Resilient Control of DC Microgrids Against Cyber Attacks: A Functional Observer Based Approach

Mohit Kachhwaha, *Student Member, IEEE*, Himani Modi, *Student Member, IEEE*, Mahesh Kumar Nehra, and Deepak Fulwani, *Member, IEEE*

***Abstract*—Direct current microgrids (DCMGs) are swiftly moving toward the realm of communication-dependent distributed cooperative control strategies. The incorporation of cyber layer for robustness, scalability, and reliability makes the system vulnerable toward cyber-attacks. The extent of damage caused by these attacks on DCMG is substantial, to the point where ceasing the operation may become necessary. This article proposes a resilient strategy for the detection and mitigation of the most prominent false data injection attacks (FDIAs) on actuators of nodes of DCMG. An accurate error-free detection is guaranteed using a state machine-based model that makes use of a dynamic signature function that monitors the actuator signal and its estimated value. Linear functional observer (LFO) based mitigation scheme is proposed, in which the affected node is switched to LFO upon a true attack detection. The proposed technique is consistent during transients. Experimentation and simulation studies are carried out for various practical situations for a four-node DCMG to validate the proposed theory.**

***Index Terms*—Cyber physical systems, cyber attacks, direct current microgrid (DCMG), distributed control, linear functional observer (LFO).**

I. Introduction

DISTRIBUTED DCMGs offer various advantages over centralized DCMGs, such as resiliency against single point of failure, low bandwidth requirement, robustness, scalability, etc. [1]. In distributed DCMG, each node communicates information to its neighboring nodes in a sparse manner making overall traffic low and the control units less burdened. In DCMG, the key objectives are to attain proportional load/current sharing, voltage regulation and energy balancing using primary, secondary, and/or tertiary control layers [1], [2].

Layers in the upper hierarchy of DCMG require a communication network to establish coordination among various agents. The merits offered by a communication network in DCMG come at the cost of its vulnerability to cyber attacks. By examining events reported in the recent past, we can gain insight into the potential damage that can be caused to the physical structure of the DCMG in an event of a cyber threat [3]. Any such occurrence has the potential to expose the pregnable grid and lead to detrimental consequences. There are few incidents of cyber-based attacks reported in the past. An industrial control system was supposedly infiltrated by a malware [4], three power companies were exposed [5], and a large power utility faced a 10 h disruption [3]. Even the control of electric vehicles was overridden due to communication network vulnerability [3].

The cooperation between cyber and physical layers of DCMG has created risks of cyber threats and as mentioned they can be malevolent, so need of constructing detection and mitigation strategies has gained notable value recently [4]. The main entities that can be compromised by a potential cyber attack the integrity of data, availability of information, and confidentiality. Among various attacks FDIAs and replay attacks [5], [6] comes under data integrity attacks in which counterfeit data is injected into sensor/actuator signals. Major data availability attacks are denial of service attacks in which partial data is made missing [7]. This manuscript targets FDIAs, that are considered to be the most pivotal attacks [8].

The research into FDIA detection in microgrids is an emerging field and with new possibilities of attacks, the existing categorization is also evolving but it can be classified into signal-based, data-based, and model-based detection approaches. In signal-based technique [9], any deviation or anomaly from the nominal values is considered as a detection phenomenon. This does not examine the relationship between the control signal and the measurement. Data-based detection includes advanced algorithm-based strategies using deep learning [10], and neural networks [11]. Despite being advanced techniques, limited predecided attack scenarios can be detected and they require substantial computational resources and extensive training data. Model-based techniques utilize mathematical model of system. Observer models are generally used to detect attacks such as unknown input observers [12], [13], generalized state extended observers [14] and sliding mode observers [15]. They possess properties like simple implementation, detection of diverse attacks etc. but are very sensitive to measurement noise and

Manuscript received 31 May 2023; revised 12 August 2023 and 11 October 2023; accepted 14 October 2023. Date of publication 23 October 2023; date of current version 6 December 2023. This work was supported by the Ministry of Electronics and Information Technology, India, under the project "Centre for Advanced Security Technology Development in Cyber-Physical Systems." Recommended for publication by Associate Editor A. Davoudi. *(Corresponding author: Deepak Fulwani.)*

The authors are with the Electrical Engineering, Indian Institute of Technology Jodhpur, Jodhpur 342030, India (e-mail: kachhwaha.1@iitj.ac.in; modi.1@iitj.ac.in; nehra.4@iitj.ac.in; df@iitj.ac.in).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TPEL.2023.3326308.

Digital Object Identifier 10.1109/TPEL.2023.3326308

model uncertainty. Cecilia et al. [16] utilized a distributed nonlinear adaptive observer to detect attacks in the presence of nonlinear constant power loads. A Kalman filter is used as an estimator, whereas χ^2 or Euclidean distance as a detector in [17], which is robust but requires a precise model and is complicated to design. Event-driven approach is considered in [18], for FDIAs. For a more comprehensive research on observer-based techniques and FDIA detection strategies, readers are referred to [19] and [20], respectively and the references there within.

Most of these aforementioned research works threw light on sensor or communication link attacks. Actuator attacks are slightly touched upon in the literature [19], [21]. In this article, we present FDI attacks on actuators. The microcontroller architecture is vulnerable to cyber attacks and an intruder may gain access to modify the actuator signal [9], [22]. A detection plus mitigation scheme is presented that utilizes linear functional observer (LFO) for actuator input estimation. An LFO can estimate specific states or a linear combination of system states [23], [24]. The LFO can also provide an estimate of the feedback control signal if it is represented as a linear combination of states. Estimation of a few states or their combination is helpful when some of the states are not measurable [25]. Estimation aids in the proper implementation of control law in such cases. LFO is the minimum order observer, thus offering a simple structure and reduced computational power.

In this work, the detection is carried out using a dynamic signature function. This function responds to the discrepancy between actual and LFO estimated control input. This function accumulates the deviations of actual actuator input from its approximated value. In an event of an attack, there is a contrast between actual and reconstructed signals, which raises the signature value to its threshold. The signature is enquired in a way that avoids any false detections and the controller of the attacked node is switched to its corresponding LFO. This whole process is done using a state machine-based model, which allows switching among different states depending upon various conditions [26]. This way detection, using a dynamic function, followed by mitigation, using an LFO, is carried out. Thus, proposed strategy is resilient i.e., DCMG functions normally during attacks and is able to cope with transients.

The key contributions of this article are as follows.

1) The proposed technique provides an effective state machine-based modeling of dynamic signature function based detection scheme.
2) The proposed LFO is computationally efficient as it uses a reduced order structure.
3) The proposed technique reduces the occurrence of false alarms due to system transients and other variations.

The rest of this article is organized as follows. Section II consists of cyber & physical layers of DCMG, control layer, system model, and FDIA model. A brief discussion on LFO and its structure for a DCMG is presented in Section III. Proposed attack detection and mitigation scheme are described in Section IV. The simulation and experimental studies are discussed in Sections V and VI, respectively. Finaaly, Section VII concludes this article.

II. System Description and Modeling

A. Cyber Layer

The mapping of a cyber network of a physical microgrid is a ring, as shown in Fig. 1. In this DCMG, each node comprises a boost converter. The communication links between converters are denoted as edges. This cyber connection lays the groundwork for a cooperative control paradigm, where neighbors' interaction can lead to global consensus. The cooperative control works on each node's local data and neighbors' data, for this communication pattern, a properly directed graph is required. In directed graph, nodes denoted as $V_G = \{v_1, v_2, \ldots, v_n\}$ are connected through edges $E_G \in V_G \times V_G$. It is associated with the adjacency matrix $A_G = [a_{ij}] \in \mathbb{R}^{N\times N}$, where N is the number of nodes [27]. The adjacency matrix contains communication weights. If information transfers from node j to node i then $a_{ij} > 0$ otherwise $a_{ij} = 0$. Here, the adjacency matrix is $A_G = [0\,1\,0\,1;\ 1\,0\,1\,0;\ 0\,1\,0\,1;\ 1\,0\,1\,0]$. The stability of communication topology is represented by the eigenvalue of the Laplacian matrix. The Laplacian matrix is defined as $\mathcal{L} = D_G^{\text{in}} - A_G$, which is a square matrix of $N \times N$ [18] where, in-degree matrix $D_G^{\text{in}} = \text{diag}\{d_i^{\text{in}}\}$ is a diagonal matrix with $d_i^{\text{in}} = \Sigma_{j\in N_i} = a_{ij}$.

B. Control Layer

1) Primary Control: The overall control structure is shown in Fig. 2. The primary dual-loop PI control configuration comprises a faster inner current control loop (having higher bandwidth) and a relatively slower outer voltage control loop (having lower bandwidth). The control signal obtained is compared with a high-frequency f_{sw} sawtooth carrier wave to generate pulsewidth modulated (PWM) signals. The inductor current can adapt more swiftly than the output voltage [28]. The stability of controller is omitted because of space constraints. The reference provided to the voltage controller which is to be compared with individual output voltage is given as

$$V_i^* = V_{\text{ref},i} - R_{di}x_{1,i} + \Delta V_i \tag{1}$$

where $V_{\text{ref},i}$, R_{di}, $x_{1,i}$, and ΔV_i are the global reference, droop resistance, inductor current, and secondary voltage correction term, respectively, for the ith converter.

2) Secondary Control: The secondary controller maintains voltage regulation and proportional current sharing using information from neighbors. The current controller, at ith node, compares the local per-unit current $i_i^{\text{pu}} = \frac{i_i}{i_i^{\text{base}}}$ with a weighted average of the neighbors' per-unit currents to find the mismatch term ΔI_i [29]. The current mismatch term ΔI_i is fed to a PI controller $H_i(s)$, which calculates the correction term for each converter ΔV_i [27].

$$\Delta I_i = \sum_{j\in N_i} \mu_i a_{ij} \left(i_j^{\text{pu}} - i_i^{\text{pu}}\right) \tag{2}$$

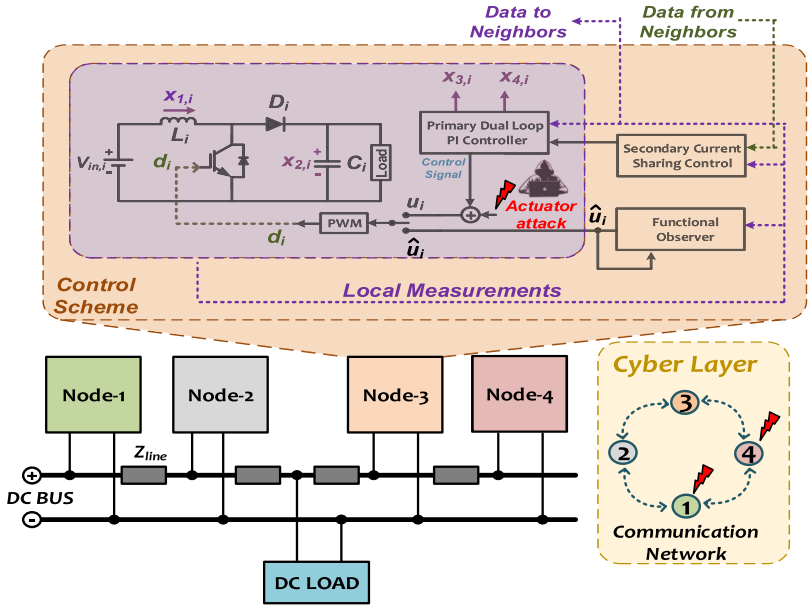

Fig. 1. Overall architecture of cyber-physical DCMG.

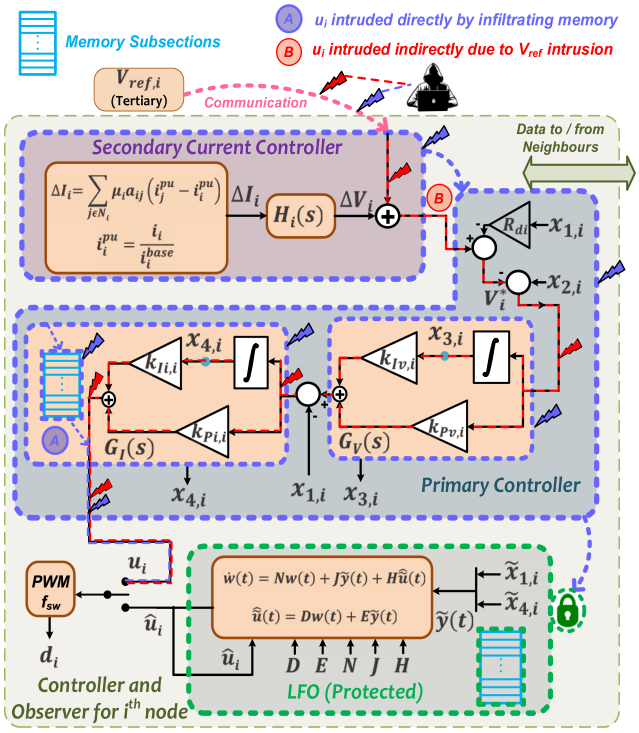

Fig. 2. Controllers and observer structure.

$$\Delta V_i = H_i(s)\Delta I_i = \left(k_{\mathrm{PH},i} + \frac{k_{\mathrm{IH},i}}{s}\right)\Delta I_i \tag{3}$$

where μ_i is the coupling gain, and $k_{\mathrm{PH},i}, k_{\mathrm{IH,i}}$ are PI gains of secondary current sharing controller. The ΔI_i term reacts to match the per-unit currents of neighboring converters and hence an overall proportional sharing is achieved.

C. Physical Layer and Modeling

The physical model of DCMG is comprised of four nodes as shown in Fig. 1. Each node consists of a dc source supplying dc loads via an interfacing boost converter. The mathematical model of ith node can be formulated as

$$L_i\dot{x}_{1,i} = V_{\mathrm{in},i} - (1-u_i)x_{2,i} \tag{4a}$$

$$\bar{C}_i\dot{x}_{2,i} = (1-u_i)x_{1,i} - x_{2,i}/R_i \tag{4b}$$

$$\dot{x}_{3,i} = V_{\mathrm{ref},i} - x_{2,i}, \tag{4c}$$

$$\dot{x}_{4,i} = -x_{1,i} + k_{Pv,i}(V_{\mathrm{ref},i} - x_{2,i}) + k_{Iv,i}x_{3,i} \tag{4d}$$

where $V_{\mathrm{in},i}$ is the source voltage, $x_{1,i}$ and $x_{2,i}$ are the inductor current and capacitor voltage, respectively, u_i is the duty cycle, L_i, $\bar{C}_i$, and R_i are the inductance, capacitance, and load of the ith node, respectively. The other two states $x_{3,i}$ and $x_{4,i}$ can be termed as flux state and charge state, respectively, as these are fundamentally integrals of voltage and current, respectively, as shown in Fig. 2. The control structure is dynamic in nature therefore it contributes to these additional states. With this control structure, the control variable is represented as a linear combination of state variables, as presented in (7). This updation is added in the control layer of each node, which later assists in designing the LFO. The proportional and integral gains of the voltage and current PI controllers are $k_{Pv,i}, k_{Iv,i}, k_{Pi,i}, k_{Ii,i}$.

Perturbations in all the states and control input are considered as $x_{1,i} = X_{1,i} + \tilde{x}_{1,i}$, $x_{2,i} = X_{2,i} + \tilde{x}_{2,i}$, $x_{3,i} = X_{3,i} + \tilde{x}_{3,i}$, $x_{4,i} = X_{4,i} + \tilde{x}_{4,i}$ and $u_i = U_i + \tilde{u}_i$. After perturbing, linearizing and separating dc and ac parts in (4), the dc values are given as, $X_i = \left[\frac{X_{2,i}}{R_i(1-U_i)} \;\; \frac{V_{in,i}}{(1-U_i)} \;\; \frac{X_{1,i}}{k_{Iv,i}} \;\; \frac{U_i}{k_{Ii,i}}\right]$ and the small-signal ac terms are given as

$$\dot{\tilde{x}}_i = A_i\tilde{x}_i + B_i\tilde{u}_i, \qquad \tilde{y}_i = C_i\tilde{x}_i \tag{5}$$

where the small-signal state vector, system, input and output matrices are $\tilde{x}_i = [\tilde{x}_{1,i}\ \tilde{x}_{2,i}\ \tilde{x}_{3,i}\ \tilde{x}_{4,i}]$, A_i, B_i and C_i as

$$A_i = \begin{bmatrix} 0 & \frac{(U_i-1)}{L_i} & 0 & 0 \\ \frac{(1-U_i)}{C_i} & \frac{-1}{R_iC_i} & 0 & 0 \\ 0 & -1 & 0 & 0 \\ -1 & -k_{Pv,i} & k_{Iv,i} & 0 \end{bmatrix}; B_i = \begin{bmatrix} \frac{X_{2,i}}{L_i} \\ \frac{-X_{1,i}}{C_i} \\ 0 \\ 0 \end{bmatrix}$$
$$C_i = [1\ 0\ 0\ 0;\ 0\ 0\ 0\ 1] \tag{6}$$

where $X_{1,i}$, $X_{2,i}$, and U_i are the inductor current, dc bus voltage, and duty cycle at the desired operating points for the ith converter. These matrices will be useful in designing LFOs in the subsequent section. Moreover

$$\tilde{u}_i = -\begin{bmatrix} k_{Pi} & k_{Pv}k_{Pi} & -k_{Iv}k_{Pi} & -k_{Ii} \end{bmatrix} \tilde{x}_i. \tag{7}$$

D. Modeling of False Data Injection Attack

The FDIA can be defined as an attack where the actuator or sensor is fed with additional or malicious data and that can potentially compromise the overall DCMG [6]. The FDIA on actuator of ith converter can be formulated as, $\bar{u}_i = u_i + \gamma_i u_{a,i}$, where $\bar{u}_i$ is the compromised actuator signal, $u_{a,i}$ is the attack signal and γ_i is a binary scalar which is 1 in presence of any attack otherwise 0. The updated model of the ith node power converter considering the attack signal will be

$$L_i\dot{x}_{1,i} = V_{\text{in},i} - (1 - u_i - u_{a,i})x_{2,i} \tag{8a}$$
$$\bar{C}_i\dot{x}_{2,i} = (1 - u_i - u_{a,i})x_{1,i} - x_{2,i}/R_i \tag{8b}$$
$$\dot{x}_{3,i} = V_{\text{ref},i} - x_{2,i} \tag{8c}$$
$$\dot{x}_{4,i} = -x_{1,i} + k_{Pv,i}(V_{\text{ref},i} - x_{2,i}) + k_{Iv,i}x_{3,i} \tag{8d}$$

The upper control layers are totally based on communication, thus vulnerable to attacks, and if primary layer is compromised then control input can also be intruded. Here, the attacks on actuators are considered not on the sensors, however, sensor attacks indirectly impact control input. The control input can get corrupted either directly in processor or indirectly due to upper layer's intrusion as shown in Fig. 2. Moreover, observer layer is assumed to be implemented in a read-only section memory using a memory protection unit, or some isolated hardware/software solution thus it is intrusion free.

III. Linear Functional Observer

The aim of an LFO is to estimate input signal. To estimate a function $\tilde{z}(t)$, which is a linear combination of system states i.e., $\tilde{z}(t) = F\tilde{x}(t)$, the observer in (10) is designed [23], [25]. The estimation of actuator input $\tilde{u}(t)$, which can be expressed as a linear combination of states as in (7), is carried out. The following structure is used for a q^{th} order observer:

$$\tilde{u}(t) = F\tilde{x}(t) = [k_{Pi}\ k_{Pv}k_{Pi}\ -k_{Iv}k_{Pi}\ -k_{Ii}]\tilde{x}(t) \tag{9}$$
$$\dot{w}(t) = Nw(t) + J\tilde{y}(t) + H\hat{\tilde{u}}(t) \tag{10a}$$
$$\hat{\tilde{u}}(t) = Dw(t) + E\tilde{y}(t) \tag{10b}$$

where gain matrix $F \in \mathbb{R}^{r\times n}$ is known, $x \in \mathbb{R}^n$ is the state vector, $w(t) \in \mathbb{R}^q$ represents the observer state, $\hat{\tilde{u}}(t) \in \mathbb{R}^r$ represents the estimation $\tilde{u}(t)$. Observer matrices $N \in \mathbb{R}^{q\times q}$, $J \in \mathbb{R}^{q\times p}$, $H \in \mathbb{R}^{q\times m}$, $D \in \mathbb{R}^{r\times q}$ and $E \in \mathbb{R}^{r\times p}$ are constructed in a way that $\hat{\tilde{u}}(t) \to \tilde{u}(t)$ as $t \to \infty$.

The model (5) is observable considering output matrix as $\tilde{y}_i = [\tilde{x}_{1,i}\ \tilde{x}_{4,i}]^T$, hence an LFO can be designed [23], [25] to estimate the actuator input of ith node power converter. All the designed matrices can be found in Section V.

The stability of an LFO can be established as follows. Similar to $\hat{\tilde{u}}(t)$, estimate of $w(t)$ should be another linear combination of $\tilde{x}_i$, say $L\tilde{x}_i$. Then, the error can be given as

$$e(t) = w(t) - L\tilde{x}(t), \quad \dot{e}(t) = \dot{w}(t) - L\dot{\tilde{x}}(t). \tag{11}$$

Using, (5) and (10) then rearranging

$$\dot{e}(t) = Ne(t) + (NL + JC - LA)\tilde{x}(t) + (H - LB)\hat{\tilde{u}}(t) \tag{12}$$

Now, clearly evident from this, the observer matrices should be designed as

$$NL + JC - LA = 0, \quad H - LB = 0 \tag{13}$$

then updated dynamics is, $\dot{e}(t) = Ne(t)$, i.e., matrix N controls the dynamics of the observer, and when we choose matrix N as Hurwitz, error dynamics will converge asymptotically

$$e(t) \to 0 \ \ as \ \ t \to \infty \tag{14}$$

Now, the error dynamics of actuator input estimation is

$$e_u(t) = \hat{\tilde{u}}(t) - F\tilde{x}(t) \tag{15a}$$
$$e_u(t) = De(t) + (DL + EC - F)\tilde{x}(t). \tag{15b}$$

Using (14) and choosing (16), $e_u(t) \to 0$ as $t \to \infty$

$$DL + EC - F = 0. \tag{16}$$

This proves the stability of LFO i.e., $e(t)$ converges to 0 which in turn makes $e_u(t)$ converge to 0 asymptotically given (13) and (16) along with matrix N designed to be Hurwitz.

IV. Proposed Attack Detection and Mitigation Technique Using LFO

The attack mitigation technique commences with a detection stage. Since the actuator input signal is being attacked, this strategy involves a dynamic signature function consisting of the actuator input signal u_i and the estimated actuator signal $\hat{u}_i$. u_i is obtained from primary and secondary controllers of the ith node whereas $\hat{u}_i$ is accessed from LFO of ith node power converter. The dynamic signature function is given by

$$\Gamma_i = \kappa_i \int_0^{T_o} (u_i - \hat{u}_i)^2\, d\tau. \tag{17}$$

The overall scheme can be understood following the state machine diagram [26] shown in Fig. 3. The detection scheme is also presented in a simpler form in Algorithm 1. The process starts with entering the state $S1$ after initializing all the variables. The control switches among $S1$, $S2$, and $S3$ states depending

Algorithm 1: Detection of an FDIA on ith Node.

1 **Input:** u_i, $\hat{u}_i$
2 **Output:** η_i which decides activation of i^{th} F.O. on an event of attack
3 Initialize $\Gamma_i := 0$, $\alpha_i := 0$, $s := 0$, $r := 0$, $\nu := 0$, $\eta_i := 0$
4 Calculate Γ_i using (17)
5 **if** ($\Gamma_i < \Gamma_{i,max}$ && $s < T_o$ && $r < T_c$) **then**
6 | **goto** *5* ;
7 **else if** ($\Gamma_i < \Gamma_{i,max}$ && $s \geq T_o$) **then**
8 | Reset Γ_i and s, ***goto*** *5* ;
9 **else if** ($\Gamma_i < \Gamma_{i,max}$ && ($r \geq T_c$ || $\nu = 1$)) **then**
10 | Reset Γ_i, α_i, ν, s and r, ***goto*** *5* ;
11 **else if** ($\Gamma_i \geq \Gamma_{i,max}$) **then**
12 | ***goto*** *14*;
13 **end** Here && is logical AND
14 **if** ($\alpha_i < \alpha_{i,max}$ && $r < T_c$) **then**
15 | Set $\alpha_i = \alpha_i + 1$, ***goto*** *21* ;
16 **else if** ($\alpha_i \geq \alpha_{i,max}$ && $r < T_c$) **then**
17 | ***goto*** *26* ;
18 **else if** ($r \geq T_c$ || $\nu = 1$) **then**
19 | Reset α_i, ν and r, ***goto*** *5*;
20 **end** Here || is logical OR
21 **if** $s \geq T_o$ **then**
22 | Reset Γ_i and s, ***goto*** *5* ;
23
24 **else if** ($r \geq T_c$ || $\nu = 1$) **then**
25 | Reset Γ_i, α_i, ν, s and r, ***goto*** *5*;
26 ***end***
27 Set $\eta_i = 1$ i.e. Switch from u_i to $\hat{u}_i$ i.e. activate i^{th} F.O.

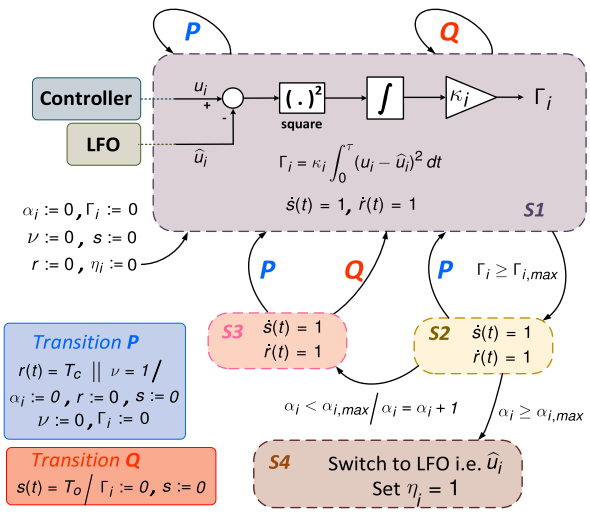

Fig. 3. State machine-based modeling of dynamic signature function based detection scheme.

upon various conditions and finally reaches state $S4$ on the occurrence of an attack.

The value of signature Γ_i is calculated dynamically in state $S1$. Γ_i resets periodically with a period of T_o using a timer function $s(t)$, κ_i is a positive constant. Under normal operating conditions, u_i and $\hat{u}_i$ are nearly the same, so Γ_i does not increase much during its one period and resets. During an attack condition on ith converter, u_i gets compromised and Γ_i reaches to a predefined threshold $\Gamma_{i,\max}$. As soon as this threshold is reached, control switches to state $S2$ (step 14 in Algorithm 1). In state $S2$, a counter α_i is programmed to count the number of times Γ_i hits the threshold value. If the counter is less than its predecided count value $\alpha_{i,\max}$, control increases α_i and switches to state $S3$ (step 21 in Algorithm 1) where it waits until Γ_i is reset by timer $s(t)$ and switches back to state $S1$ (step 5 in Algorithm 1). Here, due to presence of attack, Γ_i hits the threshold again in this period too. This way control switches back and forth among states $S1$, $S2$, and $S3$ until counter α_i counts up to $\alpha_{i,\max}$. Now, whenever the condition (i.e. $\alpha_i \geq \alpha_{i,\max}$) is met, control of the state machine switches to state $S4$ (step 26 in Algorithm 1), where a binary variable η_i is set to 1 portraying that an attack is detected and LFO is activated for the respective node, in other words, switch actuator input from u_i to $\hat{u}_i$. Further, a timer function $r(t)$, which resets with a period of T_c is used to avoid any false detection of the attack. Note that, $s(t)$ and $r(t)$ are basically clock functions having structure described in (18). In addition, manually raising value of constant ν to 1 will also reset counter α_i as described in Fig. 3 and Algorithm 1.

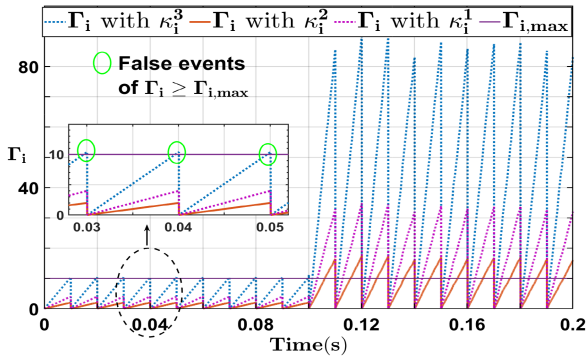

Fig. 4. Behavior of Γ_i with different κ_i.

$$\dot{s}(t) = 1, \quad \dot{r}(t) = 1. \tag{18}$$

Further, the constants κ_i, T_o, $\Gamma_{i,\max}$ and $\alpha_{i,\max}$ play different roles in attack detection. κ_i determines the rate of rise of Γ_i. With an increasing value of κ_i, threshold $\Gamma_{i,\max}$ can be attained faster but with a compromise to detect any false events. This way $\Gamma_{i,\max}$ and κ_i work in conjunction, and anyone of them can be kept fixed and the other can be adjusted according to the systems' response to attacks. T_o deals with resetting Γ_i function. With an increasing value of T_o, the detection of the threshold is delayed. Thus, it should be kept on a value where neither it delays consequent detection of $\Gamma_{i,\max}$ nor it resets Γ_i before a possible event detection. $\alpha_{i,\max}$ is the counter's threshold value, which should be kept sufficient enough that the counter gets saturated only during attacks not during transients.

To illustrate tuning of constants, refer to Figs. 4 and 5, where an attack of random value changing in the range $[-0.1, 0.1]$ is considered on ith actuator at $t = 0.1$ s. The value of the threshold is kept fixed $\Gamma_{i,\max} = 10$ for this study. It is clear from Fig. 4,

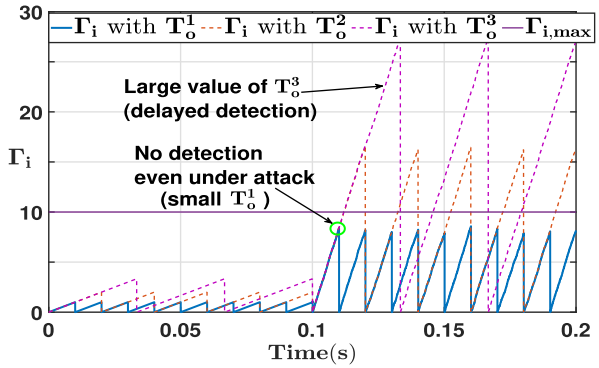

Fig. 5. Behavior of Γ_i with different T_0.

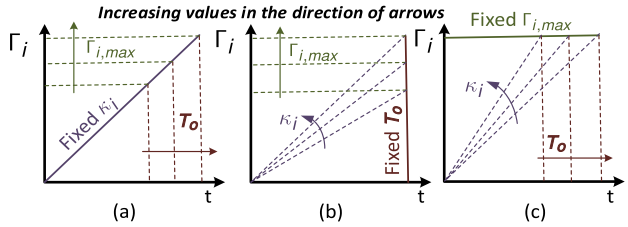

Fig. 6. Relationship among $\Gamma_{i,\max}$, κ_i and T_o.

with three different values of κ_i ($\kappa_i^1 < \kappa_i^2 < \kappa_i^3$), all three are contributing in detecting attacks but with κ_i^3, false detection is happening in absence of attack. So, this can be resolved by keeping κ_i^3 low or shifting the threshold up. Moreover, demonstration with different T_o ($T_o^1 < T_o^2 < T_o^3$) is shown in Fig. 5. T_o^1 is very small that even with an attack it resets Γ_i before it reaches the threshold $\Gamma_{i,\max}$ and T_o^3 is very large that overall detection i.e., updation of α_i will take a longer duration.

It is clear from the above discussion that choosing optimal values of constants is a crucial task. Designing κ_i and T_o such that an optimal $\Gamma_{i,\max}$ can be obtained for a given system is critically important. To deduce a relationship among $\Gamma_{i,\max}$, κ_i, and T_o, it should be known how much deviation in actuator input is permitted i.e., not considered as an attack. For a nominal value of actuator input U_i if a per unit deviation of β is allowed, then using (17), an optimal threshold can be obtained as

$$\Gamma_{i,\max} = \kappa_i \int_0^{T_o} (\beta U_i)^2 \, d\tau \;\approx \kappa_i (\beta U_i)^2 T_o. \tag{19}$$

Variations of $\Gamma_{i,\max}$, κ_i, and T_o with keeping one of them fixed can be visualized in Fig. 6. This illustration gives an insight into how a combination of constants can be chosen with one of them is constrained.

Based on the detection function (17), attacks including FDIA, replay, DoS, etc. can be detected using proposed technique. However coordinated attacks cannot be detected until they remain covert in nature i.e., system remain stable.

V. Simulation Studies

A four-node microgrid feeding dc loads is simulated in MATLAB Simulink to verify the proposed technique, as shown in Fig. 1. The microgrid primary and secondary controls are designed by taking motivation from [29]. All the relevant parameters are provided in Table I. The LFOs for individual nodes are designed, as mentioned in [23] and Section III as

TABLE I
Simulation and Experiment Parameters

Symbol	Quantity	Values
V_{in}	Input source voltage	60 V each
V_{bus}	DC bus voltage	120V
U_i	Nominal duty ratio	0.5
L_i	Boost Converter Inductance	2 mH each
$\bar{C}_i$	Boost Converter Capacitance	100 μF each
R_{Load}	Load resistance	14-20Ω
$G_V(s), G_I(s)$	Node Local voltage and current controller	$0.06 + \frac{91.4}{s}$, $0.08 + \frac{244}{s}$
$H_i(s)$	Secondary control	$1 + \frac{10}{s}$
κ_i	Detector Constant-Simulation, Experimentation	$10^6, 100$
T_o	Detector Period-Simulation, Experimentation	$0.01s, 1s$
β_i	Allowed deviation in actuator input	$0.1p.u.$
$\Gamma_{i,\max}$	Signature function threshold-Simulation, Experimentation	$25, 0.25$
$\alpha_{i,\max}$	Counter threshold-Simulation, Experimentation	$4, 5$
P	Power rating	$1kW$
f_{sw}	Switching frequency of boost Converters	$20kHz$
f_s	Sampling frequency	$100kHz$

$$A = \begin{bmatrix} 0 & -250 & 0 & 0 \\ 10638 & -443.26 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ -1 & -0.0657 & 91.4 & 0 \end{bmatrix}$$

$$B = \begin{bmatrix} 0.6000 \\ -1.0638 \\ 0 \\ 0 \end{bmatrix} * 10^5; \quad C = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$L = \begin{bmatrix} 0.0168 & 0.0054 & -6.005 & 35.6923 \end{bmatrix}$$

$$F = \begin{bmatrix} 0.0826 & 0.0054 & -6.0050 & -244 \end{bmatrix}$$

$$J = \begin{bmatrix} 31.17 & 1939 \end{bmatrix}; \quad D = \begin{bmatrix} 1 \end{bmatrix}; \quad N = \begin{bmatrix} -543.2624 \end{bmatrix}$$

$$E = \begin{bmatrix} 0.0658 & -279.6923 \end{bmatrix}; \quad H = \begin{bmatrix} 431.32 \end{bmatrix}$$

The simulation results shown are obtained for an overall loading of 1 kW. To cover a practical scenario, unequal yet proportionate loading is taken for converters $(1:2:1:2)$.

The first set of results is shown in Fig. 7 in which two out of four nodes are subjected to actuator attacks one after another. Considering the unpredictable nature of the attack, a random attack signal coming from uniformly distributed random data in the range of $[-0.35, 0.35]$, is considered. All the relevant signals are captured in this set of results. At the start, it can be seen that a steady state is reached and V_{bus}, all inductor currents and actual and estimated values of actuator input are stable. Since there is no attack, $\hat{u}_i = u_i$ for all converters. An attack on node-4 is initiated at $t = 0.1$ s, which in turn impacts V_{bus}, u_4, and various currents. It is worth noticing that fluctuations in I_4 are maximum. As a consequence of the attack, the dynamic signature function Γ_4 increases drastically and crosses threshold

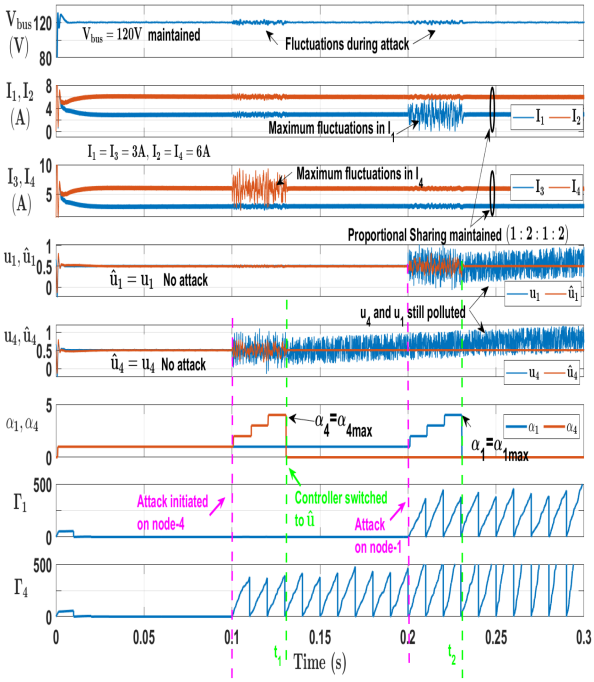

Fig. 7. Simulation study of relevant signals during attacks.

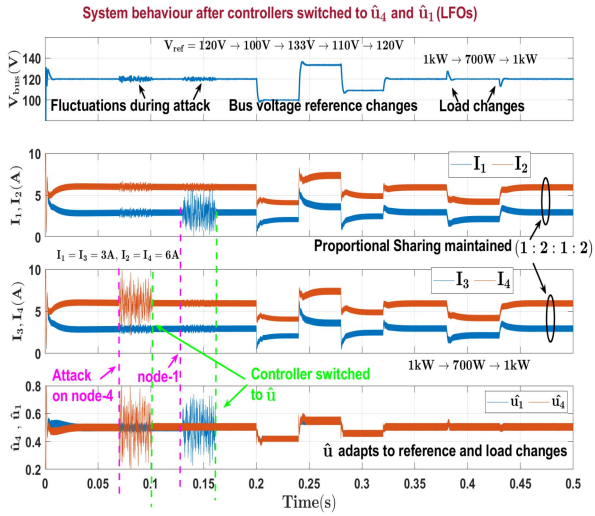

Fig. 8. Simulation study of relevant signals after attacks.

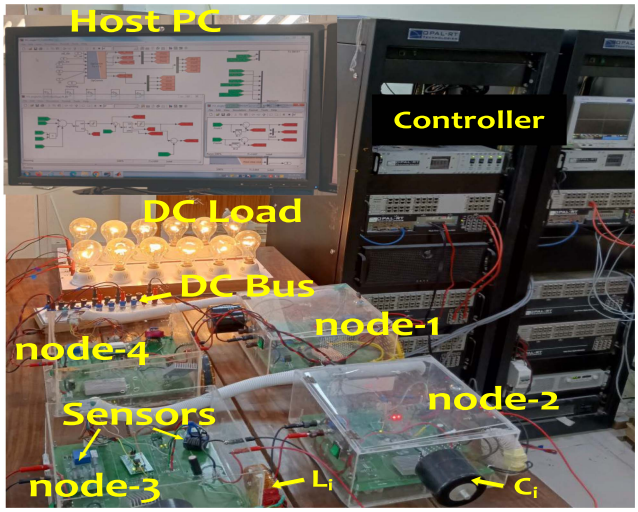

Fig. 9. Experimental setup.

$\Gamma_{4,\max}$ every subsequent period. This raises the counter α_4 to reach $\alpha_{4,\max}$, and the controller switches to LFO i.e., $\hat{u}_4$ replaces u_4 in the converter control of node-4 at time instant $t = t_1$. Once LFO is activated, all signals attain their steady-state values. At $t = 0.2\,\text{s}$, another attack is initiated on node-1 and a similar set of events occurs there also. At $t = t_2$, this attack is compensated by LFO feeding the control input $\hat{u}_1$ to converter at node-1. It is observed that the signals u_4 and u_1 are still compromised but respective LFOs take care of them. After two attacks, current sharing and bus voltage are maintained.

Further, one more set of results is captured so as to test the competence of the proposed scheme. The scheme is validated by subjecting load and bus voltage reference changes after $\hat{u}_4$ and $\hat{u}_1$ take over. It can be seen from Fig. 8 that before $t = 0.2\,\text{s}$, converters at node-4 and node-1 were attacked, respectively, one after another and their respective LFOs are activated. The system is subjected to a bus voltage reference change in a sequence of 120 V $\rightarrow$ 100 V $\rightarrow$133 V $\rightarrow$ 110 V $\rightarrow$ 120 V changed every 0.04 s. It is evidently visible that V_{bus}, $\hat{u}_4$, and $\hat{u}_1$ track these changes properly. Moreover, the system is subjected to a load change of about 30% at $t = 0.38\,\text{s}$ and $t = 0.43\,\text{s}$ in a sequence of 1 kW $\rightarrow$ 700 W $\rightarrow$ 1 kW. Clearly, load changes are also handled promisingly, and proportional current sharing is maintained during these fluctuations.

VI. Experimentation Validation

The proposed attack detection and mitigation strategy is validated through an experimental setup of 1 kW as captured in Fig. 9. This setup consists of a four-node DCMG, each node comprises of a boost converter and all converters are interfaced through a common dc Bus. A variable dc load is connected to the dc bus. The complete control algorithm consisting of communication among nodes, primary, and secondary controllers, proposed LFO-based detection and mitigation technique etc., are implemented on a high-end OPAL-Real Time Digital Simulator. Various parameters are as per Table I and LFO design parameters can be referred from Section V. The power circuit of converters is equipped with IGBTs of type FGH20N60 and power diodes of type E30ED1. Voltage sensing and current sensing are carried out using LEM-based 25-P Voltage sensors and HAL 50-S current sensors. All the converters are supplied by Keysight-make power supply. All the results are obtained for the dc microgrid, while it is functioning under primary and secondary controllers hence dc load is shared proportionally. All results are captured in the sense that all scenarios are covered. It should be noted that wherever equal sharing is mentioned all current are shared equally. However for unequal (still proportionate) sharing the loading ratio is 1 : 2 : 1 : 2 for the four nodes.

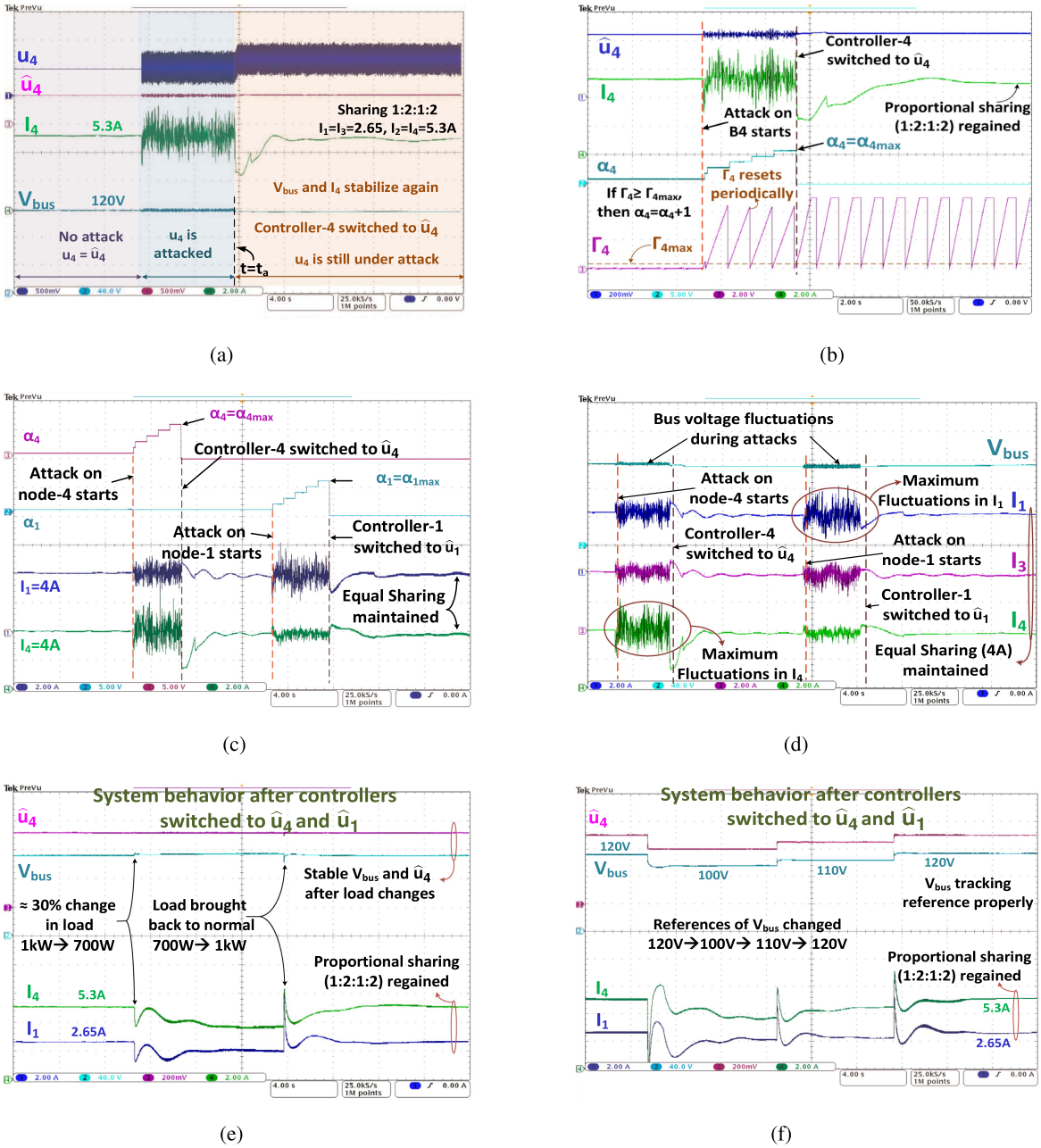

Fig. 10. Experimental validation. (a) V_{bus}, i_i, u_i and $\hat{u}_i$ during an attack. (b) Γ_i and α_i during an attack. (c) α_i and i_i during multiple attacks. (d) V_{bus} and i_i during multiple attacks. (e) Load changes with LFO activated. (f) Reference changes with LFO activated.

The proposed technique is tested for various scenarios, where one converter is attacked, two converters are attacked, for equal as well as unequal but proportionate sharing etc., and all the results are discussed. An attack similar to simulation studies is considered here also. Consider a case when converters are sharing a proportional load and u_4, $\hat{u}_4$, inductor currents and V_{bus} are at steady-state values as shown in the starting of Fig. 10(a). An attack on node-4 is initiated and it can be seen that the control input is compromised which in turn impacts bus voltage and inductor current. However, a parallel active LFO is computing an estimate of control input and that is not impacted which is clear from the figure. At $t = t_a$, the controller-4 is switched to observer i.e., instead of u_4 now $\hat{u}_4$ is going as an actuator input and it is clearly visible that while u_4 is still compromised, bus voltage, and currents are restored back to nominal values. The detection part can be understood by Fig. 10(b), where Γ_4 is continuously calculated which is the detector function. This value is based on the difference in u_4 and $\hat{u}_4$ thus it rises drastically as soon as an attack happens. Since it resets periodically, a counter α_4 counts the number of times it crosses a predefined threshold $\Gamma_{4,\max}$. As soon as the counter hits a maximum value $\alpha_{4,\max}$, the controller is switched to LFO i.e., from u_4 to $\hat{u}_4$. It is to be noted that during normal operation, the rate of rise of Γ_4 is very minute thus it resets way before it raises to $\Gamma_{4,\max}$.

A case of the attack on two of the converters back to back under equal loading is demonstrated via Fig. 10(c) and (d). Node-4 is attacked, and the proposed technique switches the controller to LFO as soon as $\alpha_4 = \alpha_{4,\max}$. As soon as the steady state is achieved, node-1 is attacked and in a similar way the counter α_1 determines the switching instant for power converter at node-1 as shown in Fig. 10(c). Fig. 10(d) elaborates the same scenario, as the bus voltage, and three of the currents (two of the attacked converters and one of the nonattacked converters) are shown. It is evidently visible that during an attack on node-4, I_4 fluctuates maximum and the same is the case with I_1 during the attack on node-1. Steady-state operation can be seen post two attacks in terms of bus voltage as well as current sharing accuracy.

A case with unequal sharing with two converters under attack is also considered to validate the system's behaviour after two controllers are switched to their respective LFOs. A study is captured to check the reliability of the system under load and bus voltage reference changes in Fig. 10(e) and (f), respectively. Both the results are captured after two of the converters (node-1 and node-4) are attacked and switched to their respective $\hat{u}$. The system is subjected to a load change of about 30% as described in Fig. 10(e). The load is changed from 1 kW to 700 W and back to 1 kW. It can be seen that the bus voltage and $\hat{u}$ are stable through these changes and also currents are regaining the proportionality. Similarly, the reference for bus voltage is changed in a 120 V $\rightarrow$ 100 V $\rightarrow$ 110 V $\rightarrow$ 120 V fashion as shown in Fig. 10(f). The bus voltage and $\hat{u}$ are tracking those changes properly. Moreover, currents are also changing and stabilizing as per their load-sharing ratios. A combination of various experimental studies is shown via proper figures. It is worth mentioning that the proposed technique is able to cope with a 50% compromised system.

VII. Conclusion

This work was proposed a LFO-based detection and mitigation strategy for potential false data injection cyber attacks on the actuators of DCMG regulated by distributed cooperative control. The technique was based on constructing an estimate of actuator input using LFO. This estimate can replace the original control input in the event of attacks. The detection of such an event was based on a dynamic signature function. Additional layers were provided to omit any untrue detection of the attack. The scheme was tested on a 4-node DCMG with up to 50% agents compromised in both equal and unequal load-sharing conditions as shown in Fig. 10(d). Moreover, once LFO takes over, it was able to cope with load and reference voltage disruptions as described in Fig. 10(e) and (f). Simulation-based studies were carried out for various possible test cases and their experimentation validation was also performed on a laboratory prototype of 1 kW.

References

[1] 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.

[2] F. Guo, L. Wang, C. Wen, D. Zhang, and Q. Xu, "Distributed voltage restoration and current sharing control in islanded DC microgrid systems without continuous communication," *IEEE Trans. Ind. Electron.*, vol. 67, no. 4, pp. 3043–3053, Apr. 2020.

[3] M. Leng, S. Sahoo, F. Blaabjerg, and M. Molinas, "Projections of cyber-attacks on stability of DC microgrids–modeling principles and solution," *IEEE Trans. Power Electron.*, vol. 37, no. 10, pp. 11774–11786, Oct. 2022.

[4] 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.

[5] 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, May 2019.

[6] P. S. Tadepalli and D. Pullaguram, "Distributed control microgrids: Cyber-attack models, impacts and remedial strategies," *IEEE Trans. Signal Inf. Process. Netw.*, vol. 8, pp. 1008–1023, 2022.

[7] P. Danzi, M. Angjelichinoski, Č. StefanoviČć, T. Dragievi, 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.

[8] D. Zhou, Q. Zhang, F. Guo, Z. Lian, J. Qi, and W. Zhou, "Distributed resilient secondary control for islanded DC microgrids considering unbounded FDI attacks," *IEEE Trans. Smart Grid*, early access, 2023, doi: 10.1109/TSG.2023.3286991.

[9] S. Tan, P. Xie, J. M. Guerrero, and J. C. Vasquez, "False data injection cyber-attacks detection for multiple DC microgrid clusters," *Appl. Energy*, vol. 310, 2022, Art. no. 118425.

[10] K. S. Suprabhath, M. V. S. Prasad, S. Madichetty, and S. Mishra, "A deep learning based cyber attack detection scheme in DC microgrid systems," *CPSS Trans. Power Electron. Appl.*, vol. 8, no. 2, pp. 119–127, Jun. 2023.

[11] A. Sargolzaei, K. Yazdani, A. Abbaspour, C. D. Crane III, and W. E. Dixon, "Detection and mitigation of false data injection attacks in networked control systems," *IEEE Trans. Ind. Informat.*, vol. 16, no. 6, pp. 4281–4292, Jun. 2020.

[12] M. Liu, C. Zhao, R. Deng, P. Cheng, and J. Chen, "False data injection attacks and the distributed countermeasure in DC microgrids," *IEEE Trans. Control Netw. Syst.*, vol. 9, no. 4, pp. 1962–1974, Dec. 2022.

[13] 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, Sep. 2020.

[14] J. Lu, X. Zhang, X. Hou, and P. Wang, "Generalized extended state observer-based distributed attack-resilient control for DC microgrids," *IEEE Trans. Sustain. Energy*, vol. 13, no. 3, pp. 1469–1480, Jul. 2022.

[15] Y. Jiang, Y. Yang, S.-C. Tan, and S. Y. Hui, "Distributed sliding mode observer-based secondary control for DC microgrids under cyber-attacks," *IEEE Trans. Emerg. Sel. Topics Circuits Syst.*, vol. 11, no. 1, pp. 144–154, Mar. 2021.

[16] A. Cecilia, S. Sahoo, T. Dragičević, R. Costa-Castelló, and F. Blaabjerg, "On addressing the security and stability issues due to false data injection attacks in DC microgrids–an adaptive observer approach," *IEEE Trans. Power Electron.*, vol. 37, no. 3, pp. 2801–2814, Mar. 2022.

[17] M. N. Kurt, Y. Yılmaz, and X. Wang, "Distributed quickest detection of cyber-attacks in smart grid," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 8, pp. 2015–2030, Aug. 2018.

[18] J. Zhang, S. Sahoo, J. C.-H. Peng, and F. Blaabjerg, "Mitigating concurrent false data injection attacks in cooperative DC microgrids," *IEEE Trans. Power Electron.*, vol. 36, no. 8, pp. 9637–9647, Aug. 2021.

[19] S. Tan, P. Xie, J. M. Guerrero, J. C. Vasquez, and R. Han, "Cyberattack detection for converter-based distributed DC microgrids: Observer-based approaches," *IEEE Ind. Electron. Mag.*, vol. 16, no. 3, pp. 67–77, Sep. 2022.

[20] 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, Jul. 2017.

[21] H. Zeng, Y. Zhao, T. Wang, and J. Zhang, "Defense strategy against false data injection attacks in ship DC microgrids," *J. Mar. Sci. Eng.*, vol. 10, no. 12, 2022.

[22] C. Wu, X. Li, W. Pan, J. Liu, and L. Wu, "Zero-sum game-based optimal secure control under actuator attacks," *IEEE Trans. Autom. Control*, vol. 66, no. 8, pp. 3773–3780, Aug. 2021.

[23] H. Trinh and T. Fernando, *Functional Observers for Dynamical Systems, Ser. Lecture Notes in Control and Information Sciences*. Berlin, Germany: Springer, 2012.

[24] T. H. Zhang J, "Design of reduced-order scalar functional observers," *Int. J. Innov. Comput. Inf. Control*, vol. 1, no. 4, pp. 791–799, 2005.
[25] D. Luenberger, "An introduction to observers," *IEEE Trans. Autom. Control*, vol. 16, no. 6, pp. 596–602, Dec. 1971.
[26] R. Alur and D. L. Dill, "A theory of timed automata," *Theor. Comput. Sci.*, vol. 126, no. 2, pp. 183–235, 1994.
[27] 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.
[28] R. Erickson and D. Maksimović, *Fundamentals of Power Electronics*, 3rd ed., Cham: Springer, Jul. 2020.
[29] X. Lu, J. M. Guerrero, K. Sun, and J. C. Vasquez, "An improved droop control method for DC microgrids based on low bandwidth communication with DC bus voltage restoration and enhanced current sharing accuracy," *IEEE Trans. Power Electron.*, vol. 29, no. 4, pp. 1800–1812, Apr. 2014.

Mohit Kachhwaha (Student Member, IEEE) received the B.Tech. degree in electrical engineering from Rajasthan Technical University (RTU), Rajasthan, India, in 2014 and the M.Tech. degree in electrical engineering from the Indian Institute of Technology Jodhpur, India, in 2017, where he is currently working toward the Ph.D. degree in microgrid control.

His current research interests include dc–dc converters, control systems, microgrids and cyber-physical systems.

Mr. Kachhwaha was a recipient of the Gold Medal for securing first position in B.Tech. in the sixth convocation of RTU.

Himani Modi (Student Member, IEEE) received the B.E. degree in electrical engineering from Gujarat Technological University (GTU), Gujarat, India, in 2016, and the M.Tech. degree in electrical engineering from IITRAM University, Gujarat, India, in 2018. She is currently working toward the Ph.D. degree in microgrid control from the Electrical Department, Indian Institute of Technology Jodhpur, India.

Her research interests include dc microgrids, multiagent systems, control systems, and cooperative control.

Mahesh Kumar Nehra received the M.Tech. degree in dynamics and control from the aerospace from the Indian Institute of Technology, Bombay, Mumbai, India, in 2017. He is currently working toward the Ph.D. degree in control systems with the Indian Institute of Technology Jodhpur, India.

He is currently with Aircraft Upgrade Research and Design Centre, Hindustan Aeronautics Limited, Nasik, India. He has 15 years of experience in Communication, Electronic Warfare, Flight control, and Navigation systems of the aircraft. His research interests include the Security of cyber-physical systems using control theory, optimal control, and robust control.

Deepak Fulwani (Member, IEEE) received the Ph.D. degree in control system from IIT Bombay, Mumbai, India, in 2009.

He was an Assistant Professor with IIT Guwahati, Guwahati, India, for one year before joining IIT Jodhpur. He also worked with IIT Kharagpur as a Visiting Faculty with the Department of Electrical Engineering. He is currently a Professor with the Department of Electrical Engineering, IIT Jodhpur. He has authored or coauthored several articles in reputed international journals and conferences. His current research interests are power electronics, microgrid, and control systems.

Dr. Fulwani was a Guest Associate Editor for a Special Issue on Structured DC Microgrid for the IEEE JOURNAL OF EMERGING AND SELECTED TOPICS IN POWER ELECTRONICS in 2017. He was an Associate Editor for IEEE TRANSACTIONS ON INDUSTRY APPLICATIONS from 2019–2022. Presently he is an editorial board member of Nature Scientific Reports. He was the recipient for Excellence in Ph.D. thesis work in IDP in systems and Control in the 48th Convocation of IIT Bombay.