Detection and Mitigation of False Data in Cooperative DC Microgrids with Unknown Constant Power Loads

Andreu Cecilia, Subham Sahoo, *Member, IEEE*, Tomislav Dragičević, *Senior Member, IEEE*, Ramon Costa-Castelló, *Senior Member, IEEE* and Frede Blaabjerg, *Fellow, IEEE*

***Abstract*—The rapid development and implementation of distributed control algorithms for DC microgrids has increased the vulnerability of this type of system to false data injection attacks, being one of the most prominent types of cyber attacks. This fact has motivated the development of different false data detection and impact mitigation strategies. A common approach for the detection is based on implementing an observer that can achieve a reliable estimation of the system states. However, approaches available in the literature assume that the underlying microgrid model is linear, which is generally not the case, specially when the DC microgrid supplies non-linear constant power loads (CPLs). Consequently, this work proposes a distributed non-linear observer approach that can robustly detect and reconstruct the applied false data attack in the DC microgrid's current sensors and cyber-links, even in the presence of local unknown CPLs. First, the system is transformed into an observable form. Second, a high-order sliding-mode observer is implemented to estimate the system states and CPL, even in the presence of false data. Finally, the estimation is used to reconstruct the attack signal. The robustness of the proposed strategy is validated through numerical simulations and in an experimental prototype under measurement noise, uncertainty and communication delays.**

***Index Terms*—Cyber-attacks, DC microgrid, non-linear observer, cyber-physical systems, resilient controller.**

I. Introduction

As power grids are experiencing higher and higher penetration of renewable energy sources, it is required to develop new power system architectures and control strategies [1]. A great example is the recent proliferation of DC microgrids. Indeed, many distributed generation units (DGUs), such as fuel cells [2], photovoltaic panels and batteries [3], can be directly integrated in a DC microgrid through DC/DC converters, which, usually make DC microgrids more efficient and simple than its AC counterparts [4].

A key aspect for the DC microgrid operation is to ensure equal current sharing between the system agents as well as stable and precise DC voltage control [4]-[5]. Centralized approaches to achieve such DGU coordination have scalability issues, that renders such strategies infeasible for large scale microgrids. As a consequence, the general interest has drifted to the distributed framework, which relaxes the scalability issues and offers additional advantages such as resiliency against single point of failure and high bandwidth [6]. A popular approach to obtain such coordination is to implement a hierarchical control scheme in which a primary controller in the converter ensures the local stability of the DGU, while secondary controllers, implemented in the distributed cyber-layer, achieve equal current sharing and average voltage restoration [7]. In this context, the microgrid coordination requires the introduction of a communication network, that allows to transfer information between DGUs.

The integration between cyber-layer and physical-layer through a communication network increases the control precision, efficiency and reliability of the DC microgrid. Nonetheless, it also introduces a risk of malicious or unintentional cyber-attacks, which can compromise the proper operation of microgrid parts or of the whole microgrid. For this reason, it is of prime interest to develop techniques to detect and mitigate adversarial attacks from a control viewpoint [8].

Cyber-attacks can be classified in several categories: False data injection attacks (FDIAs) [9], denial of service [10] and replay attacks [11]. This work will focus on the first one, as it is the most frequent cyber-attack type [12]. This type of attack is based on injecting malicious measurements in compromised sensors/cyber-links in order to tamper the closed-loop performance of the system.

The most common approach in the detection of FDIAs in power systems is based on deploying an estimator and a detector in each agent of the system. The estimator achieves a secure estimation, i.e. the accuracy is independent of the attack signal value, of the agent's states based on a real-time model of the microgrid; and, in parallel, the detector compares the estimation with the actual readings and computes the presence of an attack. Liu and others [13] deployed a weighted least squares algorithm as an estimator of the power system state variables and implemented a sparse optimization as a detector, which computes the presence of an attack under the assumption that only a few sensors have been compromised. Chaojun and others [14] implemented a similar method, but using a Kullback–Leibler distance in the detector. Manandhar and others [15] implemented an estimator through a Kalman

This work has been partially funded by the Spanish State Research Agency through the María de Maeztu Seal of Excellence to IRI (MDM-2016-0656) and by the project DOVELAR (ref. RTI2018-096001-B-C32).

A. Cecilia and R. Costa-Castelló are with the Institut de Robòtica i Informàtica Industrial, CSIC-UPC Llorens i Artigas 4-6, 08028 Barcelona, Spain (e-mail: andreu.cecilia@upc.edu and ramon.costa@upc.edu). (*Corresponding author: Andreu Cecilia*)

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

T. Dragičević is with the Center of Electric Power and Energy,Technical University of Denmark, 2800 Kgs. Lyngby, Denmark (e-mail: tomdr@elektro.dtu.dk).

filter and a Euclidean distance metric as the detector. Zhao and others [16] used a short-term state forecasting as the estimator. Nevertheless, the mentioned results were implemented in a centralized framework. As a consequence, they are not scalable, require continuous communication from the DGUs to the centralized computer and can not easily incorporate new DGUs without modifying the whole estimation scheme. For this reason, the research interest in observer-based attack detection strategies has drifted to the distributed estimation framework. Li and others [17] proposed a distributed detector based on the generalized likelihood ratio. Nishino and Ishii [18] relaxed the centralized limitation by implementing a distributed observer as the estimator. Nonetheless, the design and implementation of the observer in each DGU requires the knowledge of the full DC microgrid, which complicates the incorporation of new DGUs in the system. A distributed estimation strategy was achieved by combining a bank of unknown input observers with a bank of linear Luenberger observers [19].

Once an attack has been detected, the immediate objective is to mitigate its effect on the microgrid. Relative to the topic, an event-driven strategy has been recently employed to mitigate FDIA and generalized FDIA [20], man-in-the-middle attacks [21] for homogeneous agents and for heterogeneous agents in [22].

It should be remarked that, although the fault detection problem and the cyber-attack detection problem present some differences [23], the FDIA detection strategy can be inspired from the fault detection and isolation literature, in which distributed approaches have been recently proposed [24]–[26].

A major limitation of available estimator-based detection methods is the assumption that the underlying model is linear, which, in some situations, may not be satisfied. The load side converter is often controlled to deliver constant power to the load. In such situations, the voltage dynamics behave non-linearly [27]. In those cases, small variations of the voltage may induce large variations of the stationary operating point which renders linear approximations infeasible. Moreover, a common scenario is that the constant power load (CPL) is unknown, which complicates the dynamics linearization that is required in some non-linear observers such as the extended Kalman filter.

The aim of this work is to fill this gap and propose a distributed non-linear observer that can be used to reconstruct FDIA in microgrids with CPLs, which makes the system model non-linear. The reconstruction of an attack signal is a more restrictive process than just the detection and isolation of the cyber-attack, and it offers significant advantages. The isolation of the compromised agent offers limited options in terms of reducing the attack consequences on the system. In general, the only available option is to disconnect the attacked agent from the system. Alternatively, the reconstructed attack signal value can be used to *clean* the compromised sensor/cyber-link, which mitigates the effect of the cyber-attack on the system and increases the resilience of the DC microgrid operating with non-linear loads.

The specific contributions of this work are as follows:

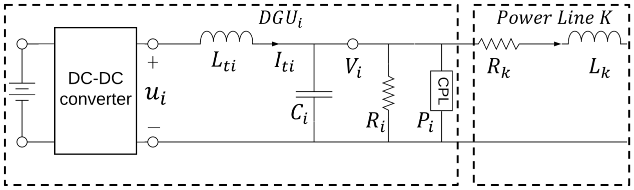

Fig. 1. Electrical scheme of the DGU and power line k. Used symbols are described in Table I.

TABLE I
SYMBOLS USED IN FIG. 1

States	
I_{ti}	DGU current
V_i	Load voltage
I_k	Power Line current
Parameters	
L_{ti}	Filter inductance
C_i	Shunt capacitor
R_i	Local load impedance
R_k	Power line resistance
L_k	Power line inductance
Inputs	
u_i	Input voltage
P_i	Local power load

- A non-linear observer-based strategy that achieves a secure state-estimation for DC microgrid models with unknown CPLs.
- An attack detector is proposed that uses the secure estimation to detect and reconstruct a FDIA signal for the current sensor.
- The proposed reconstruction scheme is validated through numerical simulations and experimental validation, where sensor noise, uncertainty and communication delays are taken into account.

The remaining of this paper is organized as follows. Section II introduces the considered DC microgrid model and formulates the estimation problem. Section III introduces the state and parameter estimation algorithm that is used for the attack reconstruction. In Section IV, the proposed approach is validated in a set of numerical simulations. In Section V, the approach is validated in a real experimental setup. In Section VI, some conclusions are drawn.

II. Cooperative DC microgrid model and Problem Formulation

The considered microgrid is formed by a set of DGUs, which are connected through a set of resistive power lines. Each DGU is modelled as a DC voltage source, which is connected to a DC/DC converter. The DGU is assumed to supply a local DC load, which is modelled as a constant impedance plus a CPL. The local load is connected to the same point of common coupling that interfaces the DGU with the power lines [28]. A general schematic of the considered DGU is depicted in Fig. 1.

Under the standard assumption that the converter operates in continuous conduction mode, the average model of the i_{th}

DGU is given by:

$$\begin{aligned} L_{ti}\dot{I}_{ti} &= -V_i + u_i \\ C_i\dot{V}_i &= I_{ti} - \sum_{k\in\mathscr{E}_i} I_{k,i} - \frac{1}{R_i}V_i - P_i\frac{1}{V_i} \\ L_k\dot{I}_k &= (V_i - V_j) - R_kI_k \quad \forall k\in\mathscr{E}_i, \end{aligned} \tag{1}$$

where the input voltage u_i depicts the average output voltage of the converter and $\mathscr{E}_i$ is the set of incident power lines.

It is assumed that the generated current, I_{ti}, and the load voltage, V_i, are being measured, but the line current, I_k, is unmeasured. Thus, the measured output vector in the i_{th} DGU is going to be defined as $\mathbf{y}_i = [y_{1,i}, y_{2,i}]^\intercal = [I_{ti}, V_i]^\intercal$.

The whole DC microgrid is modelled through an undirected communication graph $\mathscr{G} = \{\mathscr{V}, \mathscr{E}\}$, which is assumed to be connected and without self-loops. The set of nodes, $\mathscr{V}$, depicts the DGUs and the edges (or cyber-links), $\mathscr{E}$, represents the resistive lines that connect the DGUs [28]. The topology of the graph is depicted by the corresponding node-edge incident matrix $\mathscr{B} \in \mathbb{R}^{n\times m}$, where n is the number of DGUs and m the number of resistive power lines. The entries of the matrix $\mathscr{B}$ are specified as:

$$\mathscr{B}_{ij} = \begin{cases} +1, & \text{if i is the positive end of the line j} \\ -1, & \text{if j is the negative end of the line j} \\ 0, & \text{otherwise.} \end{cases} \tag{2}$$

Finally, it is assumed that the whole microgrid is controlled following the droop control philosophy and a secondary controller to compensate the error introduced by droop controller. Droop control is a common strategy used to obtain equal current sharing and voltage control in DC microgrids without communication, thereby adding a voltage offset and degrading the system performance. The idea is to equilibrate the current by imposing a voltage offset that is compensated by secondary controllers [29]. Each DGU control strategy is supplemented by the information from other DGUs to establish distributed secondary control. Each vertex sends and receives the signals $\boldsymbol{\psi}_i = [\psi_{1,i}, \psi_{2,i}]^\intercal = [\hat{v}_{dc,i}, I_{ti}]^\intercal$. The factor $\hat{v}_{dc,i}$ depicts the average voltage estimate in the i_{th} DGU [30], which is estimated through a secondary voltage observer [5]. Specifically, two voltage off-set terms for the i_{th} DGU are computed using

$$\begin{aligned} \Delta V_{1i} &= H_1(s)(V_{dc,ref} - \sum_{k\in\mathscr{E}_i}(\hat{v}_{dc,k} - \hat{v}_{dc,i})) \\ \Delta V_{2i} &= H_2(s)(I_{dc,ref} - \sum_{k\in\mathscr{E}_i}(I_{tk} - I_{ti})) \end{aligned} \tag{3}$$

where $V_{dc,ref}$ and $I_{dc,ref}$ are global voltage and current reference quantities for all the microgrid's DGU, respectively, and $H_1(s)$ and $H_2(s)$ are proportional integral (PI) controllers.

The correction terms (3) are used as an off-set in the local voltage reference that has to be tracked by the i_{th} DGU. Specifically,

$$V_{dc,ref,i} = V_{dc,ref} + \Delta V_{1i} + \Delta V_{2i}. \tag{4}$$

In this work, it is assumed that each DGU has two PI controllers, $G_v(s)$ and $G_i(s)$, connected in cascade that ensure the tracking of the local voltage reference, $V_{dc,ref,i}$. Therefore, the input voltage, u_i, ensures the tracking of a current reference signal, $I_{ref,i}$ (generated by the first PI in the cascade, $G_v(s)$), through a PI controller of the form [30]:

$$u_i = K_{pI}\Big(y_{1,i} - I_{ref,i}\Big) + K_{iI}\int\Big(y_{1,i} - I_{ref,i}\Big). \tag{5}$$

A scheme of the primary and secondary control can be seen in Fig. 2.

Using the presented consensus algorithm, the DC microgrid objectives shall converge to [6]:

$$\lim_{x\to\infty}\phi_V = V_{dc,ref}, \lim_{x\to\infty}\phi_I = 0 \quad \forall i = 1, ..., n. \tag{6}$$

The functions ϕ_V and ϕ_I are defined as:

$$\phi_V = V_i + \int_0^t \sum_{k\in\mathscr{E}_i}(\hat{v}_{dc,k} - \hat{v}_{dc,i}) \tag{7}$$

$$\phi_I = \sum_{k\in\mathscr{E}_i}(I_{tk} - I_{ti}) \tag{8}$$

where $\hat{v}_{dc,i}$ depicts the average voltage estimate in the i_{th} DGU, which is estimated through a secondary voltage observer [5] and I_{ti} is the measured DGU output current.

This paper focuses on the detection, isolation and reconstruction of a false data injection attack that can affect the generated current sensor, the cyber-link that transmits the generated current between vertices, or both. Specifically, an attack on the i_{th} agent can be modelled as:

$$\textbf{Sensor attack}: \quad \mathbf{y}_i = [I_{ti} + x_i^a, V_i]^\intercal \tag{9}$$

$$\textbf{Cyber link attack}: \quad \boldsymbol{\psi}_i = [\hat{v}_{dc,i}, I_{ti} + x_i^a]^\intercal \tag{10}$$

where x_i^a depicts the FDIA signal.

This work assumes that a sensor FDIA and a cyber link in the i_{th} DGU can be conducted separately by compromising the controller or the local communication server, respectively.

It is assumed that the signal x_i^a is a deception attack [30], i.e. the immediate objectives of the microgrid's (6) are satisfied, but may have a long term effect on the system. The design of this type of attack in cooperative DC microgrids has been addressed in previous works [30], [31]. In case of an attack that is not deceptive, the DC microgrid will be driven to an average voltage different from the established global reference value. As each DGU knows the reference value, a simple comparison can be used to detect if the microgrid is being attacked by an external agent [30].

This work assumes that the voltage sensor is free of FDIAs. In the considered system, a stealth attack is not possible by manipulating voltage sensors due to the presence of a distributed observer [31]. The attack needs to be conducted on the average voltage estimate, which is not a measurable quantity.

The main objective is to design an algorithm that can reconstruct the attack signal x_i^a, i.e., the algorithm has to generate an estimation $\hat{x}_i^a$ such that $\|x_i^a - \hat{x}_i^a\| \to 0$ in finite time. It is also worth noting that this objective is more restrictive than achieving an isolation of the attack, which only requires to find the compromised sensor or cyber-link, but does not necessarily acquire any information of the attack signal. The main advantage of reconstructing the attack signal is that the effect of the attack over the considered system can be mitigated. Specifically, assume that a sensor attack is reconstructed, i.e. $x_i^a = \hat{x}_i^a$. Then, the attacked sensor (or cyber-link) can be *cleaned* using:

$$\mathbf{y}_i^{cleaned} = [y_{1,i} - \hat{x}_i^a, y_{2,i}]^\intercal = [I_{ti}, V_i]^\intercal, \tag{11}$$

which completely eliminates the effect of the attack in the DC microgrid.

The idea is to design an observer that, irrespective of the presence of an attack, can estimate the actual value of the generated current, I_{ti}, such that $\|\hat{I}_{ti} - I_{ti}\| \rightarrow 0$ in finite time, where $\hat{I}_{ti}$ depicts the current estimation. If it is achieved, the attack can be reconstructed in finite time by comparing the estimation with the measured value of the current. Specifically, a sensor attack signal can be reconstructed by computing the following:

$$\hat{x}_i^a = y_{1,i} - \hat{I}_{ti} = I_{ti} + x_i^a - \hat{I}_{ti} \tag{12}$$

and a cyber-link attack can be reconstructed as:

$$\hat{x}_i^a = \psi_{2,i} - \hat{I}_{ti} = I_{ti} + x_i^a - \hat{I}_{ti}. \tag{13}$$

By direct inspection of (12) (13), it can be seen that $\|\hat{I}_{ti} - I_{ti}\| \rightarrow 0$ implies $\|x_i^a - \hat{x}_i^a\| \rightarrow 0$. Therefore, the problem of reconstructing the attack signal has been transformed to an observer design problem.

Notice that this approach is invariant to the reliability of the current sensor. Therefore, the presence of an attack can always be reconstructed by means of (12) and (13).

In order to ease the scalability of the algorithm, it is of prime interest to design a distributed observer algorithm. This means that the observer of the i_{th} DGU has to generate an estimation of I_{ti} based only on the signals measured in the i_{th} DGU, $\mathbf{y}_i$, and the signals transmitted through the incident cyber-links, $\boldsymbol{\psi}_i$.

The presence of CPLs introduces a non-linear term in the DGU model (1). As pointed out in the introduction, linear approximations of the model are not adequate for the considered problem. For this reason, it is of prime importance to work with the non-linear dynamics and design a non-linear observer.

In relation to the non-linear observer design, it is crucial to select the adequate measured signal that is going to be used for state estimation. An intuitive choice is to use the measured voltage, V_i. Furthermore, it is important to select the adequate observer technique. In the current state of the art, there is no generic methodology for observer design in non-linear systems. In general, each observer strategy assumes certain structures in the system equations. Thus, before selecting any observer technique, it is important to study which signals are required for the estimation of I_{ti}. Consider the following:

Lemma II.1. *The DGU output current, I_{ti}, can be reconstructed asymptotically using the CPL, P_i, the voltage, V_i, its derivative, $\dot{V}_i$, and the line currents, $I_{k,i}$, through the following expression:*

$$\hat{I}_{ti} = C_i \hat{\dot{V}}_i + \sum_{k \in \mathscr{E}_i} \hat{I}_{k,i} + \frac{1}{R_i}\hat{V}_i + \hat{P}_i \frac{1}{\hat{V}_i}. \tag{14}$$

Proof. Expression (14) is obtained by isolating I_{ti} from the second equation in (1). □

Therefore, the generated current estimation can be achieved through the estimations $\hat{\dot{V}}_i$ and $\hat{I}_{k,i}$. Assuming that one generates an estimation, $\hat{\dot{V}}_i$ and $\hat{I}_{k,i}$ such that $\|\hat{\dot{V}}_i - \dot{V}_i\| \rightarrow 0$ and $\|\hat{I}_{k,i} - I_{k,i}\| \rightarrow 0$. Then, $\|\hat{I}_{ti} - I_{ti}\| \rightarrow 0$, where $\hat{I}_{ti}$ is computed through (14) using the estimations $\hat{\dot{V}}_i$ and $\hat{I}_{k,i}$.

As it will be shown in the next section, it is possible to design an observer algorithm that achieves $\|\hat{\dot{V}}_i - \dot{V}_i\| \rightarrow 0$ and $\|\hat{I}_{k,i} - I_{k,i}\| \rightarrow 0$, even in the presence of model uncertainty. Nevertheless, there is another concern to be addressed. A common issue in DC microgrids is that the CPL, P_i, may be unknown [27], which prevents the computation of (14). In order to overcome this limitation, the proposed observer algorithm will also estimate the unknown CPL.

Notice that the reconstruction of the attack signal (12) (13) can also be employed to detect the presence of an attack, which may be later used to activate secondary security protocols. Specifically, define the following residual for the detection of a sensor attack in the i_{th} DGU:

$$r_{s,i} = y_{1,i} - \hat{I}_{ti}; \tag{15}$$

and a residual for a cyber link attack:

$$r_{cl,i} = \psi_{2,i} - \hat{I}_{ti}. \tag{16}$$

The presence of an attack can be detected by evaluating the following inequalities:

$$\textit{Sensor attack}: \quad r_{s,i} > \bar{r}_i \tag{17}$$

$$\textit{Cyber link attack}: \quad r_{cl,i} > \bar{r}_i \tag{18}$$

where $\bar{r}_i$ is a positive constant parameter designed appropriately to avoid false alarms induced by the voltage sensor noise. The design of $\bar{r}_i$ is related to the accuracy of the estimation scheme under measurement noise, which will be discussed in Section III.

III. Proposed Non-Linear Observer

Following the reasoning in the previous section, the objective here is to design an observer algorithm that can estimate, $\dot{V}$, $I_{k,i}$ for $k \in \mathscr{E}_i$ and P_i, of the i_{th} DGU.

The first step in the observer design is to define a coordinate change that transforms the system into a form that accepts an observer. It is convenient to have the coordinate transformation independent of the input, u_i. As the DC-DC converter is controlled using the measured generated current (5), the signal u_i is sensitive to the sensor FDIA. Therefore, an input-dependant coordinate transformation will be sensitive to the attack signal, which introduces an inherent bias in the estimation.

Lemma III.1. *Define m_i as the number of incident edges in the i_{th} vertex. Then, the following input-independent map*

$$\begin{bmatrix} \xi_{1,i} \\ \xi_{2,i} \\ \eta_{1,i} \\ \vdots \\ \eta_{m,i} \end{bmatrix} = \begin{bmatrix} V_i \\ \dot{V}_i \\ I_{1,i} \\ \vdots \\ I_{m_i,i} \end{bmatrix} \tag{19}$$

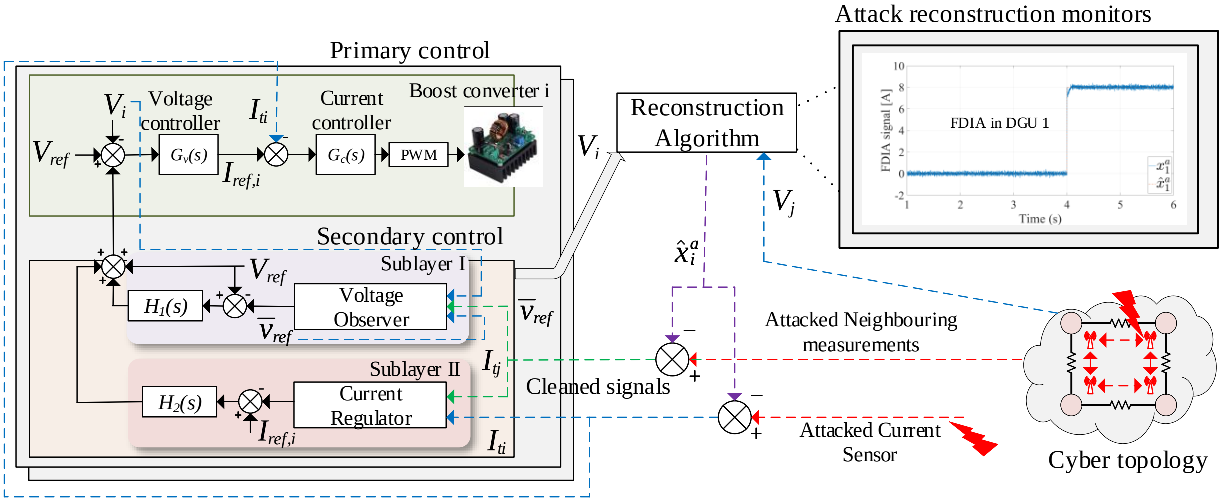

Fig. 2. General scheme of the primary control, secondary control and the proposed FDIA mitigation strategy. Sublayer I of secondary control depicts the computation of the off-set ΔV_{1i} in (3). Sublayer II of secondary control depicts the computation of the off-set ΔV_{2i} in (3). Primary control depicts the two PI in cascade that tracks the local voltage reference, $V_{dc,ref,i}$. The reconstruction algorithm block depicts the attack estimation strategy presented in this work.

defines a diffeomorphism that transforms the system (1) into the following triangular form

$$\begin{aligned}
\dot{\xi}_{1,i} &= \xi_{2,i} \\
\dot{\xi}_{2,i} &= \phi_i(\boldsymbol{\xi}_i, u_i, P_i, \boldsymbol{\eta}_i) \qquad (20) \\
\dot{\eta}_{j,i} &= \frac{1}{L_k}(\xi_{1,i} - \xi_{1,j}) - \frac{R_k}{L_k}\eta_{j,i} \quad \textit{for } j = 1, ..., m_i
\end{aligned}$$

where $\boldsymbol{\xi}_i = [\xi_{1,i}, \xi_{2,i}]^\intercal, \boldsymbol{\eta}_i = [I_{1,i}, \dots I_{m_i,i}]^\intercal$ *and*

$$\begin{aligned}
\phi_i(\boldsymbol{\xi}_i, u_i, P_i, \boldsymbol{\eta}_i) &= \frac{1}{C_i}\Bigg(\frac{1}{L_{ti}}\big(-\xi_{1,i} + u_i\big) - \frac{1}{R_i}\xi_{2,i} \\
&- \textstyle\sum_{k\in\mathscr{E}_i}\Big(\frac{1}{L_k}(\xi_{1,i} - \xi_{1,j}) - \frac{R_k}{L_k}\eta_{k,i}\Big) + P_i\frac{\xi_{2,i}}{\xi_{1,i}^2}\Bigg). \quad (21)
\end{aligned}$$

The triangular structure (20) is a well-known form that has been deeply studied in the literature. Moreover, there are multiple observer strategies that can be implemented in such non-linear structure, e.g. [32]. Nevertheless, such techniques can only achieve an estimation of $\xi_{1,i}$ and $\xi_{2,i}$, while the m_i states, $\boldsymbol{\eta}_i$, remain in the unobservable space of the system. For this reason, this work proposes dividing the observer into two parts. The first one will estimate the unobservable states $\boldsymbol{\eta}$ in open-loop. The second one will estimate the states $\xi_{1,i}$ and $\xi_{2,i}$ and the unknown parameter P_i through a high-order differentiator.

A. Estimation of $\boldsymbol{\eta}$

The dynamics of $\boldsymbol{\eta}$ (last equation of (20)) represent the zero dynamics of system (20),i.e. the states, $\boldsymbol{\eta}$, are not observable from the output, $y = \xi_{1,i}$ [33]. As a consequence, it is not directly possible to estimate its value through a tunable observer. However, as the DC microgrid is assumed to have an average voltage control, the $\boldsymbol{\eta}$ dynamics are stable (i.e. the $\boldsymbol{\eta}$ dynamics are not observable but detectable). Therefore, it is possible to estimate its value through open-loop integration.

Lemma III.2. *Assume that there is an estimation of $\xi_{1,i}$ and $\xi_{1,j}$ depicted as $\hat{\xi}_{1,i}$ and $\hat{\xi}_{1,j}$, such that $\|\xi_{1,i} - \hat{\xi}_{1,i}\| = \|\xi_{1,j} - \hat{\xi}_{1,j}\| = 0$. Then, the state $\eta_{j,i}$ can be estimated by integrating the following expression:*

$$\dot{\hat{\eta}}_{j,i} = \frac{1}{L_k}(\hat{\xi}_{1,i} - \hat{\xi}_{1,j}) - \frac{R_k}{L_k}\hat{\eta}_{j,i} \qquad (22)$$

for any initial condition $\hat{\eta}_{1,i}(0)$.

Proof. Consider the estimation error $e_\eta \triangleq \eta_{j,i} - \hat{\eta}_{j,i}$. The error dynamics are depicted by:

$$\begin{aligned}
\dot{e}_\eta &= \frac{1}{L_k}(\xi_{1,i} - \xi_{1,j}) - \frac{R_k}{L_k}\eta_{j,i} - \frac{1}{L_k}(\hat{\xi}_{1,i} - \hat{\xi}_{1,j}) + \frac{R_k}{L_k}\hat{\eta}_{j,i} \\
&= -\frac{R_k}{L_k}e_\eta \qquad (23)
\end{aligned}$$

which converges to zero, independently of the initial value $e_\eta(0)$. □

Remark III.1. *Notice that the computation of (22) requires the communication of $\hat{\xi}_{1,j}$ between observers. This transfer of information may be the entrance of other attacks. Thus, further work related to detecting attacks in $\hat{\xi}_{1,j}$ is required.*

Remark III.2. *As $\eta_{j,i}$ is estimated in open-loop, the accuracy of the estimation is sensitive to uncertainty in the parameters R_k and L_k. Moreover, the convergence rate of the estimation is not tunable. Nonetheless, for autonomous or islanded DC microgrids, it is reasonable to expect that the voltages between DGUs converge to the same value. Thus, it is expected that $\|\xi_{1,i} - \xi_{1,j}\| \to 0$, which leads to an accurate estimation of the power lines even in the presence of uncertainty. The convergence rate of the power-lines estimator depends on the converter's parameters, which are usually designed to be fast.*

B. Estimation of $\xi_{1,i}$, $\xi_{2,i}$ and P_i

The first two equations of (20) form a well-known triangular structure which accepts multiple observer strategies. Nevertheless, the implemented strategy has to also reconstruct the unknown CPL, P_i. In order to achieve the unknown parameter estimation, the idea is to design an observer that can robustly estimate the states $\xi_{1,i}$, $\xi_{2,i}$ and the function $\phi(\boldsymbol{\xi}_i, u_i, P_i, \boldsymbol{\eta}_i)$ of (21). Then, the constant parameter P_i can be solved through equation (21). Such estimation can be achieved by implementing an extended observer [34], i.e. the first two equations of (20) are going to be extended through a virtual state σ as follows:

$$\begin{aligned}\dot{\xi}_{1,i} &= \xi_{2,i}\\ \dot{\xi}_{2,i} &= \sigma \qquad (24)\\ \dot{\sigma} &= \frac{\partial\phi_i(\boldsymbol{\xi}_i, u_i, P_i, \boldsymbol{\eta}_i)}{\partial\boldsymbol{\xi}_i}\dot{\boldsymbol{\xi}}_i + \frac{\partial\phi_i(\boldsymbol{\xi}_i, u_i, P_i, \boldsymbol{\eta}_i)}{\partial\boldsymbol{\eta}_i}\dot{\boldsymbol{\eta}}_i\\ &\quad + \frac{\partial\phi_i(\boldsymbol{\xi}_i, u_i, P_i, \boldsymbol{\eta}_i)}{\partial u}\dot{u}_i.\end{aligned}$$

In particular, the function $\phi(\boldsymbol{\xi}_i, u_i, P_i, \boldsymbol{\eta}_i)$ is taken as an extra state that has to be estimated through the observer. Notice that system (24) is still a triangular structure, thus, it still accepts multiple non-linear observer strategies. This work will implement a high-order sliding-mode observer [32], mainly due to is insensitivity to uncertainty in the last equation of (24) and its finite time convergence, which allows to mitigate a false data attack in a finite time. Specifically, the observer takes the following structure:

$$\begin{aligned}\dot{\hat{\xi}}_{1,i} &= \hat{\xi}_{2,i} - \lambda_0|\hat{\xi}_{1,i} - y_{2,i}|^{(2/3)}sign(\hat{\xi}_{1,i} - y_{2,i})\\ \dot{\hat{\xi}}_{2,i} &= \hat{\sigma} - \lambda_1|\hat{\xi}_{2,i} - \dot{\hat{\xi}}_{1,i}|^{(1/2)}sign(\hat{\xi}_{2,i} - \dot{\hat{\xi}}_{1,i}) \qquad (25)\\ \dot{\hat{\sigma}} &= -\lambda_2 sign(\hat{\sigma} - \dot{\hat{\xi}}_{2,i})\end{aligned}$$

where λ_0, λ_1 and λ_2 are parameters to be tuned and $sign(\cdot)$ is the sign function which is computed as:

$$sign(x) = \begin{cases}\dfrac{x}{\|x\|} & if\ x \neq 0\\ 0 & if\ x = 0\end{cases} \qquad (26)$$

Theorem III.1. *Consider the extended system (24), the high-order sliding-mode observer (25), the generated current estimation (14) and the open-loop estimator (22). Furthermore, tune the observer design parameters as [35]:*

$$\lambda_0 = 3.4478M^{1/3},\ \lambda_1 = 5.6477M^{2/3},\ \lambda_2 = 1.1M \qquad (27)$$

where M is the upper bound of the voltage third derivative $\dot{\sigma}$, such that $\|\dot{\sigma}\| \leq M$.

Then, the observer estimation converges in finite-time, i.e. there is a positive finite time T such that, for all time $t > T$, $\|\xi_{1,i} - \hat{\xi}_{1,i}\| = 0$, $\|\xi_{2,i} - \hat{\xi}_{2,i}\| = 0$ and $\|\phi(\boldsymbol{\xi}_i, u_i, P_i, \boldsymbol{\eta}_i) - \hat{\sigma}\| = 0$. Moreover, assume that there is no generated current sensor attack, i.e. $y_{1,i} = I_{ti}$ and consider the estimation function:

$$\begin{aligned}\hat{P}_i = &\left(\frac{\hat{\xi}_{2,i}}{\hat{\xi}_{1,i}^2} + \frac{K_{pI}}{L_{ti}}\frac{1}{\hat{\xi}_{1,i}}\right)^{-1}\Bigg[C_i\hat{\sigma} + \frac{1}{L_{ti}}\hat{\xi}_{1,i}\\ &+ \sum_{k\in\mathscr{E}_i}\Big(\frac{1}{L_k}(\hat{\xi}_{1,i} - \hat{\xi}_{1,j}) + \frac{R_k}{L_k}\hat{\eta}_{k,i}\Big) - \frac{1}{R_i}\hat{\xi}_{2,i}\\ &- \frac{K_{pI}}{L_{ti}}\left(C_i\hat{\xi}_{2,i} + \sum_{k\in\mathscr{E}_i}\hat{\eta}_{k,i} + \frac{1}{R_i}\hat{\xi}_{1,i} - I_{ref,i}\right)\\ &- \frac{K_{iI}}{L_{ti}}\int\left(y_{1,i} - I_{ref,i}\right)\Bigg]. \qquad (28)\end{aligned}$$

Then, if $\|\xi_{1,i} - \hat{\xi}_{1,i}\| \to 0, \|\xi_{2,i} - \hat{\xi}_{2,i}\| \to 0$ and $\|\phi(\boldsymbol{\eta}, u_i, P_i, \boldsymbol{\eta}) - \hat{\sigma}\| \to 0$, the norm $\|P_i - \hat{P}_i\|$ also converges to zero.

Proof. Define the estimation errors $e_{1,i} = \xi_{1,i} - \hat{\xi}_{1,i}, e_{2,i} = \xi_{2,i} - \hat{\xi}_{2,i}$ and $e_{3,i} = \sigma - \hat{\sigma}$. Then, the error dynamics satisfy the following:

$$\begin{aligned}\dot{e}_1 &= e_2 - \lambda_0|e_1|^{(2/3)}sign(e_1)\\ \dot{e}_2 &= e_3 - \lambda_1|e_1|^{(1/2)}sign(e_1) \qquad (29)\\ \dot{e}_3 &= \dot{\sigma} - \lambda_2 sign(e_1).\end{aligned}$$

By assumption, the function $\dot{\sigma}$ is Lipschitz and bounded as $|\dot{\sigma}| \leq M$. Previous works [35] have already proven that for an adequate choice of λ_0, λ_1 and λ_2, the dynamics (29) converge in finite-time to the origin. Furthermore, if the design parameters are tuned following the Lyapunov methodology introduced in [35], it is possible to find an explicit upper-bound of the convergence time. Specifically, for a third-order estimator, said methodology leads to the design parameters depicted in (27).

Define the scaled errors,

$$z_1 = \frac{e_1}{M}, \quad z_2 = \frac{e_2}{3.4478M}, \quad z_3 = \frac{e_3}{5.6477M}, \qquad (30)$$

then, the convergence time, T, of the estimation error is upper-bounded by a factor that depend on the initial conditions of the estimation error [35]:

$$T(\mathbf{z}_0) \leq 13.5135 \cdot V(\mathbf{z}_0)^{0.2}, \qquad (31)$$

where $\mathbf{z}_0$ are the initial conditions of the scaled errors (30) and V is the following function:

$$\begin{aligned}V(\mathbf{z}) = &\frac{3}{5}|z_1|^{5/3} - z_1|z_2|^{\frac{2}{4}}sign(z_2) + \frac{2}{5}|z_2|^{\frac{5}{4}}\\ &+ \frac{2}{5}|z_2|^{\frac{5}{2}} - z_2|z_3|sign(z_3) + \frac{3}{5}|z_3|^{\frac{5}{3}} + 0.2|x_3|^5. \qquad (32)\end{aligned}$$

Thus, for all $t > T(\mathbf{z}_0)$, $\|\xi_{1,i} - \hat{\xi}_{1,i}\| = 0, \|\xi_{2,i} - \hat{\xi}_{2,i}\| = 0$ and $\|\phi(\boldsymbol{\xi}_i, u_i, P_i, \boldsymbol{\eta}_i) - \hat{\sigma}\| = 0$, independently of the value of the voltage third derivative, $\dot{\sigma}$.

Therefore, after a finite time, the following holds:

$$\begin{aligned}\hat{\sigma} = \phi_i(\boldsymbol{\xi}_i, u_i, P_i, \boldsymbol{\eta}_i) &= \frac{1}{C_i}\Bigg(\frac{1}{L_{ti}}\big(-\xi_{1,i}+u_i\big)\\ &- \sum_{k\in\mathscr{E}_i}\big(\frac{1}{L_k}(\xi_{1,i}-\xi_{1,j})-\frac{R_k}{L_k}\eta_{k,i}\big)-\frac{1}{R_i}\xi_{2,i}+P_i\frac{\xi_{2,i}}{\xi_{1,i}^2}\Bigg)\\ &= \frac{1}{C_i}\Bigg(\frac{1}{L_{ti}}\big(-\xi_{1,i}+K_{pI}\Big(y_{1,i}-I_{ref,i}\Big)\\ &+ K_{iI}\int\Big(y_{1,i}-I_{ref,i}\Big)\Big)\big)\\ &- \sum_{k\in\mathscr{E}_i}\big(\frac{1}{L_k}(\xi_{1,i}-\xi_{1,j})-\frac{R_k}{L_k}\eta_{k,i}\big)-\frac{1}{R_i}\xi_{2,i}+P_i\frac{\xi_{2,i}}{\xi_{1,i}^2}\Bigg).\end{aligned} \tag{33}$$

By substituting (33) in (28) and taking into account that $\|\xi_{1,i}-\hat{\xi}_{1,i}\| \rightarrow 0, \|\xi_{2,i}-\hat{\xi}_{2,i}\| \rightarrow 0$, $\|\eta_{j,i}-\hat{\eta}_{j,i}\| \rightarrow 0$ and $V_i \neq 0$, the following holds:

$$\hat{P}_i = \left(\frac{\hat{\xi}_{2,i}}{\hat{\xi}_{1,i}^2}+\frac{K_{pI}}{L_{ti}}\frac{1}{\hat{\xi}_{1,i}}\right)^{-1}\left(\frac{\xi_{2,i}}{\xi_{1,i}^2}+\frac{K_{pI}}{L_{ti}}\frac{1}{\xi_{1,i}}\right)P_i = P_i. \tag{34}$$

□

Remark III.3. *An improper parameter tuning may lead to an unstable observer, i.e. the estimation error will diverge to infinity. There are alternative parameter tuning methodologies, however, in general, it is difficult to compute an explicit time of convergence in such alternative parameter tuning.*

Remark III.4. *During a sensor attack, the CPL estimation reduces to:*

$$\hat{P}_i = P_i + \left(\frac{\hat{\xi}_{2,i}}{\hat{\xi}_{1,i}^2}+\frac{K_{pI}}{L_{ti}}\frac{1}{\hat{\xi}_{1,i}}\right)^{-1}\left(\frac{K_{pI}}{L_{ti}}x_i^a\right)P_i. \tag{35}$$

Therefore, the presence of a sensor attack introduces a bias in the constant load estimation. Nonetheless, this bias has no significant effect in the mitigation strategy. This fact will be seen in the experimental validation of Section V, where sensor FDIAs are introduced in the system and the algorithm still recovers pre-attack performances.

Nevertheless, as the observer algorithm converges in finite time, it is reasonable to assume that the CPL estimation, $\hat{P}_i$ has already converged to the true value before a sensor attack is introduced in the system. Thus, during a sensor attack, the parameter estimation can be frozen to avoid the bias introduced by the sensor attack. This approach has been validated in the first case study of the numerical simulation of Section IV.

The expression (28) is computable, if the inequality $0 \leq \hat{\xi}_{1,i} \leq \infty$ is satisfied. Most DGUs in DC microgrids operates with bounded voltages and a properly tuned and initialized observer will not reach such values. Thus, this condition is generically satisfied. It should be remarked that, alternatively to the approach in this work, the joint state and parameter estimation problem is commonly solved through an adaptive observer [36]. Nevertheless, classic adaptive observer schemes can only ensure the convergence of the parameter estimation to the actual value under a restrictive persistence of excitation condition [37], which may not be satisfied in some DC microgrid operating conditions.

Finding the positive constant M for similar sliding-mode techniques usually involve extensive simulations. Nevertheless, under the proper assumptions, this expensive computations can be avoided in the concerned microgrid.

The microgrid's cooperative secondary controller ensures the objectives depicted in (6). Moreover, due to the convergence properties of the local controllers and microgrid security concerns, it is reasonable to assume that the load voltage is bounded as $V_{min,i} < V_i < V_{max,i}$, the DGU load current is lower bounded as $I_{ti} > I_{min,i}$ and the inputs are also bounded as $u_i < u_{max,i}$.

Moreover, since the capacity of the system is planned based on the converter's capacity, using the generation-load matching criteria it is possible to show that the CPL value is bounded as $P_i < P_{max,i}$. Taking into account these details, it is possible to find an analytical expression of M. Specifically, the expression is:

$$\begin{aligned}M = \frac{-\xi_{2,i,min}}{C_i L_{ti}} - 2\frac{P_{max,i}}{C_i}\frac{\xi_{2,i,min}^2}{V_{max}^3} - \frac{\sigma_{max}}{C_i R_i}\\ + \frac{P_{max,i}}{C_i}\frac{\sigma_{max}}{V_{min}^2},\end{aligned} \tag{36}$$

where

$$\xi_{2,i,min} = I_{min,i} - \frac{\sqrt{P_{max,i}R_i}}{R_i} - \frac{P_{max,i}}{\sqrt{P_{max,i}R_i}} \tag{37}$$

$$\begin{aligned}\sigma_{max} = \frac{1}{C_i}\Bigg(\frac{1}{L_{ti}}\Big[-\frac{1}{R_i}\xi_{2,i,max}+u_{max,i}\Big]\\ + \frac{P_{max}}{C_i}\frac{\xi_{2,i,max}}{V_{min,i}^2}\Bigg).\end{aligned} \tag{38}$$

In relation to the design of the threshold values in the detection algorithm (17) and (18). Assume that the voltage sensor in the i_{th} DGU is corrupted by an additive noise signal, n_i, upper-bounded by a positive constant ε_i as $|n_i| < \varepsilon$. Then, the higher-order sliding-mode observer ensures an unbiased observation error accuracy of the order of $1.1M^{2/3}\varepsilon_i$ [35]. Therefore, the threshold functions (17) (18) will avoid false alarms induced by the noise, if $\bar{r}_i > \kappa 1.1 M^{2/3}\varepsilon_i$, where $\kappa > 1$.

C. Stabilization properties of the observer

The introduction of current FDIAs may destabilize the DC microgrid. It is well known that CPLs have a destabilizing effect on DC microgrids and local DGU controllers have to be designed to ensure the stability of the system around the considered operating point [27]. As the DGUs of the concerned microgrid are controlled through linear PI controllers, the stability can only be ensured in a region of attraction around the equilibrium point where the PI has been tuned [38]. Specifically, for a DGU modelled as in (1) and a cascaded PI as the DGU's primary control, there is a region $D_i \subset \mathbb{R}^2$ such that if $I_{ti}, V_i \in D_i$, then, the DGU's voltage and output current converge to the desired references. Otherwise, the system becomes unstable [38]. The region of attraction of cooperative DC microgrids with linear controllers can be computed through a series of sum of square optimizations [38].

Suppose that at time t_0 the i_{th} DGU's states are inside the region of attraction and the system is subjected to a cyber attack. During the attack, the system response involves large variations of the state variables which may lead to an escape of the region of attraction and, consequently, may lead to an unstable system. This fact confirms that the interaction between FDIAs and CPLs can destabilize the plant.

In such cases, it is important to study if the proposed mitigation strategy can avoid the destabilization of the i_{th} DGU during a FDIA. Suppose that the DGU is subjected to a destabilizing FDIA at time t_0 that would make the DGU escape its region of attraction at time $t_1 > t_0$. After a time $T(\mathbf{z}_0)$ computed through (31), the proposed strategy mitigates the attack and the system switches-back to the pre-FDIA operation. Then, if $T(\mathbf{z}_0) < t_1$, the FDIA is mitigated and the DGU's states are still inside the region of attraction, thus, stability is preserved. Otherwise, if $T(\mathbf{z}_0) \geq t_1$, the FDIA is eliminated but the the DGU's states are outside the region of attraction, consequently, the system remains unstable.

Therefore, the effectiveness of the proposed method under destabilizing FDIAs is limited by the time of convergence of the observer (31) and the capacity of the attacker of reducing the time of escaping the region of attraction, t_1.

IV. Numerical Simulations

The proposed observer strategy has been validated in a pair of numerical simulations. The simulations have been designed to test the performance of the reconstruction scheme in non-trivial situations. The first simulation considers a case in which all the agents of the system are being compromised by a FDIA. The second case considers a situation with a significant amount of communication and sensor high-frequency noise and model uncertainty.

A. Simulation 1: Simultaneous attack on all agents

The first simulation considers a DC microgrid composed by 4 DGUs with unknown CPL interconnected as depicted in Fig. 3. The value of the model parameters are summarized in Table II.

TABLE II
Model parameter values used in Simulation 1

Symbol	Value	Symbol	Value
L_{ti}	$1\ [H]$	R_{14}	$1.3\ [\Omega]$
C_i	$0.05\ [F]$	R_{23}	$2.3\ [\Omega]$
R_i	$96\ [\Omega]$	R_{34}	$2.1\ [\Omega]$
R_{12}	$1.8\ [\Omega]$	L_k	$50\ [\mu H]$

The whole microgrid is controlled using the distributed control strategy presented in [30], which ensures equal current sharing and average voltage control. Specifically, the control has been designed to ensure the convergence of the average voltage to $315V$. During the simulation there is a set of FDIA attacks that compromise all the agents of the microgrid and changes the behaviour of the system. At time $t = 4s$, there is a FDIA that injects a constant value of $8A$ in the cyber-link that connects the DGU 1 with its neighbours. At time $t = 4.5s$, there is a second FDIA that injects a constant value of $6A$ in the cyber-link that connects the DGU 4 with its neighbours.

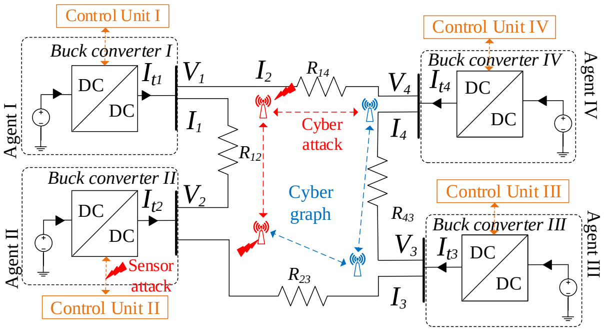

Fig. 3. Topology of the considered DC microgrid with 4 DGUs. Blue arrows represent the cyber-layer and black lines depict the physical circuit.

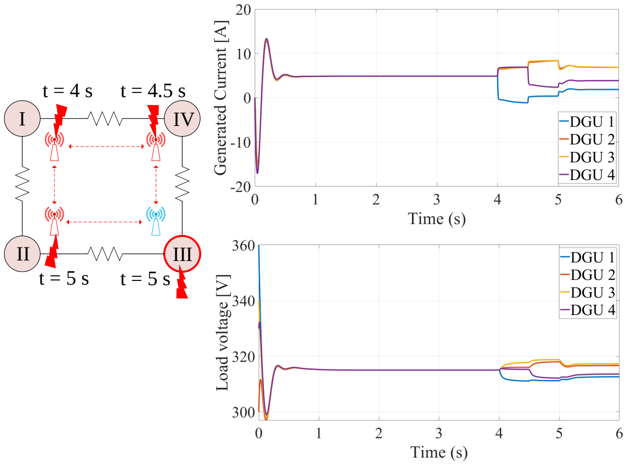

Fig. 4. Current and voltage evolution under FDIAs. At $t = 4s$ there is a FDIA in the DGU 1 cyber-links. At $t = 4.5s$ there is a FDIA in the DGU 4 cyber-links. At $t = 5s$ there is a FDIA in the DGU 2 cyber-links and a FDIA in the generated current sensor of DGU 3.

Finally, at time $t = 5s$ there is a simultaneous attack in the cyber-link of the DGU 2 and the current sensor of the DGU 3. In both cases, a constant value of $3A$ is injected. Notice that for $t > 5s$ there are 4 FDIA attacks that compromises all the agents of the system. As it can be seen in Fig. 4, during the attacks, the system behaviour is significantly affected. However, the microgrid is not destabilized and the average voltage converges to the reference value of $315V$.

Each attack can be detected and reconstructed by implementing the proposed sliding-mode observer in each DGU. After that, the reconstructed attack can be used to "clean" the attacked sensors and cyber-links as depicted in (11). Specifically, all the observers have been implemented considering a factor $M = 100$, which results in the following design parameters $\lambda_0 = 16, \lambda_1 = 121.7$ and $\lambda_2 = 110$ and ensures a convergence time of less than $1.5\ s$.

In Fig. 5 we can see the unknown power load estimation in the different observers. It can be observed that all the estimations converges asymptotically to the true value with a settling time (98%) of around 1.2 second. Thus, even in the case of having no prior information of the CPL (i.e. $\hat{P}_i$ has

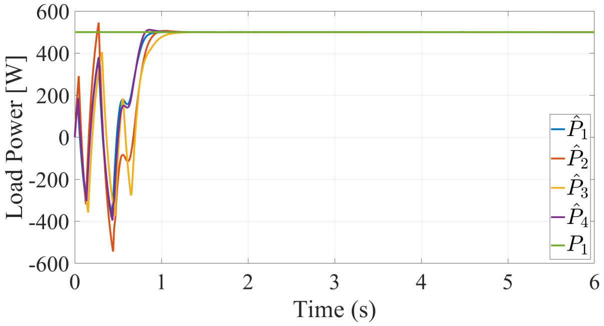

Fig. 5. Evolution of the local power load estimation and true local power load (green). All the DGUs present the same local power load, equal to P_i.

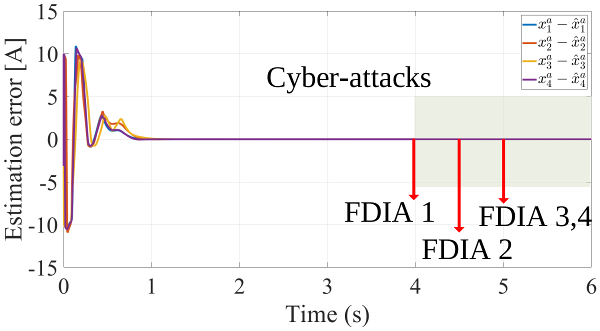

Fig. 6. Evolution of the attack estimation error in all DC microgrid DGUs. At $t = 4s$ there is a FDIA in the DGU 1 cyber-links (FDIA 1). At $t = 4.5s$ there is a FDIA in the DGU 4 cyber-links (FDIA 2). At $t = 5s$ there is a FDIA in the DGU 2 cyber-links and a FDIA in the generated current sensor of DGU 3 (FDIA 3 and 4).

been initialized at 0), the proposed scheme can estimate its true value. Notice that the parameter estimation is invariant to the presence of cyber-link attacks.

In Fig. 6, it is depicted the reconstruction error of the cyber-link attack in DGU 1, DGU 2 and DGU 4 and the sensor attack in DGU 3. In all the cases, it can be observed that all the estimation errors converge to zero in a time of approximately 1 second, indicating that the system is free of attacks. Moreover, the estimation error remains at zero as the attacks are being introduced in the system. Therefore, the proposed strategy is capable of accurately reconstructing the attack signal in all the DGUs, even in the presence of a simultaneous attack. Moreover, this result exemplifies the invariance of the attack reconstruction in the i_{th} DGU to the presence of attacks in the rest of the microgrid.

Finally, the reconstructed attacks have been used to mitigate the effect of the attack in the system (as presented in (11)). In Fig. 7, it is depicted the evolution of the generated currents and load voltages, after the attack mitigation. It can be noticed that, the reconstruction and mitigation of the FDIAs have immediately eliminated the effect of the attacks on the system, which behaves very similar before and after the presence of attacks.

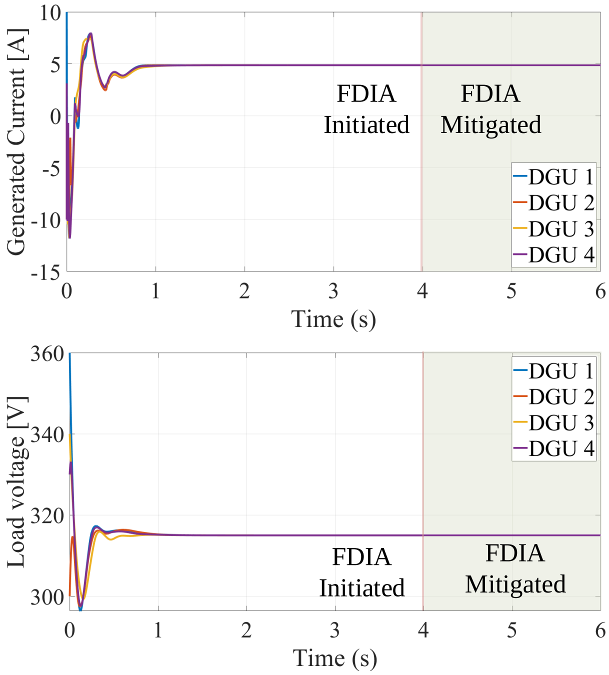

Fig. 7. Current and voltage evolution under FDIAs and observer reconstruction and mitigation. At $t = 4s$ there is a FDIA in the DGU 1 cyber-links. At $t = 4.5s$ there is a FDIA in the DGU 4 cyber-links. At $t = 5s$ there is a FDIA in the DGU 2 cyber-links and a FDIA in the generated current sensor of DGU 3.

This simulation validates the proposed reconstruction and mitigation strategy. Moreover, it exemplifies the scalability of the scheme. The observer parameter tuning and estimation accuracy in the i_{th} DGU is independent to the topology of the DC microgrid and the presence of attacks in other DGUs. Moreover, the observer implementation only requires communicating the observer with the neighbour DGUs in order to communicate $\hat{\xi}_{1,j}$ $for\ j = 1, ..., m_i$ between observers. As a consequence, new DGUs can be incorporated in the microgrid and the proposed reconstruction scheme can still be implemented with minor changes.

B. Simulation 2: Attack reconstruction in presence of sensor noise and model uncertainty

In practice, the model of the microgrid will be imperfect and the system sensors will present a certain amount of noise. The presence of these elements prevent the exact attack detection and reconstruction presented in the past simulation. For this reason, it is important to test the performance of the proposed strategy in a more realistic scenario. In this second simulation it is considered the cooperative DC microgrid studied in the past subsection with the topology presented in Fig. 3. However, it is considered a unique attack in the cyber-links that connect the DGU 1 with its neighbours. The attack consists of a step signal of value $8A$ at time $t = 4s$. As it can be seen in Fig. 8, this type of attack significantly affects the evolution of the microgrid's DGU currents and voltages, but does not prevent the convergence of the average voltage.

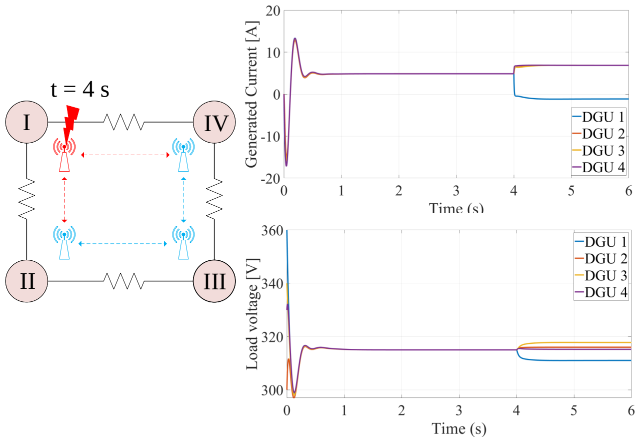

Fig. 8. Current and voltage evolution under FDIA. At $t = 4s$ there is a FDIA in the DGU 1 cyber-links.

The objective is to implement the proposed observer approach in order reconstruct and clean the attacked signal. However, in this case, it is considered that the DGU 1 model is not perfectly known. Specifically, it is assumed that there is uncertainty in the model parameters. In Table III it is depicted the true value of the DGU 1 parameters and the model values that have been used in the observer. The other DGUs parameters are the ones depicted in Table II

TABLE III
TRUE DGU 1 PARAMETERS AND MODEL PARAMETER VALUES USED IN THE OBSERVER

Symbol	True Value	Model value
L_{ti}	$1\ [H]$	$0.8\ [H]$
C_i	$0.05\ [F]$	$0.055\ [F]$
R_i	$96\ [\Omega]$	$90\ [\Omega]$
R_{k1}	$1.8\ [\Omega]$	$1.2\ [\Omega]$
R_{k2}	$1.3\ [\Omega]$	$1.7\ [\Omega]$
L_{k1}	$50 \cdot 10^{-6}\ [H]$	$43 \cdot 10^{-6}\ [H]$
L_{k2}	$50 \cdot 10^{-6}\ [H]$	$53 \cdot 10^{-6}\ [H]$
P_i	$500\ [W]$	$-\ [W]$

Moreover, the sensors of the DGU 1 are corrupted with a significant amount of high-frequency noise. The voltage sensor, V_1, and the voltage signals transmitted from the DGU 2 and DGU3 are affected by random high-frequency noise with variance 0.109. The current sensor, I_{t1}, is corrupted with high-frequency noise with variance 0.0114. In Fig. 9 it is depicted the measured voltage and current, respectively, corrupted with the presented noise.

The design parameters of the sliding-mode observer have been tuned as $\lambda_0 = 16, \lambda_1 = 121.7$ and $\lambda_2 = 110$, which ensures the convergence of the state estimation. Nonetheless, the estimation accuracy of the proposed high-order sliding-mode observer is sensitive to measurement noise. For this reason, the CPL estimation, $\hat{P}_i$, and the attack signal estimation, $\hat{x}_1^a$, have been filtered through a low-pass filter. Most spectral components of the concerned high-frequency noise are around the $1\ kHz$ frequency, the signals have been filtered through a IIR filter with cut-off frequency at $1\ kHz$.

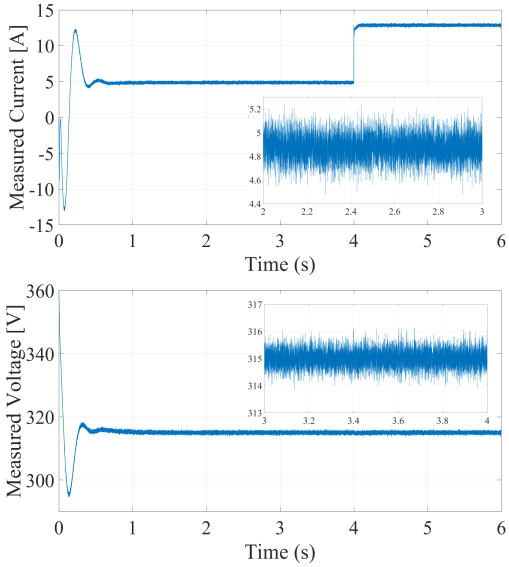

Fig. 9. Evolution of the measured voltage and measured current in the DGU 1. The voltage signal is affected by high-frequency white noise of variance 0.109. The current signal is affected by high-frequency white noise of variance 0.0114.

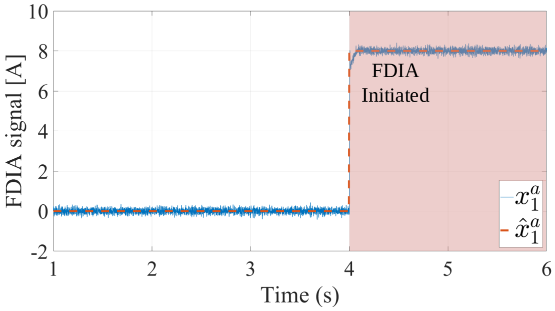

Fig. 10. Evolution of the attack reconstruction (blue) and the true attack signal (orange) in the DGU 1.

As it can be seen in Fig. 10, the presence of measurement noise does not prevent the stability of the attack signal estimation, but, naturally, the estimation converges to a bounded error around the true attack signal value. This error can be decreased by increasing the time constant of the implemented low-pass filters. However, the presence of a low-pass filter (and increasing its time constant) reduces the convergence rate of the observer which deteriorates the transient performance of the attack signal estimation. This fact can be seen by comparing the signal estimation at time $t = 4s$ in Fig. 6, where the attack estimation converges immediately to the true value, and Fig. 10, where the attack estimation requires some time to converge.

Finally, the estimated attack signal, $\hat{x}_1^a$, has been used to clean the attacked cyber-link signal. As it can be observed in Fig. 11, even in the presence of significant model uncertainty and sensor noise, the reconstruction and mitigation of the attacked signal is capable of recovering the performance of the attack-free case. In this case, as stated before, the mitigation is

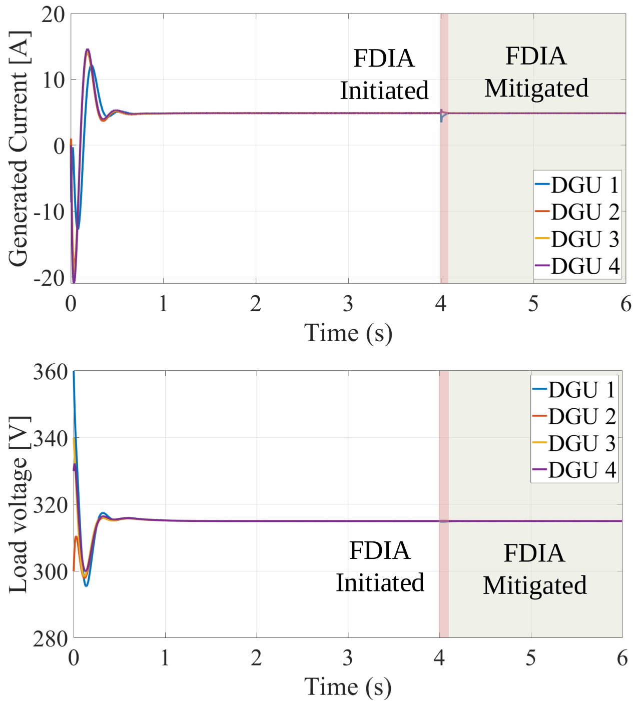

Fig. 11. Current and load voltage evolution under a FDIA in DGU 1 and observer reconstruction and mitigation. At $t = 4s$ there is a FDIA in the DGU 1 cyber-links.

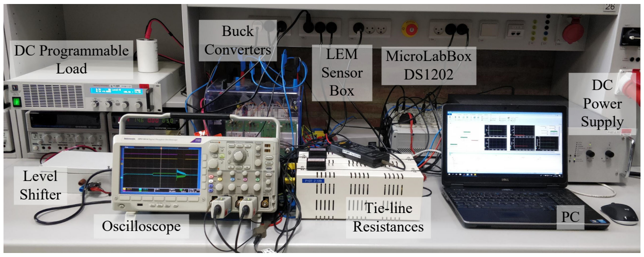

Fig. 12. Experimental setup of a cooperative DC microgrid comprising of 2 agents controlled by dSPACE MicroLabBox DS1202 supplying power to the programmable CPL.

not immediate, due to the presence of low-pass filters, which induces some delay in the attack estimation.

V. Experimental Validation

The proposed detection and reconstruction strategy has been validated in an experimental prototype of DC microgrid operating at a voltage reference $V_{dc_{ref}}$ of 48 V with 2 buck converters rated equally for 600 W, as shown in Fig. 12. Both converters are tied radially to a programmable CPL via tie-line resistances. Each converter is controlled by dSPACE MicroLabBox DS1202 (target), with control commands from the dSPACE ControlDesk from the PC (host). The controller gains are consistent for each converter. The details of the controller are presented in [30]. Using the local and neighbouring measurements, the proposed observer is modelled for every converter (as shown in Fig. 13) to mitigate false data injection attacks and meet the desired control objectives of average voltage stability and equal current sharing in DC microgrids. The experimental testbed parameters are provided in Table IV.

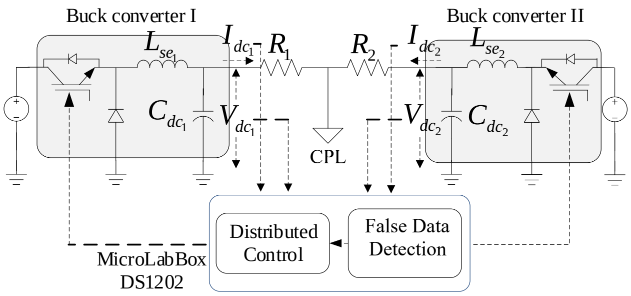

Fig. 13. Single line diagram of the experimental setup shown in Fig. 12.

TABLE IV
Experimental Testbed Parameters

Symbol	True Value
Plant	
L_{se_i}	$3\ [mH]$
C_{dc_i}	$100\ [\mu F]$
R_1	$0.8\ [\Omega]$
R_2	$1.4\ [\Omega]$
Controller	
$V_{dc_{ref}}$	$48\ [V]$
$K_P^{H_1}$	$1.92\ [-]$
$K_I^{H_1}$	$15\ [-]$
$K_P^{H_2}$	$4.5\ [-]$
$K_I^{H_2}$	$0.08\ [-]$
g	$0.64\ [-]$

The proposed reconstruction approach has been validated in three different scenarios. In the first case study in Fig. 14(a), a simultaneous cyber-attack is conducted on current measurements from both converters with the false data, given by x_1^a = 1.5 A and x_2^a = 1 A. The proposed non-linear observer has been implemented in each agent to reconstruct and mitigate the effect of the cyber-attacks. As it can be observed, after the simultaneous cyber-attack, the system restores back to the pre-attack set points. This validates the scalability of the proposed observer strategy in providing resiliency against false data injection attacks in the presence of realistic sensor noise and model uncertainty.

The proposed approach assumed that the unknown local power load is constant. This is a reasonable assumption, however, in practice, the load may vary from one constant set-point to another in order to accommodate the microgrid to demand shifts. Some adaptive observer schemes, may present problems under set-point changes, specially, when the restrictive persistence of excitation [37] condition is not satisfied. For this reason, it is of interest to test the adaptability of the proposed reconstruction scheme under local power load shifts. In the first case study in Fig. 14(a), after the introduction of the cyber-attack, the CPL of both agents has been increased. As it can be observed, this fact modifies the current set-point of both agents, but, it does not prevent the current consensus (equal current sharing) that would induce the FDIA introduced to the system. This result shows that the proposed reconstruction scheme does not cause any additional problems under dynamic load change, which is coherent with the results presented in this work. Under a local load change the constant power load assumption does not hold, i.e. $\dot{P}_i \neq 0$. This fact induces a factor $\frac{\partial \phi_i(\boldsymbol{\xi}_i, u_i, P_i, \boldsymbol{\eta}_i)}{\partial P_i}\dot{P}_i$ in the last equation of (24). This factor is not modelled, but is upper bounded. Therefore, the factor $\dot{\sigma}$ is also upper bounded and Theorem III.1 still holds true. Therefore, the proposed observer scheme presents robust stability to dynamic load changes. It should be remarked that when $\dot{P}_i \neq 0$, expression (34) reduces to

$$\hat{P}_i = P_i + \frac{\dot{P}_i}{\xi_{1,i}}. \tag{39}$$

Thus, it introduces a bias in the load estimation. Nonetheless, this bias disappears when the local power load converges to the desired set-point, and an unbiased attack reconstruction is achieved.

In the second case study in Fig. 14(b), a cyber-attack is conducted on agent I with a false data injection, given by x_1^a = 1.8 A. The aim of this second experiment is to test the resilience of the observer scheme under varying communication delay. Specifically, it has been tested the applicability of the strategy under a maximum communication delay of 250 ms. Even though the consensusability between agents is limited to large communication delay, it can be seen that when a cyber-attack is conducted under conditions which may lead to diverging control inputs, the proposed observer strategy still recovers pre-attack performance and is resilient against cyber-attacks in the presence of other cyber disturbances and load changes.

In the third case study in Fig. 14(c), two time-varying cyber-attacks are conducted on DGU II. The first is modelled as a sinusoidal function $I_2^a = 1.4(sin(0.4\pi t))\ A$; and the second one as a ramp function $I_2^a = 1.2t\ A$. Amid attacks, a decrease of the unknown CPL has been introduced. It can be observed in Fig. 14 (c) that the mitigation strategy is capable of recovering pre-attack performances in both events, which validates the capabilities of the algorithm to mitigate attacks of time-varying nature.

VI. Conclusions

This work has presented a non-linear observer-based detection and mitigation strategy for a false data attack in cooperative DC microgrids with unknown CPLs. The proposed approach is completely distributed, which eases its scalability to large scale microgrids, and operates adequately under an arbitrary number of compromised agents. Finally, through numerical and experimental testing, the observer approach has been shown to be robust to model uncertainty and/or communication delay; and present adequate performance under significant sensor and communication noise.

Nonetheless, the proposed strategy presents some limitations that should be addressed in future works. The estimation of the power line currents relies on an open-loop integration that is not tunable. Although the estimation is in general fast, this fact limits the convergence rate of the current estimation (14) and, as a consequence, of the attack estimation.

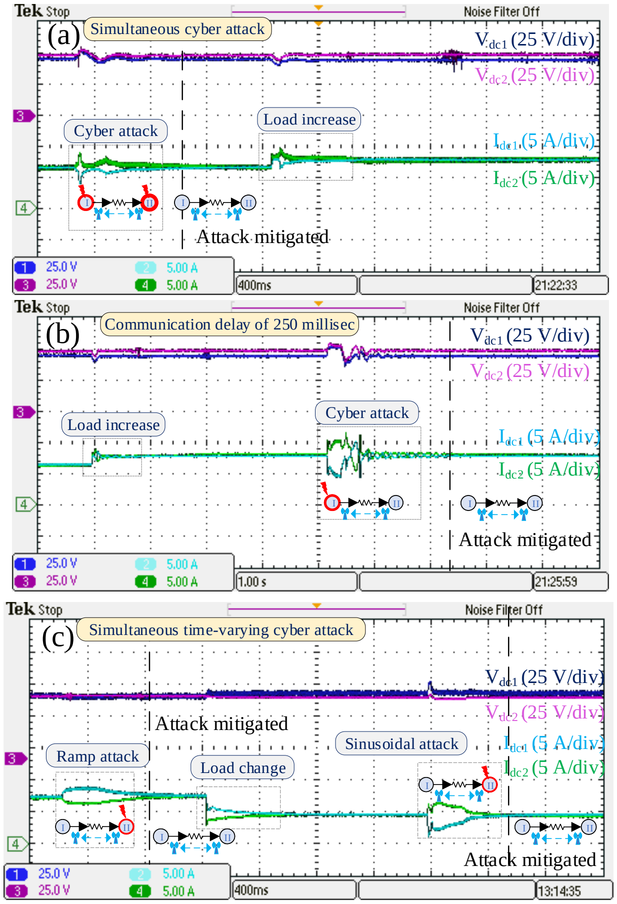

Fig. 14. Experimental validation of the proposed controller under: (a) Simultaneous cyber-attack on both agents and unknown CPL increase.The attack has been mitigated in 400 ms. (b) cyber-attack on one agent under a communication delay of 250 ms and unknown CPL increase. The attack has been mitigated in 2 s. (c) Ramp and sinusoidal attack element on agent II and unknown CPL decrease. First attack has been mitigated in 640 ms and second attack mitigated in 560 ms.

References

[1] A. Ipakchi and F. Albuyeh, "Grid of the future," *IEEE Power and Energy Magazine*, vol. 7, no. 2, pp. 52–62, Mar. 2009.

[2] A. Cecilia and R. Costa-Castelló, "High gain observer with dynamic deadzone to estimate liquid water saturation in pem fuel cells," *Rev. Iberoam. Autom. In.*, vol. 17, no. 2, Apr. 2020.

[3] A. Cecilia, J. Carroquino, V. Roda, R. Costa-Castelló, and F. Barreras, "Optimal energy management in a standalone microgrid, with photovoltaic generation, short-term storage, and hydrogen production," *Energies*, vol. 13, no. 6, p. 1454, Mar. 2020.

[4] T. Dragičević, X. Lu, J. C. Vasquez, and J. M. Guerrero, "Dc microgrids—part I: A review of control strategies and stabilization techniques," *IEEE Trans. Power Electron.*, vol. 31, no. 7, pp. 4876–4891, Jul. 2016.

[5] V. Nasirian, S. Moayedi, A. Davoudi, and F. L. Lewis, "Distributed cooperative control of dc microgrids," *IEEE Trans. Power Electron.*, vol. 30, no. 4, pp. 2288–2303, Apr. 2015.

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

[7] M. Yazdanian and A. Mehrizi-Sani, "Distributed control techniques in microgrids," *IEEE Trans. Smart Grid*, vol. 5, no. 6, pp. 2901–2909, Nov. 2014.

[8] H. Sandberg, S. Amin, and K. H. Johansson, "Cyberphysical security in networked control systems: An introduction to the issue," *IEEE Control Syst. Mag.*, vol. 35, no. 1, pp. 20–23, Feb. 2015.

[9] R. Deng, P. Zhuang, and H. Liang, “False data injection attacks against state estimation in power distribution systems,” *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 2871–2881, Jun. 2019.

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

[11] F. Pasqualetti, F. Dörfler, and F. Bullo, “Attack detection and identification in cyber-physical systems,” *IEEE Trans. Autom. Control*, vol. 58, no. 11, pp. 2715–2729, Nov. 2013.

[12] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, “A review of false data injection attacks against modern power systems,” *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1630–1638, Mar. 2017.

[13] L. Liu, M. Esmalifalak, Q. Ding, V. A. Emesih, and Z. Han, “Detecting false data injection attacks on power grid by sparse optimization,” *IEEE Trans. Smart Grid*, vol. 5, no. 2, pp. 612–621, Mar. 2014.

[14] G. Chaojun, P. Jirutitijaroen, and M. Motani, “Detecting false data injection attacks in ac state estimation,” *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2476–2483, Sept. 2015.

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

[16] J. Zhao, G. Zhang, M. La Scala, Z. Y. Dong, C. Chen, and J. Wang, “Short-term state forecasting-aided method for detection of smart grid general false data injection attacks,” *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1580–1590, Jul. 2017.

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

[18] H. Nishino and H. Ishii, “Distributed detection of cyber attacks and faults for power systems,” *IFAC Proc. Vol.*, vol. 47, no. 3, pp. 11 932 – 11 937, Aug. 2014.

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

[20] S. Sahoo, T. Dragičević, and F. Blaabjerg, “An event-driven resilient control strategy for dc microgrids,” *IEEE Trans. Power Electron.*, vol. 35, no. 12, pp. 13 714–13 724, May 2020.

[21] ——, “Multilayer resilience paradigm against cyber attacks in dc microgrids,” *IEEE Trans. Power Electron.*, vol. 36, no. 3, pp. 2522–2532, Mar. 2021.

[22] ——, “Resilient operation of heterogeneous sources in cooperative dc microgrids,” *IEEE Trans. Power Electron.*, vol. 35, no. 12, pp. 12 601–12 605, Apr. 2020.

[23] F. Pasqualetti, A. Bicchi, and F. Bullo, “Consensus computation in unreliable networks: A system theoretic approach,” *IEEE Trans. Autom. Control*, vol. 57, no. 1, pp. 90–104, Jan. 2012.

[24] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, “Distributed fault detection and isolation resilient to network model uncertainties,” *IEEE Trans. Cybern.*, vol. 44, no. 11, pp. 2024–2037, Nov. 2014.

[25] S. Riverso, F. Boem, G. Ferrari-Trecate, and T. Parisini, “Plug-and-play fault detection and control-reconfiguration for a class of nonlinear large-scale constrained systems,” *IEEE Trans. Autom. Control*, vol. 61, no. 12, pp. 3963–3978, Dec. 2016.

[26] F. Boem, R. M. G. Ferrari, C. Keliris, T. Parisini, and M. M. Polycarpou, “A distributed networked approach for fault detection of large-scale systems,” *IEEE Trans. Autom. Control*, vol. 62, no. 1, pp. 18–33, Jan. 2017.

[27] C. A. Soriano-Rangel, W. He, F. Mancilla-David, and R. Ortega, “Voltage regulation in buck-boost converters feeding an unknown constant power load: An adaptive passivity-based control,” *IEEE Trans. Control. Syst. Technol.*, pp. 1–8, Jan. 2020.

[28] S. Trip, M. Cucuzzella, X. Cheng, and J. Scherpen, “Distributed averaging control for voltage regulation and current sharing in dc microgrids,” *IEEE Contr. Syst. Lett.*, vol. 3, no. 1, pp. 174–179, Jan. 2018.

[29] N. L. Diaz, T. Dragičević, J. C. Vasquez, and J. M. Guerrero, “Intelligent distributed generation and storage units for dc microgrids—a new concept on cooperative control without communications beyond droop control,” *IEEE Trans. Smart Grid*, vol. 5, no. 5, pp. 2476–2485, Sept. 2014.

[30] 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. Ind. Electron.*, vol. 67, no. 8, pp. 6562–6571, Aug. 2020.

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

[32] A. Levant, “Higher-order sliding modes, differentiation and output-feedback control,” *Int. J. Control*, vol. 76, no. 9-10, pp. 924–941, Nov. 2003.

[33] A. Isidori, “The zero dynamics of a nonlinear system: From the origin to the latest progresses of a long successful story,” *Eur. J. Control*, vol. 19, no. 5, pp. 369 – 378, Sep. 2013.

[34] L. B. Freidovich and H. K. Khalil, “Performance recovery of feedback-linearization-based designs,” *IEEE Trans. Autom. Control*, vol. 53, no. 10, pp. 2324–2334, Nov. 2008.

[35] E. Cruz-Zavala and J. A. Moreno, “Levant’s arbitrary-order exact differentiator: A lyapunov approach,” *IEEE Trans. Autom. Control*, vol. 64, no. 7, pp. 3034–3039, Oct. 2018.

[36] O. Stamnes, O. M. Aamo, and G. Kaasa, “Adaptive redesign of nonlinear observers,” *IEEE Trans. Autom. Control*, vol. 56, no. 5, pp. 1152–1157, May 2011.

[37] A. Padoan, G. Scarciotti, and A. Astolfi, “A geometric characterization of the persistence of excitation condition for the solutions of autonomous systems,” *IEEE Trans. Autom. Control*, vol. 62, no. 11, pp. 5666–5677, Apr. 2017.

[38] B. Severino and K. Strunz, “Enhancing transient stability of dc microgrid by enlarging the region of attraction through nonlinear polynomial droop control,” *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 66, no. 11, pp. 4388–4401, Nov. 2019.