Distributed Control of Parallel DC-DC Converters Under FDI Attacks on Actuators

Sadabadi, Mahdieh S.; Mijatovic, Nenad; Tregouet, Jean Francois; Dragicevic, Tomislav

Published in:
IEEE Transactions on Industrial Electronics

Link to article, DOI:
10.1109/TIE.2021.3123613

Publication date:
2022

Document Version
Peer reviewed version

Distributed Control of Parallel DC-DC Converters Under FDI Attacks on Actuators

Mahdieh S. Sadabadi, *Senior Member, IEEE*, Nenad Mijatovic, *Senior Member, IEEE*, Jean-François Trégouët, and Tomislav Dragičević, *Senior Member, IEEE.*

***Abstract*—The parallel connection of DC-DC converters requires the development of an appropriate control strategy that regulates load voltage and shares current amongst participating converters. This paper proposes a resilient and robust cooperative distributed control approach that simultaneously ensures voltage regulation and balanced current sharing in parallel DC-DC converters in the presence of false data injection attacks on control input channels. Based on analytical tools from network control and Lyapunov stability theory, concise stability certificates are derived. The proposed cooperative distributed control strategy guarantees resilience against unknown bounded attacks on the actuators of DC-DC converters and the robustness to uncertainties in load parameters and the physical parameters of converters. Furthermore, the control design for each converter does not require any knowledge about the number of participating converters. The detailed simulation and experimental results verify the satisfactory performance of the proposed method in voltage regulation and balanced current sharing in parallel converters, as well as resilience to bounded false data injection attacks.**

***Index Terms*—Parallel DC-DC converters, cooperative distributed control, resilient control, false data injection (FDI) attacks.**

I. Introduction

THE parallel-connected DC-DC converter systems offer several advantages over a single high-capacity centralized converter, including increased reliability, potential for higher efficiency, better dynamic performance, ease of maintenance and repair, improved thermal management, and reduced stress levels on the constituent converters, as the total load current can be shared among the converters [1]–[3]. Due to their numerous advantages, they have been extensively used in a large number of applications such as railway vehicles, electric aircraft, and zero-emission ferries.

Despite the potential benefits that the parallel interconnection of DC-DC converters bring, they require appropriate control schemes to regulate load voltage and accurately share load demands amongst existing converters [2]. Unbalanced current distribution causes the converter overloading and overheating and might lead to the overall system's failure [4]. Extensive research has been carried out in the area of designing controls for accurate load sharing in parallel DC-DC converters, e.g. droop-based methods [5]–[8], integral-variable-structure- and multiple-sliding-surface-based control [9], master-slave current sharing control [10], finite-time control [11], geometric decoupling in state and input spaces [12], [13], as well as cooperative and distributed control techniques [4], [14]–[16]. These approaches assume an ideal control framework with ideal sensors, actuators, and communication networks. Nevertheless, such an assumption might not be realistic, as in practice communication links can fail and cyber-attacks can easily compromise the normal operation of control systems. These events might lead to detrimental impacts on the stability and performance of entire systems. Since parallel DC-DC converters are often used in mission-critical applications where cybersecurity and reliability are a main concern, it is essential to enhance the resilience of control systems against cyber-attacks and infiltration.

False data injection (FDI) attacks are one of the most common cyber-attacks which compromise control systems by injecting false information into their vulnerable elements; i.e. sensors, actuators, or communication links [17]. To enhance resilience in DC systems against FDI attacks, several model-based and data-driven attack detection and mitigation methods have recently been investigated in [18]–[22] and references therein. However, these approaches mainly rely on a strict assumption that at least half of the disrupted converters' neighbors should be healthy. As a result, they are not applicable for worst-case scenarios in which all DC-DC converters are subject to FDI cyber-attacks. To deal with this limitation, resilient distributed control strategies have emerged. A trust-based cooperative control strategy for DC microgrids under FDI cyber-attacks on communication links and controller hijacking has been proposed in [23]. Although this control paradigm mitigates the adverse effects of such attacks, it entails high computation burdens in order to calculate the trustworthiness of incoming information at each converter. Moreover, to ensure an attack-resilient operation of DC networks using the proposed control approach in [23], more than half of the neighboring converters should be healthy and not be under cyber-attacks. A resilient distributed adaptive control mechanism against unbounded FDI attacks on actuators has been developed in [24]. Since in practice bounded attacks are more probable [25], as any unbounded attacks can easily be

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

J. F. Trégouët is with the Univ Lyon, INSA Lyon, Université Claude Bernard Lyon 1, Ecole Centrale de Lyon, CNRS, Ampère, UMR5005, 69621 Villeurbanne, France (e-mail: jean-francois.tregouet@insa-lyon.fr).

N. Mijatovic are T. Dragičević are with the Department of Electrical Engineering, Technical University of Denmark, 2800 Kongens Lyngby, Denmark (e-mail: nm@elektro.dtu.dk and tomdr@elektro.dtu.dk).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIE.2021.3123613, IEEE Transactions on Industrial Electronics

detected by an anomaly detection protocol, the relevance of the problem presented in [24] is somewhat limited.

To the best of our knowledge, the research on cyber-attack-resilience of control mechanisms in parallel DC-DC converters is still in its infancy and can benefit from further studies. Motivated by this and the aforementioned concerns with the existing attack detection techniques, this paper presents a cooperative distributed control framework developed for parallel DC-DC converters, paying special attention to the resilience of distributed controllers against FDI cyber-attacks on control input channels (actuators). This type of cyber-attacks makes control decisions incorrect, potentially causing equipment damage and adversely impacting the system performance. The main contributions of this paper can be summarized as follows:

- In contrast to conventional cooperative and distributed control strategies (e.g., [4], [11], [14]–[16]), the proposed distributed control framework is resilient to FDI cyber-attacks on actuators. Hence, it simultaneously regulates load voltage and distributes load current equally amongst DC-DC converters in the presence of FDI cyber-attacks.
- Unlike the finite-time control technique in [11], the proposed control approach in this paper can be applied to a general case of $N \geq 2$ parallel DC-DC converters where the converters' inductances can have different values. Furthermore, the proposed controller does not require the rate of change of output voltage that is required in [9].
- Unlike the proposed attack detection and mitigation methods (e.g., [18], [19], [21]–[23]), the proposed cooperative distributed control method does not entail significant computational burdens, as the design of resilient cooperative controllers can be done in a decentralized manner. Furthermore, we do not make any restrictive assumptions on the number of compromised DC-DC converters. As a result, the proposed resilient cooperative distributed control strategy can guarantee full resilience even if all power converters are subject to FDI cyber-attacks on their control input channels.
- We propose stability certificates based on results from network control theory and Lyapunov methods. These certificates provide theoretical guarantees of voltage regulation and balanced current sharing in the parallel interconnection of DC-DC converters, regardless of the existence of FDI attacks on actuators and the number of attacked converters. The extreme attack scenario that would make the proposed control framework invalid is also analyzed in this paper. The simulation and experimental results demonstrate the effectiveness of the proposed resilient cooperative control scheme for parallel DC-DC converters.

The rest of the paper is organized as follows: Section II formulates the problem addressed in this paper. Section III proposes a resilient cooperative distributed control mechanism that guarantees the voltage regulation and balanced current sharing among constituent converters in the presence of false data injection attacks, and discusses theoretical stability analysis aspects. The FDI-attack-resilient property of the proposed cooperative distributed control approach is investigated in Section IV and comprehensive design criteria of the control parameters of the proposed resilient distributed control framework are given. The experimental results and comparative simulation case studies are given in Section V. The paper ends with concluding remarks in Section VI.

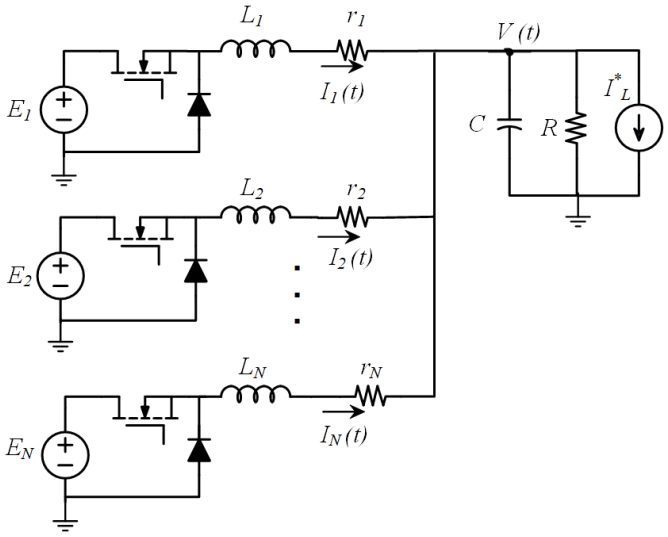

Fig. 1. The parallel connection of N DC-DC buck converters feeding a common load.

Notation: The notation used in this paper is standard. In particular, $\mathbf{1}_N$, $\mathbf{0}_N$, and $\mathbf{I}_N$ are an $N \times 1$ vector of ones, an $N \times 1$ zero vector, and an $N \times N$ identity matrix, respectively. For a symmetric matrix X, the positive definite and negative definite operators are shown by $X \succ 0$ and $X \prec 0$, respectively. The symbol $diag(x_1, \ldots, x_N)$ indicates a diagonal matrix whose diagonal elements are x_i, $i = 1, \ldots, N$.

II. Parallel DC-DC Converters

A. Dynamic Models

Consider a parallel interconnection of N heterogeneous DC-DC converters connected to a common load, as depicted in Fig. 1.

The dynamics of each DC-DC buck converter can be derived from Kirchhoff's current (KCL) and voltage laws (KVL), as follows:

$$\begin{aligned} L_i \dot{I}_i(t) &= -r_i I_i(t) - V(t) + u_i(t), \\ C\dot{V}(t) &= \sum_{i=1}^{N} I_i(t) - \frac{V(t)}{R} - I_L^*, \end{aligned} \tag{1}$$

for $i = 1, \ldots, N$, where L_i is inductance of converter i, C is the output capacitance, r_i is the parasitic resistance of the inductor L_i, $R > 0$ is the common load resistance, $I_L^* \geq 0$ is a constant current load, $I_i(t)$ is the current of converter i, and $V(t)$ is the load voltage. The control input of the converter i is $u_i(t) = E_i d_i(t)$ where $d_i(t)$ is the duty cycle of converter i and E_i is the DC voltage of the input side of converter i.

B. False Data Injection Attacks on Control Channels

Malicious attackers might inject false data to perturb the local control signal $u_i(t)$. This perturbation might lead to a

detrimental impact on the stability and performance of the parallel converter system. Hence, it is required to develop a control mechanism which is resilient to such attacks.

Under the potential FDI attacks on the control input $u_i(t)$, one obtains that:

$$\hat{u}_i(t) = u_i(t) + \Delta u_i(t), \tag{2}$$

where $\hat{u}_i(t)$ is the disrupted control input applied to the converter i, $u_i(t)$ is the desired control input, and $\Delta u_i(t)$ indicates the false data injection to the control input of the converter i. Note that by injecting false data $\Delta u_i(t)$ in (2) to control input channels $u_i(t)$, incorrect control decisions are sent to each DC-DC converter, this might lead to potential equipment damages and adversely impact the performance of parallel converter systems.

Assumption 1. *It is assumed that $\Delta u_i(t)$ is a uniformly bounded signal for each converter. Moreover, the false data injection $\Delta u_i(t)$ is independent of the current and voltage signals of converters.*

Note that the assumption on uniformly bounded false data attack injections is reasonable, as unbounded FDI cyber-attacks can easily be detected by conventional anomaly detection protocols [25]. Moreover, in the case of unbounded attack injections, simple filtering can be applied so that excessively large signals received by actuators are removed or filtered [25].

C. Control Problem Statement

The main aim of this paper is to develop a control mechanism for parallel-connected DC-DC converters so that the following objectives are guaranteed:

Voltage Regulation. The first control objective is to regulate the steady-state value of DC bus voltage $V(t)$ at a given reference value V^* for the unknown load profile; i.e.,

$$\lim_{t\to\infty} V(t) = V^*. \tag{3}$$

Balanced Current Sharing. The second objective is to equally distribute the total current demand among the converters at the steady state; i.e.,

$$\lim_{t\to\infty} I_1(t) = \cdots = \lim_{t\to\infty} I_N(t), \tag{4}$$

Resilience to FDI cyber-attacks on Actuators. The third objective is the resilience of the proposed control strategy against bounded FDI attacks $\Delta u_i(t)$ on the control input channels $u_i(t)$. As a result, the voltage regulation and balanced current sharing should be guaranteed regardless of the existence of such attacks.

III. Proposed Resilient Control Strategy

This section presents a load-independent cooperative distributed control mechanism for the voltage regulation and balanced current sharing problems in the parallel-connected DC-DC converters. We show that our proposed control strategy is resilient to the bounded perturbation in the control input channels and is robust to uncertainties in the physical parameters of DC-DC converters as well as the common load.

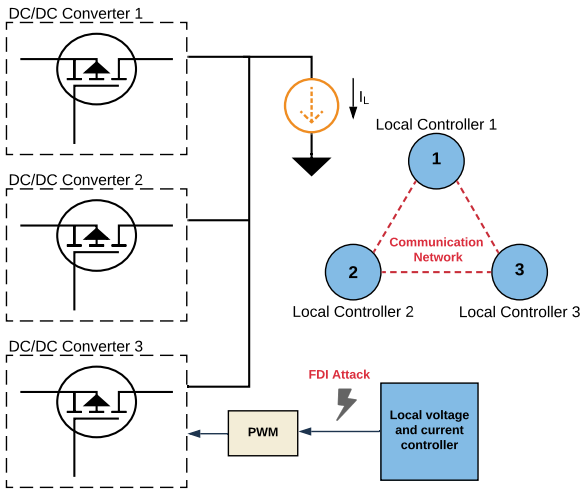

Fig. 2. A schematic diagram of a $N = 3$ parallel DC-DC converter system augmented with the proposed resilient cooperative control strategy in (5). It is assumed that the control input channels are subject to false data injection attacks. In this figure, the solid black lines show the physical interconnection of DC-DC converters whereas the red dashed lines show the communication links amongst local controllers.

A. Resilient Cooperative Distributed Control Approach

In order to guarantee both voltage regulation and current sharing problems in (3) and (4), the following local voltage and current controller is proposed for converter i; $i = 1\ldots,N$:

$$\begin{aligned} u_i(t) &= k_{i,1}V(t) + k_{i,2}I_i(t) + k_{i,3}v_i(t) + k_{i,4}\sum_{j=1}^{N}\alpha_{i,j}\left(I_i(t) - I_j(t)\right), \\ \dot{v}_i(t) &= -V(t) + V^* - \gamma\sum_{j=1}^{N}\alpha_{i,j}\left(I_i(t) - I_j(t)\right), \end{aligned} \tag{5}$$

where $\alpha_{ij} = \alpha_{ji} \geq 0$, $\gamma > 0$, and $K_i = \begin{bmatrix} k_{i,1} & k_{i,2} & k_{i,3} & k_{i,4} \end{bmatrix}$ are the control parameters which need to be properly designed. In (5), $v_i(t)$ is the state of the controller of converter i.

The parameters α_{ij}, $i,j = 1,\ldots,N$ in (5) determine the communication amongst different converters. As one can observe from (5), the controller of each converter does not require any knowledge about the physical parameters of other converters, the capacitor value, load current, and the common load value. We will show that by a proper design of the control gains $K_i = \begin{bmatrix} k_{i,1} & k_{i,2} & k_{i,3} & k_{i,4} \end{bmatrix}$, the proposed cooperative control approach in (5) guarantees the closed-loop stability and provides resilience to the FDI attacks on actuators. Without these gains, the consensus-based controllers are fragile to the perturbations and false data injections to control input channels. More details about the vulnerability of existing consensus-based controllers to FDI cyber-attacks will be presented in study cases in Section V.

Remark 1. *(Graph Representation of Communication Networks). The communication network in the control strategy proposed by (5) can be represented by a connected undirected graph $\mathcal{G}_{\mathscr{C}} = (\mathcal{V}_{\mathscr{C}}, \mathcal{E}_{\mathscr{C}})$, where $\mathcal{V}_{\mathscr{C}}$ and $\mathcal{E}_{\mathscr{C}}$ are the set of vertices and edges, respectively. Each element in the vertex set $\mathcal{V}_{\mathscr{C}} = \{1,..,N\}$ and the edge set $\mathcal{E}_{\mathscr{C}}$ respectively represents a*

DC-DC converter and the information flow amongst existing converters. Parameters $\alpha_{i,j}$ in (5) are adjacency elements associated with the edges of the communication graph $\mathcal{G}_{\mathscr{C}}$ [26].

The overall parallel-connected buck converters in (1) with the proposed resilient cooperative control strategy in (5) can be described in a vector form as follows:

$$\begin{aligned} C\dot{V}(t) =& \mathbf{1}_N^T\mathbf{I}(t) - I_L(t), \\ [L]\dot{I}(t) =& ([k_1]-\mathbf{I}_N)\mathbf{1}_N V(t) + ([k_2]-[r])\mathbf{I}(t) + [k_3]\,\mathbf{v}(t) \\ &+ [k_4]\,\mathbb{L}_{\mathscr{C}}\mathbf{I}(t) + \Delta\mathbf{u}(t), \\ \dot{\mathbf{v}}(t) =& -\mathbf{1}_N V(t) + \mathbf{1}_N V^* - \gamma\mathbb{L}_{\mathscr{C}}\mathbf{I}(t), \end{aligned} \tag{6}$$

where $\mathbf{I}(t) = [I_1(t),\ldots,I_N(t)]^T$, $\mathbf{v}(t) = [v_1(t),\ldots,v_N(t)]^T$, $\Delta\mathbf{u}(t) = [\Delta u_1(t),\ldots,\Delta u_N(t)]^T$, $[L] = \text{diag}(L_1,\ldots,L_N)$, $[r] = \text{diag}(r_1,\ldots,r_N)$, and $[k_j] = \text{diag}(k_{j,1},\ldots,k_{j,N})$ for $j = 1,\ldots,4$. Matrix $\mathbb{L}_{\mathscr{C}} \in \mathbb{R}^{N\times N}$ in (6) is the weighted Laplacian matrix associated with the undirected connected communication graph $\mathcal{G}_{\mathscr{C}}$ with an incidence matrix $\mathbb{A}_{\mathscr{C}} \in \mathbb{R}^{N\times N}$ whose (i,j) entry is $\alpha_{i,j}$ [26]. The graphical scheme of the parallel-connected DC-DC converter combined with the proposed resilient control strategy is depicted in Fig. 2.

Remark 2. *(Topology of Communication Graph). The topology of the communication graph $\mathcal{G}_{\mathscr{C}}$ is free as long as it is connected and undirected. In fact, the graph $\mathcal{G}_{\mathscr{C}}$ is assumed to belong to the following set:*

$$\Gamma_N = \left\{\mathcal{G}_{\mathscr{C}} : \textit{rank}(\mathbb{L}_{\mathscr{C}}) = N-1,\, \mathbf{1}_N^T\mathbb{L}_{\mathscr{C}} = \mathbf{0}_N^T,\, \mathbb{L}_{\mathscr{C}}\mathbf{1}_N = \mathbf{0}_N\right\}. \tag{7}$$

In this paper, the following connected undirected communication network topology is used that characterizes a trade-off between performance and the number of communication links.

$$\alpha_{i,j} = \begin{cases} 1, & \textit{if } \mid i-j \mid = 1 \textit{ or } \mid i-j \mid = N-1, \\ 0, & \textit{otherwise}. \end{cases} \tag{8}$$

B. Stability Analysis

In this subsection, the stability of the closed-loop system in (6) in the presence of FDI cyber-attacks on the control signals is analyzed. To this end, the equilibria of (6) in the absence of the attack vector $\Delta\mathbf{u}(t)$ are characterized in Lemma 1 and then the stability results are presented in Lemma 2.

Lemma 1. *Consider the parallel DC-DC buck converter in (1) augmented with the proposed resilient cooperative control scheme in (5) in the absence of the attack vector $\Delta\mathbf{u}(t)$. It is assumed that $k_{i,3} \neq 0$ for all for $i \in \mathcal{V}_{\mathscr{G}}$. There exists a unique equilibrium $(\bar{I},\bar{V},\bar{v})$ satisfying*

$$\begin{aligned} \bar{I} &= \frac{1}{N}\mathbf{1}_N\left(\frac{V^*}{R} + I_L^*\right), \\ \bar{V} &= V^*, \\ \bar{v} &= [k_3]^{-1}\left((\mathbf{I}_N - [k_1])\mathbf{1}_N V^* + ([r]-[k_2])\bar{I}\right). \end{aligned} \tag{9}$$

where $\bar{V}$, $\bar{I}$, and $\bar{v}$ are the steady state values of the load voltage $\mathbf{V}(t)$, the converter current $\mathbf{I}(t)$, and $\mathbf{v}(t)$, respectively.

Proof. See Appendix A in Section VII. □

Let define a new closed-loop state variable $x_{cl} = \begin{bmatrix} V-\bar{V} & (\mathbf{I}-\bar{I})^T & (\mathbf{v}-\bar{v})^T \end{bmatrix}^T$. The closed-loop system in (6) can be rewritten in a state-space framework as follows:

$$\dot{x}_{cl}(t) = A_{cl}x_{cl}(t) + B_{cl}\Delta\mathbf{u}(t), \tag{10}$$

where (A_{cl},B_{cl}) are defined as follows.

$$\begin{aligned} A_{cl} &= \begin{bmatrix} -\frac{1}{RC} & \frac{1}{C}\mathbf{1}_N^T & \mathbf{0}_{1\times N} \\ [L]^{-1}([k_1]-\mathbf{I}_N)\mathbf{1}_N & [L]^{-1}([k_4]\mathbb{L}_{\mathscr{C}} + [k_2] - [r]) & [L]^{-1}[k_3] \\ -\mathbf{1}_N & -\gamma\mathbb{L}_{\mathscr{C}} & \mathbf{0}_{N\times N} \end{bmatrix} \\ B_{cl} &= \begin{bmatrix} \mathbf{0}_{N\times 1} & [L]^{-1} & \mathbf{0}_{N\times N} \end{bmatrix}^T. \end{aligned} \tag{11}$$

The following lemma analyzes the stability of the parallel-converter system combined with the proposed resilient control strategy in (5).

Lemma 2. *For $i \in \mathcal{V}_{\mathscr{C}}$, let control gain $K_i = \begin{bmatrix} k_{i,1} & k_{i,2} & k_{i,3} & k_{i,4} \end{bmatrix}$ belong to the following set*

$$\chi_{[i]} = \left\{ (k_{i,1},k_{i,2},k_{i,3},k_{i,4}) : \begin{array}{l} k_{i,1} < 1, \quad k_{i,2} < r_i \\ 0 < k_{i,3} < \dfrac{1}{L_i}(r_i - k_{i,2})(1-k_{i,1}) \\ k_{i,4} = \gamma(k_{i,1}-1) \end{array} \right\}. \tag{12}$$

Then, the following statements hold.

1) *A_{cl} in (11) is Hurwitz.*
2) *The states of the closed-loop system in (10) are bounded for any bounded FDI cyber-attacks $\Delta\mathbf{u}(t)$ on the control input channels.*

Proof. See Appendix B in Section VII. □

Remark 3. *Note that $\chi_{[i]}$ is not an empty set since inequalities $k_{i,1} < 1$ and $k_{i,2} < r_i$ imply that $0 < \frac{1}{L_i}(r_i - k_{i,2})(1-k_{i,1})$.*

Remark 4. *(Robustness to Physical System Parameters). One of the main features of the proposed control technique in (5) is its robustness against uncertainties affecting the load resistance R and capacitance C. As one can observe from (5) and (12), the control law and the closed-loop stability are independent of these parameters. Therefore, the closed-loop system in (6) is robustly stable with respect to the parameter uncertainty in R and C. If the converter inductance L_i has an interval uncertainty $L_{i,min} \leq L_i \leq L_{i,max}$, the control gain $k_{i,3}$ in (5) should be chosen such that $0 < k_{i,3} < \frac{1}{L_{i,max}}(r_i - k_{i,2})(1-k_{i,1})$. As a result, the accurate voltage regulation and current sharing are achieved for every value of $R > 0$, $C > 0$, and $L_{i,min} \leq L_i \leq L_{i,max}$; $i = 1,\ldots,N$.*

IV. Attack-Resilience Feature of Proposed Cooperative Distributed Control Strategy

In this section, it is demonstrated that the proposed cooperative control approach in (5) is resilient against false data injection cyber-attacks on actuators, modeled in (2). The results are presented in the following theorem:

A. Attack-Resilience Analysis

Theorem 1. *In the presence of bounded false data injection attacks (2) on actuators, the voltage regulation and the balanced current sharing objectives can be arbitrarily accurate if $k_{i,3}, i \in \mathcal{V}_{\mathscr{C}}$, is sufficiently large and other controller gains are selected according to Table I, so that*

$$\forall \delta_V > 0, \forall \delta_I > 0,\ \exists (k_{i,1}, k_{i,2}, k_{i,3}, k_{i,4}) \in \chi_{[i]}, (i \in \mathcal{V}_{\mathscr{C}}) : \lim_{t\to+\infty} |V(t) - \bar{V}| < \delta_V,\ \lim_{t\to+\infty} \|\mathbf{I}(t) - \bar{I}\| < \delta_I, \quad (13)$$

where δ_V and δ_I are very small positive scalars, $\bar{V}$, and $\bar{I}$ are given in (9).

Proof. Consider the linear dynamics in (10). The closed-loop state vector $x_{cl}(t)$ can be obtained as follows:

$$x_{cl}(t) = e^{A_{cl}t} x_{cl}(0) + \int_0^t e^{A_{cl}(t-\tau)} B_{cl} \Delta \mathbf{u}(\tau) d\tau. \quad (14)$$

Therefore,

$$\lim_{t\to\infty} \|x_{cl}(t)\| \le \lim_{t\to\infty} \left\| e^{A_{cl}t} x_{cl}(0) \right\| + \left\| \int_0^t e^{A_{cl}(t-\tau)} B_{cl} \Delta \mathbf{u}(\tau) d\tau \right\|, \le \lim_{t\to\infty} \left\| \int_0^t e^{A_{cl}(t-\tau)} B_{cl} \Delta \mathbf{u}(\tau) d\tau \right\|, \quad (15)$$

Considering that A_{cl} is a Hurwitz matrix (see Lemma 2), $\lim_{t\to\infty} \left\| e^{A_{cl}t} x_{cl}(0) \right\| = 0$. Moreover, since $\Delta \mathbf{u}(t)$ is assumed to be uniformly bounded (see Assumption 1), there exists a constant vector $\delta_u \in \mathbb{R}^{N\times 1}$ and a positive constant $\tau^\star$ such that:

$$\left\| \int_0^t e^{A_{cl}(t-\tau)} B_{cl} \Delta \mathbf{u}(\tau) d\tau \right\| \le \left\| \int_0^t e^{A_{cl}(t-\tau)} B_{cl} \delta_u d\tau \right\|, \quad (16)$$

for all $t \ge \tau^\star$, by virtue of a trivial extension of [27, Lem.2]. Taking into account (16), one can obtain that

$$\lim_{t\to\infty} \|x_{cl}(t)\| \le \lim_{t\to\infty} \left\| \int_0^t e^{A_{cl}(t-\tau)} B_{cl} \delta_u d\tau \right\|, \le \left\| -A_{cl}^{-1} B_{cl} \delta_u \right\|, \quad (17)$$

Due to the structure of B_{cl} in (11), $B_{cl}\delta_u = \begin{bmatrix} 0 & ([L]^{-1}\delta_u)^T & \mathbf{0}_{1\times N} \end{bmatrix}^T$. By obtaining the inverse of A_{cl}^{-1} according to [28], it can be shown that $A_{cl}^{-1} B_{cl} \delta_u$ can be determined as follows:

$$A_{cl}^{-1} B_{cl} \delta_u = \begin{bmatrix} 0 \\ \mathbf{0}_{N\times 1} \\ [k_3]^{-1} \delta_u \end{bmatrix}. \quad (18)$$

Hence, for a large value of $k_{3,i}$, $\forall i \in \mathcal{V}_{\mathscr{C}}$, $x_{cl}(t)$ converges as close to zero as desired, at the steady-state. As a result, voltage regulation and balanced current sharing objectives stated in (3) and (4) are achieved with arbitrary accuracy regardless of the existence of bounded false data injection attacks on actuators. □

TABLE I
DESIGN CRITERIA OF COOPERATIVE DISTRIBUTED CONTROLLER PARAMETERS IN (5).

Control Parameter	*Design Criteria*
γ	$\gamma > 0$
$k_{i,1}$	$k_{i,1} < 1$
$k_{i,2}$	$k_{i,2} < r_i$
$k_{i,3}$	$0 < k_{i,3} < \frac{1}{L_i}(r_i - k_{i,2})(1 - k_{i,1})$ & sufficiently high
$k_{i,4}$	$k_{i,4} = \gamma(k_{i,1} - 1)$

B. Design Procedure of Proposed Resilient Cooperative Distributed Control Strategy

The design criteria for the proposed resilient cooperative distributed control strategy in (5) are summarized in Table I. According to this design guideline, the stability and resilience to FDI cyber-attacks in (2) are simultaneously ensured. As one can see from Table I, the design of control gain $K_i = \begin{bmatrix} k_{i,1} & k_{i,2} & k_{i,3} & k_{i,4} \end{bmatrix}$ for DC-DC converter i relies only on the local information of the converter and does not require the global knowledge about the number or parameters of other converters. Moreover, as discussed in Theorem 1, the value of $k_{i,3}$ plays an important role in the attack-resilience feature of the proposed distributed controller to FDI attacks on actuators. More specifically, the large value of $k_{i,3}$ enhances the resilience to FDI cyber-attacks on actuators.

C. An Extreme FDI Cyber-attack Scenario

Suppose that the magnitude of the false data injection attack vector $\Delta \mathbf{u}(t)$ in (10) is large. In view of (17) and (18), this might challenge the attack-resilience accuracy of the proposed distributed control strategy in (5), as δ_u in (17) will be large as well. Yet, the control inputs $u_i(t)$ are subject to a constraint $0 \le u_i(t) \le E_i$, so that such an attack can easily be detected by an anomaly detection algorithm [25]. As a result, the proposed FDI attack-resilient distributed control strategy can still be reliable in protecting against FDI attacks on actuators.

V. RESULTS

A. Simulation Case Studies

We consider the parallel connection of $N = 4$ DC-DC converters with different inductance values whose parameters are provided in Table II. In the simulation case studies carried out in MATLAB/Simscape environment, a switching model of DC-DC buck converters is used. The parameters of resilient distributed controller for each converter is designed based on the design criteria given in Table I.

Comparative Case Study 1: The first comparative case study evaluates the performance of the proposed resilient distributed control strategy in (5) with respect to robustness to load variations and resilience to FDI cyber-attacks on actuators modeled in (2). To this end, it is assumed that there is a load change at $t = 1.5$ *s* and the actuators of all four converters are subject to a mixture of constant and uniformly bounded time-varying FDI attacks launched at $t = 2$ *s*. The performance of the proposed resilient cooperative distributed control strategy in (5) is compared with the proposed resilient controller given

TABLE II
ELECTRICAL AND CONTROL PARAMETERS OF EXPERIMENTAL SETUP IN FIG. 5 AND SIMULATION CASE STUDIES.

Experimental Tests	
Electrical Parameters	*Value*
Voltage reference V^*	48 V
Input voltage of converters $E_i,\ i=1,2,3$	100 V
Switching frequency f_s	10 kHz
Inductance $L_i,\ i=1,2,3$	860 μH
Capacitance C	1100 μF
Control Parameters	*Value*
γ	0.25
$K_i=\begin{bmatrix} k_{i,1} & k_{i,2} & k_{i,3} & k_{i,4} \end{bmatrix},\ i=1,2,3$	$[-1\ -1\ 150\ -0.5]$
Simulation Case Studies	
Electrical Parameters	*Value*
Voltage reference V^*	48 V
Input voltage of converters $E_i,\ i=1,\ldots,4$	110 V
Switching frequency f_s	30 kHz
Inductance $[L_1\ L_2\ L_3\ L_4]$	$[1\ 1.5\ 2\ 1]$ mH
Capacitance C	1100 μF
Load resistance R	2 Ω
Control Parameters	*Value*
γ	10
$K_i=\begin{bmatrix} k_{i,1} & k_{i,2} & k_{i,3} & k_{i,4} \end{bmatrix},\ i=1,\ldots,4$	$[-2.5\ -10\ 500\ -35]$

in [24], which is based on a smooth adaptive distributed secondary control framework. The voltage and current trajectories of the converters are depicted in Fig. 3. As one can observe from this figure, both controllers are able to mitigate the adverse impact of FDI cyber-attacks on voltage regulation and current-sharing performance. However, the proposed resilient distributed control strategy in (5) provides better and more smooth transient responses and mitigates the cyber-attacks faster than the resilient distributed controller in [24].

Comparative Case Study 2: The second comparative case study tests the performance of the proposed resilient distributed control strategy in (5) and the conventional cooperative distributed secondary control in [29] in terms of voltage regulation and current sharing performance as well as robustness to load changes. Both controllers rely on the same communication network with a connected undirected communication graph belonging to (7). The load voltage is initially regulated at 48 V and the load current is equally shared amongst all four DC-DC converters. Then, the voltage reference V^* is stepped up to $V^*=60$ V at $t=2$ s. Furthermore, the common load is suddenly increased at $t=2.5$ s. The performance of both controllers is compared and the results are shown in Fig. 4. The results in Fig. 4 indicate that both controllers are able to track the reference voltage with a zero steady-state error (Fig. 4 (a), (c)); moreover, the load current is equally shared amongst participating converters (Fig. 4 (b),(d)). However, the proposed distributed control framework in (5) provides a faster and more smooth response compared to the conventional distributed control in [29] for voltage regulation and current sharing.

B. Experimental Results

Setup Description: The performance of the proposed resilient cooperative control strategy in (5) is evaluated for a case study of $N=3$ parallel DC-DC buck converters. The parallel converter system with the proposed resilient cooperative mechanism with the communication graph in (8) is implemented by an experimental setup, as illustrated in Fig. 5. The electrical and control parameters of the system under study are given in Table II. The proposed resilient controller is implemented in MATLAB/Simulink and run on a dSpace MicroLabBox embedded controller. To illustrate the performance of the proposed resilient control framework in (5) in terms of robust stability, resilience to FDI attacks, and voltage reference tracking, several case studies are presented.

Voltage Regulation: In order to assess the performance of the proposed control approach in terms of voltage reference tracking, it is assumed that the reference voltage V^* of the common load is initially set at 48 V. Then, it is respectively stepped down and up to 24 V and 72 V at different time instances. The voltage reference, voltage of the common load, current, and the duty cycle of the converters are shown in Fig. 6. As one can observe from this figure, the controllers provide an offset-free voltage tracking performance (Fig. 6 (a)); moreover, the load current is equally distributed amongst participating converters (Fig. 6 (b)).

Robustness to Load Uncertainty: This case study illustrates the robustness and load-independent feature of the proposed control strategy in (5) with respect to load variation and uncertainty in parasitic resistance of inductors. To this end, it is assumed that all DC-DC converters initially share a common load $R_0=2.13$ Ω and the load voltage is regulated at 48 V. Then, the load resistance value is increased and decreased at several time instances, as shown in Fig. 7 (b). The dynamic responses of DC-DC converters are depicted in Fig. 7. As illustrated in Section III, the balanced current sharing and voltage regulation are achieved regardless of the load condition.

Resilience to False Data Injection Attacks to Actuators: The final test evaluates the resilience of the proposed cooperative distributed control mechanism in (5) against false data injection attacks to control input channels. For this purpose, it is assumed that all DC-DC converters are subject to constant and time-varying FDI attacks $\Delta u_1(t)=10$, $\Delta u_2(t)=20\times|\sin(\frac{2\pi}{5}(t-2))|$, launched at $t=2$ s, and $\Delta u_3(t)=20\times|\sin(\frac{2\pi}{5}(t-3))|$, launched at $t=3$ s. In order to assess the resilience of the proposed controller to other types of cyber-attacks in (2), the constant false data $\Delta u_1(t)=10$, $\Delta u_2(t)=20$, and $\Delta u_3(t)=15$ are simultaneously injected to the actuators of DC-DC converters at $t=7$ s. Hence, attackers manipulate the control commands by adding incorrect signals of a maximum $\approx 42\%$ of the nominal steady-state control commands. The voltage and current trajectories as well as the control input signals are depicted in Fig. 8 (a)-(c).

In order to highlight the superiority of the proposed resilient cooperative control in (5) in terms of resilience to cyber-attacks on actuators to non-resilient cooperative control approaches, this case study is repeated where the proposed control approach method in [15] is employed. The proposed

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIE.2021.3123613, IEEE Transactions on Industrial Electronics

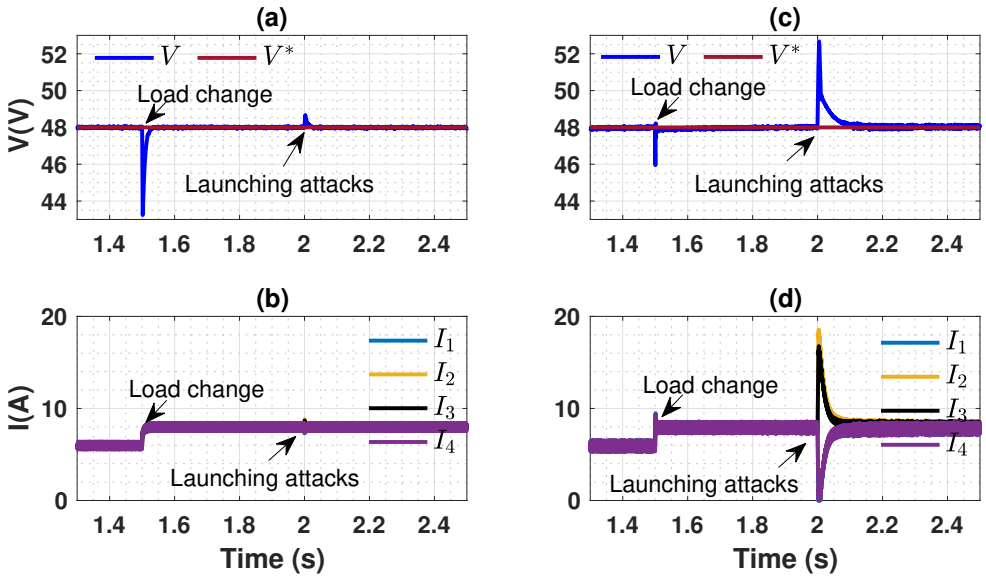

Fig. 3. Simulation results: Performance of the proposed resilient cooperative distributed controller in (5) and the resilient distributed control approach in [24] to a load change at $t = 1.5\ s$ and FDI attacks $\Delta\mathbf{u}(t)$ launched at $t = 2$ s: (a),(b) voltage and current trajectories via (5) and (c),(d) voltage and current trajectories via the resilient distributed control technique in [24].

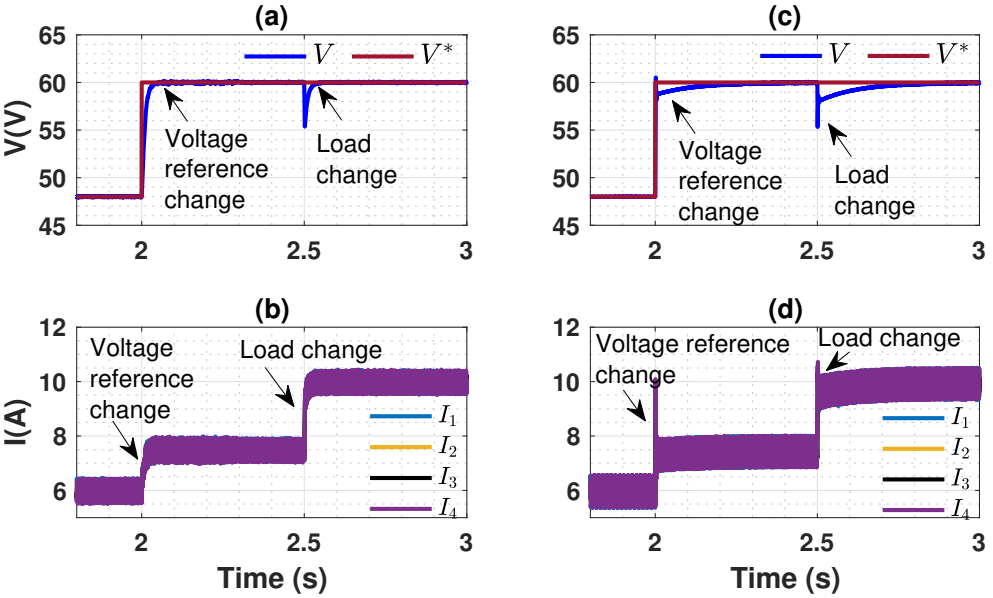

Fig. 4. Simulation results: Performance of the proposed resilient cooperative distributed controller in (5) and the conventional cooperative distributed secondary control approach in [29] to voltage reference change at $t = 2\ s$ and a load change at $t = 2.5\ s$: (a),(b) voltage and current trajectories via (5) and (c),(d) voltage and current trajectories via the conventional distributed control technique in [29].

distributed controller in [15] for converter i is as follows:

$$\begin{aligned} T_{\theta_i}\dot{\theta}_i(t) &= -\sum_{j=1}^{N}\alpha_{ij}(I_i(t)-I_j(t)),\\ T_{\phi_i}\dot{\phi}_i(t) &= -\phi_i(t)+I_i(t),\\ u_i(t) &= -K_i(I_i(t)-\phi_i(t))+\sum_{j=1}^{N}\alpha_{ij}(\theta_i(t)-\theta_j(t))+V^*, \end{aligned} \tag{19}$$

where $\alpha_{ij}=\alpha_{ji}\geq 0$, $K_i>0$, $T_{\theta_i}>0$, and $T_{\phi_i}>0$. The results are shown in Fig. 8 (d)-(f). It should be noted that the comparison results in Fig. 8 (d)-(f) are based on MATLAB simulations.

As one can observe from Fig. 8, the proposed cooperative averaging control method in [15] is fragile to FDI cyber-attacks. As a result, any perturbation $\Delta u_i(t)$ in (2) in control input signals (actuators) leads to the failure in the voltage regulation and balanced current sharing. In contrast, as discussed in Section IV, upon lunching the cyber-attacks, the proposed cooperative control mechanism in (5) mitigates the negative effects of attacks on voltage regulation and balanced current sharing. Note that the voltage fluctuations in Fig. 8 (a) are less than $\pm 0.5\%$ of the voltage reference V^*.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIE.2021.3123613, IEEE Transactions on Industrial Electronics

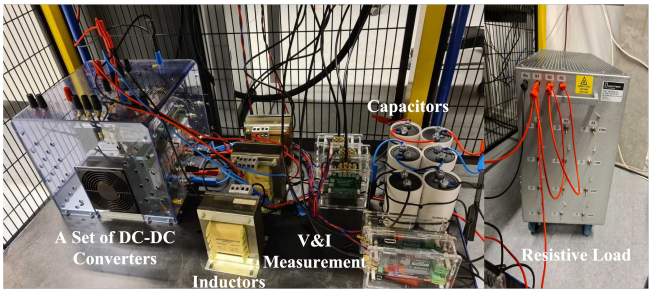

Fig. 5. Experimental setup of parallel converters comprising of three DC-DC buck converters.

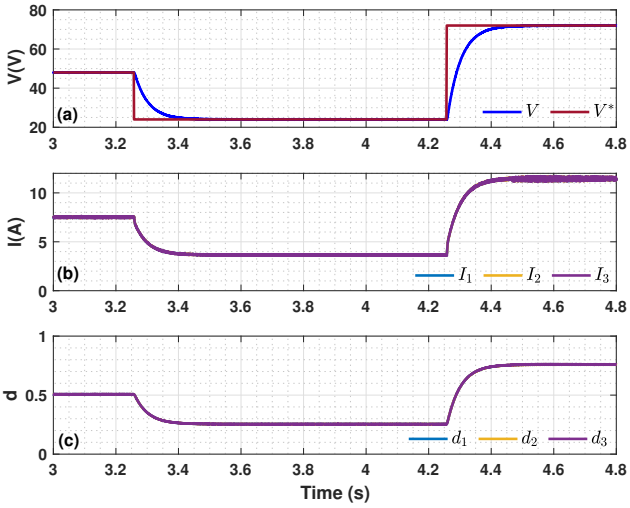

Fig. 6. Experimental results: Dynamic responses of the parallel converters in Fig. 5 to voltage reference changes: (a) common load voltage, (b) current of DC-DC converters, and (c) converters' duty cycle.

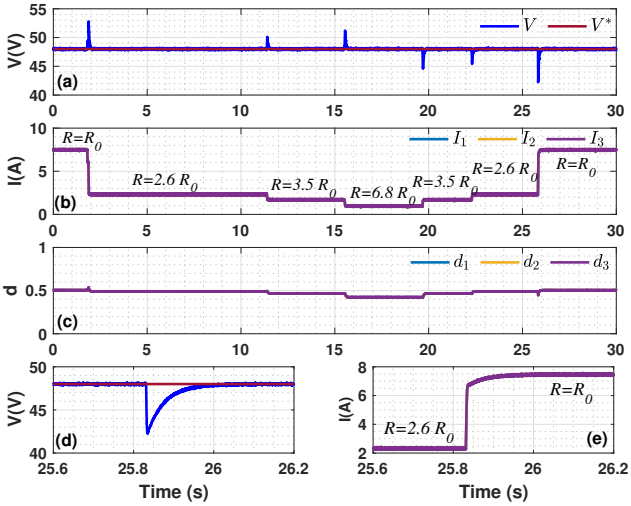

Fig. 7. Experimental results: Dynamic responses of the parallel converters to multiple load changes: (a) common load voltage, (b) current of DC-DC converters, (c) converters' duty cycle, (d) load voltage (zoomed version) for a large load change from $R = 2.6R_0$ to R_0, and (e) converters' current signals (zoomed version) for a large load change from $R = 2.6R_0$ to R_0 - The x-axis in all subplots is time (s).

VI. Conclusion

Voltage regulation and balanced current sharing in the parallel connection of DC-DC converters in the presence of false data injection cyber-attacks are challenging. In this paper, we propose a resilient cooperative distributed control strategy that simultaneously regulates load voltage and distributes load current amongst active converters. The proposed cooperative distributed controller guarantees resilience against false data injection cyber-attacks in actuators and robustness with respect to uncertainties in the physical parameters of DC-DC converters as well as loads. The paper describes theoretical aspects involved in the control design, stability analysis, as well as resilience to FDI cyber-attacks and evaluates the performance of the proposed control mechanism based on comparative simulation case studies and experimental results. The future work will consider (i) the resilience to FDI attacks on communication links in cooperative and distributed control systems, (ii) the analysis of communication failures and delays in the proposed distributed control approach, and (iii) the extension of stability and attack-resilience analysis to state-dependent FDI cyber-attacks.

VII. Appendixes

Appendix A: Proof of Lemma 1

Consider the closed-loop system in (6). In the steady state, we have

$$0 = \mathbf{1}_N^T \bar{I} - \bar{I}_L, \tag{20a}$$

$$\mathbf{0}_N = -\mathbf{1}_N \bar{V} + \mathbf{1}_N V^* - \gamma \mathbb{L}_{\mathscr{G}} \bar{I}, \tag{20b}$$

$$\mathbf{0}_N = ([k_1] - \mathbf{I}_N)\mathbf{1}_N \bar{V} + ([k_2] - [r])\bar{I} + [k_3]\,\bar{v} + [k_4]\,\mathbb{L}_{\mathscr{G}} \bar{I}, \tag{20c}$$

where $\bar{I}_L = \frac{\bar{V}}{R} + I_L^*$. By multiplying both sides of (20b) by $\frac{1}{N}\mathbf{1}_N^T$, one obtains that

$$\frac{1}{N}\mathbf{1}_N^T \mathbf{1}_N (-\bar{V} + V^*) - \frac{\gamma}{N}\mathbf{1}_N^T \mathbb{L}_{\mathscr{G}} \bar{I} = 0. \tag{21}$$

Since $\mathbf{1}_N^T \mathbb{L}_{\mathscr{G}} = \mathbf{0}_N^T$ [26], from the above equation one obtains that $\bar{V} = V^*$. Replacing $\bar{V}$ with V^* in (20b) results into the following equation:

$$-\mathbf{1}_N V^* + \mathbf{1}_N V^* - \gamma \mathbb{L}_{\mathscr{G}} \bar{I} = \mathbf{0}_N. \tag{22}$$

Hence, $\mathbb{L}_{\mathscr{G}} \bar{I} = \mathbf{0}_N$ (note that $\gamma \neq 0$). Since $\mathbf{1}_N$ is an eigenvector of the Laplacian associated with a zero eigenvalue [26], $\mathbb{L}_{\mathscr{G}} \bar{I} = \mathbf{0}_N$ implies that $\bar{I} = \mathbf{1}_N i^*$, where $i^* = \frac{1}{N}\bar{I}_L$ and $\bar{I}_L = \frac{V^*}{R} + I_L^*$. From (20c), $\bar{v}$ is obtained as follows:

$$\bar{v} = [k_3]^{-1} \left((\mathbf{I}_N - [k_1])\mathbf{1}_N V^* + ([r] - [k_2])\bar{I} \right). \tag{23}$$

This completes the proof.

Appendix B: Proof of Lemma 2

Let $\Delta \mathbf{u}(t) = \mathbf{0}_N$ in (10). It suffices to show that the origin in (10) is globally asymptotically stable. To this end, we first pick any $(k_{i,1}, k_{i,2}, k_{i,3}, k_{i,4})$ in $\chi_{[i]}$ and then compute following scalars:

$$\rho_{i,1} = \frac{1}{(1 - k_{i,1} - L_i \rho_{i,2})} > 0, \;\; \rho_{i,2} = \frac{k_{i,3}}{(r_i - k_{i,2})} > 0. \tag{24}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIE.2021.3123613, IEEE Transactions on Industrial Electronics

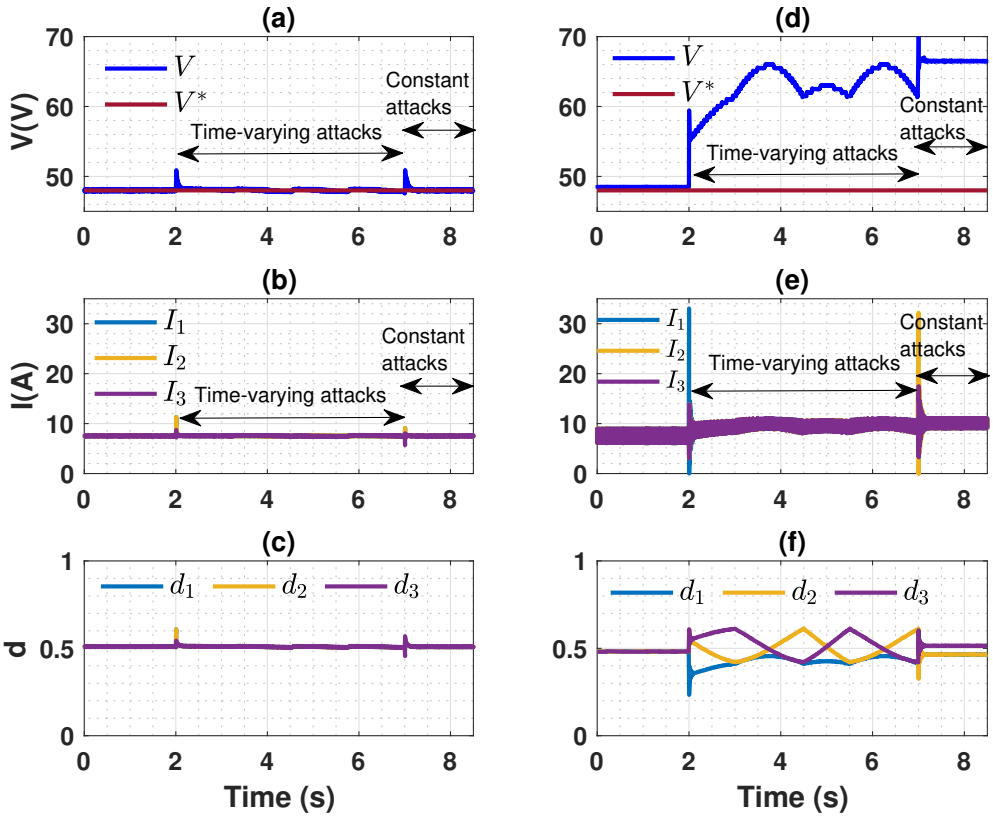

Fig. 8. Performance of the proposed resilient cooperative controller in (5) and the cooperative averaging control method in [15] to (i) time-varying FDI attacks $\Delta\mathbf{u}(t)$ launched at $t=2$ s and $t=3$ s and (ii) constant FDI attacks $\Delta\mathbf{u}(t)$ launched at $t=7$ s: (a)-(c) voltage, current, and duty cycle trajectories via (5) and (d)-(f) voltage, current, and duty cycle trajectories via the non-resilient cooperative control technique in [15].

We then consider the following separable quadratic-type Lyapunov function $\mathscr{V}$ for the parallel interconnection of N converters augmented with the resilient cooperative controllers in (5):

$$\mathscr{V}=\frac{1}{2}\sum_{i=1}^{N}\begin{bmatrix} e_1(t) & e_{2_i}(t) & e_{3_i}(t)\end{bmatrix}\text{diag}(C,\rho_i)\begin{bmatrix} e_1(t)\\ e_{2_i}(t)\\ e_{3_i}(t)\end{bmatrix}, \tag{25}$$

where $e_1=V-\bar{V}$, $e_2=\mathbf{I}-\bar{I}$, $e_3=\mathbf{v}-\bar{v}$, and $\rho_i\succ 0$ is structured as follows:

$$\rho_i=\begin{bmatrix} L_i\rho_{i,1} & -L_i\rho_{i,2}\rho_{i,1}\\ -L_i\rho_{i,2}\rho_{i,1} & \rho_{i,2}(L_i\rho_{i,1}\rho_{i,2}+1)\end{bmatrix}. \tag{26}$$

From this definition, it comes out that $\mathscr{V}\geq 0$. The time derivative of $\mathscr{V}$ along the closed-loop trajectories of (6) are obtained as:

$$\begin{aligned}\dot{\mathscr{V}}&=-\frac{1}{R}e_1^2(t)+\frac{1}{2}\sum_{i=1}^{N}x_{cl_i}^T(t)Q_ix_{cl_i}(t)\\&+\frac{1}{2}\sum_{i=1}^{N}\left(\begin{bmatrix} e_{2_i}\\ e_{3_i}\end{bmatrix}^T\rho_i\begin{bmatrix}\frac{-1+k_{i,1}}{L_i}\\ -1\end{bmatrix}e_{4_i}+e_{4_i}\begin{bmatrix}\frac{-1+k_{i,1}}{L_i}\\ -1\end{bmatrix}^T\rho_i\begin{bmatrix} e_{2_i}\\ e_{3_i}\end{bmatrix}\right),\end{aligned} \tag{27}$$

where $x_{cl_i}(t)$ is defined as $x_{cl_i}(t)=\begin{bmatrix} e_1(t) & e_{2_i}(t) & e_{3_i}(t)\end{bmatrix}^T$, $e_{4_i}(t)=\gamma\sum_{j=1}^{N}\alpha_{i,j}\left(e_{2_i}(t)-e_{2_j}(t)\right)$, and

$$\begin{aligned}Q_i=&\text{diag}(1,\rho_i)\begin{bmatrix}0 & 1 & 0\\ \frac{-1+k_{i,1}}{L_i} & \frac{-r_i+k_{i,2}}{L_i} & \frac{k_{i,3}}{L_i}\\ -1 & 0 & 0\end{bmatrix}\\&+\begin{bmatrix}0 & 1 & 0\\ \frac{-1+k_{i,1}}{L_i} & \frac{-r_i+k_{i,2}}{L_i} & \frac{k_{i,3}}{L_i}\\ -1 & 0 & 0\end{bmatrix}^T\text{diag}(1,\rho_i).\end{aligned} \tag{28}$$

From (24), one obtains that $1-k_{i,1}=\rho_{i,1}^{-1}+L_i\rho_{i,2}$. Hence, we have

$$\begin{aligned}&\begin{bmatrix} e_{2_i}\\ e_{3_i}\end{bmatrix}^T\rho_i\begin{bmatrix}\frac{-1+k_{i,1}}{L_i}\\ -1\end{bmatrix}e_{4_i}=e_{2_i}\left(\rho_{i,1}(-1+k_{i,1})+L_i\rho_{i,2}\rho_{i,1}\right)e_{4_i}\\&+e_{3_i}\left(-\rho_{i,1}\rho_{i,2}(-1+k_{i,1})-\rho_{i,2}(L_i\rho_{i,1}\rho_{i,2}+1)\right)e_{4_i}\\&=-e_{2_i}e_{4_i}.\end{aligned}$$

Therefore, $\dot{\mathscr{V}}(e_1(t),e_2(t),e_3(t))$ can be rewritten as follows:

$$\begin{aligned}\dot{\mathscr{V}}&=-\frac{1}{R}e_1^2(t)+\frac{1}{2}\sum_{i=1}^{N}x_{cl_i}^T(t)Q_ix_{cl_i}(t)-\frac{1}{2}e_4^T(t)e_2(t)-\frac{1}{2}e_2^T(t)e_4(t),\\&=-\frac{1}{R}e_1^2(t)+\frac{1}{2}\sum_{i=1}^{N}x_{cl_i}^T(t)Q_ix_{cl_i}(t)-\frac{\gamma}{2}e_2^T(t)\left(\mathbb{L}_{\mathscr{C}}+\mathbb{L}_{\mathscr{C}}^T\right)e_2(t),\\&=-\frac{1}{R}e_1^2(t)+\frac{1}{2}\sum_{i=1}^{N}x_{cl_i}^T(t)Q_ix_{cl_i}(t)-\gamma e_2^T(t)\mathbb{L}_{\mathscr{C}}e_2(t).\end{aligned} \tag{29}$$

It is obvious that the negative semi-definiteness of Q_i is equivalent to the negative semi-definiteness of matrix $\tilde{Q}_i = \text{diag}(1,\rho_i^{-1})Q_i\,\text{diag}(1,\rho_i^{-1})$. From the structure of ρ_i in (26), one gets:

$$\tilde{Q}_i = \begin{bmatrix} 0 & \underbrace{(L_i^{-1}\rho_{i,1}^{-1}+\rho_{i,2}-L_i^{-1}(1-k_{i,1}))}_{\tilde{q}_{i,12}} & 0 \\ \tilde{q}_{i,12} & \frac{2}{L_i}((-r_i+k_{i,2})(L_i^{-1}\rho_{i,1}^{-1}+\rho_{i,2})+k_{i,3}) & \tilde{q}_{i,32} \\ 0 & \underbrace{\frac{1}{L_i}(-r_i+k_{i,2}+k_{i,3}\rho_{i,2}^{-1})}_{\tilde{q}_{i,32}} & 0 \end{bmatrix}.$$

Then, considering (24), one obtains that

$$\tilde{Q}_i = \begin{bmatrix} 0 & 0 & 0 \\ 0 & \frac{2}{L_i}(-L_i^{-1}(-r_i+k_{i,2})(1-k_{i,1})+k_{i,3}) & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

From (12), it comes out that $\tilde{Q}_i \preceq 0$ and, in turn, $Q_i \preceq 0$ hold. Together with $\gamma > 0$, and $\mathbb{L}_{\mathscr{C}} \succeq 0$, this proves that $\dot{\mathscr{V}} \leq 0$ holds for all $(e_1(t), e_2(t), e_3(t))$, meaning that all the state trajectories in (10) are bounded. We use the LaSalle's invariance principle to show that origin of $\dot{x}_{cl}(t) = A_{cl}x_{cl}(t)$ is globally asymptotically stable. Observe that $\dot{\mathscr{V}}(e_1^\star, e_2^\star, e_3^\star) = 0$ is equivalent to

$$e_1^\star = 0, \tag{30}$$

$$e_2^\star \in \ker(\mathbb{L}_{\mathscr{C}}) \Leftrightarrow e_2^\star \in \text{span}(\mathbf{1}_N), \tag{31}$$

$$x_i^\star = \begin{bmatrix} e_1^\star & e_{2_i}^\star & e_{3_i}^\star \end{bmatrix}^T \in \ker(Q_i) \Leftrightarrow e_{2_i}^\star - \rho_{i,2}e_{3_i}^\star = 0. \tag{32}$$

Trajectories of system (10) converge to the largest invariant subset $\mathscr{I}$ of the set defined by the above equations. From (10), $\mathbf{1}_N^T e_2^\star - \frac{1}{R}e_1^\star = 0$ must hold for all $(e_1^\star, e_2^\star, e_3^\star) \in \mathscr{I}$. From (30), (31), and (32), this implies that $e_2^\star = \mathbf{0}_N$ and, in turn, $e_3^\star = \mathbf{0}_N$ holds in $\mathscr{I}$. Therefore, $\mathscr{I}$ reduces to the origin, so that origin of $\dot{x}_{cl}(t) = A_{cl}x_{cl}(t)$ is globally asymptotically stable and A_{cl} is Hurwitz. As a result, the closed-loop system in (6) is input-to-state stable (ISS) [30]. This implies that for any bounded $\Delta\mathbf{u}(t)$, the states of the closed-loop system are bounded too.

REFERENCES

[1] V. J. Thottuvelil and G. C. Verghese, "Analysis and control design of paralleled DC/DC converters with current sharing," *IEEE Trans. on Power Electronics*, vol. 13, no. 4, pp. 635–644, July 1998.

[2] Y. Huang and C. K. Tse, "Circuit theoretic classification of parallel connected DC–DC converters," *IEEE Trans. on Circuits and Systems-I*, vol. 54, no. 5, pp. 1099–1108, May 2007.

[3] H. Mao, L. Yao, C. Wang, and I. Batarseh, "Analysis of inductor current sharing in nonisolated and isolated multiphase dc–dc converters," *IEEE Trans. on Industrial Electronics*, vol. 54, no. 6, pp. 3379–3388, Dec. 2007.

[4] H. Behjati, A. Davoudi, and F. Lewis, "Modular DC–DC converters on graphs: Cooperative control," *IEEE Trans. on Power Electronics*, vol. 29, no. 12, pp. 6725–6741, Dec. 2014.

[5] J. W. Kim, H. S. Choi, and B. H. Cho, "A novel droop method for converter parallel operation," *IEEE Trans. on Power Electronics*, vol. 17, no. 1, pp. 25–32, Jan. 2002.

[6] S. Anand and B. G. Fernandes, "Modified droop controller for paralleling of DC–DC converters in standalone DC system," *IET Power Electronics*, vol. 5, no. 6, pp. 782–789, July 2012.

[7] J. B. Wang, "Parallel DC/DC converters system with a novel primary droop current sharing control," *IET Power Electronics*, vol. 5, no. 8, pp. 1569–1580, Sept. 2012.

[8] G. Xu, D. Sha, and X. Liao, "Decentralized inverse-droop control for input-series–output-parallel DC–DC converters," *IEEE Trans. on Power Electronics*, vol. 30, no. 9, pp. 4621–4625, Sept. 2015.

[9] S. Mazumder, A. Nayfeh, and A. Borojevic, "Robust control of parallel DC-DC buck converters by combining integral-variable-structure and multiple-sliding-surface control schemes," *IEEE Transactions on Power Electronics*, vol. 17, no. 3, May 2002.

[10] S. K. Mazumder, M. Tahir, and K. Acharya, "Master–slave current-sharing control of a parallel DC–DC converter system over an RF communication interface," *IEEE Trans. on Industrial Electronics*, vol. 55, no. 1, pp. 59–66, Jan. 2008.

[11] H. Du, C. Jiang, G. Wen, W. Zhu, and Y. Cheng, "Current sharing control for parallel DC–DC buck converters based on finite-time control technique," *IEEE Trans. on Industrial Informatics*, vol. 15, no. 4, pp. 2186–2198, Apr. 2019.

[12] J. F. Tregouet and R. Delpoux, "New framework for parallel interconnection of buck converters: Application to optimal current-sharing with constraints and unknown load," *Control Engineering Practice*, vol. 87, pp. 59–75, 2019.

[13] J. Kreiss, J. F. Tregouet, D. Eberard, R. Delpoux, J. Y. Gauthier, and X. Lin-Shi, "Hamiltonian point of view on parallel interconnection of buck converters," *IEEE Trans. on Control Systems Technology*, pp. 1–10, Jan. 2020.

[14] S. Moayedi, V. Nasirian, F. Lewis, and A. Davoudi, "Team-oriented load sharing in parallel DC–DC converters," *IEEE Trans. on Industry Applications*, vol. 51, no. 1, pp. 479–490, Jan./Feb. 2015.

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

[16] M. S. Sadabadi, "A distributed control strategy for parallel DC-DC converters," *IEEE Control Systems Letters*, vol. 5, no. 4, pp. 1231–1236, Oct. 2021.

[17] B. Zhu, A. Joseph, and S. Sastry, "A taxonomy of cyber attacks on SCADA systems," in *2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing*, Dalian, China, Oct. 2011, pp. 380–388.

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

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

[20] S. Sahoo, J. C. Peng, A. Devakumar, S. Mishra, and T. Dragičević, "On detection of false data in cooperative DC microgrids—A discordant element approach," *IEEE Trans. on Industrial Electronics*, vol. 67, no. 8, pp. 6562–6571, Aug. 2020.

[21] A. Kavousi-Fard, W. Su, and T. Jin, "A machine-learning-based cyber attack detection model for wireless sensor networks in microgrids," *IEEE Trans. on Industrial Informatics*, vol. 17, no. 1, pp. 650–658, Jan. 2021.

[22] M. R. Habibi, H. R. Baghaee, T. Dragičević, and F. Blaabjerg, "False data injection cyber-attacks mitigation in parallel DC/DC converters based on artificial neural networks," *IEEE Trans. on Circuits and Systems II: Express Briefs*, vol. 68, no. 2, pp. 717–721, Feb. 2021.

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

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

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

[26] R. Olfati-Saber and R. M. Murray, "Consensus problems in networks of agents with switching topology and time-delays," *IEEE Trans. on Automatic Control*, vol. 49, no. 9, pp. 1520–1533, Sept. 2004.

[27] H. Dong, C. Li, and Y. Zhang, "Resilient consensus of multi-agent systems against malicious data injections," *Journal of the Franklin Institute*, vol. 357, p. 2217–2231, 2020.

[28] R. A. Horn and C. R. Johnson, *Matrix Analysis*. New York, NY, USA: Cambridge University Press, Second Edition, 2013.

[29] V. Nasirian, S. Moayedi, A. Davoudi, and F. L. Lewis, "Distributed cooperative control of DC microrgids," *IEEE Trans. on Power Electronics*, vol. 30, no. 4, pp. 2288–2303, Apr. 2015.

[30] H. K. Khalil, *Nonlinear Systems*. New Jersey: Prentice Hall, 2006.

Mahdieh S. Sadabadi is currently an Assistant Professor with the Department of Automatic Control and Systems Engineering, University of Sheffield, United Kingdom. Prior to that, she was a Research Associate at the Department of Engineering, the University of Cambridge, and affiliated with Trinity College in Cambridge. She was a Postdoctoral Fellow in the Division of Automatic Control at the Department of Electrical Engineering, Linkoping University in Sweden. She received her Ph.D. in Control Systems from Automatic Control Laboratory (LA), Swiss Federal Institute of Technology in Lausanne (EPFL), Switzerland in February 2016. She was a Visiting Scholar at the Electrical Engineering Department, Ecole Polytechnique de Montreal, QC, Canada, Methods and Algorithms for Control (MAC) group, LAAS-CNRS in Toulouse, France, and HHMI Janelia Research Campus in Ashburn, VA, USA. Her research interests are generally centered on robust fixed-structure control of large-scale uncertain systems and resilient control systems with applications in power grids, microgrids, and power electronics converters.

Nenad Mijatovic after obtaining his Dipl.Ing. education in Electrical Power Engineering at University of Belgrade, Serbia in 2007, was enrolled as a doctoral candidate at Technical University of Denmark. He received his Ph.D. degree from Technical University of Denmark for his work on technical feasibility of novel machines and drives for wind industry. Upon completion of his PhD, he continued work within the field of wind turbine direct-drive concepts as an Industrial PostDoc.

Dr. N. Mijatovic currently holds position of Associate Professor at Technical University of Denmark where he is in charge of managing research projects and education related to the field of electrical machines and drives, power electronic convertors, motion control, application of energy storage and general applications of low frequency electromagnetism and large scale application of superconductivity with main focus on emerging eMobility and renewable energy generation.

He is a member of IEEE since 2008 and senior member of IEEE since 2018 and his field of interest and research includes novel electrical machine drives/actuator designs, operation, control and diagnostic of electromagnetic assemblies, advance control of drives and grid connected power electronics, energy storage and eMobility.

Jean-François Trégouët received the Ph.D. degree from Supaéro, Toulouse, France, in 2012, after performing his research at LAAS-CNRS, Toulouse. He spent several months in various research institutions such as the Politecnico di Milano, Milan, Italy, Kyoto University, Kyoto, Japan, Curtin University, Bentley, WA, Australia. He is currently an Assistant Professor with the Institut National des Sciences Appliquées de Lyon (INSA-Lyon), Villeurbanne, France. His main research interests include control design for over-actuated systems, with applications in power electronics.

Tomislav Dragičević (S'09-M'13-SM'17) received the M.Sc. and the industrial Ph.D. degrees in Electrical Engineering from the Faculty of Electrical Engineering, University of Zagreb, Croatia, in 2009 and 2013, respectively. From 2013 until 2016 he has been a Postdoctoral researcher at Aalborg University, Denmark. From 2016 until 2020 he was an Associate Professor at Aalborg University, Denmark. Currently, he is a Professor at the Technical University of Denmark. He made a guest professor stay at Nottingham University, UK during spring/summer of 2018. His research interest is application of advanced control, optimization and artificial intelligence inspired techniques to provide innovative and effective solutions to emerging challenges in design, control and diagnostics of power electronics intensive electrical distributions systems and microgrids. He has authored and co-authored more than 330 technical publications (more than 150 of them are published in international journals, mostly in IEEE), 10 book chapters and a book in this field, as well as filed for several patents.

He serves as an Associate Editor in the IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, in IEEE TRANSACTIONS ON POWER ELECTRONICS, in IEEE Emerging and Selected Topics in Power Electronics and in IEEE Industrial Electronics Magazine. Prof. Dragičević is a recipient of the Končar prize for the best industrial PhD thesis in Croatia, a Robert Mayer Energy Conservation award, and he is a winner of an Alexander von Humboldt fellowship for experienced researchers.