Cross-Layer Distributed Control Strategy for Cyber Resilient Microgrids

Quan Zhou, *Senior Member, IEEE*, Mohammad Shahidehpour, *Life Fellow, IEEE*, Ahmed Alabdulwahab, *Senior Member, IEEE*, Abdullah Abusorrah, *Senior Member, IEEE*, Liang Che, *Member, IEEE*, and Xuan Liu, *Member, IEEE*

***Abstract*—The widespread adoption of communication and control infrastructures will not only improve the microgrid system performance in normal conditions but also increase microgrid cybersecurity risks. Potential cyberattacks can deteriorate microgrid performances by corrupting and intercepting data exchanges among participating DERs, whereby microgrids deviate from desired operating conditions and stable microgrid operations are jeopardized. In this paper, a cross-layer control strategy is proposed to enhance the microgrid resilience against false data injection (FDI) and denial of service (DoS) attacks. On the one hand, the proposed control strategy will not interfere with microgrid normal operations when there are no cyberattacks. On the other hand, the proposed control strategy can effectively mitigate the impacts of FDI and DoS attacks on microgrids without relying on prompt detection and isolation of cyberattacks. The stability of the proposed control strategy is demonstrated using the Lyapunov theory under different scenarios, including without and with FDI and DoS attacks. The effectiveness of the proposed cross-layer resilient control strategy against cyberattacks is validated in a 12-bus microgrid system using time-domain PSCAD/EMTDC simulations.**

***Index Terms*—Cross-layer distributed control, cybersecurity, microgrid, resilience.**

Manuscript received August 10, 2020; revised December 27, 2020; accepted February 26, 2021. Date of publication March 29, 2021; date of current version August 23, 2021. This work was supported in part by the National Natural Science Foundation of China under Grant 51777062, and in part by the Deanship of Scientific Research (DSR) at King Abdulaziz University under Grant RG-10-135-41. Paper no. TSG-01231-2020. *(Corresponding author: Xuan Liu.)*

Quan Zhou is with the School of Electrical and Information Engineering, Hunan University, Changsha 410000, China, and also with the Department of Electrical and Computer Engineering, Illinois Institute of Technology, Chicago, IL 60616 USA (e-mail: qzhou15@hawk.iit.edu).

Mohammad Shahidehpour is with the ECE Department, Illinois Institute of Technology, Chicago, IL 60616 USA and also with the Center of Research Excellence in Renewable Energy and Power Systems, King Abdulaziz University, Jeddah 21589, Saudi Arabia (e-mail: ms@iit.edu).

Ahmed Alabdulwahab and Abdullah Abusorrah are with the Department of Electrical and Computer Engineering, Faculty of Engineering, King Abdulaziz University, Jeddah 21589, Saudi Arabia, and also with the Center of Research Excellence in Renewable Energy and Power Systems, King Abdulaziz University, Jeddah 21589, Saudi Arabia (e-mail: aabdulwhab@kau.edu.sa; aabusorrah@kau.edu.sa).

Liang Che and Xuan Liu are with the School of Electrical and Information Engineering, Hunan University, Changsha 410000, China (e-mail: lche@hawk.iit.edu; xliu108@hawk.iit.edu).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TSG.2021.3069331.

Digital Object Identifier 10.1109/TSG.2021.3069331

NOMENCLATURE

Index and Sets

i, j	Index of participating DERs
$\|\cdot\|_{\max}$	Maximum norm of the vector
$\|\cdot\|_2$	Euclidean norm of the vector
$(\cdot)^T$	Transpose of the matrix
$diag(\cdot)$	Diagonal matrix
$(\cdot)^*$	System equilibrium point with FDI attacks
$(\cdot)'$	System equilibrium point with DoS attacks
$\lambda_{\min}(\cdot)$	Smallest eigenvalue of the matrix.

Parameters

n	Number of participating DERs in the microgrid
m_i	Droop coefficient of DER i
L_ω	Laplacian matrix of the control network layer
G_ω	Pinning matrix of the control network layer
F	FDI attack matrix
L_η	Laplacian matrix of the parallel control network layer
B_η	A positive definite diagonal matrix
C	Coupling matrix between the control and parallel control network layers
ω_0	Rated frequency
α	Gain of coupling matrix C
$\bar{\mu}$	Upper bound of FDI attack signals.

Variables:

$\boldsymbol{\omega}$	Vector of DER frequencies
$\boldsymbol{\mu}$	Vector of FDI attack signals
$\boldsymbol{\eta}$	Vector of state variables in the parallel control network layer
$\boldsymbol{e}, \boldsymbol{\varepsilon}, \boldsymbol{\rho}, \boldsymbol{\sigma}$	Vectors of state variables Other notations are defined in the text.

I. INTRODUCTION

WITH the proliferation of distributed energy resources (DERs), microgrids provide a promising solution to accommodating and coordinating various DERs by forming flexible and efficient self-controlled electric networks [1]. The inverter-based DERs usually feature good controllability and fast-response, which would not contribute to the total system inertia [2]. Considering the low-inertia characteristic of microgrids, Dörfler *et al.* [3]

propose to break the microgrid control hierarchy and implement control tasks on different time scales simultaneously for offering fast and robust control performance.

Using the centralized control strategy, a master controller deployed in the microgrid processes the collected local DER data and sends control commands to participating DERs for guiding their operations. In [4], [5], the power outputs of wind turbines are optimally controlled by the master controller for providing effective ancillary services. But the master controller might be incapable of managing and regulating the increasing number of heterogeneous and geographically dispersed DERs due to its limited communication and computation capabilities. Also, the centralized control strategy might make the microgrid system fragile due to its vulnerability to single-point-failures. Comparatively, using the distributed control strategy, participating DERs only exchange data with their neighbors, which allows parallel data processing and accelerates the control responses to local disturbances. Compared with the centralized control strategy, the distributed control strategy could feature enhanced scalability, reliability, resilience, and computational and communication efficiency [6], [7]. Thus, distributed control strategies are widely applied to coordinate a multitude of participating DERs in microgrids, where the coordinated control tasks are divided among these DERs.

Distributed control strategy allows participating DERs to exchange data with their neighbors for driving their designated consensus variables to the equilibrium. In [8], a distributed-averaging proportional-integral (DAPI) control strategy is proposed to achieve precise frequency and active power sharing regulation and a tunable tradeoff between voltage and reactive power sharing regulation, where the low-bandwidth communication network is deployed to enable data exchange among neighboring DERs. The DAPI control strategy is model-free and features a flexible plug-and-play property, which would not require a priori knowledge of network topology and line impedance.

In [9], the uncertainties of communication networks, e.g., time delays, link failures, and packet losses, and their impacts on the performance of distributed control strategy are systematically analyzed. Shi *et al.* [10] propose a PI-consensus distributed control strategy with an enhanced robustness against time delays, system initial conditions, and controller input disturbances, where both the consensus variable and its accumulative errors are exchanged among neighboring DERs. Reference [11] is the first work to establish a general modeling of time-delayed distributed cyber-physical power systems (CPPSs), which can systematically guide the practical implementations of CPPSs under fully distributed control. Khayat *et al.* [12] review and categorize communication-based distributed control strategies in microgrids, where these control strategies are graphically illustrated and several critical issues are identified.

The performance of distributed control strategy in microgrids depends on a reliable and secure communication network, which makes the microgrid vulnerable to potential cybersecurity issues. Also, microgrid with distributed control strategy has a limited global system situational awareness since there is no central entity to directly monitor all the DER activities, which would introduce additional cybersecurity risks. The weakness in cybersecurity could pose serious threats to microgrid operations due to the massive adoption of inverter-based DERs, software-intensive information and communication technology (ICT) infrastructure. In 2015, the BlackEnergy virus targeting Ukrainian distribution power systems has led to a six-hour blackout for more than 225,000 residents around Kyiv [13]. It is reported in [14] that 80% of the surveyed electric utilities have encountered at least one large-scale denial of service (DoS) attack on communication networks and 85% of them have suffered from network intrusions. These incidents and their severe impacts have raised extensive concerns about the emerging cybersecurity threats in CPPSs [15].

Potential cyberattacks can deteriorate microgrid operations by corrupting and intercepting the communication among participating DERs, which might lead to severe violations of DER power ratings and even system-wide instability [16]. Cyberattacks in microgrids mainly include false data injection (FDI) attacks [17]–[27] and DoS attacks [28]–[38]. FDI attack, which is also defined as deception or integrity attack, aims to access and tamper with data exchanges among participating DERs. The major techniques developed for coping with FDI attacks include trust/reputation-based cooperative control [17], dynamic state estimation [18], Kalman-filter [19], Kullback–Leibler distance algorithm [20], maximum game-theoretic resilient control [21], matrix separation [22], dynamic watermarking [23], signal temporal logic [24], supervised learning [25], unsupervised learning [26], reinforcement learning [27], etc. DoS attack aims at jeopardizing the availability of communication services by jamming the communication channels or flooding packets in the network. The major techniques adopted for handling DoS attacks include event-triggered control [28], risk-sensitive control [29], fallback control [30], distributed output-feedback control [31], proactive aperiodic intermittent control [32], authentication protocol [33], FloodDefender [34], software-defined networking [35], machine learning [36], data mining [37], network intelligence [38], etc.

These countermeasures for cyberattacks can be categorized into model-based and data-driven schemes [39]. The effectiveness of these model-based schemes [17]–[24], [28]–[35] depends on accurate system modeling and detailed system parameters without requiring historical data. The model-based schemes usually feature high scalability, modularity, and compatibility for flexible utilizations and future expansions. But the potential detection and localization delays might lead to high cybersecurity risks and serious instability issues. Comparatively, the effectiveness of these data-driven schemes [25]–[27], [36]–[38] depends on sufficient historical data sets and efficient training processes, which restrains their scalability and compatibility. The data-driven schemes are usually independent of system modeling and parameters, which feature fast dynamic response and high adaptability to varying operating conditions and unexpected disturbances.

Most existing countermeasures against cyberattacks are designed to detect cyber intrusions and isolate corrupted components for deterring adversaries from executing effective cyberattacks. However, the emergence of stealthy cyberattacks could deteriorate microgrid operations in a concealed fashion without triggering conventional detection and localization schemes, especially when adversaries have obtained a priori knowledge of communication and electric networks [40]. These stealthy cyberattacks will be difficult to be detected and isolated promptly. Moreover, combined FDI and DoS attacks could have more severe effects and lower detection probabilities than those of FDI or DoS attacks [41]. Thus, one fundamental yet challenging task is to maintain the coordinated DER operations in a microgrid that is inevitably disrupted by certain stealthy cyberattacks.

In this paper, we propose a cross-layer distributed control strategy to enhance the microgrid resilience against both FDI and DoS attacks. The main contributions of this paper are summarized as follows.

1) The proposed cross-layer resilient control strategy consists of control and parallel control network layers. The cooperation between the two layers could effectively mitigate the respective effects of cyberattacks without relying on prompt detection and isolation schemes for cyberattacks;

2) The proposed cross-layer resilient control strategy can cope with FDI, DoS, and combined attacks. The adversaries are considered to have a priori knowledge of the communication and electric networks, and the corresponding cyberattacks are difficult to be detected and isolated timely. Also, the effects of FDI and DoS attacks on microgrid operations are analyzed theoretically, which demonstrate how FDI and DoS attacks deteriorate the microgrid operations;

3) The stability of the proposed cross-layer resilient control strategy is demonstrated using the Lyapunov theory under different scenarios including without cyberattacks, with FDI attacks, and with DoS attacks. The proposed control strategy can retain coordinated DER operations irrespective of when and where these cyberattacks occur in microgrids. Also, the proposed approach will not interfere with the microgrid normal operations when there are no cyberattacks.

The remainder of this paper is organized as follows. Section II introduces the communication network of an islanded microgrid. Also, the models of FDI and DoS attacks are discussed and their effects on microgrid operations are demonstrated. In Section III, the cross-layer resilient control strategy is proposed, and the stability without cyberattacks is demonstrated. In Section IV, the stability of the proposed cross-layer resilient control strategy under FDI and DoS attacks is demonstrated using the Lyapunov theory. In Section V, the effectiveness of the proposed cross-layer resilient control strategy is validated in a 12-bus microgrid using the PSCAD/EMTDC platform. Section VI concludes this paper.

II. FDI and DoS Attacks in Islanded Microgrids

This section introduces the communication network for the implementation of distributed control strategy in an islanded microgrid. Then, we will demonstrate the effects of FDI and DoS attacks on microgrid operations.

A. Communication Network of an Islanded Microgrid

Consider there are n dispatchable inverter-based DERs in an islanded microgrid. The dispatchable inverter-based DERs are operated in a grid-forming mode, which would participate in frequency and voltage regulations while maintaining the microgrid system power balance. Participating DERs exchange data with their neighbors via a communication network, which is modeled as an undirected graph. The corresponding Laplacian matrix is defined as:

$$(L_\omega)_{ij} = \begin{cases} \sum_{j=1}^{n} a_{ij} & if\ i = j \\ -a_{ij} & if\ i \neq j \end{cases} \tag{1}$$

where $a_{ij} = 1$ if and only if there is a communication link between DERs i and j, otherwise, $a_{ij} = 0$.

In the microgrid, only a small proportion of DERs have access to the reference information for frequency restoration, which are defined as pinned DERs. The remaining DERs will track pinned DERs to realize frequency restoration. Accordingly, the DER frequency dynamics are stated as:

$$\dot{\boldsymbol{\omega}} = -L_\omega \boldsymbol{\omega} - G_\omega(\boldsymbol{\omega} - \boldsymbol{\omega}_0) \tag{2}$$

In (2), the first term $-L_\omega\boldsymbol{\omega}$ represents the data exchange among neighboring DERs, which would synchronize the DER frequencies. The second term $-G_\omega(\boldsymbol{\omega}-\boldsymbol{\omega}_0)$ represents the pinning control signal imposed on pinned DERs, which would restore pinned DER frequencies to the rated value. In this paper, the control design in (2) is a typical distributed control without the proposed cross-layer strategy, which does not consider cybersecurity.

The communication network deployed in the microgrid provides facilitates the coordinated operations of participating DERs. However, such communication infrastructures pose potential cyberattack risks, which might deteriorate microgrid operations and lead to microgrid instability. Fig. 1 shows potential cybersecurity threats in an islanded microgrid, where pinning control signals, local communication, and DERs might be corrupted or intercepted by potential cyberattacks. Thus, it is critical to theoretically analyze the effects of cyberattacks on microgrid operations for developing effective countermeasures against cybersecurity threats.

B. FDI Attack and Its Effects

FDI attack, which introduce the corrupted information in microgrids, aims to falsify data exchanges among participating DERs [17]–[27]. Here, FDI attack is considered a uniformly bounded time-varying malicious signal imposed on some DERs and communication links. An effective stealthy FDI attack is designed within a normal margin of error to avoid false alarms [40]. The FDI attack which is unbounded will be signified by its abnormally large magnitude and subsequently be detected and isolated by common cyber defense measures. Thus, the bounded FDI attack signal is denoted by $\boldsymbol{\mu} = [\mu_1, \mu_2, \ldots, \mu_n]^T$, which satisfies $\|\boldsymbol{\mu}\|_{\max} \leq \bar{\mu}$. The

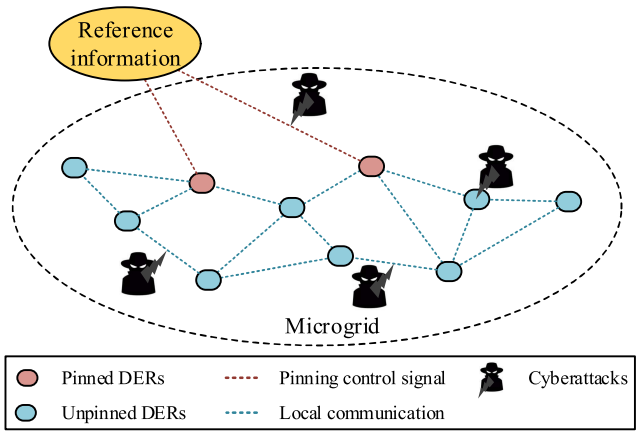

Fig. 1. Cybersecurity threats in an islanded microgrid.

DER frequency dynamics under FDI attacks are modified as:

$$\dot{\boldsymbol{\omega}} = -L_\omega \boldsymbol{\omega} - G_\omega(\boldsymbol{\omega} - \boldsymbol{\omega}_0) + \boldsymbol{\mu} \tag{3}$$

Considering that adversaries have full knowledge of communication network, the dynamics of FDI attack signal are stated as:

$$\dot{\boldsymbol{\mu}} = -\boldsymbol{\mu} + F\boldsymbol{\omega} \tag{4}$$

where the FDI attack matrix F might take a similar form as the Laplacian matrix of the communication network L_ω. Then, for each corrupted DER, the FDI attack is only composed of its neighboring DER frequencies without including any external signals, which makes it difficult to detect such FDI attacks.

The state error is defined as the difference between the DER frequencies and the rated value, i.e., $\mathbf{e} = \boldsymbol{\omega} - \boldsymbol{\omega}_0$. Then, the state error dynamics in FDI attacks are stated as:

$$\dot{\mathbf{e}} = -(L_\omega + G_\omega)\mathbf{e} + \boldsymbol{\mu} \tag{5}$$

The solution of state error dynamics in (5) is stated as:

$$\mathbf{e}(t) = e^{-(L_\omega + G_\omega)t}\mathbf{e}(t_0) + \int_0^t e^{-(L_\omega + G_\omega)(t-s)}\boldsymbol{\mu}(s)ds \tag{6}$$

Since the matrix $L_\omega + G_\omega$ is positive definite, the first term in (6) would converge to zero. Without the loss of generality, the FDI attack signal is assumed positive, i.e., $\boldsymbol{\mu}(t) > \boldsymbol{\mu}_0 > 0$. Then, we have:

$$\begin{aligned}\lim_{t\to\infty}\mathbf{e}(t) &= \lim_{t\to\infty}\int_{t_0}^t e^{-(L_\omega+G_\omega)(t-s)}\boldsymbol{\mu}(s)ds \\ &> \lim_{t\to\infty} e^{-(L_\omega+G_\omega)t}\left(e^{(L_\omega+G_\omega)t} - e^{(L_\omega+G_\omega)t_0}\right) \\ &\quad \times (L_\omega + G_\omega)^{-1}\boldsymbol{\mu}_0 \\ &= (L_\omega + G_\omega)^{-1}\boldsymbol{\mu}_0 \geq \mathbf{0}\end{aligned} \tag{7}$$

Similarly, we can demonstrate that the negative FDI attack would also cause the state error to deviate from zero. The non-zero FDI attacks can usually drive the state error away from zero no matter the FDI attacks are positive or negative. Accordingly, state errors in FDI attacks will not converge to zero, implying that rated DER frequency is not restored because of FDI attacks which culminate in microgrid divergence from the desired operating conditions.

C. DoS Attack and Its Effects

DoS attack intends to intercept pinning control signals or data exchanges among participating DERs, and then some communication network links would be disabled [28]–[38]. Here, DoS attacks partitions the communication network into m isolated sub-networks. The DER frequency dynamics under DoS attacks are stated as:

$$\dot{\boldsymbol{\omega}} = -L'_\omega \boldsymbol{\omega} - G'_\omega(\boldsymbol{\omega} - \boldsymbol{\omega}_0) \tag{8}$$

where $L'_\omega = diag(L'_{\omega(i)}, \ldots, L'_{\omega(m)})$ is a block-diagonal matrix representing the Laplacian matrix of the communication network compromised by DoS attacks, and the pinning matrix is modified as $G'_\omega = diag(G'_{\omega(1)}, \ldots, G'_{\omega(m)})$.

The state error dynamics under DoS attacks are stated as:

$$\dot{\mathbf{e}} = -\left(L'_\omega + G'_\omega\right)\mathbf{e} \tag{9}$$

where the augmented Laplacian matrix of the compromised communication network is a block-diagonal matrix stated as:

$$L'_\omega + G'_\omega = diag\left(L'_{\omega(i)} + G'_{\omega(1)}, \ldots, L'_{\omega(m)} + G'_{\omega(m)}\right) \tag{10}$$

If an arbitrary sub-network k does not have any pinned DERs or the corresponding pinning control signals are disabled (i.e., $G'_{\omega(k)} = \mathbf{0}$), the augmented Laplacian matrix $L'_{\omega(k)} + G'_{\omega(k)}$ will have a zero eigenvalue. Then, $L'_\omega + G'_\omega$ will also have zero eigenvalues since the eigenvalues of $L'_\omega + G'_\omega$ are the union of the eigenvalues of the diagonal blocks. Thus, the solution of state error dynamics in (9) will not converge to zero, which is stated as:

$$\mathbf{e}(t) = e^{-(L'_\omega + G'_\omega)t}\mathbf{e}(t_0) \tag{11}$$

Accordingly, DoS attacks can impede the DER frequency restoration by disabling some communication links and partitioning the communication network into several sub-networks. Local DERs in sub-networks without pinning control signals will not have access to the reference information and their frequencies will not be restored to the rated value. The interdependency of communication and electric networks is discussed in [42], which illustrates that any communication link failures can seriously affect microgrid operations. In summary, both FDI and DoS attacks can deteriorate the microgrid operations and drive the microgrid away from desired operating conditions, which might lead to violations of DER power ratings and system-wide instability.

III. Proposed Cross-Layer Resilient Control Strategy

In this section, a cross-layer resilient control strategy is proposed for islanded microgrids to cope with FDI and DoS attacks. First, the proposed cross-layer resilient control design is presented. Second, the stability of the proposed control strategy without cyberattacks is demonstrated using the Lyapunov theory.

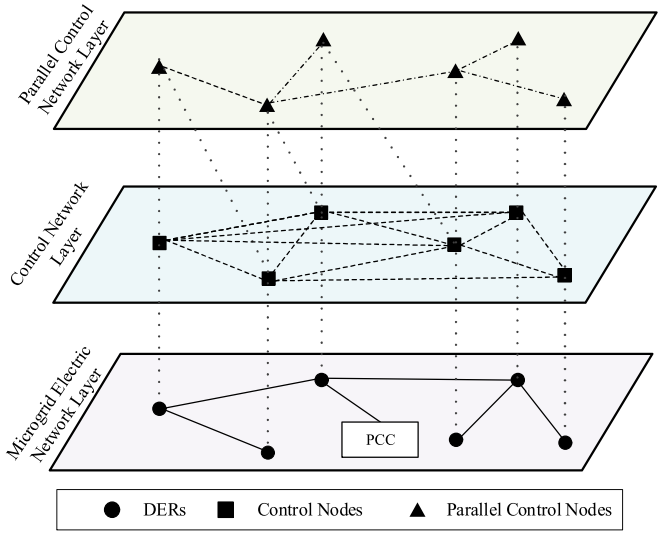

Fig. 2. Proposed cross-layer resilient control strategy in islanded microgrids.

A. Design of the Proposed Cross-Layer Resilient Control

Consider the proposed hierarchy in Fig. 2. The bottom layer is the microgrid electric network for allowing participating DERs to supply local loads in the microgrid. The middle layer enables data exchanges among DERs, which is labeled as the control layer. The top layer is the designed parallel control network layer, which provides resilient control commands for mitigating the effects of cyberattacks when the cyberattacks cannot be addressed timely. The proposed cross-layer resilient control strategy is stated as:

$$\dot{\boldsymbol{\omega}} = -(L_\omega + G_\omega)\boldsymbol{\omega} + G_\omega\boldsymbol{\omega}_0 + \alpha C\boldsymbol{\eta} \tag{12}$$

$$\dot{\boldsymbol{\eta}} = -\big(L_\eta + B_\eta\big)\boldsymbol{\eta} + \alpha C\boldsymbol{\omega}_0 - \alpha C\boldsymbol{\omega} \tag{13}$$

where the state information is shared between the control network layer (12) and the parallel control network layer (13) for enhancing system resilience against cyberattacks.

In Fig. 2, the control network layer (12) features high network connectivity while increasing cybersecurity risks. This implies that the microgrid would be vulnerable to cyberattacks if only the control network layer is deployed. Conversely, the parallel control network layer (13) that is implemented using software-defined networking (SDN) features low network connectivity and relatively sufficient cyber defense resources with low cybersecurity risks [35], [43]. Due to the low network connectivity, the desired convergence performance might fail to be achieved if only the parallel control network layer is deployed. Here, the coupled control and parallel control network layers cooperate to enhance the microgrid resilience and its convergence performance via incorporating more communication and control redundancies.

B. Stability of the Proposed Cross-layer Resilient Control Strategy Without Cyberattacks

Using the proposed control strategy, the state error dynamics without cyberattacks are presented as:

$$\begin{cases} \dot{\mathbf{e}} = -(L_\omega + G_\omega)\mathbf{e} + \alpha C\boldsymbol{\eta} \\ \dot{\boldsymbol{\eta}} = -\big(L_\eta + B_\eta\big)\boldsymbol{\eta} - \alpha C\mathbf{e} \end{cases} \tag{14}$$

Consider the following Lyapunov function:

$$V = \frac{1}{2}\mathbf{e}^T\mathbf{e} + \frac{1}{2}\boldsymbol{\eta}^T\boldsymbol{\eta} \tag{15}$$

Since both $L_\omega + G_\omega$ and $L_\eta + B_\eta$ are positive definite, the time derivative of the Lyapunov function (15) is stated as:

$$\begin{aligned} \dot{V} &= \mathbf{e}^T\dot{\mathbf{e}} + \boldsymbol{\eta}^T\dot{\boldsymbol{\eta}} \\ &= \mathbf{e}^T[-(L_\omega + G_\omega)\mathbf{e} + \alpha C\boldsymbol{\eta}] + \boldsymbol{\eta}^T\big[-\big(L_\eta + B_\eta\big)\boldsymbol{\eta} - \alpha C\mathbf{e}\big] \\ &= -\mathbf{e}^T(L_\omega + G_\omega)\mathbf{e} - \boldsymbol{\eta}^T\big(L_\eta + B_\eta\big)\boldsymbol{\eta} < 0 \end{aligned} \tag{16}$$

Accordingly, the microgrid system equilibrium point is demonstrated to be asymptotical stable, which implies that the proposed control strategy would not interfere with the microgrid operations when there are no cyberattacks. Also, the convergence of the control strategy can be estimated based on the time interval that allows the Lyapunov function to drop to zero from its initial state [44]. According to (16), the proposed cross-layer control features a faster convergence rate than that of the distributed control strategy without the proposed cross-layer strategy stated in (2). A similar analysis can be conducted for applying the proposed cross-layer resilient control design to the proportional active power sharing among participating DERs in an islanded microgrid.

IV. Stability of the Proposed Cross-Layer Resilient Control Strategy Under FDI and DoS Attacks

In this section, we discuss the stability of the proposed cross-layer resilient control strategy considering FDI and DoS attacks in islanded microgrids. With the proposed control strategy, the microgrid system equilibrium point under FDI and DoS attacks is demonstrated to be asymptotically stable using the Lyapunov theory.

A. Stability Under FDI Attacks

Consider some DERs and communication links are corrupted by FDI attack signals modeled in (4). Using the proposed cross-layer resilient control strategy, the DER frequency dynamics under FDI attacks are stated as:

$$\begin{cases} \dot{\boldsymbol{\omega}} = -(L_\omega + G_\omega)\boldsymbol{\omega} + G_\omega\boldsymbol{\omega}_0 + \alpha C\boldsymbol{\eta} + \boldsymbol{\mu} \\ \dot{\boldsymbol{\eta}} = -\big(L_\eta + B_\eta\big)\boldsymbol{\eta} + \alpha C\boldsymbol{\omega}_0 - \alpha C\boldsymbol{\omega} \end{cases} \tag{17}$$

Here, the equilibrium point of (17) is denoted by:

$$\begin{cases} \boldsymbol{\omega}^* = \big[\omega_1^*, \omega_2^*, \ldots, \omega_n^*\big]^T \\ \boldsymbol{\eta}^* = \big[\eta_1^*, \eta_2^*, \ldots, \eta_n^*\big]^T \end{cases} \tag{18}$$

which satisfies the following conditions:

$$\begin{cases} -(L_\omega + G_\omega)(\boldsymbol{\omega}^* - \boldsymbol{\omega}_0) + \alpha C\boldsymbol{\eta}^* + \boldsymbol{\mu}^* = 0 \\ -\big(L_\eta + B_\eta\big)\boldsymbol{\eta}^* - \alpha C(\boldsymbol{\omega}^* - \boldsymbol{\omega}_0) = 0 \\ \boldsymbol{\mu}^* + F\boldsymbol{\omega}^* = 0 \end{cases} \tag{19}$$

Define state errors as the difference between the current states and equilibrium points, i.e., $\boldsymbol{\varepsilon} = \boldsymbol{\omega} - \boldsymbol{\omega}^*$, $= \boldsymbol{\rho} = \boldsymbol{\eta} - \boldsymbol{\eta}^*$, and $\boldsymbol{\sigma} = \boldsymbol{\mu} - \boldsymbol{\mu}^*$. Combining (17) and (19), the state error dynamics for DERs under FDI attacks are stated as:

$$\begin{cases} \dot{\boldsymbol{\varepsilon}} = -(L_\omega + G_\omega)\boldsymbol{\varepsilon} + \alpha C\boldsymbol{\rho} + \boldsymbol{\sigma} \\ \dot{\boldsymbol{\rho}} = -\big(L_\eta + B_\eta\big)\boldsymbol{\rho} - \alpha C\boldsymbol{\varepsilon} \end{cases} \tag{20}$$

Based on the converse Lyapunov theorem, if the conditions (19) hold, there exists a Lyapunov function V_η that satisfies $\dot{V}_\eta \leq -\gamma^2\|\boldsymbol{\sigma}\|_2^2$, where $\gamma = 1/2\sqrt{\lambda_{\min}(L_\omega + G_\omega)}$ [45].

Consider the following Lyapunov function:

$$V = \frac{1}{2}\boldsymbol{\varepsilon}^T\boldsymbol{\varepsilon} + \frac{1}{2}\boldsymbol{\rho}^T\boldsymbol{\rho} + V_\eta \tag{21}$$

The time derivative of Lyapunov function (21) is stated as:

$$\begin{aligned}\dot{V} &= \boldsymbol{\varepsilon}^T\dot{\boldsymbol{\varepsilon}} + \boldsymbol{\rho}^T\dot{\boldsymbol{\rho}} + \dot{V}_\eta \\ &= \boldsymbol{\varepsilon}^T\left[-(L_\omega + G_\omega)\boldsymbol{\varepsilon} + \alpha C\boldsymbol{\rho} + \boldsymbol{\sigma}\right] \\ &\quad + \boldsymbol{\rho}^T\left[-\left(L_\eta + B_\eta\right)\boldsymbol{\rho} - \alpha C\boldsymbol{\varepsilon}\right] + \dot{V}_\eta \\ &= -\boldsymbol{\varepsilon}^T(L_\omega + G_\omega)\boldsymbol{\varepsilon} - \boldsymbol{\rho}^T\left(L_\eta + B_\eta\right)\boldsymbol{\rho} + \dot{V}_\eta + \boldsymbol{\varepsilon}^T\boldsymbol{\sigma} \\ &\leq -\lambda_{\min}(L_\omega + G_\omega)\boldsymbol{\varepsilon}^T\boldsymbol{\varepsilon} - \boldsymbol{\rho}^T\left(L_\eta + B_\eta\right)\boldsymbol{\rho} - \gamma^2\boldsymbol{\sigma}^T\boldsymbol{\sigma} + \boldsymbol{\varepsilon}^T\boldsymbol{\sigma} \\ &= -\boldsymbol{\rho}^T\left(L_\eta + B_\eta\right)\boldsymbol{\rho} - \left\|\sqrt{\lambda_{\min}(L_\omega + G_\omega)}\boldsymbol{\varepsilon} - \gamma\boldsymbol{\sigma}\right\|_2^2 \\ &< 0\end{aligned} \tag{22}$$

Therefore, with the proposed cross-layer resilient control strategy, the equilibrium point of the islanded microgrid system under FDI attacks is demonstrated to be asymptotically stable. Based on (19), there is

$$\left\|\boldsymbol{\omega}^* - \boldsymbol{\omega}_0\right\|_2 = \left\|K^{-1}\right\|_2\left\|\boldsymbol{\mu}^*\right\|_2 \leq \left\|K^{-1}\right\|_2\bar{\mu} \tag{23}$$

where $K = (L_\omega + G_\omega) + \alpha^2 C(L_\eta + B_\eta)^{-1}C$. Accordingly, DER frequencies can be restored to the rated value ω_0 if the gain $\|K\|_2$ is properly set.

According to (23), the control accuracy is determined by the matrix K, which is related to the augmented Laplacian matrix of the control network layer $(L_\omega + G_\omega)$, the augmented Laplacian matrix of the parallel control network layer $(L_\eta + B_\eta)$, and the interactive matrix C. Theoretically, we could increase the gain $\|K\|_2$ to improve the control accuracy by adjusting the coefficient α and optimizing the network design, which would make the control input in (12)-(13) be more sensitive to relative state deviations among participating DERs. It might cause transitory overshoots, which would lead to oscillations in DER frequencies and active power outputs. Under such circumstances, a saturation function could be used to enforce a predetermined upper bound for restricting potential overshoots of control input. In [46], a tangent function is adopted to construct a bounded and finite-time distributed control strategy in microgrids. Therefore, it is important to properly set the gain $\|K\|_2$ as a tradeoff between convergence performance and dynamic response.

B. Stability Under DoS Attacks

Consider some communication links among neighboring DERs in the communication network are disabled by DoS attacks. The corresponding augmented Laplacian matrix $L'_\omega + G'_\omega$ is positive semidefinite rather than positive definite. With the proposed cross-layer resilient control strategy, the DER frequency dynamics under DoS attacks are stated as:

$$\begin{cases}\dot{\boldsymbol{\omega}} = -\left(L'_\omega + G'_\omega\right)\boldsymbol{\omega} + G_\omega\boldsymbol{\omega}_0 + \alpha C\boldsymbol{\eta} \\ \dot{\boldsymbol{\eta}} = -\left(L_\eta + B_\eta\right)\boldsymbol{\eta} + \alpha C\boldsymbol{\omega}_0 - \alpha C\boldsymbol{\omega}\end{cases} \tag{24}$$

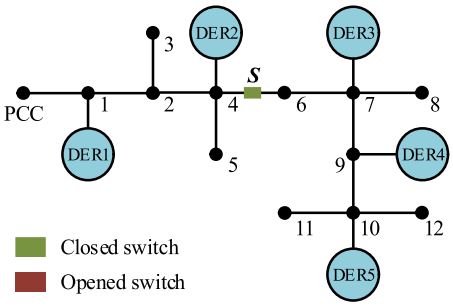

Fig. 3. A 12-bus microgrid system.

The equilibrium point of (24) is denoted by:

$$\begin{cases}\boldsymbol{\omega}' = \left[\omega'_1, \omega'_2, \ldots, \omega'_n\right]^T \\ \boldsymbol{\eta}' = \left[\eta'_1, \eta'_2, \ldots, \eta'_n\right]^T\end{cases} \tag{25}$$

which satisfies the following conditions:

$$\begin{cases}-\left(L'_\omega + G'_\omega\right)\left(\boldsymbol{\omega}' - \boldsymbol{\omega}_0\right) + \alpha C\boldsymbol{\eta}' = 0 \\ -\left(L_\eta + B_\eta\right)\boldsymbol{\eta}' - \alpha C\left(\boldsymbol{\omega}' - \boldsymbol{\omega}_0\right) = 0\end{cases} \tag{26}$$

Here, we define the state errors as the difference between the current states and the equilibrium points, i.e., $\boldsymbol{\varepsilon}' = \boldsymbol{\omega} - \boldsymbol{\omega}'$ and $\boldsymbol{\rho} = \boldsymbol{\eta} - \boldsymbol{\eta}'$. Then, the state error dynamics for DERs under DoS attacks are stated as:

$$\begin{cases}\dot{\boldsymbol{\varepsilon}}' = -\left(L'_\omega + G'_\omega\right)\boldsymbol{\varepsilon}' + \alpha C\boldsymbol{\rho}' \\ \dot{\boldsymbol{\rho}}' = -\left(L_\eta + B_\eta\right)\boldsymbol{\rho}' - \alpha C\boldsymbol{\varepsilon}'\end{cases} \tag{27}$$

Consider the following Lyapunov function:

$$V = \frac{1}{2}\boldsymbol{\varepsilon}'^T\boldsymbol{\varepsilon}' + \frac{1}{2}\boldsymbol{\rho}'^T\boldsymbol{\rho}' \tag{28}$$

Since $L'_\omega + G'_\omega$ is positive semidefinite and $L_\eta + B_\eta$ is positive definite, the time derivative of the Lyapunov function (28) is stated as:

$$\begin{aligned}\dot{V} &= \boldsymbol{\varepsilon}'^T\dot{\boldsymbol{\varepsilon}}' + \boldsymbol{\rho}'^T\dot{\boldsymbol{\rho}}' \\ &= \boldsymbol{\varepsilon}'^T\left[-\left(L'_\omega + G'_\omega\right)\boldsymbol{\varepsilon}' + \alpha C\boldsymbol{\rho}'\right] \\ &\quad + \boldsymbol{\rho}'^T\left[-\left(L_\eta + B_\eta\right)\boldsymbol{\rho}' - \alpha C\boldsymbol{\varepsilon}'\right] \\ &= -\boldsymbol{\varepsilon}'^T\left(L'_\omega + G'_\omega\right)\boldsymbol{\varepsilon}' - \boldsymbol{\rho}'^T\left(L_\eta + B_\eta\right)\boldsymbol{\rho}' \\ &\leq -\boldsymbol{\rho}'^T\left(L_\eta + B_\eta\right)\boldsymbol{\rho}' < 0\end{aligned} \tag{29}$$

Also, based on (26), there is

$$\left\|\boldsymbol{\omega}' - \boldsymbol{\omega}_0\right\|_2 = 0 \tag{30}$$

Accordingly, DER frequencies can be restored to the rated value ω_0 under DoS attacks. Thus, the stability of the proposed cross-layer resilient control strategy under DoS attacks is demonstrated using the Lyapunov theory.

V. Case Studies

The effectiveness of the proposed cross-layer resilient control strategy is validated in a 12-bus microgrid system using time-domain PSCAD/EMTDC platform. In Fig. 3, the 12-bus microgrid includes five DERs (located at Buses 1, 4, 7, 9, and 10, respectively) and five loads (located at Buses 3, 5, 6, 8, and 11, respectively), where each load is set as 60kW+6kVar.

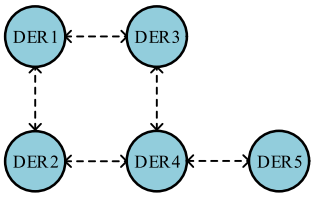

Fig. 4. Communication network of the 12-bus microgrid system.

Fig. 4 shows the corresponding communication network connecting the five DERs. DER 1 is chosen as the pinned DER with access to the reference frequency information, where the pinning gain is set as 1.

The total simulation time is 40 seconds. Initially, the total microgrid load is proportionally shared among the five DERs, which are operated at around 59.4 Hz. The proposed cross-layer resilient control strategy is activated at t = 10s. Also, the distributed control without the proposed cross-layer strategy in (2) is implemented as a comparison to illustrate the effects of FDI and DoS attacks on microgrid operations. Then, an additional load (180kW+18kVar) is connected to Bus 2 at t = 20s. Later, the two loads located at Buses 8 and 11 are curtailed at t = 30s. Here, both B_η and C are set as identity matrices for simplicity.

In this section, there are four cases conducted, including:

1) Without cyberattacks;
2) Only FDI attacks;
3) Only DoS attacks;
4) Combined FDI and DoS attacks.

The four cases are discussed next.

A. Performance Under Normal Operations

When there are no cyberattacks, the performance of the proposed cross-layer resilient control strategy in case of load variations is presented in Fig. 5. Initially, the five loads are proportionally shared among the five DERs, which are operated around 59.4Hz. The proposed cross-layer resilient control strategy activated at t = 10s restores the DER frequencies to 60Hz without interrupting the proportional active power sharing. In the presence of load variations t = 20s and t = 30s, the five DERs readjust their active power outputs to mitigate the system power imbalance as their frequencies deviate from the rated value. With the proposed cross-layer resilient control strategy, the DER frequencies can be rapidly restored to the rated 60Hz while maintaining the proportional active power sharing among participating DERs, implying that the coordinated operations of DERs are achieved and the microgrid is ensured to be operated in the desired operating condition.

Fig. 6 shows the microgrid operation without cyberattacks when using the distributed control which does not consider the proposed cross-layer strategy stated in (2). When there are no cyberattacks, the distributed control without the proposed cross-layer strategy can also achieve the desired control objectives (i.e., frequency restoration and proportional active power sharing). But the corresponding convergence rate is significantly slower than that of the proposed cross-layer resilient control strategy, as shown in Figs. 5 and 6, which corroborates the theoretical analysis of (16).

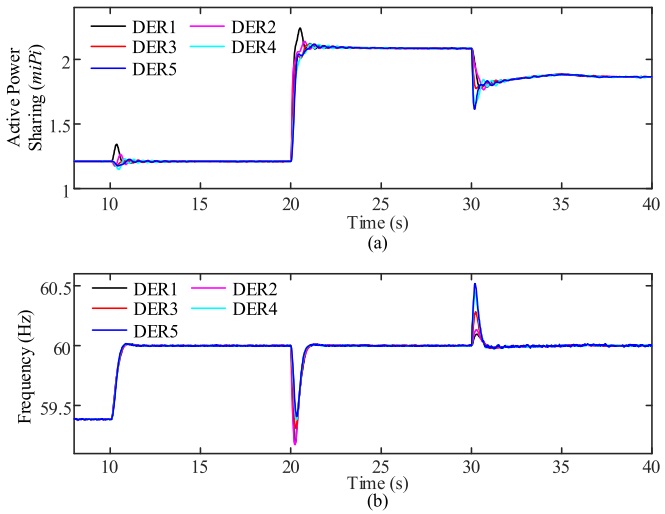

Fig. 5. Performance of the proposed cross-layer resilient control strategy under normal operations without cyberattacks: a) Active power sharing; b) Frequency.

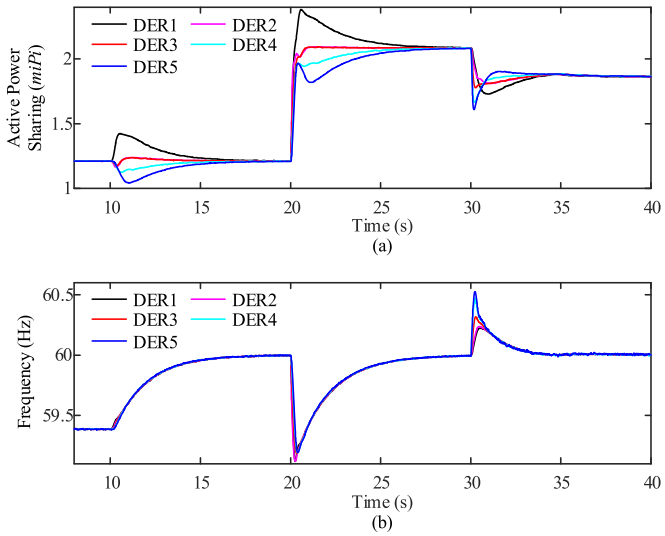

Fig. 6. Performance of the distributed control without the proposed cross-layer strategy under normal operations without cyberattacks: a) Active power sharing; b) Frequency.

B. Performance Against FDI Attacks

1) Impacts of FDI Attacks: In this case, DERs 2 and 4 are corrupted by FDI attacks modeled in (4) at t = 20s and t = 30s, respectively. Considering the adversaries have the full knowledge of the communication network, the Laplacian matrix is utilized by the adversaries to construct the FDI attack, where the elements of FDI attack matrix F in (4) are set as $(F)_{ij} = |(L_\omega)_{ij}|$. Then, for the attacked DERs 2 and 4, the FDI attacks are only composed of their neighbors' frequencies, which are difficult to be detected. Also, the FDI attack is assumed to be bounded by 5, i.e., $\|\boldsymbol{\mu}\|_{\max} \leq \bar{\mu} = 5$. First, we consider the scenario that the FDI attacks and load variations are occurred simultaneously, as shown in Figs. 7 and 8. When the FDI attacks and load variations occur simultaneously, the FDI attacks might be mistaken for normal disturbances and

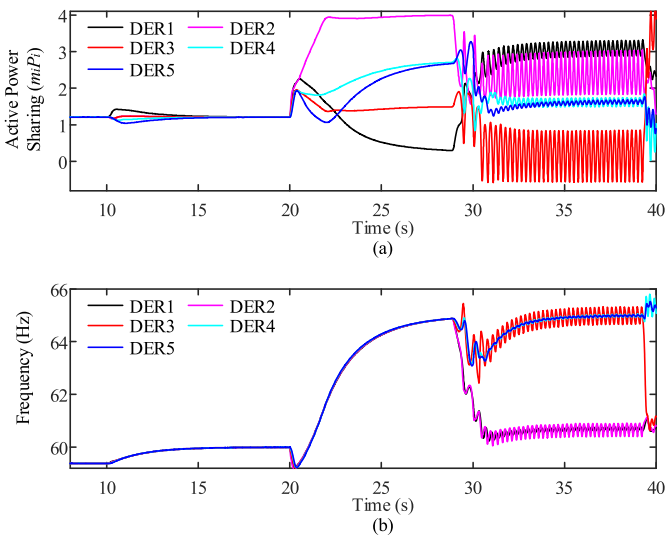

Fig. 7. Effects of FDI attacks on microgrid operation when using the distributed control without the proposed cross-layer strategy: a) Active power sharing; b) Frequency.

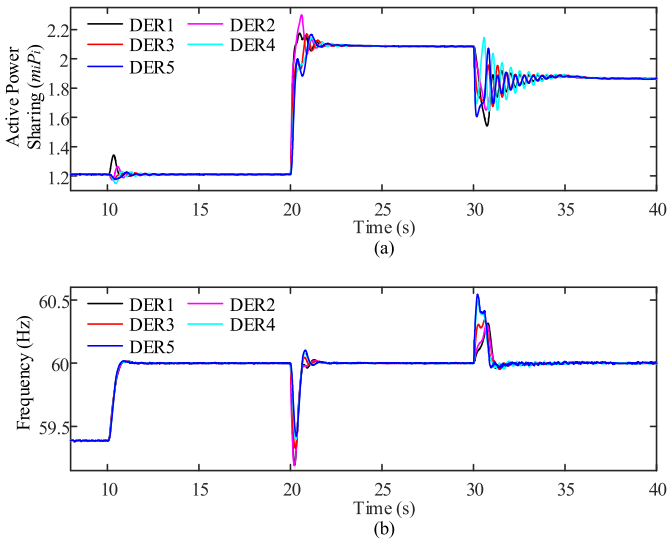

Fig. 8. Performance of the proposed cross-layer resilient control strategy against FDI attacks: a) Active power sharing; b) Frequency.

then easily bypass the conventional detection schemes. In addition, we consider a scenario that the microgrid system load is fixed (i.e., no load variations) for better illustrating the impacts of FDI attacks on microgrid operations, as shown in Figs. 9 and 10.

Fig. 7 shows the effects of FDI attacks on microgrid operation when using the distributed control without the proposed cross-layer strategy. In Fig. 7, DER frequency deviations are mitigated while proportional active power sharing among participating DERs is maintained after the distributed control without the proposed cross-layer strategy is implemented at t = 10s. Then, DER2 is corrupted by the FDI attack at t = 20s. In Fig. 7(a), the proportional active power sharing is interrupted due to the FDI attack, resulting in severe violations of DER active power ratings. In Fig. 7(b), DER frequencies diverge from the rated 60Hz. Later, the microgrid system performance is further deteriorated by the FDI attack imposed on DER4 at t = 30s, where DER active power sharing and frequencies start to oscillate significantly and the microgrid becomes unstable.

Fig. 8 shows the performance of the proposed cross-layer resilient control strategy against FDI attacks. After the proposed cross-layer resilient control strategy is implemented at t = 10s, the proportional active power sharing and the rated operating frequency of participating DERs are always maintained throughout the control process. The effects of FDI attacks at t = 20s and t = 30s are successfully mitigated by the proposed cross-layer resilient control strategy, which ensures the desired control performance after small oscillations.

In Fig. 9, when there are no load variations, the frequency restoration and proportional active power sharing are still interrupted by the FDI attacks occurred at t = 20s and t = 30s. Under such a scenario, the occurrence of FDI attacks might be easily noticed since there are no external disturbances happened. The DER states exhibit oscillatory behaviors, resulting in that the localization of corrupted components (i.e., attacked DERs 2 and 4), which is still a challenging task. Then, these corrupted components continue to mislead the microgrid operation until the system has collapsed. In Fig. 10, the proposed cross-layer resilient control strategy prevents the microgrid normal operation from being interrupted by FDI attacks, showing similar simulation results as those in Fig. 8.

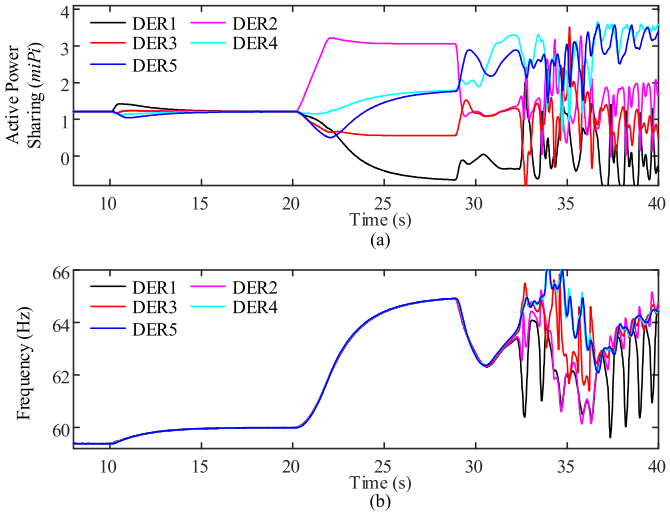

Fig. 9. Effects of FDI attacks on microgrid operation without load variations when the distributed control does not apply the proposed cross-layer strategy: a) Active power sharing; b) Frequency.

2) Impacts of FDI Attacks With a Large Bound: In this case, the FDI attack is set to be bounded by 10, i.e., $\|\boldsymbol{\mu}\|_{\max} \leq \bar{\mu} = 10$. In Fig. 11, the impacts of FDI attacks with a large bound are much more significant as compared with those in Fig. 7. In the presence of such FDI attacks, the distributed control without the proposed cross-layer strategy fails to maintain the rated frequency and the proportional active power sharing. Subsequently, the microgrid system collapses after significant oscillations. Such FDI attacks with a large bound might

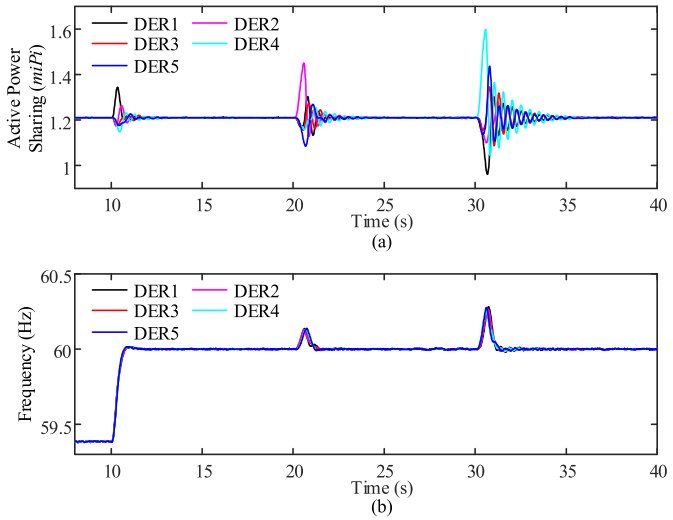

Fig. 10. Performance of the proposed cross-layer resilient control strategy against FDI attacks without load variations: a) Active power sharing; b) Frequency.

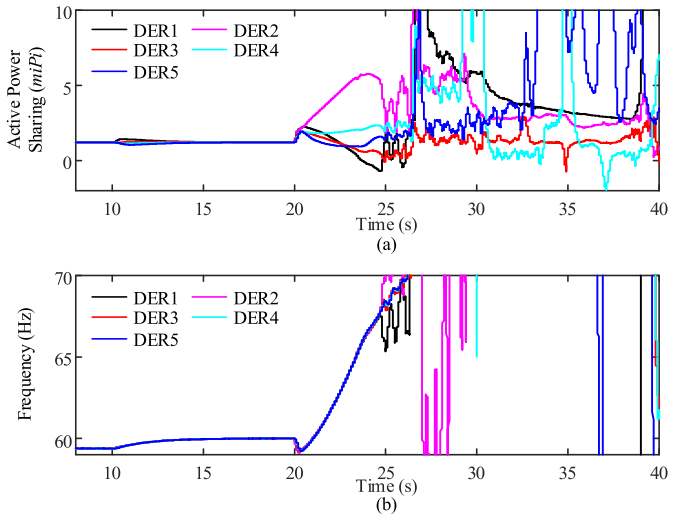

Fig. 11. Effects of FDI attacks with a large bound on microgrid operation when using the distributed control without the proposed cross-layer strategy: a) Active power sharing; b) Frequency.

be more easily detected by common cybersecurity defense schemes due to their abnormally large magnitudes.

Comparatively, in Fig. 12, the proposed cross-layer resilient control strategy is still capable of effectively mitigating the impacts of FDI attacks with a large bound, where the rated DER frequency and the proportional active power sharing among participating DERs are retained. But it is expected that the corresponding oscillatory behaviors in Fig. 12 are more significant than those in Fig. 8.

3) Impacts of FDI Attacks on Phase Information: In this case, after the load variations at t = 20s and t = 30s, the switch is scheduled to be opened at t = 60s and the microgrid will be divided into two sub-microgrids, as shown in Fig. 13. The phase information of Buses 4 and 6 can be used to regulate participating DERs for achieving a smooth reconfiguration operation [47]. At t = 50s, the communication links 1-3 and

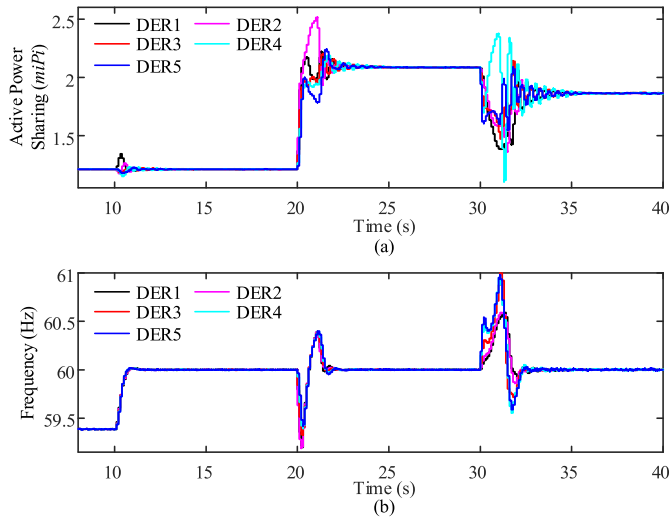

Fig. 12. Performance of the proposed cross-layer resilient control strategy against FDI attacks with a large bound: a) Active power sharing; b) Frequency.

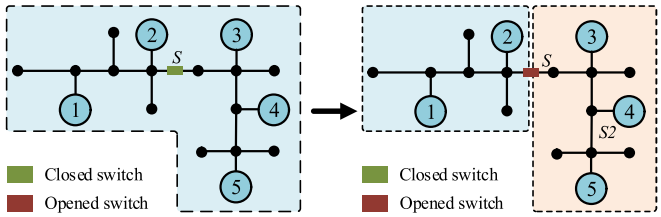

Fig. 13. Microgrid reconfiguration operation.

2-4 are disabled, and DERs 2 and 3 start to receive the reference frequency information and the phase information of Buses 4 and 6. DERs 2 and 3 will use the received phase information to regulate their power outputs for eliminating the power flow through the switch, and the three other DERs will follow DERs 2 and 3. Here, the phase information received by DERs 2 and 3 is corrupted by FDI attacks. In Fig. 14, the corrupted phase information cannot be addressed if we use the distributed control without the proposed cross-layer strategy, which would mislead the DER operations and introduce serious microgrid instability issues.

In Fig. 15(c), the active power flow from Bus 6 to Bus 4 could be regulated to zero regardless of the corrupted phase information. The two sub-microgrids could start to operate in parallel after t = 50s, where the DERs in the same sub-microgrid (e.g., DERs 1 and 2) have the same active power sharing while operating at the rated frequency. It implies that the corresponding effects of FDI attacks on phase information are effectively mitigated by the proposed cross-layer resilient control strategy, which ensures that the opening of switch S at t = 60s is a smooth reconfiguration operation without introducing any significant transients.

C. Performance Against DoS Attacks

In this case, the communication links 1-3 and 2-4 are disabled by DoS attack at t = 20s. Then, the communication network is partitioned into two isolated sub-networks. At

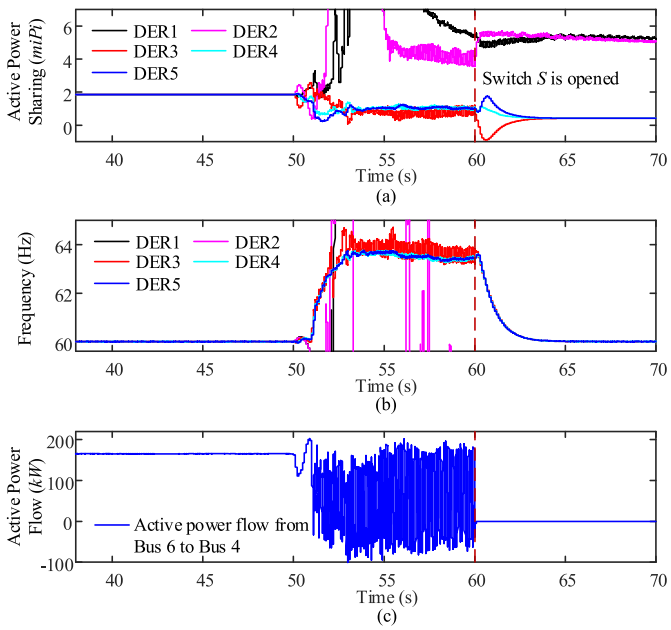

Fig. 14. Microgrid operation under FDI attacks on phase information when using the distributed control without the proposed cross-layer strategy: a) Active power sharing; b) Frequency; c) Active power flow through switch *S*.

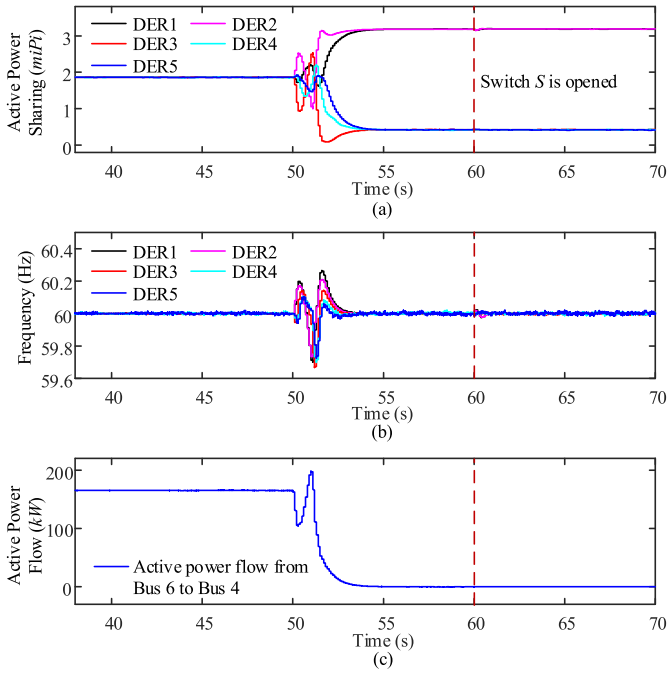

Fig. 15. Performance of the proposed cross-layer resilient control strategy against FDI attacks on phase information: a) Active power sharing; b) Frequency; c) Active power flow through switch *S*.

t = 30s, the pinning control signal is disabled by the DoS attack. Fig. 16 shows the effects of DoS attacks on microgrid operation when the distributed control without the proposed cross-layer strategy is applied. Fig. 17 shows the performance of the proposed cross-layer resilient control strategy under DoS attacks.

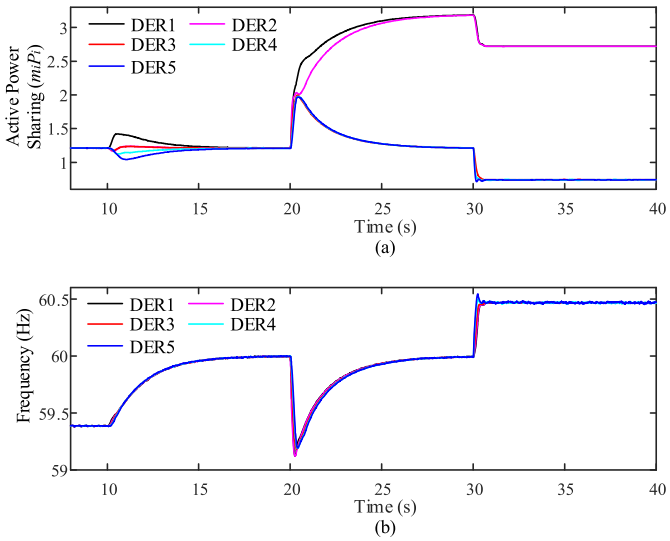

Fig. 16. Effects of DoS attacks on microgrid operation when using the distributed control without the proposed cross-layer strategy: a) Active power sharing; b) Frequency.

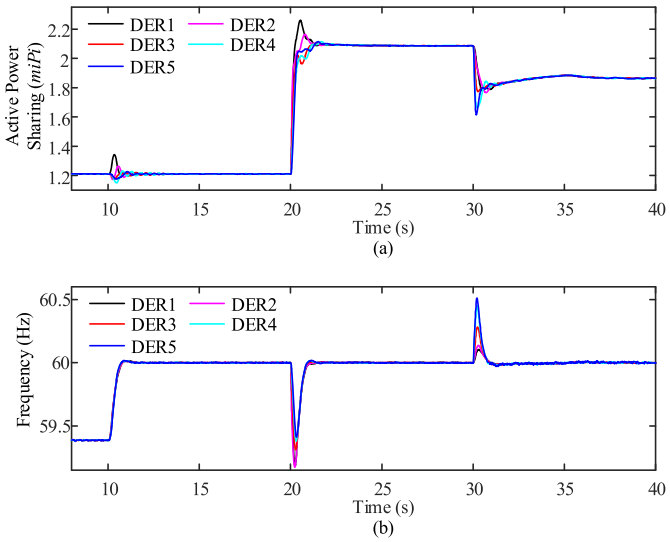

Fig. 17. Performance of the proposed cross-layer resilient control strategy against DoS attacks: a) Active power sharing; b) Frequency.

In Fig. 16, the proportional active power sharing is interrupted by the DoS attack at t = 20s, though DER frequencies are synchronized at the rated 60Hz. Here, the active power sharing of DERs 1 and 2 is different from that of DERs 3-5 due to the communication network partitioning caused by DoS attacks. Later, the pinning control signal imposed on DER1 is disabled by DoS attack, which implies that no DERs will have access to the reference frequency information. Accordingly, the distributed control without the proposed cross-layer strategy cannot mitigate DER frequency deviations. Then, DER frequencies diverge from the rated 60Hz and the proportional active power sharing is further disrupted. Figs. 7 and 16 show that the impacts of FDI attacks on microgrid operations are usually more serious than those of DoS attacks. In Fig. 17, DER frequencies are restored to the rated 60Hz while maintaining the proportional active power sharing regardless of DoS

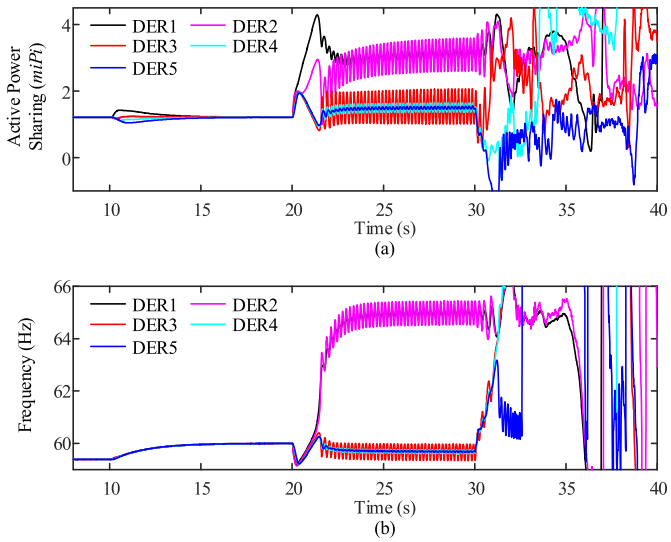

Fig. 18. Effects of combined attacks on microgrid operation when using the distributed control without the proposed cross-layer strategy: a) Active power sharing; b) Frequency.

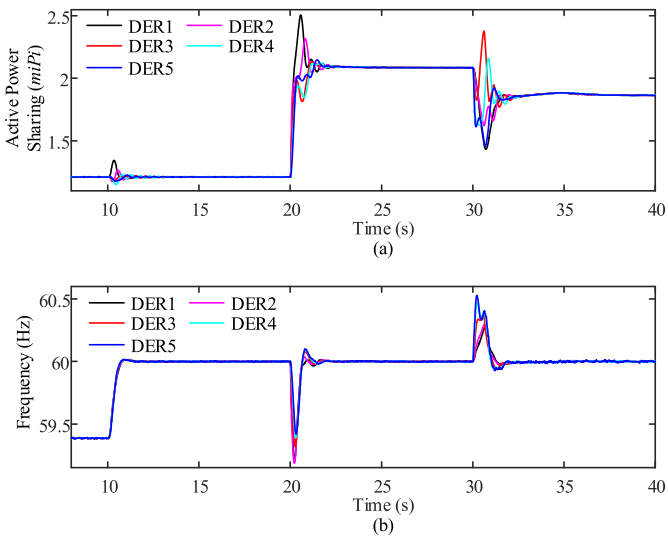

Fig. 19. Performance of the proposed cross-layer resilient control strategy against combined attacks: a) Active power sharing; b) Frequency.

attacks, which implies that the proposed cross-layer resilient control strategy can mitigate the effects of DoS attacks for maintaining the coordinated operations of DERs.

D. Performance Against Combined Attacks

In this case, DER1 as the only pinned DER is corrupted by the FDI attack at t = 20s. Meanwhile, the communication links 1-3 and 2-4 are disabled by the DoS attack at t = 20s. At t = 30s, DER3 is corrupted by the FDI attack, and the communication 4-5 is disabled by the DoS attack. Fig. 18 shows the effects of the combined FDI and DoS attacks on microgrid operation when the distributed control without the proposed cross-layer strategy is applied. Fig. 19 shows the performance of the proposed cross-layer resilient control strategy against such combined attacks.

In Fig. 18, DER active power sharing and frequencies exhibit oscillatory behaviors and fail to be synchronized due to the combined attack at t = 20s. The combined attack in Fig. 18 causes more serious effects on the microgrid operations, as compared with those of FDI or DoS attacks in Figs. 7 and 16. Later, DER frequencies and active power sharing fluctuate significantly due to the combined attack at t = 30s, which destabilizes the microgrid. In Fig. 19, the implemented cross-layer resilient control strategy drives the DER active power sharing to be identical while maintaining DER frequencies at the rated 60Hz, which validates the effectiveness of the proposed cross-layer resilient control strategy in coping with combined attacks.

In summary, FDI, DoS, and combined attacks can deteriorate the microgrid operations in terms of DER proportional active power sharing and frequency restoration, which might lead to violations of DER power ratings and microgrid instability, as shown in Figs. 7, 16, and 18. Comparatively, the effects of these cyberattacks can be mitigated by implementing the proposed cross-layer resilient control strategy, which ensures that the desired microgrid operating conditions can be maintained under cyberattacks, as shown in Figs. 8, 17, and 19. It is demonstrated that the proposed cross-layer resilient control strategy provides a viable solution against stealthy cyberattacks in islanded microgrids.

VI. Conclusion

The integration of communication and control infrastructure into microgrids has raised extensive concerns about potential cybersecurity threats with catastrophic consequences. Cybersecurity threat is emerging as a critical issue for microgrid operations, especially considering the increasing penetration of various DERs and the relatively low system inertia. In this paper, the vulnerability of microgrid operations to FDI and DoS attacks is theoretically analyzed when the conventional distributed control strategy is applied. A cross-layer resilient control strategy is proposed for islanded microgrids to cope with FDI and DoS attacks, where the coupled control and parallel control network layers cooperate to mitigate the effects of cyberattacks on microgrid operations. The stability of the proposed cross-layer resilient control strategy is demonstrated by using the Lyapunov theory considering different scenarios, including without and with FDI and DoS attacks.

Extensive case studies are conducted to validate the effectiveness of the proposed cross-layer resilient control strategy in terms of mitigating the effects of FDI, DoS, and combined attacks on microgrid operations. It is illustrated that the desired control performance can always be retained by the proposed control strategy irrespective of when and where these stealthy cyberattacks occur in microgrids. The proposed cross-layer resilient control strategy offers a promising solution to enhancing microgrid resilience against potential cybersecurity issues, which would promote the wide deployment of ICT integrated microgrids in the smart grid.

References

[1] J. Li, Y. Liu, and L. Wu, "Optimal operation for community-based multi-party microgrid in grid-connected and islanded modes," *IEEE Trans. Smart Grid*, vol. 9, no. 2, pp. 756–765, Mar. 2018.

[2] D. K. Molzahn *et al.*, "A survey of distributed optimization and control algorithms for electric power systems," *IEEE Trans. Smart Grid*, vol. 8, no. 6, pp. 2941–2962, Nov. 2017.

[3] F. Dörfler, J. W. Simpson-Porco, and F. Bullo, "Breaking the hierarchy: Distributed control and economic optimality in microgrids," *IEEE Trans. Control Netw. Syst.*, vol. 3, no. 3, pp. 241–253, Sep. 2016.

[4] X. Lyu, Y. Jia, and Z. Xu, "A novel control strategy for wind farm active power regulation considering wake interaction," *IEEE Trans. Sustain. Energy*, vol. 11, no. 2, pp. 618–628, Apr. 2020.

[5] X. Lyu, Y. Jia, Z. Xu, and J. Østergaard, "Mileage-responsive wind power smoothing," *IEEE Trans. Ind. Electron.*, vol. 67, no. 6, pp. 5209–5212, Jun. 2020.

[6] Q. Zhou, M. Shahidehpour, A. Paaso, S. Bahramirad, A. Abdulwhab, and A. Abusorrah, "Distributed control and communication strategies in networked microgrids," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 4, pp. 2586–2633, 4th Quart., 2020.

[7] Y. Xue, Z. Li, C. Lin, Q. Guo, and H. Sun, "Coordinated dispatch of integrated electric and district heating systems using heterogeneous decomposition," *IEEE Trans. Sustain. Energy*, vol. 11, no. 3, pp. 1495–1507, Jul. 2020.

[8] J. W. S. Porco, Q. Shafiee, F. Dörfler, J. C. Vasquez, J. M. Guerrero, and F. Bullo, "Secondary frequency and voltage control of islanded microgrids via distributed averaging," *IEEE Trans. Ind. Electron.*, vol. 62, no. 11, pp. 7025–7038, Nov. 2015.

[9] J. Schiffer, F. Dörfler, and E. Fridman, "Robustness of distributed averaging control in power systems: Time delays & dynamic communication topology," *Automatica*, vol. 80, pp. 261–271, Jun. 2017.

[10] M. Shi, X. Chen, J. Zhou, Y. Chen, J. Wen, and H. He, "PI-consensus based distributed control of AC microgrids," *IEEE Trans. Power Syst.*, vol. 35, no. 3, pp. 2268–2278, May 2020.

[11] L. Xu, Q. Guo, Z. Wang, and H. Sun, "Modeling of time-delayed distributed cyber-physical power systems for small-signal stability analysis," *IEEE Trans. Smart Grid*, early access, Jan. 18, 2021, doi: 10.1109/TSG.2021.3052303.

[12] Y. Khayat *et al.*, "On the secondary control architectures of AC microgrids: An overview," *IEEE Trans. Power Electron.*, vol. 35, no. 6, pp. 6482–6500, Jun. 2020.

[13] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 Ukraine blackout: Implications for false data injection attacks," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 3317–3318, Jul. 2017.

[14] C. Peng, H. Sun, M. Yang, and Y.-L. Wang, "A survey on security communication and control for smart grids under malicious cyber attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 49, no. 8, pp. 1554–1569, Aug. 2019.

[15] 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, Nov. 2013.

[16] 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.*, early access, Nov. 14, 2019, doi: 10.1109/JESTPE.2019.2953480.

[17] S. Abhinav, H. Modares, F. L. Lewis, F. Ferrese, and A. Davoudi, "Synchrony in networked microgrids under attacks," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 6731–6741, Nov. 2018.

[18] S. Li, Y. Yılmaz, and X. Wang, "Quickest detection of false data injection attack in wide-area smart grids," *IEEE Trans. Smart Grid*, vol. 6, no. 6, pp. 2725–2735, Nov. 2015.

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

[20] G. Chaojun, P. Jirutitijaroen, and M. Motani, "Detecting false data injection attacks in AC state estimation," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2476–2483, Sep. 2015.

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

[22] B. Li, T. Ding, C. Huang, J. Zhao, Y. Yang, and Y. Chen, "Detecting false data injection attacks against power system state estimation with fast go-decomposition approach," *IEEE Trans. Ind. Informat.*, vol. 15, no. 5, pp. 2892–2904, May 2019.

[23] B. Satchinandan and P. R. Kumar, "Dynamic watermarking: Active defense of networked cyber-physical systems," *Proc. IEEE*, vol. 105, no. 2, pp. 219–240, Feb. 2017.

[24] O. A. Beg, L. V. Nguyen, T. T. Johnson, and A. Davoudi, "Signal temporal logic-based attack detection in DC microgrids," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 3585–3595, Jul. 2019.

[25] Y. Wang, M. M. Amin, J. Fu, and H. B. Moussa, "A novel data analytical approach for false data injection cyber-physical attack mitigation in smart grids," *IEEE Access*, vol. 5, pp. 26022–26033, 2017.

[26] S. Ahmed, Y. Lee, S. Hyun, and I. Koo, "Unsupervised machine learning-based detection of covert data integrity assault in smart grid networks utilizing isolation forest," *IEEE Trans. Inf. Forensics Security*, vol. 14, pp. 2765–2777, 2019.

[27] M. N. Kurt, O. Ogundijo, C. Li, and X. Wang, "Online cyber-attack detection in smart grid: A reinforcement learning approach," *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 5174–5185, Sep. 2019.

[28] V. S. Dolk, P. Tesi, C. De Persis, and W. P. M. H. Heemels, "Event-triggered control systems under denial-of-service attacks," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 1, pp. 93–105, Mar. 2017.

[29] G. K. Befekadu, V. Gupta, and P. J. Antsaklis, "Risk-sensitive control under markov modulated denial-of-service (DoS) attack strategies," *IEEE Trans. Autom. Control*, vol. 60, no. 12, pp. 3299–3304, Dec. 2015.

[30] M. Chlela, D. Mascarella, G. Joós, and M. Kassouf, "Fallback control for isochronous energy storage systems in autonomous microgrids under denial-of-service cyber-attacks," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4702–4711, Sep. 2018.

[31] D. Zhang, L. Liu, and G. Feng, "Consensus of heterogeneous linear multiagent systems subject to aperiodic sampled-data and DoS attack," *IEEE Trans. Cybern.*, vol. 49, no. 4, pp. 1501–1511, Apr. 2019.

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

[33] P. Gope, J. Lee, and T. Q. S. Quek, "Resilience of DoS attacks in designing anonymous user authentication protocol for wireless sensor networks," *IEEE Sensors J.*, vol. 17, no. 2, pp. 498–503, Jan. 2017.

[34] S. Gao, Z. Peng, B. Xiao, A. Hu, and K. Ren, "FloodDefender: Protecting data and control plane resources under SDN-aimed DoS attacks," *Proc. IEEE INFOCOM*, May 2017, pp. 1–9.

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

[36] M. Agarwal, D. Pasumarthi, S. Biswas, and S. Nandi, "Machine learning approach for detection of flooding DoS attacks in 802.11 networks and attacker localization," *Int. J. Mach. Learn. Cybern.*, vol. 7, no. 6, pp. 1035–1051, Dec. 2016.

[37] N. Lyamin, D. Kleyko, Q. Delooz, and A. Vinel, "Real-time jamming DoS detection in safety-critical V2V C-ITS using data mining," *IEEE Commun. Lett.*, vol. 23, no. 3, pp. 442–445, Mar. 2019.

[38] S. Xu, Y. Qian, and R. Q. Hu, "Data-driven network intelligence for anomaly detection," *IEEE Netw.*, vol. 33, no. 3, pp. 88–95, May/Jun. 2019.

[39] A. S. Musleh, G. Chen, and Z. Y. Dong, "A survey on the detection algorithms for false data injection attacks in smart grids," *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2218–2234, May 2020.

[40] S. Sahoo, S. Mishra, J. C. Peng, and T. Dragičević, "A stealth cyber-attack detection strategy for DC microgrids," *IEEE Trans. Power Electron.*, vol. 34, no. 8, pp. 8162–8174, Aug. 2019.

[41] K. Pan, A. Teixeira, M. Cvetkovic, and P. Palensky, "Cyber risk analysis of combined data attacks against power system state estimation," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 3044–3056, May 2019.

[42] Q. Zhou, Z. Tian, M. Shahidehpour, X. Liu, A. Alabdulwahab, and A. Abusorrah, "Optimal consensus-based distributed control strategy for coordinated operation of networked microgrids," *IEEE Trans. Power Syst.*, vol. 35, no. 3, pp. 2452–2462, May 2020.

[43] Y. Li, Y. Qin, P. Zhang, and A. Herzberg, "SDN-enabled cyber-physical security in networked microgrids," *IEEE Trans. Sustain. Energy*, vol. 10, no. 3, pp. 1613–1622, Jul. 2019.

[44] Q. Zhou, M. Shahidehpour, M. Yan, X. Wu, A. Abdulwahab, and A. Abusorrah, "Distributed secondary control for islanded microgrids with mobile emergency resources," *IEEE Trans. Power Syst.*, vol. 35, no. 2, pp. 1389–1399, Mar. 2020.

[45] C. M. Kellett, "Classical converse theorems in Lyapunov's second method," *Discr. Continuous Dyn. Syst., Series B*, vol. 20, no. 8, pp. 2333–2360, Aug. 2015.

[46] Z. Deng, Y. Xu, H. Sun, and X. Shen, "Distributed, bounded and finite-time convergence secondary frequency control in an autonomous microgrid," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 2776–2788, May 2019.

[47] Y. Du, X. Lu, J. Wang, and S. Lukic, "Distributed secondary control strategy for microgrid operation with dynamic boundaries," *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 5269–5282, Sep. 2019.

Quan Zhou (Senior Member, IEEE) received the B.S. and M.S. degrees from the Department of Electrical Engineering, Shanghai Jiao Tong University, Shanghai, China, in 2011 and 2016, respectively, and the Ph.D. degree from the Illinois Institute of Technology, Chicago, IL, USA, in 2019. He is currently with Hunan University, and he is also a Senior Research Associate with the Robert W. Galvin Center for Electricity Innovation, Illinois Institute of Technology. His research interests include distributed control and communication, networked microgrids, cybersecurity, and smart cities.

Mohammad Shahidehpour (Life Fellow, IEEE) received the Honorary Doctorate degree in electrical engineering from the Polytechnic University of Bucharest, Bucharest, Romania. He is the Bodine Chair Professor and the Director of Robert W. Galvin Center for Electricity Innovation with IIT, Chicago, USA. He is a Fellow of the American Association for the Advancement of Science, National Academy of Inventors, a Laureate of Khwarizmi International Award, and an Elected Member of the U.S. National Academy of Engineering. He is listed on the Web of Science as a highly cited researcher.

Ahmed Alabdulwahab (Senior Member, IEEE) received the Ph.D. degree in electrical engineering from the University of Saskatchewan, Saskatoon, SK, Canada. He is a Professor with the Department of Electrical Engineering and Computer Engineering, King Abdulaziz University, Jeddah, Saudi Arabia. He is also the Dean with the Jeddah Community College.

Abdullah Abusorrah (Senior Member, IEEE) received the Ph.D. degree in electrical engineering from the University of Nottingham, Nottingham, U.K. He is currently a Professor with the Department of Electrical and Computer Engineering, King Abdulaziz University, Jeddah, Saudi Arabia, where he is also the Head of the Center for Renewable Energy and Power Systems. His interests include energy systems, smart grid, and system analyses.

Liang Che (Member, IEEE) received the B.S. degree in electrical engineering from Shanghai Jiaotong University, China, in 2006, and the Ph.D. degree in electrical engineering from the Illinois Institute of Technology, Chicago, IL, USA, in 2015. He was a Power System Planning Consultant with Siemens PTI, Minnetonka, MN, USA, from 2015 to 2016, and an EMS Engineer with Midcontinent Independent System Operator, Carmel, IN, USA, from 2017 to 2019. He is currently a Professor with the College of Electrical and Information Engineering, Hunan University, China.

Xuan Liu (Member, IEEE) received the B.S. and M.S. degrees in electrical engineering from Sichuan University, China, in 2008 and 2011, and the Ph.D. degree in electrical engineering from the Illinois Institute of Technology, Chicago, IL, USA, in 2015. He is currently a Professor with the College of Electrical and Information Engineering, Hunan University, China. His research interests include smart grid security, operation, and economics of power systems.