A Resilient-by-Design Distributed Control Framework for Cyber-Physical DC Microgrids

DOI:
10.1109/TCST.2023.3324530

Document Version
Accepted author manuscript

Link to publication record in Manchester Research Explorer

Citation for published version (APA):

Published in:
IEEE Transactions on Control Systems Technology

Citing this paper
Please note that where the full-text provided on Manchester Research Explorer is the Author Accepted Manuscript or Proof version this may differ from the final Published version. If citing, it is advised that you check and use the publisher's definitive version.

General rights
Copyright and moral rights for the publications made accessible in the Research Explorer are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

Takedown policy
If you believe that this document breaches copyright please refer to the University of Manchester’s Takedown Procedures [http://man.ac.uk/04Y6Bo] or contact uml.scholarlycommunications@manchester.ac.uk providing relevant details, so we can investigate your claim.
A Resilient-by-Design Distributed Control Framework for Cyber-Physical DC Microgrids

Mahdieh S. Sadabadi

Abstract—Much like any other cyber-physical systems, DC microgrids are at risk of cyberattacks that aim to disrupt their normal operation. To enhance the security and resilience of DC microgrids against cyberattacks, the development of resilient control strategies is crucial. This paper develops a distributed control approach for DC microgrids with an emphasis on resilience against a strategic cyberattack, where an attacker selects a subset of computational nodes in microgrids’ control systems to inject bounded false attack signals and change their update rules. By means of the proposed resilient distributed control mechanism interconnected with DC microgrids, the adverse effects of the false data injection (FDI) cyberattack on average voltage regulation and proportional current sharing are mitigated. Furthermore, the stability of DC microgrids in the presence of such attacks is guaranteed via a Lyapunov-based framework. Using the proposed distributed control approach, attack detection mechanisms are developed. Furthermore, it is shown that the proposed distributed controller is able to mitigate the adverse impacts of stealthy strategic FDI attacks that can bypass the attack detection system. The effectiveness of the proposed attack-resilient distributed control approach is evaluated by simulation case studies.

Index Terms—DC microgrids, resilient distributed secondary control, eavesdropping attacks, FDI cyberattacks.

I. INTRODUCTION

DISTRIBUTED control of power-electronics-dominated direct current (DC) microgrids has recently received significant attention, driven by their potential advantages compared to centralized control in terms of improved scalability, reliability, resilience to a single point of failure, and reduced communication cost. However, the integration of communication and information flow through communication channels in a distributed control framework increases the vulnerability of DC microgrids, which are examples of cyber-physical systems, to cyberattacks and infiltration [1], [2]. The attackers manipulate the availability, integrity, or confidentiality of exchanged data in microgrids’ control systems [3]. Such manipulation might lead to a collapse of the entire microgrid and an interruption in voltage regulation and accurate load sharing; therefore, it may result in serious consequences and some physical damage to power electronics converters and loads. As microgrids are used in several critical applications where high-quality and secure power is essential, enhancing their resilience against cyberattacks is also essential.

To deal with underlying challenges in resilience against cyberattacks in power-electronics-interfaced DC microgrids, several attack-detection strategies have been developed in the literature, e.g., [4]–[7]. These strategies are based on attack detection and mitigation platforms, where misbehaving distribution generation (DG) units are detected, identified, and removed or overcome. A cooperative mechanism for the detection of generalized false data injection (FDI) attacks in DC microgrids has been developed in [4]. Further studies on a discordant element-based detection approach for DC microgrids subject to FDI attacks have been carried out in [5]. An attack-detection mechanism based on identifying changes in the sets of inferred candidate invariants has been proposed in [6]. A distributed monitoring algorithm based on a Luenberger observer and a bank of unknown-input observers at each DG unit has been developed in [7]. The drawback of most of the existing attack-detection-based algorithms is the limitation on the number of compromised DG units, as the main assumption in these approaches is that more than half of the neighbors of an attacked DG unit are un-attacked. The other issue with these approaches is about the time required to detect cyberattacks. The identification and mitigation of cyberattacks in converter-interfaced DC microgrids must be fast before their stability and performance have been disrupted [8]. The fundamental limitations of the attack-detection-based category have been analyzed in [2]. The undetectable and unidentifiable attacks from a graph theory perspective have been characterized in [2]. Generally, it may not be possible to identify all potential attacks in a cyber-physical system. Hence, it is desirable to develop resilient distributed control strategies to enhance the resilience of DC microgrids against unknown sophisticated cyberattacks that are not easily detectable.

Extensive research has been carried out on the development of distributed control approaches in DC microgrids, e.g., [9]–[13] and references therein. However, these control strategies have not considered the attack-resilience feature in the control design. As a result, they are not intrinsically resilient to any perturbations or cyberattacks. For instance, a case study on a DC microgrid consisting of eight DG units, equipped with a conventional (non-resilient) distributed control, in [14] shows that a false data injection to the actuator of only one of the DG units disturbs the normal operation of the overall microgrid. To the best of our knowledge, a few resilient distributed control approaches for DC microgrids have been adopted, e.g., [14]–[17], which either assume some specific topology for microgrids or consider only FDI cyberattacks on actuators. The authors in [15] proposed a resilient distributed adaptive secondary control mechanism against unbounded FDI attacks on control input channels in the secondary control layer. In [17] and its extended version in [14], a distributed control strategy has been proposed that is resilient to FDI attacks on actuators in a DC microgrid with meshed topology while [16]...
defines the paper ends with concluding remarks in Section VIII. Section VI. Section VII includes simulation results. Finally, the resilience performance analysis of the proposed distributed stability conditions are presented. Cyberattack scenarios and is developed in Section IV where rigorous Lyapunov-based statement is presented in Section II. Section III describes the (external curious attacks).

The rest of the paper is organized as follows: The problem statement is presented in Section II. Section III describes the dynamics of the physical and cyber layers of DC microgrids. A resilient distributed control approach for DC microgrids is developed in Section IV where rigorous Lyapunov-based stability conditions are presented. Cyberattack scenarios and the resilience performance analysis of the proposed distributed control approach are respectively discussed in Section V and Section VI. Section VII includes simulation results. Finally, the paper ends with concluding remarks in Section VIII.

Notation: Throughout this paper, $1_n$ is an $n \times 1$ vector of ones, $0_{n \times 1}$ is an $n \times 1$ vector of zeros, $0_n$ is an $n \times n$ zero matrix, and $I_n$ is an $n \times n$ Identity matrix. The symbols $X^T$, $X^+$, and $X = [x_{ij}]$ denote the transpose of matrix $X$, Moore-Penrose inverse of $X$, and a matrix with entries $x_{i,j}$; moreover, $x = \text{diag}(x_1, x_2, \ldots, x_n)$, where $x_i \in \mathbb{R}; i = 1, \ldots, n$. For a symmetric matrix $X$, positive definite and positive semidefinite operators are shown by $X > 0$ and $X \geq 0$, respectively. We define $\mathbb{R}_+ := \{x \in \mathbb{R} | x > 0\}$ and $\mathbb{R}_{\geq 0} := \{x \in \mathbb{R} | x \geq 0\}$.

II. Problem Statement

In a DC microgrid with $n$ distributed generation (DG) units, two key control objectives are to proportionally distribute total load demand amongst DG units at the steady state (proportional current sharing) and to regulate the average weighted steady-state value of DC bus voltages $\mathbf{V}(t)$ across the microgrid to a global reference value $V^*$ for unknown load profiles (voltage balancing) [18]. The objectives are mathematically formulated as follows:

$$\lim_{t \to \infty} 1_n^T W^{-1} (\mathbf{V}(t) - 1_n V^*) = 0,$$  \hspace{1cm} (2)

where $\mathbf{V}(t) = [V_1(t), \ldots, V_n(t)]^T \in \mathbb{R}^n$ is a vector of voltage signals at Point of Common Couplings (PCC), $I_i(t) \in \mathbb{R}$, $I_j(t) \in \mathbb{R}$ are the current of DC-DC converter $i$ and $j$, $I_i^* \in \mathbb{R}_+$ is the rated current of DG $i$, and $W^{-1} = \text{diag}(I_1^*, \ldots, I_n^*)$.

Remark 1. In DC microgrids, the voltage regulation objective is to regulate the PCC voltages at the desired voltage level of DC microgrids $V^*$. However, the current sharing requirement in (1) does not permit identical voltage values at each PCC at the steady-state [18]. Hence, as discussed in [18], instead of exact voltage regulation, the weighted average voltage regulation problem is considered as formulated in (2).

To achieve the above-mentioned objectives, distributed control algorithms can be used in which the local controllers of DG units communicate with each other through a connected communication network. A major concern in communication schemes and transmission of information amongst the control module of DG units is the existence of cyberattacks, which potentially manipulate the integrity of exchanged data by injection attack signals and might have a detrimental impact on microgrid stability and performance.

The existing methods of cybersecurity in DC microgrids are mainly based on attack detection techniques. Most of these approaches rely on a strict assumption that at least half of the attacked DG units’ neighbors should be healthy (unattacked). Furthermore, the main focus of most of the existing works in the literature is on constant attacks or simple FDI attacks and the effects of time-varying stealthy attacks have not fully been analyzed. Therefore, it is essential to develop a resilient distributed control algorithm for DC microgrids that is resilient to a strategic FDI cyberattack, wherein an attacker selects a set of computational nodes in microgrids’ distributed control systems to inject bounded time-varying or constant attack signals. In this paper, no assumptions on the number of attacked DG units are made. This motivates us to focus on the following problem:

Problem 1. How to design a cyberattack-resilient distributed controller for DC microgrids such that in the presence of a strategic stealthy cyberattack, injecting false data to a subset of nodes in the controller, the following objectives are achieved?

$$\lim_{t \to \infty} \left| \frac{I_i(t)}{I_i^*} - \frac{I_j(t)}{I_j^*} \right| \leq \epsilon_I, \quad \text{for all } i, j \in \{1, \ldots, n\}$$

$$\lim_{t \to \infty} 1_n^T W^{-1} (\mathbf{V}(t) - 1_n V^*) \leq \epsilon_V.$$  \hspace{1cm} (3)

where $\epsilon_I$ and $\epsilon_V$ are small non-negative scalars.

In this paper, we address Problem 1 by developing a novel resilient distributed control strategy. It will be demonstrated that for a sufficiently large value of the resilient parameter, the conditions in (3) are satisfied.
III. MODEL OF CYBER-PHYSICAL DC MICROGRIDS

DC Microgrids are cyber-physical systems consisting of a physical power network, modeled as a large-scale interconnected system, combined with control and communication systems. The physical layer is composed of interconnected distributed generation (DG) units that include renewable energy sources with a DC output type, DC-DC converters, and loads. The cyber layer monitors and controls the physical layer to keep a balance between power generation and load demands.

In this section, a detailed dynamic model of the physical layer of DC microgrids is presented and the vulnerability of the cyber layer to cyberattacks is then discussed.

A. Physical Layer of DC Microgrids

The physical layer of DC microgrids can be modeled by a connected undirected graph $G = (\mathcal{V}, \mathcal{E})$. The vertex set $\mathcal{V} = \{1, \ldots, n\}$ and the edge set $\mathcal{E} = \{1, \ldots, m\}$ respectively represent the set of DG units and distribution lines connecting the corresponding DG units.

Assuming that DC-DC converters in each DG are buck-type converters, the dynamics of each node $i \in \mathcal{V}$ can be presented by the following equations [19]:

$$
\begin{align*}
\text{DG } i: \quad & \begin{cases} 
C_i \dot{V}_i(t) = I_i(t) - Y_i V_i(t) - \sum_{j \in \mathcal{N}_i} I_{ij}(t) , \\
L_i \dot{I}_i(t) = -V_i(t) - r_i I_i(t) + u_i(t),
\end{cases} \\
\text{where } \mathcal{N}_i \text{ is the set of neighbors of DG } i, V_i(t) \text{ is the voltage at PCC, } I_i(t) \text{ is the filter current of the DC-DC converter } i, \text{ and } u_i(t) \text{ is the control input of DG } i.
\end{align*}
$$

where $\mathcal{N}_i$ is the set of neighbors of DG $i$, $V_i(t)$ is the voltage at PCC, $I_i(t)$ is the filter current of the DC-DC converter $i$, $u_i(t) = d_i(t) V_{dc,i}$ is the control input of DG $i$, $d_i(t)$ is the duty cycle of the converter $i$, and $V_{dc,i}$ is the voltage of the input side of the converter $i$. The parameters $(r_i, L_i, C_i)$ are the filter parameters of the DC-DC converter $i$, and $Y_i$ is the load conductance of DG $i$ connected at PCC $i$.

The current signal of the distribution line connecting DG $i$ to DG $j$ is denoted by $I_{ij}(t)$ and represented as follows:

$$
\text{Line } ij: \quad L_{ij} \dot{I}_{ij}(t) = -R_{ij} I_{ij}(t) + V_i(t) - V_j(t),
$$

where $R_{ij}$ and $L_{ij}$ are line resistance and inductance, respectively. Since the power lines in DC microgrids are predominantly resistive, the effects of line inductance can be neglected [20]. Note that the proposed results in this paper can be extended to more detailed line dynamics. However, the added dynamics would complicate the notation and calculations in Section VI.

Let $V(t) = [V_1(t), \ldots, V_n(t)]^T \in \mathbb{R}^n$, $I(t) = [I_1(t), \ldots, I_n(t)]^T \in \mathbb{R}^n$, and $u(t) = [u_1(t), \ldots, u_n(t)]^T \in \mathbb{R}^n$, then the dynamics of the physical layer of DC microgrids are described in a vector format as follows:

$$
\begin{align*}
[ C ] \dot{V}(t) &= I(t) - [ Y ] V(t) - L_v V(t), \\
[ L ] \dot{I}(t) &= -V(t) - [ r ] I(t) + u(t),
\end{align*}
$$

where $L_v = [B][R]^{-1}[B]^T \in \mathbb{R}^{n \times n}$ is the weighted Laplacian matrix of the graph $G$, $B = [b_{ik}] \in \mathbb{R}^{n \times m}$ is the oriented incidence matrix of $G$, and $[R] \in \mathbb{R}^{m \times m}$ is a diagonal matrix whose diagonal elements are line resistances. The entries of $B$ $(b_{ik})$ are formulated as follows [21]:

$$
\begin{align*}
b_{ik} = \begin{cases} 
1 & \text{if } i \text{ is the positive end of } k, \\
-1 & \text{if } i \text{ is the negative end of } k, \\
0 & \text{otherwise}.
\end{cases}
\end{align*}
$$

B. Cyber Layer of DC Microgrids

Energy management and control systems in microgrids rely on information and communication technologies, also called cyber layers, that provide an efficient way and flexibility in sharing information amongst sensors, actuators, and information processing nodes via a communication network. However, the cyber layer is vulnerable to cyberattacks that might cause physical damage to microgrids’ physical components.

C. Strategic Cyberattacks in Microgrids’ Distributed Control

To achieve the current sharing objective in (1), a consensus-based distributed controller is required. The conventional distributed controllers such as the ones proposed in [11] and [12] include an auxiliary control state whose dynamics are given as follows:

$$
\dot{\theta}_i(t) = -\sum_{j=1}^{n} \nu_{i,j} \left( \frac{I_i(t)}{I_i^s} - \frac{I_j(t)}{I_j^s} \right) + d_{\theta,i}(t),
$$

for $i = 1, \ldots, n$, where $\nu_{i,j} \in \mathbb{R}_+$ if DG $i$ and DG $j$ are connected by a communication link; otherwise, $\nu_{i,j} = 0$.

The above control dynamics might be subject to a potential strategic cyberattack where an attacker selects a subset of computational nodes in the distributed control system in (8) to change their update rules by injecting false data $d_{\theta,i}(t)$ as follows:

$$
\dot{\theta}_i(t) = -\sum_{j=1}^{n} \nu_{i,j} \left( \frac{I_i(t)}{I_i^s} - \frac{I_j(t)}{I_j^s} \right) + d_{\theta,i}(t),
$$

Note that $d_{\theta,i}(t) = 0$ if a control node is not affected by the cyberattack. If the initial value of the auxiliary control state $\theta_i(0)$ is designed so that $\sum_{i=1}^{n} \theta_i(0) = 0$, the cyberattack $d_{\theta,i}(t)$ can easily be detected by checking the following conditions:

$$
\begin{align*}
\sum_{i=1}^{n} \theta_i(t) = 0, \forall t \geq 0 : & \text{ normal operation}, \\
\sum_{i=1}^{n} \theta_i(t) \neq 0, \forall t \geq 0 : & \text{ abnormal operation}.
\end{align*}
$$

However, an intelligent adversary might aim at corrupting the node dynamics in (8) to adversely impact the normal operation of microgrids (current sharing objective in this case) without being detected using the anomaly detection mechanism in (10). This type of cyberattack on computational nodes of control systems, referred to as stealthy attacks, has been used in some other works, e.g., [22]–[24]. An example of the stealthy attacks that are invisible to (10) is when the fake data injection $d_{\theta,i}(t)$ meets the following constraints:

$$
\sum_{i=1}^{n} d_{\theta,i}(t) = 0, \forall t \geq 0
$$
The above stealthy cyberattack cannot be detected via the detection mechanism in (10). Therefore, the cyberattack can adversely impact the microgrid operation, e.g., the current sharing objective in (1), if it cannot appropriately be detected and/or mitigated.

In this paper, a novel resilient distributed secondary control strategy is developed that ensures current sharing and voltage regulation objectives of DC microgrids in (3) while being resilient to the stealthy strategic cyberattacks on its computational nodes.

IV. RESILIENT DISTRIBUTED SECONDARY CONTROL

In order to deal with Problem 1, a novel distributed secondary control approach for DC microgrids in (6) is developed. The proposed distributed controllers are resilient to a strategic FDI cyberattack, where malicious attackers select a subset of nodes in microgrids’ secondary control systems to inject false data while bypassing detection mechanisms.

A. Proposed Distributed Secondary Controller

The conventional distributed control systems in DC microgrids require sharing the current and/or voltage of DG units amongst their neighbors. This might jeopardize the privacy of this data-sharing approach and increase the vulnerability of the controller to eavesdropping cyberattacks. In the proposed distributed controller in this paper, for privacy reasons, it is assumed that DG units do not communicate their local states \((I_i(t), V_i(t))\) (original data) amongst their neighbors. Instead, some auxiliary states (synthesized data) are communicated through a communication graph. This motivates the development of a distributed secondary control strategy with the following structure:

\[
\begin{align*}
    u_i(t) &= k_{1,i} V_i(t) + k_{2,i} I_i(t) + k_{3,i} w_i(t) \\
    &+ k_{4,i} (v_i(t) - \kappa I_i(t) + \phi_i(t)), \\
    \tau_i \dot{v}_i(t) &= -\alpha (v_i(t) - \kappa I_i(t) + \phi_i(t)) \\
    &+ K_i \beta \sum_{j=1}^{n} \nu_{ij} (\theta_i(t) - \theta_j(t)) \\
    &- K_P \sum_{j \in \mathcal{N}_i} \eta_{ij} \left( \frac{v_i(t)}{I_i} - \frac{v_j(t)}{I_j} \right), \\
    \tau \dot{\theta}_i(t) &= -\gamma \theta_i(t) - \beta \sum_{j=1}^{n} \nu_{ij} \left( \frac{v_i(t)}{I_i} - \frac{v_j(t)}{I_j} \right), \\
    \tau \dot{\phi}_i(t) &= \alpha (v_i(t) - \kappa I_i(t)), \\
    \tau \dot{w}_i(t) &= -(V_i(t) - V^*) + \alpha (v_i(t) - \kappa I_i(t) + \phi_i(t)),
\end{align*}
\]

for \(i = 1, \ldots, n\), where \(\tau_0, \tau_0, \tau_0, \tau_0, \tau_0, \tau_0, \tau_0, \tau_0, \gamma, \beta, \eta_{ij}, \nu_{ij}, \alpha, \beta, \gamma, \kappa, \in \mathbb{R}^+\), and \(K_i \in \mathbb{R}^+, K_P \in \mathbb{R}^+, \gamma \in \mathbb{R}^+, \beta \in \mathbb{R}^+, \eta_{ij} \in \mathbb{R}^+, \nu_{ij} \in \mathbb{R}^+\), \(\kappa \in \mathbb{R}^+\), and \(\alpha \in \mathbb{R}^+\). In (12), \(v_i(t), \theta_i(t), \phi_i(t), \) and \(w_i(t)\) are the states of the control module of DG \(i\).

As one can observe from (12), the proposed distributed secondary control requires communication and information exchange among DGs’ secondary control units. According to (12), the secondary controller needs exchanging the auxiliary states \((v_i(t), \theta_i(t))\) with communication weights \((\eta_{ij}, \nu_{ij})\) with other DG units’ controllers. Specifically, \(\nu_{ij} \in \{0, 1\}\) where \(\nu_{ij} = 1\) if there is a communication link between DG \(i\)’s controller and DG \(j\)’s controller; otherwise, \(\nu_{ij} = 0\). Also, \(\eta_{ij} > 0\) determines the weights of communication between two neighboring DG \(i\) and DG \(j\); i.e., DG units that are physically connected via a distribution power line.

In (12), \(K_i = [k_{1,i} k_{2,i} k_{3,i} k_{4,i}]^T \in \mathbb{R}^4\) are the design parameters of the distributed control protocol that should be properly designed such that the closed-loop stability is guaranteed. The design procedure of these parameters is given in Lemma 2.

Remark 2. The proposed secondary controller in (12) is a 4th-order controller that includes four state variables \(v_i(t), \theta_i(t), \phi_i(t), \) and \(\omega_i(t)\). The control states \(\theta_i(t)\) and \(v_i(t)\) are added to enforce consensus on \(v_i(t)\) (and therefore on \(I_i(t)\) according to the dynamics of \(\phi_i(t)\)). In addition, the state variables \(v_i(t)\) and \(w_i(t)\) aim at achieving the average voltage regulation in (2).

In (12), there are two communication networks with the same node set \(\mathcal{V}_c = \{1, \ldots, n\}\) and different edge sets. It is assumed that the communication network amongst \(v_j(t)\) in (12b) is based on a neighbor-to-neighbor communication with a Laplacian matrix \(\mathbb{L} = [l_{ij}]\), whereas the communications amongst \(\theta_j(t)\) in (12b) and \(v_j(t)\) in (12c) are based on a Laplacian matrix \(\mathbb{L}_h = [h_{ij}]\). The elements of the graph Laplacian matrices \(\mathbb{L}\) and \(\mathbb{L}_h\) are defined as follows:

\[
    l_{ij} = \begin{cases} 
    \sum_{k \in \mathcal{N}_i} \eta_{ik} & \text{if } i = j, \\
    -\eta_{ij} & \text{if } i \neq j. 
    \end{cases}
\]

\[
    h_{ij} = \begin{cases} 
    \sum_{k = 1}^{n} \nu_{ik} & \text{if } i = j, \\
    -\nu_{ij} & \text{if } i \neq j. 
    \end{cases}
\]

By the representation of \(\mathbb{L}\) in the canonical form as \(\mathbb{L} = U \Sigma_L U^T\), where \(U\) is the right eigenvector matrix of \(\mathbb{L}\) and \(\Sigma_L\) is a diagonal matrix consisting of the eigenvalues of \(\mathbb{L}\), \(\mathbb{L}_h\) is designed as follows:

\[
    \mathbb{L}_h = U \sqrt{\Sigma_L} U^T,
\]

where \(\sqrt{\Sigma_L}\) is a diagonal matrix whose diagonal entries are the square roots of the eigenvalues of \(\mathbb{L}\). Note that \(U\) is a unitary matrix, i.e., \(U^TU = UU^T = \mathbb{I}_n\). As a result, it can be shown that \(\mathbb{L} = \mathbb{L}_h^2\).

Assumption 1. It is assumed that the underlying communication graphs in (12), associated with the Laplacian matrices \(\mathbb{L}\) and \(\mathbb{L}_h\), are connected and undirected.

As one can observe from (12), the control node \(i\) receives the physical states \((I_i(t), V_i(t))\), the auxiliary variables \((v_i(t), w_i(t), \phi_i(t), \theta_i(t))\) in (12), as well as \((v_j(t), \theta_j(t))\) from neighboring nodes in the control layer. Finally, the control node \(i\) in \(\mathcal{V}_c\) sends back \(u_i(t)\) to the DC-DC converter of DG \(i\). The interaction between each control node and its corresponding DG is decentralized; however, the interaction between two different control nodes is distributed.
\[ A = T^{-1} \left[ \begin{array}{cccccc} -\alpha I_n & -K_PWLW & \beta K_IWL_{lh} & 0_n & -\alpha I_n & 0_n \\ -\beta_lhW & -\gamma I_n & 0_n & 0_n & 0_n & 0_n \\ 0_n & 0_n & -[Y] - L_B & 0_n & 0_n & 0_n \\ \alpha I_n & 0_n & 0_n & 0_n & 0_n & 0_n \\ \alpha I_n & 0_n & 0_n & 0_n & 0_n & 0_n \\ [k_4] & 0_n & [k_4] - I_n & [k_4] & [k_4] - [r] - \kappa[k_4] & 0_n \
\end{array} \right], \quad B = T^{-1} \left[ \begin{array}{cc} 0_n x_1 \\ 0_n x_1 \\ 0_n x_1 \\ 0_n x_1 \\ 0_n x_1 \\ 0_n x_1 \end{array} \right], \quad (18) \]

\[ C = \begin{bmatrix} 0_n & 0_n & I_n & 0_n & 0_n & 0_n & 0_n \\ 0_n & 0_n & 0_n & 0_n & 0_n & 0_n & I_n \end{bmatrix}, \quad T = \text{diag}(\tau_L I_n, \tau_L I_n, [C], \tau_L I_n, \tau_L I_n, [L]). \]

**Remark 3.** Note that \( L_B \) shows the physical electrical connection of DG units in the physical layer of microgrids while \( L \) and \( \bar{L} \) are the Laplacian matrices of the communication networks in the cyber layer.

**B. Closed-loop Dynamics**

Let \( w(t) = [w_1(t), \ldots, w_n(t)]^T \in \mathbb{R}^n, \phi(t) = [\phi_1(t), \ldots, \phi_n(t)]^T \in \mathbb{R}^n, V(t) = [v_1(t), \ldots, v_n(t)]^T \in \mathbb{R}^n, \) and \( \theta(t) = [\theta_1(t), \ldots, \theta_n(t)]^T \in \mathbb{R}^n. \) The overall DC microgrid, i.e., the interconnection of the physical converter layer in (6) and the control layer in (12) can be described by the following dynamical equations:

\[
\begin{align*}
\tau_L \dot{V}(t) &= -\alpha (V(t) - \kappa I(t) + \phi(t)) + \beta K_I WL_{lh}\theta(t) \\
&= -K_PWLW V(t), \\
\tau_L \dot{\theta}(t) &= -\gamma \theta(t) - \beta_LhW V(t), \\
[C] \dot{V}(t) &= I(t) - [Y] V(t) - L_B V(t), \\
\tau_L \dot{\phi}(t) &= \alpha (V(t) - \kappa I(t)), \\
\tau_L w(t) &= -V(t) + l_n V^* + \alpha (V(t) - \kappa I(t) + \phi(t)), \\
[L] I(t) &= ([k_1] - I_n) V(t) + ([k_2] - [r]) I(t) + [k_3] w(t) + [k_4] (V(t) - \kappa I(t) + \phi(t)).
\end{align*}
\]

\[ (16) \]

By defining a closed-loop state vector \( x(t) = [v^T(t), \theta^T(t), V^T(t), \phi^T(t), w^T(t), I^T(t)]^T \in \mathbb{R}^{6n} \) and an output vector \( y(t) = [V^T(t), I^T(t)]^T \in \mathbb{R}^{2n}, \) the dynamics of the proposed cyber-physical microgrid in (16) can be represented in a state-space framework as follows:

\[ \dot{x}(t) = Ax(t) + Bv^*, \quad y(t) = Cx(t), \]

where the state, input, and output matrices \( A, B, \) and \( C \) are defined in (18). In the following, the equilibrium of the closed-loop system in (17) are characterized and we then proceed with the results concerning stability analysis.

**C. Stability Analysis**

The equilibrium of the cyber-physical DC microgrid in (16) is obtained by the following lemma:

**Lemma 1.** Consider the cyber-physical DC microgrid in (16). Under Assumption 1 and also assuming that \( k_{3,i} \) in (12a) is not zero, i.e., \( k_{3,i} \neq 0 \) for all \( i \in V_c, \) the following statements hold:

1) For the closed-loop system in (16), there exists a unique equilibrium \( \bar{x} = [\bar{v}^T, \bar{\theta}^T, V^T, \bar{\phi}^T, w^T, \bar{I}^T]^T \) that satisfies the following equations:

\[
\begin{align*}
\bar{V} &= \left[ \begin{array}{c} \Delta V \\
\bar{I} = (\bar{Y} + L_B) \bar{V}, \\
\bar{v} = \kappa \bar{I}, \\
\bar{\theta} &= -\gamma^{-1} \beta_L h \bar{W} \bar{v}, \\
\bar{\phi} &= \alpha^{-1} (\bar{V} - l_n V^*), \\
\bar{w} &= (k_3)^{-1} ((1 - k_1) \bar{V} + ([r] - [k_2]) \bar{I} - [k_4] \bar{\phi}),
\end{array} \right]
\end{align*}
\]

where

\[
\sigma_W = I_n - W^{-1} l_n (I_n^T W^{-1} l_n)^{-1} I_n, \\
\Delta V = [Y] + L_B - \frac{W^{-1} I_n^T W^{-1} I_n}{\kappa (K_P + \gamma^{-1}\beta_L^2 K_I)}.
\]

2) The pair \( (\bar{V}, \bar{I}) \) satisfies the following equations:

\[
1_{6n}^T \bar{W}^{-1} (\bar{V} - l_n V^*) = 0, \\
L W \bar{I} = -\frac{1}{\kappa (K_P + \gamma^{-1}\beta_L^2 K_I)} \bar{W}^{-1} (\bar{V} - l_n V^*).
\]

**Proof.** Consider the closed-loop dynamics of the cyber-physical DC microgrid in (16). The equilibrium of (16), \( \bar{x} = [\bar{v}^T, \bar{\theta}^T, V^T, \bar{\phi}^T, w^T, \bar{I}^T]^T, \) can be obtained by solving the following algebraic equations:

\[
\begin{align*}
0_{n \times 1} &= -\alpha I_n (\bar{v} - \kappa \bar{I} + \bar{\phi} - K_P WLW \bar{v} + \beta K_I WL_{lh} \bar{\theta}), \\
0_{n \times 1} &= \gamma \bar{\theta} + \beta_L h \bar{W} \bar{v}, \\
0_{n \times 1} &= \bar{I} - [Y] \bar{V} - L_B \bar{V}, \\
0_{n \times 1} &= \alpha (\bar{v} - \kappa \bar{I}), \\
0_{n \times 1} &= -\bar{V} + l_n V^* + \alpha (\bar{v} - \kappa \bar{I} + \bar{\phi}), \\
0_{n \times 1} &= (k_3)^{-1} ((1 - k_1) \bar{V} + ([r] - [k_2]) \bar{I} - [k_4] \bar{\phi}).
\end{align*}
\]

From (22b) and (22d), one can obtain that \( \bar{\theta} = -\gamma^{-1} \beta_L h \bar{W} \bar{v} \) and \( \bar{v} = \kappa \bar{I}. \) Therefore, (22a) and (22e) can be rewritten as follows:

\[
\begin{align*}
(K_P + \beta^2 \gamma^{-1} K_I) WLW \bar{v} &= -\alpha \bar{\phi}, \\
-(\bar{V} - l_n V^*) + \alpha \bar{\phi} &= 0.
\end{align*}
\]

Hence,

\[
(K_P + \beta^2 \gamma^{-1} K_I) WLW \bar{v} = -(\bar{V} - l_n V^*).
\]
By left-multiplying (24) by $1_n^T W^{-1}$ and invoking the properties of the Laplacian matrix $L$, one obtains that
\[ 1_n^T W^{-1} \left( \dot{V} - 1_n V^* \right) = 0. \]  
(25)

Moreover, (24) can be rewritten as follows:
\[ L W \dot{V} = -(K_P + \gamma^{-1} \beta^2 K_I)^{-1} W^{-1} \left( \dot{V} - 1_n V^* \right). \]  
(26)

By left-multiplying both sides of (26) by $L L^T$ and taking into account $L L^T = L$ [25], it follows that
\[ L W \left( \dot{V} + \frac{1}{(K_P + \gamma^{-1} \beta^2 K_I)^2} W L^T W^{-1} \left( \dot{V} - 1_n V^* \right) \right) = 0. \]  
(27)

Since $1_n v^*$, $v^* \in \mathbb{R}$, is an eigenvector of $L$ associated with a zero eigenvalue, from the above equation, it is concluded that
\[ \dot{V} = W^{-1} 1_n v^* - \frac{1}{(K_P + \gamma^{-1} \beta^2 K_I)^2} W L^T W^{-1} \left( \dot{V} - 1_n V^* \right). \]  
(28)

Moreover, from (22c), it yields that
\[ \bar{I} = ([Y] + L \bar{B}) \dot{V}. \]  
(29)

Taking into account $1_n^T \bar{I} = \kappa^{-1} 1_n^T \dot{V} = 1_n^T [Y] \dot{V}$ and (28), $v^*$ is obtained as follows:
\[ v^* = \frac{\kappa 1_n^T [Y] \dot{V} + \frac{1}{(K_P + \gamma^{-1} \beta^2 K_I)^2} 1_n^T W L^T W^{-1} \left( \dot{V} - 1_n V^* \right)}{1_n^T W^{-1} 1_n}. \]  
(30)

Therefore, $\bar{V}$ can be rewritten as follows:
\[ \bar{V} = \frac{1}{1_n^T W^{-1} 1_n} \left( \kappa^{-1} 1_n^T \dot{V} - \sigma_W W^{-1} L^T (K_P W + \gamma^{-1} \beta^2 K_I W)^{-1} \left( -\dot{V} + 1_n V^* \right) \right), \]  
(31)

where $\sigma_W = 1_n - W^{-1} 1_n (1_n^T W^{-1} 1_n)^{-1} 1_n^T$. Then, by considering (29) and (31), $V$ is determined as follows:
\[ \Delta V \bar{V} = -\frac{1}{\kappa} \sigma_W W^{-1} L^T (K_P W + \gamma^{-1} \beta^2 K_I W)^{-1} W^{-1} 1_n V^*, \]  
(32)

where $\Delta V$ is defined in (20). Hence, from (25) and the above equality, one obtains that
\[ \left[ \frac{\Delta V}{1_n^T W^{-1}} \right] \bar{V} = \left[ -\frac{1}{\kappa (K_P + \gamma^{-1} \beta^2 K_I)^2} \sigma_W W^{-1} L^T + W^{-1} 1_n V^* \right]. \]  
(33)

Since $Z$ is a full column-rank matrix, $\bar{V}$ is determined from the following equation:
\[ \bar{V} = Z^+ \left[ -\frac{1}{\kappa (K_P + \gamma^{-1} \beta^2 K_I)^2} \sigma_W W^{-1} L^T + W^{-1} 1_n V^* \right]. \]  
(34)

Finally, from (22c), the equilibrium $\bar{w}$ is obtained as follows:
\[ \bar{w} = [k_3]^{-1} \left( [1 - k_1] \bar{V} + (|r| - [k_2]) \bar{I} - [k_3] \bar{p} \right). \]  
(35)

It should be noted that since $k_{3,i} \neq 0 ; \forall i \in \mathcal{V}_c$, $[k_3]$ is invertible. Hence, $\bar{w}$ can uniquely be obtained from (35).

To show the uniqueness of the equilibrium point, at the steady-state, from (17), one can obtain that
\[ A \bar{x} + B \bar{V}^* = 0_{6n \times 1}. \]  
(36)

Lemma 2 will show that $A \bar{x}$ is Hurwitz; hence, it is invertible. As a result, $\bar{x} = -A^{-1} B \bar{V}^*$ is unique. This implies the uniqueness of the equilibrium point given in (19). This completes the proof.

By defining a closed-loop error vector $e(t) = x(t) - \bar{x}$ and an output error vector $y_e(t) = y(t) - \bar{y}$ where $y = [Y^T, I^T]^T$, the dynamics of the proposed cyber-physical DC microgrid in (16) can be represented in the error coordinate as follows:
\[ \dot{e}(t) = A e(t), \]  
\[ y_e(t) = C e(t), \]  
(37)

where $A$ and $C$ are defined in (18).

The following lemma analyzes the stability of cyber-physical DC microgrids in (37). The derived stability conditions are decentralized and line-independent; it means that the controller design for each DG unit does not depend on the parameters of other DG units and distribution lines.

**Lemma 2.** Let Assumption 1 hold. If $\beta \in \mathbb{R}_+$, $\gamma \in \mathbb{R}_+$, $\kappa \in \mathbb{R}_+$, $K_P \in \mathbb{R}_+$, $K_I \in \mathbb{R}_+$, $\alpha \in \mathbb{R}_+$, $\tau_\nu \in \mathbb{R}_+$, $t_\tau \in \mathbb{R}_+$, $\tau_w \in \mathbb{R}_+$, $\tau_\phi \in \mathbb{R}_+$, and $(k_{1,i}, k_{2,i}, k_{3,i}, k_{4,i})$ belongs to the following set
\[ Z_{[i]} = \left\{ \begin{array}{l} k_{1,i} < 1, \quad k_{2,i} < 1, \\
0 < k_{3,i} < \frac{\tau_w}{\tau_i} (1 - k_{1,i}) (r_i - k_{2,i}). \end{array} \right. \]  
(38)

for $i \in \mathcal{V}_c$, then the origin of the error system in (37) is globally asymptotically stable.

**Proof.** We define the following quadratic-type Lyapunov function:
\[ V(e) = \frac{\kappa}{2} e_v^T(t) [C] e_v(t) + \frac{\tau_v}{2} e_v^T(t) e_v(t) + \frac{K_I \tau_\theta}{2} e_\theta^T(t) e_\theta(t) + \frac{\tau_\phi}{2} e_\phi^T(t) e_\phi(t) + \frac{1}{2} \sum_{i=1}^{n} [e_i(t), e_w(t)] P_i [e_i(t), e_w(t)]^T \]  
(39)

where $e_v = \bar{V} - \bar{v}$, $e_v = v - \bar{v}$, $e_\theta = \theta - \bar{\theta}$, $e_\phi = \phi - \bar{\phi}$, $e_i = \bar{I} - \bar{I}$, and $e_w = w - \bar{w}$. $P_i \in \mathbb{R}^{2 \times 2}$ in (39) is structured as follows:
\[ P_i = \kappa \begin{bmatrix} L_i \rho_i & -\frac{1}{\tau_w} \rho_i \nu_i \\
-\frac{1}{\tau_\tau} \rho_i \nu_i & \nu_i (1 + \frac{1}{\tau_\tau} \rho_i \nu_i) \end{bmatrix}, \]  
(40)

where $\rho_i$ and $\nu_i$ are chosen based on any values of $(k_{1,i}, k_{2,i}, k_{3,i})$ in $Z_{[i]}$ given in (38) as follows:
\[ \rho_i = \frac{r_i - k_{2,i}}{(r_i - k_{2,i})(1 - k_{1,i}) - \frac{\tau_w}{\tau_\tau} k_{3,i}}, \quad \nu_i = \frac{\tau_w}{r_i - k_{2,i}}. \]  
(41)

Based on $Z_{[i]}$, it is obvious that $\rho_i > 0$ and $\nu_i > 0$. Moreover, it can be shown that $\rho_i$ and $\nu_i$ satisfy the following condition:
\[ \rho_i \left( \frac{k_{1,i} - 1}{r_i - k_{2,i}} + \frac{L_i}{\tau_\tau} \nu_i \right) = -1. \]  
(42)
\[ \dot{V}(e) = \frac{\kappa}{2} e^T e + \frac{\kappa}{2} e^T e \left( [Y] + L_B \right) + \left( [Y] + L_B \right)^T e V - \frac{1}{2} \kappa e \left( e \dot{e} + \kappa e \right) - \frac{1}{2} \kappa e \left( e^T W \left( L + L^T \right) e \right) \]
\[ - \frac{K_P}{2} \left( e^T W (L + L^T) e \right) - \frac{\beta K_I}{2} \left( e^T W (L e) + e^T W (L^e e) \right) - \gamma K_I e^T e - \frac{\alpha}{2} \left( e \kappa e \kappa e \right) e \phi \]
\[ + \frac{1}{2} \sum_{i=1}^{n} [e_{iL} e_{iW}] Q_i \left[ e_{iL} e_{iW} \right]^T \]
\[ + \frac{1}{2} \sum_{i=1}^{n} \left( e_{iL} e_{iW} \right) P_i B_i V_i e_{iL} + e_{iW} B_i^T P_i \left[ e_{iL} e_{iW} \right]^T \]
\[ + \frac{1}{2} \sum_{i=1}^{n} \alpha_i \left( \left[ e_{iL} e_{iW} \right] P_i B_i \phi_i \left( e_{iL} - \kappa e_{iL} + e_{iW} \right) \right) \]
\[ + \frac{1}{2} \sum_{i=1}^{n} \alpha_i \left( \left( e_{iL} - \kappa e_{iL} + e_{iW} \right) B_i \phi_i P_i \left[ e_{iL} e_{iW} \right]^T \right) \]

where \( Q_i = P_i A_i + A_i^T P_i \) and
\[ A_i = \left[ \begin{array}{cc} k_{1,i} r_{1,i} & k_{1,i} r_{1,i} \\ \frac{k_{1,i}}{L_i} & 0 \end{array} \right] \], \( B_i = \left[ \begin{array}{cc} \frac{k_{1,i}}{L_i} & 0 \\ \frac{k_{1,i}}{L_i} & 0 \end{array} \right] \], \( B_i \phi_i = \left[ \begin{array}{c} \kappa \\ 0 \end{array} \right] \).

By direct calculations and taking into account (40)-(42), one obtains that
\[ Q_i = -2 \kappa \rho_i \left( r_i - k_{2,i} \right) \left[ \begin{array}{cc} 1 & -\frac{\nu}{\tau e} \\ -\frac{\nu}{\tau e} & \frac{\nu}{\tau e} \end{array} \right] \]
\[ P_i B_i \phi_i = P_i B_i \phi_i = \left[ \begin{array}{c} \kappa \\ 0 \end{array} \right] .\]

Therefore, considering the above equations and the symmetric property of the Laplacian matrix \( L \) and \( [Y] + L_B \), \( \dot{V}(e) \) in (43) can be rewritten as
\[ \dot{V}(e) = -\kappa e^T e \left( [Y] + L_B \right) e V - K P e^T W L W e - \gamma K_I e^T e - \frac{\alpha}{2} \left( e \kappa e \kappa e \right) e \phi \]
\[ + \frac{1}{2} \sum_{i=1}^{n} [e_{iL} e_{iW}] Q_i \left[ e_{iL} e_{iW} \right]^T \]
\[ - \kappa e \left( e \dot{e} + \kappa e \right) \]
\[ - \frac{1}{2} \kappa e \left( e^T W \left( L + L^T \right) e \right) - \frac{\beta K_I}{2} \left( e^T W (L e) + e^T W (L^e e) \right) \]
\[ + \frac{1}{2} \sum_{i=1}^{n} \alpha_i \left( \left[ e_{iL} e_{iW} \right] P_i B_i \phi_i \left( e_{iL} - \kappa e_{iL} + e_{iW} \right) \right) \]
\[ + \frac{1}{2} \sum_{i=1}^{n} \alpha_i \left( \left( e_{iL} - \kappa e_{iL} + e_{iW} \right) B_i \phi_i P_i \left[ e_{iL} e_{iW} \right]^T \right) \]

In can be shown that \( \text{trace}(Q_i) = -2 \kappa \rho_i \left( r_i - k_{2,i} \right) \left( 1 + \frac{\kappa^2}{2} \right) < 0 \) and \( \text{det}(Q_i) = 0 \). Since \( Q_i \in \mathbb{R}^{2 \times 2} \), \( Q_i \leq 0 \). Therefore, \( \dot{V}(e) \leq 0 \). To conclude the proof, LaSalle’s invariance principle is used. To this end, we define \( S = \{ e(t) : \dot{V}(e) = 0 \} \).

If \( \dot{V}(e) = 0 \), then \( e_V = 0 \), \( e_V = \kappa e \left( e^T W \left( L + L^T \right) e \right) \).

Furthermore, the closed-loop trajectories in (16) imply that \( e_{iL} = e_{iW} \gamma_{iL} \).

Remark 4. Note that the set \( Z[i] \) of stabilizing controllers in (38) is not empty, as \( k_{1,i} < 1 \) and \( k_{2,i} < r_i \) imply that \( \gamma_{iL} > 0 \). Therefore, there exists a scalar \( k_{3,i} \) so that \( 0 < k_{3,i} < \gamma_{iL} \).

Remark 5. Lemma 2 implies that \( A \) is a Hurwitz matrix.

V. CYBERATTACK SCENARIOS

The microgrids’ distributed secondary control system in (12) is vulnerable to cyberattacks. The attackers might impact the integrity, availability, and confidentiality of data in the control systems of microgrids to disrupt the normal operation of microgrids. In the following, two types of cyberattacks are considered: External eavesdropping attacks (curious attacks) and false data injection integrity attacks (malicious attacks).

A. Eavesdropping Attacks

Eavesdropping attacks, also known as sniffing or snooping, are privacy threats that disclose the local information of DG units transmitted over a network in a distributed control framework. This information includes current outputs, voltage signals, and the current capacities of converters. Eavesdropping attackers read some or all of the transmitted data and save them for later processing. As stated in [3], this type of attack could be the first stage of a more disruptive cyberattack such as replay attacks. Hence, to avoid potential privacy threats, it is important to preserve the privacy of exchanged local information. The focus of this paper is on external curious (not malicious) attacks and the case of adversarial curious internal attacks is not in the scope of this paper. It is worth mentioning that microgrids usually have one owner; hence, the case of internal curious cyberattacks might not be applicable to a single microgrid. However, in the case of networked microgrids, each microgrid might have a different owner and the owners might care about the privacy of the private information of their own microgrids. In this case, it is important to consider the case of internal curious cyberattacks.

As one can observe from (12), the proposed distributed control does not require transmitting the physical data \( (V_i(t), I_i(t)) \) from DG \( i \) to the control module of neighboring DG \( j, j \in N_i \), as required in the conventional droop-based and non-droop-based secondary control mechanism, e.g., [11], [12], [15]. However, (12) requires exchanging the auxiliary variables \( (v_i(t), \theta_i(t)) \) in the control layer, where \( v_i(t) \) asymptotically tracks \( \kappa I_i(t) \). As discussed in [26] and [27], this property of the proposed distributed control algorithm enhances the privacy-preserving of the current and voltage signals \( (I_i(t), V_i(t)) \) against external eavesdropping attacks, as the dynamics and steady-state value of \( v_i(t) \) differ from those of \( I_i(t) \). In fact, \( v_i(t) \) acts as a time-varying local mask that renders the physical state of DG \( i \) indiscernible by eavesdropping attacks (external attacks).

The following assumption is made on the knowledge set of external eavesdropping adversaries.

Assumption 2. It is assumed that an external eavesdropping adversary has knowledge about the exchanged data \( (\theta_i(t), v_i(t)) \), \( \forall i \in V_C \), but the knowledge about the value of \( \kappa \) and microgrid topology is unknown to the adversary.
Lemma 3. Under Assumption 2, the proposed distributed secondary control in (12) ensures the indiscernibility of the DG units’ physical states $I(t)$ and $V(t)$.

Proof. We consider the case where an external eavesdropping adversary aims to find/estimate $I_i(t)$, $\forall i \in V_c$. One possible way for the adversary to proceed with this estimation is to find $I_i(t)$ from $(\theta_i(t), v_i(t))$. As the initial dynamics, and steady-state value of $v_i(t)$ are different from the physical state $I_i(t)$, it is not possible to directly find $I_i(t)$ from $v_i(t)$. Furthermore, due to the incapacity of the adversary’s knowledge about the value of $\kappa$, microgrid topology, and some DG’s local parameters (e.g., $k_{1i}, k_{2i}, k_{3i}, k_{4i}$), estimating $I_i(t)$ from the closed-loop dynamics in (12) cannot be cast as a state estimation or an observer design problem. Thus, there are two possible approaches for the external eavesdropping adversary to estimate $I_i(t)$. The first approach relies on a system identification scheme and then a state estimator. However, it requires the adversary’s appropriate knowledge of the closed-loop microgrid dynamics in (12) and also collecting appropriate input-output data for the system identification purpose. Since the adversary does not have full knowledge of the cooperative system and also, considering that the input-output data in DC microgrids converge to constant values, the system identification for (12) may not be correctly carried out.

The second approach is based on building the dynamic solution of the current state as

$$I(t) = C_1 \exp(A t)x(0) + \int_0^t C_1 \exp(A(t-\tau))B V^* d\tau. \quad (47)$$

where $C_1 = [0_n \ 0_n \ 0_n \ 0_n \ 0_n \ \mathbf{I}_n \]$. Nevertheless, the correct estimation of the right-hand side of the above equation requires the adversary’s full knowledge about $A$ and initial conditions $x(0)$. Hence, $I(t)$ and also $V(t)$ are indiscernible.

B. FDI Cyberattacks in Microgrids’ Control Systems

As discussed in Section III-C, the second type of cyberattack considered in this paper is a strategic attack where an attacker selects a subset of computational nodes in the distributed control system in (12) to change their update rules by injecting false data. The DC microgrid’s controller in the presence of control system in (12) to change their update rules by injecting select a subset of computational nodes in the distributed

Remark 6. (Comments on Assumption 3) It is reasonable to assume that false injection signals $d_{\nu}(t)$ and $d_{\theta}(t)$ are bounded, as from the defender’s perspective, in the presence of unbounded false data injection, filtering techniques can be used to remove excessively large signals received at each control node [24].

Therefore, any intelligent attacker would aim at disturbing distributed control systems by a bounded injection in order to avoid attack detection [24].

C. Cyberattack Detection Mechanisms

To detect the abnormality, i.e., the existence of cyberattacks $d_{\nu}(t)$ and $d_{\theta}(t)$, in microgrids’ control systems, two baseline cyberattack-detection algorithms are implemented to monitor the behavior of the controller in (48). The cyberattack detectors are supposed to be colocated with the distributed controller; hence, they have access to the controller inputs and states to evaluate the normal or abnormal behavior of the microgrid.

The detection systems for the detection of FDI attacks $d_{\theta}(t)$ and $d_{\nu}(t)$ respectively act based on the following tests:

$$\begin{align*}
\sum_{i=1}^{n} \theta_i(t) & = 0, \forall t \geq 0 : \text{normal operation,} \\
\sum_{i=1}^{n} \theta_i(t) & \neq 0, \forall t \geq 0 : \text{abnormal operation.} \quad (49)
\end{align*}$$

$$\begin{align*}
1_n^T \dot{\phi} = 0 : \text{normal operation,} \\
1_n^T \dot{\phi} & \neq 0 : \text{abnormal operation.} \quad (50)
\end{align*}$$

were $\phi$ is the steady-state value of $\phi(t)$.

In the following, the operation of the above detection systems is explained.

It is assumed that $\theta_i(0)$ in (12) is initialized so that $\sum_{i=1}^{n} \theta_i(0) = 0$. In the absence of $d_{\nu}(t)$, due to the properties of the Laplacian matrix $\mathbf{L}_\nu$, i.e., $1_n^T \mathbf{L}_\nu = 0_n \times 1$, one obtains that $1_n^T \dot{\phi}(t) = -c_k 1_n^T \theta(t)$; as a result, $\sum_{i=1}^{n} \theta_i(t) = 0, \forall t \geq 0$. However, in the presence of $d_{\nu}(t)$, this condition might not be necessarily true, ultimately leading to the activation of the attack-detection system in (49). Similarly, it can be shown that in the presence of $d_{\nu}(t)$, $1_n^T \mathbf{L}_\nu \phi \neq 0$, or equivalently, $1_n^T \mathbf{L}_\nu (V - 1_n V^*) \neq 0$; as a result, the average voltage regulation might be violated. Hence, the FDI cyberattack $d_{\nu}(t)$ might be detected by the proposed attack detection technique in (50). Although the detection mechanism in (50) relies on $\phi$, by an appropriate design of control parameters in (12), the microgrid system response will be fast so that it reaches the steady state quickly.

D. Stealthy FDI Cyberattacks

Although the baseline cyberattack-detection algorithms in (49) and (50) are able to detect simple FDI cyberattacks $d_{\theta}(t)$ and $d_{\nu}(t)$, they might fail to detect the presence of sophisticated cyberattacks, referred to as stealthy attacks. To
model such cyberattacks that bypass the abnormality detection algorithms in (49) and (50), we define the concept of congruence between two matrices taken from [28].

**Definition.** A Laplacian matrix $L$ is said to be congruent to a matrix $H \in \mathbb{R}^{n \times n}$ if $L' = L$ implies that $H' = H$. In the case of stealthy attacks, intelligent attackers might inject $\delta(t) = H_0\delta_0(t)$ and $\delta(t) = WH_0\delta_0(t)$, where $\delta_0(t)$ and $\delta(t)$ are bounded signals, to a set of nodes in microgrids' control systems in (48), where $L$ is congruent to both $H_0 \in \mathbb{R}^{n \times n}$ and $H_e \in \mathbb{R}^{n \times n}$. It can be shown this stealthy attack representation is not detectable by the baseline cyberattack-detection algorithms in (49) and (50). In this paper, the main focus is on the stealthy attacks $H_0\delta_0(t)$ and $WH_0\delta_0(t)$.

VI. **Resilience Analysis of DC Microgrids**

The cyber-physical DC microgrid in (37) in the presence of the stealthy strategic cyberattacks $H_0\delta_0(t)$ and $WH_0\delta_0(t)$ can be described as follows:

$$\dot{e}(t) = Ae(t) + B_3H\delta(t),$$

$$y_e(t) = Ce(t)$$

(51)

where $A$ and $C$ are defined in (18), $\delta(t) = [\delta^T(\tau), \delta^T(\tau)]^T$, and $B_3$ and $H$ are defined as follows:

$$B_3 = \begin{bmatrix}
\tau_0 & 0_n \\
0_n & \tau_0 & 0_n \\
0_n & 0_n & 0_n \\
0_n & 0_n & 0_n
\end{bmatrix},
H = \begin{bmatrix}
WH_0 & 0_n \\
0_n & H_0
\end{bmatrix}.$$  

(52)

As seen from (51), by injecting the stealthy false data $H\delta(t)$, it might be possible for the attackers to change the equilibrium of the cyber-physical microgrid and distrust the microgrid's normal operation. In the following, the resilience of (51) is analyzed in the presence of the stealthy strategic attacks $H_0\delta_0(t)$ and $WH_0\delta_0(t)$. We show the closed-loop state vector $y_e(t)$ can be obtained as follows:

$$y_e(t) = C \exp A t(e(0) + \int_0^t C \exp A(t-\tau) B_3H\delta(\tau)d\tau).$$

Hence,

$$\lim_{t \to \infty} \|y_e(t)\| \leq \lim_{t \to \infty} \left\| \int_0^t C \exp A(t-\tau) B_3H\delta(\tau)d\tau \right\| \leq \lim_{t \to \infty} \left\| \int_0^t C \exp A(t-\tau) \|B_3H\delta(\tau)\|d\tau \right\|.$$  

(54)

Note that since $A$ is Hurwitz (see Remark 5), $\lim_{t \to \infty} \|C \exp A t e(0)\| = 0$. Moreover, as $\delta(t)$ is assumed to be bounded, there exists a constant vector $\Delta \in \mathbb{R}^{2n}$ such that the following inequality holds [29]:

$$\left\| \int_0^t C \exp A(t-\tau) B_3H\delta(\tau)d\tau \right\| \leq \left\| \int_0^t C \exp A(t-\tau) \|B_3H\delta(\tau)\|d\tau \right\| \leq \left\| \int_0^t C \exp A(t-\tau) \|B_3\| \|H\delta(\tau)\|d\tau \right\|.$$  

(55)

where $\Delta = [\Delta_0^T \Delta_\theta^T]^T$, $\Delta_0 \in \mathbb{R}^n$, and $\Delta_\theta \in \mathbb{R}^n$ are constant vectors. As a result, $\lim_{t \to \infty} \|y_e(t)\| = 0$.

In the next step, $A^{-1}B_3H\Delta = J^{-1}TB_3H\Delta$ should be derived. To this end, $J^{-1}$ is parameterized as follows:

$$J^{-1} = \begin{bmatrix}
j_{j11} & \ldots & j_{j16} \\
\vdots & \ddots & \vdots \\
j_{j61} & \ldots & j_{j66}
\end{bmatrix}$$

(57)

where $j_{ql}, l = 1, \ldots, 6$. Hence, $CA^{-1}B_3H\Delta$ is obtained as follows:

$$CA^{-1}B_3H\Delta = \begin{bmatrix}
j_{j31} & \ldots & j_{j36} & j_{j37} \\
j_{j61} & \ldots & j_{j66}
\end{bmatrix}.$$  

(58)

By obtaining the inverse of $J$ according to [30], $j_{ql}, l = 1, \ldots, 6$ and $l = 1, 2$, can be expressed as follows:

$$j_{j11} = -K_PWLW - \beta^2 K_g^2 W\gamma^2 - \kappa^2 - (|Y| + \tau_0)^{-1}$$

$$j_{j12} = -\kappa^{-1}L_h Wj_{j11}$$

$$j_{j13} = \kappa^{-1}j_{j11}$$

$$j_{j14} = \kappa^{-1}j_{j11}$$

$$j_{j15} = \kappa^{-1}j_{j11}$$

$$j_{j16} = \kappa^{-1}j_{j11}.$$  

(59)

Note that since $|Y| > 0$, according to Weyl's inequality [31], $|Y| + \tau_0 > 0$ and $K_PWLW - \beta^2 K_g^2 W\gamma^2 - \kappa^2 - (|Y| + \tau_0)^{-1} < 0$. As a result, these two matrices are invertible.

According to (56) and (59), it can be shown that $\lim_{t \to \infty} CA^{-1}B_3H\Delta = 0$. Hence, $\lim_{t \to \infty} \|y_e(t)\| = 0$. Therefore, for sufficiently large value of $\beta$, $y_e(t)$ converges to zero at the steady-state. This implies that $\lim_{t \to \infty} V(t) = V$ and $\lim_{t \to \infty} I(t) = I$, where $V$ and $I$ satisfy the following conditions (see Lemma 1):

$$-1^T W^1 (V - 1_nV^*) = 0,$$

$$\|LW\bar{I}\| = \kappa^{-1} (K_P + \gamma^2 \beta^2 K_I^T) W^{-1} (V - 1_nV^*).$$  

(60a)

(60b)
Since $\beta$ is sufficiently large, $(K_P + \gamma^{-1} \beta^2 K_I)^{-1}$ is sufficiently small; therefore, $LW I \approx 0_{n \times 1}$. As a result, $I \approx W^{-1} I_m t^*$, where $t^* \in \mathbb{R}$ is a constant scalar whose value depends on load conditions. This implies that the proportional current sharing objective in (1) is guaranteed for a sufficiently large value of $\beta$. Moreover, according to (60), the voltage balancing in (2) is also achieved.

The results of Theorem 1 show that by using the proposed resilient secondary control approach in (12), $I_m W^{-1} (\bar{V} - I_m V^*) = 0$ (see (60a)). This implies that $\epsilon_V = 0$ regardless of the value of $\beta$. Moreover, according to (60b), by increasing the value of $\beta$, $\epsilon_I$ will decreases. In particular, if $\beta \to \infty$, then $\epsilon_I \to 0$.

VII. SIMULATION RESULTS

In this section, a converter-interfaced DC microgrid case study, borrowed from [32], is considered. The DC microgrid consists of $n = 4$ DG units connecting via $m = 4$ distribution lines in loop topology. The parameters of the microgrid and the resilient distributed control system are given in Appendix. Fig. 1 shows the architecture of the cyber-physical DC microgrid. Several case studies in MATLAB/Simscape Electrical are conducted to evaluate the robustness and resilience features of the proposed distributed control approach in (12) to uncertainties and disturbances in both physical and cyber layers of the microgrid. In these simulation case studies, the realistic model of DC-DC power converters in MATLAB/Simscape Electrical is utilized. To highlight the superiority of the proposed attack-resilient distributed control approach compared to conventional distributed control strategies in DC microgrids, a comparative case study is also undertaken.

A. Robustness to Uncertainties in Microgrids’ Physical Layer

Load Variation. In order to assess the robustness of the proposed distributed control approach to load variation in the microgrid, it is assumed that the resistive load at PCC 4 is halved at $t = 1$ s and is doubled at $t = 2$ s. The dynamic responses of DG units are depicted in Fig. 2. The current and voltage responses show that voltage regulation and proportional current sharing are achieved regardless of the load uncertainties. Moreover, the effects of such uncertainties in the transient voltage and current responses are small. Besides, although the PCC voltages are not regulated at the reference voltage $V^*$, the deviation from $V^*$ is within $\pm5\%$ of $V^*$.

Input Voltage Variation. This case study investigates the impact of input voltage variation (input voltage of DC-DC converters) on voltage regulation and current-sharing objectives in DC microgrids. To this end, the input voltage of the converter of DG 3 is decreased by $15\%$ at $t = 0.5$ s. As observed from the current and voltage trajectories of the microgrid in Fig. 3, once the input voltage changes, the controllers compensate for the impact of such changes on voltage regulation and current sharing performance.

B. Resilience to Cyberattacks in Microgrids’ Cyber Layer

Constant Stealthy FDI Attacks. The third case study evaluates the performance of the proposed attack-resilient distributed control approach in voltage tracking and proportional current sharing in the presence of stealthy cyberattacks:

$$\delta(t) = \begin{bmatrix} W \mathbb{I} \delta_v(t) \\ \mathbb{I} \delta_i(t) \end{bmatrix},$$  \hspace{1cm} (61)
where $\delta_v(t)$ and $\delta_\theta(t)$ are constant signals that are randomly chosen. The attack signals are launched at $t = 0.5$ s. The current and voltage trajectories of DG units are depicted in Fig. 4. As one can observe from this figure, once the attacks are launched, the controller mitigates the adverse impact of the attacks on voltage regulation and current-sharing performance.

**Time-varying Stealthy FDI Attacks.** In the fourth case study, we consider the case of time-varying stealthy FDI cyberattacks where $\delta_v(t)$ and $\delta_\theta(t)$ in (61) are designed as follows:

$$\delta_v(t) = \begin{bmatrix} 10\cos(t) & -10 & 10\sin(t) & 10\end{bmatrix}^T \times U(t-3),$$

$$\delta_\theta(t) = \begin{bmatrix} 10\cos(5t) & 5 & 10\sin(t) & 5\cos(5t) \end{bmatrix}^T \times (U(t-3.5) - U(t-4.5))$$

(62)

where $U(t)$ is a unit step function. Although introducing $\beta$ in (12) increases the complexity of the distributed controller and communication requirements, according to (21) and the results of Theorem 1, a sufficiently large $\beta$ improves the current sharing and attack-resilient performance of a cyber-physical microgrid augmented with the proposed resilient distributed secondary control scheme in (12).

The performance of the proposed resilient distributed control approach in terms of resilience to cyberattacks given in (61)-(62) is compared with the performance of the proposed distributed control strategy in [11]. In both control strategies, the information exchange is based on a neighbor-to-neighbor communication scheme. The voltage and current trajectories of the microgrid using both control strategies are depicted in Fig. 5. As one can observe from Fig. 5 (a)-(b), the proposed resilient distributed control mechanism in (12) mitigates the adverse effects of cyberattacks on the stability and desired performance of DC microgrids. As a result, proportional current-sharing and voltage regulation are achieved regardless of the existing attacks in the control system. However, the distributed control method in [11] is not resilient to the cyberattacks in (62), as observed from Fig. 5 (c)-(d). Hence, upon launching attacks, voltage regulation and current sharing are no longer guaranteed. Note that the proposed distributed control in [11] assumes ideal inductors with zero parasitic resistances. That is why the average voltage of PCC voltages in Fig. 5 (d) is not regulated at $V^* = 315$ V for $t \leq 3$.

**C. Privacy versus Performance**

In this case study, the impact of the parameter $\kappa$ in (12) in the transient response of current and voltage state trajectories is evaluated. To this end, the performance of the microgrid is evaluated under load variation at $t = 5.5$ s and $t = 5.8$ s for two cases of $\kappa = 100$ and $\kappa = 0.01$. The results of this case study are depicted in Fig. 6.

A small or large value of $\kappa$ enhances the privacy feature of the proposed distributed secondary control, as the steady-state value of $v(t)$ becomes much smaller or larger than the steady-state value of $I(t)$. However, the large value of $\kappa$ adversely impacts the transient response of the voltage and current trajectories of microgrids (see Fig. 6 (a)-(b)). Moreover, according to (21), the small values of $\kappa$ have an adverse effect on the current sharing performance (see Fig. 6 (c)-(d)). The results of this case study indicate the trade-off between the privacy-enhancing feature and performance satisfaction by the proposed resilient distributed secondary controller in (12).

**VIII. Conclusion**

This paper develops a distributed control framework for cyber-physical DC microgrids with an emphasis on improving the resilience of the distributed controller against eavesdropping attacks and strategic FDI cyberattacks. In this attack scenario, an attacker selects a subset of computational nodes in the controller to inject false data. The proposed attack-resilient control mechanism attenuates the adverse effects of such attacks on the stability as well as voltage balancing and current-sharing performance of DC microgrids. Simulation case studies in MATLAB/Simscape Electrical environment evaluate the effectiveness of the proposed attack-resilient...
distributed control approach. As a future work, the effects of nonlinear loads such as constant power loads (CPLs) and ZIP loads in the stability and resilience analysis under FDI cyberattacks will be analyzed.

APPENDIX: SIMULATION PARAMETERS

The microgrid consists of four DG units respectively rated 5 kW, 5 kW, 1.66 kW, and 1.66 kW, connected via four tie-lines. The desired reference voltage level is $V^* = 315 V$.

Lines: $R_{12} = 0.6 \, \Omega, L_{12} = 50 \, \mu H, R_{13} = 1 \, \Omega, L_{13} = 60 \, \mu H, R_{23} = 1.8 \, \Omega, L_{23} = 65 \, \mu H, R_{34} = 3 \, \Omega, L_{34} = 75 \, \mu H$.

DC-DC converters: $r_i = 0.1 \, \Omega, L_{i} = 3 \, \mu H$, and $C_{i} = 250 \, \mu F$ for $i = 1, \ldots, 4$. $I_{1}^0 = I_{2}^0 = 15$ and $I_{3}^0 = I_{4}^0 = 5$.

Resilient distributed controllers: $\gamma = 0.1, \beta = 200, K_p = 1, K_i = 10, \kappa = 0.1, \tau_w = 0.01, \tau_0 = 0.001, \tau_c = 0.001, \alpha = 10, k_{1,i} = -10, k_{2,i} = -100, k_{3,i} = 5, k_{4,i} = 110$.

REFERENCES


