Resilient Cooperative Secondary Control of Islanded AC Microgrids Utilizing Inverter-Based Resources Against State-Dependent False Data Injection Attacks

Mahmood Jamali, Mahdieh S. Sadabadi, *Senior Member, IEEE*, Masoud Davari*, *Senior Member, IEEE*, Subham Sahoo, *Senior Member, IEEE*, and Frede Blaabjerg, *Fellow, IEEE*

***Abstract*—This paper investigates the impact of potential state-dependent false data injection cyber-attacks on frequency synchronization and active power management in islanded ac microgrids. One potential way of affecting microgrid reliability is by forcing a generation outage. Thus, the attacker could potentially aim to desynchronize inverter-based resources in microgrids by manipulating their frequency with malicious injections. The attack signals are injected to manipulate control input channels, sensor nodes, reference values, and the information exchanged through communication networks. In order to mitigate the adverse impacts of such cyber-attacks, firstly, the conventional distributed consensus-based secondary control approach is modified and complemented in the presence of cyber-attacks. Secondly, a resilient cooperative distributed secondary control scheme is proposed by utilizing the concept of a virtual layer interconnected with the main network layer. Thirdly, theoretical stability, resilience analysis, and design considerations of interconnection matrices are also provided. Finally, simulations through MATLAB/Simulink and experimental results are presented in order to illustrate the robust performance of the proposed control scheme.**

***Index Terms*—False data injection (FDI), inverter-based resources (IBRs), islanded ac microgrids, resilient active power-sharing, resilient cooperative control, resilient frequency synchronization, state-dependent FDI cyber-attacks.**

The work of Masoud Davari was supported in part by the U.S.-Denmark INNOVATOR program between Georgia Southern University, Statesboro, GA, USA, and Aalborg University, Aalborg, Denmark, funded by the International Research Experiences for Students (IRES) program in the Office of International Science and Engineering (OISE) in the U.S. National Science Foundation (U.S. NSF) under U.S. NSF OISE-IRES Award #2152905, in part by the U.S. NSF under ECCS-EPCN Awards #1902787 and #1808279, and in part by the dSPACE company, Verivolt company, the professional development part of Masoud Davari's Discovery & Innovation Award from the 2020–2021 University Awards of Excellence at Georgia Southern University, and his 2022 Impact Area Accelerator Grant partially funded by Georgia Southern University—at which all experiments to test the effectiveness of the proposed method were conducted. *(*Corresponding author: Masoud Davari.)*

M. Jamali is with the Department of Automatic Control and Systems Engineering, University of Sheffield, Sheffield S1 3JD, United Kingdom (e-mail: mahmood.jamali@sheffield.ac.uk).

M. S. Sadabadi is with the School of Electronic Engineering and Computer Science, Queen Mary University of London, London E1 4NS, United Kingdom (e-mail: m.sadabadi@qmul.ac.uk).

Masoud Davari is with the Department of Electrical and Computer Engineering, Georgia Southern University (Statesboro Campus), Statesboro, GA 30460 USA (e-mail: mdavari@georgiasouthern.edu; davari@ualberta.ca).

Subham Sahoo and Frede Blaabjerg are with AAU Energy (Department of Energy), Aalborg University, Aalborg 9220, Denmark (e-mails: sssa@energy.aau.dk; fbl@energy.aau.dk).

NOMENCLATURE

A. IBRs' Variables

v_i^n, w_i^n	Voltage and frequency of each IBR provided for the internal control loops.
v_{odi}	Direct components of the output voltage of each IBR.
ω_i, P_i, Q_i	Frequency, active power and reactive power of each IBR.
ω^{ref}	Reference frequency value.
m_i^P, n_i^Q	Active power and reactive power droop coefficients of each IBR.
u_i^ω	Auxiliary frequency inputs of each IBR.

B. Control Parameters

c_ω	Positive coupling gain.
β	Positive control parameter.
K, $\mathcal{H}$, M, D	Interconnection matrices.

C. Attack Parameters

δ_i^S, δ_i^0	FDI cyber-attacks on the *i*-th IBR's sensors and reference frequency.
δ_i^C, δ_i^a	FDI cyber-attacks on the *i*-th IBR's transmitted data and actuators.
α	Bounded weight gain used for attacks on sensors and the reference frequency.

I. INTRODUCTION

Microgrids have the capability of operating in grid-connected and islanded modes. Even though microgrids' stability can be achieved through well-designed control algorithms in the grid-connected mode, the islanded mode of operation in microgrids is more intensely vulnerable to any disturbances, such as load changes [1]. Control objectives for the islanded mode of ac microgrids are commonly performed hierarchically, consisting of primary, secondary, and tertiary levels [2]. In order to improve the reliability, scalability, and sparseness of communication networks in microgrids, distributed control methodologies are preferred at the secondary level of microgrids based on inverter-based resources (IBRs); for example, see [3]. However, the vulnerability of microgrids to cyber-attacks will be rather increased due to insufficient global information

in distributed cyber topologies [4]. According to [5] and [6], cyber-attacks in control systems can generally be in the form of replay, *denial-of-service* and *false data injection* (FDI) attacks, influencing sensor readings, control input channels, and communication networks. This study focuses on the so-called FDI attacks, which are low visible to attack detectors and high risk rather than the other categories.

The significant research on cyber-security in the control layers of microgrids has mainly focused on (i) attack detection methods and (ii) resilient control strategies. The first group primarily investigates the identification of adversarial agents and, afterward, the use of intelligent algorithms to isolate the compromised IBRs. For frequency synchronization in microgrids, the authors in [7] employed a confidence factor to identify only constant-valued FDI attacks and exclude the corrupted IBRs. Also, a cyber-attack resilient control strategy for islanded microgrids was suggested in [8] to provide timely detection and isolation of malicious transmitted data and local controllers in a distributed fashion. The authors in [9] have discussed the conditions where a skilled attacker can be successful and also derive equations to determine the threshold for the proposed FDI attack detection strategy. However, the drawback of detection methods is that they can identify the compromised IBRs as long as the communication network is highly sparse. Since the FDI attack detection significantly relies on graph-related theoretical methods, the detection method will fail if the neighbors of the targeted unit are all under attack [10], [11]. Moreover, the removal of a unit might potentially cause stability issues as the (graph) topology changes. It can also be shown that well-planned FDI attacks are capable of bypassing the existing attack identification observers [12]. Recent literature has effectively investigated the destructive effects and detection problems of stealthy FDI attacks in networked control systems—see [13], [14]—where the measurement and control data are modified before transmission. Nevertheless, such methods only address the detection procedure and do not discuss the design of resilient control schemes.

Conversely, the main objective of the attack-mitigation strategies is to design resilient control algorithms to alleviate the devastating impacts of cyber-attacks and restore the desirable performance of the microgrid. In order to enhance the resilient performance of the primary level control against attacks on hardware firmware and sensors in the zero-level control system, a reliable control method based on a sliding mode algorithm is proposed for microgrids in [15]. Also, the authors in [16] bring forth a novel mathematical approach to assure proper economic optimization while data integrity attacks target microgrids' tertiary layers.

For the secondary control, [1] has proposed a cyber-resilient detection/mitigation platform based on a sliding-mode consensus algorithm against FDI attacks on the transmission data. However, this algorithm relies on the isolation of attacked nodes. Similarly, an event-driven attack-resilient controller has been suggested in [17] to mitigate stealthy FDI attacks in ac microgrids. Still, it can only establish resilient synchronization for a limited number of malicious IBRs. The authors in [18] have presented an attack-mitigation technique to improve the resilience of distributed secondary control of ac microgrids against FDI attacks. This approach, nevertheless, relies on the suggested Kullback-Leibler detector to measure the trustworthiness of the IBR units' information. The secondary control scheme in [19] has provided the desired performance under unreliable actuators and sensor circumstances stemming from cyber threats; this methodology immensely depends on fault detectors. The control approach influenced by the weighted mean subsequence reduced technique has been proposed for reliable operation in ac microgrids [20]; the controller succeeds in discarding the corrupted data. However, it needs to be equipped with a communication graph with a minimum connectivity criterion.

Inspired by [21], in which the concept of a virtual layer for multi-agent systems has been fostered, some studies have developed cooperative distributed controllers for the microgrid's secondary control layer [22]–[25]. Although the methods proposed in those studies improve cyber-attack-resilience in microgrids, they are limited to simple FDI attack scenarios where the attack policy is not chosen to be necessarily smart. Furthermore, these methods rely on a key but restrictive assumption that the attacker cannot manipulate all vulnerable locations in the secondary control of microgrids, e.g., sensors, reference values, communication links, and control input channels.

For example, different attack categories on ac microgrids are considered, which can affect the communication channels, information exchange, and local feedback controllers; see [22]. In this control scheme, requiring two leaders, it is assumed that there exists a directed path from at least one leader to each local IBR in the graph topology. Apart from the restriction on the communication graph connectivity and the requisite number of leader nodes, this paper only deals with state-independent FDI attacks. Similarly, the proposed distributed secondary control in [25] is resilient to only state-independent FDI attacks. The authors in [23] and [24] have also addressed the problem of attack-resilient control for islanded microgrids when only the control inputs are exposed to linear state-dependent FDI attacks injected in control inputs. To the best of the authors' knowledge, the research on the resilience of control mechanisms against state-dependent FDI attacks is still in its infancy and requires further investigation.

Inspired by the limitations of the current research on cybersecurity in islanded microgrids, this paper considers the problem of attack-resilient cooperative secondary frequency synchronization and active power management in islanded ac microgrids subject to complex FDI cyber-attacks. In particular, the main focus (of this paper) is on state-dependent FDI cyber-attacks, where the attacker's goal is to destabilize microgrids and drive their trajectories to an unsafe operating condition while remaining stealthy. The term "state-dependent" means that the FDI attack policy is dynamic and varies in accordance with the frequency (state trajectory) transients. By employing a first-order dynamic model of the attack, the inadequacy of the conventional control algorithm against such attacks is demonstrated. The main contribution of the paper can be listed as follows.

1) This article proposes a control scheme to ensure the

microgrids' secondary control objectives and guarantee microgrids' stability despite the existence of state-dependent attacks. To this end, a virtual network layer is designed—which is interconnected with the main communication layer but shielded from attackers. The proposed resilient secondary control scheme provides an acceptable level of operational normalcy in microgrids against cyber-attacks without the need for any attack detection mechanisms.

2) Unlike the previous studies (e.g., [23] and [24]), this work considers state-dependent attacks with linear/nonlinear dynamics—which can easily distort all vulnerable locations in microgrids' secondary frequency control, i.e., the control commands, communication channels, sensor nodes, and reference values. Additionally, it takes into account a special state-dependent attack that targets the leader node in the secondary control system.
3) In contrast to the existing detection/mitigating approaches (e.g., [7] and [8]), the proposed cooperative control framework does not have any assumptions on the number of IBRs being attacked. As a result, the microgrid maintains its stability and desired performance even though all units are affected by intrusions.
4) Rigorous stability analysis based on the Lyapunov method is also provided in order to reveal how interconnection matrices should be designed to guarantee resilient frequency synchronization in ac microgrids.

The rest of the paper is organized as follows. The dynamic model of ac microgrids is presented in Section II. Next, the model of cyber-attacks and their impacts on the microgrid performance is discussed in Section III. Section IV is devoted to the resilient design of cooperative secondary controllers in ac microgrids and to show its resilience in the presence of state-dependent FDI attacks. Comparative simulations along with experimental results are given in Section V. Section VI concludes this paper.

Notation: Throughout this paper, $\mathbf{1_N}$, $\mathbf{0_N}$, and I_N are an $N \times 1$ vector of ones, $N \times 1$ vector of zeros, and $N \times N$ identity matrix, respectively. Y^T and $det(Y)$ stand for the transpose and the determinant of the matrix Y, respectively. For a symmetric matrix Y, the positive definite and the negative semi-definite operators are indicated by $Y > 0$ and $Y \leq 0$, respectively. The symbol $diag(y_1, ..., y_N)$ represents a diagonal matrix whose diagonal elements are y_i. $\|.\|$ denotes the standard Euclidean norm. $\mathbb{R}_+$ and $\mathbb{R}_{\geq 0}$ are the set of positive and non-negative real numbers, respectively.

Preliminaries: For an undirected graph topology with the adjacency matrix $\mathcal{A}$ and out-degree matrix $\mathcal{D}_{out}$, the Laplacian matrix, described by $\mathcal{L} = \mathcal{D}_{out} - \mathcal{A}$, is symmetric and zero row-sums, i.e., $\mathcal{L} = \mathcal{L}^T$ and $\mathcal{L} \times \mathbf{1_N} = \mathbf{0_N}$ [26].

II. Cyber-Physical Islanded AC Microgrids Based on IBRs

A. Primary Control of Islanded AC Microgrids Based on IBRs

In ac microgrids with *N* IBRs, the dynamics of each IBR are modeled in its rotating direct-quadrature reference frame (also known as the *dq*-reference frame). The active and reactive powers delivered to each bus have a nonlinear relation with the output voltage and frequency of the IBR. The droop control technique establishes a linear relationship between the frequency and the active power, as well as between the voltage and the reactive power. This relationship is typically expressed as follows

$$\begin{cases} v_{odi} = v_{ni} - n_i^Q Q_i \\ \omega_i = \omega_{ni} - m_i^P P_i \end{cases} \tag{1}$$

for $i \in \{1, ..., N\}$, where v_{odi} and ω_i are the voltage and frequency of each IBR, respectively, provided for the internal control loops. P_i and Q_i are the active and reactive output powers of the *i*-th IBR, respectively. m_i^P and n_i^Q are the droop coefficients chosen according to the IBR's power rating. ω_{ni} and v_{ni} are the reference values for the primary control prescribed by the secondary control layer.

B. Cooperative Secondary Control of Islanded AC Microgrids Based on IBRs

The droop control mechanism usually results in the deviation of the frequency of IBRs from their nominal reference value. In order to deal with this issue, a secondary control layer is embedded in the hierarchical control structure of islanded microgrids, providing set-points for the primary layer to synchronize the frequency of IBRs with the reference value (ω^{ref}). The secondary control objectives of each IBR are mathematically expressed in (2).

$$\lim_{t\to\infty} \omega_i - \omega^{ref} = 0, \tag{2a}$$

$$\lim_{t\to\infty} m_i^P P_i - m_j^P P_j = 0 \text{ for } i, j \in \{1, ..., N\}. \tag{2b}$$

The objectives expressed in (2) can be achieved by exchanging information among IBRs on a communication network (see Fig. 1). The auxiliary control input for the secondary control layer can be derived from (1), i.e., $\dot{\omega}_i = u_i^\omega$, and then appropriate set-points for the primary layer, i.e., ω_{ni}, are constructed as follows.

$$\omega_{ni} = \int (u_i^\omega + m_i^P \dot{P}_i) d\tau. \tag{3}$$

The conventional cooperative frequency control strategy, based on the data exchange of neighboring IBRs on a strongly connected undirected graph and the reference node, is stated as follows [27].

$$u_i^\omega = -c_\omega \left(\sum_{j \in \mathcal{N}_i} a_{ij}(\omega_{n_i} - \omega_{n_j}) + a_{i0}(\omega_{n_i} - \omega_{n0}) \right) \tag{4}$$

where $\mathcal{N}_i$ is the set of IBRs neighboring *i*-th IBR, a_{ij} and $a_{i0} \in \mathbb{R}_{\geq 0}$ are, respectively, the elements of the Laplacian matrix and the pining gain, $c_\omega \in \mathbb{R}_+$ is a coupling gain and $\omega_{n0} = \omega^{ref} + m_i^P P_i$. While frequency synchronization can be achieved through the use of (4), this article will show that this approach is not resilient against state-dependent FDI cyber-attacks. Therefore, it is required to devise a resilient cooperative secondary frequency control to ensure stability and desired performance in microgrids regardless of the presence of cyber-attacks.

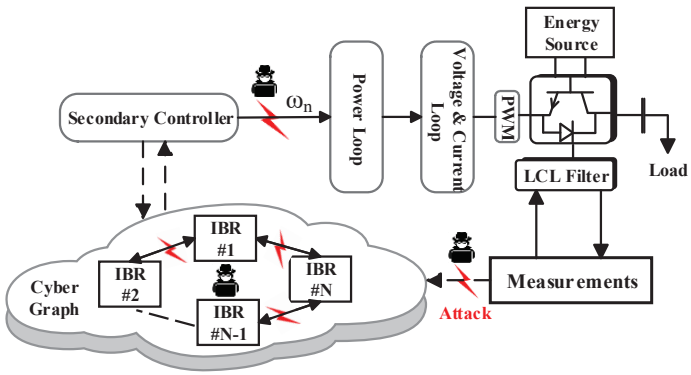


Fig. 1. Diagram of cyber-physical ac microgrids controlled by a secondary control scheme under cyber-attacks manipulating communication channels, control inputs, and sensors.

III. State-Dependent FDI Attack Scenarios and Their Impacts

A. FDI Attack Policy

As distributed control schemes require information exchange amongst IBRs via a communication network infrastructure, microgrids' secondary control system is prone to cyber-attacks. Precisely, a malicious attacker might inject exogenous data to control inputs (actuators), transmitted data, and sensor outputs to make the frequency of microgrids deviate from its reference value [7], [28]. Unlike the existing literature, this paper assumes that all vulnerable locations in microgrids' secondary frequency control systems, i.e., sensors, actuators, reference value, and communication links, are subject to FDI cyber-attacks.

Let δ_i^S, δ_i^0, δ_i^C, and δ_i^a denote the potential state-dependent FDI cyber-attacks applied by the adversary on the *i*-th IBR's sensors, reference value, transmitted data, and actuators, respectively. The cooperative control in (4) in the presence of such FDI attacks can be written as follows.

$$\dot{\omega}_{n_i} = -\sum_{j\in\mathcal{N}_i} c_\omega a_{ij}(\bar{\omega}_{n_i} - \bar{\omega}_{n_j}) + c_\omega a_{i0}(\bar{\omega}_{n_i} - \bar{\omega}_{n0}) + \delta_i^a \quad (5)$$

where $\bar{\omega}_{n_i} = \omega_{n_i} + \delta_i^S$ is a corrupted signal received from *i*-th IBR's sensor, and $\bar{\omega}_{n_j} = \omega_{n_j} + \delta_j^S + \delta_j^C$ is the signal transmitted from its neighbors. Furthermore, the reference frequency ω_0 is subject to FDI attacks, indicated in (5) by $\bar{\omega}_{n0} = \omega^{ref} + \delta_i^0$. The cooperative consensus algorithm (5) can be written in a compact form as

$$\dot{\omega}_n = -c_\omega \left(\mathcal{L}\omega_n + \mathcal{L}\delta^S - \mathcal{A}\delta^C + \bar{\mathcal{G}}\left(\omega_n - \omega_0\right) - \bar{\mathcal{G}}\delta^0\right) + \delta^a \quad (6)$$

where $\omega_n = [\omega_{n1}, ..., \omega_{nN}]^T$, $\delta^S = [\delta_1^S, ..., \delta_N^S]^T$, $\delta^0 = [\delta_1^0, ..., \delta_N^0]^T$ $\delta^C = [\delta_1^C, ..., \delta_N^C]^T$, $\delta^a = [\delta_1^a, ..., \delta_N^a]^T$ and $\omega_0 = [\omega_{10}, ..., \omega_{N0}]^T$. In (6), $\bar{\mathcal{G}} = diag(g_i)$ is the pinning matrix and $g_i \in \mathbb{R}_+$ if the *i*-th IBR has access to the reference frequency ω^{ref}; otherwise, $g_i = 0$. Let us define $\mathcal{G} = \mathcal{L} + \bar{\mathcal{G}}$, then according to undirected graph properties mentioned in Preliminaries, one can reformulate (6) as

$$\dot{\omega}_n = -c_\omega \mathcal{G}(\omega_n + \delta^S - \omega_0 - \delta^0) + c_\omega \mathcal{A}\delta^C + \delta^a. \quad (7)$$

The attacker's policy is to drive the frequency of microgrids to an intolerable value (instability) by the selective design of FDI attack signals δ^a, δ^C, δ^S, and δ^0 in (7) while remaining stealthy to adversary-detection systems. "Stealthy" FDI attacks refer to those made by adversaries whose presence would not be detected by the attack-detector mechanisms employing control inputs and measured data, such as observers and privacy-preserving techniques [29]. This means that the control center might not generate any alerts as a result of data corruption. In the following, strategic FDI attack models are presented.

B. Strategic State-Dependent FDI Attack Models

This article considers sophisticated and stealthy strategic attacks in which the attacker utilizes the frequency of IBRs to destabilize the microgrid. As discussed in the literature, e.g., [21], [30], one can assume that the attacker "*avoids inserting unbounded external signals*" to make the injection undetectable and more invisible to detection mechanisms. This assumption is practical and reasonable as any unbounded injections can be easily identified and rejected by adversary-detection methods. Moreover, in the case of injecting large magnitude false data, any well-designed control scheme can enable each node to remove such large data sent by other neighbors. This article assumes that the malicious attacker has full knowledge of microgrids' controller in (5); thus, it has access to ω_n. Therefore, the attacker properly designs the false data injection δ^a, δ^C, δ^S, and δ^0 in (7) so that the microgrid controlled by (5) becomes unstable. To this end, the following assumption for the dynamics of FDI attacks is considered.

Assumption 1. Any effective state-dependent FDI attacks are assumed to be "*uniformly bounded*" for any bounded ω_n and have the following general dynamics.

$$\begin{cases} \dot{\delta}^a = f_1(\delta^a, \omega_n) \\ \dot{\delta}^C = f_2(\delta^C, \omega_n) \end{cases}, \quad (8)$$

and

$$\begin{cases} \delta^S = \alpha\omega_n \\ \delta^0 = \alpha\omega_0 \end{cases} \quad (9)$$

where f_1 and f_2 are the general functions, with a finite L_2 gain, for attacks on control inputs and transmitted data, respectively, and α is a bounded weight constant used for attacks on sensors and the reference frequency value. Note that the attack dynamics in (8) and (9) are called state-dependent attacks as the dynamics of attack signals depend on the state of microgrids, i.e., ω_n. In Subsection III-C, it will be shown (that) how the attack dynamics in (8) and (9) adversely impact the microgrid stability. The above attack dynamics have been considered in previous studies such as [21] and [31]. Based on the Lyapunov converse theorem [32], for the injections in (8), with equilibrium points δ_e^a, δ_e^C, and ω_{ne}, there exist Lyapunov candidates V_i for $i = \{1, 2\}$ such that

$$\begin{cases} \gamma_{j1}\left\|\delta^j-\delta_e^j\right\|^2 \le V_i \le \gamma_{j2}\left\|\delta^j-\delta_e^j\right\|^2 \\ \frac{\partial V_i}{\partial \delta^j} f_i(\delta^j,\omega_{ne}) \le -\gamma_{j3}\left\|\delta^j-\delta_e^j\right\| \\ \left\|\frac{\partial V_i}{\partial \delta^j}\right\| \le \gamma_{j4}\left\|\delta^j-\delta_e^j\right\| \\ \left\|f_i(\delta^j,\omega_n)-f_i(\delta^j,\omega_{ne})\right\| \le \gamma_{j5}\left\|\omega_n-\omega_{ne}\right\| \\ \left\|f_i(\delta^j,\omega_{ne})-f_i(\delta_e^j,\omega_{ne})\right\| \le \gamma_{j6}\left\|\delta^j-\delta_e^j\right\| \end{cases} \tag{10}$$

where $j \in \{a, C\}$, $\gamma_{jm} \in \mathbb{R}_+$ for $m = 1, ..., 6$, and $\gamma_{j2} \ge \gamma_{j1}$. Note that δ_e^a and δ_e^C are the solutions to the $f_1 = 0$ and $f_2 = 0$ equations, respectively; ω_{ne} is the operating point of the system expressed in (6)—which the attacker aims to change to an unstable one.

Considering the state-dependent attack models in (8) and (9), the cooperative dynamic system in (7) can be rewritten as follows.

$$\dot{\omega}_n = -c_\omega \mathcal{G}(\alpha+1)(\omega_n-\omega_0) + c_\omega \mathcal{A}\delta^C + \delta^a, \tag{11a}$$

$$\dot{\delta}^a = f_1(\delta^a, \omega_n), \text{ and} \tag{11b}$$

$$\dot{\delta}^C = f_2(\delta^C, \omega_n). \tag{11c}$$

Note that, in order to have a feasible injection in sensors and reference signal(s) ω_0, the attacker in (9) should avoid to generating negative signals for the frequency, as any baseline detection mechanisms could easily detect this matter. Thus, any effective attacks on sensors and reference values in the form of (9) should be chosen so that $\alpha > -1$. Taking this assumption avoids constructing negative frequency values; consequently, rejecting by threshold checkers in each node.

C. Attack Impacts

This subsection shows that each potential attack can make the frequency of each IBRs controlled by (6) diverge from the desired reference value ω^{ref}. In this regard, the destabilizing impact of each attack is separately investigated in the absence of other ones.

When sensors and reference value(s) are attacked ($\delta^a = \delta^C = 0$), equation (11a) leads to $\dot{\omega}_n = -c_\omega \mathcal{G}(\alpha+1)(\omega_n-\omega_0)$. Obviously, for any $\alpha < -1$, the frequency of IBRs grows unbounded. In the case of attacks on transmitted data, where $\delta^a = \delta^S = 0$, assume that the state-dependent attack in (8) is chosen as a linear model in form of $\dot{\delta}^C = -\lambda I_N \delta^C + \mathcal{A}^{-1}\mathcal{G}\omega_n$, where λ is a scalar. Note that the inverse of the adjacency matrix only exists under some assumptions for the graph. Assuming the existence of $\mathcal{A}^{-1}$ and $c_\omega = 1$, by merging (8) and (11a), the following state-space model is obtained.

$$\begin{bmatrix}\dot{\omega}_n \\ \dot{\delta}^C\end{bmatrix} = -\begin{bmatrix}\mathcal{G} & -\mathcal{A} \\ -\mathcal{A}^{-1}\mathcal{G} & \lambda I_N\end{bmatrix}\begin{bmatrix}\omega_n \\ \delta^C\end{bmatrix} + \begin{bmatrix}\mathcal{G} \\ 0\end{bmatrix}\omega_0. \tag{12}$$

The characteristic equation of the model in s-domain is

$$\begin{aligned}\det\left(sI_N + \mathcal{G} - \mathcal{A}(s+\lambda)^{-1}\mathcal{A}^{-1}\mathcal{G}\right) \times \det((s+\lambda)I_N) \\ = \det(s^2 I_N + (\mathcal{G}+\lambda I_N)s + (\lambda-1)\mathcal{G}).\end{aligned} \tag{13}$$

For any $\lambda < 1$, the microgrid obviously becomes unstable. The attacker might select the actuator injection model as $\dot{\delta}^a = -\lambda I_N \delta^a + \mathcal{G}\omega_n$ to destabilize the microgrid. The determinantal equation can be obtained similar to the previous case as follows.

$$\begin{aligned}\det\left(sI_N + \mathcal{G} - (s+\lambda)^{-1}\mathcal{G}\right) \times \det((s+\lambda)I_N) \\ = \det(s^2 I_N + (\mathcal{G}+\lambda I_N)s + (\lambda-1)\mathcal{G}).\end{aligned} \tag{14}$$

One can show that this equation also has positive roots for $\lambda < 1$. There are abundant choices of the attack model in (8) that can adversely impact the instability of microgrids. The above illustrative examples highlight the complexity of state-dependent attacks and their adverse impacts on the stability of microgrids. Therefore, it is essential to design a resilient cooperative secondary control system for ac microgrids against possible time-varying and state-dependent FDI attacks, as modeled by (8) and (9).

IV. Resilient Cooperative Frequency Control

A. Control Design

This section aims to develop an attack-resilient cooperative frequency control mechanism that ensures the synchronization of the frequency of IBRs to the nominal operating point ω^{ref}, while IBRs are under state-dependent FDI attacks in (8) and (9). To this end, the conventional secondary controller in (4) is modified by augmenting its dynamics with a virtual layer. Firstly, the dynamics of the virtual layer and its interconnection with the main cooperative dynamics (4) are presented.

The virtual layer in the proposed approach plays the role of an auxiliary control state, and as the name suggests, its virtual states z do not have any physical meaning (virtual nodes). Therefore, this part of the proposed controller can be implemented as internal signal components via the recent advanced cloud-based methods [33]. It is worth mentioning that the main dynamic of the microgrid in (7) is affected by the incorporation of $\beta K z$ as an interaction term. However, as discussed in the following subsection, the introduction of the virtual layer does not change the microgrid's desired performance—provided that the parameter β is chosen to be sufficiently large. Next, the conditions for the interconnection matrices to ensure that the frequency of each IBR is synchronized with the reference frequency are presented. Concerning the model in (4) in the absence of any attacks, this article proposes the following cooperative frequency control and its virtual network; see Fig. 2.

$$\begin{cases}\dot{\omega}_n = -c_\omega \mathcal{G}(\omega_n-\omega_0) + \beta K z \\ \dot{z} = -\mathcal{H} z - \beta M \omega_n + \beta D \omega_0\end{cases} \tag{15}$$

where z and $\mathcal{H}$ are $N \times 1$ state vector and $N \times N$ graph representation matrix of the virtual layer, respectively. This paper assumes that $\mathcal{H}$ is a diagonal matrix whose diagonal elements are positive. As a result, $\mathcal{H} > 0$ and $-\mathcal{H}$ is a Hurwitz matrix. K, M and D are $N \times N$ interconnection matrices and $\beta \in \mathbb{R}_+$ is a control parameter to be designed. The state of the virtual layer, z, might not be observable by the attacker. As a result, this research assumes that the data exchanged in this layer is healthy and unaffected by cyber-attacks. It is noteworthy that the case in which the virtual layer is also subjected to cyber-attacks requires further research and is this study's future work. Since the matrices $-\mathcal{G}$ and $-\mathcal{H}$ are Hurwitz, according to the Lyapunov theory [32], there exist

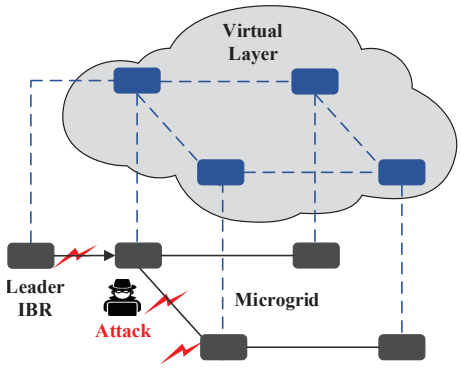


Fig. 2. Resilient control strategy along with the proposed virtual layer—the solid black lines indicate the communication between the leader IBR and the follower IBRs—and the dashed blue lines show the interconnection between the microgrid control system and the proposed virtual layer, as well as the communication lines in the virtual layer.

$N \times N$ symmetric positive definite matrices, such as P_1 and P_2, so that $\mathcal{G}^T P_1 + P_1^T \mathcal{G} > 0$ and $\mathcal{H}^T P_2 + P_2^T \mathcal{H} > 0$. Since the underlined communication graph is assumed to be strongly connected and undirected, $\mathcal{G} > 0$; consequently, P_1 can be chosen to be an identity matrix, i.e., $P_1 = I_N$. Moreover, $\mathcal{H} > 0$, $P_2 = I_N$ can be chosen. Due to this fact, the following essential conditions for the defined matrices in (15) should be satisfied in order to reach frequency synchronization and active power-sharing objectives.

$$\begin{cases} K^T = M \\ D = M \end{cases}. \tag{16}$$

It should be noted that M in (16) has to be an invertible matrix. The reason will be demonstrated in the next subsection. The necessity of conditions in (16) can be figured out by Lyapunov-based stability analysis. To this end, let us define the error term for the frequency reference value, $\bar{\omega}_n = \omega_n - \omega_0$. Then, the dynamics of interconnected system in (15) by replacing $D = M$ (see (16)) can be written as

$$\begin{cases} \dot{\bar{\omega}}_n = -c_\omega \mathcal{G} \bar{\omega}_n + \beta K z \\ \dot{z} = -\mathcal{H} z - \beta M \bar{\omega}_n \end{cases}. \tag{17}$$

Considering a Lyapunov function $V(\bar{\omega}_n, z) = \frac{1}{2}\bar{\omega}_n^T \bar{\omega}_n + \frac{1}{2} z^T z$, and taking its time derivative along with the closed-loop dynamics in (17), one can obtain

$$\begin{aligned} \dot{V} &= \frac{1}{2}\dot{\bar{\omega}}_n{}^T \bar{\omega}_n + \frac{1}{2}\bar{\omega}_n^T \dot{\bar{\omega}}_n + \frac{1}{2}\dot{z}^T z + \frac{1}{2} z^T \dot{z} \\ &= -\frac{1}{2} c_\omega \bar{\omega}_n^T (\mathcal{G}^T + \mathcal{G}) \bar{\omega}_n - \frac{1}{2} z^T (\mathcal{H}^T + \mathcal{H}) z \\ &\quad + \beta z^T (K^T - M) \bar{\omega}_n. \end{aligned} \tag{18}$$

Therefore, by applying the condition for the interconnection matrices, one can obtain that $\dot{V} = -c_\omega \bar{\omega}_n^T \mathcal{G} \bar{\omega}_n - z^T \mathcal{H} z < 0$. Thus, the origin of the system in (17) is globally asymptotically stable. As a result, $\omega_n \longrightarrow \omega_0$ at the steady-state. The above stability analysis demonstrates that in the absence of FDI cyber-attacks, the proposed cooperative secondary controller in (15) ensures synchronization to the reference point ω_0. In the following, the stability of the proposed cooperative secondary system in (15) in the presence of state-dependent FDI attack dynamics in (8) and (9) is analyzed.

B. Stability Analysis

According to the results from the previous subsection, the overall dynamic model for the proposed secondary frequency controller in (15) with state-dependent FDI attacks is as follows.

$$\begin{cases} \dot{\omega}_n = -c_\omega \mathcal{G}(\alpha+1)(\omega_n - \omega_0) + c_\omega \mathcal{A}\delta^C + \delta^a + \beta K z \\ \dot{z} = -\mathcal{H} z - \beta(\alpha+1) M(\omega_n - \omega_0) \\ \dot{\delta}^a = f_1(\delta^a, \omega_n) \\ \dot{\delta}^C = f_2(\delta^C, \omega_n) \end{cases}. \tag{19}$$

The following theorem demonstrates that the proposed control mechanism in (15) guarantees the stability of the microgrid and the frequency synchronization of IBRs to the reference frequency in the presence of state-dependent FDI cyber-attacks modeled in (8) and (9). In more detail, this paper will show that even if all IBRs are under attack, the attack-resilience performance in microgrids is achieved by choosing a sufficiently large value of β.

Theorem 1. *Consider the proposed cooperative control scheme in* (19)*. The frequency synchronization and the active power-sharing of ac microgrids in the presence of cyber-attacks satisfying Assumption 1 can be achieved if β is selected to be sufficiently large. In other words, if $\epsilon \in \mathbb{R}_+$ is defined as a sufficiently small scalar, it can be mathematically shown that*

$$\lim_{t\to\infty} \omega_n(t) - \omega_0 = \underbrace{\frac{(c_\omega \mathcal{G} + \beta^2 K \mathcal{H}^{-1} M)^{-1}(c_\omega \mathcal{A}\delta_e^C + \delta_e^a)}{(\alpha+1)}}_{\approx \epsilon}. \tag{20}$$

Proof. First, using the error term $\bar{\omega}_n = \omega_n - \omega_0$ and defining $\bar{\delta}^C = \delta^C - \delta_e^C$ and $\bar{\delta}^a = \delta^a - \delta_e^a$, the system dynamics in (19) can be re-framed as

$$\begin{cases} \dot{\bar{\omega}}_n = -c_\omega(\alpha+1)\mathcal{G}\bar{\omega}_n + \beta K z + \mathcal{A}\bar{\delta}^C + \bar{\delta}^a \\ \dot{z} = -\mathcal{H} z - \beta(\alpha+1) M \bar{\omega}_n \\ \dot{\bar{\delta}}^a = f_1(\bar{\delta}^a, \bar{\omega}_n) \\ \dot{\bar{\delta}}^C = f_2(\bar{\delta}^C, \bar{\omega}_n) \end{cases}. \tag{21}$$

Next, in order to prove the asymptotic stability of (21), the following Lyapunov function is considered.

$$\begin{aligned} V &= \beta(\alpha+1)\bar{\omega}_n^T \bar{\omega}_n + \beta z^T z + 2 c_\omega z^T (M^{-T}\mathcal{A})\bar{\delta}^C \\ &\quad + 2 z^T (M^{-T})\bar{\delta}^a + V_1 + V_2 \end{aligned} \tag{22}$$

where V_1 and V_2 are the Lyapunov candidates given in (10). Obviously, $V > 0$ for all large values of β. Taking the derivation of (22) with respect to time and substituting (21), one can obtain

$$\begin{aligned}\dot{V} = &-c_\omega\sigma(\alpha+1)\bar{\omega}_n^T\mathcal{G}^T\bar{\omega}_n + \beta\sigma z^T K^T\bar{\omega}_n + c_\omega\sigma\bar{\delta}^{C^T}\mathcal{A}^T\bar{\omega}_n \\ &+ \sigma\bar{\delta}^{a^T}\bar{\omega}_n - c_\omega\sigma(\alpha+1)\bar{\omega}_n^T\mathcal{G}\bar{\omega}_n + \beta\sigma\bar{\omega}_n^T Kz \\ &+ c_\omega\sigma\bar{\omega}_n^T\mathcal{A}\bar{\delta}^C + \sigma\bar{\omega}_n^T\bar{\delta}^a - \beta z^T\mathcal{H}^T z - \beta\sigma\bar{\omega}_n^T M^T z \\ &- \beta z^T\mathcal{H}z - \beta\sigma z^T M\bar{\omega}_n - 2c_\omega z^T\psi\bar{\delta}^C - 2z^T\phi\ \bar{\delta}^a \\ &- 2\sigma\bar{\omega}_n^T M^T(M^{-T})\bar{\delta}^a - 2c_\omega\sigma\omega_n^T M^T(M^{-T}\mathcal{A})\bar{\delta}^C \\ &+ 2c_\omega z^T(M^{-T}\mathcal{A})\left(f_2(\delta^C,\omega_n) - f_2(\delta_e^C,\omega_{ne})\right) \\ &+ 2z^T(M^{-T})\left(f_1(\delta^a,\omega_n) - f_1(\delta_e^a,\omega_{ne})\right) + \dot{V}_1 + \dot{V}_2.\end{aligned} \tag{23}$$

Next, adding and subtracting $f_1(\delta^a,\omega_{ne})$ and $f_2(\delta^C,\omega_{ne})$ to and from (23) yield (24).

$$\begin{aligned}\dot{V} = &-c_\omega\sigma(\alpha+1)\bar{\omega}_n^T\mathcal{G}^T\bar{\omega}_n + \beta\sigma z^T K^T\bar{\omega}_n \\ &+ c_\omega\sigma\bar{\delta}^{C^T}\mathcal{A}^T\bar{\omega}_n + \sigma\bar{\delta}^{a^T}\bar{\omega}_n - c_\omega\sigma(\alpha+1)\bar{\omega}_n^T\mathcal{G}\bar{\omega}_n \\ &+ \beta\sigma\bar{\omega}_n^T Kz + c_\omega\sigma\bar{\omega}_n^T\mathcal{A}\bar{\delta}^C + \sigma\bar{\omega}_n^T\bar{\delta}^a - \beta z^T\mathcal{H}^T z \\ &- \beta\sigma\bar{\omega}_n^T M^T z - \beta z^T\mathcal{H}z - \beta\sigma z^T M\bar{\omega}_n - 2c_\omega z^T\psi\bar{\delta}^C \\ &- 2c_\omega\sigma\omega_n^T\mathcal{A}\bar{\delta}^C - 2z^T\phi\bar{\delta}^a - 2\sigma\bar{\omega}_n^T\bar{\delta}^a \\ &+ 2c_\omega z^T(M^{-T}\mathcal{A})\left(f_2(\delta^C,\omega_{ne}) - f_2(\delta_e^C,\omega_{ne})\right) \\ &+ 2c_\omega z^T(M^{-T}\mathcal{A})\left(f_2(\delta^C,\omega_n) - f_2(\delta^C,\omega_{ne})\right) \\ &+ 2z^T(M^{-T})\left(f_1(\delta^a,\omega_{ne}) - f_1(\delta_e^a,\omega_{ne})\right) \\ &+ 2z^T(M^{-T})\left(f_1(\delta^a,\omega_{ne}) - f_1(\delta_e^a,\omega_{ne})\right) + \dot{V}_1 + \dot{V}_2\end{aligned} \tag{24}$$

where $\sigma = \beta(\alpha+1)$, $\phi = \mathcal{H}^T M^{-T}$ and $\psi = \mathcal{H}^T M^{-T}\mathcal{A}$. Recalling (16) and (10), one can come up with the following inequality.

$$\begin{aligned}\dot{V} \le &-c_\omega\sigma(\alpha+1)\bar{\omega}_n^T\left(\mathcal{G}^T+\mathcal{G}\right)\bar{\omega}_n \\ &- \beta z^T\left(\mathcal{H}^T+H\right)z - \gamma_{C3}\left\|\delta^C\right\|^2 - \gamma_{a3}\|\delta^a\|^2 \\ &+ \gamma_{C4}\gamma_{C5}\left\|\bar{\delta}^C\right\|\|\bar{\omega}_n\| + \gamma_{a4}\gamma_{a5}\left\|\bar{\delta}^a\right\|\|\bar{\omega}_n\| \\ &- 2c_\omega(1-\gamma_{C6})\|z\|\|\psi\|\left\|\bar{\delta}^C\right\| - 2(1-\gamma_{a6})\|z\|\|\phi\|\left\|\bar{\delta}^a\right\| \\ &+ 2c_\omega\gamma_{C5}\|z\|\|\psi\|\|\bar{\omega}_n\| + 2\gamma_{a5}\|z\|\|\phi\|\|\bar{\omega}_n\|.\end{aligned} \tag{25}$$

As one can observe, the quadratic terms are negative with respect to $\bar{\omega}_n$ and z. Since other terms in (25) are independent of β, $\dot{V}$ is negative-definite for all sufficiently large values of β. Therefore, the error system in (21) is asymptotically stable; equivalently, $\bar{\omega}_n$ converges to zero at the steady-state for large values of β. Given the asymptotic stability, $\dot{\omega}_n$ and $\dot{z}$ in (19) are zero at the steady-state, and as a result, the ultimate bound in (20) can be obtained. This matter means the secondary control objectives of the theorem, i.e., frequency synchronization and proportional active power-sharing, are achieved regardless of the presence of the state-dependent FDI cyber-attacks. This statement completes the proof. □

V. Case Study

A. Simulation Results

This section tests the performance of the proposed control scheme on an islanded multi-IBRs microgrid shown in Fig. 3. The simulations, conducted in the MATLAB/Simulink software environment, are carried out for several scenarios and verify the effectiveness of the proposed control mechanism. The parameters of the microgrid and the primary controllers are given in Table I. The microgrid's nominal frequency and line-to-line rms voltage references are set to 60 Hz and 208 V, respectively. The converters in the test microgrid are non-ideal, and the switching frequency is chosen as $f_{sw} = 8.1\ kHz$. The IBRs can exchange the information through a neighbor-by-neighbor communication topology as shown in Fig. 3. The proposed controller in the secondary levels is applied to the Fig. 3 control system. For this simulation, the control matrices of the main layer and virtual layer presented in (19) are set to be $\mathcal{H} = 20I_n$, $M = [-2\ 1\ 0\ 0; 1\ -2\ 0\ 1; 0\ 0\ -2\ 0; 0\ 1\ 0\ -2]$, $K = M^T$ and $D = M$.

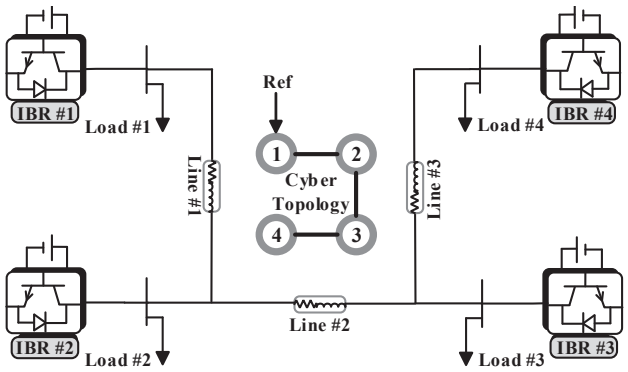


Fig. 3. Single line diagram of the islanded microgrid under study and the cyber (communication) topology used in the secondary control layer.

TABLE I
Parameters of the Microgrid under Test in Section V.

Description	Value
$\mathbf{m^P}$	9.4×10^{-6}
$\mathbf{n^Q}$	1.3×10^{-4}
$\mathbf{K_{PV}}$	0.1
$\mathbf{K_{IV}}$	420
$\mathbf{K_{PC}}$	15
$\mathbf{K_{IC}}$	20000
LCL Filters	$R_f = 0.05\,\Omega, L_f = 1.5\,\text{mH}, C_f = 50\,\mu F$ $R_c = 0.1\,\Omega, L_c = 1.35\text{mH}$ $R_g = 0.03\,\Omega, L_g = 0.35\text{mH}$
Lines	$R_{12} = 0.8\,\Omega, L_{12} = 3.6\,\text{mH}, R_{23} = 0.4\,\Omega$ $L_{23} = 1.8\ \text{mH},\ R_{34} = 0.03\,\Omega, L_{34} = 0.35\text{mH}$

Two attack scenarios are considered in order to evaluate the performance of the microgrid controlled by the proposed distributed secondary control strategy under state-dependent FDI attacks. *Case I* presents the results for linear dynamics FDI attacks—and *Case II* is dedicated to assessing the performance of the microgrid, augmented with the proposed control strategy, in the presence of nonlinear dynamic state-dependent attacks. In each case, the simulation results of the conventional distributed secondary control approach in the absence of a virtual layer under the same attack scenario are provided. The results illustrate the inadequacy of the conventional distributed secondary control method against such attacks.

Case I: This case study considers attacks with linear dynamics

on IBRs based on *Assumption 1*; the attacker uses the frequency of the microgrid and generates "*bounded*" malicious injections. The attack signals are chosen as $\dot{\delta}^C = A\omega_n - B\delta^C$, $\dot{\delta}^a = A\omega_n - B\delta^a$, $\delta^S = 0.2\omega_n$ and $\delta^0 = 0.2\omega_0$, where $A = [-1\ 0\ -4\ -2; 5\ 2\ -1\ -3; 2\ -2\ 0\ -2; 0\ -1\ 2\ -3]$ and $B = 25I_4$. The control parameters are $\beta = 550$ and $c_\omega = 10$. Note that the attacks are launched at $t = 2$ s and ended at $t = 4$ s, the load in IBR #2 is suddenly increased (1.55 kW) at $t = 6$ s and is then decreased to its initial value at $t = 8$ s. The simulation results for the frequency of the microgrid, active power capability, voltage, and reactive power of IBRs are shown in Fig. 4. By deploying the proposed control schemes, the microgrid's frequency indeed remains within the allowable frequency bound—and active power is equally shared regardless of the presence of FDI cyber-attacks. As one can observe from Fig. 5, before launching attacks, the conventional distributed secondary control approach regulates the frequency of IBRs to its prescribed value; in addition, the active power is equally generated by each IBR. However, after the cyber-attack invasion, the frequency synchronization and equal active power-sharing are destroyed.

Case II: This case study considers the malicious attacker choosing more general dynamics than the previous case to generate malicious injections. The microgrid augmented with the proposed resilient cooperative distributed frequency control in (19) is subject to state-dependent FDI attacks with the dynamics $\dot{\delta}^C = 5sin(\omega_n + \delta^C)$, $\dot{\delta}^a = 5sin(\omega_n + \delta^a)$, $\delta^S = 1.5\omega_n$ and $\delta^0 = 1.5\omega_0$. The control parameters of this attack scenario are chosen to be the same as *Case I*. The performance of the proposed control strategy is also evaluated in terms of load changes similar to the previous case. The results of this attack scenario for the proposed control scheme and the conventional approach are indicated in Fig. 6 and Fig. 7, respectively. As a result of attacks at $t = 2$ s, the conventional controller in (4) cannot maintain the frequency and equal active power-sharing among IBRs—while the proposed resilient cooperative secondary control strategy mitigates the adverse effects of the malicious injections.

B. Experimental Results

The test rig depicted in Fig. 8 is utilized to conduct experimental examinations related to the VSC simulated in this section. It is built by SEMIKRON intelligent power modules using insulated gate bipolar transistors (IGBTs) (based on "SKM 50 GB 123 D" modules). Besides, SEMIKRON "SKHI 21A (R)" gate drives and protection circuitry are employed to make the converter functional. Verivolt "IsoBlock I-ST-1c"/"IsoBlock V-1c" current/voltage sensors are hooked to digital inputs to measure the currents and the voltages, respectively. dSPACE "MicroLabBox (MLBX)" using a real-time processor, field-programmable gate arrays, and different inputs/outputs channels connects the VSC under test to the measurement and drive circuitry. Furthermore, all the parameters of the setup deployed are similar to those of simulations and are reported in Table I. Therefore, the comparison between simulation and experimental results is feasible. In this regard, Figs. 9–12 replicate simulations

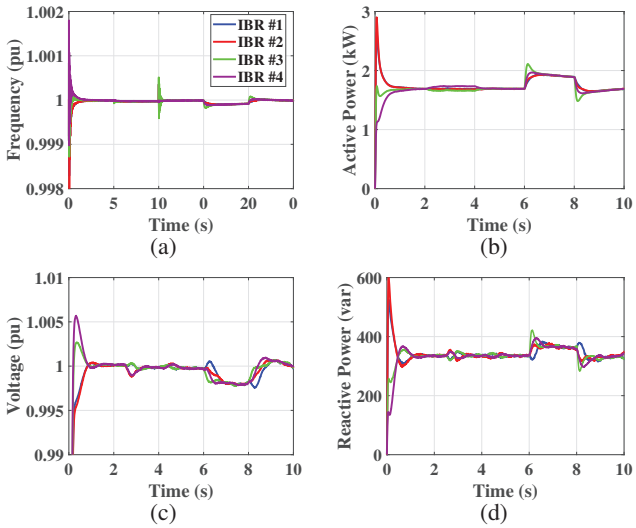


Fig. 4. Performance of the proposed resilient distributed secondary control scheme for *Case I*: (a) frequency, (b) active power, (c) voltage, and (d) reactive power of IBRs.

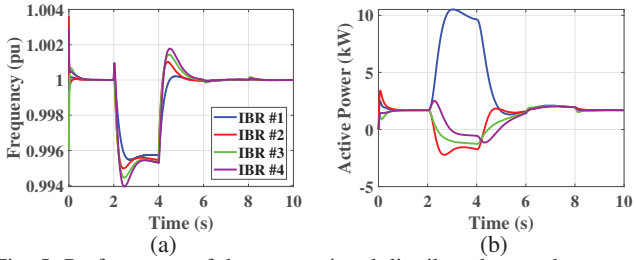


Fig. 5. Performance of the conventional distributed secondary control algorithm for *Case I*: (a) frequency and (b) active power of IBRs.

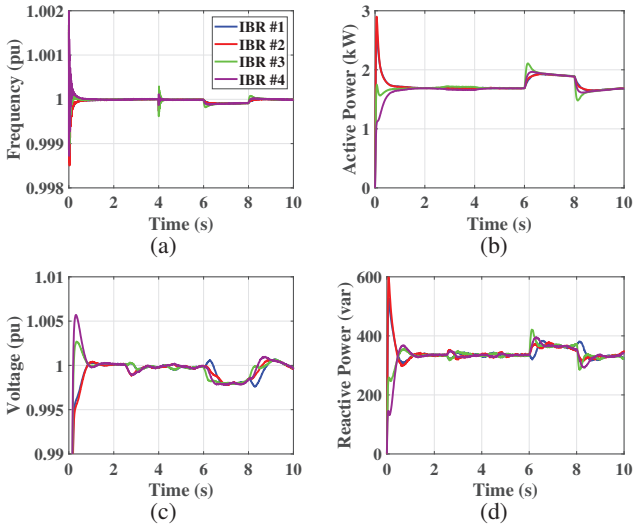
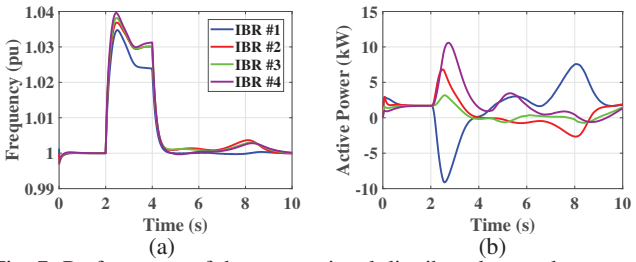


Fig. 6. Performance of the proposed resilient distributed secondary control scheme for *Case II*: (a) frequency, (b) active power, (c) voltage, and (d) reactive powers of IBRs.

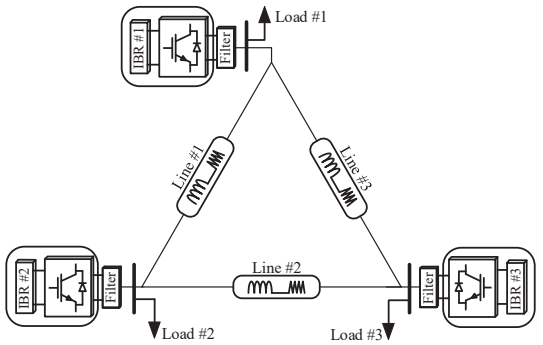
associated with Case I and Case II for the 3-IBR version of the microgrid in displayed Fig. 3—according to the available facilities—thereby revealing the effectiveness of the proposed control methodology.

This article has been accepted for publication in IEEE Transactions on Industrial Electronics. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIE.2023.3281698

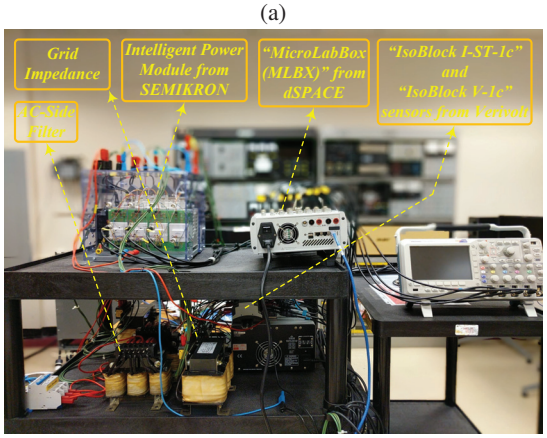


(a) (b)

Fig. 7. Performance of the conventional distributed secondary control algorithm for *Case II*: (a) frequency and (b) active power of IBRs.



(a)

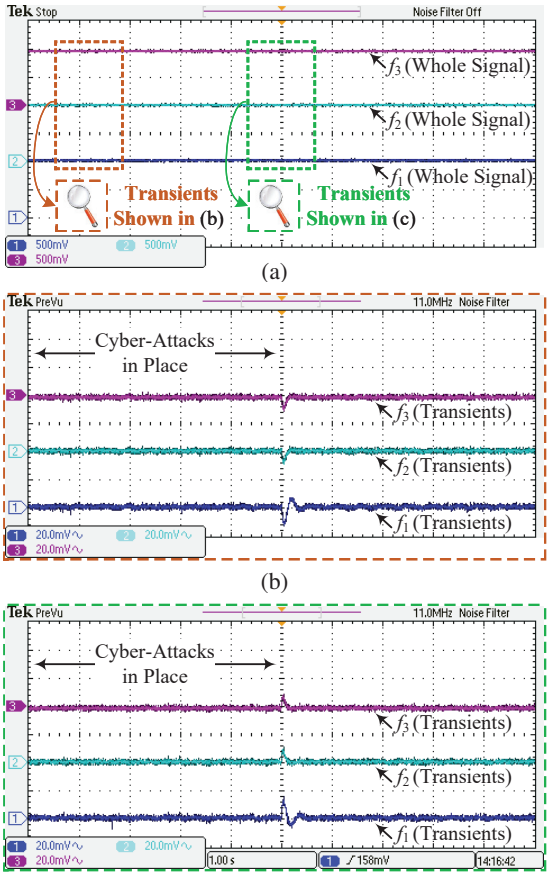


(b)

Fig. 8. Test rig deployed to carry out experiments: (a) the microgrid under test and (b) details of one IBR—housed in the Laboratory for Advanced Power and Energy Systems (LAPES) at Georgia Southern University—where experiments have been conducted.

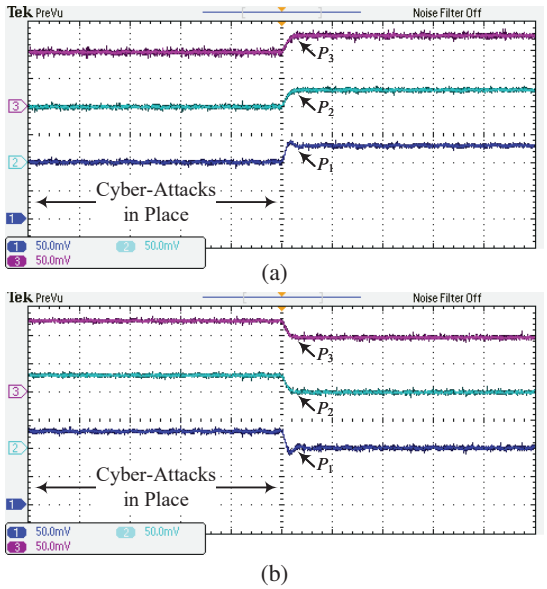
C. Discussion on Simulations and Experimental Results

As evident in the results presented in this section, when the microgrid is equipped with the proposed resilient secondary control scheme, the steady-state errors of frequencies (between the actual and the reference value) are less than %0.2—which is within the permissible boundary. Also, the error in active power sharing caused by the FDI attack is approximately around %1.5—which is negligible compared to the output active power scale of each IBR. Although this paper considers no specific resilient secondary voltage control mechanism, results demonstrate that in a safe circumstance with no attacks on voltage control channels, the voltages of IBRs become pretty synchronized; in this regard, the regulation error is below %0.5 as well.



(a) (b) (c)

Fig. 9. Experimental results of *Case I* (with the 1 s/div horizontal axis) (a) the whole frequency signal 30 Hz/div, (b) transients (ac component) indicated in Fig. 9(a) with 0.012 Hz/div when the attack is launched, and transients (ac component) shown in Fig. 9(a) with 0.012 Hz/div when the load change occurs.



(a) (b)

Fig. 10. Experimental results of *Case I* (with the 1 s/div horizontal axis) (a) load increase with 540 W/div and (b) load decrease with 540 W/div.

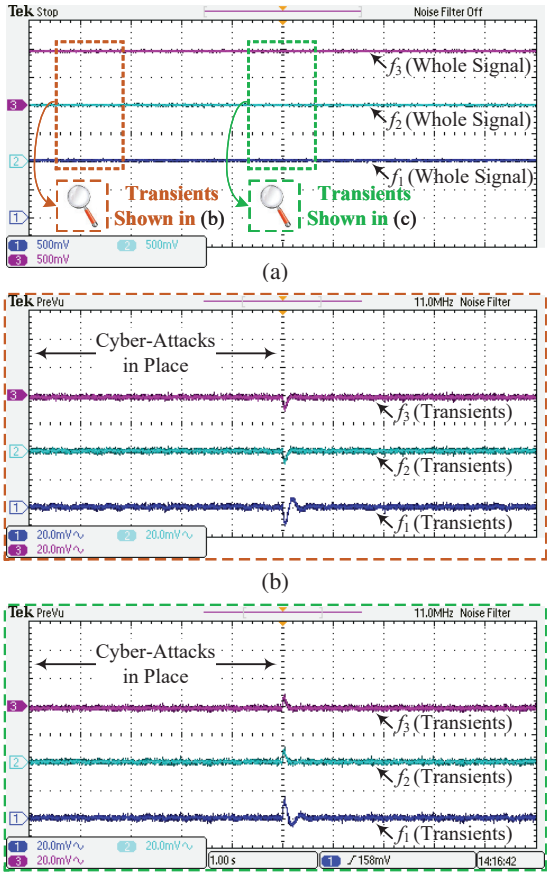


Fig. 11. Experimental results of *Case II* (with the 1 s/div horizontal axis) (a) the whole frequency signal 30 Hz/div, (b) transients (ac component) indicated in Fig. 11(a) with 0.012 Hz/div when the attack is launched, and transients (ac component) shown in Fig. 11(a) with 0.012 Hz/div when the load change occurs.

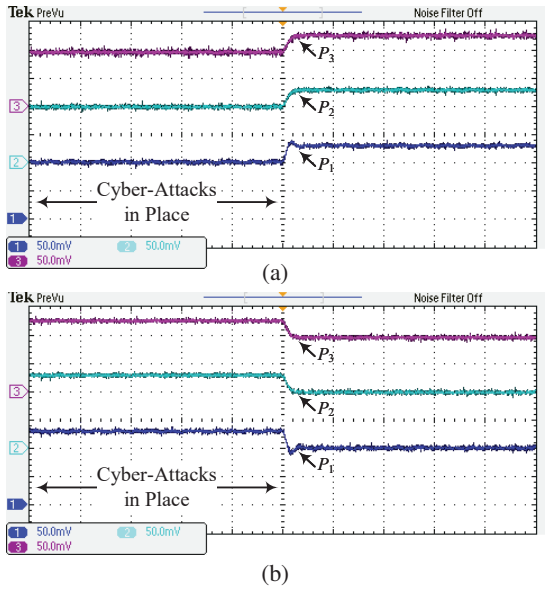


Fig. 12. Experimental results of *Case II* (with the 1 s/div horizontal axis) (a) load increase with 540 W/div and (b) load decrease with 540 W/div.

VI. Conclusion

The distributed control systems in islanded ac microgrids are vulnerable to potential cyber threats. This paper has proposed a resilient cooperative frequency control framework for ac microgrids in the presence of state-dependent false data injection cyber-attacks aiming to destabilize microgrids. Using the concept of virtual layers, the proposed controller has guaranteed frequency synchronization and proportional active power-sharing while all distributed generation units have been attacked. Also, the attacker might manipulate data exchange, transmitted data, control inputs, sensors, and reference frequency. Rigorous Lyapunov-based stability analysis and the design considerations of control matrices have also been presented. The performance and effectiveness of the proposed control strategy have been evaluated by MATLAB/Simulink simulations and experimental results.

References

[1] A. J. Abianeh, M. M. Mardani, F. Ferdowsi, R. Gottumukkala, and T. Dragicevic, "Cyber-resilient sliding mode consensus secondary control scheme for islanded ac microgrids," *IEEE Transactions on Power Electronics*, vol. 37, no. 5, pp. 6074–6089, 2021.

[2] Y. Khayat, Q. Shafiee, R. Heydari, M. Naderi, T. Dragičević, J. W. Simpson-Porco, F. Dörfler, M. Fathi, F. Blaabjerg, J. M. Guerrero *et al.*, "On the secondary control architectures of ac microgrids: An overview," *IEEE Transactions on Power Electronics*, vol. 35, no. 6, pp. 6482–6500, 2019.

[3] O. Qasem, M. Davari, W. Gao, D. R. Kirk, and T. Chai, "Hybrid iteration ADP algorithm to solve cooperative, optimal output regulation problem for continuous-time, linear, multi-agent systems: Theory and application in islanded modern microgrids with IBRs," *IEEE Transactions on Industrial Electronics*, early access, Feb. 28, 2023, doi: 10.1109/TIE.2023.3247734.

[4] A. Gusrialdi, Y. Xu, Z. Qu, and M. A. Simaan, "Resilient cooperative voltage control for distribution network with high penetration distributed energy resources," in *Proceedings of European Control Conference (ECC)*. IEEE, 2020, pp. 1533–1539.

[5] R. Alguliyev, Y. Imamverdiyev, and L. Sukhostat, "Cyber-physical systems and their security issues," *Computers in Industry*, vol. 100, pp. 212–223, 2018.

[6] L. K. Carvalho, Y.-C. Wu, R. Kwong, and S. Lafortune, "Detection and mitigation of classes of attacks in supervisory control systems," *Automatica*, vol. 97, pp. 121–133, 2018.

[7] S. Abhinav, H. Modares, F. L. Lewis, F. Ferrese, and A. Davoudi, "Synchrony in networked microgrids under attacks," *IEEE Transactions on Smart Grid*, vol. 9, no. 6, pp. 6731–6741, 2017.

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

[9] A. S. Mohamed, M. F. M. Arani, A. A. Jahromi, and D. Kundur, "False data injection attacks against synchronization systems in microgrids," *IEEE Transactions on Smart Grid*, vol. 12, no. 5, pp. 4471–4483, 2021.

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

[11] H. Modares, B. Kiumarsi, F. L. Lewis, F. Ferrese, and A. Davoudi, "Resilient and robust synchronization of multiagent systems under attacks on sensors and actuators," *IEEE Transactions on Cybernetics*, vol. 50, no. 3, pp. 1240–1250, 2019.

[12] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1630–1638, 2016.

[13] Z.-H. Pang, L.-Z. Fan, J. Sun, K. Liu, and G.-P. Liu, "Detection of stealthy false data injection attacks against networked control systems via active data modification," *Information Sciences*, vol. 546, pp. 192–205, 2021.

[14] Z.-H. Pang, L.-Z. Fan, Z. Dong, Q.-L. Han, and G.-P. Liu, "False data injection attacks against partial sensor measurements of networked control systems," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 69, no. 1, pp. 149–153, 2021.

[15] M. Davari, M. P. Aghababa, F. Blaabjerg, and M. Saif, "An innovative, adaptive faulty signal rectifier along with a switching controller for reliable primary control of gc-vsis in cps-based modernized microgrids," *IEEE Transactions on Power Electronics*, vol. 36, no. 7, pp. 8370–8387, 2020.

[16] M. Davari, H. Nafisi, M.-A. Nasr, and F. Blaabjerg, "A novel igdt-based method to find the most susceptible points of cyberattack impacting operating costs of vsc-based microgrids," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 9, no. 3, pp. 3695–3714, 2020.

[17] S. Sahoo, Y. Yang, and F. Blaabjerg, "Resilient synchronization strategy for ac microgrids under cyber attacks," *IEEE Transactions on Power Electronics*, vol. 36, no. 1, pp. 73–77, 2020.

[18] A. Mustafa, B. Poudel, A. Bidram, and H. Modares, "Detection and mitigation of data manipulation attacks in ac microgrids," *IEEE Transactions on Smart Grid*, vol. 11, no. 3, pp. 2588–2603, 2019.

[19] M. Raeispour, H. Atrianfar, M. Davari, and G. B. Gharehpetian, "Fault-tolerant, distributed control for emerging, vsc-based, islanded microgrids—an approach based on simultaneous passive fault detection," *IEEE Access*, vol. 10, pp. 10 995–11 010, 2021.

[20] A. Bidram, B. Poudel, L. Damodaran, R. Fierro, and J. M. Guerrero, "Resilient and cybersecure distributed control of inverter-based islanded microgrids," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 3881–3894, 2019.

[21] A. Gusrialdi, Z. Qu, and M. A. Simaan, "Competitive interaction design of cooperative systems against attacks," *IEEE Transactions on Automatic Control*, vol. 63, no. 9, pp. 3159–3166, 2018.

[22] S. Zuo, O. A. Beg, F. L. Lewis, and A. Davoudi, "Resilient networked ac microgrids under unbounded cyber attacks," *IEEE Transactions on Smart Grid*, vol. 11, no. 5, pp. 3785–3794, 2020.

[23] Y. Chen, D. Qi, H. Dong, C. Li, Z. Li, and J. Zhang, "A fdi attack-resilient distributed secondary control strategy for islanded microgrids," *IEEE Transactions on Smart Grid*, vol. 12, no. 3, pp. 1929–1938, 2020.

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

[25] M. S. Sadabadi, S. Sahoo, and F. Blaabjerg, "A fully resilient cyber-secure synchronization strategy for ac microgrids," *IEEE Transactions on Power Electronics*, vol. 36, no. 12, pp. 13 372–13 378, 2021.

[26] F. Bullo, *Lectures on network systems*, 1st ed. Available: http://motion.me.ucsb.edu/book-lns: Seattle, WC, USA: Kindle Direct Publishing. [Online], 2020.

[27] A. Bidram, A. Davoudi, F. L. Lewis, and J. M. Guerrero, "Distributed cooperative secondary control of microgrids using feedback linearization," *IEEE Transactions on Power Systems*, vol. 28, no. 3, pp. 3462–3470, 2013.

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

[29] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "Revealing stealthy attacks in control systems," in *Proceedings of the 50th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*. IEEE, 2012, pp. 1806–1813.

[30] A. Gusrialdi, Z. Qu, and M. A. Simaan, "Robust design of cooperative systems against attacks," in *Proceedings of American Control Conference*. IEEE, 2014, pp. 1456–1462.

[31] T. Yucelen, W. M. Haddad, and E. M. Feron, "Adaptive control architectures for mitigating sensor attacks in cyber-physical systems," *Cyber-Physical Systems*, vol. 2, no. 1-4, pp. 24–52, 2016.

[32] H. K. Khalil, *Nonlinear systems*. 3rd ed. London, U.K.: Prentice-Hall, 2002.

[33] D. Gebbran, A. Barragán-Moreno, P. I. Gómez, R. K. Subroto, M. M. Mardani, M. López, J. Quiroz, and T. Dragičević, "Cloud and edge computing for smart management of power electronic converter fleets: A key connective fabric to enable the green transition," *IEEE Industrial Electronics Magazine*, early access, Oct. 18, 2022, doi: 10.1109/MIE.2022.3211125.

Mahmood Jamali received the B.Sc. degree in Control-Electrical Engineering from the Ferdowsi University of Mashhad, Mashhad, Iran, in 2017, and the M.Sc. degree in Control Engineering from the Amirkabir University of Technology (Tehran Polytechnic), Tehran, Iran, in 2020, respectively. He is currently pursuing the Ph.D. degree in Automatic Control and System Engineering with the University of Sheffield, United Kingdom. His research interests include control, cyber-security and stability of modern power systems.

Mahdieh S. Sadabadi (Senior Member, IEEE) is currently an Assistant Professor in the School of Electronic Engineering and Computer Science at the Queen Mary University of London (QMUL), London, United Kingdom. Prior to joining QMUL, she was an Assistant Professor in the Department of Automatic Control and Systems Engineering (ACSE), University of Sheffield, United Kingdom. She was a Postdoctoral Research Associate in the Department of Engineering, University of Cambridge, and a Postdoctoral Fellow in the Division of Automatic Control in the Department of Electrical Engineering, Linkoping University in Sweden. She received her Ph.D. in Control Systems from Automatic Control Laboratory, Swiss Federal Institute of Technology in Lausanne (EPFL), Switzerland in February 2016. Her research interests are generally centered on fundamental theoretical and applied research on robust, resilient, secure, and scalable control strategies for cyber-physical systems under uncertainty. Her research is inspired by control and resilience challenges involved in the integration and interconnection of power electronics converters into future power networks.

Masoud Davari (Senior Member, IEEE) was born in Isfahan, Iran, on September 14, 1985. He received the B.Sc. degree (summa cum laude) in electrical engineering (power) from the Isfahan University of Technology, Isfahan, in 2007, the M.Sc. degree (summa cum laude) in electrical engineering (power) from the Amirkabir University of Technology (Tehran Polytechnic), Tehran, Iran, in 2010, and the Ph.D. degree in electrical engineering (power electronics in energy systems with distinction/honors) from the University of Alberta, Edmonton, AB, Canada, in 2016.

He was with Iran's Grid Secure Operation Research Center and Iran's Electric Power Research Institute (EPRI), Tehran, Iran, from January 2010 to December 2011. From April 2015 to June 2017, he was a Senior R & D Specialist and Senior Consultant with Quanta-Technology Company, Markham, ON, Canada, in the field of the dynamic interaction of renewables with smart ac/dc grids and control, protection, and automation of microgrids. In July 2017, he joined as a tenure-track Assistant Professor with the Allen E. Paulson College of Engineering and Computing, Department of Electrical and Computer Engineering, Georgia Southern University (GSU), Statesboro, GA, USA—where he was recommended for being granted "*early*" promotion to Associate Professor and award of "*early*" tenure on December 3, 2021, and officially approved for both on February 16, 2022. He is the founder and the director of the Laboratory for Advanced Power and Energy Systems [LAPES (watch it on https://www.youtube.com/watch?v=mhVHp7uMNKo)] in the state-of-the-art Center for Engineering and Research (CEaR) established in 2021 with GSU. He has developed and implemented several experimental test rigs for research universities and the power and energy industry. He has also authored several papers published in IEEE Transactions and journals. His research interests include the dynamics, controls, and protections of different power electronic converters utilized in the hybrid ac/dc smart grids, and hardware-in-the-loop (HIL) simulation-based testing of modernized power systems.

Dr. Davari has been an active member and a chapter lead in the IEEE Power & Energy Society Task Force on "*Innovative Teaching Methods for Modern Power and Energy Systems*" since July 2020. He has been an active member and a chapter lead (for Chapter 3) in the IEEE Working Group P2004—a newly established IEEE working group entitled "*Hardware-in-the-Loop (HIL) Simulation Based Testing of Electric Power Apparatus and Controls*" for IEEE Standards Association since June 2017. He is an invited member of the Golden Key International Honour Society. He was the Chair of the Literature Review Subgroup of DC@Home Standards for the IEEE Standards Association from April 2014 to October 2015. He is an invited reviewer of several of the IEEE TRANSACTIONS/JOURNALS, IET journals, *Energies* journal, and various IEEE conferences, the invited speaker at different universities and in diverse societies, and the Best Reviewer of the IEEE TRANSACTIONS ON POWER SYSTEMS in 2018 and 2020. He is the recipient of the 2019–2020 Allen E. Paulson College of Engineering and Computing (CEC) Faculty Award for Outstanding Scholarly Activity in the Allen E. Paulson CEC at GSU, the Discovery & Innovation Award from the 2020–2021 University Awards of Excellence at GSU, and one of the awardees of the 2021–2022 Impact Area Accelerator Grants (partially funded) at GSU.

Subham Sahoo (Senior Member, IEEE) received the B.Tech. & Ph.D. degree in Electrical and Electronics Engineering from VSSUT, Burla, India and Electrical Engineering at Indian Institute of Technology, Delhi, New Delhi, India in 2014 & 2018, respectively. He is currently an Assistant Professor in the Department of Energy, Aalborg University (AAU), Denmark, where he is also the vice-leader of the research group on Reliability of Power Electronic Converters (ReliaPEC) in AAU Energy.

He is a recipient of the Indian National Academy of Engineering (INAE) Innovative Students Project Award for the best PhD thesis across all the institutes in India for the year 2019. He is selected into EU-US National Academy of Engineering (NAE) Frontier of Engineering (FOE) Class of 2021. He was also a distinguished reviewer for IEEE Transactions on Smart Grid in 2020. He is currently the vice-chair of IEEE PELS Technical Committee (TC) 10 on Design Methodologies. He is an Associate Editor on IEEE Transactions on Transportation Electrification.

His research interests are control, optimization, cybersecurity, and stability of power electronic dominated grids and application of artificial intelligence and machine learning in power electronic systems.

Frede Blaabjerg (Fellow, IEEE) received the Ph.D. degree in electrical engineering from Aalborg University, Aalborg, Denmark, in 1995. From 1987 to 1988, he was with ABBScandia, Randers, Denmark. He became an Assistant Professor, an Associate Professor, and a Full Professor of power electronics and drives with Aalborg University, in 1992, 1996, and 1998, respectively. In 2017, he became a Villum Investigator. Additionally, he is Honoris Causa with University Politehnica Timisoara (UPT), Timisoara, Romania, and Tallinn Technical University, Tallin, Estonia. He has authored or coauthored four monographs, published more than 600 journal articles in the fields of power electronics and its applications and was an editor of ten books in power electronics and its applications. His current research interests include power electronics and its applications, such as in wind turbines, PV systems, reliability, harmonics, and adjustable speed drives. He was a recipient of the 33 IEEE Prize Paper Awards, the IEEE PELS Distinguished Service Award in 2009, the EPE-PEMC Council Award in 2010, the IEEE William E. Newell Power Electronics Award 2014, the Villum Kann Rasmussen Research Award 2014, the Global Energy Prize in 2019, and the 2020 IEEE Edison Medal. From 2006 to 2012, he was the Editor-in-Chief for the IEEE TRANSACTIONS ON POWER ELECTRONICS. From 2005 to 2007, he was a Distinguished Lecturer of the IEEE Power Electronics Society and the IEEE Industry Applications Society from 2010 to 2011 and from 2017 to 2018. From 2019 to 2020, he was the President of IEEE Power Electronics Society. He was the Vice President of the Danish Academy of Technical Sciences, Lyngby, Denmark. From 2014 to 2020, he was nominated by Thomson Reuters, Toronto, Canada, to be between the most 250 cited researchers in engineering in the world.