLC has been applied in this system.
4. Based on the proposed system model and the FLC, a new distributed fuzzy output consensus control strategy is proposed to realize accurate current sharing control among batteries in the presence of DoS and FDI attacks.

Compared with the literature [25,33], the accurate current sharing among batteries in the presence of DoS and FDI attacks has been realized and the burden of communication has also been further reduced by applying the FLC. Finally, the numerical simulation examples have been provided to verify the feasibility of the proposed control strategy.

Author Contributions: Methodology, X.T.; Software, S.Z.; Validation, X.T.; Investigation, B.H.; Resources, W.W.; Writing—original draft, X.T.; Writing—review & editing, L.Z. and R.W.; Project administration, R.W. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported by the National Natural Science Foundation of China under Grant 52307194, in part by the Young Elite Scientists Sponsorship Program by CAST under Grant YESS20230026, in part by the Guangdong Basic and Applied Basic Research Foundation under Grant 2021A1515110915, in part by the Fundamental Research Funds for the Central Universities in China under Grant N2204014, Liaoning Provincial Science and Technology Program-Natural Science Foundation of the Department of Science and Technology under Grant 2023-BS-056 (Corresponding authors: Rui Wang).

Data Availability Statement: Data are contained within the article.

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

References

1. Ma, D.; Hu, X.; Zhang, H.; Sun, Q.; Xie, X. A Hierarchical Event Detection Method Based on Spectral Theory of Multidimensional Matrix for Power System. *IEEE Trans. Syst. Man Cybern. Syst.* **2021**, *51*, 2173–2186. [CrossRef]
2. Wang, R.; Sun, Q.; Hu, W.; Xiao, J.; Zhang, H.; Wang, P. Stability-Oriented Droop Coefficients Region Identification for Inverters Within Weak Grid: An Impedance-Based Approach. *IEEE Trans. Syst. Man Cybern. Syst.* **2021**, *51*, 2258–2268. [CrossRef]
3. Rey, J.M.; Rosero, C.X.; Velasco, M.; Martí, P.; Miret, J.; Castilla, M. Local Frequency Restoration for Droop-Controlled Parallel Inverters in Islanded Microgrids. *IEEE Trans. Energy Convers.* **2019**, *34*, 1232–1241. [CrossRef]
4. Potty, K.A.; Bauer, E.; Li, H.; Wang, J. Smart Resistor: Stabilization of DC Microgrids Containing Constant Power Loads Using High-Bandwidth Power Converters and Energy Storage. *IEEE Trans. Power Electron.* **2020**, *35*, 957–967. [CrossRef]
5. Xu, Q.; Jiang, W.; Blaabjerg, F.; Zhang, C.; Zhang, X.; Fernando, T. Backstepping Control for Large Signal Stability of High Boost Ratio Interleaved Converter Interfaced DC Microgrids With Constant Power Loads. *IEEE Trans. Power Electron.* **2020**, *35*, 5397–5407. [CrossRef]
6. Mukherjee, N.; De, D. A New State-of-Charge Control Derivation Method for Hybrid Battery Type Integration. *IEEE Trans. Energy Convers.* **2017**, *32*, 866–875. [CrossRef]
7. Wang, R.; Sun, Q.; Han, J.; Zhou, J.; Hu, W.; Zhang, H.; Wang, P. Energy-Management Strategy of Battery Energy Storage Systems in DC Microgrids: A Distributed Dynamic Event-Triggered H ∞ Consensus Control. *IEEE Trans. Syst. Man Cybern. Syst.* **2022**, *52*, 5692–5701. [CrossRef]
8. Marroyo, L.; Sanchis, P.; Urtasun, A. State-of-charge-based droop control for stand-alone AC supply systems with distributed energy storage. *Energy Convers. Manag.* **2015**, *106*, 709–720. [CrossRef]
9. Wang, R.; Sun, Q.; Ma, D.; Liu, Z. The Small-Signal Stability Analysis of the Droop-Controlled Converter in Electromagnetic Timescale. *IEEE Trans. Sustain. Energy* **2019**, *10*, 1459–1469. [CrossRef]
10. Huang, W.; Abu Qahouq, J.A. Energy Sharing Control Scheme for State-of-Charge Balancing of Distributed Battery Energy Storage System. *IEEE Trans. Ind. Electron.* **2015**, *62*, 2764–2776. [CrossRef]
11. Zhou, J.; Xu, Y.; Sun, H.; Wang, L.; Chow, M.Y. Distributed Event-Triggered H_∞ Consensus Based Current Sharing Control of DC Microgrids Considering Uncertainties. *IEEE Trans. Ind. Inform.* **2020**, *16*, 7413–7425. [CrossRef]
12. Morstyn, T.; Hredzak, B.; Agelidis, V.G. Distributed Cooperative Control of Microgrid Storage. *IEEE Trans. Power Syst.* **2015**, *30*, 2780–2789. [CrossRef]
13. Cai, H.; Hu, G. Distributed Control Scheme for Package-Level State-of-Charge Balancing of Grid-Connected Battery Energy Storage System. *IEEE Trans. Ind. Inform.* **2016**, *12*, 1919–1929. [CrossRef]
14. Hoang, K.D.; Lee, H.H. Accurate Power Sharing With Balanced Battery State of Charge in Distributed DC Microgrid. *IEEE Trans. Ind. Electron.* **2019**, *66*, 1883–1893. [CrossRef]
15. Chen, X.; Hu, S.; Li, Y.; Yue, D.; Dou, C.; Ding, L. 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* **2022**, *13*, 2357–2368. [CrossRef]
16. Chu, Z.; Zhang, J.; Kosut, O.; Sankar, L. Vulnerability Assessment of Large-scale Power Systems to False Data Injection Attacks. In Proceedings of the 2020 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), Tempe, AZ, USA, 11–13 November 2020.
17. Beg, O.A.; Johnson, T.T.; Davoudi, A. Detection of False-Data Injection Attacks in Cyber-Physical DC Microgrids. *IEEE Trans. Ind. Inform.* **2017**, *13*, 2693–2703. [CrossRef]
18. Beg, O.A.; Nguyen, L.V.; Johnson, T.T.; Davoudi, A. Signal Temporal Logic-Based Attack Detection in DC Microgrids. *IEEE Trans. Smart Grid* **2019**, *10*, 3585–3595. [CrossRef]
19. Sahoo, S.; Peng, J.C.H.; Devakumar, A.; Mishra, S.; Dragičević, T. On Detection of False Data in Cooperative DC Microgrids—A Discordant Element Approach. *IEEE Trans. Ind. Electron.* **2020**, *67*, 6562–6571. [CrossRef]
20. Gallo, A.J.; Turan, M.S.; Boem, F.; Parisini, T.; Ferrari-Trecate, G. A Distributed Cyber-Attack Detection Scheme With Application to DC Microgrids. *IEEE Trans. Autom. Control* **2020**, *65*, 3800–3815. [CrossRef]
21. Bompard, E.; Napoli, R.; Xue, F. Vulnerability of interconnected power systems to malicious attacks under limited information. *Eur. Trans. Electr. Power* **2013**, *18*, 820–834. [CrossRef]
22. Abhinav, S.; Modares, H.; Lewis, F.L.; Davoudi, A. Resilient Cooperative Control of DC Microgrids. *IEEE Trans. Smart Grid* **2019**, *10*, 1083–1085. [CrossRef]
23. Habibi, M.R.; Baghaee, H.R.; Dragičević, T.; Blaabjerg, F. False data injection cyber-attacks mitigation in parallel DC/DC converters based on artificial neural networks. *IEEE Trans. Circuits Syst. II Express Briefs* **2020**, *68*, 717–721. [CrossRef]
24. Sahoo, S.; Dragičević, T.; Blaabjerg, F. An event-driven resilient control strategy for dc microgrids. *IEEE Trans. Power Electron.* **2020**, *35*, 13714–13724. [CrossRef]
25. Huo, S.; Huang, D.; Zhang, Y. Secure output synchronization of heterogeneous multi-agent systemsagainst false data injection attacks. *Sci. China Inf. Sci.* **2022**, *65*, 162204. [CrossRef]
26. Liu, X.K.; Wen, C.; Xu, Q.; Wang, Y.W. Resilient control and analysis for DC microgrid system under DoS and impulsive FDI attacks. *IEEE Trans. Smart Grid* **2021**, *12*, 3742–3754. [CrossRef]

27. Feng, Z.; Hu, G. Secure Cooperative Event-Triggered Control of Linear Multiagent Systems Under DoS Attacks. *IEEE Trans. Control Syst. Technol.* **2020**, *28*, 741–752. [CrossRef]
28. Zhang, D.; Liu, L.; Feng, G. Consensus of Heterogeneous Linear Multiagent Systems Subject to Aperiodic Sampled-Data and DoS Attack. *IEEE Trans. Cybern.* **2019**, *49*, 1501–1511. [CrossRef]
29. Hu, S.; Yuan, P.; Yue, D.; Dou, C.; Cheng, Z.; Zhang, Y. Attack-Resilient Event-Triggered Controller Design of DC Microgrids Under DoS Attacks. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2020**, *67*, 699–710. [CrossRef]
30. Wu, W.; Chen, Y.; Zhou, L.; Luo, A.; Zhou, X.; He, Z.; Yang, L.; Xie, Z.; Liu, J.; Zhang, M. Sequence Impedance Modeling and Stability Comparative Analysis of Voltage-Controlled VSGs and Current-Controlled VSGs. *IEEE Trans. Ind. Electron.* **2019**, *66*, 6460–6472. [CrossRef]
31. Han, R.; Meng, L.; Guerrero, J.M.; Vasquez, J.C. Distributed Nonlinear Control with Event-Triggered Communication to Achieve Current-Sharing and Voltage Regulation in DC Microgrids. *IEEE Trans. Power Electron.* **2018**, *33*, 6416–6433. [CrossRef]
32. Sadabadi, M.S.; Shafiee, Q.; Karimi, A. Plug-and-Play Robust Voltage Control of DC Microgrids. *IEEE Trans. Smart Grid* **2018**, *9*, 6886–6896. [CrossRef]
33. Han, J.; Zhang, H.; Jiang, H.; Sun, X. H_∞consensus for linear heterogeneous multi-agent systems with state and output feedback control. *Neurocomputing* **2017**, *275*, 2635–2644. [CrossRef]
34. He, W.; Xu, W.; Ge, X.; Han, Q.L.; Du, W.; Qian, F. Secure Control of Multiagent Systems Against Malicious Attacks: A Brief Survey. *IEEE Trans. Ind. Inform.* **2022**, *18*, 3595–3608. [CrossRef]
35. Zhao, H.; Shan, J.; Peng, L.; Yu, H. Data-Driven Event-Triggered Bipartite Consensus for Multi-Agent Systems Preventing DoS Attacks. *IEEE Control Syst. Lett.* **2023**, *7*, 1915–1920. [CrossRef]
36. Carl, G.; Kesidis, G.; Brooks, R.; Rai, S. Denial-of-service attack-detection techniques. *IEEE Internet Comput.* **2006**, *10*, 82–89. [CrossRef]
37. Arcos-Aviles, D.; Pascual, J.; Marroyo, L.; Sanchis, P.; Guinjoan, F. Fuzzy Logic-Based Energy Management System Design for Residential Grid-Connected Microgrids. *IEEE Trans. Smart Grid* **2018**, *9*, 530–543. [CrossRef]
38. Zhang, H.; Lewis, F.L.; Das, A. Optimal Design for Synchronization of Cooperative Systems: State Feedback, Observer and Output Feedback. *IEEE Trans. Autom. Control* **2011**, *56*, 1948–1952. [CrossRef]
39. Tian, X.; Jiang, C.; Qian, B.; Wang, R. Current sharing control strategy with uncertainties and network attacks for electric vehicle charging station. *IET Energy Syst. Integr.* **2023**. [CrossRef]