2024 European Control Conference (ECC)
June 25-28, 2024. Stockholm, Sweden

Cyber-Attack Resilient DC Microgrids under Distributed Control: An Energy Perspective

Cornelia Skaga and Gilbert Bergna-Diaz
Department of Electric Energy, Norwegian University of Science and Technology, 7011 Trondheim, Norway
e-mails: cornelia.skaga@ntnu.no; gilbert.bergna@ntnu.no

Abstract— **In this paper, we adopt an energy perspective to analyze the stability of converter-dominated dc grids under a hierarchical (primary/secondary) optimal control strategy based on distributed communications, and its robustness against cyber-threats. First, we begin by showing that both the *decentralized* droop-controlled dc microgrid, as well as the *distributed* secondary controller, admit a port-Hamiltonian description. Second, we exploit the fact that the closed-loop system can be interpreted as a *lossy-interconection* between their *(incremental)* models to prove stability for the unperturbed system. Third, we analyze the effect of malicious attacks on the (linear) system and robustify the control system such that *resilience against cyber threats* always is ensured at steady state. Additionally, we show that by adequately tuning the controllers we are able to significantly reduce the attack influence on the desired steady state. Finally, we use time-domain simulations to support our findings in a case study involving a low-voltage DC microgrid.**

I. Introduction

Power systems are using more renewable energy sources (RES), causing the modern grids to gradually evolve into multi-agent converter-dominated grids [1] [2]. On the low to medium voltage end, dc microgrids (MGs) have gained extensive attention as a solution to effectively implement these green energy-generating units, due to the electrical nature of the RES [3]. From a control perspective, it is crucial to shift paradigms and develop new control schemes that are suitable for a rapidly and continuously expanding RES-grid, and thus able to safely *scale* with the grid without risking unstable operations. In addition, distributed control strategies have emerged as a promising solution for ensuring optimal operation of the grid with reduced communications, providing flexibility and reliability to the grid. The use of communication networks and cooperative decision-making additionally provides resilience to single-point-of-failure [4] [5]. Despite these operational advantages, communication between neighboring units increases the system's vulnerability to cyber-attacks [6].

In the literature, the most prominent type of potential cyber threat is *false data injection attack* (FDIA) propagating the system signals by adding false information on top of existing signals. When FDIAs are perturbing even more discretely in the dynamics, control objectives such as load (power or current) sharing based on consensus protocols still converge, however at a non-optimal operating point. This subclass of attacks is then classified as an intelligent *stealth-attack* as it can deceive the control system, hence, making it even harder to detect and mitigate [7]. Several cyber security strategies have been proposed as a solution to mitigate the influence of these attacks, where the main techniques are categorized into detection/mitigation or protection strategies [8]. Several detection and mitigation strategies concerning FDIA in dc MGs have been proposed in [7], [9]–[11]. Present challenges in the design of robust control strategies for microgrids revolve around precise detection, localization, and identification of cyber-attacks. A denser network topology is often necessary within the cyber network, driven by the need for increased communication among units, as additional information exchange becomes essential in the detection and mitigation processes [7]. Additionally, these existing approaches are often time-sensitive, requiring rapid threat removal before the attacks compromise the reliability and stability of the MG [12]. In order to provide privacy and security in the network, even in hostile situations [4], [12]–[14] proposes a distributed controller with the additional control objective of *resilience against cyber threats*; i.e., aiming to ensure that the MG operates as close as possible to the unforced system while being perturbed by potential cyber threats, regardless of the attack location.

In [3] a nonlinear dc MG was proposed with a communication-reliant distributed (primary and secondary) controller, ensuring *asymptotic stability* at the optimal equilibrium where both control objectives *proportional power/current sharing* and *average voltage control* are ensured simultaneously. Due to the exploitation of communication technologies, the system is prone to cyber infiltration, and we aim to extend this model by investigating the robustness of the distributed controller against different cyber-attacks. We are interested in the ability to always ensure convergence to the desired optimal equilibrium and the capacity to always guarantee stable operation. Firstly, we show that the nonlinear system admits a port-Hamiltonian (pH) representation and assess the asymptotic stability of the system seen from an energy viewpoint by applying Lyapunov theory. Secondly, motivated by the resilient algorithm in [12], the distributed control framework is robustified. We then apply Lyapunov theory to the linear dc MG, aiming to ensure *input-to-state* stability and consequently boundedness. Finally, we propose a modified resilient version of the controller capable of ensuring proportional current-sharing and average voltage regulation in steady state even when subjected to potential attacks.

II. Energy Modelling, Stability and Equilibrium

This section reviews the distributed control and optimization proposal in *unperturbed conditions* from [3] used as a starting point in our work, included here for completeness. Throughout the paper, we use the following notations, $\mathbb{R}^{n\times m}$ and $\mathbb{R}^n$ denotes a set of $n\times m$ real matrices and $n\times 1$ real vectors, respectively. $\mathrm{col}(\cdots)\in\mathbb{R}^n$ denotes a column vector of numbers and $\mathrm{blkcol}\{\cdots\}$ denotes a column vector of vectors of appropriate dimensions.

$\mathrm{blkdiag}\{\cdots\}$ denotes a diagonal matrix of vectors of appropriate dimensions and $\mathrm{diag}(\cdots)\in\mathbb{R}^{n\times n}$ denotes a diagonal matrix of numbers. $\mathcal{I}$ denotes a diagonal identity matrix. Given a scalar or a vector x, the value at the equilibrium point is indicated as $\bar{x}$.

A. Electrical Network: Physical Layer

The DC microgrid structure and parameters under consideration are based on the model presented in [3]. The agents are the distributed generators (DGs), located close to the power-consuming loads (ZIP-loads), and are effectively interfaced with the rest of the MG through voltage-controlled converters. The DGs are interconnected both electrically and via distributed communication links, forming a cyber-physical grid (CPG). Graph theory is used to establish the physical and virtual interconnections, see Section II in [3] for precise definitions of the included graphs. Following the model presented in [3], the electrical dynamics are presented in a compact form in (1). The converters are considered equivalent zero-order models, hence, the internal voltage controller and associated inner-loop dynamics are not considered.

$$L^{\mathcal{G}}\dot{I}^{\mathcal{G}}=V^{\mathcal{G}}-\beta^{\mathcal{G}}V^{\mathcal{N}}-R^{\mathcal{G}}I^{\mathcal{G}} \tag{1a}$$
$$L^{\mathcal{E}}\dot{I}^{\mathcal{E}}=-\beta^{\mathcal{E}}V^{\mathcal{N}}-R^{\mathcal{E}}I^{\mathcal{E}} \tag{1b}$$
$$\mathcal{C}^{\mathcal{N}}\dot{V}^{\mathcal{N}}=\beta^{\mathcal{E}\top}I^{\mathcal{E}}+\beta^{\mathcal{G}\top}I^{\mathcal{G}}-I^{L} \tag{1c}$$
$$I^{L}=G^{\mathrm{cte}}V^{\mathcal{N}}+I^{\mathrm{cte}}+P^{\mathrm{cte}}/V^{\mathcal{N}} \tag{1d}$$
$$V^{\mathcal{G}}=V^{\mathrm{ref}}=\mathbf{1}_n V_{\mathrm{nom}}-R^{\mathcal{D}}I^{\mathcal{G}}+u^{\mathrm{el}}, \tag{1e}$$

where $L^{\mathcal{G}}=\mathrm{diag}(L_i^{\mathcal{G}})\in\mathbb{R}^{n_i\times n_i}$, $R^{\mathcal{G}}=\mathrm{diag}(R_i^{\mathcal{G}})\in\mathbb{R}^{n_i\times n_i}$, $I^{\mathcal{G}}=\mathrm{col}(I_i^{\mathcal{G}})\in\mathbb{R}^{n_i}$, $R^{\mathcal{D}}=\mathrm{diag}(R_i^{\mathcal{D}})\in\mathbb{R}^{n_i\times n_i}$, $u^G=\mathrm{col}(u_i^G)\in\mathbb{R}^{n_i}$ are respectively the inductance, resistance, current, droop resistance and control (voltage) input of the DGs $\forall i\in R^{\mathcal{G}}$. $L^{\mathcal{E}}=\mathrm{diag}(L_j^{\mathcal{E}})\in\mathbb{R}^{n_j\times n_j}$, $R^{\mathcal{E}}=\mathrm{diag}(R_j^{\mathcal{E}})\in\mathbb{R}^{n_j\times n_j}$, $I^{\mathcal{E}}=\mathrm{col}(I_j^{\mathcal{E}})\in\mathbb{R}^{n_j}$ are respectively the inductance, resistance, and current of the transmission lines $\forall j\in\mathbb{R}^{\mathcal{E}}$. $C^{\mathcal{N}}=\mathrm{diag}(C_k^{\mathcal{N}})\in\mathbb{R}^{n_k\times n_k}$, $V^{\mathcal{N}}=\mathrm{col}(V_k^{\mathcal{N}})\in\mathbb{R}^{n_k}$, $G^{\mathrm{cte}}=\mathrm{diag}(G_k^{\mathrm{cte}})\in\mathbb{R}^{n_k\times n_k}$, $I^{\mathrm{cte}}=\mathrm{col}(I_k^{\mathrm{cte}})\in\mathbb{R}^{n_k}$, $P^{\mathrm{cte}}=\mathrm{diag}(P_k^{\mathrm{cte}})\in\mathbb{R}^{n_k}$ are respectively the shunt capacitance, its voltage, the constant conductance, constant current and constant power of the power-consuming loads $\forall k\in\mathbb{R}^{\mathcal{N}}$. Finally, V_{nom} is the nominal voltage, and $\beta^{\mathcal{G}}=[b_{ik}]\in\mathbb{R}^{n_k\times n_i}$, and $\beta^{\mathcal{E}}=[b_{jk}]\in\mathbb{R}^{n_k\times n_j}$ are the incidence matrices defining the network topology.

1) pH Representation: The *input-state-output* pH formalism is now used to represent the electrical system in (1). The set of transmission lines $\mathcal{E}$, power-consuming loads $\mathcal{N}$, and DGs $\mathcal{G}$ all admit a port-Hamiltonian formalism, and thus the power-preserving interconnection of these three subsystems together constitute a pH system as well, as illustrated in Fig.1. Furthermore, the DGs have additional *port* variables, u_{el} and y_{el}, respectively defined as the input and output vectors that will be used to interconnect the distributed *passivity based* secondary controller. It is easy to see that the compact dynamics of the physical system in (1) admit the following pH-representation

$$\sum_{\mathrm{el}}:\begin{cases}\dot{x}_{\mathrm{el}}=(\mathcal{J}_{\mathrm{el}}-\mathcal{R}(V^{\mathcal{N}}))\nabla\mathcal{H}_{\mathrm{el}}(x_{\mathrm{el}})+E_{\mathrm{el}}\\ y_{\mathrm{el}}=g_{\mathrm{el}}^{\top}\nabla\mathcal{H}_{\mathrm{el}}(x_{\mathrm{el}}),\end{cases} \tag{2}$$

with $x_{\mathrm{el}}=\mathrm{blkcol}\{\varphi^{\mathcal{G}},\varphi^{\mathcal{E}},q^{\mathcal{N}}\}\in\mathbb{R}^n$ a collection of the flux linkages of the DGs $\varphi^{\mathcal{G}}=\mathrm{col}(\varphi_i^{\mathcal{G}})\in\mathbb{R}^{n_i}$, the flux linkages of the transmission lines $\varphi^{\mathcal{E}}=\mathrm{col}(\varphi_j^{\mathcal{E}})\in\mathbb{R}^{n_j}$, and the electrical charges of the loads $q^{\mathcal{N}}=\mathrm{col}(q_k)\in\mathbb{R}^{n_k}$ with cardinality $n\triangleq(n_i+n_j+n_k)$. $\mathcal{J}_{\mathrm{el}}=-\mathcal{J}_{\mathrm{el}}^{\top}\in\mathbb{R}^{n\times n}$ is a skew-symmetric matrix containing all electrical interconnections, given as

$$\mathcal{J}_{\mathrm{el}}\triangleq\begin{bmatrix}\mathbf{0}&\mathbf{0}&-\beta^{\mathcal{G}}\\ \mathbf{0}&\mathbf{0}&-\beta^{\mathcal{E}}\\ \beta^{\mathcal{G}\top}&\beta^{\mathcal{E}\top}&\mathbf{0}\end{bmatrix}$$

while $\mathcal{R}=\mathcal{R}^{\top}\in\mathbb{R}^{n\times n}$ is the dissipation matrix, defined as $\mathcal{R}(V^{\mathcal{N}})\triangleq\mathrm{blkdiag}\{R^{\mathcal{G}}+R^{D},R^{\mathcal{E}},G^{\mathrm{cte}}+\frac{P^{\mathrm{cte}}}{V_{\mathcal{N}}^2}\}$. $u_{\mathrm{el}}=\mathrm{col}(u_i^{\mathcal{G}})\in\mathbb{R}^{n_i}$ contains the control input of DG's, with associated input allocation vector $g_{\mathrm{el}}=\mathrm{blkdiag}\{\mathcal{I}_{n_i\times n_i},\mathbf{0}_{(n-n_i)\times n_i}\}\in\mathbb{R}^{n\times n_i}$. Its corresponding natural or passive output is then $y_{\mathrm{el}}=\mathrm{col}(y_i^{\mathcal{G}})\in\mathbb{R}^{n_i}$. $E_{\mathrm{el}}\triangleq\mathrm{col}(\mathbf{1}_{n_i}V_{\mathrm{nom}},\mathbf{0}_{n_j},-I^{\mathrm{cte}})\in\mathbb{R}^n$ is a constant column vector containing all constant sources of the electrical network. $\mathcal{H}_{\mathrm{el}}(x_{\mathrm{el}})=\frac{1}{2}x_{\mathrm{el}}^{\top}\mathcal{Q}_{\mathrm{el}}x_{\mathrm{el}}$ is the energy storage function (Hamiltonian), where $\mathcal{Q}_{\mathrm{el}}=\mathrm{blkdiag}\{L_{\mathcal{G}}^{-1},L_{\mathcal{E}}^{-1},C_{\mathcal{N}}^{-1}\}\in\mathbb{R}^{n\times n}$.

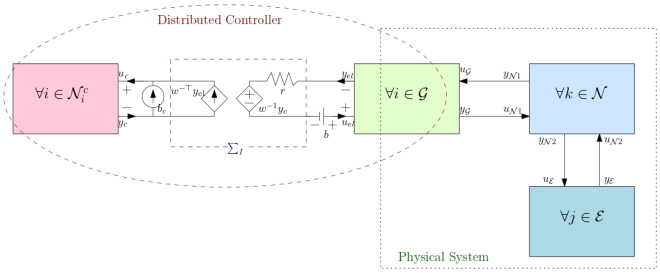

Fig. 1: Closed-Loop MG based on the port-Hamiltonian Structure

B. Communication Network: Cyber Layer

Section III in [3] included the communication network model and distributed control framework. In summary, the communication model is based on an economic dispatch convex optimization formulation, and communication between neighboring units using a leaderless consensus protocol, aiming to ensure the two control objectives: proportional power sharing and average voltage regulation. $\mathcal{N}_i^c$ is the set of the neighboring DGs in the communication network and the proposed distributed integral controller, $v_c=\mathrm{col}(v_i^c)\in\mathbb{R}^{n_i^c},\forall i\in\mathbb{R}^{\mathcal{N}^c}$ and following pH model of the communication system is given in (3), where $u_c=\mathrm{col}(u_i^c)\in\mathbb{R}^{n_i^c}:\ \forall i\in\mathbb{R}^{\mathcal{N}^c}$ is the communicated values among the DGs. $K^I>0$ is the integral gain and Finally, $\mathcal{L}=[l_{ij}]\in\mathbb{R}^{n_i^c\times n_i^c}$ is the *Laplacian* matrix, containing the consensus properties of the strongly connected communication network.

$$\sum_c\begin{cases}\dot{v}_c=g_c u_c & g_c=-K_I\mathcal{L}\\ y_c=g_c^{\top}\nabla\mathcal{H}_c(v_c),\end{cases} \tag{3}$$

$g_c\in\mathbb{R}^{n_i^c\times n_i^c}$ contains the information about where, and how the input values from the electrical network are entering the communication network, with $y_c=\mathrm{col}(y_i^c)\in\mathbb{R}^{n_i^c}$ the output vector, and $\mathcal{H}_c(v_c)=\frac{1}{2}v_c^{\top}K_I^{-1}v_c$ the Hamiltonian.

C. Cyber-Physical Network Interconnection

Fig. 1 represents the interconnection between the systems (2) and (3), both shown to admit the pH formalism, through the

following *lossy-interconnection* subsystem

$$\sum_I : \begin{bmatrix} u_{\rm el} \\ u_c \end{bmatrix} = \begin{bmatrix} -r & -(w^{-1}) \\ (w^{-1})^\top & 0 \end{bmatrix} \begin{bmatrix} y_{\rm el} \\ y_c \end{bmatrix} + \begin{bmatrix} b \\ b_c \end{bmatrix}, \quad (4)$$

where $w^{-1} = \mathrm{diag}\{w_{ij}^{-1}\} \in \mathbb{R}^{n_i \times n_i^c}$ represents added weightings in the power-preserving interconnections, important to ensure voltage regulation of the MG, further explained in Section II-E. In addition, $r > 0 \in \mathbb{R}^{n_i^c \times n_i^c}$ contains the proportional part of a PI-controller K_P and can be viewed as the dissipation of the interconnection between both networks. For generality, the power-preserving interconnections also include some constants vectors, b and $b_c \in \mathbb{R}^{n_i}$. The pH model of the closed-loop system is then given in (5), by coupling the pH systems (2) and (3) through the lossy interconnection (4).

$$\dot{x}_{\rm t} = \mathcal{F}\big(V^{\mathcal{N}}\big)\nabla\mathcal{H}_{\rm t}(x_{\rm t}) + E_{\rm t}, \quad (5)$$
$$\dot{x}_t = \begin{bmatrix} \dot{x}_{\rm el} \\ \dot{x}_c \end{bmatrix}, \quad \mathcal{F}\big(V^{\mathcal{N}}\big) = \begin{bmatrix} \mathcal{J}_{\rm el} - (\mathcal{R}\big(V^{\mathcal{N}}\big) + r) & -g_{\rm el}\omega^{-1}g_c^\top \\ g_c\omega^{-\top}g_{\rm el}^\top & \mathbf{0} \end{bmatrix},$$
$$\nabla\mathcal{H}_{\rm t}(x_{\rm t}) = \begin{bmatrix} \nabla\mathcal{H}_{\rm el}(x_{\rm el}) \\ \nabla\mathcal{H}_c(x_c) \end{bmatrix}, \quad E_{\rm t} = \begin{bmatrix} E_{\rm el} + g_{\rm el}b \\ g_c b_c \end{bmatrix}.$$

D. Lyapunov Stability Assessment

Proposition *1:* Consider the pH system in (2) coupled with the controller system (3) through the lossy interconnection (4). If r is positive-definite, then the origin is asymptotically stable in the following domain

$$\mathbb{D} = \{\tilde{x} \in \mathbb{R}^n : G^{\rm cte} > \frac{P^{\rm cte}}{\bar{V}^{\mathcal{N}}(\tilde{V}^{\mathcal{N}} + \bar{V}^{\mathcal{N}})}\}$$

Proof: Considering the equilibria equations of (2), (3) and (4), and defining the incremental variables $\tilde{x}_{\rm el} \triangleq x_{\rm el} - \bar{x}_{\rm el}$ and $\tilde{x}_c \triangleq x_c - \bar{x}_c$, the closed-loop *incremental model* is then defined as

$$\dot{\tilde{x}}_{\rm t} = \mathcal{F}_{\rm I}\Big(\tilde{V}^{\mathcal{N}}\Big)\nabla\mathcal{H}_{\rm t}(\tilde{x}_{\rm t}), \quad (6)$$

when replacing the resistance matrix of (5) with

$$\mathcal{R}_{\rm I}\Big(\tilde{V}^{\mathcal{N}}\Big) \triangleq \mathrm{blkdiag}\{R^{\mathcal{G}} + R^D, R^{\mathcal{E}}, G^{\rm cte} - G\Big(\tilde{V}^{\mathcal{N}}\Big)\},$$

when $G\Big(\tilde{V}^{\mathcal{N}}\Big) = P^{\rm cte}/\bar{V}^{\mathcal{N}}(\tilde{V}^{\mathcal{N}} + \bar{V}^{\mathcal{N}})$. Adding the *incremental* storage functions of subsystems (2) and (3), we obtain the Lyapunov function

$$\mathcal{V}(\tilde{x}_{\rm t}) \triangleq \mathcal{H}_{\rm el}(\tilde{x}_{\rm el}) + \mathcal{H}_{\rm c}(\tilde{x}_{\rm c})\} > 0,$$

with a minimum value at the equilibrium. The derivative along the trajectories of the system (6) then reads

$$\begin{aligned} \dot{\mathcal{V}}_{\rm t} &= \nabla^\top\mathcal{V}_{\rm t}(\tilde{x}_{\rm t})\dot{\tilde{x}}_{\rm t} = \nabla^\top\mathcal{V}_{\rm t}(\tilde{x}_{\rm t})\mathcal{F}_{\rm I}\Big(\tilde{V}^{\mathcal{N}}\Big)\nabla\mathcal{V}_{\rm t}(\tilde{x}_{\rm t}) \\ &= -\nabla^\top\mathcal{H}_{\rm el}(\tilde{x}_{\rm el})(\mathcal{R}\Big(\tilde{V}^{\mathcal{N}}\Big) + r)\nabla\mathcal{H}_{\rm el}(\tilde{x}_{\rm el}). \end{aligned} \quad (7)$$

Asymptotic stability follows for all $\tilde{x} \in \mathbb{D}$, since $\mathcal{R}(\tilde{V}^{\mathcal{N}}) \geq 0$, and $r > 0$ by design, leading to $\dot{\mathcal{V}}_{\rm t} \leq 0$. ■

Corollary *1:* Suppose *Proposition* 1 holds, and let $P^{\rm cte} = 0$. Then the closed-loop system is globally exponentially stable.

Proof: When $P^{\rm cte} = 0$ the physical resistance matrix is expressed as $\mathcal{R}_{\rm I} = \mathrm{blkdiag}\{R^{\mathcal{G}} + R^D, R^{\mathcal{E}}, G^{\rm cte}\} \succ 0$. For a given $r > 0$, $\mathcal{F}_{\rm I}|_{\rm sym}$ becomes a matrix consisting of solely positive definite terms. Consequently, the Lyapunov function $\mathcal{V}(\tilde{x}_t)$ takes on a quadratic form and hence *radially unbounded*, such that the equilibrium becomes *globally asymptotically stable* for $\tilde{x}_t \in \mathbb{R}^n$. ■

E. Optimal steady state and closed-loop equilibrium

The matrix containing the primary control parameters is defined as positive definite, $\boldsymbol{\alpha} > 0$. In [3], an optimal economic dispatch problem was formulated for the microgrid under consideration as

$$\min \sum_{i=1}^{n_i} \mathcal{C}_i(I_i^{\mathcal{G}}), \quad \text{s.t.} \quad \sum_{i=1}^{n_i} I_i^{\mathcal{G}} = I_{\rm demand},$$

with $\mathcal{C}_i(I_i^{\mathcal{G}}) \triangleq \alpha_i(I_i^{\mathcal{G}})^2 + \beta_i(I_i^{\mathcal{G}}) + \gamma_i$ the cost function for the ith generator, and weighted cost function parameters in the economic dispatch optimizer α_i, β_i and γ_i. When this convex optimization problem is solved with the Lagrangian method, the Karush-Kuhn-Tucker (KKT) conditions for primal-dual optimality give the necessary and sufficient *stationary* condition

$$\lim_{t\to\infty} \lambda_i = \lambda_j = \lambda_{\rm opt}, \quad \text{with} \quad \lambda_i = 2\alpha_i y_i^{\rm el} + \beta_i, \quad (8)$$

or alternatively, in compact form:

$$\lambda = 2\alpha y_{\rm el} + \beta \quad (9)$$

with $\alpha = \mathrm{diag}(\alpha_i) \in \mathbb{R}^{n_i \times n_i}$ and $\mathcal{B} = \mathrm{col}(\beta_i) \in \mathbb{R}^{n_i}$.

Proposition *2 (Proposition 3 in [3]):* Consider the following definitions

$$b = -K_p w^{-1}\mathcal{L}\mathcal{B}, \qquad b_c = \mathcal{B},$$
$$r = -R^D + K_p w^{-1}\mathcal{L}w^{-1}, \quad w^{-1} = 2\alpha.$$

If the communication network is strongly connected and undirected, the KKT optimality condition (8) is achieved at the equilibrium point of the dc microgrid in closed-loop with the controller of [3]. The controller also guarantees a *near-nominal voltage formation*, which can be formulated as

$$\lim_{t\to\infty} \sum_{i=1}^{n_i} \omega_i V_i^{\mathcal{G}} = V_{\rm nom} \sum_{i=1}^{n_i} \omega_i.$$

Proof: We derive the steady state equations of (5) by setting $\dot{x}_{\rm t} = 0_n$. Hence, the equilibrium set is given by

$$\mathscr{E} \triangleq \{x_{\rm t} \in \mathbb{R}^n : 0 = \mathcal{F}_{\rm I}\big(V^{\mathcal{N}}\big)\nabla\mathcal{H}_{\rm t}(x_{\rm t}) + E_{\rm t}\}. \quad (10)$$

The steady state equilibrium of the cyber layer (3) is then $0 = -K_I\mathcal{L}\lambda$. Due to the Laplacian property $\mathcal{L}\mathbf{1}_n = 0$ the above expression is satisfied when $\lambda = \lambda_{\rm opt}\mathbf{1}_{n_i^c}$. Hence, the KKT condition (8) is satisfied at the equilibrium ensuring proportional current sharing. Subsequently, we investigate the near-nominal voltage regulation in steady state. Following *Proposition* 2 and by multiplying the sum of the weighted voltages $\mathbf{1}_{n_i} w$ on each side of the closed-loop controller in (1e), the weighted voltage sum is expressed as

$$\begin{aligned} \mathbf{1}_{n_i}^\top w\bar{V} = {} & \mathbf{1}^\top w\mathbf{1}_{n_i} V_{\rm nom} \\ & - \mathbf{1}_{n_i}^\top w\big[K_p w^{-1}\mathcal{L}w^{-1}\bar{y}_{\rm el} + K_p w^{-1}\mathcal{L}\mathcal{B}\big] - \mathbf{1}_{n_i}^\top \bar{y}_c \end{aligned} \quad (11)$$

Using the pH system definition in (3), and the Laplacian property $1_n^\top\mathcal{L} = 0$, (11) simplifies to

$$\mathbf{1}_{n_i}^\top w\bar{V} = \mathbf{1}_{n_i}^\top w\mathbf{1}_{n_i} V_{\rm nom}. \quad (12)$$

The above equation reveals that the control ensures that the weighted average voltage is regulated to $V_{\rm nom}$ at the equilibrium; i.e., near-nominal voltage regulation in steady state. ■

III. DC Microgrid Subject to Cyber-Attacks

In this section, we analyse the linear dc MG following *Corollary* 1, together with the controller in [3] under perturbed conditions; i.e., where $x_{\rm t}$ is influenced by additional time-dependent bounded disturbances under the following assumption.

Assumption 1: All potential cyber-attacks perturbing the microgrids can be modeled as unknown, yet uniformly bounded attacks. We evaluate the stability of the perturbed system using Lyapunov theory, bounding the stability through the *input-to-state* property induced by the attacks. Then we impose three different cyber-attacks to the MG under considerations as follows. First, we impose a false data injection attack (FDIA) in the actuators of the generators: i.e., adding false values on top of existing signals. Secondly, we construct an FDIA perturbing the current measurements of the DGs. The current sensors are located in the converters in the physical network. However, as the DGs are the communicating units, the potential cyber attacker may malign the measured values, affecting the control configurations (both droop and secondary). Finally, we impose a third-party man-in-the-middle (MITM) attack infiltration in the communication links of the distributed control network. An MITM attack may interfere with the system as either a hijacking attack: i.e., completely replacing the existing signals, or an FDIA. Regardless of the behavior of the attack, the MITM attack changes the communicated values between the DGs in the cyber layer of the MG.

In Section II-D under *Corollary* 1 the unforced linear system is proven to globally asymptotically (exponentially) converge to a stable equilibrium point. We now leverage *Lemma 4.5* in [15], which asserts that if the unperturbed system is globally exponentially stable, the perturbed system is *input-to-state stable* (ISS) and bounded by the external attacks. Furthermore, due to the linearity of the system, *boundedness* immediately follows.

1) Cyber-Attack 1; FDIA in the Actuators of the Generators: Δu is the attack-vector perturbing the energy transfer to the system; hence, $u_{\rm el}=-ry_{\rm el}-w^{-1}y_c+b+\Delta u$. For the incremental system, the attack-vector is then included in $\tilde{u}_{\rm el}$ in (5) changing the time-derivative of the Hamiltonian of the physical system, and thereby the Lyapunov function as follows

$$\dot{V}_{C1}(\tilde{x}_{\rm t})=\dot{V}_{\rm t}(\tilde{x}_{\rm t})+\nabla^{\top}\mathcal{H}_{\rm el}(\tilde{x}_{\rm el})g_{\rm el}\zeta\Delta\tilde{u}. \tag{13}$$

Corollary *2:* When the linear ISS system (2), (3), (4) is subject cyber-attack 1, we can express the restrictive stability bound of the states under the *bounded input-bounded-state* property (BIBS) as

$$\|\nabla^{\top}\mathcal{H}_{\rm el}(\tilde{x}_{\rm el})\|\geq\frac{\|g_{\rm el}\zeta\Delta\tilde{u}\|}{\lambda_{\min}(\mathcal{R}_{\rm I}+r)}. \tag{14}$$

Proof: We bound the stability of the Lyapunov function in (13) subject to cyber-attack 1 as follows

$$\begin{aligned}\dot{V}_{C1}(\tilde{x}_{\rm t})&=\dot{V}_{\rm t}(\tilde{x}_{\rm t})+\nabla^{\top}\mathcal{H}_{\rm el}(\tilde{x}_{\rm el})g_{\rm el}\zeta\Delta\tilde{u},\\&=-\nabla^{\top}\mathcal{H}_{\rm el}(\tilde{x}_{\rm el})(\mathcal{R}_{\rm I}+r)\nabla\mathcal{H}_{\rm el}(\tilde{x}_{\rm el}),\\&\leq-\lambda_{\min}(\mathcal{R}_{\rm I}+r)\|\nabla\mathcal{H}_{\rm el}(\tilde{x}_{\rm el})\|^2\\&\quad+\|\nabla^{\top}\mathcal{H}_{\rm el}(\tilde{x}_{\rm el})\|\|g_{\rm el}\zeta\Delta\tilde{u}\|\leq 0\end{aligned} \tag{15}$$

where we have used (7) in the second equality, the eigenvalue norm in the first inequality together with Cauchy-Schwarz inequality. The proof is completed by forcing the last inequality to be negative semi-definite and solving for $\|\mathcal{H}_{\rm el}(\tilde{x}_{\rm el})\|$. ■

2) Cyber-Attack 2; FDIA in the Current Sensors of the Physical System: ΔI is modeled as the attack-vector and the two controllers of the closed-loop control system, are given as: $u_{\rm el}=ry_{\rm el}-w^{-1}y_c-r\Delta I+b$ and $u_c=w^{-1^{\top}}y_{\rm el}+w^{-1}\Delta I+b_c$.

3) Cyber-Attack 3; MITM attack in the Communication Links: The communicated values are previously defined as all the parameters following the Laplacian. We define $\Delta\lambda$ and Δv_c as the attack-vectors, and the two (cyber and physical) inputs are in closed-loop re-defined as: $u_{\rm el}=-ry_{\rm el}+w^{-1}y_c+b+r_1\Delta\lambda+r_2\Delta v_c$ and $u_c=2\alpha y_{\rm el}+b_c+\Delta\lambda$, where $r_1\triangleq-w^{-1}K_p\mathcal{L}$ and $r_2\triangleq-2\alpha\mathcal{L}K_I$.

IV. Perturbed Equilibrium and Resilience Strategy

The perturbed linear system is proven to be ISS against any potential cyber-attack. The subsequent objective is to assess the capability to stabilize around an optimal operating point under a resilient control strategy, ensuring both the KKT condition in (8) and maintaining average voltage regulation, even under hostile conditions.

A. Proposed Resilient Control Tuning Strategy

The controller under consideration is highly dependent on the control parameter α, which suggests adopting the following initial resilience strategy as a starting point.

Hypothesis *1: The resilience is ensured when tuning the primary control parameter matrix* $\boldsymbol{\alpha}$ *by a scalar to a sufficiently high value, removing the effect of the perturbation term and establishing a resilient controller robust against all cyber-attacks.* Notice that $\mathcal{B}$ and γ will need to be appropriately scaled to prevent modifying the objective of the original cost function.

In the upcoming section, we evaluate the effectiveness of the controller in steering the MG to an optimal steady state, where the control objectives are met under perturbed conditions. Our analysis reveals that *Hypothesis* 1, does not fully mitigate the influence of attacks. More precisely, in hostile situations, increasing the control parameter α is shown to improve the consensus property at the equilibrium, but not improving the improving the average voltage regulation. Motivated by this shortcoming, we propose a new control modification aimed at regulating the average voltage to a desired reference level.

Definition *1:* The secondary control tuning parameter ζ is added in the voltage controller resulting in

$$\begin{aligned}V^{\mathcal{G}}&=V_{nom}-R^{\mathcal{D}}I^{\mathcal{G}}+\zeta u_{\rm el},\\\text{with}\quad u_{\rm el}&=-r_{\rm new}y_{\rm el}-\omega^{-1}y_c+b,\end{aligned} \tag{16}$$

with $r_{\rm new}=-\frac{1}{\zeta}R^D+K_pw^{-1}\mathcal{L}w^{-1}$, $K_p>0$ and $\zeta=\frac{1}{\mu}>0$. The ultimate resilient tuning strategy is subsequently introduced, combining *Hypothesis* 1 with the proposed modifications.

Hypothesis *2: The resilience is ensured when tuning both the primary control parameters* $\boldsymbol{\alpha}$*,* $\mathcal{B}$ *and the secondary control parameter* ζ *to appropriate values, removing the effect of the perturbation term introduced by all cyber-attacks.*

B. Equilibrium Analysis

1) Cyber-Attack 1: Following the same approach as in Section II-E the weighted voltage sum in steady state under the attack is

$$1_{n_i}^{\top}w\bar{V}=1_{n_i}^{\top}w1_{n_i}V_{nom}+1_{n_i}^{\top}w\zeta\Delta\bar{u} \tag{17}$$

Recall, from the definitions in *Proposition* 2 that $\omega^{-1}=2\alpha$. Hence, increasing only this *primary* control parameter is not sufficient to reduce the influence of the attack. However, following *Hypothesis* 2 sufficiently high tuning values of μ are shown to reduce the influence of the attack, to the point where the average voltage regulation is achieved at the new equilibrium. On the other hand, following *Hypothesis* 2, the steady state operations of the cyber layer is redefined as $0=-\zeta K_I \mathcal{L}\bar{\lambda}$. The new steady state does not hinder convergence to a unified optimal value of λ. However, when considering the dynamics given in (9), it becomes evident that care must be taken when tuning these control parameters as $\mu \gg 2\boldsymbol{\alpha}$ (i.e., $\zeta \ll 2\boldsymbol{\alpha}$). To prevent the derivative of the system tends to zero regardless of the consensus value, under the significant small ζ, we recommend the following practical tuning criteria: *While μ is tuned to a significantly high value above a given threshold, $\boldsymbol{\alpha}$ needs to be tuned with at least half the value of μ.*

2) Cyber-Attack 2: For the attack under consideration, the equilibrium of (3) now reads:

$$0=-\zeta\mathcal{L}(2\alpha(\bar{y}_{\text{el}}+\Delta\bar{I})+\mathcal{B})=-\zeta\mathcal{L}\bar{\lambda}^*. \tag{18}$$

The above expression indicates that the forced control network converges to the steady state equilibrium when $-\mathcal{L}\bar{\lambda}^*$ equals zero, which implies that $\bar{\lambda}^* = \mathbf{1}_{n_i^c}\lambda^*$ is the consensus value. However, $\mathbf{1}_{n_i^c}\bar{\lambda}^* \neq \mathbf{1}_{n_i^c}\bar{\lambda}_{\text{opt}}$. Hence, the obtained consensus property significantly diverges the converged equilibrium from the unforced equilibrium. Eq. (18) indicates that neither tuning of α nor ζ reduces the influence of the attack. When assessing the voltage controller under this attack, the Laplacian ensures that eq. (12) is satisfied, regardless of the attack or the tuning of α and ζ. This is because the attack classifies as a stealth attack, perturbing more discrete in the dynamics, able to deceive the voltage controller. Both objectives appear to be ensured, however, the consensus value is not the true optimal, preventing the controller from steering the MG to the desired operation.

3) Cyber-Attack 3: For the attack under consideration, the equilibrium of (3) now reads:

$$0=g_c\bar{u}_c=-\zeta\mathcal{L}(\bar{\lambda}+\Delta\bar{\lambda})=-\zeta\mathcal{L}\big((2\alpha\bar{y}_{\text{el}}+\mathcal{B})+\Delta\bar{\lambda}\big) \tag{19}$$

The above expression demonstrates that the converged equilibrium is not the optimum. From the above equation, it can be seen that tuning of α (and $\mathcal{B}$) to significantly high values in line with *Hypothesis* 1 reduces the effect of the attack as $\bar{\lambda}=2\alpha\bar{y}_{\text{el}}+\mathcal{B}$ will be significantly greater than the attack value. When assessing the voltage controller, under this attack, the Laplacian ensures that (12) is satisfied, regardless of the attack or the tuning of α and ζ.

V. Case Studies

In this section, the controller of [3] under our proposed resilient tuning strategy is tested on a 48-volt dc network, powered by 4 DGs. The specifications of the generators, loads, transmission lines, and control parameters follow the specifications given in Table I in Section IV in [3]. To attain desired resilient performance, α and $\mathcal{B}$ are tuned to 50, and μ is tuned to 100 such that $\zeta=1/100$.

Optimal Operations: Initially, the unperturbed MG is simulated serving as the baseline scenario. In the following subsections, this system is simulated under the three hostile cyber-attacks while the resilient strategy is implemented, aiming to maintain optimality. At $t=3$s, the distributed controller is activated, replacing the primary droop controller. Additionally, the optimal performance of the controller is tested under smaller system changes, increasing and decreasing the power consumption at the loads up to 75%. The simulations in Fig.2 illustrate a stable system, able to ensure both control objectives in steady state. Fig.2(a) shows that the distributed DGs compensate by cooperatively reducing and increasing their voltages in these events, and simultaneously achieving average voltage containment given in Fig.2(b). Additionally, they proportionally share their generated currents in steady state as all DGs contribute with the same amount of rated power, given in Fig.2(c) and Fig.2(d) illustrates the optimal generated currents under these events.

Cyber-Attack 1. The system is now simulated under the influence of the FDI attack-vector: $\Delta u = [5,1,0,10]^\top$. Fig.3(e) illustrates that the attack prevents the system from achieving average voltage regulation. However, under the proposed resilient strategy the MG is steered to the optimal steady state where near-nominal voltage regulation is ensured within a practically tolerated $\pm 5\%$ deviation, as illustrated in Fig.3(f)[1]

Cyber-Attack 2. The stealth attack-vector: $\Delta I = [1,3,6,0]^\top$ is implemented as a perturbation in the current sensors of the DGs.

[1]In Section IV-B.1-IV-B.3 neither the imposed cyber-attacks nor the resilient strategy hinders proportional power sharing (under attack 1) or near-nominal voltage regulation (under attack 2 and 3). This is also validated through simulations, however, the simulation results have been omitted for compactness.

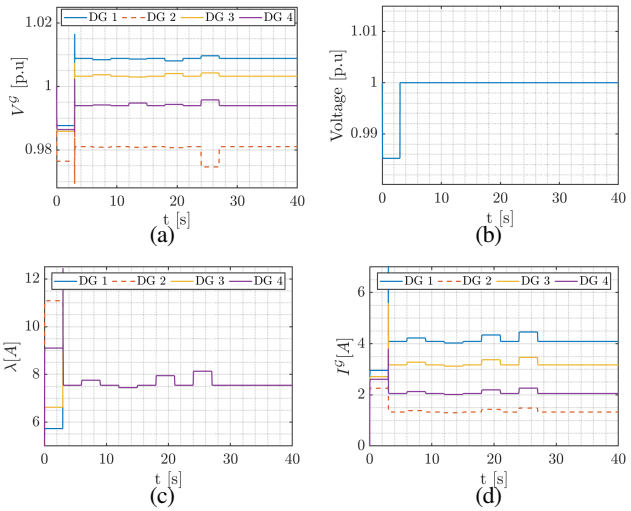

Fig. 2: Results for the unforced MG: (a) Generated voltages, (b) Average sum of generated voltage, (c) Individual λ values, d) Generated currents.

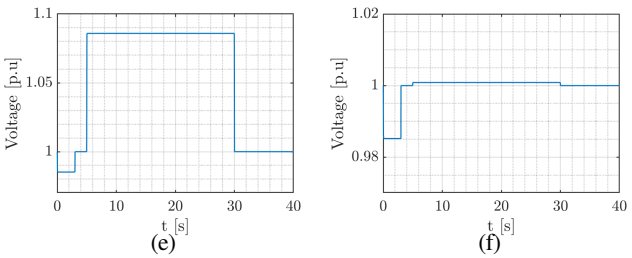

Fig. 3: MG under cyber-attack 1: Average sum of generated voltages (e) without and (f) with proposed resilient tuning.

Fig.4(g) shows that the DGs agree upon a rated current value when subject to the attack, however higher than the optimal value in Fig.2(c), consequently affecting the generated currents in Fig.4(h). Additionally, Fig.4(i)(j) shows that our strategy does not remove the influence of the perturbation. *Cyber-Attack 3.* The MITM attack-vectors are simulated as perturbations in the communication links between the DGs. To test the resilience against both constant and time-varying attacks, we simulate $\Delta\lambda(t) = [5\cdot\sin(t),3,8,0]^\top$ and $\Delta v_c = [1,15,0,3]^\top$. Fig.5(k)(l) shows that the DGs agree upon a consensus value, varying and higher than the optimal value, consequently disturbing the generated currents. However, Fig.5(m)(n) shows that the resilient strategy ensures optimal operations, reducing the influence of the attack. Even though the consensus value λ_{opt} is significantly scaled due to the resilient tuning, this optimal tuning still guarantees optimal operations of the physical system as illustrated in Fig.5(n).

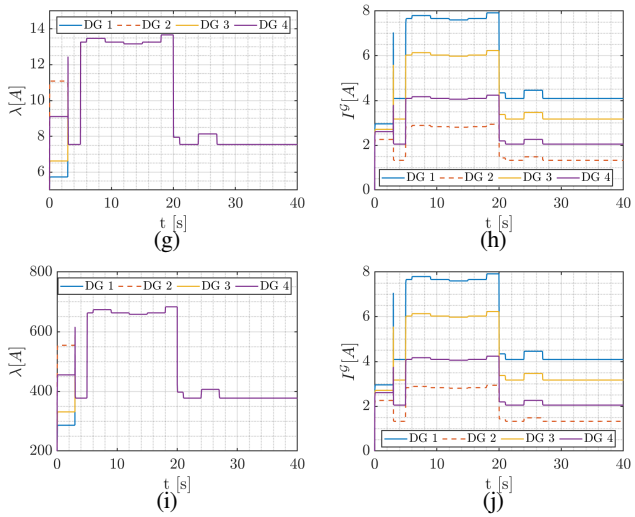

Fig. 4: MG under cyber-attack 2: (g) λ_i values, (h) Generated currents, effect of proposed tuning on (i) λ_i values and (j) Generated currents.

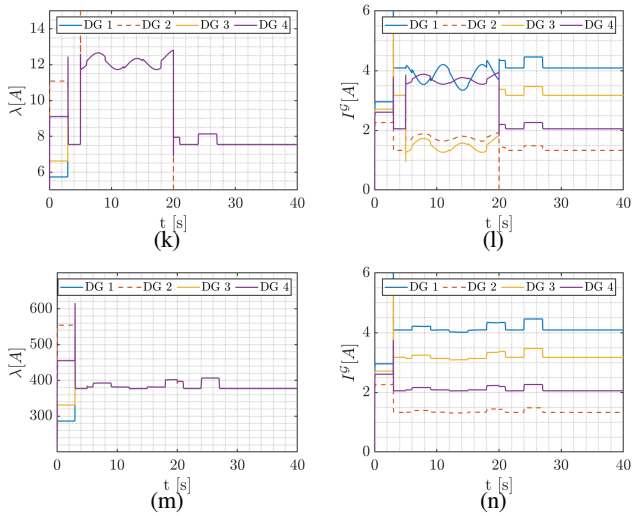

Fig. 5: MG under cyber-attack 3: (k) λ_i values, (l) Generated currents; effect of proposed tuning on (m) λ_i values and (n) Generated currents.

VI. Conclusion

This paper investigated the impact of cyber-threats of a dc microgrid under the distributed (energy-based) control and optimization proposal of [3], and proposed a tuning strategy along with minor structural modifications to increase its resilience. After reviewing the contribution in [3], we used the port-Hamiltonian approach to ease the procedure in finding a Lyapunov function, which we used to conclude *input-to-state stability* and *boundedness* of the system, even in the presence of (bounded) cyber-attacks. Furthermore, through a thorough equilibrium analysis this control strategy is evaluated with respect to its ability to still ensure optimal operations in steady state, giving rise to a tuning strategy as well as a minor modification in the controller structure which made it resilient against False Data Injection Attacks (FDIA) and MITM attacks. However, for the more discrete stealth attacks, in the current measurements of the voltage controller, these modifications were not sufficient to bring the system close to the unperturbed optimal operating conditions. The controller ensures both control objectives in steady state, but achieves consensus under false premises. Finally, through time-domain simulations, we demonstrate the effectiveness of the method and validity of the analysis for both time-varying and constant attack-vectors.

References

[1] B. Abdolmaleki, J. Simpson-Porco, and G. Bergna-Diaz, "Distributed optimization for reactive power sharing and stability of inverter-based resources under voltage limits," *IEEE Trans. Smart Grid*, to be published.

[2] L. Xiong, X. Liu, Y. Liu, and F. Zhuo, "Modeling and stability issues of voltage-source converter-dominated power systems: A review," *CSEE Journal of PES*, vol. 8, no. 6, pp. 1530–1549, 2022.

[3] B. Abdolmaleki and G. Bergna-Diaz, "Distributed control and optimization of dc microgrids: A port-hamiltonian approach," *IEEE Access*, vol. 10, pp. 64 222–64 233, june 2022.

[4] M. Sadabadi and A. Gusrialdi, "On resilient design of cooperative systems in presence of cyber-attacks," *2021 Eur. Control Conf. (ECC)*, pp. 946–951, 2021.

[5] S. Subham, T. Dragičević, and F. Blaabjerg, "An event-driven resilient control strategy for dc microgrids," *IEEE Trans. on Pow. Electron.*, vol. 35, no. 12, pp. 13 714–13 724, 2020.

[6] S.Sahoo, J. Chih-Hsien, S.Mishra, and T. Dragičević, "Distributed screening of hijacking attacks in dc microgrids," *IEEE Trans. on Power Electr.*, vol. 35, no. 7, pp. 7574–7582, 2020.

[7] D. Annavaram, S.Sahoo, and S.Mishra, "Stealth attacks in microgrids: Modeling principles and detection," *2021 9th IEEE Int. Conf. on Pow. Syst. (ICPS)*, pp. 1–6, 2021.

[8] M. Sadabadi, S. Sahoo, and F. Blaabjerg, "Resilient distributed control strategies in microgrids against cyber attacks," in *Cyber Security for Microgrids*, S. Subham, T. Dragičević, and F. Blaabjerg, Eds. Stevenage: The Institution of Engineering and Technology, 2022, p. 227 –245.

[9] O. Beg, T. Johnson, and A. Davoudi, "Detection of false-data injection attacks in cyber-physical dc microgrids," *IEEE Trans, on Ind. Inform.*, vol. 13, no. 5, p. 2693–2704, 2017.

[10] A. Cecilia, S. Sahoo, T. Dragičević, R. Costa-Castelló, and F. Blaabjerg, "Detection and mitigation of false data in cooperative dc microgrids with unknown constant power loads," *IEEE Trans. on Power Electr.*, vol. 36, no. 8, pp. 9565–9577, 2021.

[11] A. Gallo, M. Turan, F. Boem, T. Parisini, and G. Ferrari-Trecate, "A distributed cyber-attack detection scheme with application to dc microgrids," *IEEE Trans. on Aut. Contr.*, vol. 65, no. 9, p. 3800–3815, 2020.

[12] M. Sadabadi, S. Sahoo, and F. Blaabjerg, "Stability-oriented design of cyberattack-resilient controllers for cooperative dc microgrids," *IEEE Trans. on Power Electr.*, vol. 37, no. 2, pp. 1310–1321, 2022.

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

[14] M. Sadabadi, "Attack-resilient distributed control in dc microgrids," *2021 European Control Conference (ECC)*, pp. 503–508, 2021.

[15] H. K. Khalil, *Nonlinear Control*, 1st ed. Pearson Education, 2015.