






Distributed Resilient Control for Energy Storage Systems in Cyber–Physical Microgrids

Chao Deng , Yu Wang , *Member, IEEE*, Changyun Wen , *Fellow, IEEE*, Yan Xu , *Senior Member, IEEE*, and Pengfeng Lin , *Student Member, IEEE*

Abstract—As a cyber–physical system (CPS), the security of microgrids (MGs) is threatened by unknown faults and cyberattacks. Most existing distributed control methods for MGs are proposed based on the assumption that secondary controllers of distributed generation units operate in normal conditions. However, the faults and attacks of the distributed control system could lead to a significant impact and consequently influence the security and stability of MGs. In this article, a distributed resilient control strategy for multiple energy storage systems (ESSs) in islanded MGs is proposed to deal with these hidden but lethal issues. By introducing an adaptive technique, a distributed resilient control method is proposed for frequency/voltage restoration, fair real power sharing, and state-of-charge balancing in MGs with multiple ESSs in abnormal condition. The stability of the proposed method is rigorously proved by Lyapunov methods. The proposed method is validated on test systems developed in OPAL-RT simulator under various cases.

Index Terms—Cyber–physical systems (CPS), distributed resilient control, energy storage systems (ESSs), islanded microgrids (MGs).

I. INTRODUCTION

MICROGRIDS (MGs) are developing toward cyber–physical systems (CPSs), which consist of electric-coupled physical systems and communication-coupled cyber systems [1]–[3]. The evolution of MGs happens on both physical and cyber sides. In the physical layer, energy storage systems (ESSs) are widely integrated to mitigate the power fluctuations of renewable energy sources (RESs) and provide grid ancillary services [4]–[6]. In the cyber layer, to enhance the flexibility and reliability of MG systems, the networked and distributed control theory has been widely applied, with realization on multiagent systems and peer-to-peer communications [7], [8].

Manuscript received March 12, 2020; accepted March 14, 2020. Date of publication March 17, 2020; date of current version November 18, 2020. This work was supported by the Ministry of Education of Singapore Grant MOE2017-T2-1-050 and in part by the Joint Funds of the National Natural Science Foundation of China under Grant U1966202. Paper no. TII-20-0599. (Corresponding author: Yu Wang.)

The authors are with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, 639798 (e-mail: cdeng@ntu.edu.sg; wang_yu@ntu.edu.sg; ecywen@ntu.edu.sg; xuyan@ntu.edu.sg; linp0010@e.ntu.edu.sg).

Color versions of one or more of the figures in this article are available online at <http://ieeexplore.ieee.org>.

Digital Object Identifier 10.1109/TII.2020.2981549

For droop-controlled distributed generators in MGs, hierarchical control has become a standard framework [9]. The distributed secondary control aims at eliminating frequency and voltage deviations caused by droop control while maintaining accurate power sharing among distributed generators (DGs) [10]–[12]. In MGs with multiple ESSs, state-of-charge (SoC) balancing is usually taken into account in the original secondary control framework [13]–[15]. Distributed SoC balancing of multiple ESSs has been proposed by using linear consensus algorithms [4], and nonlinear methods to improve the performance [14], [16]. However, as a CPS, an MG with multiple ESSs can suffer from both faults and attacks of each layer, which is a potential and lethal problem to be studied.

Security issues are recognized as a vital problem for CPSs, where a typical example is modern electric power systems [17], [18]. The faults and attacks in both physical and cyber layers could dramatically influence the stable and secure operation of a single MG or even the entire power system. The abnormal conditions and power failures can be caused by various reasons such as equipment failures, manual misbehavior, cyber–physical attacks, etc. Typical examples include Ukraine power grid cyber attacks in 2015 [19] and manual misbehavior for Taiwan blackout in 2017 [20]. Great economic loss and social impacts will be induced by the intentional or unintentional security issues of power systems.

Regarding the security of CPSs, there are three important aspects to be protected: confidentiality, integrity, and availability [21]. Correspondingly, attack models of CPSs can be characterized into three categories, denoted as *DDD attacks*: disclosure attacks, deception attacks, and disruption attacks [22], [23]. Disclosure attacks could lead to unauthorized information release. Deception attacks aims to corrupt the real data, such as false-data injection (FDI) attacks. Disruption attacks will cause denial of use of the information, known as denial-of-service (DoS) attack [24]. To ensure the security of CPSs under various cyber attacks, suitable defense mechanisms must be designed to enhance the performance of CPSs under attacks. In existing works, the defense mechanisms can be characterized as three categories [22], [23]: 1) *prevention*: to postpone the onset of an attack, 2) *resilience*: to tolerate the maximum impact of the attack and operate as closely to the normal state as possible, and 3) *attack detection and isolation*: to identify the source of the attack, isolate the corrupted subsystems, and restore the normal mode as quickly as possible. In this article, we focus on the second term, i.e., *resilience enhancement*, where distributed

resilience control strategies for MGs with multiple ESSs are investigated.

In an MG system, faults and attacks can happen in various locations of the secondary control system. Particularly, the control and communication devices, which have network access are vulnerable to cyber-attacks [25], [26]. For example, if the secondary control is implemented on host computers or embedded systems, both the control signals and measured system states could be manipulated on the devices and during the data transmission process [3], [27]. From the perspective of CPS security in MG systems, many existing works focus on the *attack detection and isolation* techniques. In [26], a prototype tool called Hynger is developed to obtain the candidate invariants, which are to be compared with actual invariants to identify FDI attacks. In [28], distributed secondary control of islanded MGs is achieved by primal-dual algorithm, and model-based anomaly detection and localization strategies are proposed. Sahoo *et al.* [29] investigated the stealthy cyber-attack detection strategy for dc MGs. On the other hand, to enhance the resilient of the MG system, cyber-resilient control scheme is proposed by recent research in [30] and [31]. In [30], an observer-based control with confidence and trust factors is proposed to achieve frequency/voltage restoration under cyber attacks. In [31], based on weighted mean subsequence reduced algorithm, a cyber-secure control scheme is proposed for islanded MGs. The corrupted information from neighbors is discarded by managing the connectivity of communication graphs. In addition, a quantity of research has been conducted to investigated communication issues and mitigation methods for MG systems, such as communication noise [32], delays [33], and packet loss [34]. From the literature, there are two noticeable research gaps. 1) CPS security issues of MGs with multiple ESSs have not been paid much attention. As the key elements in future power systems, the security and stability of ESSs are worth of investigation. 2) Distributed resilient control schemes under faults and attacks for the secondary control process are important for resilience enhancement. However, very limited results on resilient oriented control of MGs are available.

Therefore, the aim of this article is to study and compensate the effects of bias and manipulation in secondary control signals caused by attacks/faults. Different from [30], [31], the controller design is inspired from adaptive resilient control of multiagent systems [35], [36]. The main approaches and contributions of this article are summarized as follows:

- 1) This article is the first to consider the resilient control for multiple ESSs in islanded MGs under faults and attacks of secondary controllers. The problem is formulated as distributed control of a multiagent system under faults/attacks.
- 2) A novel distributed resilient control method is provided to solve the considered problem. The effectiveness of the proposed approach is validated by applying the distributed resilient controller on test systems developed in OPAL-RT simulator under various cases.
- 3) By introducing an adaptive gain, which can be viewed as the adaptive version of the σ -modification method in [35] and [36], a *distributed resilient controller avoiding the strictly increasing behavior of controller gain is proposed* to compensate for the influence of faults/attacks.

This article is organized as follows. In Section II, the preliminaries including modeling and problem formulation are introduced. Next, the proposed distributed resilient control for ESSs is presented in Section III. The case studies and OPAL-RT test results are presented in Section IV. Finally, Section VI concludes this article.

Notation: I is the identity matrix with appropriate dimension. $A \otimes B$ means the Kronecker product of A and B . $\mathbf{1} = \text{col}\{1, \dots, 1\} \in \mathbb{R}^N$. $A = \text{diag}\{A_1, A_2, \dots, A_N\}$ denotes a diagonal matrix with matrix A_1, \dots, A_N on its diagonal elements.

II. PROBLEM STATEMENT AND PRELIMINARIES

A. Graph Theory

Consider that the control agent of each ESS can exchange information through a communication network. The communication topology is described as an undirected graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where $\mathcal{V} = \{\mathcal{V}_1, \mathcal{V}_2, \dots, \mathcal{V}_N\}$ is a set of nodes and $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ is a set of edges. A node j is called a neighbor of node i if there is an edge defined as $(\mathcal{V}_i, \mathcal{V}_j) \in \mathcal{E}$. All the neighbors of node i is defined as $\mathcal{N}_i = \{j | (\mathcal{V}_i, \mathcal{V}_j) \in \mathcal{E}\}$. An adjacency matrix is defined as $A = [a_{ij}]$, where $a_{ii} = 0$ ($\forall i = 1, \dots, N$), $a_{ij} = 1$ if $(\mathcal{V}_i, \mathcal{V}_j) \in \mathcal{E}$, and $a_{ij} = 0$ otherwise. $\mathcal{D} = \text{diag}\{d_1, d_2, \dots, d_N\}$ is defined as a degree matrix of graph \mathcal{G} , where $d_i = \sum_{j=1}^N a_{ij}$. The Laplacian matrix \mathcal{L} of graph \mathcal{G} is defined as $\mathcal{L} = \mathcal{D} - A$. A path is a sequence of connected edges in a graph. The graph \mathcal{G} is connected if there exists a path between any nodes. In this article, it assumes that only a part of DGs can achieve the reference values of frequency and voltage. Let $\mathcal{B} = \text{diag}\{b_1, \dots, b_N\}$, where $b_i = 0$ means that DG i cannot receive the reference values and $b_i = 1$ otherwise. Define $\mathcal{H} = \mathcal{L} + \mathcal{B}$ [37].

B. MGs and Droop Control

The droop control of power inverters emulates the behavior of synchronous generators in large power systems. It is used to regulate the system frequency ω_i and voltage amplitude V_i with only local measurement of real power P_i and reactive power Q_i , respectively. The typical droop control equations are represented as follows [9], [10]:

$$\omega_i = \omega_i^{\text{nom}} - K_i^P P_i \quad (1)$$

$$V_i = V_i^{\text{nom}} - K_i^Q Q_i \quad (2)$$

where ω_i^{nom} and V_i^{nom} are the nominal set-points of frequency and voltage amplitude, respectively. K_i^P and K_i^Q are droop coefficients, which are selected based on $K_i^P = \Delta\omega/P_i^{\text{max}}$ and $K_i^Q = \Delta V/Q_i^{\text{max}}$. It is noted that ω_i here is actually the angular frequency in rad/s, which can be converted into hertz by $f_i = \omega_i/2\pi$. V_i is voltage magnitude of the i th unit.

Remark 1: In this article, the framework and notions from hierarchical control of MG systems are followed [9]–[12]. In the primary/local control level, there are several control loops. The voltage and current control loops have a faster response speed than that of droop control as well as higher level control. Thus, the dynamics of these two control loops can be neglected when analyzing the higher level control performance [12]. Typically,

primary controllers implemented on digital signal processors are operated locally and thus are not vulnerable to cyber attacks [38].

C. Energy Storage Systems

By measuring the power output and considering the charging and discharging efficiency of the i th ESS, the SoC or energy level can be estimated by [13]–[15]:

$$\text{SoC}_i = \text{SoC}_{i,t=0} - \int_0^T \frac{\tilde{\eta}_i P_i}{3600 C_i^E} dt \quad (3)$$

where C_i^E and $\text{SoC}_{i,t=0}$ are the capacity (kWh) and initial SoC of the i th ESS. C_i^E is multiplied by 3600 to convert its unit from kilowatt-hour to kilowatt. The charging and discharging efficiency of each ESS can be represented by

$$\tilde{\eta}_i = \begin{cases} \eta_i^{\text{ch}}, & P_i < 0 \\ 1/\eta_i^{\text{dis}}, & P_i > 0 \end{cases} \quad (4)$$

For simplicity, symbol E_i is used to represent SoC_i . Combining (3) and (4), and differentiating at both side, the relationship between P_i and E_i can be expressed as follows:

$$\dot{E}_i = -\frac{\tilde{\eta}_i P_i}{3600 C_i^E} = K_i^E P_i \quad (5)$$

where $K_i^E = -\tilde{\eta}_i/3600 C_i^E$ is a coefficient between P_i and E_i . Without loss of generality, in this article, it is considered that the maximum power output of each ESS is proportional to its capacity, i.e., $C_i^E/C_j^E = P_i^{\text{max}}/P_j^{\text{max}}$. Additionally, we define an auxiliary control variable as $\Phi_i(t) = K_i^E P_i(t)$. Taking the derivative of it, i.e., $\dot{\Phi}_i(t) = K_i^E \dot{P}_i(t)$, a double integral model of i th ESS can be formulated as follows:

$$\begin{cases} \dot{E}_i(t) = \Phi_i(t) \\ \dot{\Phi}_i(t) = u_i^E(t) \end{cases} \quad (6)$$

where $u_i^E(t)$ is the control input to be designed for achieving SoC balancing and proportional power sharing. A group of ESSs coupled with communication networks can be viewed as a multiagent system. Define $x_i(t) = [E_i(t), \Phi_i(t)]^T$ and $u_i(t) = u_i^E(t)$. Based on (6), and considering the disturbance term of the input, we have

$$\dot{x}_i(t) = A x_i(t) + B(u_i(t) + d_i(t)), \quad i = 1, 2, \dots, N \quad (7)$$

where $A = [0 \ 1; 0 \ 0]$, $B = [0 \ 1]^T$. $d_i(t)$ is a time-varying and bounded external disturbance, i.e., there exists an unknown constant \bar{d}_i such that $|d_i(t)| \leq \bar{d}_i$.

D. Formulation of Secondary Control

The droop-based primary control can cause frequency and voltage deviation for load sharing in islanded MGs. Thus, the basic objective of secondary control is to restore the frequency and voltage magnitude back to their reference values. To perform secondary control, differentiating (1) and (2) yields

$$\dot{\omega}_i(t) = \dot{\omega}_i^{\text{nom}} - K_i^P \dot{P}_i(t) \quad (8)$$

$$\dot{V}_i(t) = \dot{V}_i^{\text{nom}} - K_i^Q \dot{Q}_i(t). \quad (9)$$

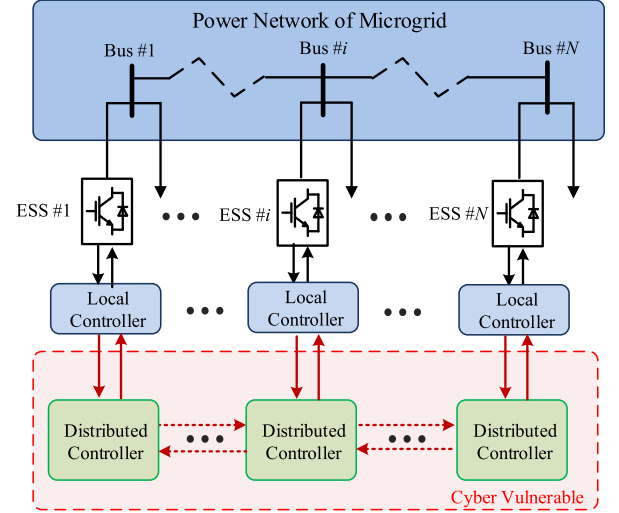


Fig. 1. Distributed control framework of a MG system with multiple ESSs.

As discussed in [1] and [39], the frequency and voltage of each ESS can be controlled in the secondary level by $\dot{\omega}_i(t) = u_i^\omega(t)$, $\dot{V}_i(t) = u_i^V(t)$. It is noted that voltage control is considered in this article, since there is a tradeoff relationship between voltage restoration and reactive power sharing [11], [12]. The functionality of SoC balancing is also included in the secondary control hierarchy as an additional control objective. It should be noted that the dynamics involved in frequency and voltage restoration is much faster than that of SoC balancing process [16]. Thus, the control problem can be further decoupled to consider two different time scales of dynamics, which can be solved by designing respective controllers. In the secondary level for SoC balancing, the real power output of each ESS can be controlled by $K_i^E \dot{P}_i(t) = u_i^E(t)$. The nominal set-points ω_i^{nom} and V_i^{nom} are adjusted by the secondary control as follows [39]:

$$\omega_i^{\text{nom}} = \int (u_i^\omega + K_i^P \dot{P}_i) = \int (u_i^\omega + K_i^P / K_i^E u_i^E) \quad (10)$$

$$V_i^{\text{nom}} = \int (u_i^V + K_i^Q \dot{Q}_i) \quad (11)$$

where $u_i^\omega(t)$, $u_i^E(t)$, and $u_i^V(t)$ are control inputs to be designed. To see where such attacks/faults possibly appear in the control loops, a block diagram of the distributed resilient secondary control that is to be designed is given in Fig. 2. It is noted that the secondary controllers are usually implemented on embedded systems with communication networks access. Therefore, the secondary controllers as well as their data transmission process are more vulnerable to cyber threats [29], [30].

E. Faults and Attacks of Secondary Controllers

The considered faults or attacks contain the changes in the gain and bounded disturbance injection to secondary control outputs. A sophisticated form of faults or attacks on the secondary controller can be modeled [17], [30] by

$$u_i^F(t) = \varphi_i(t) u_i(t) + \delta_i(t) \quad (12)$$

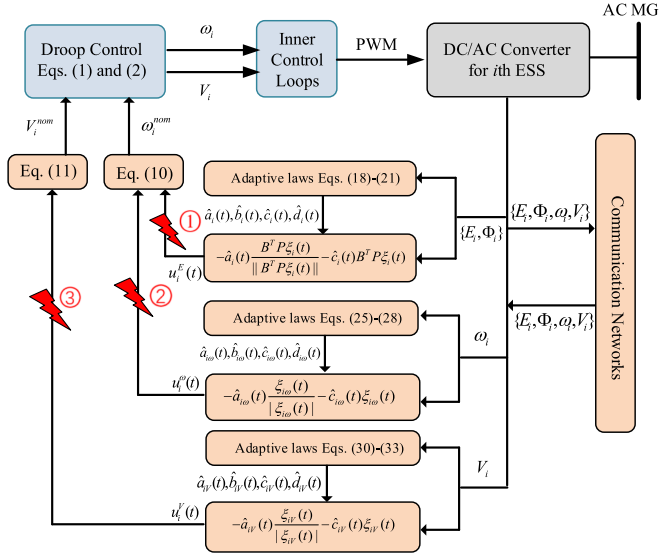


Fig. 2. Block diagram of the distributed resilient secondary control.

where $u_i(t)$ (i.e., $u_i^\omega(t)$, $u_i^E(t)$, $u_i^V(t)$) represent the original signal, and $u_i^F(t)$ is the secondary control output under the unknown faults or attacks. $\varphi_i(t)$ represents a nonzero bounded changes in the gain coefficient and $\delta_i(t)$ is a bounded disturbance injected into the secondary control by faults and attacks, respectively. $\varphi_i(t) = 1$ and $\delta_i(t) = 0$ represent absence of faults and attacks of the secondary control, while $\varphi_i(t) = 1$ and $\delta_i(t) \neq 0$ represent the disturbance injected into the secondary control by faults and attacks. $\varphi_i(t) \neq 1$ and $\delta_i(t) = 0$ represent the changes in the gain under faults and attacks ($\varphi_i(t)$ is bounded and satisfies $\varphi_i(t) \leq \bar{\varphi}_i$). $\varphi_i(t) \neq 1$ and $\delta_i(t) \neq 0$ represent the changes in the gain and disturbance injected into the secondary control by faults and attacks at the same time. It is noted that the influence of (12) is to change secondary control signal $u_i^E(t)$, $u_i^\omega(t)$, and $u_i^V(t)$ in locations ①, ②, and ③ of Fig. 2, respectively. The faults/attacks in locations ① and ② have the same effect, as the changes of $u_i^E(t)$ and $u_i^\omega(t)$ will finally influence the integration term in (10). The signal changes in locations ③ will make negative impact on (11). For brevity, the attacks/faults happened in SoC control loops are demonstrated in Section IV.

Remark 2: For the i th agent, the changes in the gain coefficient and disturbance injected signal are time-varying and bounded, i.e., there exist unknown constants $\underline{\varphi}_i$, $\bar{\varphi}_i$, and $\bar{\delta}_i$ such that $0 < \underline{\varphi}_i \leq \varphi_i(t) \leq \bar{\varphi}_i$ and $|\delta_i(t)| \leq \bar{\delta}_i$.

Remark 3: In this article, we use the unified model (12) to unify the effects of faults and attacks possibly occurring in secondary controllers. However, the faults and attacks have the following differences: First, the faults may happen randomly to alter the control signal of secondary controllers, while attacks contain the case that the attackers have the access of the embedded system or data transmission networks to manipulate the control signal u_i . Second, faults are considered as events that affect the behavior of the secondary controllers, where simultaneous events are assumed to be noncolluding, i.e., the events do not act in a coordinated way. Attacks may be performed over a

significant number of attack points in a coordinated fashion [40], which is usually have an intent or objective to fulfill. Third, from a system theoretical point of view, faults only involves data loss-of-effectiveness (which implies that $\varphi_i(t) \in (0, 1)$) and bias in (12), while for attacks there are changes in the gain (i.e., $\varphi_i(t) \in (0, \bar{\varphi}_i)$ with $\bar{\varphi}_i > 1$) and bias of secondary controllers. Thus, faults and attacks have inherently distinct characteristics. In this article, they are considered simultaneously on the secondary controllers with the unified model (12).

F. Distributed Resilient Control Objective

The objective is to develop distributed resilient controllers for each ESS with faults/attacks on secondary controllers such that

- 1) SoC balancing and proportional power sharing problems are solved, i.e.,

$$\lim_{t \rightarrow \infty} (E_i(t) - E_j(t)) = 0 \quad (13)$$

$$\lim_{t \rightarrow \infty} (\Phi_i(t) - \Phi_j(t)) = 0. \quad (14)$$

- 2) Frequency and voltage restoration problems are solved, i.e.,

$$\lim_{t \rightarrow \infty} (\omega_i(t) - \omega^{\text{ref}}) = 0 \quad (15)$$

$$\lim_{t \rightarrow \infty} (V_i(t) - V^{\text{ref}}) = 0. \quad (16)$$

where ω_i^{ref} and V_i^{ref} are the reference values of frequency and voltage amplitude, respectively.

III. DESIGN OF DISTRIBUTED RESILIENT CONTROLLERS

As shown in Fig. 2, three control loops are designed for SoC balancing control ($u_i^E(t)$), frequency restoration ($u_i^\omega(t)$), and voltage restoration ($u_i^V(t)$). We now design each of these controllers in the following sections.

A. Distributed Resilient Control for SoC Balancing and Proportional Power Sharing

For SoC balancing and proportional power sharing problem, the following distributed resilient controller is designed:

$$u_i^E(t) = -\hat{a}_i(t) \frac{B^T P \xi_i(t)}{\|B^T P \xi_i(t)\|} - \hat{c}_i(t) B^T P \xi_i(t) \quad (17)$$

where $\xi_i(t) = \sum_{j=1}^N a_{ij}(x_i(t) - x_j(t))$. $\hat{a}_i(t)$ and $\hat{c}_i(t)$ are time-varying gains, which are updated by

$$\dot{\hat{a}}_i(t) = \gamma_{i1} \|\xi_i^T(t) P B\| - \gamma_{i2} (\hat{a}_i(t) - \hat{b}_i(t)) \quad (18)$$

$$\dot{\hat{c}}_i(t) = \gamma_{i3} \|\xi_i^T(t) P B\|^2 - \gamma_{i4} (\hat{c}_i(t) - \hat{d}_i(t)) \quad (19)$$

where γ_{i1} , γ_{i2} , γ_{i3} , and γ_{i4} are positive constants. $\hat{b}_i(t)$ and $\hat{d}_i(t)$ are adaptive parameters and the dynamics are given by

$$\dot{\hat{b}}_i(t) = \gamma_{i5} (\hat{a}_i(t) - \hat{b}_i(t)) \quad (20)$$

$$\dot{\hat{d}}_i(t) = \gamma_{i6} (\hat{c}_i(t) - \hat{d}_i(t)) \quad (21)$$

where γ_{i5} and γ_{i6} are positive constants. Besides, $\hat{a}_i(0) > \hat{b}_i(0) > 0$ and $\hat{c}_i(0) > \hat{d}_i(0) > 0$. P is given by the following

algebraic Riccati equation:

$$PA + A^T P - 2PBB^T P = -Q \quad (22)$$

where Q is an arbitrary positive definite matrix.

Remark 4: The controller $u_i^E(t)$ in (17) consists of two parts. The first term is used to compensate for the influence of external disturbance $d_i(t)$ and the bias $\delta_i(t)$ injected by faults and attacks. The second term is used to achieve consensus among all ESSs.

Let $x(t) = \text{col}\{x_1(t), \dots, x_N(t)\}$. Define $\bar{x}(t) = (\mathcal{N} \otimes I)x(t)$ with $\mathcal{N} = I - \frac{1}{N}\mathbf{1}\mathbf{1}^T$. According to $\mathcal{L}\mathcal{N} = \mathcal{N}\mathcal{L} = \mathcal{L}$, we have

$$\dot{\bar{x}}(t) = (I \otimes A)\bar{x}(t) + (\mathcal{N} \otimes B) (\varphi(t)u^E(t) + \delta(t) + d(t)) \quad (23)$$

where $u^E(t) = \text{col}\{u_1^E(t), \dots, u_N^E(t)\}$, $\varphi(t) = \text{diag}\{\varphi_1(t), \dots, \varphi_N(t)\}$, $\delta(t) = \text{col}\{\delta_1(t), \dots, \delta_N(t)\}$, and $d(t) = \text{col}\{d_1(t), \dots, d_N(t)\}$.

As discussed in [37], if the communication graph \mathcal{G} is connected, then $\mathcal{L}\mathbf{1} = 0$. Hence, $\bar{x}(t) = 0$ is equivalent to $x_1(t) = \dots = x_N(t)$. Thus, the SoC balancing and proportional power sharing problem is equivalent to design the controller (17) with adaptive laws (18) and (20), such that the system (23) is asymptotic stability.

Theorem 1: Assume that the communication graph \mathcal{G} is connected. The SoC balancing and proportional power sharing problems (13) and (14) under unknown faults and cyber attacks in (12) can be solved by the distributed resilient controller (17) and with adaptive laws (18)–(21).

Proof: Please see the Appendix. ■

B. Distributed Resilient Control for Frequency and Voltage Restoration

For frequency restoration problem, the following distributed resilient controller is designed:

$$u_i^\omega(t) = -\hat{a}_{i\omega}(t) \frac{\xi_{i\omega}(t)}{\|\xi_{i\omega}(t)\|} - \hat{c}_{i\omega}(t)\xi_{i\omega}(t) \quad (24)$$

where $\xi_{i\omega}(t) = \sum_{j=1}^N a_{ij}(\omega_i(t) - \omega_j(t)) + b_i(\omega_i(t) - \omega^{ref})$. $\hat{a}_{i\omega}(t)$ and $\hat{c}_{i\omega}(t)$ are time-varying gains, which are updated by

$$\dot{\hat{a}}_{i\omega}(t) = \gamma_{i1}^\omega \|\xi_{i\omega}^T(t)\| - \gamma_{i2}^\omega (\hat{a}_{i\omega}(t) - \hat{b}_{i\omega}(t)) \quad (25)$$

$$\dot{\hat{c}}_{i\omega}(t) = \gamma_{i3}^\omega \|\xi_{i\omega}^T(t)\|^2 - \gamma_{i4}^\omega (\hat{c}_{i\omega}(t) - \hat{d}_{i\omega}(t)) \quad (26)$$

where γ_{i1}^ω , γ_{i2}^ω , γ_{i3}^ω , and γ_{i4}^ω are positive constants. $\hat{b}_{i\omega}(t)$ and $\hat{d}_{i\omega}(t)$ are adaptive parameters and the dynamics are given by

$$\dot{\hat{b}}_{i\omega}(t) = \gamma_{i5}^\omega (\hat{a}_{i\omega}(t) - \hat{b}_{i\omega}(t)) \quad (27)$$

$$\dot{\hat{d}}_{i\omega}(t) = \gamma_{i6}^\omega (\hat{c}_{i\omega}(t) - \hat{d}_{i\omega}(t)) \quad (28)$$

where γ_{i5}^ω and γ_{i6}^ω are positive constants. Besides, $\hat{a}_{i\omega}(0) > \hat{b}_{i\omega}(0) > 0$ and $\hat{c}_{i\omega}(0) > \hat{d}_{i\omega}(0) > 0$.

For voltage restoration problem, the following distributed resilient controller is designed:

$$u_i^V(t) = -\hat{a}_{iV}(t) \frac{\xi_{iV}(t)}{\|\xi_{iV}(t)\|} - \hat{c}_{iV}(t)\xi_{iV}(t) \quad (29)$$

where $\xi_{iV}(t) = \sum_{j=1}^N a_{ij}(V_i(t) - V_j(t)) + b_i(V_i(t) - V^{ref})$. $\hat{a}_{iV}(t)$ and $\hat{c}_{iV}(t)$ are time-varying gains, which are updated by

$$\dot{\hat{a}}_{iV}(t) = \gamma_{i1}^V \|\xi_{iV}^T(t)\| - \gamma_{i2}^V (\hat{a}_{iV}(t) - \hat{b}_{iV}(t)) \quad (30)$$

$$\dot{\hat{c}}_{iV}(t) = \gamma_{i3}^V \|\xi_{iV}^T(t)\|^2 - \gamma_{i4}^V (\hat{c}_{iV}(t) - \hat{d}_{iV}(t)) \quad (31)$$

where γ_{i1}^V , γ_{i2}^V , γ_{i3}^V , and γ_{i4}^V are positive constants. $\hat{b}_{iV}(t)$ and $\hat{d}_{iV}(t)$ are adaptive parameters and the dynamics are given by

$$\dot{\hat{b}}_{iV}(t) = \gamma_{i5}^V (\hat{a}_{iV}(t) - \hat{b}_{iV}(t)) \quad (32)$$

$$\dot{\hat{d}}_{iV}(t) = \gamma_{i6}^V (\hat{c}_{iV}(t) - \hat{d}_{iV}(t)) \quad (33)$$

where γ_{i5}^V and γ_{i6}^V are positive constants. Besides, $\hat{a}_{iV}(0) > \hat{b}_{iV}(0) > 0$ and $\hat{c}_{iV}(0) > \hat{d}_{iV}(0) > 0$.

Theorem 2: Assume that the communication graph \mathcal{G} is connected and there exists at least one node that can achieve the reference values of frequency and voltage. The frequency and voltage restoration problems (15) and (16) under unknown faults and cyber attacks in (12) can be solved by the distributed resilient controller (24) with adaptive laws (25)–(28) and controller (29) with adaptive laws (30)–(33), respectively.

Proof: The results can be obtained by extending Theorem 1. We omit the proof due to the limited space. ■

Remark 5: If the denominators of the distributed resilient controllers (17), (24), and (29) tend to zero, the chattering phenomenon will be presented. Similar to [36], the well-known boundary layer approach can be used to solve this problem.

Remark 6: As discussed in [29] and [30], the stealth attack refers to the attack which cannot be detected or mitigated using existing disturbance attenuation or noise filtering techniques. In this article, stealth attacks in the form of both the constant bias signal in single node [30] and the coordinated node attacks [29] are considered and to be illustrated in case studies.

IV. CASE STUDIES AND RESULTS

In this article, the effectiveness of the proposed control method is validated with real-time test on OPAL-RT. In test systems, average converter model and lithium-ion battery model are applied. The inner control loops of primary control are developed based on [42]. The MG test systems are simulated with the time step of $1e-5$ s. The results data are saved with 200 points per second. In Test Cases 1–3, a 4-ESS MG test system is considered, where the topologies of both electrical and communication networks are demonstrated in Fig. 3. The parameters of the MG test system are given in Table 1. In Test Case 4, the proposed control method is tested on a modified IEEE 33-bus test system with six ESSs.

Inspired by the previous research [25]–[31], the test cases are categorized single node faults/attacks as in Cases 1 and 2, and coordinated node attacks in Cases 3 and 4. The single node faults/attacks events in Test Cases 1 and 2 are shown in Fig. 4. The test events are illustrated in the time sequence as follows:

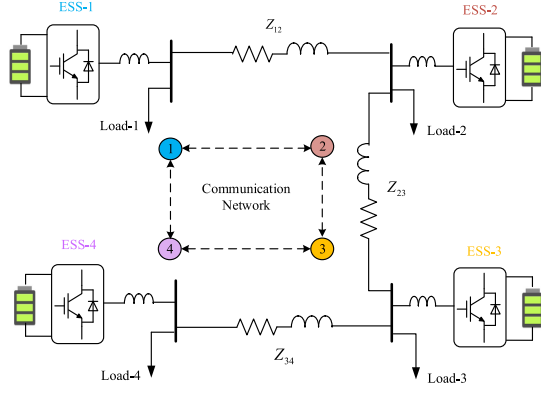


Fig. 3. Electrical and communication topologies of the MG test system.

TABLE I
PARAMETERS OF THE MG TEST SYSTEM

ESS (Bus No.)	1	2	3	4
m_i (rad/W)	2.512e-4	2.512e-4	1.256e-4	1.256e-4
n_i (V/Var)	4e-4	4e-4	2e-4	2e-4
C_i^E (kWh)	1e3	1e3	2e3	2e3
$\eta_i^{ch} = \eta_i^{dis}$	0.98	0.98	0.97	0.97
Load (Bus No.)	1	2	3	4
R (Ω)	300	40	50	50
L (mH)	477	64	64	95
Line (No.)	1-2	2-3	3-4	
R (Ω)	0.8	0.4	0.7	
L (mH)	3.6	1.8	1.9	
Inverters (#1-4)	$C_f = 25\mu F$	$L_f = 1.8mH$	$L_o = 1.8mH$	
Reference	$\omega^* = 100\pi$ (rad)	$V^* = 230\sqrt{2}$ (V)		

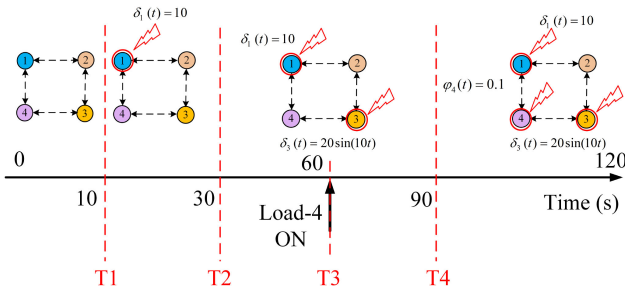


Fig. 4. Faults and attacks in Cases 1 and 2.

- 1) $0 \leq t \leq 10$ s. Initially, the OPAL-RT test starts with all ESSs. Loads 1–3 are connected in the MG. The initial SoCs for ESSs 1–4 are 50%, 49%, 48%, and 47%.
- 2) $10 \leq t \leq 30$ s. The control agent of ESS-1 is subjected to a bias fault or attack, i.e., $\delta_1(t) = 10$ for $t \geq 10$ s.
- 3) $30 \leq t \leq 90$ s. The control agent of ESS-3 is subjected to an attack, i.e., $\delta_3(t) = 20 \sin(10t)$ for $t \geq 30$ s. Additionally, Load-4 is connected into the MG at $T_3 = 60$ s.
- 4) $90 \leq t \leq 120$ s. The control agent of ESS-4 is subjected to a change in the gain of fault or attack of the secondary controller, i.e., $\varphi_4(t) = 0.1$ for $t \geq 90$ s.

In addition, the coordinated node attacks can be deployed in a stealthy way, which is investigated in Test Case 3. In Test Case 4, a coordinated node attack with balanced signal is considered.

A. Test Case 1: Existing Linear Distributed Control Method

In this case, the control performance of MG system with commonly used linear distributed control method for multiple ESSs under single node faults/attacks is evaluated. This test case will serve as the benchmark for comparison with Test Case 2. According to the existing result [15], frequency/voltage restoration and SoC balancing controllers can be summarized as follows:

$$u_i^\omega = k_{i\omega} \left[\sum_{j=1}^N a_{ij}(\omega_j - \omega_i) + g_i(\omega^{\text{ref}} - \omega_i) \right] \quad (34)$$

$$u_i^V = k_{iV} \left[\sum_{j=1}^N a_{ij}(V_j - V_i) + g_i(V^{\text{ref}} - V_i) \right] \quad (35)$$

$$u_i^E = \sum_{j=1}^N a_{ij} [k_{iE}(E_j - E_i) + k_{i\Phi}(\Phi_j - \Phi_i)] \quad (36)$$

where control gains are chosen as $k_{i\omega} = 30$, $k_{iV} = 30$, $k_{iE} = -40$, and $k_{i\Phi} = 1$ in this simulation. The OPAL-RT real-time test results are shown in Fig. 5(a)–(d), which are illustrated in the time sequence as follows:

- 1) $0 \leq t \leq 10$ s: As shown in Fig. 5(a) and (d), the MG frequency and voltage can be restored to reference values with the typical control laws in (34) and (35). The SoC of each ESS also trends to equalizing with the control law in (36).
- 2) $10 \leq t \leq 30$ s: Due to the bias fault or attack of $\delta_1(t) = 10$ at $T_1 = 10$ s, the MG frequency is hijacked to 50.2 Hz under normal control laws and cannot be back to the reference value.
- 3) $30 \leq t \leq 90$ s: Due to the bias fault or attack of $\delta_3(t) = 20 \sin(10t)$ at $T_2 = 30$ s, the system frequency, real power output, and voltage magnitude start to oscillate. There is a load change in $T_3 = 60$ s.
- 4) $90 \leq t \leq 120$ s: The magnitude of oscillations is mitigated due to the changes in the gain of the secondary controller, i.e., $\varphi_4(t) = 0.1$ at $T_4 = 90$ s.

B. Test Case 2: Distributed Resilient Control Method

In this case, the proposed distributed resilient control method is used to compensate for the influence of single node faults/attacks. In this simulation, parameters of the proposed controllers are chosen as $\gamma_{ij} = \gamma_{ij}^\omega = \gamma_{ij}^V = 10$ ($i = 1, 2, 3, 4$ and $j = 1, 2, \dots, 6$). The OPAL-RT real-time test results of frequency, real power, SoC and voltage magnitude are shown in Fig. 6(a)–(d), which are illustrated in the time sequence as follows:

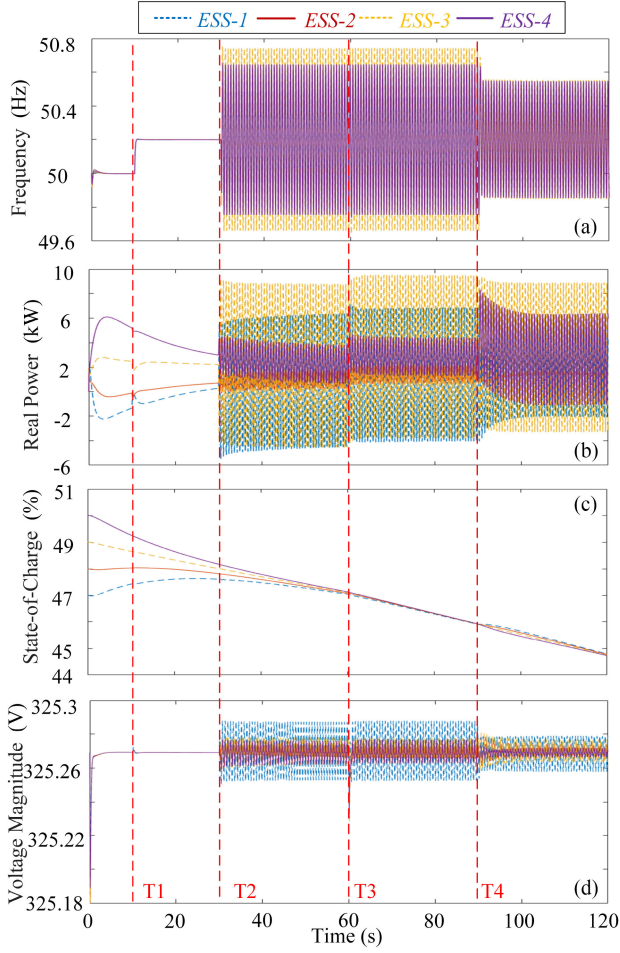


Fig. 5. Real-time test results by using the existing method in [15]. (a) Frequency response. (b) Real power output. (c) State-of-charge. (d) Voltage magnitude.

- 1) $0 \text{ s} < t \leq 10 \text{ s}$: It can be found that the proposed control method offers similar control performance under normal working conditions as in Case 1.
- 2) $10 \text{ s} < t \leq 30 \text{ s}$: Due to the bias fault or attack of $\delta_1(t) = 10$ at $T_1 = 10 \text{ s}$, there will be an overshoot for MG frequency. The proposed control method can react timely to compensate for the bias signals and the MG frequency can be controlled back to the reference value.
- 3) $30 \text{ s} < t \leq 90 \text{ s}$: Although there is a bias fault or attack of $\delta_3(t) = 20 \sin(10t)$ at $T_2 = 30 \text{ s}$, the system frequency, real power output, and voltage magnitude remain almost the same as normal conditions. From the zoom-in figure of Fig. 6(a), it can be found the proposed method mitigate the oscillation into a very small extent. Besides, the control functions operate normally when there is a load change in $T_3 = 60 \text{ s}$.
- 4) $90 \text{ s} < t \leq 120 \text{ s}$: The changes in the gain of the secondary controller at $T_4 = 90 \text{ s}$ is also overcome by the proposed control method.

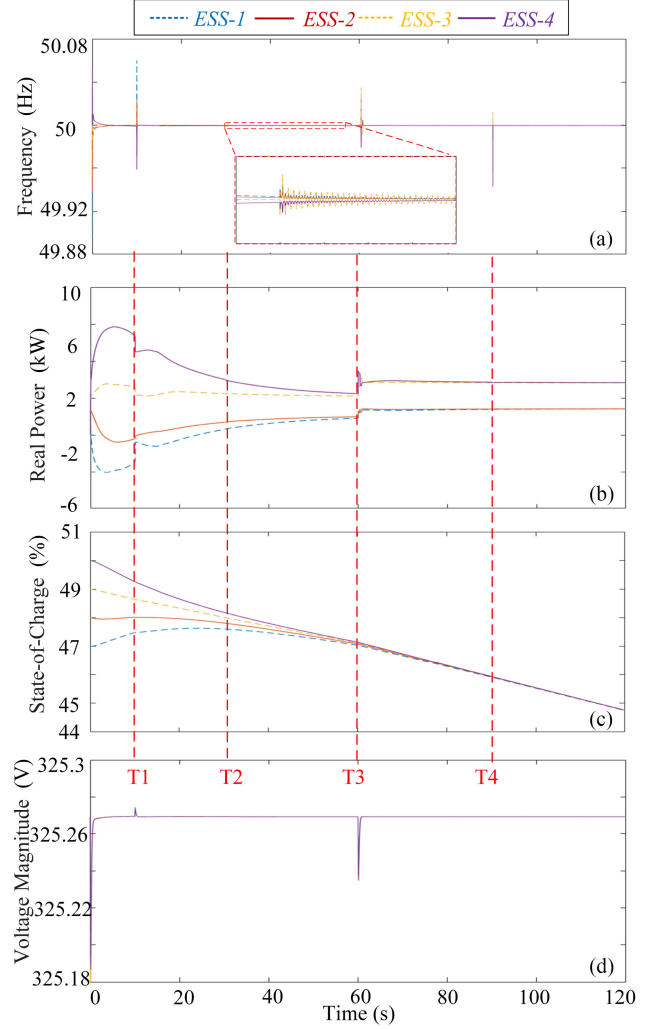


Fig. 6. Real-time test results by using the proposed distributed resilient control method: (a) Frequency response. (b) Real power output. (c) State-of-charge. (d) Voltage magnitude.

C. Test Case 3: Stealth Coordinated Node Attacks

In this case, the proposed control method is validated under stealth coordinated node attacks. For the coordinated node attacks in the secondary controller, the attack signal can be injected as $\sum_{i=1}^N \delta_i = 0$. In this manner, the frequency will not be deviated by this attack, i.e., $\lim_{t \rightarrow \infty} (\omega_i(t) - \omega^{\text{ref}}) = 0$. Similarly, for attack signal injected as $\delta_i = \delta_j$, the power sharing performance will not be distorted $\lim_{t \rightarrow \infty} (\Phi_i(t) - \Phi_j(t)) = 0$. The above coordinated node attacks belong to stealth attacks, as discussed in [29].

In this case, it is considered that a coordinated node attack $\delta(t) = [2, 2, -2]$ (Stealth Attack-1) occurs in $t = 10 \text{ s}$. Then another coordinated node attack $\delta(t) = [2, 2, 2, 2]$ (Stealth Attack-2) occurs in $t = 30 \text{ s}$. By using the proposed resilient control method, the real-time test results are shown in Fig. 7, which shows that the proposed method is able to handle this kind of stealth attacks.

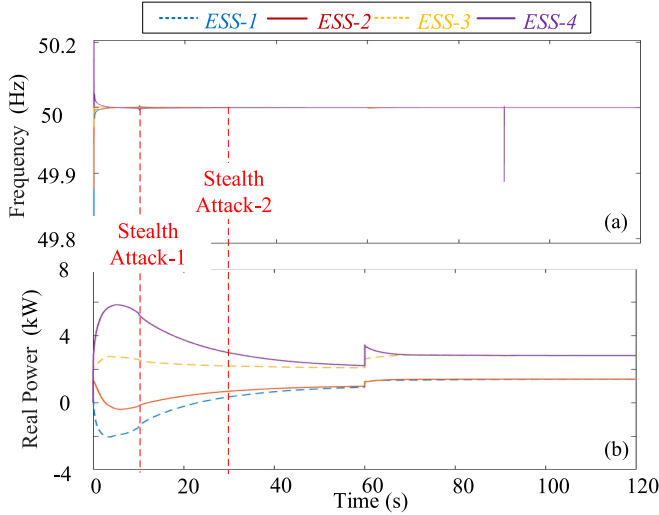


Fig. 7. Real-time test results of the distributed resilient control under stealth coordinated node attacks. (a) Frequency response. (b) Real power output.

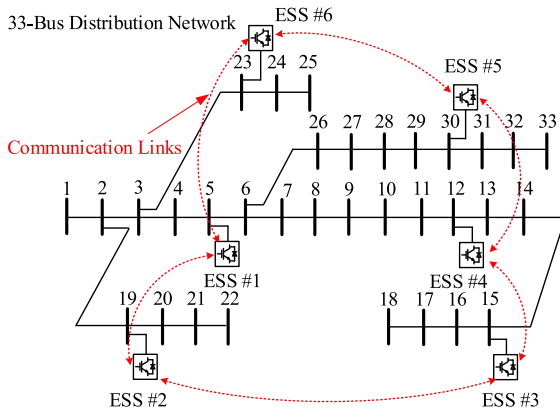


Fig. 8. Modified IEEE 33-bus test systems with six ESSs.

D. Test Case 4: Coordinated Node Attacks in 33-Bus System

In this case, a modified IEEE 33-bus distribution network in [43] is used to test the proposed distributed resilient control method in a larger scale power network. As shown in Fig. 8, six ESSs are located at bus 5, 12, 15, 19, 23, and 30. Their initial SoCs are 0.47, 0.48, 0.49, 0.51, 0.52, and 0.53. The communication links among ESSs are also shown in Fig. 8. The OPAL-RT test results of frequency, real power, SoC and voltage magnitude are shown in Fig. 9(a)–(d). Coordinated node attacks with balanced signal injection are considered in this case. The attack signal of $\delta_i(t) = 20$ occur in all nodes at $t = 10$ s, while the attack signal of $\delta_i(t) = 20 \sin(10t)$ present at $t = 30$ s. As observed from Fig. 9, the proposed control method can react timely to compensate for these attack signals. The MG frequency and voltage can be restored to their reference values in a short time after cyber attacks. The MG system can response normally to load change at $t = 60$ s. It can be concluded that the proposed method is applicable to practical large scale systems.

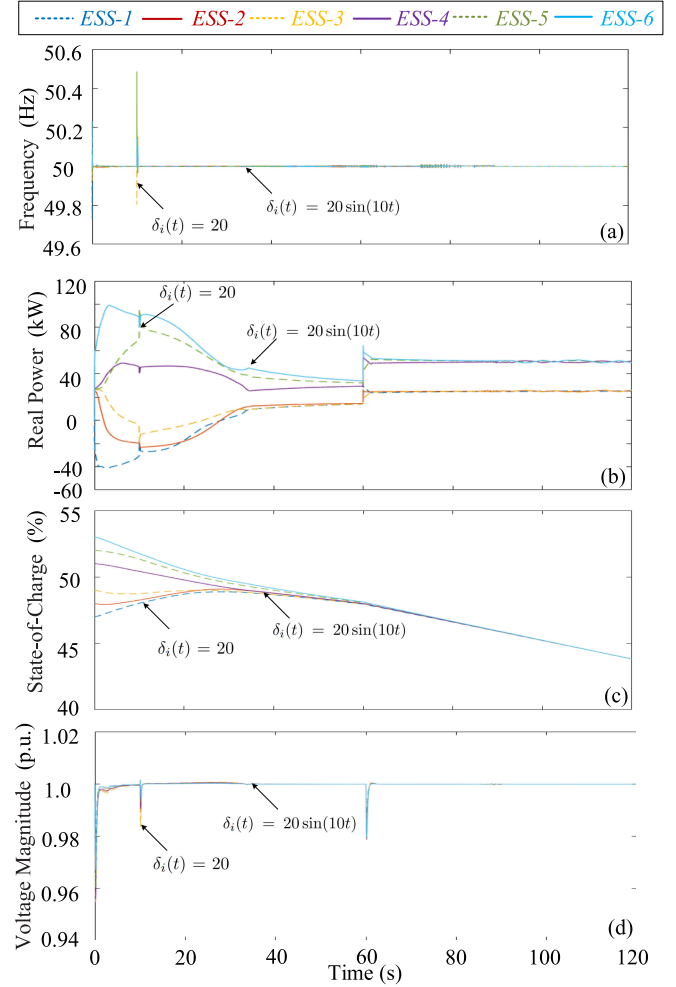


Fig. 9. Real-time test results by using the proposed distributed resilient control method. (a) Frequency response. (b) Real power output. (c) State-of-charge. (d) Voltage magnitude.

V. CONCLUSION

In this article, a novel distributed resilient control method for SoC balancing, proportional power sharing, and frequency and voltage restoration was proposed for ESSs in cyber-physical MGs. The control problems were formulated as leader-following and leaderless consensus problems under the presence of faults/attacks in the secondary control process. By using the adaptive technique, distributed resilient controllers were designed to compensate for the influence of faults and attacks. It was proved that the stability of the error systems can be achieved by the developed method. Besides, the proposed controllers were implemented in MG test systems on OPAL-RT. The test results validated the effectiveness of the proposed method under various faults and attacks. It was found that the proposed distributed resilient control method can deal with both single node and multiple nodes attacks scenarios.

APPENDIX: PROOF OF THEOREM 1

To prove the theorem, we introduce the following lemma.

Lemma 1. [44]: If $\hat{a}_i(0) > \hat{b}_i(0)$ and $\hat{c}_i(0) > \hat{d}_i(0) > 0$, then $\hat{a}_i(t) > \hat{b}_i(t) \geq 0$ and $\hat{c}_i(t) > \hat{d}_i(t) \geq 0$ for all $t > t_0$.

Then, we prove Theorem 1. Consider the Lyapunov function

$$\begin{aligned} V(t) = & \bar{x}^T(t)(\mathcal{L} \otimes P)\bar{x}(t) \\ & + \sum_{i=1}^N \varphi_i \left(\frac{1}{\gamma_{i1}} \tilde{a}_i^2(t) + \frac{\gamma_{i2}}{\gamma_{i1}\gamma_{i5}} \tilde{b}_i^2(t) \right. \\ & \left. + \frac{1}{\gamma_{i3}} \tilde{c}_i^2(t) + \frac{\gamma_{i4}}{\gamma_{i3}\gamma_{i6}} \tilde{d}_i^2(t) \right) \end{aligned}$$

where $\tilde{a}_i(t) = \hat{a}_i(t) - \frac{\delta_i + \bar{d}_i}{\varphi_i}$, $\tilde{b}_i(t) = \hat{b}_i(t) - \frac{\delta_i + \bar{d}_i}{\varphi_i}$, $\tilde{c}_i(t) = \hat{c}_i(t) - \frac{c}{\varphi_i}$ and $\tilde{d}_i(t) = \hat{d}_i(t) - \frac{c}{\varphi_i}$. The derivative of $V(t)$ along the closed-loop system (23) yields

$$\begin{aligned} \dot{V}(t) = & 2\bar{x}^T(t)(\mathcal{L} \otimes PA)\bar{x}(t) \\ & + 2 \sum_{i=1}^N \xi_i^T PB (\delta_i(t) + d_i(t) + \varphi_i(t)u_i^E(t)) \\ & + 2 \sum_{i=1}^N \varphi_i \left(\frac{1}{\gamma_{i1}} \tilde{a}_i(t)\dot{\tilde{a}}_i(t) + \frac{1}{\gamma_{i3}} \tilde{c}_i(t)\dot{\tilde{c}}_i(t) \right. \\ & \left. + \frac{\gamma_{i2}}{\gamma_{i1}\gamma_{i5}} \tilde{b}_i(t)\dot{\tilde{b}}_i(t) + \frac{\gamma_{i4}}{\gamma_{i3}\gamma_{i6}} \tilde{d}_i(t)\dot{\tilde{d}}_i(t) \right). \end{aligned}$$

Using the controller (17) and Lemma 1, we have

$$\begin{aligned} \dot{V}(t) \leq & \bar{x}^T(t)(\mathcal{L} \otimes (PA + A^T P) - 2c\mathcal{L}^2 \otimes PBB^T P)\bar{x}(t) \\ & + 2 \sum_{i=1}^N \|\xi_i^T(t)PB\|((\bar{\delta}_i + \bar{d}_i) - \varphi_i \hat{a}_i(t)) \\ & + 2 \sum_{i=1}^N \|\xi_i^T(t)PB\|^2(c - \varphi_i \hat{c}_i(t)) \\ & + 2 \sum_{i=1}^N \varphi_i \left(\frac{1}{\gamma_{i1}} \tilde{a}_i(t)\dot{\tilde{a}}_i(t) + \frac{\gamma_{i2}}{\gamma_{i1}\gamma_{i5}} \tilde{b}_i(t)\dot{\tilde{b}}_i(t) \right. \\ & \left. + \frac{1}{\gamma_{i3}} \tilde{c}_i(t)\dot{\tilde{c}}_i(t) + \frac{\gamma_{i4}}{\gamma_{i3}\gamma_{i6}} \tilde{d}_i(t)\dot{\tilde{d}}_i(t) \right) \end{aligned}$$

where $c = \frac{1}{\lambda_2}$ with $\lambda_2 > 0$ (where $\lambda_2 > 0$ is the minimum nonzero eigenvalue as discussed in [37] under the condition of the communication graph \mathcal{G} is connected). From (18) to (22) and the definition of c , it is shown that

$$\begin{aligned} \dot{V}(t) \leq & -\bar{x}^T(t)(\mathcal{L} \otimes Q)\bar{x}(t) - 2 \sum_{i=1}^N \varphi_i \tilde{a}_i(t) \|\xi_i^T(t)PB\| \\ & + 2 \sum_{i=1}^N \varphi_i \left(\tilde{a}_i(t) (\|\xi_i^T(t)PB\| - \frac{\gamma_{i2}}{\gamma_{i1}} (\hat{a}_i(t) - \hat{b}_i(t))) \right. \\ & \left. + \frac{\gamma_{i2}}{\gamma_{i1}} \tilde{b}_i(t) (\hat{a}_i(t) - \hat{b}_i(t)) \right) \\ & - 2 \sum_{i=1}^N \varphi_i \tilde{c}_i(t) \|\xi_i^T(t)PB\|^2 \end{aligned}$$

$$\begin{aligned} & + 2 \sum_{i=1}^N \varphi_i \left(\tilde{c}_i(t) (\|\xi_i^T(t)PB\|^2 - \frac{\gamma_{i4}}{\gamma_{i3}} (\hat{c}_i(t) - \hat{d}_i(t))) \right. \\ & \left. + \frac{\gamma_{i4}}{\gamma_{i3}} \tilde{d}_i(t) (\hat{c}_i(t) - \hat{d}_i(t)) \right) \\ = & -\bar{x}^T(t)(\mathcal{L} \otimes Q)\bar{x}(t) - 2 \sum_{i=1}^N \frac{\gamma_{i2}}{\gamma_{i1}} \varphi_i (\hat{a}_i(t) - \hat{b}_i(t))^2 \\ & - 2 \sum_{i=1}^N \frac{\gamma_{i4}}{\gamma_{i3}} \varphi_i (\hat{c}_i(t) - \hat{d}_i(t))^2 \\ \leq & 0 \end{aligned}$$

which implies that $\lim_{t \rightarrow \infty} \bar{x}(t) = 0$. This completes the proof.

REFERENCES

- [1] A. Bidram, F. L. Lewis, and A. Davoudi, "Distributed control systems for small-scale power networks: Using multiagent cooperative control theory," *IEEE Trans. Control Syst. Mag.*, vol. 34, no. 6, pp. 56–77, Nov. 2014.
- [2] X. Yu, and Y. Xue, "Smart grids: A cyber-physical systems perspective," *Proc. IEEE*, vol. 104, no. 5, pp. 1058–1070, Mar. 2016.
- [3] Y. Wang, T. L. Nguyen, Y. Xu, Z. Li, Q. Tran, and R. Caire, "Cyber-physical design and implementation of distributed event-triggered secondary control in islanded microgrids," *IEEE Trans. Ind. Appl.*, vol. 55, no. 6, pp. 5631–5642, Nov./Dec. 2019.
- [4] T. Morstyn, B. Hredzak, and V. G. Agelidis, "Control strategies for microgrids with distributed energy storage systems: An overview," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 3652–3666, Dec. 2016.
- [5] H. Cai and G. Hu, "Distributed control scheme for package-level state-of-charge balancing of grid-connected battery energy storage system," *IEEE Trans. Ind. Informat.*, vol. 12, no. 5, pp. 1919–1929, Aug. 2016.
- [6] L. Xing *et al.*, "Dual-consensus-based distributed frequency control for multiple energy storage systems," *IEEE Trans. Smart Grid*, vol. 10, no. 6, pp. 6396–6403, Nov. 2019.
- [7] L. Ding, Q. L. Han, and X. M. Zhang, "Distributed secondary control for active power sharing and frequency regulation in islanded microgrids using an event-triggered communication mechanism," *IEEE Trans. Ind. Informat.*, vol. 15, no. 7, pp. 3910–3922, Jul. 2019.
- [8] Y. Wang, M. H. Syed, E. Guillo-Sansano, Y. Xu, and G. M. Burt, "Inverter-based voltage control of distribution networks: A three-level coordinated method and power hardware-in-the-loop validation," *IEEE Trans. Sustain. Energy*, to be published, doi: [10.1109/TSTE.2019.2957010](https://doi.org/10.1109/TSTE.2019.2957010).
- [9] J. M. Guerrero, J. C. Vasquez, J. Matas, and L. G. de Vicuna, "Hierarchical control of droop-controlled AC and DC microgrids—A general approach toward standardization," *IEEE Trans. Ind. Electron.*, vol. 58, no. 1, pp. 158–172, Jan. 2011.
- [10] Q. Shafiee, J. M. Guerrero, and J. C. Vasquez, "Distributed secondary control for islanded microgrids—A novel approach," *IEEE Trans. Power Electron.*, vol. 29, no. 2, pp. 1018–1031, Feb. 2014.
- [11] F. Guo, C. Wen, J. Mao, and Y. Song, "Distributed secondary voltage and frequency restoration control of droop-controlled inverter-based microgrids," *IEEE Trans. Ind. Electron.*, vol. 62, no. 7, pp. 4355–4364, Jul. 2015.
- [12] J. W. Simpson-Porco, Q. Shafiee, F. Dorfler, 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, May 2015.
- [13] X. Lu, K. Sun, J. Guerrero, and J. Vasquez, "State-of-charge balance using adaptive droop control for distributed energy storage systems in DC microgrid applications," *IEEE Trans. Ind. Electron.*, vol. 61, no. 6, pp. 2804–2815, Jun. 2014.
- [14] J. Khazaei and Z. Miao, "Consensus control for energy storage systems," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 3009–3017, Jul. 2018.
- [15] Y. Wang, Y. Xu, Y. Tang, K. Liao, and M. Syed, "Aggregated energy storage for power system frequency control: A finite-time consensus approach," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 3675–3686, Jul. 2019.
- [16] R. Zhang and B. Hredzak, "Nonlinear sliding mode and distributed control of battery energy storage and photovoltaic systems in AC microgrids with time delays," *IEEE Trans. Ind. Informat.*, vol. 15, no. 9, pp. 5149–5160, Sep. 2019.

- [17] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Trans. Autom. Control*, vol. 58, no. 11, pp. 2715–2729, Jun. 2013.
- [18] Y. Liu, H. Xin, Z. Qu, and D. Gan, "An attack-resilient cooperative control strategy of multiple distributed generators in distribution networks," *IEEE Trans. Smart Grid*, vol. 7, no. 6, pp. 2923–2932, Mar. 2016.
- [19] R. M. Lee, M. J. Assante, and T. Conway, "Analysis of the cyber attack on the Ukrainian power grid," *Electricity Inf. Sharing Anal. Center*, 2016.
- [20] "Taiwan: Massive power blackout affects millions," 2017. [Online]. Available: <https://time.com/4902500/taiwan-power-cut/>
- [21] Y. Cherdantseva and J. Hilton, "A reference model of information assurance & security," in *Proc. IEEE Int. Conf. Availability, Rel. Secur.*, 2013, pp. 546–555.
- [22] S. M. Dibaji, M. Pirani, D. B. Flamholz, A. M. Annaswamy, K. H. Johansson, and A. Chakraborty, "A systems and control perspective of CPS security," *Annu. Rev. Control*, vol. 47, pp. 394–411, 2019.
- [23] 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, 2019, doi: [10.1016/j.arcontrol.2019.08.002](https://doi.org/10.1016/j.arcontrol.2019.08.002).
- [24] 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.
- [25] S. Sahoo, T. Dragičević, and F. Blaabjerg, "Cyber security in control of grid-tied power electronic converters—challenges and vulnerabilities," *IEEE J. Emerg. Sel. Topics Power Electron.*, to be published, doi: [10.1109/JESTPE.2019.2953480](https://doi.org/10.1109/JESTPE.2019.2953480).
- [26] 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, Jan. 2017.
- [27] S. Sahoo, J. C. Peng, S. Mishra, and T. Dragicevic, "Distributed screening of hijacking attacks in DC microgrids," *IEEE Trans. Power Electron.*, vol. 35, no. 7, pp. 7574–7582, Jul. 2020.
- [28] L. Y. Lu, H. J. Liu, H. Zhu, and C. C. Chu, "Intrusion detection in distributed frequency control of isolated microgrids," *IEEE Trans. Smart Grid*, vol. 10, no. 6, pp. 6502–6515, Nov. 2019.
- [29] S. Sahoo, S. Sahoo, S. Mishra, J. Peng, and T. Dragicevic, "A stealth cyber-attack detection strategy for DC microgrids," *IEEE Trans. Power Electron.*, vol. 34, no. 8, pp. 8162–8174, Nov. 2018.
- [30] 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, Jun. 2017.
- [31] A. Bidram, B. Poudel, L. Damodaran, R. Fierro, and J. M. Guerrero, "Resilient and cybersecure distributed control of inverter-based islanded microgrids," *IEEE Trans. Ind. Informat.*, vol. 16, no. 6, pp. 3881–3894, Jun. 2020.
- [32] N. M. Dehkordi, H. R. Baghaee, N. Sadati, and J. M. Guerrero, "Distributed noise-resilient secondary voltage and frequency control for islanded microgrids," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 3780–3790, Jul. 2019.
- [33] L. Ding, Q. Han, L. Wang, and E. Sindi, "Distributed cooperative optimal control of DC microgrids with communication delays," *IEEE Trans. Ind. Informat.*, vol. 14, no. 9, pp. 3924–3935, Jan. 2018.
- [34] J. Duan and M. Y. Chow, "Robust consensus-based distributed energy management for microgrids with packet losses tolerance," *IEEE Trans. Smart Grid*, vol. 11, no. 1, pp. 281–290, Jan. 2020.
- [35] C. Deng and G. Yang, "Distributed adaptive fault-tolerant control approach to cooperative output regulation for linear multi-agent systems," *Automatica*, vol. 103, pp. 62–68, May 2019.
- [36] C. Deng, G. Yang, and M. Er, "Decentralized fault-tolerant MRAC for a class of large-scale systems with time-varying delays and actuator faults," *J. Process Control*, vol. 75, pp. 171–186, Mar. 2019.
- [37] G. Royle and C. Godsil, "Algebraic Graph Theory," in *Springer Graduate Texts in Mathematics*, Berlin, Germany: Springer-Verlag, 2001, vol. 207.
- [38] J. M. Guerrero, J. Matas, L. Garcia de Vicuna, M. Castilla, and J. Miret, "Decentralized control for parallel operation of distributed generation inverters using resistive output impedance," *IEEE Trans. Ind. Electron.*, vol. 54, no. 2, pp. 994–1004, Apr. 2007.
- [39] A. Bidram, A. Davoudi, F. L. Lewis, and Z. Qu, "Secondary control of microgrids based on distributed cooperative control of multi-agent systems," *IET Gener., Transmiss. Distrib.*, vol. 7, no. 8, pp. 822–831, Aug. 2013.
- [40] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "A secure control framework for resource-limited adversaries," *Automatica*, vol. 51, pp. 135–148, Jan. 2015.
- [41] Y. Mo and B. Sinopoli, "On the performance degradation of cyber-physical systems under stealthy integrity attacks," *IEEE Trans. Autom. Control*, vol. 61, no. 9, pp. 2618–2624, Sep. 2016.
- [42] J. Rocabert, A. Luna, A. Luna, and P. Rodríguez, "Control of power converters in AC microgrids," *IEEE Trans. Power Electron.*, vol. 27, no. 11, pp. 4734–4749, Nov. 2012.
- [43] M. E. Baran and F. F. Wu, "Network reconfiguration in distribution systems for loss reduction and load balancing," *IEEE Trans. Power Del.*, vol. 4, no. 2, pp. 1401–1407, Apr. 1989.
- [44] C. Deng, "Cooperative fault-tolerant output regulation of linear heterogeneous multi-agent systems under directed network topology," *IEEE Trans. Syst. Man Cybern. Syst.*, to be published, doi: [10.1109/TSMC.2019.2944254](https://doi.org/10.1109/TSMC.2019.2944254).



Chao Deng received the Ph.D. degree in control engineering from Northeastern University, Shenyang, China, in 2018.

He is currently a Postdoctoral Research Fellow with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore. His research interests include distributed fault-tolerant control, event-triggered control, microgrids and cyber-physical systems.



Yu Wang (Member, IEEE) received the B.Eng. degree from the School of Electrical Engineering and Automation, Wuhan University, China, in 2011, and the M.Sc. and Ph.D. degrees in power engineering from Nanyang Technological University, Singapore, in 2012 and 2017, respectively.

He is currently a Research Fellow with Nanyang Technological University. He is leading and investigating industry projects in hybrid microgrid systems, energy storage systems, and cyber-security of power systems. His research interests include distributed control and optimization in electrical power systems, microgrids and cyber-physical systems.



Changyun Wen (Fellow, IEEE) received the B.Eng. degree in control engineering from Xi'an Jiaotong University, Xi'an, China, in 1983 and the Ph.D. degree in control engineering from the University of Newcastle, Newcastle, Australia, in 1990.

Since August 1991, he has been with School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, where he is currently a Full Professor of Control Engineering. His main research activities include the areas of control systems and applications, smart grids, cyber-physical systems, complex systems, and networks.

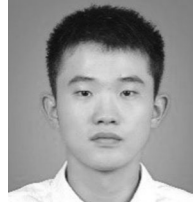
Dr. Wen was a member of IEEE Fellow Committee from January 2011 to December 2013. He is an Associate Editor of a number of journals including *Automatica*, *IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS* and *IEEE CONTROL SYSTEMS MAGAZINE*. He is the Executive Editor-in-Chief of *Journal of Control and Decision*. He was an Associate Editor with the *IEEE TRANSACTIONS ON AUTOMATIC CONTROL* from January 2000 to December 2002.



Yan Xu (Senior Member, IEEE) received the B.E. and M.E. degrees in electrical engineering from South China University of Technology, Guangzhou, China, in 2008 and 2011, respectively, and the Ph.D. degree in electrical engineering from The University of Newcastle, Australia, in 2013.

He is currently a Nanyang Assistant Professor of Electrical and Electronics Engineering with the School of Electrical and Electronic Engineering, Nanyang Technological University (NTU), and a Cluster Director with Energy Research Institute @NTU (ERI@N), Singapore. Previously, he held The University of Sydney Post-doctoral Fellowship in Australia. His research interests include power system stability and control, microgrid, and data-analytics for smart grid applications.

Dr Xu is an Editor for IEEE TRANSACTIONS ON SMART GRID, IEEE TRANSACTIONS ON POWER SYSTEMS, IEEE POWER ENGINEERING LETTERS, Chinese Society for Electrical Engineering (CSEE) Journal of Power and Energy Systems, and an Associate Editor for Institution of Engineering and Technology (IET) Generation, Transmission and Distribution.



Pengfeng Lin (Student Member, IEEE) received the B.S. and M.S. degrees in electrical engineering from Southwest Jiaotong University, Chengdu, China, in 2013 and 2015, respectively, and the Ph.D. degree in power engineering from Nanyang Technological University, Singapore, in 2019.

He is currently with Energy Research Institute @ NTU (Eri@N) as a Research Fellow. His research interests include power system stability/reliability analyses, smart grid cyber–physical security, and artificial intelligence analytics.