A Resilience Enhanced Secondary Control for AC Micro-grids

Xiao, Junjie; Wang, Lu; Qin, Zian; Bauer, Pavol

DOI
10.1109/TSG.2023.3268245

Publication date
2024

Document Version
Final published version

Published in
IEEE Transactions on Smart Grid

Citation (APA)
Xiao, J., Wang, L., Qin, Z., & Bauer, P. (2024). A Resilience Enhanced Secondary Control for AC Micro-grids. *IEEE Transactions on Smart Grid*, *15*(1), 810 - 820. https://doi.org/10.1109/TSG.2023.3268245

A Resilience Enhanced Secondary Control for AC Micro-Grids

Junjie Xiao, *Graduate Student Member, IEEE*, Lu Wang, *Graduate Student Member, IEEE*, Zian Qin, *Senior Member, IEEE*, and Pavol Bauer, *Senior Member, IEEE*

***Abstract*—Communication-based distributed secondary control is deemed necessary to restore the state of islanding AC microgrids to set points. As its limited global information, the microgrids become vulnerable to cyber-attacks, which by falsifying the communicating singles, like the angular frequency, can disturb the power dispatch in the microgrids or even induce blackout by pushing the microgrids beyond the safe operation area and triggering the protection. To make the microgrids more cyber secure, adaptive resilient control for the secondary frequency regulation is proposed. It assumes that each converter is communicating with its adjacent converters. With the proposed control, the weight of the communication channel being attacked is automatically reduced, and the more the communicating signals are falsified, the further the weight of that communication channel is weakened. The proposed approach does not rely on attack detection and thereby is easy to implement; Besides, it still works when challenged by a combination of multi-attack signals; Moreover, it applies to multiple communication lines getting attacked cases. Finally, the effectiveness and feasibility of the proposed resilient control scheme are validated by both simulations and experimental results.**

***Index Terms*—Distributed control, adaptive control, cyber-attack, AC micro-grid.**

I. Introduction

MICROGRID is a prospective power system adapted to the needs of the industrial world by integrating emerging resources such as fuel cells, solar power units, micro wind turbines, and distributed generation (DG) [1].

Distributed Secondary Control (DSC) is gaining popularity for AC microgrids, with which the set point of a converter is calculated following the information of the neighbour converters to regulate the output voltage. By avoiding a centralized secondary control, the AC microgrid is immunized to a single failure in the controller [2]. However, limited global information makes it vulnerable to cyber attacks, which may affect control accuracy and system stability [3].

Manuscript received 27 October 2022; revised 7 January 2023 and 6 March 2023; accepted 8 April 2023. Date of publication 18 April 2023; date of current version 26 December 2023. This work was supported by China Scholarship Council under Grant 202106280042. Paper no. TSG-01610-2022. *(Corresponding author: Zian Qin.)*

The authors are with the Department of Electrical Sustainable Energy, DCE&S Group, Delft University of Technology, 2628 CD Delft, The Netherlands (e-mail: J.Xiao-2@tudelft.nl; L.Wang-11@tudelft.nl; z.qin-2@tudelft.nl; P.Bauer@tudelft.nl).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TSG.2023.3268245.

Digital Object Identifier 10.1109/TSG.2023.3268245

Among different kinds of cyber attacks, False Data Injection attacks (FDIAs) [4], and Denial-of-Service (DoS) attacks [5] are the two most widely discussed cyber-attacks relevant in Microgrids. These attacks jeopardize the confidentiality, integrity, and availability of information in the microgrid, disrupt control objectives, and deserve attention.

Moreover, a series of recent cyber attack security incidents have demonstrated that the existing technology is insufficient to defend against hackers' elaborate virus data [6].

A review of the previous work suggests that the responses to cyber attacks fall into three types of mechanisms [7]: a) prevention: to avoid directing cyber attacks onto the system, b) resilience: to endure the most significant of an attack and to operate as close to normality as possible, and c) attack detection and isolation: recognize the target of the attack, to isolate the damaged subsystem, and to recover the usual pattern as efficiently as possible.

In reality, it is impossible to establish a communication infrastructure that avoids any cyber attack, so the microgrid should have some resilience to operate under cyber attacks and reduce the damage. Once the microgrid gets attacked, the attack will be detected and classified, and then the resilient scheme should be employed to make the system more robust. Then, the controller should isolate the severely infected unit immediately to save the whole system. Therefore, to meet data privacy demands and microgrid stability, cyber security deserves additional investigation [8].

A resilience enhance controller equipped with a detector is a traditional way to mitigate cyber-attacks. Different cyber-attack detection methods could be broadly classified into two types. The Kalman filter-based detector in [9] and [10] serves to identify FDIA in power systems. Nevertheless, a well-designed cyber attack with in-depth knowledge of the system is likely to hinder state estimation [11]. In [12], sliding mode control is used to compensate for the attack signal to remove adverse effects. However, the attack signal reconstruction results in a slower controller response. Moreover, this model-based method relies on the systematic model's correctness, making them elusive in practical implementations because of their inevitable mismatch with complicated real-world power electronic systems. In addition, some kinds of intelligent attacks can evade detection by traditional methods, which are pretty challenging to diagnose [13]. Model-free approaches such as AI-based algorithms [14] has also been proven to be prospective methods for cyber-attack detection. However, it increases the computational burden [15]. Obviously, these

detection schemes impose an additional computational burden on the participating units. Inevitably, the dependence on these sophisticated detection algorithms causes the controller to respond slowly to attacks, which is not applicable under demanding case [16], [17].

A further problem concerns that the current work focusing on resilient control-related projects in microgrid systems mainly considers only a single attack. For example, the stability conditions of microgrids under DoS attacks have been studied in some detail [18], [19]. Nonetheless, it is also indispensable to consider a combination of DoS and FDIA owing to the different features of various attacks. Besides, in [20], [21], an adaptive law-based approach is presented to promote microgrid resilience by adaptively modifying the consensus gain among the related agents. In [22], the information picked up from the attacked unit is dropped by disabling the corresponding network link as a basic method to avoid spreading attacks to the local controller. However, directly dropping the information propagated by the communication network will disrupt the convergence theories.

Another pending issue is that applied resilient schemes restrict the number of infected agencies. To increase the resilience of the microgrid, an event-trigger resilient control is proposed [23]. The rationale behind such an approach is that a carefully designed event trigger judges the decision to perform a defence mechanism. The corrupted data is reconstructed from the healthy channel data, and intuitively, this method fails when all channels are under attack. In [24], the defence mechanism will not work if over half of the units are under attack. The mitigation scheme proposed in [25] ensures that the grid system remains operational when N-1 out of N units are attacked in a system. This framework generally limits its ability to be resilient to worst-case attacks.

From the above literature review, four significant research gaps of interest can be summarized as follows. (1) The reliance on attack detectors slows down the suppression of attack vectors by controllers [9], [12], [14]; (2) Insufficient research on the combination of cyber attacks [18], [19]; (3) Blocking attacked channels disrupts the convergence law [20], [21], [22]; (4) The resilience method limits the number of infected units [23], [24], [25].

Motivated by the above gaps, this paper proposes an adaptive control method that achieves resilience to implement output voltage restorations and output power sharing of inverters in AC microgrids. The contributions of this paper are listed as follows: 1) The method proposed in this paper is not dependent on detecting cyber attacks and therefore responds fast to attack signals; 2) Two types of attacks and their combination are formulated, and their impacts on MG system performance are demonstrated. In the presence of these attacks, the proposed mechanism can achieve a fast restoration of optimal operational objectives (i.e., proportional active power sharing and frequency restoration); 3) The proposed method dispatches a relatively healthy communication line for propagating information. Thus, it will not stop convergence law in the communication network; 4) The proposed method will not limit the number of attacked units. It still works when all channels are attacked; 5) The proposed defence strategy provides timely mitigation for corrupted participants in a distributed manner without impeding the normal operation of the microgrid, and its stability is verified by Lyapunov Criteria. The adaptability of the proposed control strategy is also tested in various attacks, also including load variations.

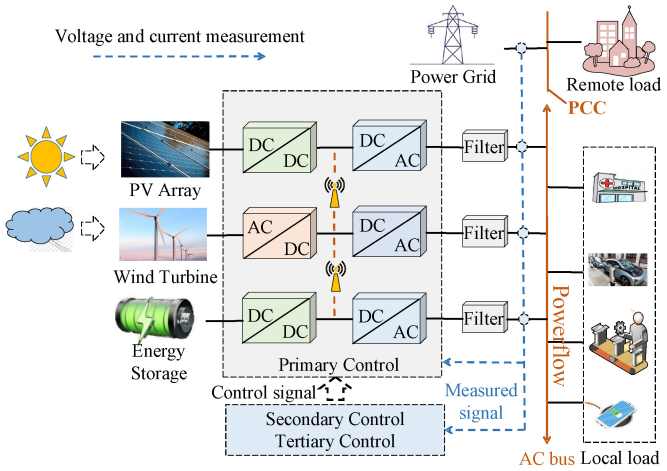

Fig. 1. Block diagram of the microgrid with distributed control.

II. Communication-Based Cooperative Secondary Control Strategy Microgrid

The typical micro-grid and its control program are shown in Fig. 1, where N energy storage units are connected through DC-DC and DC-AC converters and form a cyber-physical system. A sparse communication network connecting different agencies propagates reference information to share the state of each inverter unit. The controller's significant goals are voltage regulation and proportional power-sharing, while the object of the communication control is to realize the optimal operation. To achieve synchrony in islanding ac micro-grids, a hierarchical structure is adopted in this paper where the primary control layer regulates the output voltage while the secondary control layer compensates for the error caused by the primary control.

A. Sparse Communication Network

Our research object is a microgrid system with N inverters operating in islanded operation mode involved in regulating the frequency and amplitude of the voltage to maintain the power balance.

An undirected cyber graph of the communication network is considered to show how the involved converters share data with their neighbours. For every local converter-*ith* of the microgrid, the communication graph with all its neighbours-*jth* can be written as a digraph via edges and links via communication adjacency matrix $A = (a_{ij})_{N\times N}$. The communication weight $a_{ij} = 1$ if the *ith* unit and the *jth* unit are in regular communication; otherwise, $a_{ij} = 0$. The degree of vertex ζ_i is given as $d_i = \sum_{j=1}^{N} a_{ij}$. $D = diag(d_1, \cdots, d_N)$ is the corresponding degree matrix. Further, the Laplacian matrix L of the communication network L is defined as $L = D - A$.

With the sparse communication network outlined above, distributed generation units can communicate with each other to propagate reference information.

B. Primary Droop Control

Droop control is the most widely used primary control strategy for islanded ac microgrids. Droop control [2] philosophy ensures equal active power-sharing. The $P-\omega$ and $Q-V$ droop control mechanism can be written as (1), (2):

$$\omega_i = \omega_{si} + m_{Pi}\left(P_{iref} - P_i\right). \tag{1}$$

$$V_i = V_{si} + n_{Qi}\left(Q_{iref} - Q_i\right). \tag{2}$$

where ω_i and V_i are the output angular frequency and voltage amplitude which are used as a reference to regulate the output voltage; P_{iref} stands for active power reference and Q_{iref} represents reactive power reference; P_i and Q_i are the measured active power and reactive power of *ith* DG; m_{Pi} and n_{Qi} are the corresponding droop coefficient of the P/Q loop, which are given according to the power-sharing ratio; ω_{si} and V_{si} are the frequency and voltage set points, respectively, which are defined by the secondary control layer.

C. Distributed Secondary Control

The droop control method suffers from frequency and voltage amplitude deviation. Therefore, the secondary control strategy is employed to restore the frequency and voltage amplitude [22], [26]. Differentiating the droop characteristic in (1) yields:

$$\dot{\omega}_i = \dot{\omega}_{si} - m_{Pi}\dot{P}_i. \tag{3}$$

$$\dot{\omega}_{si} = \int \vartheta\, dt = \int \left(\dot{\omega}_i + \dot{\delta}_i\right)dt = \int \left(\vartheta_i^{\omega} + \vartheta_i^{\delta}\right)dt \tag{4}$$

where $\delta_i = m_{Pi}P_i$ and ϑ_i are the auxiliary control input for adjusting the secondary control set-points.

$$\vartheta_i^{\omega} = K_{\omega}\left[\sum_{j\in Ni} a_{ij}\left(\omega_j - \omega_i\right) + g_i(\omega_0 - \omega_i)\right] \tag{5}$$

$$\vartheta_i^{\delta} = K_{\delta}\sum_{j\in Ni} a_{ij}\left(\delta_j - \delta_i\right) \tag{6}$$

where the loop gain $g_i = 1$ is a pinning gain in island mode when the secondary control is enabled; The convergence coefficient $K_{\omega} > 0$ and we will give the detail of parameter selection in the later chapters; ω_0 is the nominal amplitude-frequency which is predefined; ϑ_i^{ω} is employed to maintain the frequency synchronized among different agencies and promise frequency coverage to ω_0 at last. With ϑ_i^{δ}, the active power during the whole process of microgrid operation is proportionally shared by all converters.

The research objective of this paper is an inverter-connected island microgrid, and the control diagram of each converter is shown in Fig. 2. It should be noticed that this paper focuses on frequency set-point ω_{si}. The voltage set-point V_{si} comes from a voltage-reactive power control loop. With the proposed distributed secondary control algorithm, the microgrid in islanding mode can recover the frequency and share the power proportionally among the participant converters. The control

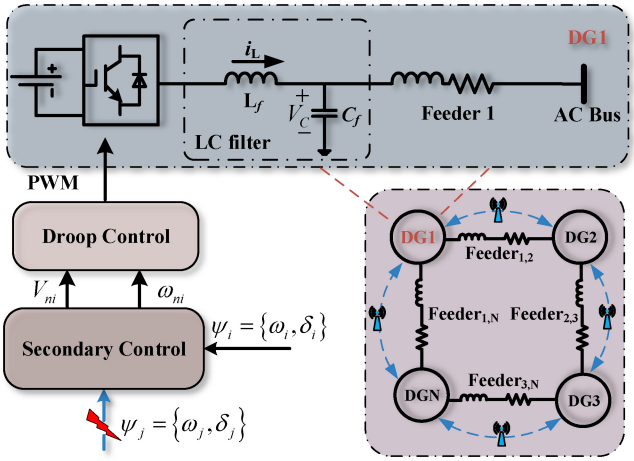

Fig. 2. The control diagram of an AC microgrid with distributed secondary control strategy consisting of N converters.

objective for the active power control loop can be represented as follows:

$$\lim_{i\to\infty} \omega_i(t) = \omega_0, \forall i \in \{1, 2, \ldots, N\} \tag{7}$$

$$\lim_{i\to\infty} m_{Pi}P_i(t) = \lim_{i\to\infty} m_{Pj}P_j(t) \tag{8}$$

III. Cyber Attack on Inverter Control

As we discussed before, the distributed secondary control can keep synchronizing frequency. However, the malicious can destabilize the AC microgrids depending on the attack intensity. This section introduces and models the false data injection attack (FDIA) and the denial of service (DoS) attack. Then, we formulate the secondary resilience synchronization problem for island AC microgrids in the presence of FDIA and DoS attacks. Herein, we only consider the modelling of the secondary frequency control and cyber-attacks model in the frequency data exchanging process in this paper. It should be noted that this procedure can also be extended to the active power control loop and secondary reactive-voltage control loop.

A. Modeling of the Cyber Attack

The proposed distributed control framework given by (5) and (6) relies heavily on exchanging $\varphi_j = \{\omega_j, \delta_j\}$ among different converters, which makes the cyber-physical system vulnerable to cyber-attacks. FDIA and DoS attacks are typical cyber-attacks. FDIA can be modelled as false data injection [12] while DoS attacks can be considered failing to get the information of the neighbouring converters [27]. Cyber attacks on the frequency propagation channel from the neighbouring agent can be modelled in (9).

$$\omega_{a,j} = K_j\left[\omega_j + \eta_j\varepsilon(t)\right] \tag{9}$$

where $\omega_{a,j}$ denotes the frequency information corrupted by cyber attack. ω_j represents the real frequency signal of the *jth* agent. η_j and K_j are both binary variables which indicate the existence of FDIA and DoS attack as shown in Table I.

Specifically, $\eta_j = 0$ and $K_j = 0$ indicate there is only a DoS attack; $\eta_j = 0$ and $K_j = 1$ manifest the microgrid system

TABLE I
CHARACTERIZATION OF THE FDIA AND DOS ATTACK

	$K_j = 0$	$K_j = 1$
$\eta_j = 0$	DoS	normal state
$\eta_j = 1$	FDIA and DoS	FDIA

works in the normal state without any cyber-attack; $\eta_j = 1$ and $K_j = 0$ represent the system is challenged by DoS attack and FDIA at the same time; while $\eta_j = 1$ and $K_j = 1$ denote the presence of FDIA with the malicious element $\varepsilon(t)$;

In the presence of cyber attacks, (5) can be rewritten as (10)

$$\dot{\omega}_i = K_\omega \left[\sum_{j \in Ni} a_{ij}\left(\omega_{a,j} - \omega_i\right) + g_i(\omega_0 - \omega_i) \right] \tag{10}$$

The state error e_i, which is expected to be 0, is defined as the error between the *ith* inverters' frequency and the nominal frequency, i.e., $e_i = \omega_i - \omega_0$. The dynamics of state errors with attacks on communication links are stated as follows:

$$\dot{e}(t) = -K_\omega(L+G)e(t) + B\varepsilon(t) \tag{11}$$

where L is the Laplacian matrix of the communication network. $G = diag(g_1, \ldots, g_N)$ denotes the enabling of secondary control. $K_\omega(L+G)$ characterizes the algebraic connectivity of the augmented communication graph, which suggests the convergence rate of distributed control strategies. Obviously, a large $K_\omega(L+G)$ value results in more efficient communication between the involved inverters, and thereby, information can propagate faster in the neighbour-neighbour communication network. Since the L and G are demonstrated by the communication network, K_ω is the only factor we can adjust the convergence rate of the distributed control strategy in (4) which also affects the speed of frequency synchronization in an islanded ac microgrid. So nonzero values of K_ω are chosen to be sufficiently high. On the other hand, the limitation for K_ω choosing is that the secondary is compensation for the power loop. Thus, the responding speed of the secondary control loop should be lower than the power loop. As the cut-off angular frequency of the power loop's filter is 100 rad/s, K_ω is chosen to be 50 rad/s, half of the inner loop bandwidth. B is the communication network incidence matrix between the cyber attack vector and the state error.

B. Control Problem Statement

According to the described system (11), the state error vector can be represented as:

$$e(t) = e^{-K_\omega(L+G)t}e(t_0) + \int_0^t e^{K_\omega(L+G)(\tau-t)}B\varepsilon(\tau)d\tau \tag{12}$$

If no cyber attacks exist in the microgrid system. In this case, e(t) will gradually reduce to a value that is close to zero since the matrix $-K_\omega(L+G)$ is negative-definite and invertible [22]. When there is a cyber-attack, we assume that the attack signal can be expressed as $\varepsilon(t)$ as we discussed in (9). Furthermore, for a time instant, the fake data can be considered a constant denoted as ε_0. The error will converge to a non-zero value decided by $\varepsilon(t)$ as stated in (13):

$$\begin{aligned} \lim_{t\to\infty} e(t) &= \int_{t_0}^{t} e^{-K_\omega(L+G)(t-\tau)}B\varepsilon(\tau)d\tau \\ &= \lim_{t\to\infty} \frac{1 - e^{-K_\omega(L+G)(t-t_0)}}{K_\omega(L+G)}B\varepsilon_0 \\ &= [K_\omega(L+G)]^{-1}B\varepsilon_0 \end{aligned} \tag{13}$$

As shown in (13), the state error fails to converge to zero with false data infecting the system, which implies that the cyber-attack would impede the synchronization of frequencies. The proposed secondary cooperative control approach expressed as (11) can also be rewritten as follows:

$$\dot{\omega}_i = -K_\omega(L+G)\left(\omega_i - \underbrace{\left(\omega_0' - \Delta\omega_L\right)}_{\omega_0}\right) + B\varepsilon(t) \tag{14}$$

From (14) we can find that there should be a $\Delta\omega_L$ which makes $-K_\omega(L+G)(\Delta\omega_L) + B\varepsilon = 0$. In this case, the state error space equation can be written as follows:

$$\dot{e}_a = -K_\omega(L+G)e_a \tag{15}$$

where $e_a = \omega_i - \omega_0'$. As shown in (15), the output frequency would converge to ω_0', but not the nominal frequency ω_0. As the FDIA is bounded false data, the state error will not diverge. It converges to a non-optimal point determined by the inserted fake data $\varepsilon(t)$.

When the microgrid system is under DoS attack, with the same philosophy to (12)-(15), the output will converge to an abnormal value.

In summary, the cyber-attack signals in communication links would propagate through the sparse communication network, distorting the microgrid operating points and driving the microgrid system away from the optimal operating conditions.

IV. PROPOSED RESILIENT CONTROL AND STABILITY ANALYSIS

In this paper, we employ adaptive philosophy to configure the controller in a manner that can automatically adjust to the varying conditions of cyber attacks. As is shown in Fig. 3, to accomplish attack mitigation in AC microgrids, the following adaptive control framework composed of four terms is proposed (16)-(19):

$$\lambda_{ij} = \kappa|\omega_i - \omega_{a,j}| \tag{16}$$

where λ_{ij} is an auxiliary state of the controller of the *ith* unit. Equation (16) is the attack severity measure term, which is used to calculate the level of the malicious signal. At this moment, we suppose that $\omega_{a,j}$ is the output of various state estimators, such as the Kalman filter in [9], since the effect of noise is excluded. κ is the gain of the cyber attack measure term, which should be designed large enough so that a slight attack contributes significantly to adjusting the communication weight. Intuitively, a larger κ increases the sensitivity of the proposed approach towards attacks. Under the satisfaction of this paper on the cyber attack suppression accuracy, $\kappa = 6$.

$$\Omega_{ij} = e^{-\lambda_{ij}} \tag{17}$$

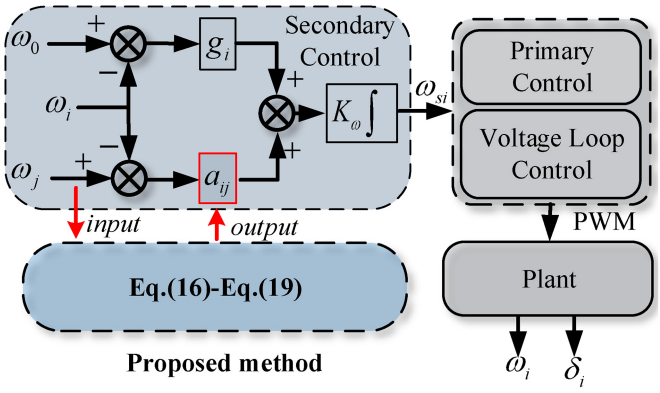

Fig. 3. Proposed resilience scheme for cyber attacks.

In this resilience-enhanced scheme, by (17), the negative relationship between cyber attacks and communication weights is developed. With this term, a more significant attack vector will cause a smaller communication weight. This way, the infected data will not be picked up, and cyber attacks will be rejected. The exponential function is adopted to decrease communication weights because it's more sensitive to attacks than other correlation functions.

$$\rho_{ij} = \Omega_{ij} / \left(\Omega_{ij} + \cdots + \Omega_{iN}\right) \tag{18}$$

In (18), a comparing algorithm is proposed to identify the severity of the attacks on each communication line. It is adopted to choose an optimal communication line when all the neighbours are infected. With this term, the less infected line would be chosen to propagate information.

$$\dot{a}_{ij} = \xi \rho_{ij}(t) - \xi a_{ij} \tag{19}$$

The term (19) is essentially a low pass filter, which is added to prevent unwanted oscillations in the frequency response of converters. ξ demonstrates the cutoff frequency of the Low pass filter. A too-slow response speed will restrict the mitigation speed of the proposed defence strategy. By trade-off between the noise suppression effect of the filter and the response speed of the proposed strategy. We take $\xi = 100$.

By using the proposed controller, the communication weight inputs previously defined in (5) are updated with cyber-attacks as shown in Fig. 3.

Algorithm 1 presents the details of the proposed procedures for mitigating the cyber attack when the communication channels are invaded. To analyze the stability of the proposed method, the following Lyapunov candidate is chosen:

$$v(e) = \frac{1}{2} e^T e \tag{20}$$

The time derivative of $v(e)$ along the trajectories (20) is obtained as follows:

$$\begin{aligned} \dot{v}(e) &= e^T \dot{e} \\ &= -K_\omega (\omega_i - \omega_0)^T [(L+G)(\omega_i - \omega_0) + L\varepsilon(t)] \end{aligned} \tag{21}$$

According to the adaptive law, when one line gets attacked, the communication weight of the corrupted line is sufficiently low, so the cyber attack's impact is almost zero, denoted as $L\varepsilon(t) \approx 0$. Since the matrix $-K_\omega(L+G)$ is negative-definite and inevitable as we discussed before, $\dot{v}(e) < 0, \forall e \neq 0$. Hence, the origin in (20) is globally asymptotically stable. This way, $v(e)$ would eventually converge to zero, meaning the frequency would remain 50Hz.

When all communication lines get attacked, according to the rule of (18), the severe attacks would be disregarded, while the less infected line will cause $L\varepsilon(t)$ will be kept at a relatively small value. The origin in (20) is Lyapunov stable. This way, the error between the real frequency and the nominal point will also be small. In other words, the small error will not affect the operation of the microgrid. This implies that the control objectives in (7) and (8) can be reached relatively satisfactorily even in the presence of a cyber-attack vector.

Algorithm 1 Implementation of the Proposed Mechanism

Real-time calculation procedure
Conventional droop control in (1) and (2)
Input: Adjacent frequency $\omega_{a,j}$.
Output: Communication weight a_{ij}.
Step1: Attack measure in (16).
If $|\omega_i - \omega_{a,j}| = 0$.
  For all adjacent converters, $a_{ij} = 1$.
Else execute step2 to step4
  Step2: Communication weight generation in (17).
  Step3: Attack severity comparison in (18).
  Step4: Low Pass Filter in (19).
  End
End
a_{ij} is updated in distributed secondary control in (5).

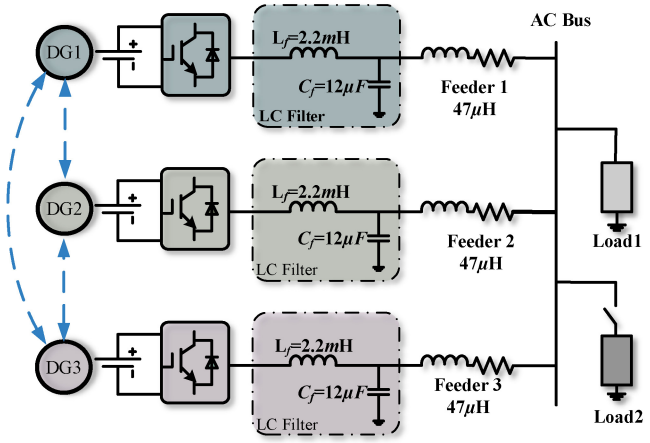

Fig. 4. Verification plant of simulation.

V. Simulation Results

The proposed adaptive control strategy has been tested in a simulation of a distributed AC micro-grid with three inverters connected in parallel to validate its effectiveness, as shown in Fig. 4. In this microgrid system, the output side of the inverters is connected to the AC bus through an LC filter and line impedance.

TABLE II
PARAMETERS OF THE MICROGRID IN SIMULATION

Parameters	Value
Line impedance (L_{line})	47μH
Inductor of LC filter (L_f)	$2.2m$H
Capacitor of LC filter(C_f)	12μF
Inverter 1 active power reference (P_{1ref})	1000
Inverter 2 active power reference (P_{2ref})	2000
Inverter 3 active power reference (P_{3ref})	3000
Droop coefficient of Inverter 1 (m_{P1})	1/1000
Droop coefficient of Inverter 2 (m_{P2})	1/2000
Droop coefficient of Inverter 3 (m_{P3})	1/3000
Convergence coefficient (K_ω)	50
Gain of cyber attack detection term (κ)	6
Coefficient of resilient term filter (ξ)	100
Nominal angular frequency (ω_0)	$314rad/s$
Nominal voltage amplitude	190V

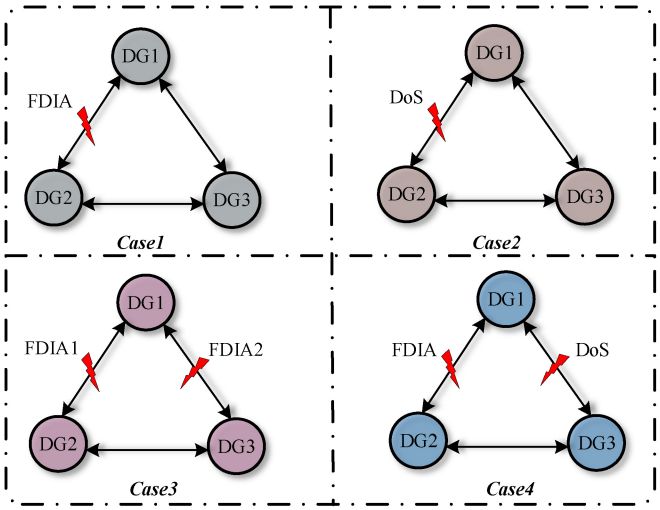

Fig. 5. The illustration of different cases.

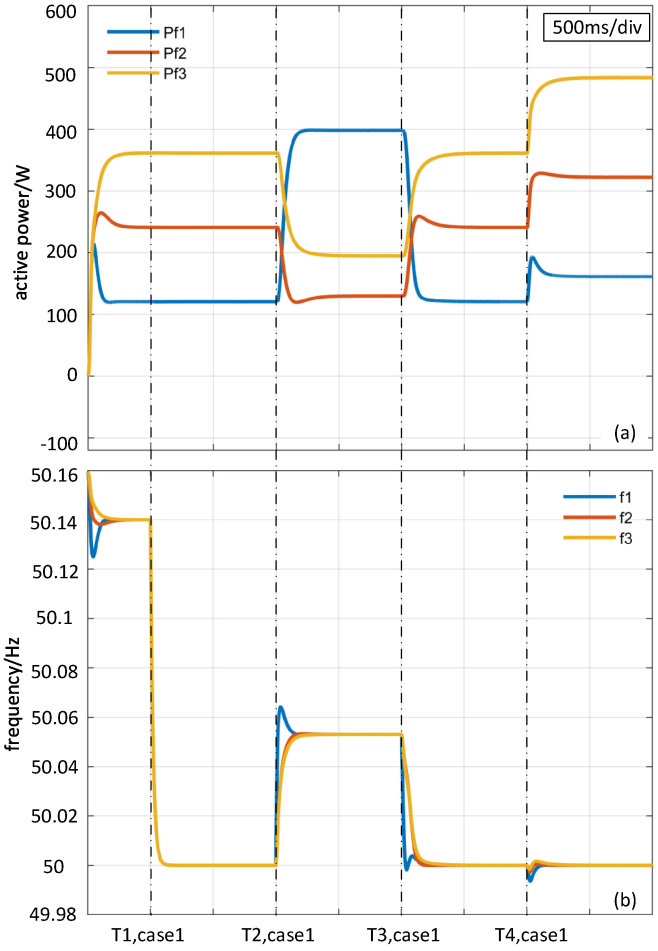

Fig. 6. The performance of the proposed strategy under single FDIA: a) Active power sharing; b) Frequency.

In this paper, the inverters' output active power rate follows the maximum capacity proportion set as 1:2:3. To investigate the influence of the proposed strategy on the load switch, the load is initially set as 720W and then increased by 240W.

Following the structure in Fig. 4, an analysis to investigate the impact of different cyber attacks on active power sharing and frequency convergence of microgrids is carried out. The simulation plant and control parameters of the microgrid are provided in Table II. The following procedures occur in the microgrid successively:

(1) Starting the microgrid;
(2) Activating the secondary control algorithm;
(3) Launching the Cyber attack;
(4) Enabling the defense mechanism;
(5) Switching the Load;

To verify the effectiveness of the proposed adaptive control scheme against FDIA and DoS attacks, four cyber-attack cases are conducted in this paper, as provided in Fig. 5, including:

Case 1: Single FDIA is launched;
Case 2: Single DoS attack is launched;
Case 3: A combination of different levels of FDIA invading all communication lines;
Case 4: A combination of FDIA and DoS attack to invade all communication lines;

In fact, there is a potential Case 5, which consists of DoS attacks acting on different communication lines. As this case has been detailed studied in (19), this paper turns to focus on Case 1-Case 4. As shown in Fig. 5, Case 1 and Case 2 demonstrate the effectiveness of mitigating the cyber attack when one of the communication lines is attacked. Case 3 and Case 4 illustrate all communication lines are aggrieved situations. It should note that for all cases, initially, the output frequency of the microgrid system is around 50.14 Hz as we apply the droop control for providing the proportional active power sharing with the pre-set ratio among participating inverters.

Case1: Single FDIA Corruption

In this case, the communication line 2 to 1 is attacked at *T1,case1* by FDIA. Fig. 6 shows the impact of the FDIA attack in terms of active power and frequency, where the designed FDIA can be modeled as frequency offset. It also shows the performance of the proposed strategy for FDIA mitigation.

In Fig. 6, the active power is proportionally shared among participating inverters at the start stage, and frequencies are restored at the rated 50 Hz after the distributed secondary control method is enabled at *T1,case1*. During the recovering

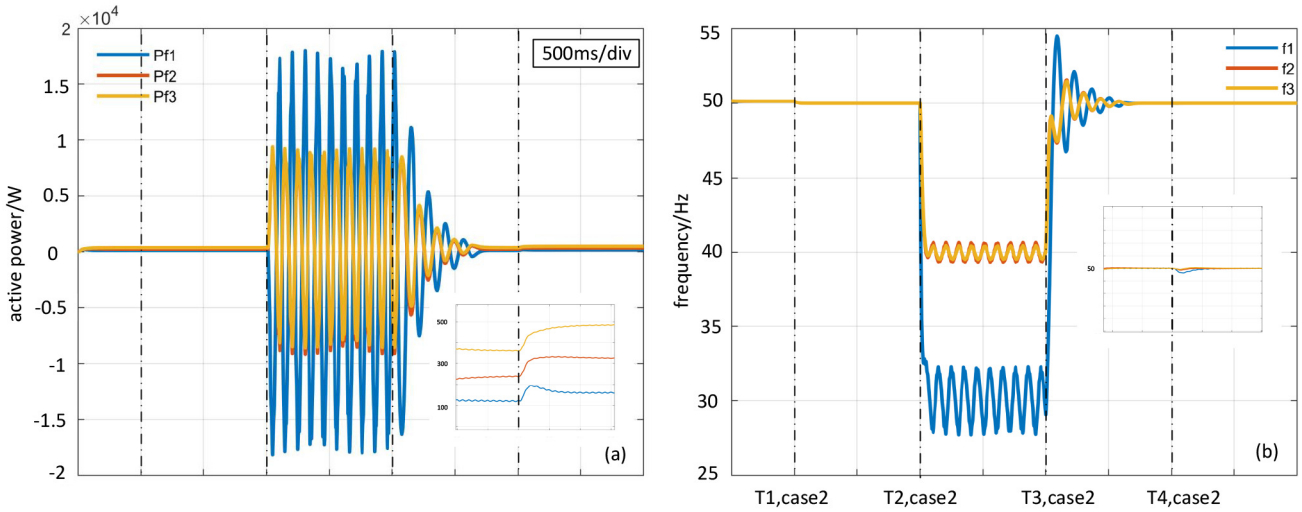

Fig. 7. The performance of the proposed strategy under single DoS: a) Active power sharing; b) Frequency.

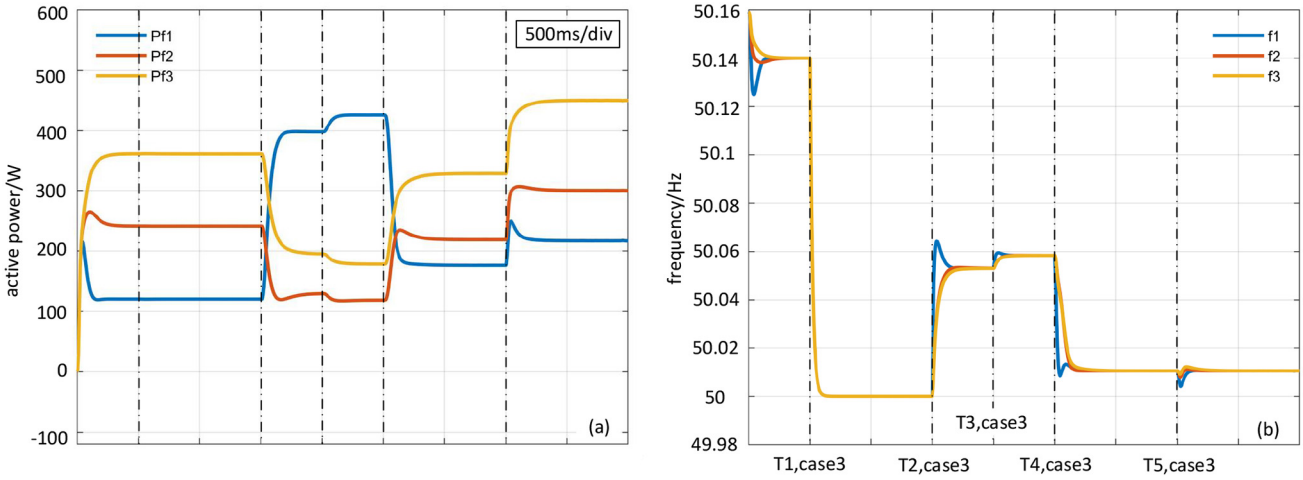

Fig. 8. The performance of the proposed strategy under a combination of FDIAs: a) Active power sharing; b) Frequency.

TABLE III
ATTACK SIGNALS AND MITIGATE THE EFFECTS OF DIFFERENT CASES IN SIMULATIONS

Case	Attack line	False data	Frequency (attacked)	Power ratio (attacked)	Frequency (defense)	Power ratio (defense)
1	Inverte2-Inverter1	1	50.05Hz	3.3:1:1.6	50Hz	1:2:3
2	Inverte3-Inverter1	DoS	Oscillation	Oscillation	50Hz	1:2:3
3	Inverte2-Inverter1 Inverte3-Inverter1	0.1 1	50.06Hz	3.8:1:1.7	50.01Hz	1:1.3:1.9
4	Inverte2-Inverter1 Inverte3-Inverter1	0.1 DoS	Oscillation	Oscillation	50.01Hz	1:1.3:1.9

frequency period, the active power will stay output smoothly because of the active power synchronization term in the distributed secondary control. At *T2,case1*, the information in the network is corrupted by injecting false data $\varepsilon_{2,1}(t) = 1$ on communication line 2-1, which shifts the frequency to about 50.05Hz, and the proportionally active power sharing is interrupted. This implies that the inverter system will not perform at the default nominal frequency point. The inverters cannot share the active power as the capacity ratio. At *T3,case1*, the adaptive scheme is triggered, after which the communication weight of the attacked line is automatically reduced, thus preventing the propagation of the compromised signal. As a result, the frequency will return to 50 Hz, and the active power-sharing ratio will recover from 3.3:1:1.6 to 1:2:3. The present proposed control strategy is also implemented in the load-switching scenario. We add 240W load at *T4,case1*, and the frequency shows regular fluctuations, which will quickly return to the nominal value. In other words, activating the proposed defences will not affect the load-switching features of the microgrid.

Case2: Single DoS Attack Corruption

In this case, The single DoS hack the communication line 2 to 1 at *T2,case1*. Fig. 7 shows the effect of the DoS attack

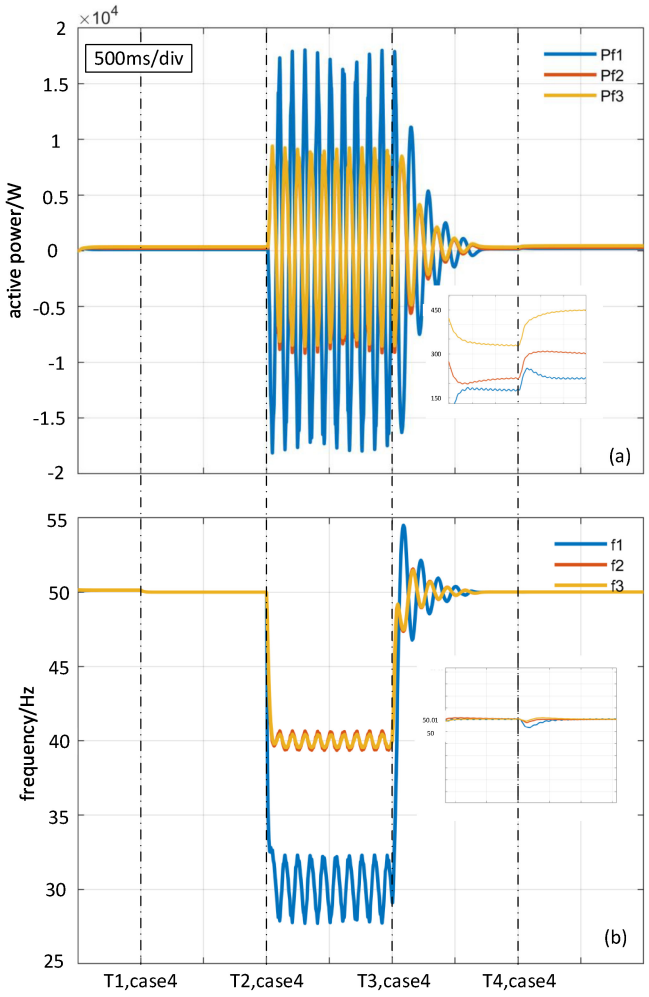

Fig. 9. The performance of the proposed strategy under a combination of FDIA and DoS: a) Active power sharing; b) Frequency.

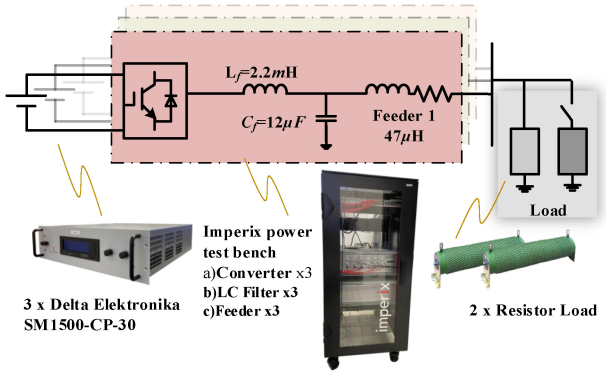

Fig. 10. Experimental setup.

on the output active power and frequency and then indicates the effect of the proposed defence mechanism against the DoS attack. With the cooperation of droop control and distributed secondary control algorithms from *T1,case1*, the frequency and power dispatch of the microgrid are both desirable. However, after the DoS attack is launched at *T2,case2*, the frequency is sharply decreased to break the regular operating limits, and active power will suffer a critical oscillation

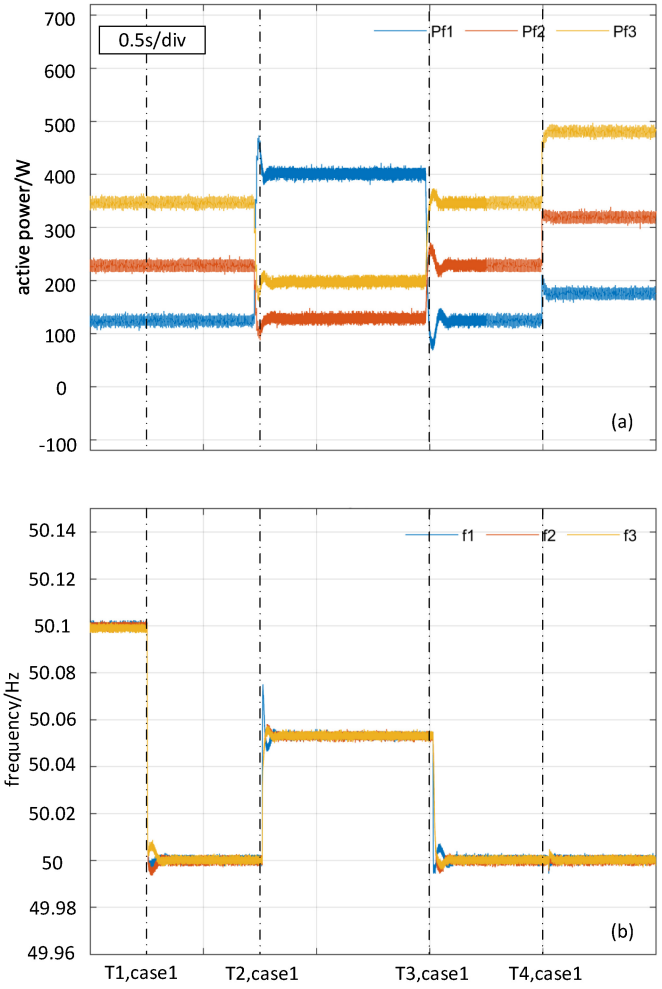

Fig. 11. The performance of the proposed strategy under single FDIA: a) Active power sharing; b) Frequency.

which will destroy the physical inverter-connected system. At *T3,case2*, the proposed strategy is enabled for attenuating the DoS attack effect so that the corrupted signal cannot compromise the overall microgrid system. Subsequently, the frequency restores to 50Hz gradually. The active power-sharing ratio also returns to 1:2:3.

It is notable that with the defence measure, the adverse effect of cyber attacks is eliminated as the system is restored to its normal state.

Case3: A Combination of FDIAs Corruption.

Fig. 8 shows the waveforms of the output frequency and active power of inverters when different levels of FDIA invade all communication lines. Before *T2,case3*, when the system is not subject to any cyber attack, the output frequency and active power are managed by the conventional distributed secondary control to track the reference. False data $\varepsilon_{2,1}(t) = 1$ upon communication line 2-1 is launched at *T2,case3*.

In this case, there would be a frequency deviation from the optimal point because the fake data injected into the communication network leads to a devastating frequency convergence performance. The malicious signals in the attacked communication also disrupt the proportional active power sharing

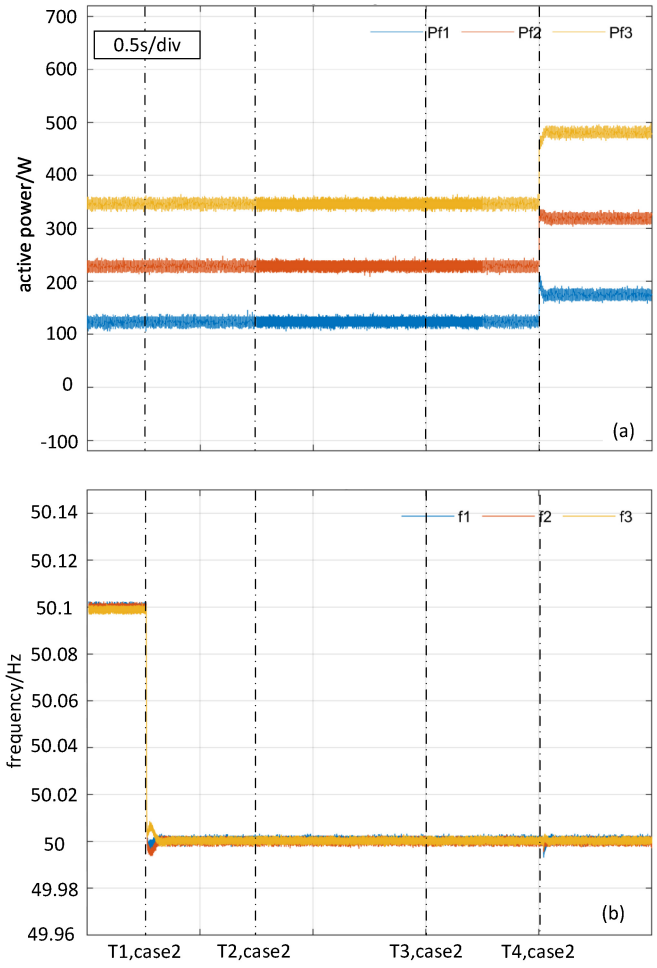

Fig. 12. The performance of the proposed strategy under single DoS: a) Active power sharing; b) Frequency.

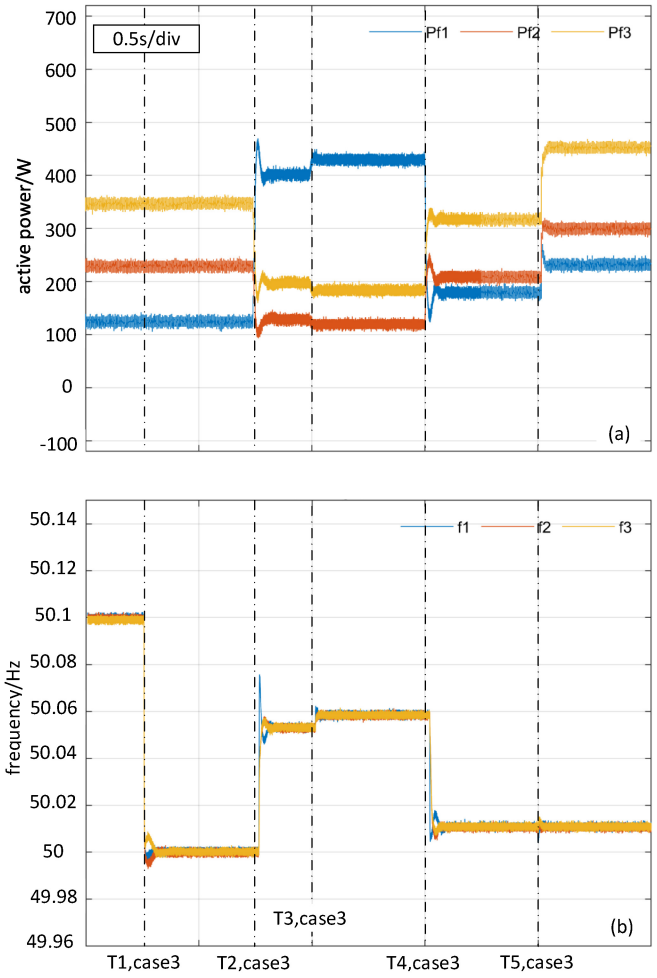

Fig. 13. The performance of the proposed strategy under a combination of FDIAs: a) Active power sharing; b) Frequency.

among participating inverters. At *T2,case3*, Another FDIA $\varepsilon_{3,1}(t) = 0.1$ on communication line 3-1 is imposed, which will further deteriorate frequency convergence performance to 50.06Hz from 50.05Hz and active power sharing ratio to 3.8:1:1.7 from the ratio of 3.3:1:1.6. At *T4,case3*, the proposed adaptive strategy is activated. The microgrid performance will be restored to a satisfactory state as the proposed resilient controller would almost block the more serious infected signal.

Case4: A Combination of FDIA and DoS Corruption.

In Fig. 9, a combination attack consisting of a DoS attack and FDIA infests all communication lines. The details of the offensive and defensive performance is analyzed as follows.

At *T2,case4*, the DoS attack on communication line 3-1 and FDIA on communication line 2-1 are imposed at the same time. As the neighbours' information turns damaged, the performers of active power and frequency will suffer a severe oscillation. The impact of the additional FDIA is significantly less than that caused by DoS. Therefore its reflection in Fig. 9 is insignificant. At *T3,case4*, the DoS attack would be disregarded as defensive measures take effect. In this case, the microgrid system would keep a relatively normal state where the frequency is 50.01Hz and the active power sharing ratio can be recovered to 1:1.3:1.9. At *T4,case4*, we add 240W load into the inverters system. It is illustrated that the adopted adaptive strategy will not affect the regular load switch operation for all communication line-attacked scenarios.

In summary, the single attack or combination of attacks on communication links would disrupt the participating inverters' proportional active power sharing and frequency restoration. By using the proposed control strategy, the corrupted links are damped. As a result, a microgrid's optimal control objectives will be satisfied under various scenarios, including load switching, hackers invading by a single attack or a combination of attacks.

VI. Experiment Results

Experiments are conducted on a microgrid with three inverters connected to the AC bus via an LC filter and line impedance as shown in Fig. 4.

The experiment platform is shown in Fig. 10. Parameters in the experiment are the same as the simulation in Table II, except that the droop coefficient $m_{P1} = 1/300$, $m_{P2} = 1/600$, and $m_{P3} = 1/900$. The switching frequency is 20kHz.

The experimental time instants (*T1,case1*; *T2,case1*; $\cdots$.) in Fig. 11-Fig. 14 are the same as the simulation, representing

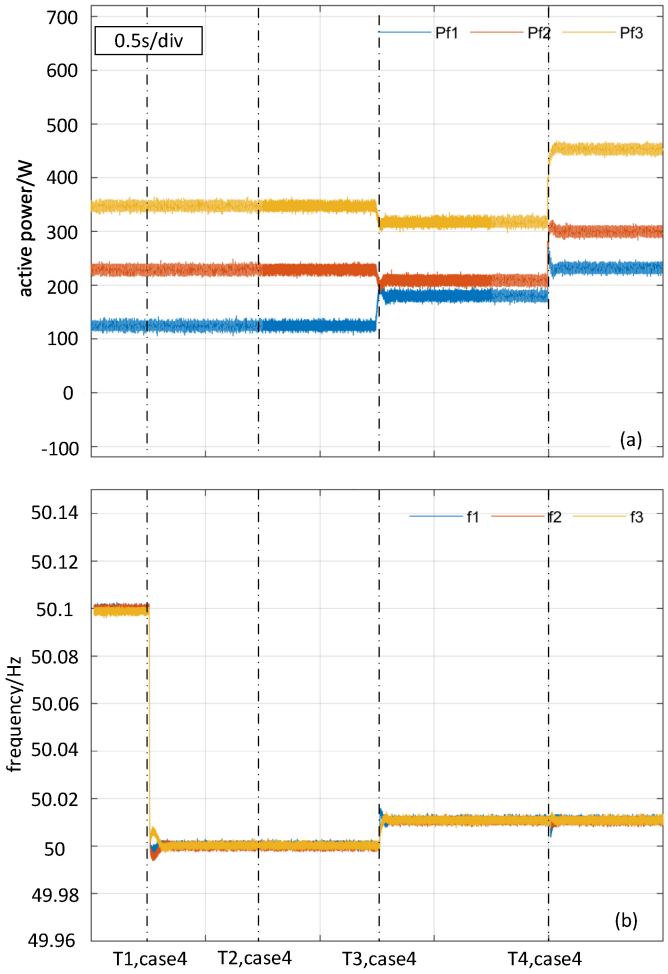

Fig. 14. The performance of the proposed strategy under a combination of FDIA and DoS: a) Active power sharing; b) Frequency.

the trigger times of the different operations of the inverter system.

At the initial stage, the inverters system shares active power proportionally with the preset ratio 1:2:3, at the same time the frequency will converge to 50.1Hz according to the droop law. Then the secondary control strategy is employed to compensate for the frequency offset caused by droop control while maintaining proportionally active power sharing. At last, experiments for the load variation scenario are carried out in the four involved cases.

It should note that the implementation of the DoS attack will lead to a severe power oscillation as shown in simulation results in Fig. 7, which will trigger the over-current protection of the platform. To avoid this problem, We change the order of the experiment procedure, first enabling the defence mechanism and then imposing the DoS attack in Case 2 and Case 4.

For Case 1 and Case 2, FDIA and DoS attack are launched on communication line 2-1 at *T2,case1* and *T2,case2* respectively, as shown in Fig. 11 and Fig. 12. The undesirable state caused by the corrupted signal is eliminated with the proposed method for the infected data is significant attenuation. Thus, it will not propagate in the communication network.

For Case 3 and Case 4, as shown in Fig. 13 and Fig. 14, a combination of cyber attacks occur on communication lines 2-1 and 3-1 at the same time, which is more deteriorating active power and frequency performance. The output frequency is modulated at the relative nominal value by activating the proposed scheme of Case 3 and Case 4 at *T4,case3* and *T3,case4* respectively. At the same time, the active power-sharing ratio will be as close to the preset ratio as it was before, which denotes the effectiveness of the proposed strategy.

VII. Conclusion

This paper presents a control scheme for FDIA and DoS attacks in the secondary-frequency layer of AC microgrids. It assumes there is communication between each two neighbour units. With the proposed control, the signals from the attacked communication channel will be weighted lower. The more the signal deviates from the average, the lower it is weighted. The effect of the corrupted signal will be exponentially attenuated when the signal deviates from the norm. In this way, even if all the communications to a unit are corrupted, the signals from each communication line are optimally weighted depending on how much the signals are falsified. As a result, the proposed control significantly enhances the resilience of AC microgrids under cyber-attack.

References

[1] H. A. Rahman, M. S. Majid, A. R. Jordehi, G. C. Kim, M. Y. Hassan, and S. O. Fadhl, "Operation and control strategies of integrated distributed energy resources: A review," *Renew. Sustain. Energy Rev.*, vol. 51, pp. 1412–1420, Nov. 2015.

[2] A. Bidram, A. Davoudi, and F. L. Lewis, "A multiobjective distributed control framework for islanded AC microgrids," *IEEE Trans. Ind. Informat.*, vol. 10, no. 3, pp. 1785–1798, Aug. 2014.

[3] J. Xiao, L. Wang, Z. Qin, and P. Bauer, "An adaptive cyber security scheme for AC micro-grids," in *Proc. IEEE Energy Convers. Congr. Expo. (ECCE)*, 2022, pp. 1–6.

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

[5] S. Liu, Z. Hu, X. Wang, and L. Wu, "Stochastic stability analysis and control of secondary frequency regulation for islanded microgrids under random denial of service attacks," *IEEE Trans. Ind. Informat.*, vol. 15, no. 7, pp. 4066–4075, Jul. 2019.

[6] M. Shahidehpour, F. Tinney, and Y. Fu, "Impact of security on power systems operation," *Proc. IEEE*, vol. 93, no. 11, pp. 2013–2025, Nov. 2005.

[7] H. S. Sánchez, D. Rotondo, T. Escobet, V. Puig, and J. Quevedo, "Bibliographical review on cyber attacks from a control oriented perspective," *Annu. Rev. Control*, vol. 48, pp. 103–128, Oct. 2019.

[8] A. Cecilia, S. Sahoo, T. Dragičević, R. Costa-Castelló, and F. Blaabjerg, "On addressing the security and stability issues due to false data injection attacks in DC microgrids—An adaptive observer approach," *IEEE Trans. Power Electron.*, vol. 37, no. 3, pp. 2801–2814, Mar. 2022.

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

[10] J. Xiao, L. Wang, Z. Qin, and P. Bauer, "Detection of cyber attack in smart grid: A comparative study," in *Proc. IEEE 20th Int. Power Electron. Motion Control Conf. (PEMC)*, 2022, pp. 48–54.

[11] J. Zhao, L. Mili, and M. Wang, "A generalized false data injection attacks against power system nonlinear state estimator and countermeasures," *IEEE Trans. Power Syst.*, vol. 33, no. 5, pp. 4868–4877, Sep. 2018.

[12] Y. Jiang, Y. Yang, S.-C. Tan, and S. Y. Hui, "Distributed sliding mode observer-based secondary control for DC microgrids under cyber-attacks," *IEEE J. Emerg. Sel. Topics Circuits Syst.*, vol. 11, no. 1, pp. 144–154, Mar. 2021.

[13] M. H. Ranjbar, M. Kheradmandi, and A. Pirayesh, "Assigning operating reserves in power systems under imminent intelligent attack threat," *IEEE Trans. Power Syst.*, vol. 34, no. 4, pp. 2768–2777, Jul. 2019.
[14] Y. Wan and T. Dragičević, "Data-driven cyber-attack detection of intelligent attacks in islanded DC microgrids," *IEEE Trans. Ind. Electron.*, vol. 70, no. 4, pp. 4293–4299, Apr. 2023.
[15] A. S. Musleh, G. Chen, and Z. Y. Dong, "A survey on the detection algorithms for false data injection attacks in smart grids," *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2218–2234, May 2020.
[16] L. Che, X. Liu, Z. Li, and Y. Wen, "False data injection attacks induced sequential outages in power systems," *IEEE Trans. Power Syst.*, vol. 34, no. 2, pp. 1513–1523, Mar. 2019.
[17] Q. Zhou, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, "Flexible division and unification control strategies for resilience enhancement in networked microgrids," *IEEE Trans. Power Syst.*, vol. 35, no. 1, pp. 474–486, Jan. 2020.
[18] J. Liu, X. Lu, and J. Wang, "Resilience analysis of DC microgrids under denial of service threats," *IEEE Trans. Power Syst.*, vol. 34, no. 4, pp. 3199–3208, Jul. 2019.
[19] J. Liu, Y. Du, S.-I. Yim, X. Lu, B. Chen, and F. Qiu, "Steady-state analysis of microgrid distributed control under denial of service attacks," *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 9, no. 5, pp. 5311–5325, Oct. 2021.
[20] S. Sahoo, T. Dragičević, Y. Yang, and F. Blaabjerg, "Adaptive resilient operation of cooperative grid-forming converters under cyber attacks," in *Proc. IEEE CyberPELS (CyberPELS)*, 2020, pp. 1–5.
[21] W. Yao, Y. Wang, Y. Xu, and C. Deng, "Cyber-resilient control of an islanded microgrid under latency attacks and random DoS attacks," *IEEE Trans. Ind. Informat.*, vol. 19, no. 4, pp. 5858–5869, Apr. 2023.
[22] Q. Zhou, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, "A cyber-attack resilient distributed control strategy in islanded microgrids," *IEEE Trans. Smart Grid*, vol. 11, no. 5, pp. 3690–3701, Sep. 2020.
[23] S. Sahoo, T. Dragičević, and F. Blaabjerg, "An event-driven resilient control strategy for DC microgrids," *IEEE Trans. Power Electron.*, vol. 35, no. 12, pp. 13714–13724, Dec. 2020.
[24] S. Abhinav, H. Modares, F. L. Lewis, F. Ferrese, and A. Davoudi, "Synchrony in networked microgrids under attacks," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 6731–6741, Nov. 2018.
[25] S. Sahoo, Y. Yang, and F. Blaabjerg, "Resilient synchronization strategy for AC microgrids under cyber attacks," *IEEE Trans. Power Electron.*, vol. 36, no. 1, pp. 73–77, Jan. 2021.
[26] J. W. Simpson-Porco, Q. Shafiee, F. Dörfler, J. C. Vasquez, J. M. Guerrero, and F. Bullo, "Secondary frequency and voltage control of islanded microgrids via distributed averaging," *IEEE Trans. Ind. Electron.*, vol. 62, no. 11, pp. 7025–7038, Nov. 2015.
[27] C. Deng, Y. Wang, C. Wen, Y. Xu, and P. Lin, "Distributed resilient control for energy storage systems in cyber–physical microgrids," *IEEE Trans. Ind. Informat.*, vol. 17, no. 2, pp. 1331–1341, Feb. 2021.

Junjie Xiao (Graduate Student Member, IEEE) received the B.Sc. degree in electrical engineering from Sichuan Agricultural University, Yaan, China, in 2018, and the M.Sc. degree from Xi'an Jiaotong University, Xian, China, in 2021. He is currently pursuing the Ph.D. degree in electrical engineering with the Delft University of Technology, Delft, The Netherlands.

His research interests include cyber security of microgrids and coordinated control of grid-tied inverters.

Lu Wang (Graduate Student Member, IEEE) received the B.Sc. degree in electrical engineering from the Beijing Institute of Technology, Beijing, China, in 2015, and the M.Sc. degree (cum laude) in electrical sustainable engineering from the Delft University of Technology, Delft, The Netherlands, in 2018. He is currently pursuing the Ph.D. degree with the DC Systems, Energy Conversion and Storage Group.

His research interests include power quality and stability issues induced by EV charging.

Zian Qin (Senior Member, IEEE) received the B.Eng. degree in electrical engineering from Beihang University, Beijing, China, in 2009, the M.Eng. degree in electrical engineering from the Beijing Institute of Technology, Beijing, in 2012, and the Ph.D. degree in electrical engineering from Aalborg University, Aalborg, Denmark, in 2015.

In 2014, he was a Visiting Scientist with Aachen University, Aachen, Germany. He is an Assistant Professor with the Delft University of Technology, Delft, The Netherlands. He has published more than 100 journals/conference papers, four book chapters, two international patents, and also worked on several European and Dutch national projects in these areas. His research interests include power quality and stability of power electronics-based grid, and solid state transformers. He is an Associate Editor of IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, and the Guest Associate Editor of IEEE JOURNAL OF EMERGING AND SELECTED TOPICS and IEEE TRANSACTIONS ON ENERGY CONVERSION. He is a Distinguished Reviewer for 2020 of IEEE TRANSACTIONS OF INDUSTRIAL ELECTRONICS. He served as the Technical Program Chair of IEEE-PEDG 2023, IEEE-ISIE 2020, and IEEE-COMPEL 2020.

Pavol Bauer (Senior Member, IEEE) received the master's degree in electrical engineering from the Technical University of Kosice, Kosice, Slovakia, in 1985, and the Ph.D. degree in power electronics from the Delft University of Technology, Delft, The Netherlands, in 1995.

From 2002 to 2003, he was with KEMA (DNV GL), Arnhem, The Netherlands. He is currently a Full Professor with the Department of Electrical Sustainable Energy, Delft University of Technology, and the Head of DC Systems, Energy Conversion, and Storage Group. He is also a Professor with the Brno University of Technology, Brno, Czech Republic, and an Honorary Professor with the Politehnica University Timisoara, Timisoara, Romania. He has authored or coauthored 8 books and more than 120 journal articles and 500 conference papers. He holds seven international patents and organized several tutorials at international conferences. He has worked on many projects for the industry concerning wind and wave energy, power electronic applications for power systems, such as Smarttrafo; HVdc systems, projects for smart cities, such as photovoltaic (PV) charging of electric vehicles, PV and storage integration, contactless charging; and he participated in several Leonardo da Vinci and H2020, and Electric Mobility Europe EU projects as a Project Partner (ELINA, INETELE, E-Pragmatic, Micact, Trolley 2.0, OSCD, P2P, and Progressus) and a Coordinator (PEMCWebLab.com-Edipe, SustEner, Eranet DCMICRO).

Dr. Bauer is the Former Chairman of Benelux IEEE Joint Industry Applications Society, Power Electronics, and Power Engineering Society Chapter, the Chairman of the Power Electronics and Motion Control Council, a member of the Executive Committee of European Power Electronics Association and the International Steering Committee at numerous conferences.