Article:
Sad Abadi, M.S., Sahoo, S. and Blaabjerg, F. (2022) Stability oriented design of cyber attack resilient controllers for cooperative DC microgrids. IEEE Transactions on Power Electronics, 37 (2). pp. 1310-1321. ISSN: 0885-8993

https://doi.org/10.1109/tpel.2021.3104721

Stability Oriented Design of Cyber Attack Resilient Controllers for Cooperative DC Microgrids

Mahdieh S. Sadabadi, *Member, IEEE*, Subham Sahoo, *Member, IEEE*, and Frede Blaabjerg, *Fellow, IEEE*

***Abstract*—Due to the importance of reliability and security in DC microgrids, it is essential to provide maximum resilience against cyber-attacks. However, insufficient global information in the microgrid makes it difficult to accurately identify the location of these attacks. To address these issues, this paper develops a novel resilient distributed control mechanism, which ensures average voltage regulation and proportional load sharing in DC microgrids under unknown cyber-attacks. The proposed resilient control design does not require any information regarding the nature or location of the attacks. By virtue of a graph theoretical approach and a Lyapunov-based framework, the proposed resilient distributed control strategy is designed in a way such that the system stability is always guaranteed following a comprehensive design mechanism. Finally, the robustness of the proposed resilient distributed control approach is demonstrated via simulations and validated by experimental results.**

***Index Terms*—DC microgrids, distributed control, resilient control, cyber-attack, stability analysis.**

I. Introduction

DISTRIBUTED control offers a promising solution for the control of Direct Current (DC) microgrids. They bring several advantages such as improved scalability, reliability, flexibility, and efficiency [1]. However, due to limited global information, they are prone to cyber-attacks, thereby affecting the stability and operation of DC microgrids. To accommodate privacy and security in DC microgrids, the resilience of distributed control algorithms against cyber threats need further improvement [2].

Recently there has been an increasing attention towards attack detection techniques and development of resilient distributed control algorithms. The main focus of the existing literature is devoted to attack detection and mitigation platform, where the misbehaving distribution generation (DG) units are detected, identified, and removed. O. Beg *et al.* in [3] have proposed a false data injection attack (FDIA) detection framework based on identifying a change in sets of inferred candidate invariants. Detection theories for detecting FDIAs on the current sensors, communication networks in the control architecture, as well as sensors and communication channels have been developed in [4], [5], and [6]. Several detection algorithms for different types of cyber-attacks such as denial-of-service (DoS) attacks [6], [7], stealth attack [8], [9], hijacking attacks [10], and man-in-the-middle (MITM) attacks [11] have been developed in the literature. Although these approaches propose various detection algorithms for detecting and/or mitigating the cyber-attacks, the limitations on the number of compromised DG units constrain their applicability for the case where most or all DG units are subject to cyber-attack. Furthermore, in these algorithms, the detection and mitigation of cyber-attacks must be fast, before the stability and performance of the microgrid is disrupted [9].

To deal with the above-mentioned challenges of the attack-detection techniques, the resilience to the malicious attacks should be considered as one of the main properties of the distributed control algorithms. Although extensive research has been carried out on the development of distributed control approaches for voltage regulation and current sharing in DC networks, e.g. [12], [13], the research on stability oriented resilience of the distributed control algorithms has still not been extensively explored. To the best of our knowledge, there exists a few approaches in the literature that solely consider the resilience property of the distributed control algorithms for DC microgrids in [14], [15]. These approaches aim to enhance the resilience of the distributed control algorithms such that DC microgrids operate as close to normal as possible while under cyber-attack. In [15], a secondary control in DC microgrids has been developed which is resilient against FDI attacks on the actuators. However, the proposed control strategy in [15] requires exchanging both current and voltage (estimate of the PCC voltages) of DG units amongst their neighbors, which increases the vulnerability of DC microgrids to cyber attacks on the communication links. Embedding the aforementioned discussions into future research efforts, it is essential to address the following concerns:

- Can a DC microgrid be uncompromised and stable at the same time?
- Is resilience feasible under worse case cyber intrusions?

Motivated by these points, this paper aims to design a resilient distributed control algorithm that steers DC microgrids as close as possible to their desired equilibrium and stability bounds regardless of the presence of any potential unknown cyber-attacks. In this paper, two types of cyber-attack are considered, which can compromise the system performance: (i) false data injection attacks, where the adversary injects false data to the actuators of DC-DC converters and/or transmitted data and (ii) man-in-the-middle attacks, which involve infiltrating the communicated information by a third party [11]. In contrast to the existing attack detection followed by mitigation

The work was supported by 2020-2021 National Productivity Investment Fund (NPIF). The preliminary results of this paper were presented at the European Control Conference 2021 (ECC'21).

M. S. Sadabadi is with the Department of Automatic Control and Systems Engineering, University of Sheffield, Sheffield, United Kingdom (e-mail: m.sadabadi@sheffield.ac.uk).

S. Sahoo and F. Blaabjerg are with the Department of Energy, Aalborg University, 9220 Aalborg, Denmark (e-mail: sssa@energy.aau.dk; fbl@energy.aau.dk).

approaches, the proposed distributed control technique in this paper does not require any information about the locations and nature of the cyber-attacks. In addition to the attack resilient property of the proposed distributed control technique, it works satisfactorily for other cyber-physical disturbances. A rigorous stability analysis based on a graph theoretical approach and the Lyapunov stability methods show that the proposed resilient control strategy guarantees overall stability of DC microgrids with DC-DC buck converters, which has been explained in detail through a comprehensive set of design guidelines. Finally, a unified design of a stability oriented cyber-attack resilient distributed controller has been designed for DC microgrids.

The rest of the paper is structured as follows. The model of DC microgrids is presented in Section II. The resilient design of distributed controllers in DC microgrids is proposed in Section III. Section IV is devoted to simulation and experimental results. Finally, the paper ends with concluding remarks in Section V.

Notation: Throughout this paper, $\mathbf{1}_n$ is an $n \times 1$ vector of ones, $\mathbf{0}_n$ is an $n \times 1$ zero vector, $\mathbf{I}_n$ is an $n \times n$ identity matrix, and $\mathbf{0}_{n\times m}$ is a zero matrix of dimension $n \times m$. The symbols X^T, X^+, $tr(X)$, $det(X)$, and $X = [x_{ij}]$ denote the transpose, the Moore Penrose inverse, trace, determinant of matrix X, and a matrix with entries $x_{i,j}$, respectively. Throughout the paper, $\mathrm{col}(x) = \begin{bmatrix} x_1^T & x_2^T & \dots & x_n^T \end{bmatrix}^T$ and $[a] = \mathrm{diag}(a_1, a_2, \dots, a_n)$. For a symmetric matrix X, the positive definite and positive semidefinite operators are respectively shown by $X \succ 0$ and $X \succeq 0$. We define the sets $\mathbb{R}_+ := \{x \in \mathbb{R} \ | x > 0\}$ and $\mathbb{R}_{\geq 0} := \{x \in \mathbb{R} \ | x \geq 0\}$.

Preliminaries: Let $\mathcal{L} \in \mathbb{R}^{n\times n}$ be a Laplacian matrix for a connected undirected graph. Then, $\mathcal{L} = \mathcal{L}^T$, $\mathcal{L}\mathbf{1}_n = \mathbf{0}_n$, and $\mathbf{1}_n^T\mathcal{L} = \mathbf{0}_n^T$ [16].

II. Cyber-Physical DC Microgrids

A. Modeling

Consider a DC microgrid consisting of n distributed generation (DG) units with DC-DC buck converters, which are physically connected via m distribution lines, as shown in Fig. 1(a). The dynamics of DG i connected to DG j via a distribution line can be described by the following equations:

$$\begin{aligned} L_i\dot{I}_i(t) &= -V_i(t) - r_iI_i(t) + u_i(t), \\ C_i\dot{V}_i(t) &= I_i(t) - Y_iV_i(t) - \mathcal{B}_{ij}I_{ij}(t), \\ L_{ij}\dot{I}_{ij}(t) &= -R_{ij}I_{ij}(t) + \mathcal{B}_{ij}(V_i(t) - V_j(t)), \end{aligned} \tag{1}$$

where $I_i(t)$, $V_i(t)$, $I_{ij}(t)$, and $u_i(t) = V_{dc,i}d_i(t)$ are the current of the power converter i, the voltage at the point of common coupling (PCC) i, the current of the distribution line connecting DG i to DG j, and the control input ($V_{dc,i}$ is the DC voltage of the input side of the converter i and $d_i(t)$ is the duty cycle of DC-DC converter i), respectively. (L_i, r_i, C_i) are the filter parameters of the DC-DC buck converter i, (R_{ij}, L_{ij}) are the parameters of the line, and Y_i is the load conductance of DG i. $\mathcal{B}_{ij}$ determines the direction of the line current $I_{ij}(t)$. $\mathcal{B}_{ij} = 1$ if line current leaves DG i; $\mathcal{B}_{ij} = -1$ if line current enters DG i; otherwise, $\mathcal{B}_{ij} = 0$. $\mathcal{B}$ is the incidence matrix of the graph.

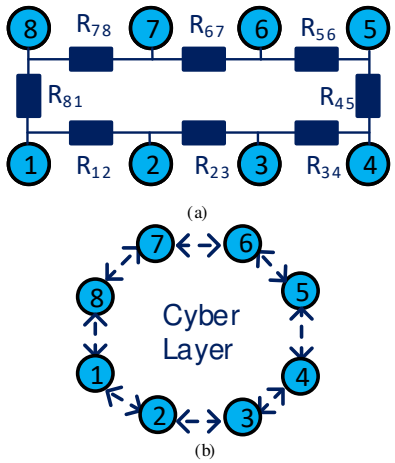

Fig. 1. Schematic of the (a) physical and (b) cyber layer of DC microgrid under study with eight DG units – the physical layer consists of n = 8 DGs (represented as a node) connected via distribution lines, whereas the cyber layer includes distributed control modules and communication links.

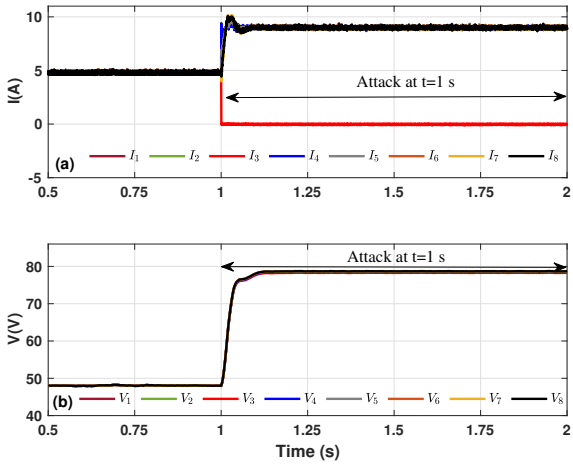

Fig. 2. Performance of distributed control in (5) in the presence of cyber-attack at $t = 1s$ for the microgrid in Fig. 1.

The physical layer of DC microgrids can be modeled by an undirected graph whose node set $\mathcal{V} = \{1, \dots, n\}$ and edge set $\mathcal{E} = \{1, \dots, m\}$ represent the DG units and the distribution lines, respectively.

B. cyber-attacks and their impact

The common control objectives in DC microgrids are current sharing and voltage regulation [9], [15] where the total load demand is proportionally shared amongst the DG units at the steady-state and the average voltage of the microgrid is regulated at a given reference setpoint V^*. These objectives are mathematically formulated here:

$$\frac{1}{I_i^s}\lim_{t\to\infty} I_i(t) = \frac{1}{I_j^s}\lim_{t\to\infty} I_j(t), \ i, j \in \mathcal{V} \tag{2}$$

$$\lim_{t\to\infty} \frac{1}{n}\sum_{i=1}^{n} V_i(t) = V^*, \tag{3}$$

where $I_i^s \in \mathbb{R}_+$ is the rated current of DG i.

The above control objectives can be achieved via a distributed control strategy. In this control setting, each converter transmits $I_i(t)$ and/or $V_i(t)$ to its neighboring DG units on a communication graph with an adjacency matrix $\mathcal{A} = [a_{ij}] \in \mathbb{R}^{n\times n}$. The Laplacian matrix of the undirected graph is presented by $\mathcal{L} = \mathcal{D} - \mathcal{A}$, where $\mathcal{D}$ is degree matrix presenting the incoming information to each node [16]. Using the cyber graph topology as shown in Fig. 1(b), the information is transmitted between the neighboring DG units.

To achieve the control objectives in (2) and (3), [17] proposes the following distributed averaging controller:

$$\begin{aligned} \mathbf{u}(t) &= \mathbf{1}_n V^* - [\alpha]\left(\mathbf{I}(t) - \phi(t)\right) + W\mathcal{L}^T\theta(t), \\ [T_\theta]\,\dot{\theta}(t) &= -\mathcal{L}W\mathbf{I}(t), \\ [T_\phi]\,\dot{\phi}(t) &= -\phi(t) + \mathbf{I}(t), \end{aligned} \tag{4}$$

where $[T_\theta] \succ 0$, $[T_\phi] \succ 0$, $[\alpha] \succ 0$, $\mathbf{u}(t) = \mathrm{col}(u(t))$, $\mathbf{I}(t) = \mathrm{col}(I(t))$, $W = \mathrm{diag}(\frac{1}{I^s})$, and $\mathcal{L} \in \mathbb{R}^{n\times n}$ is a Laplacian matrix associated with a connected undirected communication graph. $\theta(t) \in \mathbb{R}^n$ (in [V]) and $\phi(t) \in \mathbb{R}^n$ (in [A]) are the states of the distributed controller.

The distributed control systems are subject to cyber-attacks. In this paper, we specifically consider two types of attacks: (i) false data injection (FDI) attacks where attackers distort control input channels by injecting false data and (ii) man-in-the-middle (MITM) attacks involving infiltrating the communicated information by a third party [11]. In this paper, we assume that FDI attacks are only on control input channels.

The distributed control (4) under these attacks can be written as follows:

$$\begin{aligned} \mathbf{u}(t) =& \mathbf{1}_n V^* - \alpha\left(\mathbf{I}(t) - \phi(t)\right) + W\mathcal{L}^T(\theta(t) + \mathbf{d}_1(t)) + \Delta\mathbf{u}(t) \\ [T_\theta]\,\dot{\theta}(t) &= -\mathcal{L}W\left(\mathbf{I}(t) + \mathbf{d}_2(t)\right), \\ [T_\phi]\,\dot{\phi}(t) &= -\phi(t) + \mathbf{I}(t), \end{aligned} \tag{5}$$

where $\Delta\mathbf{u}(t) \in \mathbb{R}^n$, $\mathbf{d}_1(t) \in \mathbb{R}^n$, and $\mathbf{d}_2(t) \in \mathbb{R}^n$ represent the attack vectors.

In Fig. 2, it can easily be shown that for a DC microgrid with n = 8 DG units the voltage regulation and current sharing objectives in (2) and (3) are no longer achieved by using the distributed control in (4) in the presence of cyber-attacks. At $t = 1s$, DG 3 is subject to bounded attacks $\Delta\mathbf{u}(t)$, $\mathbf{d}_1(t)$, and $\mathbf{d}_2(t)$. The cyber-physical architecture of the considered DC microgrid is shown in Fig. 1. As it can be seen in Fig. 2, the existence of such attacks at $t = 1s$ leads to non-zero offsets in PCC voltages; furthermore, the load current is no longer proportionally shared amongst the DG units. Therefore, it is essential to develop an attack-resilient distributed control mechanism for DC microgrids so that the effects of the cyber-attacks on the voltage regulation and proportional current sharing are mitigated. At the same time, it is important to prevent the system from unbounded attacks.

III. Resilient Distributed Control in Microgrids

This section details out the design of a distributed resilient control strategy for DC microgrids which are subject to the aforementioned cyber-attacks. It will be shown that the states of DC microgrids equipped with the proposed distributed control remain bounded when attacks occur. Moreover, the control objectives in (2) and (3) are guaranteed following the proper design of control parameters.

We propose the following distributed control strategy composed of n nodes, where each node corresponds to a DG unit. The dynamics of node i are given as follows:

$$\begin{aligned} u_i(t) &= k_{1,i}V_i(t) + k_{2,i}I_i(t) + k_{3,i}v_i(t) \\ &\quad + k_{4,i}\sum_{j\in N_i}\eta_{i,j}\left(\frac{I_i(t)}{I_i^s} - \frac{I_j(t)}{I_j^s}\right) \\ &\quad + k_{5,i}\gamma\sum_{j\in N_i}\eta_{i,j}\left(\theta_i(t) - \theta_j(t)\right) + k_{6,i}\left(I_i(t) - \phi_i(t)\right), \\ T_{v_i}\dot{v}_i(t) &= \frac{\beta}{I_i^s}\left(-V_i(t) + V^*\right) + \frac{\gamma\beta}{I_i^s}\sum_{j\in N_i}\eta_{i,j}\left(\theta_i(t) - \theta_j(t)\right) \\ &\quad - \frac{\alpha_i\beta}{I_i^s}\left(I_i(t) - \phi_i(t)\right) - \frac{K\beta}{I_i^s}\sum_{j\in N_i}\eta_{i,j}\left(\frac{I_i(t)}{I_i^s} - \frac{I_j(t)}{I_j^s}\right), \\ T_{\theta_i}\dot{\theta}_i(t) &= -\gamma\sum_{j\in N_i}\eta_{i,j}\left(\frac{I_i(t)}{I_i^s} - \frac{I_j(t)}{I_j^s}\right) - \sum_{j\in N_i}\eta_{i,j}\left(\theta_i(t) - \theta_j(t)\right), \\ T_{\phi_i}\dot{\phi}_i(t) &= -\phi_i(t) + I_i(t), \end{aligned} \tag{6}$$

where $v_i(t)$, $\theta_i(t)$, and $\phi_i(t)$ are the states of the controller. In (6), N_i is the set of neighboring DG units of DG i, $T_{\theta_i} \in \mathbb{R}_+$, $T_{\phi_i} \in \mathbb{R}_+$, $T_{v_i} \in \mathbb{R}_+$, $K \in \mathbb{R}_+$, $\gamma \in \mathbb{R}_+$, $\alpha_i \in \mathbb{R}_+$, $\beta \in \mathbb{R}_+$, and $\eta_{i,j} \in \mathbb{R}_+$. The gain parameters $k_{j,i}$, $j = 1,\ldots,6$ and $i = 1,\ldots,n$, affect the stability and performance of DC microgrids. The control structure for each DG has been shown in Fig. 3. The control parameters can be designed based on the design criteria using Theorem 1 in Subsection III-A.

Assumption 1. *It is assumed that the undirected communication graph in the distributed controller in (6) is connected.*

The dynamics of cyber-physical DC microgrids under the potential FDI and MITM attacks are described by the following dynamic equations:

$$\begin{aligned} [C]\,\dot{\mathbf{V}}(t) &= \mathbf{I}(t) - [Y]\,\mathbf{V}(t) - \mathcal{B}\mathbf{I}_l(t), \\ [L_l]\,\dot{\mathbf{I}}_l(t) &= -[R_l]\,\mathbf{I}_l(t) + \mathcal{B}^T\mathbf{V}(t), \\ [L]\,\dot{\mathbf{I}}(t) &= \left([k_1] - \mathbf{I}_n\right)\mathbf{V}(t) + \left([k_2] - [r]\right)\mathbf{I}(t) + [k_3]\,\mathbf{v}(t) \\ &\quad + [k_4]\,\mathcal{L}W\left(\mathbf{I}(t) + \mathbf{d}_2(t)\right) + \gamma\,[k_5]\,\mathcal{L}^T\left(\theta(t) + \mathbf{d}_1(t)\right) \\ &\quad + [k_6]\left(\mathbf{I}(t) - \phi(t)\right) + \mathbf{d}_5(t), \\ [T_v]\,\dot{\mathbf{v}}(t) &= -\beta W\left(\mathbf{V}(t) - \mathbf{1}_n V^*\right) - K\beta W\mathcal{L}W\left(\mathbf{I}(t) + \mathbf{d}_2(t)\right) \\ &\quad - W\,[\alpha]\beta\left(\mathbf{I}(t) - \phi(t)\right) + \gamma\beta W\mathcal{L}^T\left(\theta(t) + \mathbf{d}_1(t)\right) + \mathbf{d}_3(t), \\ [T_\theta]\,\dot{\theta}(t) &= -\mathcal{L}\left(\theta(t) + \gamma W\mathbf{I}(t) + \mathbf{d}_4(t)\right), \\ [T_\phi]\,\dot{\phi}(t) &= -\phi(t) + \mathbf{I}(t), \end{aligned} \tag{7}$$

where $\mathbf{V}(t) = \mathrm{col}(V(t))$, $\mathbf{I}(t) = \mathrm{col}(I(t))$, $\mathbf{v}(t) = \mathrm{col}(v(t))$, $\phi(t) = \mathrm{col}(\phi(t))$, $\theta(t) = \mathrm{col}(\theta(t))$, $\mathbf{I}_l(t)$ is a vector of line currents, and $\mathbf{d}_k(t) \in \mathbb{R}^n$, $k = 1,\ldots,5$, denote the attack vectors. $[L_l]$ and $[R_l]$ are diagonal matrices whose diagonal elements are the line inductance and resistance values, respectively. In (7), $\mathbf{d}_k(t) \in \mathbb{R}^n$, $k = 1,\ldots,4$, represent the effects of MITM attacks on communication links whereas $\mathbf{d}_5(t) \in \mathbb{R}^n$ represents the existence of FDI attacks on control input channels (actuators). Fig. 4 shows the block diagram of the DC microgrid controlled by the cooperative resilient distributed

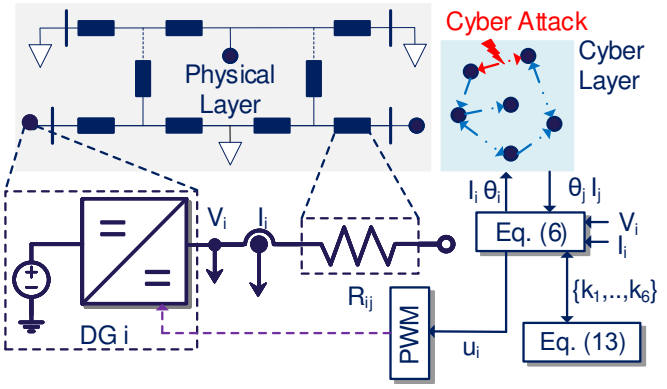

Fig. 3. A networked DC microgrid with n DG units operating with a distributed cyber graph, equipped with the proposed distributed control scheme in (6).

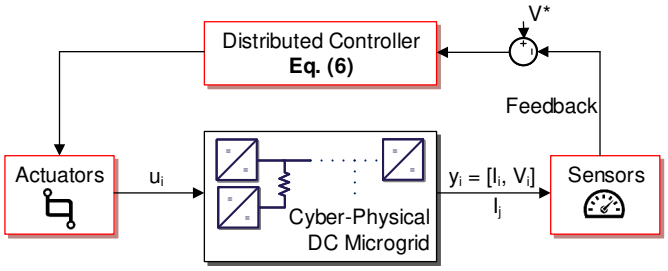

Fig. 4. Block diagram of the cooperatively controlled DC microgrid – The blocks highlighted with red indicate the attack vulnerable sections.

controller in (6). The figure highlights the vulnerable areas of the cooperatively controlled DC microgrid to cyber-attacks that includes sensors, actuators, and communication channels.

Assumption 2. *It is assumed that the attack vectors* $\mathbf{d}_k(t)$, $k = 1,\dots,5$ *are uniformly bounded, i.e.,* $\|\mathbf{d}_k(t)\| \leq \delta_k$, $\forall t \geq 0$.

Assumption 2 is reasonable from a practical perspective, since any intelligent attacker would aim at destabilizing distributed control systems with a bounded injection to avoid the attack detection. In the case of unbounded attacks, a defensive mechanism, called bad data detection, can be used. In the bad data detection mechanism, excessively large values received at each control node are rejected/filtered by applying a threshold-based defensive protocol proposed in [18]. To this end, a compact set Ω is defined for all feasible values of exchanged variables. If a received state variable at each node belongs to Ω, it will be accepted. Otherwise, it will be removed or filtered. The bad data detection mechanism can be incorporated before applying the proposed resilient control strategy.

The cyber-physical DC microgrids in (7) can be considered as a perturbed linear system, where $\mathbf{d}_k(t)$, $k = 1,\dots,5$ depict the perturbation terms. To ensure the stability of the perturbed microgrid under unknown bounded cyber-attacks, $[k_q]$ with $q = 1,\dots,6$ in (7) need to be designed following a certain policy. This will be explained in details in the next subsection.

A. Stability analysis

The stability analysis of the cyber-physical DC microgrids in (7) is discussed in Theorem 1.

For the cyber-physical DC microgrid in (7), the error vector $\tilde{x}(t) = x(t) - \bar{x}$ and $\tilde{d}(t)$ are defined, where

$$\begin{aligned} x(t) &= \left[\mathbf{V}^T(t), \mathbf{I}^T(t), \mathbf{I}_l^T(t), \mathbf{v}^T(t), \theta^T(t), \phi^T(t)\right]^T, \\ \tilde{d}(t) &= \left[\mathbf{d}_1^T(t), \mathbf{d}_2^T(t), \mathbf{d}_3^T(t), \mathbf{d}_4^T(t), \mathbf{d}_5^T(t)\right]^T, \end{aligned} \tag{8}$$

and

$$\bar{x} = \left[\bar{\mathbf{V}}^T, \bar{\mathbf{I}}^T, \bar{\mathbf{I}}_l^T, \bar{\mathbf{v}}^T, \bar{\theta}^T, \bar{\phi}^T\right]^T, \tag{9}$$

are the equilibria of (7) for the case where $\tilde{d}(t) = 0$. The equilibria $\bar{x}$ can be obtained as follows (see Lemma 2 in Appendix B):

$$\begin{aligned} \bar{\mathbf{V}} &= \Delta V^+ \begin{bmatrix} \frac{\sigma_W W^{-1}\mathcal{L}^+(\mathbf{1}_n V^*)}{(K+\gamma^2)} \\ \mathbf{1}_n^T V^* \end{bmatrix}, \\ \bar{\mathbf{I}} &= \left([Y] + \mathcal{B}\,[R_l]^{-1}\,\mathcal{B}^T\right)\bar{\mathbf{V}}, \\ \bar{\mathbf{I}}_l &= [R_l]^{-1}\,\mathcal{B}^T\bar{\mathbf{V}}, \\ \bar{\mathbf{v}} &= [k_3]^{-1}([1-k_1]\,\bar{\mathbf{V}} + ([r]-[k_2]-[k_4]\,\mathcal{L}W)\,\bar{\mathbf{I}} - \gamma\,[k_5]\,\mathcal{L}^T\bar{\theta}) \\ \bar{\theta} &= \mathbf{1}_n\theta^* - \gamma W\bar{\mathbf{I}}, \\ \bar{\phi} &= \bar{\mathbf{I}}, \end{aligned} \tag{10}$$

where

$$\begin{aligned} \sigma_W &= \mathbf{I}_n - W^{-1}\mathbf{1}_n\left(\mathbf{1}_n^T W^{-1}\mathbf{1}_n\right)^{-1}\mathbf{1}_n^T, \\ \theta^* &= \frac{\mathbf{1}_n^T\,[T_\theta]^{-1}}{\mathbf{1}_n^T\,[T_\theta]^{-1}\,\mathbf{1}_n}\left(\theta(0) + \gamma W\bar{\mathbf{I}}\right), \\ \Delta V &= \begin{bmatrix} \mathcal{B}\,[R_l]^{-1}\,\mathcal{B}^T + \sigma_W\,[Y] + \frac{\sigma_W W^{-1}\mathcal{L}^+ W^{-1}}{(K+\gamma^2)} \\ \mathbf{1}_n^T \end{bmatrix}. \end{aligned} \tag{11}$$

The dynamics of the error system are represented by:

$$\dot{\tilde{x}}(t) = \mathbf{A}\tilde{x}(t) + \mathbf{B}\tilde{d}(t), \tag{12}$$

where $\mathbf{A}$ and $\mathbf{B}$ are defined by (34) in Appendix A. As one can observe from the above equation, the term $\tilde{d}(t)$ appears as perturbations in the linear dynamics (12). Therefore, in order to show the stability of the cyber-physical DC microgrid in (7), it is sufficient to show that $\mathbf{A}$ in (12) is a Hurwitz matrix. Note that $\tilde{d}(t)$ does not depend on $\tilde{x}(t)$.

The following theorem illustrates the input-to-state stability (ISS) of the cyber-physical microgrid in (7). As a result of ISS, the states $x(t)$ in (7)-(8) are uniformly bounded under all the potential bounded attacks $\mathbf{d}_i(t)$, $i = 1,\dots,5$.

Theorem 1. *Let's assume that the communication graph associated with* $\mathcal{L}$ *in (7) is connected. If* $K \in \mathbb{R}_+$, $\gamma \in \mathbb{R}_+$, $\beta \in \mathbb{R}_+$, $[\alpha] \succ 0$, $[T_v] \succ 0$, $[T_\theta] \succ 0$, $[T_\phi] \succ 0$, *and* $k_{j,i}$, *for* $i \in \mathcal{V}$ *and* $j = 1,\dots,6$, *belongs to the following set:*

$$\mathcal{Z}_{[i]} = \left\{ \begin{array}{l} k_{1,i} < 1, \quad k_{2,i} < r_i, \\ 0 < k_{3,i} < \dfrac{T_{v_i}}{\beta L_i}\,(1-k_{1,i})\,(r_i - k_{2,i}), \\ k_{4,i} = -\dfrac{K}{I_i^s}(1-k_{1,i}), \;\; k_{5,i} = \dfrac{1}{I_i^s}(1-k_{1,i}) \\ k_{6,i} = \alpha_i(k_{1,i}-1) \end{array} \right\}. \tag{13}$$

then, the matrix $\mathbf{A}$ *in (34) (see Appendix A) is Hurwitz.*

Proof. Let $\tilde{d}(t) = 0$ in (12). Then, it is sufficient to show that the origin in (12) is globally asymptotically stable. To this end, we consider the following Lyapunov function:

$$\mathcal{V}(\tilde{x}) = \frac{1}{2}\tilde{V}^T(t)\,[C]\,\tilde{V}(t) + \frac{1}{2}\tilde{I}_l^T(t)\,[L_l]\,\tilde{I}_l(t) + \frac{1}{2}\tilde{\theta}^T(t)\,[T_\theta]\,\tilde{\theta}(t) + \frac{1}{2}\tilde{\phi}^T(t)\,[\alpha]\,[T_\phi]\,\tilde{\phi}(t) + \frac{1}{2}\sum_{i=1}^{n}\left[\tilde{I}_i(t)\ \tilde{v}_i(t)\right]P_i\left[\tilde{I}_i(t)\ \tilde{v}_i(t)\right]^T, \tag{14}$$

where $\tilde{V}(t) = \mathbf{V}(t) - \bar{\mathbf{V}}$, $\tilde{I}(t) = \mathbf{I}(t) - \bar{\mathbf{I}}$, $\tilde{I}_l(t) = \mathbf{I}_l(t) - \bar{\mathbf{I}}_l$, $\tilde{\theta}(t) = \theta(t) - \bar{\theta}$, $\tilde{\phi}(t) = \phi(t) - \bar{\phi}$, and $\tilde{v}(t) = \mathbf{v}(t) - \bar{\mathbf{v}}$. Matrix P_i in (14) is defined as follows:

$$P_i = \begin{bmatrix} L_i\rho_i & -\beta\frac{L_i}{T_{v_i}}\rho_i\omega_i \\ -\beta\frac{L_i}{T_{v_i}}\rho_i\omega_i & \omega_i\left(1+\beta^2\frac{L_i}{T_{v_i}^2}\rho_i\omega_i\right) \end{bmatrix}, \tag{15}$$

where $\rho_i \in \mathbb{R}_+$ and $\omega_i \in \mathbb{R}_+$ are determined based on any values of $(k_{1,i}, k_{2,i}, k_{3,i}, T_{v_i})$ in $\mathcal{Z}_{[i]}$ given in (13) as follows:

$$\begin{aligned} \rho_i &= \frac{(r_i - k_{2,i})}{(r_i - k_{2,i})(1-k_{1,i}) - \beta\frac{L_i}{T_{v_i}}k_{3,i}}, \\ \omega_i &= T_{v_i}\frac{k_{3,i}}{\beta(r_i - k_{2,i})}. \end{aligned} \tag{16}$$

Note that $P_i \in \mathbb{R}^{2\times 2}$, $tr(P_i) > 0$, and $det(P_i) = L_i\rho_i\omega_i > 0$, hence $P_i \succ 0$. The time derivative of $\mathcal{V}(\tilde{x})$ in (14) along the trajectories (12) is expressed as follows:

$$\begin{aligned} \dot{\mathcal{V}}(\tilde{x}) = {} & \frac{1}{2}\left(\tilde{V}^T\tilde{I} + \tilde{I}^T\tilde{V} - \tilde{V}^T\mathcal{B}\tilde{I}_l - \tilde{I}_l^T\mathcal{B}^T\tilde{V}\right) - \tilde{V}^T\,[Y]\,\tilde{V} \\ & + \frac{1}{2}\left(\tilde{I}_l^T\mathcal{B}^T\tilde{V} + \tilde{V}^T\mathcal{B}\tilde{I}_l\right) - \tilde{I}_l^T\,[R_l]\,\tilde{I}_l \\ & - \frac{1}{2}\tilde{\theta}^T(\mathcal{L}+\mathcal{L}^T)\tilde{\theta} - \frac{\gamma}{2}\left(\tilde{\theta}^T\mathcal{L}W\tilde{I} + \tilde{I}^TW\mathcal{L}^T\tilde{\theta}\right) \\ & + \frac{1}{2}\left(\tilde{\phi}^T\,[\alpha]\left(-\tilde{\phi}+\tilde{I}\right) + \left(-\tilde{\phi}+\tilde{I}\right)^T\,[\alpha]\,\tilde{\phi}\right) \\ & + \frac{1}{2}\sum_{i=1}^{n}\left[\tilde{I}_i\ \tilde{v}_i\right]Q_i\left[\tilde{I}_i\ \tilde{v}_i\right]^T \\ & + \frac{1}{2}\sum_{i=1}^{n}\left(\left[\tilde{I}_i\ \tilde{v}_i\right]P_iB_{V_i}\tilde{v}_i + \tilde{v}_iB_{V_i}^TP_i\left[\tilde{I}_i\ \tilde{v}_i\right]^T\right) \\ & + \frac{1}{2}\sum_{i=1}^{n}\left(\left[\tilde{I}_i\ \tilde{v}_i\right]P_iB_{\phi_i}\left(-\tilde{\phi}_i+\tilde{I}_i\right)\right) \\ & + \frac{1}{2}\sum_{i=1}^{n}\left(\left(-\tilde{\phi}_i+\tilde{I}_i\right)B_{\phi_i}^TP_i\left[\tilde{I}_i\ \tilde{v}_i\right]^T\right) \\ & + \frac{1}{2}\sum_{i=1}^{n}\left(\left[\tilde{I}_i\ \tilde{v}_i\right]P_iB_{\theta_i}\sum_{j=1}^{n}\eta_{i,j}\left(\tilde{\theta}_i(t)-\tilde{\theta}_j(t)\right)\right) \\ & + \frac{1}{2}\sum_{i=1}^{n}\left(\sum_{j=1}^{n}\eta_{i,j}\left(\tilde{\theta}_i(t)-\tilde{\theta}_j(t)\right)B_{\theta_i}^TP_i\left[\tilde{I}_i\ \tilde{v}_i\right]^T\right) \\ & + \frac{1}{2}\sum_{i=1}^{n}\left[\tilde{I}_i\ \tilde{v}_i\right]P_iB_{I_i}\sum_{j=1}^{n}\eta_{i,j}\left(\frac{I_i(t)}{I_i^s}-\frac{I_j(t)}{I_j^s}\right) \\ & + \frac{1}{2}\sum_{i=1}^{n}\sum_{j=1}^{n}\eta_{i,j}\left(\frac{I_i(t)}{I_i^s}-\frac{I_j(t)}{I_j^s}\right)B_{I_i}^TP_i\left[\tilde{I}_i\ \tilde{v}_i\right]^T, \end{aligned} \tag{17}$$

where

$$\begin{aligned} Q_i &= P_i\begin{bmatrix}\frac{k_{2,i}-r_i}{L_i} & \frac{k_{3,i}}{L_i}\\ 0 & 0\end{bmatrix} + \begin{bmatrix}\frac{k_{2,i}-r_i}{L_i} & \frac{k_{3,i}}{L_i}\\ 0 & 0\end{bmatrix}^TP_i, \\ B_{V_i} &= \begin{bmatrix}\frac{k_{1,i}-1}{L_i}\\ \frac{-\beta}{T_{v_i}I_i^s}\end{bmatrix},\ B_{\phi_i} = \begin{bmatrix}\frac{k_{6,i}}{L_i}\\ \frac{-\alpha_i\beta}{I_i^sT_{v_i}}\end{bmatrix}, \\ B_{\theta_i} &= \gamma\begin{bmatrix}\frac{k_{5,i}}{L_i}\\ \frac{\beta}{I_i^sT_{v_i}}\end{bmatrix},\ B_{I_i} = \begin{bmatrix}\frac{k_{4,i}}{L_i}\\ -\beta\frac{K}{I_i^sT_{v_i}}\end{bmatrix}. \end{aligned} \tag{18}$$

By direct calculations and taking into account (15)-(16), it follows that

$$\rho_i\left((k_{1,i}-1) + \beta^2\frac{L_i}{T_{v_i}^2}\omega_i\right) = -1, \tag{19}$$

and

$$\begin{aligned} Q_i &= -2\rho_i\begin{bmatrix}(r_i-k_{2,i}) & -\beta\frac{(r_i-k_{2,i})}{T_{v_i}}\omega_i\\ -\beta\frac{(r_i-k_{2,i})}{T_{v_i}}\omega_i & \frac{\beta^2\nu_i^2}{T_{v_i}^2}(r_i-k_{2,i})\end{bmatrix}, \\ P_iB_{V_i} &= \begin{bmatrix}-1\\ 0\end{bmatrix},\ P_iB_{\phi_i} = \alpha_i\begin{bmatrix}-1\\ 0\end{bmatrix}, \\ P_iB_{\theta_i} &= \frac{\gamma}{I_i^s}\begin{bmatrix}1\\ 0\end{bmatrix},\ P_iB_{I_i} = \frac{K}{I_i^s}\begin{bmatrix}-1\\ 0\end{bmatrix}. \end{aligned} \tag{20}$$

Therefore, considering the above equations and the symmetric property of the Laplacian matrix $\mathcal{L}$, $\dot{\mathcal{V}}(\tilde{x})$ in (17) can be rewritten as

$$\begin{aligned} \dot{\mathcal{V}}(\tilde{x}) = {} & -\tilde{V}^T\,[Y]\,\tilde{V} - \tilde{I}_l^T\,[R_l]\,\tilde{I}_l - \tilde{\theta}^T\mathcal{L}\tilde{\theta} - K\tilde{I}^TW\mathcal{L}W\tilde{I} \\ & - \left(\tilde{I}-\tilde{\phi}\right)^T\,[\alpha]\left(\tilde{I}-\tilde{\phi}\right) + \frac{1}{2}\sum_{i=1}^{N}\left[\tilde{I}_i\ \tilde{v}_i\right]Q_i\left[\tilde{I}_i\ \tilde{v}_i\right]^T. \end{aligned} \tag{21}$$

In can be shown that $tr(Q_i) = -2\rho_i(r_i-k_{2,i})(1+\beta^2\frac{\omega_i^2}{T_{v_i}^2}) < 0$ and $det(Q_i) = 0$. Since $Q_i \in \mathbb{R}^{2\times 2}$, $Q_i \preceq 0$. Therefore, $\dot{\mathcal{V}}(\tilde{x}) \leq 0$. Now, we define $\mathcal{S} = \left\{x(t) :\ \dot{\mathcal{V}}(\tilde{x}) = 0\right\}$. If $\dot{\mathcal{V}}(\tilde{x}) = 0$, then $\tilde{V} = 0$, $\tilde{I}_l = 0$, $\tilde{\theta} = \mathbf{1}_n e_\theta^*$ ($e_\theta^* \in \mathbb{R}$), $\tilde{I} = \tilde{\phi}$, $\tilde{I} = W^{-1}\mathbf{1}_n e_I^*$ ($e_I^* \in \mathbb{R}$), and $\left[\tilde{I}_i\ \tilde{v}_i\right]^T \in ker(Q_i)$, $i = 1, \ldots, n$. The closed-loop trajectories in (12) imply that $\tilde{I} = \tilde{\phi} = 0$ and $\tilde{v} = 0$. As $\mathbf{1}_n^T\,[T_\theta]^{-1}\,\tilde{\theta} = 0$, $e_\theta^* = 0$; hence, $\tilde{\theta} = 0$. Thus, the only solution that can stay identically in $\mathcal{S}$ is $\tilde{x}(t) = 0$. Therefore, the origin in (12) is the globally asymptotically stable. As a result, $\mathbf{A}$ in (34) is Hurwitz (see Appendix A). Therefore, the closed-loop system in (12) is input-to-state stable (ISS). This implies that for a potential bounded attack $\tilde{d}(t)$, the states of the cyber-physical DG microgrid in (7) are bounded. □

B. Steady-state analysis

In this subsection, it will be shown that by means of the cyber-attack-resilient distributed control approach in (6) the average voltage regulation and proportional current sharing objectives in (2) and (3) are achieved in steady-state despite the presence of unknown attacks.

Lemma 1. *Consider the cyber-physical DC microgrid (7) in the presence of the unknown bounded attacks* $\mathbf{d}_i(t)$*,* $i = 1, \ldots, 5$*. Under the stability conditions given in Theorem 1, for a sufficiently large* γ *and* β*, the proportional current-sharing and average voltage regulation in (2) and (3) are achieved.*

Proof. Considering the error dynamics in (12), the error state vector $\tilde{x}(t)$ can be obtained as follows:

$$\tilde{x}(t) = e^{\mathbf{A}t}\tilde{x}(0) + \int_0^t e^{\mathbf{A}(t-\tau)}\mathbf{B}\tilde{d}(\tau)\ d\tau. \tag{22}$$

By invoking the properties of norms, we have:

$$\lim_{t\to\infty} \|\tilde{x}(t)\| \leq \lim_{t\to\infty} \left\|e^{\mathbf{A}t}\tilde{x}(0)\right\| + \left\|\int_0^t e^{\mathbf{A}(t-\tau)}\mathbf{B}\tilde{d}(\tau)d\tau\right\|. \tag{23}$$

Given the stability of the error system in (12), $\lim_{t\to\infty}\left\|e^{\mathbf{A}t}\tilde{x}(0)\right\| = 0$. As a result,

$$\lim_{t\to\infty} \|\tilde{x}(t)\| \leq \lim_{t\to\infty} \left\|\int_0^t e^{\mathbf{A}(t-\tau)}\mathbf{B}\tilde{d}(\tau)\ d\tau\right\|. \tag{24}$$

Since the cyber-attack $\tilde{d}(t)$ is assumed to be uniformly bounded (see Assumption 2), it can be shown that there exists a constant vector Δ and a positive constant $t^\star$ such that for all $t \geq t^\star$, we have

$$\left\|\int_0^t e^{\mathbf{A}(t-\tau)}\mathbf{B}\tilde{d}(\tau)\ d\tau\right\| \leq \left\|\int_0^t e^{\mathbf{A}(t-\tau)}\mathbf{B}\Delta\ d\tau\right\|. \tag{25}$$

Thus,

$$\lim_{t\to\infty} \|\tilde{x}(t)\| \leq \lim_{t\to\infty} \left\|\int_0^t e^{\mathbf{A}(t-\tau)}\mathbf{B}\Delta\ d\tau\right\| = \left\|-\mathbf{A}^{-1}\mathbf{B}\Delta\right\|. \tag{26}$$

By calculating $\mathbf{A}^{-1}$ using the results in [19], it can be shown that for a sufficiently large γ and β, $\left\|-\mathbf{A}^{-1}\mathbf{B}\Delta\right\| \approx 0$. Hence, $\lim_{t\to\infty}\|\tilde{x}(t)\| \approx 0$. As a result, at the steady-state, $\lim_{t\to\infty} x(t) \approx \bar{x}$, where $\bar{x}$ is given in (10). Thus, at the steady state, one can obtain:

$$0 = -\bar{\phi} + \bar{\mathbf{I}} \tag{27a}$$
$$0 = \beta W\left(\left(-\bar{\mathbf{V}} + \mathbf{1}_n V^*\right) - K\mathcal{L}W\bar{\mathbf{I}} + \gamma\mathcal{L}\bar{\theta}\right) \tag{27b}$$
$$0 = \mathcal{L}\left(\bar{\theta} + \gamma W\bar{\mathbf{I}}\right). \tag{27c}$$

By left multiplying (27b) by $\frac{1}{n\beta}\mathbf{1}_n^T W^{-1}$ and invoking the properties of the Laplacian matrices $\mathcal{L}$, one obtains:

$$\frac{1}{n}\mathbf{1}_n^T\bar{\mathbf{V}} = V^*. \tag{28}$$

From (27c), one obtains that $\mathcal{L}\bar{\theta} = -\mathcal{L}\left(\gamma W\bar{\mathbf{I}}\right)$. Eliminating $\mathcal{L}\bar{\theta}$ from (27b) yields:

$$\left(K + \gamma^2\right) W\mathcal{L}W\bar{\mathbf{I}} = W(-\bar{\mathbf{V}} + \mathbf{1}_n V^*). \tag{29}$$

The above equation can be rewritten as:

$$\mathcal{L}W\bar{\mathbf{I}} = \frac{1}{(K+\gamma^2)}\left(-\bar{\mathbf{V}} + \mathbf{1}_n V^*\right). \tag{30}$$

For a sufficiently large γ, from (30) one obtains that

$$\lim_{\gamma\to\infty} \mathcal{L}W\bar{\mathbf{I}} = 0. \tag{31}$$

In this case, $\bar{\mathbf{I}} = W^{-1}\mathbf{1}_n i^*$, where $i^* \in \mathbb{R}$ is a scalar. As a result,

$$\frac{\bar{I}_i}{I_i^s} = \frac{\bar{I}_j}{I_j^s},\ i,j \in \mathcal{V}. \tag{32}$$

From (28) and (32), one can observe that the average voltage regulation and the proportional current-sharing are achieved regardless of the existence of potential cyber-attacks. □

TABLE I
DESIGN CRITERIA OF CONTROL PARAMETERS IN (6).

Parameter	Design Criteria
$k_{1,i}$	$k_{1,i} < 1$
$k_{2,i}$	$k_{2,i} < r_i$
$k_{3,i}$	$0 < k_{3,i} < \frac{T_{v_i}}{\beta L_i}(1-k_{1,i})(r_i - k_{2,i})$
$k_{4,i}$	$k_{4,i} = -\frac{K}{I_i^s}(1-k_{1,i})$
$k_{5,i}$	$k_{5,i} = \frac{1}{I_i^s}(1-k_{1,i})$
$k_{6,i}$	$k_{6,i} = \alpha_i(k_{1,i}-1)$

C. Design Guidelines

Table I summarizes the design criteria for the proposed resilient distributed controller in (6), where T_{θ_i}, T_{ϕ_i}, T_{v_i}, K, and α_i are positive quantities.

In general, the smaller values of $(T_{\theta_i}, T_{\phi_i}, T_{v_i})$ lead to faster responses. As discussed in Lemma 1, γ and β should be sufficiently large in order to achieve current sharing and voltage regulation in the presence of cyber-attacks. Moreover, the value of $k_{3,i}$ provides a trade-off between the speed of the response and overshoot, i.e., a higher value of $k_{3,i}$ will result in faster convergence with a higher overshoot.

Remark 1. *The proposed resilient control approach in this paper can be applied to DC microgrids with constant power loads (CPLs). Assuming that the DC microgrid with CPLs admits an equilibrium point, the nonlinear terms associated with CPLs can be linearized around the equilibrium point. The details about the linearization can be found in [20]. In this case, the effects of CPLs with a constant power of P_{L_i} appear in the first block of $\mathbf{A}$ in (34) as $-[C]^{-1}([Y]-Y_{CPL})$, where $Y_{CPL} = \mathrm{diag}(\frac{P_{L_1}}{V_1^2}, \ldots, \frac{P_{L_n}}{V_n^2})$.*

IV. RESULTS

A. Simulation Results

This subsection evaluates the performance of the proposed resilient distributed control strategy in (6) for a case study of a DC microgrid operating at a voltage reference $V^* = 48$ V. The microgrid consists of $n = 8$ DG units with DC-DC buck converters connecting via $m = 8$ resistive-inductive power lines, as schematically shown in Fig. 1. The microgrid topology and the parameters of the DG units has been referred from [15]. The control parameters of the proposed control strategy are designed based on the design criteria outlined in Table I and their numerical values are provided in Appendix C in Section VI. The rated current of the DC-DC converters are $I_1^s = I_4^s = I_5^s = I_8^s = 1$ and $I_2^s = I_3^s = I_6^s = I_7^s = 2$. In simulation case studies in MATLAB/Simscape, a Simulink switching model has been used.

First, the robust performance of the proposed distributed control strategy for the DC microgrid in Fig. 1 is assessed. To this end, it is assumed that the load conductance at PCC 2 is doubled at $t = 1s$. Next, we evaluate the performance of the proposed distributed control mechanism in (6) against the unknown constant cyber-attacks. It is assumed that the cyber-physical DC microgrid is attacked by injecting the false data $\mathbf{d}_1 = [0\ 0\ 0\ 5\ 0\ 0\ 0\ 0]^T$, $\mathbf{d}_2 = [5\ 0\ 0\ 0\ 0\ 0\ 0\ 0]^T$,

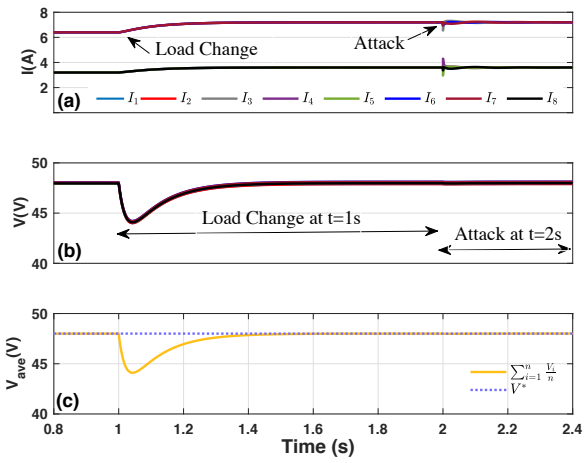

Fig. 5. Performance of the proposed resilient distributed controller in the presence of load change and constant FDI and MITM attacks: (a) currents of DC-DC converters, (b) load voltages at PCCs, and (c) average voltage across the microgrid.

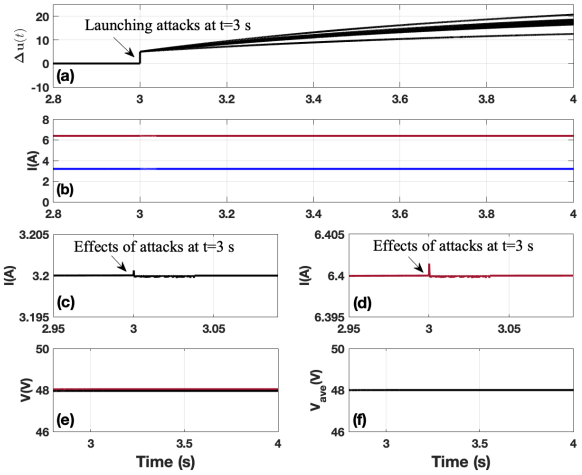

Fig. 6. Performance of the proposed attack-resilient distributed controller in the presence of time-varying dynamic FDI attacks on the actuators (The x-axis in all sub-figures is time $t(s)$).

$\mathbf{d}_4 = [10\ 0\ 0\ 5\ 0\ 0\ 0\ 0]^T$ to the communication links $\theta(t)$ and $\mathbf{I}(t)$, as presented in (7), $\mathbf{d}_5 = [5\ 15\ 5\ 10\ 10\ 10\ 15\ 5]^T$ to the actuators of all DC-DC converters at $t = 2s$. Moreover, the microgrid is also subject to the MITM attack $\mathbf{d}_3 = [0\ 5\ 0\ 15\ 0\ -7\ 10\ 5]^T$ at $t = 2s$. The currents of the DG units, voltages at PCCs, and the average of the PCC voltages are depicted in Fig. 5.

As one can observe in Fig. 5, when false data injection and MITM attacks are launched simultaneously at $t = 2s$, the resilient distributed controller mitigates the adverse effect of the attack on voltage and current signals. As a result, the sharing accuracy and consensus between DG units is unaltered despite the presence of the cyber-attack. The results show that by means of the proposed resilient control strategy, the average voltage regulation and proportional current sharing in the microgrid are achieved satisfactorily even in the presence

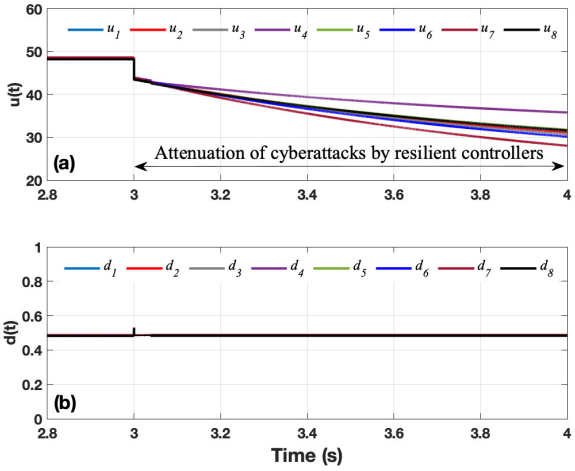

Fig. 7. Attack attenuation performance of the proposed distributed controllers: (a) control signals $u_i(t)$ and (b) duty cycles of DC-DC converters.

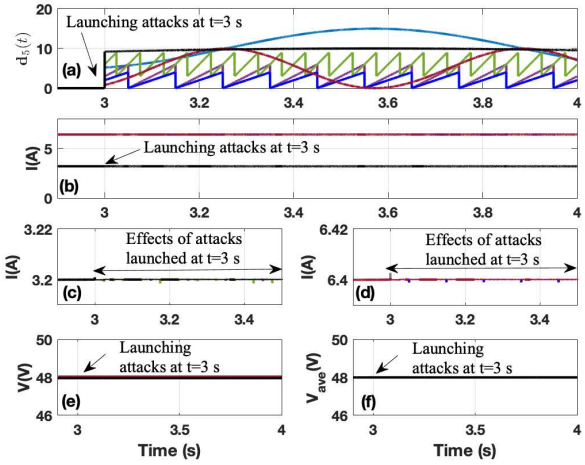

Fig. 8. Performance of the proposed resilient distributed controller in the presence of constant, sinusoidal, and sawtooth FDI attacks on actuators launched at $t = 3\ s$ (The x-axis in all sub-figures is time $t(s)$).

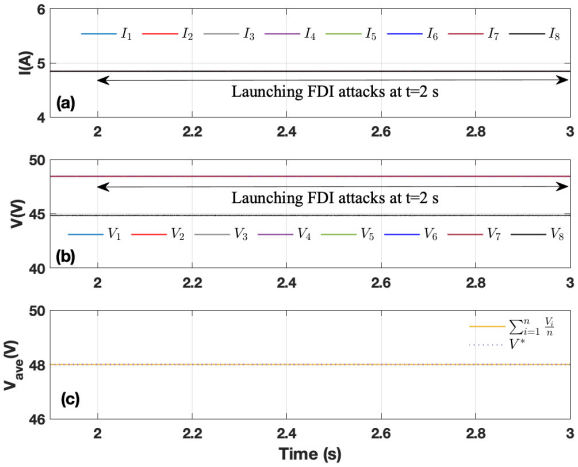

Fig. 9. Attack-resilient feature of the proposed distributed controller for a DC microgrid with different types of DC-DC converters: (a) equal current sharing of DC-DC converters, (b) load voltages at PCCs, (c) average voltage across the microgrid.

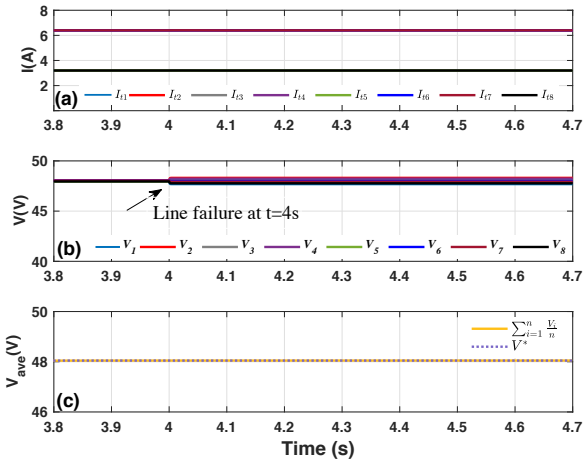

Fig. 10. Robustness of the proposed resilient distributed controller to the disconnection of the line connecting DG 1 to DG 2: (a) converter currents, (b) load voltages at PCCs, and (c) average voltage across the microgrid.

of the cyber-attacks and load changes.

In the next case study shown in Fig. 5, the performance of the proposed resilient control technique is assessed under the following dynamic bounded FDI attacks on the actuators at $t = 3s$:

$$\begin{aligned} \dot{\delta}(t) &= -\delta(t) + B_\delta \delta_0, \\ \mathbf{d}_5(t) &= \delta(t) + \delta_0, \end{aligned} \tag{33}$$

where $B_\delta \in \mathbb{R}^{8\times 8}$ is a random matrix and $\delta_0 = 5 \times \mathbf{1}_8$. The time-varying attack $\mathbf{d}_5(t)$ is shown in Fig. 6 (a). The current of DC-DC converters, the zoom version of the current of converters 1, 4, 5, 8, the zoom version of the current of converters 2, 3, 6, 7, the load voltages at PCCs, and the average voltage across the microgrid $(\frac{1}{n}\sum_{i=1}^{n} V_i(t))$ are respectively shown in Fig. 6 (b), (c), (d), (e), and (f).

Note that since the dynamic system in (33) is stable, $\mathbf{d}_5(t)$ is bounded. Moreover, the attack dynamics in (33) are not known to the control system. This figure illustrates that the effects of the dynamic attacks $\mathbf{d}_5(t)$ on the voltage and currents of DG units are fully compensated by the attack-resilient distributed control system in (6). As expected from Lemma 1, the proposed control framework achieves proportional current sharing; moreover, the average voltage is regulated at the specific value of $V^* = 48\ V$.

Fig. 7 illustrates how the resilient distributed controllers mitigate the effects of the time-varying dynamic attacks defined in (33). Upon launching the attacks at $t = 3s$, the controller attenuates the attacks as shown in Fig. 7(a). Furthermore, the duty cycles of each DG is shown in Fig. 7(b).

In order to show the performance of the proposed resilient control strategy against sinusoidal and sawtooth false data injection attacks, a new case study in carried out. In this case study, false data in terms of constant, sinusoidal, and sawtooth signals of different magnitudes and frequencies (see Fig. 8 (a)) are injected to control input channels at $t = 3\ s$. The current trajectories of DC-DC converters, the zoom version of the current of converters 1, 4, 5, 8, the zoom version of the current of converters 2, 3, 6, 7, the load voltages at PCCs,

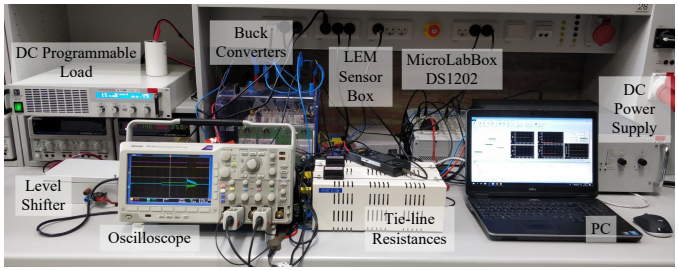

Fig. 11. Experimental setup of a DC microgrid comprising of $n = 2$ DG units controlled by dSPACE MicroLabBox DS1202 supplying power to a programmable DC load.

and the average voltage across the microgrid are respectively depicted in Fig. 8 (b), (c), (d), (e), and (f). The results in Fig. 8 highlight the attack-resilience feature of the proposed resilient distributed controller in (6).

In the next case study, it is assumed that DG 8 includes a DC-DC boost converter, while other DG units are DC-DC buck converters. The current rating of all the converters are assumed to be equal. Also, it is assumed that control input channels are subject to a variety of FDI attacks launched at $t = 2\ s$ where the false injection is in terms of constant, sinusoidal, white noise, and sawtooth signals. The current and voltage trajectories are shown in Fig. 9. As one can observe from this figure, average voltage regulation and equal current sharing are achieved regardless of the existence of cyber-attacks in the controller.

The final case study in Fig. 10 evaluates the performance and robustness of the proposed control approach to line failures. When the power line connecting DG 1 to DG 2 is disconnected at $t = 4s$, the dynamic responses of the microgrid under study are shown in Fig. 10. As one can observe from the figure, the average voltage regulation and accurate current sharing are unaffected even under physical line disconnection.

B. Experimental Results

The proposed resilient distributed strategy is experimentally validated in a DC microgrid composed of $n = 2$ DG units with DC-DC buck converters and programmable loads (voltage-dependent mode). Each converter is controlled by dSPACE MicroLabBox DS1202 (target), with control commands from ControlDesk from a PC (host). The DC microgrid operates at a voltage reference $V^* = 48\ V$. The experimental setup is shown in Fig. 11. The parameters of the experimental setup are given in Appendix D in Section VI.

Fig. 12(a) shows the performance of the proposed distributed control in voltage tracking and current sharing under the presence of false constant data injection attacks to both DG units' actuators ($u_1(t)$ and $u_2(t)$). When the false data injection attack is launched, it can be seen that the proposed resilient distributed controller mitigates the effects of the attacks following a transient. As one can observe, after some transient time, the total load current is equally shared between the converters. In Fig. 12(b), the performance of the proposed controller is assessed with respect to time delays in

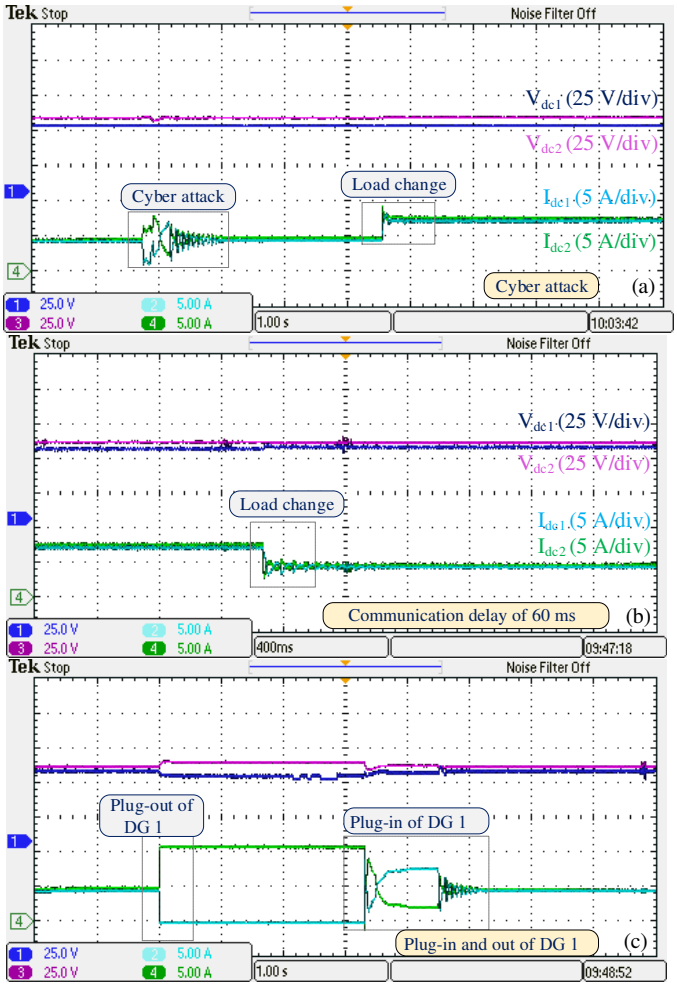

Fig. 12. Experimental validation of the proposed resilient distributed controller for (a) load change and false data injection attack, (b) time delay of $\tau = 60\ ms$, and (c) plug-and-play operation.

communication. For a maximum time delay of $\tau = 60\ ms$ in transmitting $I_2(t)$ to the controller of DG 1, the performance of the proposed distributed controller in voltage regulation and current sharing is satisfactory. The maximum time delay for the asymptotic stability of the DC microgrid with the proposed resilient distributed control approach in (6) can be obtained based on linear matrix inequalities (LMIs) proposed in Theorem 2, given in Appendix E. Finally, Fig. 9(c) reveals the performance of the resilient distributed controller in plug-and-play functionality of DG units, where DG 1 is plugged out and plugged-in. As depicted in Fig. 12(c), when DG 1 is disconnected, the total load current is provided only by DG 2. However when it is plugged back in, the load current is equally shared with voltage regulated according to the defined objective.

V. Conclusion

This paper presents a novel stability oriented resilient distributed control strategy for converter-interfaced DC microgrids, which are subject to cyber-attacks. The attackers inject false data into actuators and/or transmitted data within the microgrid and its control system to infiltrate the information. The proposed resilient control algorithm steers DC microgrids as close as possible to their desired equilibrium regardless of potential unknown cyber-attacks and guarantees average voltage regulation and proportionate current sharing. Furthermore, a comprehensive design criteria of the control parameters using a thorough stability analysis has been conducted to ensure stability and resilience simultaneously. The resilience of the microgrid with the proposed distributed control strategy to cyber-attacks and its robustness to cyber-physical disturbances are assessed via simulations and experimental case studies on a DC microgrid in the presence of false data injection and man-in-the-middle attacks. As a future work, (i) the effects of larger communication time delays in the design of the proposed resilient distributed controller, stability, and consensusability as well as (ii) the extension of results to DC microgrids with different types of DC-DC converters will be analyzed in detail. Moreover, we will consider the robustness of the proposed attack-resilient control framework under different protection mechanisms for DC grids, where grid faults need to be distinguished against cyber-attacks.

VI. Appendices

Appendix A: State Space Matrices in (12)

The state-space matrices of cyber-physical DC microgrids in (12) are defined by (34).

Appendix B: Equilibria of Unperturbed System

Lemma 2. *Consider the DC microgrid (7). It is assumed that* $\mathbf{d}_i(t) = 0,\ i = 1,\dots,5$. *Then, for a non-zero* $k_{3,i}$, *there exits an equilibrium point* $\bar{x} = \left[\bar{\mathbf{V}}^T, \bar{\mathbf{I}}^T, \bar{\mathbf{I}}_l^T, \bar{\mathbf{v}}^T, \bar{\theta}^T, \bar{\phi}^T\right]^T$ *that satisfies the following equations:*

$$
\begin{aligned}
&\bar{\mathbf{V}} = \Delta V^+ \begin{bmatrix} \frac{\sigma_W W^{-1}\mathcal{L}^+(\mathbf{1}_n V^*)}{(K+\gamma^2)} \\ \mathbf{1}_n^T V^* \end{bmatrix},\\
&\bar{\mathbf{I}} = \left([Y] + \mathcal{B}\,[R_l]^{-1}\mathcal{B}^T\right)\bar{\mathbf{V}}, \quad \bar{\mathbf{I}}_l = [R_l]^{-1}\mathcal{B}^T\bar{\mathbf{V}},\\
&\bar{\mathbf{v}} = [k_3]^{-1}([1-k_1]\,\bar{\mathbf{V}} + ([r]-[k_2]-[k_4]\,\mathcal{L}W)\,\bar{\mathbf{I}} - \gamma\,[k_5]\,\mathcal{L}^T\bar{\theta}),\\
&\bar{\theta} = \mathbf{1}_n\theta^* - \gamma W\bar{\mathbf{I}}, \quad \bar{\phi} = \bar{\mathbf{I}},
\end{aligned}
\tag{35}
$$

where

$$
\begin{aligned}
&\sigma_W = \mathbf{I}_n - W^{-1}\mathbf{1}_n\left(\mathbf{1}_n^T W^{-1}\mathbf{1}_n\right)^{-1}\mathbf{1}_n^T,\\
&\theta^* = \frac{\mathbf{1}_n^T\,[T_\theta]^{-1}}{\mathbf{1}_n^T\,[T_\theta]^{-1}\,\mathbf{1}_n}\left(\theta(0) + \gamma W\bar{\mathbf{I}}\right),\\
&\Delta V = \begin{bmatrix} \mathcal{B}\,[R_l]^{-1}\mathcal{B}^T + \sigma_W\,[Y] + \frac{\sigma_W W^{-1}\mathcal{L}^+ W^{-1}}{(K+\gamma^2)} \\ \mathbf{1}_n^T \end{bmatrix}.
\end{aligned}
\tag{36}
$$

Proof. The equilibria of (7) with $\mathbf{d}_i(t) = 0,\ i = 1,\dots,5$ can be obtained by solving the following algebraic equations:

$$
\begin{aligned}
0 &= \bar{\mathbf{I}} - \bar{\phi}, && \text{(37a)}\\
0 &= \beta W\left(\left(-\bar{\mathbf{V}} + \mathbf{1}_n V^*\right) - K\mathcal{L}W\bar{\mathbf{I}} + \gamma\mathcal{L}\bar{\theta}\right), && \text{(37b)}\\
0 &= \mathcal{L}\left(\bar{\theta} + \gamma W\bar{\mathbf{I}}\right), && \text{(37c)}\\
0 &= -\bar{\mathbf{V}} + [r]\,\bar{\mathbf{I}} + \bar{\mathbf{u}}, && \text{(37d)}\\
\bar{\mathbf{u}} &= [k_1]\,\bar{\mathbf{V}} + [k_2]\,\bar{\mathbf{I}} + [k_3]\,\bar{\mathbf{v}} + [k_4]\,\mathcal{L}W\bar{\mathbf{I}} + [k_5]\,\mathcal{L}^T\bar{\theta} && \text{(37e)}\\
0 &= -[R_l]\,\bar{\mathbf{I}}_l + \mathcal{B}^T\bar{\mathbf{V}}, && \text{(37f)}\\
0 &= \bar{\mathbf{I}} - [Y]\,\bar{\mathbf{V}} - \mathcal{B}\bar{\mathbf{I}}_l. && \text{(37g)}
\end{aligned}
$$

$$\mathbf{A}=\begin{bmatrix} -[C]^{-1}[Y] & [C]^{-1} & -[C]^{-1}\mathcal{B} & \mathbf{0}_n & \mathbf{0}_n & \mathbf{0}_n \\ [L]^{-1}[k_1-1] & [L]^{-1}([k_2]+[k_4]\mathcal{L}W-[r]+[k_6]) & \mathbf{0}_n & [L]^{-1}[k_3] & \gamma[L]^{-1}[k_5]\mathcal{L}^T & -[L]^{-1}[k_6] \\ [L_l]^{-1}\mathcal{B}^T & \mathbf{0}_n & -[L_l]^{-1}[R_l] & \mathbf{0}_n & \mathbf{0}_n & \mathbf{0}_n \\ -\beta[T_v]^{-1}W & -\beta[T_v]^{-1}(KW\mathcal{L}W+[\alpha]) & \mathbf{0}_n & \mathbf{0}_n & \beta[T_v]^{-1}\gamma W\mathcal{L}^T & \beta[T_v]^{-1}W[\alpha] \\ \mathbf{0}_n & -[T_\theta]^{-1}\mathcal{L}\gamma W & \mathbf{0}_n & \mathbf{0}_n & -[T_\theta]^{-1}\mathcal{L} & \mathbf{0}_n \\ \mathbf{0}_n & [T_\phi]^{-1} & \mathbf{0}_n & \mathbf{0}_n & \mathbf{0}_n & -[T_\phi]^{-1} \end{bmatrix},$$

$$\mathbf{B}=\begin{bmatrix} \mathbf{0}_n & \mathbf{0}_n & \mathbf{0}_n & \mathbf{0}_n & \mathbf{0}_n \\ [L]^{-1}[k_5]\mathcal{L}^T & [L]^{-1}[k_4]\mathcal{L}W & \mathbf{0}_n & \mathbf{0}_n & [L]^{-1} \\ \mathbf{0}_n & \mathbf{0}_n & \mathbf{0}_n & \mathbf{0}_n & \mathbf{0}_n \\ \gamma[T_v]^{-1}W\mathcal{L}^T & -K[T_v]^{-1}W\mathcal{L}W & [T_v]^{-1} & \mathbf{0}_n & \mathbf{0}_n \\ \mathbf{0}_n & \mathbf{0}_n & \mathbf{0}_n & -[T_\theta]^{-1}\mathcal{L} & \mathbf{0}_n \\ \mathbf{0}_n & \mathbf{0}_n & \mathbf{0}_n & \mathbf{0}_n & \mathbf{0}_n \end{bmatrix}. \tag{34}$$

First, from (37a), we obtain that $\bar{\phi} = \bar{\mathbf{I}}$. Next, by left multiplying (37b) by $\frac{1}{n\beta}\mathbf{1}_n^T W^{-1}$ and taking into account the properties of the laplacian matrix $\mathcal{L}$, one obtains:

$$\frac{1}{n}\mathbf{1}_n^T\bar{\mathbf{V}} = V^*. \tag{38}$$

Eliminating $\mathcal{L}\bar{\theta}$ from (37b) using (37c) yields:

$$\left(K+\gamma^2\right)W\mathcal{L}W\bar{\mathbf{I}} = W(-\bar{\mathbf{V}}+\mathbf{1}_nV^*). \tag{39}$$

By left multiplying the above equation by $W^{-1}\mathcal{L}\mathcal{L}^+$ and taking into account $\mathcal{L}\mathcal{L}^+\mathcal{L}=\mathcal{L}$, it follows:

$$\mathcal{L}\left(W\bar{\mathbf{I}} - \frac{1}{(K+\gamma^2)}\mathcal{L}^+\left(-\bar{\mathbf{V}}+\mathbf{1}_nV^*\right)\right) = 0. \tag{40}$$

Hence, $W\bar{\mathbf{I}} - \frac{1}{(K+\gamma^2)}\mathcal{L}^+\left(-\bar{\mathbf{V}}+\mathbf{1}_nV^*\right) = \mathbf{1}_ni^*$, where i^* is a scalar. Therefore,

$$\bar{\mathbf{I}} = W^{-1}\mathbf{1}_ni^* + \frac{1}{(K+\gamma^2)}W^{-1}\mathcal{L}^+\left(-\bar{\mathbf{V}}+\mathbf{1}_nV^*\right) \tag{41}$$

Left multiplying both sides of (37g) and (41) by $\mathbf{1}_n^T$ yields:

$$\begin{aligned} &\mathbf{1}_n^T\bar{\mathbf{I}} = \mathbf{1}_n^T[Y]\bar{\mathbf{V}}, \\ &\mathbf{1}_n^T\bar{\mathbf{I}} = \mathbf{1}_n^TW^{-1}\mathbf{1}_ni^* + \frac{\mathbf{1}_n^TW^{-1}\mathcal{L}^+}{(K+\gamma^2)}\left(-\bar{\mathbf{V}}+\mathbf{1}_nV^*\right). \end{aligned} \tag{42}$$

From the above equations, i^* is obtained as follows:

$$i^* = \frac{\mathbf{1}_n^T[Y]\bar{\mathbf{V}} - \left(\frac{\mathbf{1}_n^TW^{-1}\mathcal{L}^+}{(K+\gamma^2)}\left(-\bar{\mathbf{V}}+\mathbf{1}_nV^*\right)\right)}{(\mathbf{1}_n^TW^{-1}\mathbf{1}_n)}. \tag{43}$$

Therefore, $\bar{\mathbf{I}}$ is obtained as follows:

$$\begin{aligned} \bar{\mathbf{I}} =& \frac{1}{\mathbf{1}_n^TW^{-1}\mathbf{1}_n}\left(W^{-1}\mathbf{1}_n\mathbf{1}_n^T[Y]\bar{\mathbf{V}}\right) \\ &+ \frac{\sigma_W}{(K+\gamma^2)}W^{-1}\mathcal{L}^+\left(-\bar{\mathbf{V}}+\mathbf{1}_nV^*\right), \end{aligned} \tag{44}$$

where σ_W is defined in (36). Moreover, from (37f) and (37g), one obtains:

$$\bar{\mathbf{I}}_l = [R_l]^{-1}\mathcal{B}^T\bar{\mathbf{V}},\ \bar{\mathbf{I}} = \left([Y]+\mathcal{B}[R_l]^{-1}\mathcal{B}^T\right)\bar{\mathbf{V}}. \tag{45}$$

According to the above equation, (38), and (44), it follows:

$$\Delta V\bar{\mathbf{V}} = \begin{bmatrix} \frac{\sigma_WW^{-1}\mathcal{L}^+\left(\mathbf{1}_nV^*\right)}{(K+\gamma^2)} \\ \mathbf{1}_nV^* \end{bmatrix}, \tag{46}$$

where ΔV is defined in (36). As a result, $\bar{V}$ can be obtained by (35). From (37c), we have $\bar{\theta} = \mathbf{1}_n\theta^* - \gamma W\bar{\mathbf{I}}$, where θ^* is a scalar. Moreover, it can be shown that $\mathbf{1}_n^T[T_\theta]^{-1}\left(\bar{\theta}-\theta(0)\right) = 0$. Therefore, θ^* is obtained as $\theta^* = \frac{\mathbf{1}_n^T[T_\theta]^{-1}}{\mathbf{1}_n^T[T_\theta]^{-1}\mathbf{1}_n}\left(\theta(0)+\gamma W\bar{\mathbf{I}}\right)$. Finally, from (37e), $\bar{\mathbf{v}}$ is obtained. □

Appendix C: Simulation Parameters

The DC microgrid consists of eight DG units with DC-DC buck converters, rated equal to 500 W and 1000 W, connected via eight tie-lines, which are equipped with the proposed resilient distributed controller.

Lines: $R_{ij} = 0.5\ \Omega$ and $L_{ij} = 2\ \mu H$.

Converters: $L_i = 2.64\ \mu H$ and $C_i = 2.2\ mF$ for $i = 1,\ldots,8$.

Controller: $\eta_{i,j} = 0.01$, $\gamma = 500$, $\beta = 250$, $K = 1$, $[T_\theta] = [T_\phi] = [T_v] = 0.01\mathbf{I}_8$, $[\alpha] = 100\mathbf{I}_8$, $k_{1,i} = -10$, $k_{2,i} = -100$, $k_{3,i} = 10$, $k_{4,i} = \frac{-11}{I_i^s}$, $k_{5,i} = \frac{11}{I_i^s}$, and $k_{6,i} = -1100$, for $i = 1,\ldots,8$.

Appendix D: Experimental Setup Parameters

The DC microgrid consists of two DC/DC buck converters each rated equal to 600 W and equipped with a resilient distributed controller.

Lines: $R_{1L} = 1.2\ \Omega$, $R_{2L} = 1.8\ \Omega$.

Converters: $L_i = 3\ mH$, $C_i = 100\ \mu F$, $I_1^s = I_2^s = 12.5$.

Controller: $\gamma = 68.4$, $\beta = 36.1$, $K = 0.006$, $[T_\theta] = [T_\phi] = 0.004\mathbf{I}_2$, $[T_v] = 0.001\mathbf{I}_2$, $[\alpha] = 50\mathbf{I}_2$, $k_{1,i} = -8.4$, $k_{2,i} = -0.45$, $k_{3,i} = 0.92$, $k_{4,i} = \frac{-0.0564}{I_i^s}$, $k_{5,i} = \frac{9.4}{I_i^s}$, and $k_{6,i} = -470$, for $i = 1, 2$.

Appendix E: Stability Analysis of Time-Delay Systems

Consider the following linear time-delay system:

$$\begin{aligned} &\dot{x}(t) = A_1x(t) + A_2x(t-h), \\ &x(t) = \psi(t),\ \forall t\in[-h,0], \end{aligned} \tag{47}$$

where $A_1 \in \mathbb{R}^{n\times n}$, $A_2 \in \mathbb{R}^{n\times n}$ are known constant matrices, $\psi(t)$ is continuous initial conditions, and $h \in \mathbb{R}_+$ is a constant time-delay.

The following theorem proposed in [21] discusses the asymptotic stability of the time-delay system in (47):

Theorem 2. *The time-delay system in (47) is asymptotically stable for any time delay h satisfying $0 < h < \bar{h}$ if there exist*

$P \succ 0$, $Q \succ 0$, *and* $R \succ 0$ *such that the following linear matrix inequality (LMI) holds:*

$$\left[\begin{array}{cc} PA_1 + A_1^T P + Q & PA_2 \\ A_2^T P & -Q \end{array} \right] + \bar{h} \left[\begin{array}{c} A_1^T \\ A_2^T \end{array} \right] R \left[\begin{array}{c} A_1^T \\ A_2^T \end{array} \right]^T - \frac{1}{\bar{h}} \left[\begin{array}{c} \mathbf{I}_n \\ -\mathbf{I}_n \end{array} \right] R \left[\begin{array}{c} \mathbf{I}_n \\ -\mathbf{I}_n \end{array} \right]^T \prec 0. \tag{48}$$

Proof. To demonstrate the asymptotic stability of the time-delay system in (47), the following Lyapunov-Krasovskii functional is chosen [21]:

$$\tilde{\mathcal{V}} = x^T(t)Px(t) + \int_{t-h}^{t} x^T(\theta)Qx(\theta)d\theta + \int_{t-h}^{t}\int_{s}^{t} \dot{x}^T(\theta)R\dot{x}(\theta)d\theta ds, \tag{49}$$

where $P \succ 0$, $Q \succ 0$, and $R \succ 0$. The time-derivative of $\tilde{\mathcal{V}}$ along the system trajectories in (47) can be obtained as follows [21]:

$$\dot{\tilde{\mathcal{V}}} = 2x^T(t)P\dot{x}(t) + x^T(t)Qx(t) - x^T(t-h)Qx(t-h) + h\dot{x}^T(t)R\dot{x}(t) - \int_{t-h}^{t} \dot{x}^T(\theta)R\dot{x}(\theta)d\theta. \tag{50}$$

It can be shown that $\dot{\tilde{\mathcal{V}}} \leq x_{aug}^T(t)M(h)x_{aug}(t)$ where

$$x_{aug}(t) = \left[\begin{array}{c} \dot{x}(t) \\ x(t) \\ x(t-h) \\ z(t) \end{array} \right], \; M(h) = \left[\begin{array}{cccc} hR & P & 0 & 0 \\ P & Q & 0 & 0 \\ 0 & 0 & -Q & 0 \\ 0 & 0 & 0 & -\frac{1}{h}R \end{array} \right], \quad z(t) = x(t) - x(t-h). \tag{51}$$

Moreover, it can be shown that the extended variable $x_{aug}(t)$ satisfies $Bx_{aug} = 0$, where

$$B = \left[\begin{array}{cccc} \mathbf{I}_n & -A_1 & -A_2 & \mathbf{0}_{n\times n} \\ \mathbf{0}_{n\times n} & -\mathbf{I}_n & \mathbf{I}_n & \mathbf{I}_n \end{array} \right]. \tag{52}$$

The time-delay system in (47) is asymptotically stable if for all $x_{aug}(t)$ such that $Bx_{aug} = 0$, the inequality $x_{aug}^T(t)M(h)x_{aug}(t) < 0$ holds. This condition is equivalent to $B_o^T(t)M(h)B_o < 0$, where B_o is a right orthogonal complement of B, thanks to Finsler lemma [21]. Moreover, it can be easily shown that $M(h) \leq M(\bar{h})$ if $h < \bar{h}$. By simple calculations, we can show that $B_o^T(t)M(\bar{h})B_o < 0$ is equivalent to the conditions given in (48). This completes the proof of Theorem 2. □

Using the proposed condition (48), one might obtain the maximum time delay for the asymptotic stability of DC microgrids with the proposed resilient distributed control approach in (6).

REFERENCES

[1] T. Dragicevic, X. Lu, J. C. Vasquez, and J. M. Guerrero, "DC microgrids– Part II: A review of power architectures, applications, and standardization issues," *IEEE Trans. Power Electron.*, vol. 31, no. 5, pp. 3528–3549, May 2016.

[2] T. V. Vu, B. L. H. Nguyen, Z. Cheng, M. Y. Chow, and B. Zhang, "Cyber-physical microgrids: Toward future resilient communities," *IEEE Ind. Electron. Mag*, vol. 14, no. 3, pp. 4–17, Sept. 2020.

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

[4] S. Sahoo, J. C. Peng, A. Devakumar, S. Mishra, and T. Dragicevic, "On detection of false data in cooperative DC microgrids-A discordant element approach," *IEEE Trans. Ind. Electron.*, vol. 67, no. 8, pp. 6562–6571, Aug. 2020.

[5] A. J. Gallo, M. S. Turan, F. Boem, T. Parisini, and G. Ferrari-Trecate, "A distributed cyber-attack detection scheme with application to DC microgrids," *IEEE Trans. Autom. Control*, vol. 65, no. 9, pp. 3800–3815, Sept. 2020.

[6] 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.

[7] P. Danzi, M. Angjelichinoski, C. Stefanovic, T. Dragicevic, 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, Sept. 2019.

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

[9] S. Sahoo, T. Dragicevic, and F. Blaabjerg, "An event-driven resilient control strategy for dc microgrids," *IEEE Trans. Power Electron.*, vol. 35, no. 12, pp. 13 714–13 724, Dec. 2020.

[10] S. Sahoo, J. C. Peng, S. Mishra, and T. Dragicevic, "Distributed screening of hijacking attacks in DC microgrids," *IEEE Trans. Power Electron.*, vol. 35, no. 7, pp. 7574–7582, Jul. 2020.

[11] S. Sahoo, T. Dragicevic, and F. Blaabjerg, "Multilayer resilience paradigm against cyber attacks in DC microgrids," *IEEE Trans. Power Electron.*, vol. 36, no. 3, pp. 2522–2532, Mar. 2021.

[12] M. S. Sadabadi, "A distributed control strategy for parallel DC-DC converters," *IEEE Contr. Syst. Lett.*, vol. 5, no. 4, pp. 1231–1236, Oct. 2021.

[13] S. Sahoo and S. Mishra, "A distributed finite-time secondary average voltage regulation and current sharing controller for dc microgrids," *IEEE Transactions on Smart Grid*, vol. 10, no. 1, pp. 282–292, 2019.

[14] S. Abhinav, H. Modares, F. L. Lewis, and A. Davoudi, "Resilient cooperative control of DC microgrids," *IEEE Trans. Smart Grid*, vol. 10, no. 1, pp. 1083–1085, Jan. 2019.

[15] S. Zuo, T. Altun, F. L. Lewis, and A. Davoudi, "Distributed resilient secondary control of DC microgrids against unbounded attacks," *IEEE Trans. Smart Grid*, vol. 11, no. 5, pp. 3850–3859, Sept. 2020.

[16] F. Bullo, *Lectures on Network Systems*, 1st ed. Kindle Direct Publishing, 2020, with contributions by J. Cortes, F. Dorfler, and S. Martinez. [Online]. Available: http://motion.me.ucsb.edu/book-lns

[17] S. Trip, M. Cucuzzella, X. Cheng, and J. Scherpen, "Distributed averaging control for voltage regulation and current sharing in DC microgrids," *IEEE Contr. Syst. Lett.s*, vol. 3, no. 1, pp. 174–179, Jan. 2019.

[18] 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, Sept. 2018.

[19] T. T. Lu and S. H. Shiou, "Inverses of 2×2 block matrices," *Computers and Mathematics with Applications*, vol. 43, pp. 119–129, 2002.

[20] M. S. Sadabadi and Q. Shafiee, "Robust voltage control of DC microgrids with uncertain constant power loads," *IEEE Trans. Power Syst.*, vol. 35, no. 1, pp. 508–515, Jan. 2020.

[21] F. Gouaisbaut and D. Peaucelle, "Delay-dependent robust stability of time delay systems," in *5th IFAC Symposium on Robust Control Design*, vol. 39, Jul. 2006, pp. 453–458.