energies

MDPI

Article

Distributed Mitigation Layers for Voltages and Currents Cyber-Attacks on DC Microgrids Interfacing Converters

Ahmed H. EL-Ebiary [1], Mohamed Mokhtar [1], Atef M. Mansour [2], Fathy H. Awad [2], Mostafa I. Marei [1,*] and Mahmoud A. Attia [1]

[1] Department of Electrical Power & Machines, Faculty of Engineering, Ain Shams University, Cairo 11517, Egypt
[2] Power Electronics and Energy Conversion Department, Electronics Research Institute, Cairo 12622, Egypt
* Correspondence: mostafa_ibrahim@eng.asu.edu.eg

Abstract: The wide use of communication layers in DC microgrids to transmit voltage and current measurements of each distributed generator unit (DGU) increases the possibility of exposure to cyber-attacks. Cyber-attackers can manipulate the measured data to distort the control system of microgrids, which may lead to a shutdown. This paper proposes distributed mitigation layers for the false data injection attacks (FDIA) on voltages and currents of DGUs in meshed DC microgrids. The proposed control strategy is based on integrating two layers for cyber-attack detection and mitigation to immune the primary and the secondary control loops of each DGU. The first layer is assigned to mitigate FDIAs on the voltage measurements needed for the voltage regulation task of the primary control loop. The second layer is devoted to the mitigation of FDIAs on the DGU current measurements, which are crucial for the secondary control level to guarantee the proper current sharing of each DGU. Artificial neural networks (ANNs) are employed to support these layers by estimating the authenticated measurements. Different simulation and experimental case studies are provided to demonstrate the proposed mitigation layers' effectiveness in detecting and mitigating cyber-attacks on voltage and current measurements. The simulation and experimental results are provided to evaluate the dynamic performance of the suggested control approach and to ensure the accurate operation of DC microgrids despite the existence of cyber-attacks on the measurements employed in the control strategy. Moreover, the control strategy succeeds to keep the maximum voltage error and the maximum error in current sharing within tolerance.

Keywords: control; cyber-security; microgrids; false data injection attacks; mitigation layer

check for updates

Citation: EL-Ebiary, A.H.; Mokhtar, M.; Mansour, A.M.; Awad, F.H.; Marei, M.I.; Attia, M.A. Distributed Mitigation Layers for Voltages and Currents Cyber-Attacks on DC Microgrids Interfacing Converters. *Energies* **2022**, *15*, 9426. https://doi.org/10.3390/en15249426

Academic Editors: Djamila Rekioua, Saad Mekhilef and Youcef Soufi

Received: 15 October 2022
Accepted: 9 December 2022
Published: 13 December 2022

1. Introduction

Environmental concerns and the need to reduce fossil fuel consumption have introduced the concept of distributed generators (DGs). These DGs may be renewable energy sources (RESs), energy storage systems (ESSs), or electric vehicles (EVs). DGs are connected in different structures, forming microgrids to supply their common and local loads. Microgrids (MGs) can have an AC or DC nature, depending on the nature of the loads supplied by the microgrids and the nature of the DGs forming the microgrid. However, DC microgrids have some advantages over AC ones [1,2]. DC microgrids have a simple control strategy [3–5], because there is no reactive power control or frequency control [6], and only voltage regulation and proper current sharing between DGs are the main target for the control strategy [7–9]. In addition to that, most of the renewable energy resources have a DC nature, such as photovoltaic (PV) systems and fuel cells. Wind turbines could be connected to DC microgrids through machine-side converters. Moreover, a wide range of loads need a DC supply for operation. Furthermore, DC microgrids could be integrated with AC grids to form hybrid microgrids [10].

Microgrids introduced new challenges from a technical and operational point of view. One of these challenges is that communication links between microgrid components are intertwined with cyber threats. Therefore, securing microgrids from potential cyber-attacks that can cause a lot of damage is an emerging challenge. Cyber-attackers can manipulate the measurements being transmitted from and to each DGU through communication links, thus deceiving the controllers and leading them to take a wrong control action. However, other attacks affect the control signal directly sent from the controller to the DGU, leading to performance degradation. The goals of cyber-attackers may be terroristic, cyber warfare, or commercial advantage. Therefore, we need to update the microgrid control strategies to make it secure against different types of cyber-attacks.

Cyber-attacks on communication channels can have physical consequences such as damaging the equipment and may lead to blackouts and system instability. Therefore, defensive strategies against cyber-attacks are mandatory. These defensive strategies are divided into two main groups that are mainly based on protection and detection/mitigation.

1.1. Literature Review

The authors of [11] discussed mitigation of false data injection attacks on DC microgrids, in which a cooperative mechanism was used to avoid a class of stealth attacks that could bypass the manipulated data detectors. However, the introduced strategy focused on parallel-structure DC microgrids controlled by the hierarchical control strategy based on droop control. This strategy neglected the other structures of DC microgrids and the associated control strategies. The work in [12] presented a framework that can detect the change in a set of candidate invariants for a DC microgrid that is controlled by a consensus controller. Different strategies for protecting the smart meters against cyber-attacks to ensure data validity were discussed in [13–15].

A strategy based on an artificial neural network (ANN) to detect a false data injection attack (FDIA) on voltage measurements of DC bus voltages of DC microgrids was presented [16]. These attacks will affect the DC voltage stabilization process and may destruct the microgrid control system. However, this strategy condoned the possibility of cyber-attacks on the current measurements, as well as considering the droop controller as a primary controller, which only has several drawbacks. On the contrary, a strategy based on a distributed control system to detect the FDIA on current measurements, while neglecting attacks on voltage measurements, was proposed [17]. In [18], two types of cyber-attacks were detected, which were FDIAs and denial of service (DOS) attacks on the DC microgrid that depend on a distributive cooperative control strategy.

An ANN estimator is proposed to monitor the DC–DC converter output current and compare it with the measured signal [19]. This method is used to detect, mitigate FDIA, and calculate the value of false injected data but for attacks on current measurements only. The authors of [20,21] introduced an attack detection module consisting of a local state estimator based on a Luenberger observer to estimate the local measurements of each DGU in a DC microgrid. Furthermore, in this method, unknown input observers estimate the states of the neighboring DGs that are transmitted by the communication links. Alternatively, a nonlinear disturbance observer is used to estimate the attack signal on the communication link, and then, an isolation scheme is used to isolate the attacked agent in the cooperative control strategy [22].

An analytical consistency-based strategy for anomaly detection is proposed to improve the ability of deception attack detection [23]. This mechanism extended the consensus-based algorithm for proper current sharing, as well as distributed voltage control, and it succeeds in detecting the attack; however, it cannot mitigate its effect. A recurrent neural network (RNN) was used in [24] to detect cyber-attacks on DC microgrids and, specify, the attacked DG unit. The recurrent neural network is trained online based on a nonlinear autoregressive exogenous model (NARX) to estimate DC voltages and currents. The estimated error is determined based on the estimated output DC voltages and currents of DG units, and then, this error is used to detect cyber-attacks. This strategy only detects FDIAs and cannot mitigate their effects.

The authors of [25] proposed a strategy for the detection and mitigation of FDIA, as it is the most common type of cyber-attack. This strategy is based on a nonlinear distributed observer that can detect and determine the false data injected in cyber links, as well as current sensors. In the same context, a method to detect and mitigate FDIAs was introduced in [26]. This method is based on model predictive control (MPC) and artificial neural networks. This strategy is implemented for parallel DC/DC converters and has not taken into consideration other types of DC microgrid configurations. Supervised learning classifiers were introduced in [27] to detect stealth FDIAs on smart grids. The classifier converted the false data detection problem into a binary classification problem, so the detector could achieve better performance, specifically for stealth attacks. These detectors can be improved to determine where false data is being injected, but the cost analysis and runtime of these detectors should be further investigated.

In [28], an innovative soft computing strategy for the cybersecurity of smart energy grids was introduced. To model the general level of security, it uses Mamdani fuzzy inference, fuzzy cognitive mapping, and soft computing techniques. However, fuzzy systems depend on the human experience and knowledge. Examples of how FDIAs are constructed, detected, and mitigated in smart microgrids were given in [29]. Moreover, examples of current global cyber-security projects, as well as crucial smart grid cyber-security standards were presented. FDIAs on islanded microgrids were studied in [30], and a resilient control method was proposed for mitigation and recovery from the attack effects. The authors of [31] showed that there are several security and privacy challenges for smart grids. Therefore, the smart grid necessitates the appropriate design features and communication technology to maintain data privacy and protection against cyber-attacks.

1.2. Paper Approach

Based on this discussion, most of the literature has focused on the cyber security of DC microgrids with parallel and radial structures and neglected the meshed structure for microgrids, despite the fact that it is the most prominent structure in practice. Moreover, researchers have focused on securing the microgrid from either attacks on voltage measurements or attacks on current measurements and have not taken into consideration the possibility that the attacker can merge both attacks together. In this paper, a distributed control strategy for meshed DC microgrids is modified by introducing a voltage and current cyber-attack detection and mitigation layers. These layers are used to detect and mitigate FDIAs on both voltage and current measurements that are being locally or globally transmitted, along with the communication links in DC microgrids. A meshed DC microgrid with a distributed control scheme is modeled, and the control system is modified by adding voltage and current cyber-attack detection and mitigation layers to primary and secondary loops, respectively. Hence, the novelty of the modified control strategy is taking into consideration cyber-attacks on voltage and current measurements simultaneously. Moreover, it is a droopless control strategy that eliminates the drawbacks of the droop control as a poor dynamic performance.

The paper contributions can be listed as follows:

- Securing meshed DC microgrids control system by exploiting artificial neural networks for estimating authenticated measurements.
- Introducing distributed detection and mitigation layers for FDIAs on both voltage and current measurements.
- Keeping proper current sharing and decent reference voltage tracking, regardless of the presence of FDIA.
- Experimentally evaluating the dynamic performance of the proposed mitigation layers under different FDIA attack values.

2. System Model and Control Scheme

In this section, the system model is discussed at first. Then, the distributed control strategy is introduced where a state feedback primary controller is used for the voltage regulation of each DGU. Moreover, a consensus based secondary controller is used to add a correction term to the voltage reference of the primary controller in order to achieve proper current sharing between all DGUs. Afterwards, the primary controller is modified by adding a voltage cyber-attack detection and mitigation layer for each DGU to secure the voltage measurements. Finally, a current cyber-attack detection and mitigation layer is integrated with the secondary controller of each DGU to protect the current measurements. Thus, the system with the modified primary and the modified secondary loops can be considered as advanced power system with nonlinear technology [32].

2.1. System Model

Figure 1 depicts the mesh configuration of the DC microgrid under consideration, which consists of four DGUs, each of which may stand for a fuel cell, a solar or photovoltaic system, or a wind system. Additionally, these DGs are connected to one another using tie line circuit breakers (CBs).

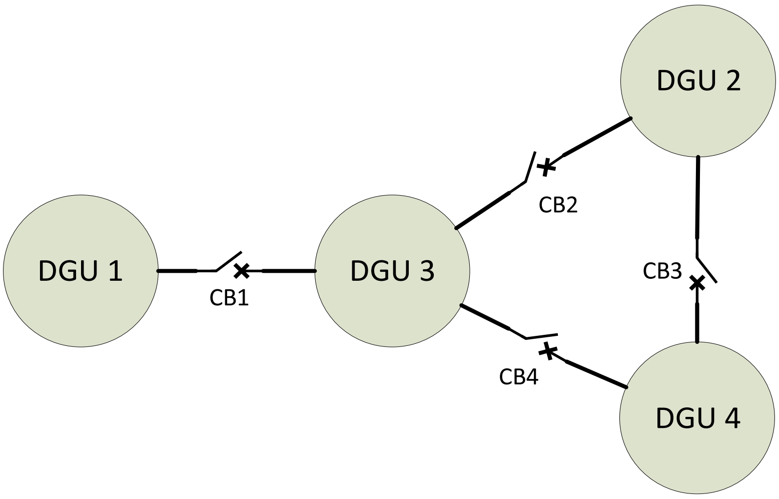


Figure 1. Mesh DC microgrid.

It is assumed that each DGU has its own converter, as indicated in Figure 2a. Each DGU can be modeled by the following equations [33]:

$$\frac{dv_i}{dt} = \frac{I_{ti}}{C_{ti}} + \sum\left[\frac{v_j}{C_{ti}R_{ij}} - \frac{v_i}{C_{ti}R_{ij}}\right] - \frac{I_{li}}{C_{ti}} \tag{1}$$

$$\frac{dI_{ti}}{dt} = \frac{-1}{L_{ti}}v_i - \frac{R_{ti}}{L_{ti}}I_{ti} + \frac{1}{L_{ti}}v_{ti} \tag{2}$$

where L_{ti} and C_{ti} are the inductance and capacitance of the LC filter used for buck converter of the ith DGU, respectively, v_{ti} and v_i are the ith DGU terminal voltages before and after the LC filter, respectively, I_{ti} and I_{li} are the inductor and local load currents of the ith DGU, respectively, and R_{ij} and L_{ij} are the resistance and inductance of the line connecting ith and jth DGUs, respectively. This system can be represented in the state space as follows [33]:

$$\dot{x}_{[i]}(t) = A_{ii}x_{[i]}(t) + B_i u_{[i]}(t) + M_i d_{[i]}(t) + \xi_{[i]}(t) \tag{3}$$

$$y_{[i]}(t) = C_i x_{[i]}(t) \tag{4}$$

$$z_{[i]}(t) = H_i y_{[i]}(t) \tag{5}$$

where $x_{[i]}(t) = [v_i,\ I_{ti}]^T$ is the DGU state vector, which consists of the ith DGU terminal voltage after the LC filter v_i and the inductor current I_{ti}, respectively, $u_{[i]}(t) = v_{ti}$ refers to the input control action to the system, which is the ith DGU terminal voltage before the LC filter, $\xi_{[i]}(t)$ represents the coupling of DGUi, with each neighboring DGUj as described in Equation (6), $d_{[i]}(t) = I_{li}$ represents the external disturbance, which is the local load current, $y_{[i]}(t) = x_{[i]}(t) = [v_i,\ I_{ti}]^T$ is the measured output vector from the system, and $z_{[i]}(t) = v_i$ is the controlled variable.

$$\xi_{[i]}(t) = \sum\nolimits_{j\ \in Ni}\ A_{ij}x_{[j]} \tag{6}$$

where N_i represents neighboring DGUs to the DGUi. The matrices of the state space model are given as follows:

$$A_{ii}= \begin{bmatrix} \sum_{j\ \in Ni} \frac{-1}{R_{ij}C_{ti}} & \frac{1}{C_{ti}} \\ \frac{-1}{L_{ti}} & -\frac{R_{ti}}{L_{ti}} \end{bmatrix} \tag{7a}$$

$$B_i= \begin{bmatrix} 0 \\ \frac{1}{L_{ti}} \end{bmatrix} \tag{7b}$$

$$M_i = \begin{bmatrix} \frac{-1}{C_{ti}} \\ 0 \end{bmatrix} \tag{7c}$$

$$C_i= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{7d}$$

$$H_i = [1 \quad 0] \tag{7e}$$

$$A_{ij} = \begin{bmatrix} \dfrac{1}{R_{ij}C_{ti}} & 0 \\ 0 & 0 \end{bmatrix} \tag{7f}$$

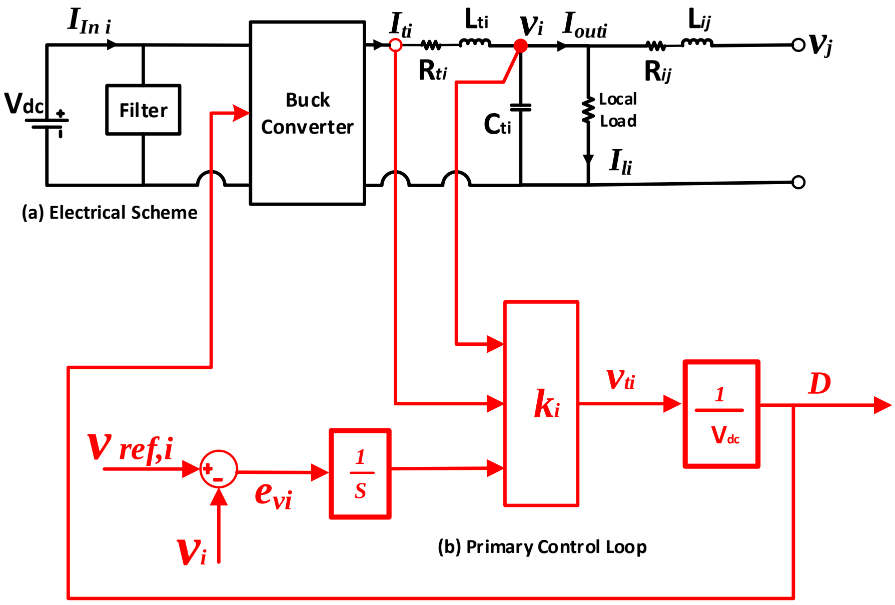


Figure 2. Distributed generator unit i with local primary voltage controller: (**a**) electrical scheme and (**b**) state feedback primary control loop.

System Model after Adding the Integral Action

Let $z_{ref[i]}(t)= v_{refi}$ represents the desired reference for the controlled output $z_{[i]}(t)$. To track $z_{ref[i]}(t)$, an integral action should be added to the state vector to eliminate the steady-state error $e_{[i]}(t)$ =$z_{ref[i]}(t) - z_{[i]}(t)$. The dynamic action of the integrator is described by [33]:

$$\dot{\mathrm{v}}_{\mathrm{i}}(\mathrm{t}) = \mathrm{e}_{[\mathrm{i}]}(t) = z_{ref\ [\mathrm{i}]}(t) - z_{[\mathrm{i}]}(t) = z_{ref\ [\mathrm{i}]}(t) - H_iC_ix_{[\mathrm{i}]}(\mathrm{t}) \tag{8}$$

As a result, the state vector of the system is updated to be $x^u_{[i]}(\mathrm{t}) = [v_i,\ I_{ti}\ ,\mathrm{v}_{\mathrm{i}}]^T$ after adding the integral action. The new updated state space model is given by Equations (9)–(12). The measured output vector of the system will be $y^u_{[i]}(\mathrm{t})$ = $[v_i,\ I_{ti}, \mathrm{v}_{\mathrm{i}}]^T$. However, the input and controlled variables remain the same as $u_{[i]}(t) = v_{ti}$ and $z^u_{[i]}(t) = v_i$, respectively. The external disturbance vector is modified to include the reference signal and the load current, such that $d^u_{[i]}(\mathrm{t}) = [I_{li}, z_{ref\ [\mathrm{i}]}(t)]$. In addition, the coupling of the DGUi with each neighboring DGUj, $\xi^u_{[i]}(\mathrm{t})$, is updated as (10). Moreover, the matrices of the new state space model are given by Equations (13a)–(13f).

$$\dot{x}^u_{[i]}(t) = A^u_{ii}x^u_{[i]}(\mathrm{t}) + B^u_i u_{[i]}(t) + M^u_i d^u_{[i]}(\mathrm{t}) + \xi^u_{[i]}(\mathrm{t}) \tag{9}$$

$$\xi^u_{[i]}(\mathrm{t}) = \sum\nolimits_{j\ \in Ni}\quad A^u_{ij}x^u_{[j]} \tag{10}$$

$$y^u_{[i]}(\mathrm{t}) = C^u_i x^u_{[i]}(\mathrm{t}) \tag{11}$$

$$z^u_{[i]}(t) = z_{[i]}(t) = H^u_i y^u_{[i]}(\mathrm{t}) \tag{12}$$

$$A^u_{ii}= \begin{bmatrix} \sum_{j\ \in Ni} \frac{-1}{R_{ij}C_{ti}} & \frac{1}{C_{ti}} & 0 \\ \frac{-1}{L_{ti}} & -\frac{R_{ti}}{L_{ti}} & 0 \\ -1 & 0 & 0 \end{bmatrix} \tag{13a}$$

$$B^u_i= \begin{bmatrix} 0 \\ \frac{1}{L_{ti}} \\ 0 \end{bmatrix} \tag{13b}$$

$$M^u_i = \begin{bmatrix} \frac{-1}{C_{ti}} & 0 \\ 0 & 0 \\ 0 & 1 \end{bmatrix} \tag{13c}$$

$$C^u_i= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \tag{13d}$$

$$H^u_i = \begin{bmatrix} 1 & 0 & 0 \end{bmatrix} \tag{13e}$$

$$A^u_{ij} = \begin{bmatrix} \frac{1}{R_{ij}C_{ti}} & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \tag{13f}$$

2.2. System Control Strategy

Each DGU in the meshed DC microgrid has two control loops. The first one is the primary control loop, which is responsible for the regulation of the DGUi voltage, v_i, as shown in Figure 2. The other loop is a secondary control loop, which is used to achieve proper current sharing between all DG units based on their rating, as illustrated in Figure 3a.

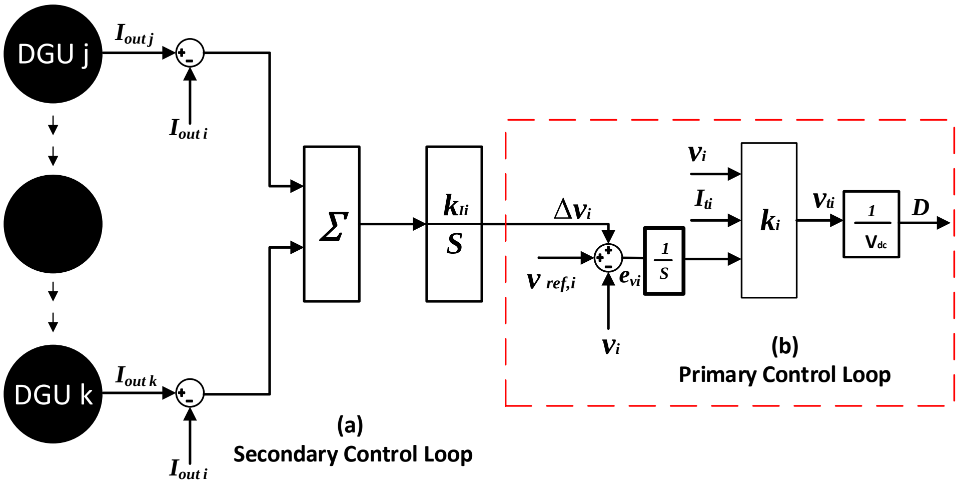


Figure 3. Hierarchical control scheme of the microgrid under study: (**a**) consensus-based secondary controller and (**b**) state feedback primary controller.

2.2.1. State Feedback Primary Controller

The primary controller in Figure 2b is based on a state feedback controller, where the control action v_{ti} is given by (14), which is used to obtain the duty cycle, D, of the DGU*i* converter [33].

$$v_{ti} = u_i(t) = k_i x_{u[i]} = DV_{dc} \tag{14}$$

The vector $k_i = [k_{1i}\,, k_{2i}\,, k_{3i}]$ is obtained by solving a linear matrix inequality (LMI) problem, as in [33,34]. Additionally, V_{dc} is the input voltage of the buck converter, and v_{refi} is the reference voltage signal of the controlled variable v_i.

2.2.2. Consensus Based Secondary Controller

The secondary control layer depends on a consensus-based algorithm [9,34] based on (15), which adds a correction term Δv_i to the reference voltage of the primary controller to achieve proper current sharing.

$$\Delta \dot{v}_i = k_{Ii} \sum_{j=1,\ j\neq i}^{N} \left(I_{outj} - I_{outi}\right) \tag{15}$$

where k_{Ii} is the integral gain of the secondary controller, I_{outi} is the DGU*i* injected output current, and N is the total number of DGUs. The overall hierarchical control scheme for a meshed DC microgrid without cyber-attack layers is shown in Figure 3. This hierarchical control is distinguished by elimination of the droop controller, which has poor dynamic performance and voltage deviations.

3. Proposed Modified Control Scheme

The performance of the primary and secondary control loops is based on the accuracy of voltage and current measurements. Therefore, it is crucial to modify the microgrid control strategy to thwart cyber-attacks in order to secure these measurements.

As mentioned before, the cyber-attacks may target the voltage or the injected current of each DGU. Firstly, FDIA on the voltage is considered. The manipulated voltage v_i^a can be considered as a summation of two terms as follows:

$$v_i^a = v_i + \alpha_i \tag{16}$$

The first term is the actual voltage, v_i, while the second term is the false term α_i applied by attackers. This term may be positive or negative. As a result of this term, the controller will take a wrong action to make v_i^a follow the reference signal v_{refi}. Hence, if the attack is determined, the final value of voltage v_i is based on the reference signal, as well as the false term α_i, as expressed in (17):

$$v_{i\ ss} = v_{refi} - \alpha_i \tag{17}$$

The vital issue here is that the voltage v_i can converge onto a value outside the allowable tolerance. This action may lead to the shutdown of the DC microgrid.

In the same context, a similar FDIA can target the current measurements as follows:

$$I_i^a = I_i + I_{Fi} \tag{18}$$

where I_{Fi} is the false term injected into the current measurement I_i of the DGU*i*. These attacks aim to mislead the current sharing between all DGUs. Therefore, the primary and secondary controllers should be modified to be able to withstand cyber-attacks on both voltage and current measurements.

3.1. Modified Primary Controller

The primary controller is modified to detect and mitigate the manipulated voltage measurement, v_i. This measurement is used in the state feedback controller as given by (14), which is crucial for reference voltage tracking. Consequently, a voltage cyber-attack detection and mitigation layer is added to the primary control loop to make sure that the voltage measurement v_i is the real value even in the presence of a FDIA on v_i.

Exploiting the estimation capability of an ANN, cyber-attacks can be detected by comparing the measured DGU*i* voltage v_i^a with the estimated voltage $\overline{v}_i$ produced by the ANN. In turn, the error between the measurement and estimated signals is utilized to detect and mitigate the cyber-attack. A voltage cyber-attack detection and mitigation layer is shown in Figure 4, where the FDIA is represented by α_i, which is added to the measured voltage v_i. The signal $\theta_i(t)$ [16], expressed in (19), is the corrected voltage measurement sent to the primary controller.

$$\theta_i(t) = \underbrace{v_i + \alpha_i}_{v_i^a} + \beta_i(t) \tag{19}$$

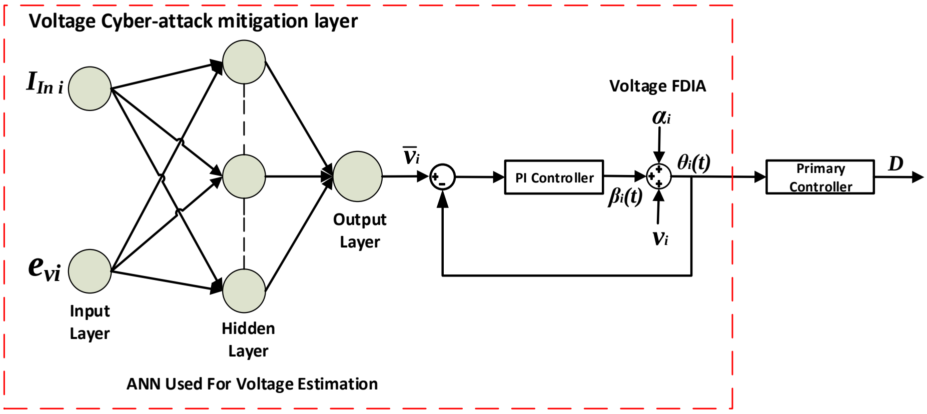


Figure 4. Voltage cyber-attack detection and mitigation layer proposed for the primary controller of DGU*i*.

A closed loop feedback system is employed in which $\theta_i(t)$ is subtracted from the estimated DGU*i* voltage $\overline{v}_i$ by the ANN. The error is processed by a conventional PI controller to produce the voltage correction term $\beta_i(t)$, which is used to detect and mitigate the effect of α if there is a FDIA. It is worth mentioning that the conventional PI controller is used to converge the measured terminal voltage onto the estimated output voltage by the neural network $\overline{v}_{i,}$ even in the presence of a FDIA. Therefore, the steady-state value of $\theta_i(t)$ should be

$$\theta_{i\ ss} = \overline{v}_i \tag{20}$$

Inspecting (19) and (20), the output of the PI controller β_i is settled to (21).

$$\beta_i = \theta_{i\ ss} - v_i^a = \overline{v}_i - v_i^a \tag{21}$$

Therefore, if DGUi voltage is estimated accurately, $\overline{v}_i = v_i$, and β_i is forced to be equal to $-\alpha_i$, and the effect of the cyber-attack is completely mitigated. In other words, the output of the PI controller $\beta_i(t)$ is converging to $-\alpha_i$ to remove a false measurement from being used by the primary controller of DGUi. Therefore, it is mandatory to have an accurate estimation of the DGUi voltage, utilizing ANN to guarantee the proper operation of the voltage cyber-attack detection and mitigation layer.

3.2. Modified Secondary Controller

In case of the presence of FDIA on the output current I_{outi} of DGUi, the secondary control layer of DGUi receives I_{outi}^a, which is the attacked current measurement, and it is given by:

$$I_{outi}^a = I_{outi} + I_{Fi} \tag{22}$$

where I_{Fi} is the false data injected in the output current measurements of the DGUi. The proposed current cyber-attack detection and mitigation layer for DGUi is shown in Figure 5, where an ANN is used to estimate $\overline{I}_{outi}$. The error between the estimated current and the current measurement, needed for the secondary controller, is diminished by a conventional PI controller to obtain the current correction term $\gamma_i(t)$ such that the corrected current measurement $\mu_i(t)$ [16] is given by:

$$\mu_i(t) = I_{outi} + I_{Fi} \ + \gamma_i(t) \tag{23}$$

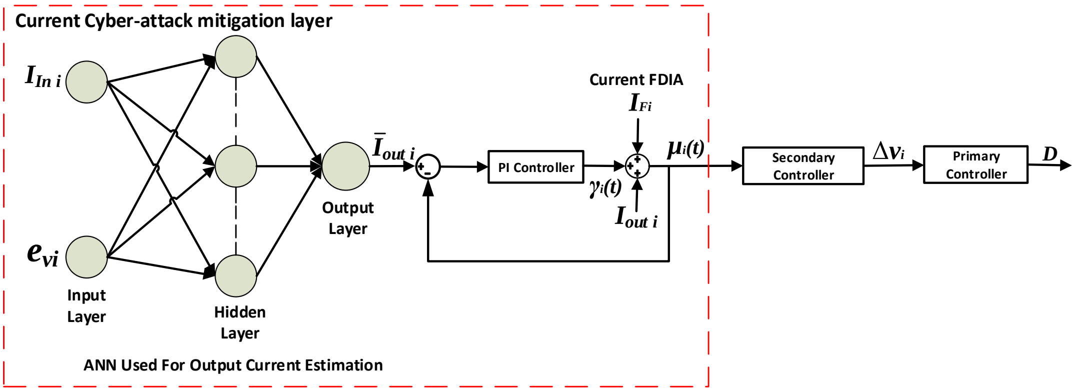


Figure 5. Current cyber-attack detection and mitigation layer proposed for the secondary controller of DGUi.

To mitigate the FDIA on the measured current, $\gamma_i(t)$ should cancel out $I_{Fi,}$ as follows:

$$\gamma_i(t) = -I_{Fi} \tag{24}$$

This action ensures that the secondary controller of DGUi receives the true output current measurements, and consequently, current sharing is maintained.

The overall system components with the control strategy can be summarized as follows:

- DC microgrid system, including four meshed DGUs.
- Modified primary controller, which is based on a state feedback controller, Equation (14), integrated with a voltage cyber-attack detection, and mitigation layer.
- Modified secondary controller, which is based on a consensus based controller, Equation (15), where a current cyber-attack detection and mitigation layer is incorporated.

The overall block diagram of the proposed distributed control strategy after integrating both voltage and current cyber-attack detection and mitigation layers is shown in Figure 6.

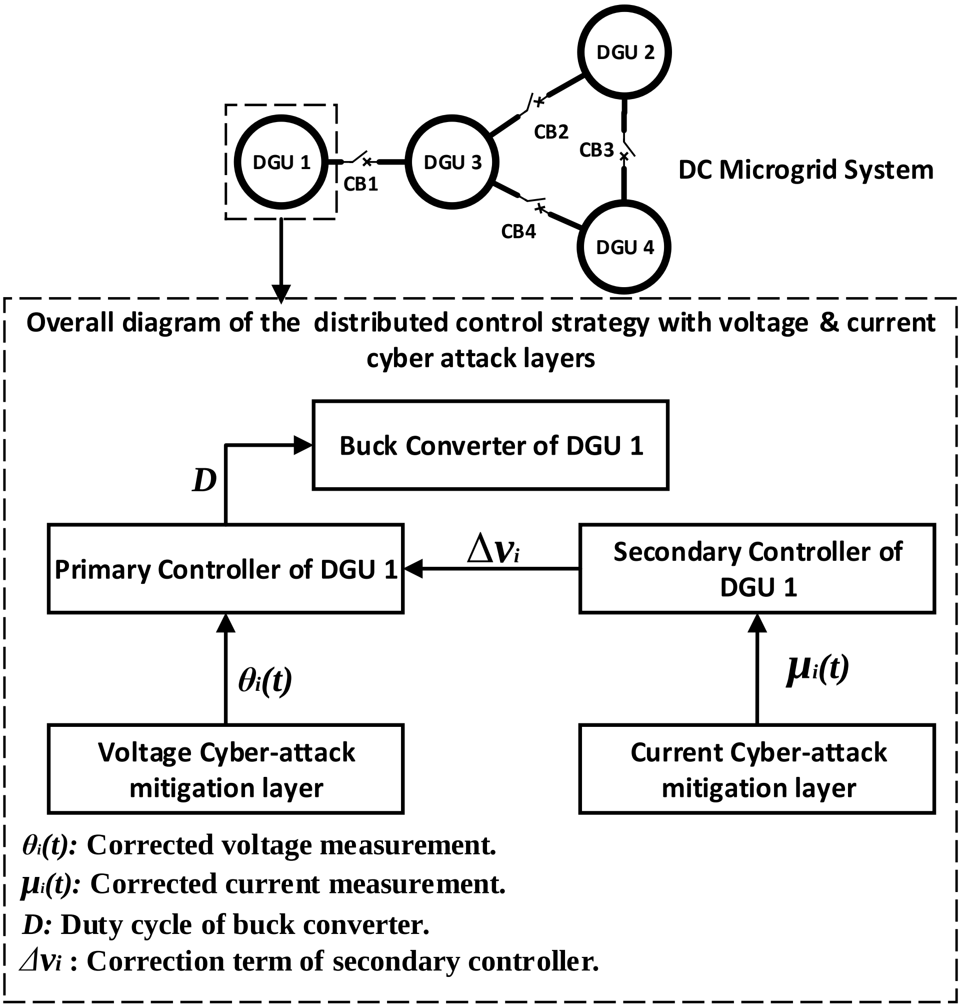

DGU 1
DGU 2
DGU 3
DGU 4
CB1
CB2
CB3
CB4
DC Microgrid System
Overall diagram of the distributed control strategy with voltage & current cyber attack layers
Buck Converter of DGU 1
D
Primary Controller of DGU 1
Δvᵢ
Secondary Controller of DGU 1
θᵢ(t)
μᵢ(t)
Voltage Cyber-attack mitigation layer
Current Cyber-attack mitigation layer
θᵢ(t): Corrected voltage measurement.
μᵢ(t): Corrected current measurement.
D: Duty cycle of buck converter.
Δvᵢ : Correction term of secondary controller.

Figure 6. Overall system with the distributed control strategy blocks for a single DGU.

The flowchart of the overall distributed control strategy with the integrated detection and mitigation layers is presented in Figure 7.

3.3. Cyber-Attack Detection and Mitigation Layers Training

Supervised learning is used in this paper, where a feed-forward neural network with three layers is used for both voltage and current cyber-attack mitigation layers. Both ANNs have an input layer with two inputs, one hidden layer with ten neurons, and an output layer with a single neuron. Therefore, the ANN configuration is (2-10-1). The training data used is sampled from the DC microgrid in healthy conditions without any cyber-attack.

Both ANNs take the input current of the DGUi, $I_{In\ i}$, and the DGUi voltage error, e_{vi}, as inputs. Moreover, the output of the voltage cyber-attack ANN is the estimated voltage of DGUi, $\overline{v}_i$, while the output of the current cyber-attack ANN is the estimated output current of DGUi, $\overline{I}_{out\ i}$.

The feed-forward neural networks are chosen due to their good ability of estimation and their flexible implementation, design, and training [35]. The training process, illustrated in Figure 8, is carried out using Levenberg–Marquardt optimization, which is a backpropagation algorithm to update the weights and the bias of the neural network in order to improve the neural network performance [36]. This performance is measured using the mean squared error (MSE) as given by:

$$\text{MSE} = \frac{1}{n}\sum_{i=1}^{n}\left(Y_i - \hat{Y}_i\right)^2 \tag{25}$$

where n is number of samples, Y_i is the target output, and $\hat{Y}_i$ is the estimated output by the ANN. When the MSE is kept below a small value, the training of the ANNs is achieved, and the optimal weights of the ANNs are reached. A well-trained ANN will be able to accurately estimate the healthy un-attacked measurements. This action is crucial for proper operation of the proposed cyber-attach detection and mitigation layer to effectively mitigate the FDIAs.

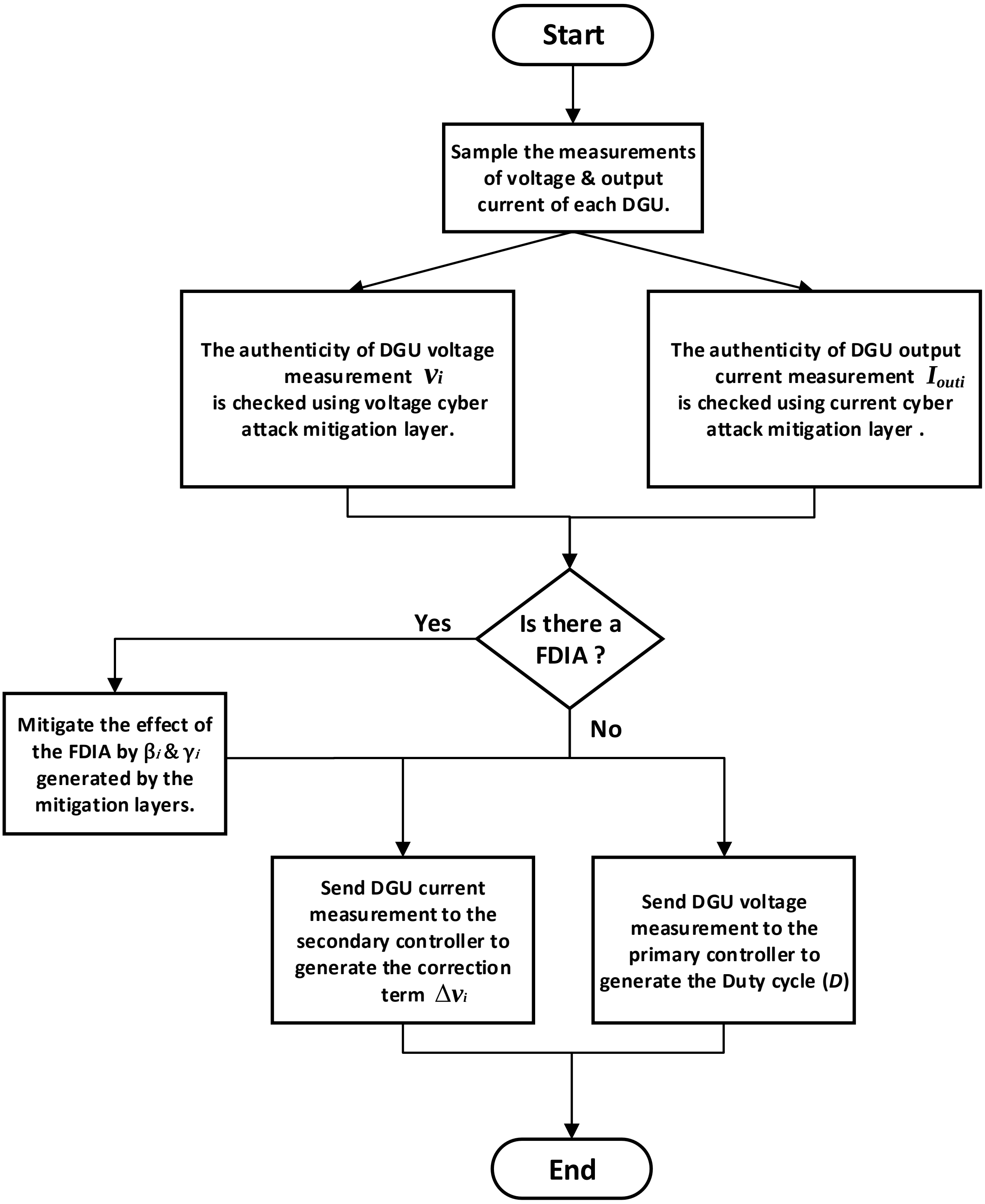

Start
Sample the measurements of voltage & output current of each DGU.
The authenticity of DGU voltage measurement V_i is checked using voltage cyber attack mitigation layer.
The authenticity of DGU output current measurement I_{outi} is checked using current cyber attack mitigation layer .
Is there a FDIA ?
Yes
No
Mitigate the effect of the FDIA by β_i & γ_i generated by the mitigation layers.
Send DGU current measurement to the secondary controller to generate the correction term Δv_i
Send DGU voltage measurement to the primary controller to generate the Duty cycle (*D*)
End

Figure 7. Flowchart for the overall control strategy with cyber-attack mitigation layers.

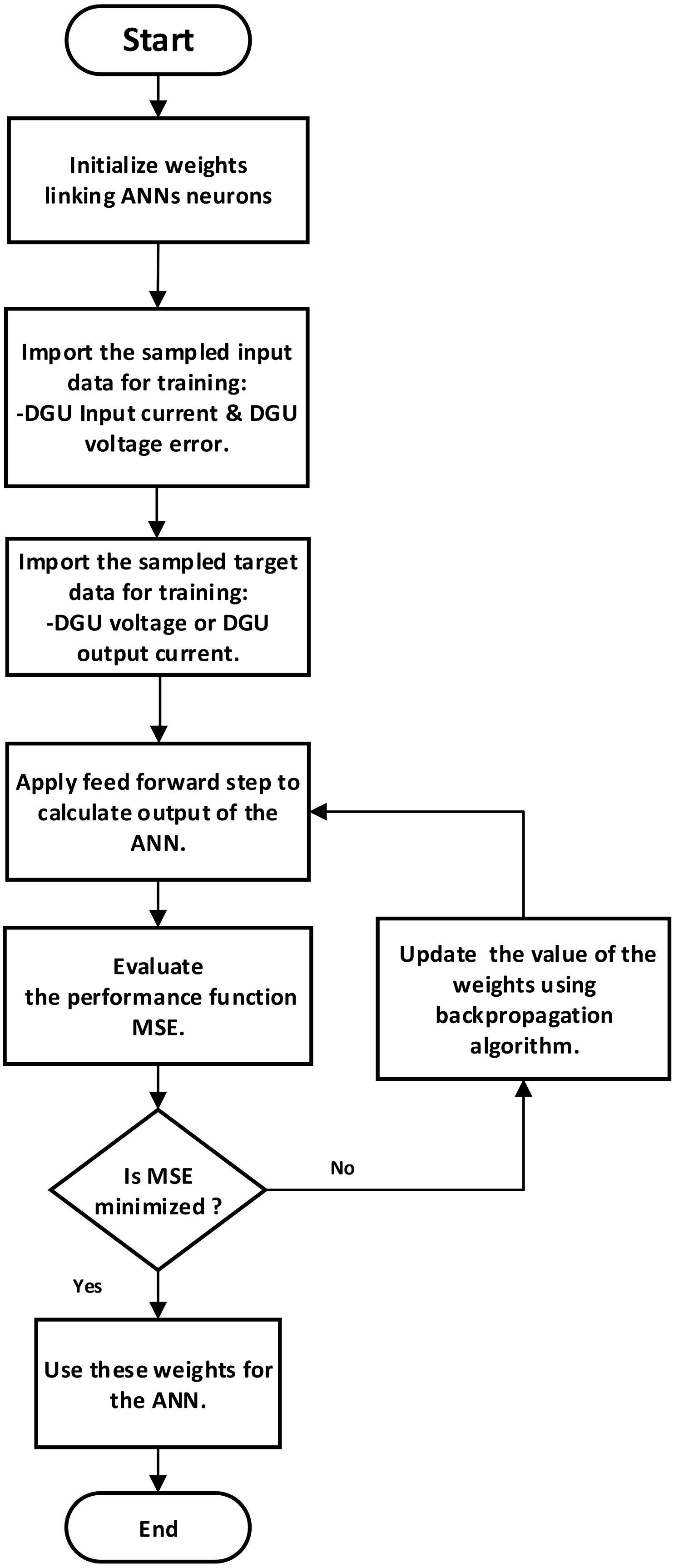

Start
Initialize weights linking ANNs neurons
Import the sampled input data for training: -DGU Input current & DGU voltage error.
Import the sampled target data for training: -DGU voltage or DGU output current.
Apply feed forward step to calculate output of the ANN.
Evaluate the performance function MSE.
Update the value of the weights using backpropagation algorithm.
Is MSE minimized ?
No
Yes
Use these weights for the ANN.
End

Figure 8. Flowchart for voltage and current cyber-attack ANNs training.

4. Simulation Results

Utilizing the MATLAB/Simulink program, the suggested control strategy is tested on the meshed DC microgrid shown in Figure 1 with the parameters listed in Tables 1 and 2. In addition, the gains of different primary and secondary controllers are given in Table 3. A voltage cyber-attack detection and mitigation layer is added to the primary controller of each DGU. This layer is used to detect and mitigate a FDIA on voltage measurements of the primary controller. Moreover, a current cyber-attack detection and mitigation layer is implemented in each DGU secondary controller to detect and mitigate FDIAs on output current measurements of DGUs. To assess the efficacy of the suggested cyber-attack detection and mitigation layers, FDIAs for voltage and current measurements are performed on the system.

Table 1. Line parameters.

Connected DGUs (*i,j*)	Resistance R_{ij} (Ω)	Inductance L_{ij} (µH)
Line 1–3	0.07	2.1
Line 2–3	0.04	2.3
Line 2–4	0.08	1.8
Line 3–4	0.07	1

Table 2. Buck converters and filter parameters.

Input/Output Voltages: 100 V /48 V				
DGU *i*	Resistance R_{ti} (Ω)	Inductance L_{ti} (mH)	Capacitance C_{ti} (mF)	Local Load (Ω)
DGU 1	0.2	1.8	2.2	10
DGU 2	0.3	2.0	1.9	9
DGU 3	0.1	2.2	1.7	8
DGU 4	0.5	3.0	2.5	7

Table 3. Primary and secondary layer controller parameters.

	Primary Controllers' Gains
DGU 1	$k_1 = [-2.13, -0.16, 13.55]$
DGU 2	$k_2 \ = [-0.87, -0.05,\ 48.28]$
DGU 3	$k_3 \ = [-0.48, -0.108,\ 30.67]$
DGU 4	$k_4 = [-7, -0.175,\ 102.96]$
Secondary Integral Controller Gain: $k_{Ii} = 0.02$	

For all the following case studies, the tie line breakers are closed at t = 1.5 s to create a meshed DC microgrid, and the secondary controller is enabled at the same instant. In addition, v_{ref} = 48 V for all DGUs. To evaluate the performance of the two added layers, the percentage voltage error $(\%Ve_i)$ and percentage change in current sharing for DGUi $(\%Ic_i)$ are calculated as follows:

$$\%Ve_i = \frac{v_{refi} \ - v_i}{v_{refi}} \times 100 \tag{26}$$

$$\%\ Ic_i = \frac{I_{es} - I_{out\ i}}{I_{es}} \times 100 \tag{27}$$

$$I_{es} = \frac{1}{N}\sum_{i=1}^{i=N} I_{out\ i} \tag{28}$$

where I_{es} is the equal current sharing value, which is calculated by (28).

Figure 9 summarizes the conducted five simulation case studies to evaluate the effectiveness of the proposed voltage and current cyber-attack mitigation layers.

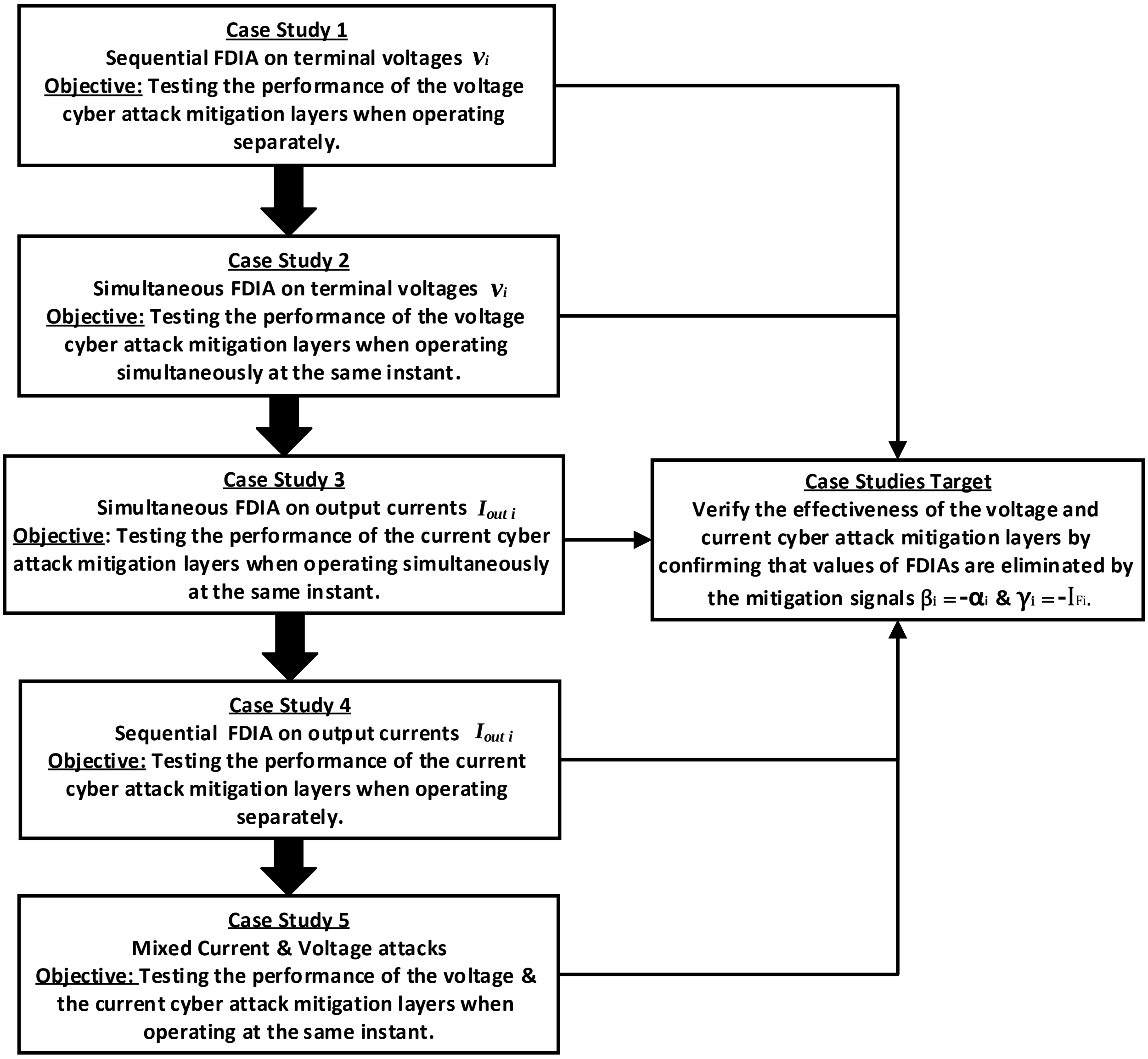

Case Study 1
Sequential FDIA on terminal voltages V_i
Objective: Testing the performance of the voltage cyber attack mitigation layers when operating separately.
Case Study 2
Simultaneous FDIA on terminal voltages V_i
Objective: Testing the performance of the voltage cyber attack mitigation layers when operating simultaneously at the same instant.
Case Study 3
Simultaneous FDIA on output currents $I_{out\ i}$
Objective: Testing the performance of the current cyber attack mitigation layers when operating simultaneously at the same instant.
Case Study 4
Sequential FDIA on output currents $I_{out\ i}$
Objective: Testing the performance of the current cyber attack mitigation layers when operating separately.
Case Study 5
Mixed Current & Voltage attacks
Objective: Testing the performance of the voltage & the current cyber attack mitigation layers when operating at the same instant.
Case Studies Target
Verify the effectiveness of the voltage and current cyber attack mitigation layers by confirming that values of FDIAs are eliminated by the mitigation signals $\beta_i = -\alpha_i$ & $\gamma_i = -I_{Fi}$.

Figure 9. Simulation case studies: objectives and targets.

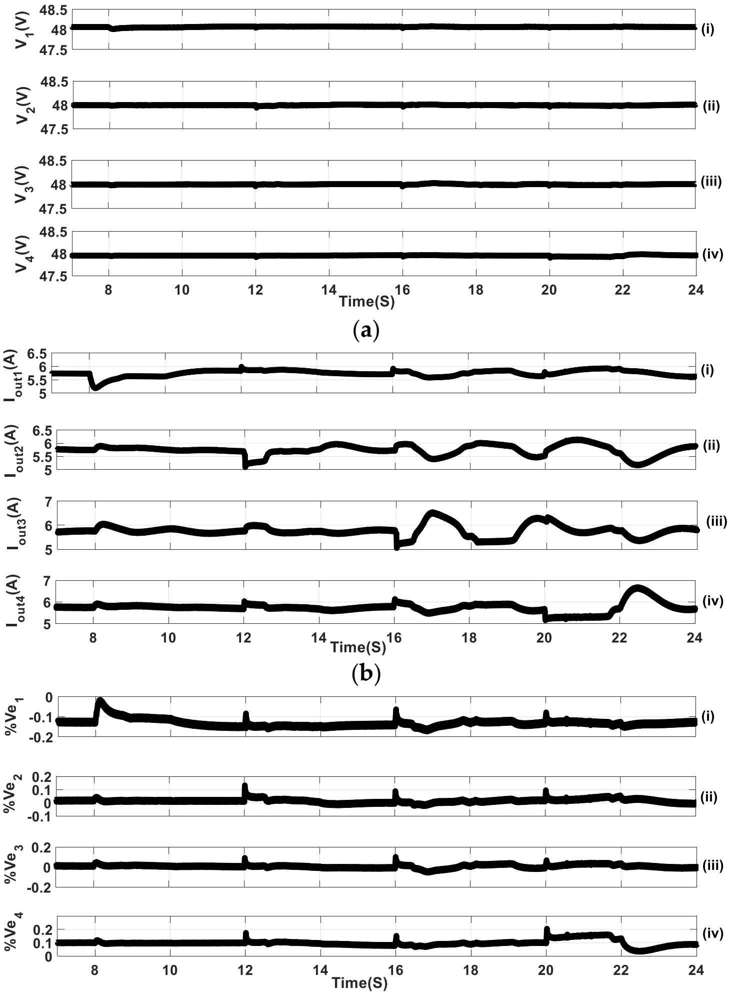
4.1. Sequential FDIA on Terminal Voltages of DGUs

In this case study, the dynamic performance of the proposed cyber-attack mitigation layers is investigated under sequential FDIA on the local voltage measurements of each DGU, as described in Table 4. Firstly, DGU 1 is attacked by $\alpha_1 = +5\ V$ from t = 8 s to t = 10 s. Subsequently, DGU 2 is attacked by $\alpha_2 = +10\ V$ from t = 12 s to t = 14 s, followed by an attack on DGU 3 of $\alpha_3 = +10\ V$ from t = 16 s to t =18 s, and finally, DGU 4 is attacked by $\alpha_4 = +5\ V$ from t = 20 s to t = 22 s.

The results in Figure 10 illustrate that the voltage cyber-attack detection and mitigation layer managed to cancel out the effect of different values of FDIA on voltage measurements. Figure 10a indicates voltages of all DGUs which are successfully maintained at 48 V, regardless of the presence of an attack. Moreover, Figure 10b shows that current sharing loop is still operating properly, even when the microgrid system is under the attack. The percentage voltage error and percentage change in current sharing are kept in the acceptable limits, as exhibited in Figure 10c,d. In addition, the proposed distributed voltage cyber-attack mitigation layer prevents overloading DGUs, as demonstrated in Figure 10d. Figure 10e illustrates the correction term added by the voltage mitigation layer implemented in each DGU primary control loop. For each DGU, it is obvious that the correction term reaches the false term, $\beta_{\mathrm{i}} = -\alpha_i$, which indicates that the ANNs work properly and produce accurate estimates of the DGUs voltages. These results show that there is no cross-coupling between the different voltage cyber-attack mitigation layers, and the proposed distributed control scheme succeeds in securing the primary control level of the meshed DC microgrid.

Table 4. Sequential voltage FDIA parameters.

DGU *i*	FDIA Value	Attack Instant
DGU *1*	$\alpha_1 = +5\ V$	*t* = [8–10 s]
DGU 2	$\alpha_2 = +10\ V$	*t* = [12–14 s]
DGU *3*	$\alpha_3 = +10\ V$	*t* = [16–18 s]
DGU *4*	$\alpha_4 = +5\ V$	*t* = [20–22 s]

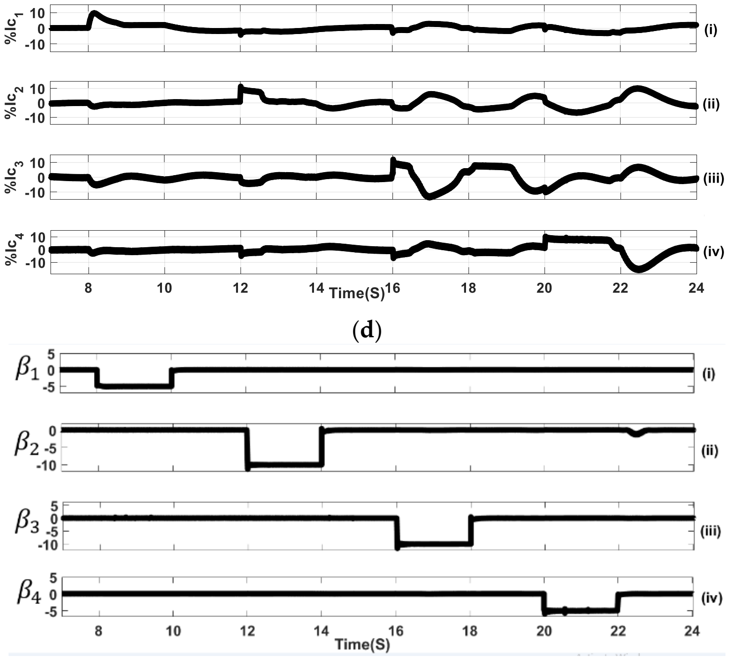


(**a**)

(**b**)

(**c**)

Figure 10. *Cont.*



(d)

(e)

Figure 10. First case study: (**a**) DGU voltages v_i, (**b**) DGU output currents $I_{out\ i}$, (**c**) percentage errors in DGU voltages $\%Ve_i$, (**d**) percentage change in current sharing $\%Ic_i$, (**e**) voltage cyber-attack mitigation signals for DGUs, β_{i}.

4.2. Simultaneous FDIA on Terminal Voltages of DGUs

In this scenario, FDIAs of $\alpha_i = -20\ V$ are applied on the voltage measurements of DGUs 1, 2, and 4 at the same instant from t = 5 s to t = 7 s, as indicated in Table 5.

Table 5. Simultaneous voltage FDIA parameters.

DGU i	FDIA Value	Attack Instant
DGU *1*	$\alpha_1 = -20\ V$	t = [5–7 s]
DGU *2*	$\alpha_2 = -20\ V$	t = [5–7 s]
DGU *4*	$\alpha_4 = -20\ V$	t = [5–7 s]

Figure 11a shows that the voltage deviations are not notable, while appropriate current sharing is demonstrated in Figure 11b. In addition, it is clear from Figure 11c that the voltage cyber-attack detection and mitigation layer succeeds in securing accurate reference voltage tracking, and hence, proper current sharing is achieved, as indicated in Figure 11d. Figure 11e illustrates the generated correction terms for different DGUs, where β_1, β_2, and β_4 are quickly set at $-\alpha_i$ to cancel out the FDIA effect on their corresponding DGUs.

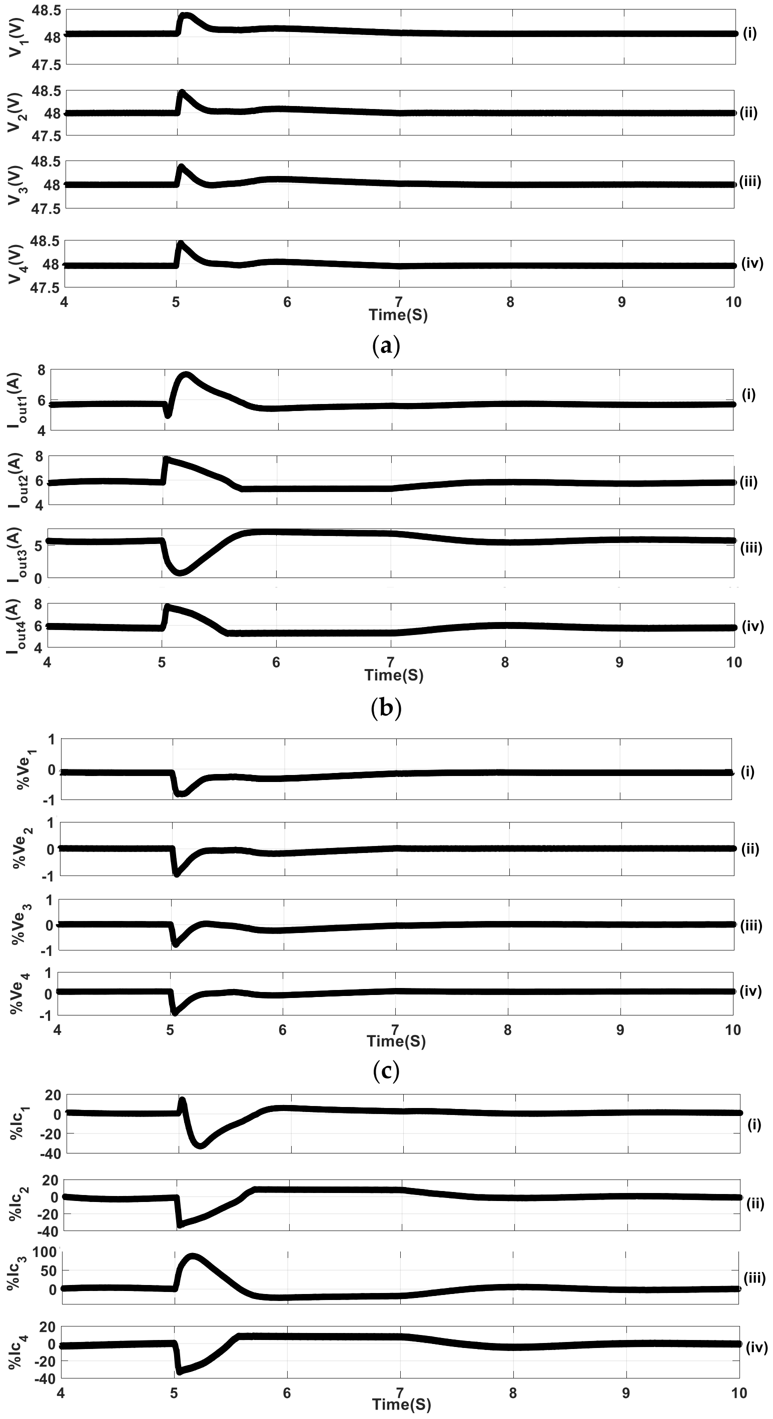
The findings of Figure 11 demonstrate that simultaneous FDIAs on the terminal voltages of DGUs linked to a meshed DC microgrid are mitigated by the proposed voltage cyber-attack detection and mitigation layers.

4.3. Simultaneous FDIA on Output Currents of DGUs

In this case study, the dynamic performance of the current cyber-attack detection and mitigation layer is investigated by applying multiple FDIAs of I_{Fi} = +3 A on all the output current measurements used for the secondary controllers of each DGU during the interval [7 s, 10 s], as illustrated in Table 6.

Table 6. Simultaneous current FDIA parameters.

DGU i	FDIA Value	Attack Instant
DGU *1*	$I_{F1} = +3\ A$	t = [7–10 s]
DGU *2*	$I_{F2} = +3\ A$	t = [7–10 s]
DGU *3*	$I_{F3} = +3\ A$	t = [7–10 s]
DGU *4*	$I_{F4} = +3\ A$	t = [7–10 s]



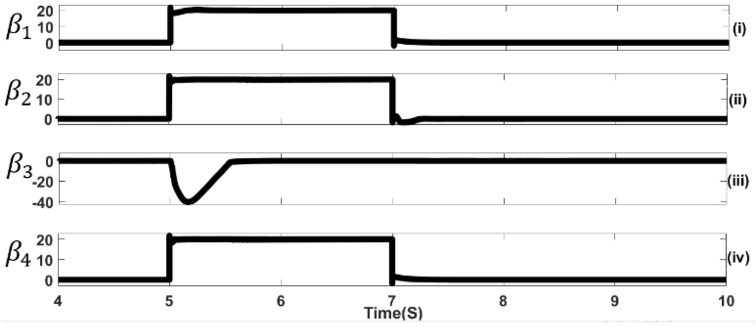
(**a**)

(**b**)

(**c**)

(**d**)

Figure 11. *Cont.*



(**e**)

Figure 11. Second case study: (**a**) v_i, (**b**) $I_{out\ i}$, (**c**) $\%Ve_i$, (**d**) $\%Ic_i$, and (**e**) voltage cyber-attack mitigation signals for DGUs, β_{i}.

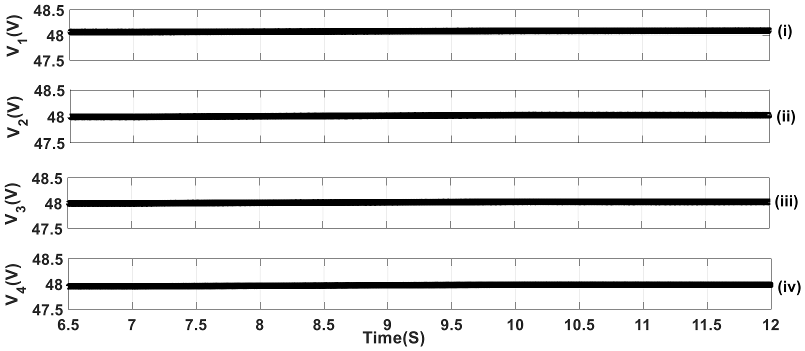
Figure 12a,b indicate that the proposed current cyber-attack mitigation layer successfully mitigates the effect of FDIAs on DGUs voltages and output currents. In addition, the percentage error in voltage and the percentage change in current sharing of each DGU are negligible as indicated in Figure 12c,d, respectively. The actions of current cyber-attack mitigation layers are presented in Figure 12e. The correction terms γ_{i} are approximately equal to −3 A to cancel out the injected false data, $I_{Fi} = +3$ A. This result makes it clear that the suggested cyber-attack mitigation layers enable the distributed secondary controllers of DGUs to sustain current sharing without cross-coupling and independent of when and where FDIA happens in meshed DC microgrid.

4.4. Sequential FDIA on Output Currents of DGUs

This case study focuses on analyzing how the suggested current cyber-attack mitigation loop behaves, which is added to the secondary control layer to protect against sequential FDIA on output current measurements of each DGU. All the DGUs are attacked at different instants, such that $I_{F1} = I_{F3} = +3$ A and $I_{F2} = I_{F4} = +2$ A, as summarized in Table 7. The intervals of FDIA on DGU1, DGU2, DGU3, and DGU4 are [8–10 s], [12–14 s], [16–18 s], and [20–22 s], respectively.

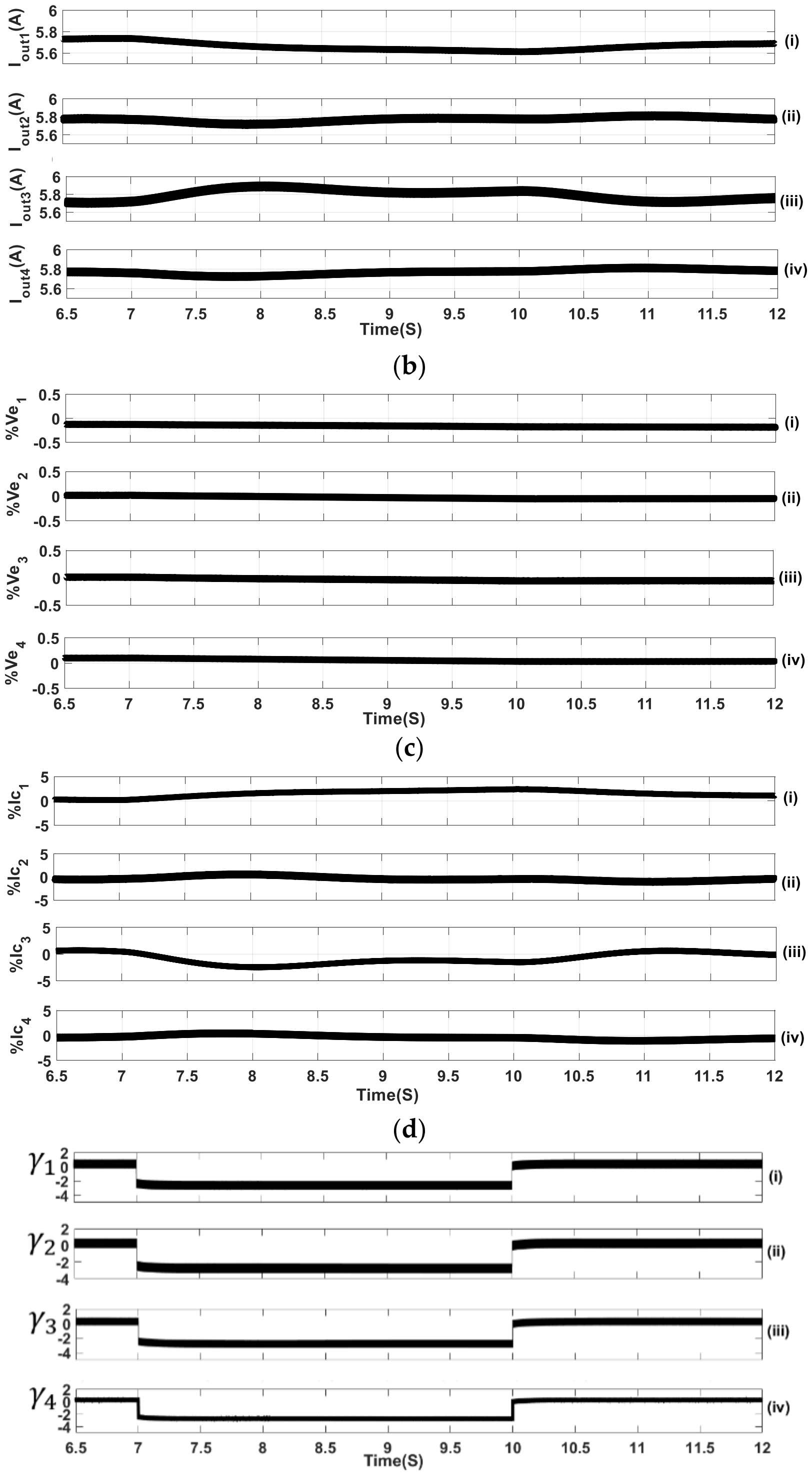
Table 7. Sequential current FDIA parameters.

DGU *i*	FDIA Value	Attack Instant
DGU *1*	$I_{F1} = +3\ A$	*t* = [8–10 s]
DGU *2*	$I_{F2} = +2\ A$	*t* = [12–14 s]
DGU *3*	$I_{F3} = +3\ A$	*t* = [16–18 s]
DGU *4*	$I_{F4} = +2\ A$	*t* = [20–22 s]



(**a**)

Figure 12. *Cont.*



(**b**)

(**c**)

(**d**)

(**e**)

Figure 12. Third case study: (**a**) v_i, (**b**) $I_{out\ i}$, (**c**) $\%Ve_i$, (**d**) $\%Ic_i$, and (**e**) current cyber-attack mitigation signals for DGUs, γ_i.

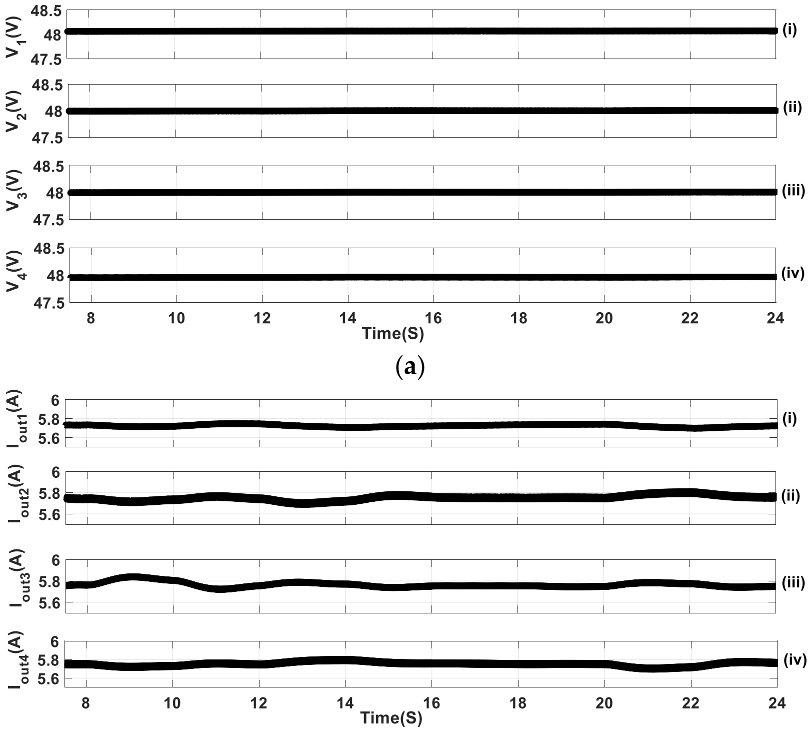
Figure 13a,b demonstrate that, with the current cyber-attack mitigation layer, all the DGU voltages are maintained at v_{ref} = 48 V, and current sharing is achieved even in the presence of FDIAs on the output current measurements. Figure 13c shows that the proposed mitigation layer succeeds to diminish percentage voltage errors. Moreover, the percentage change in currents sharing is almost negligible as shown in Figure 13d. As a result, voltage deviations are eliminated, and proper current sharing between DGUs is secured. Figure 13e portrays the correction term added by the current mitigation layer implemented in the secondary control loop of each DGU. For each DGU, it is obvious that the correction term reaches the false term, $\gamma_{\mathrm{i}} = -I_{Fi}$, which indicates that the ANNs work properly and produce accurate estimate of the DGUs currents. Moreover, there are no cross-coupling between different current cyber-attack mitigation layers. Additionally, the suggested distributed control strategy succeeds in securing the meshed DC microgrid's secondary control level.

4.5. Mixed Current and Voltage FDIAs on DGUs

The suggested current and voltage cyber-attack mitigation layers are assessed in this case study under simultaneous FDIAs on voltage and current measurements, as given in Table 8. DGU1 is exposed to FDIAs of $\alpha_1 = +5\ V$ and $I_{F1}\ = +3$ A simultaneously through the interval [7 s, 9 s]. Throughout the interval [12 s, 14 s], DGU2 is subjected to FDIAs of $\alpha_2 = +10\ V$ and $I_{F2}\ = +3$ A. During the interval [16 s, 18 s], DGU3 experiences FDIA on its terminal voltage of $\alpha_3 = -10\ V$, and at the same instant, the output current of DGU4 is attacked by $I_{F4} = +3$ A.

Table 8. Mixed current and voltage FDIA parameters.

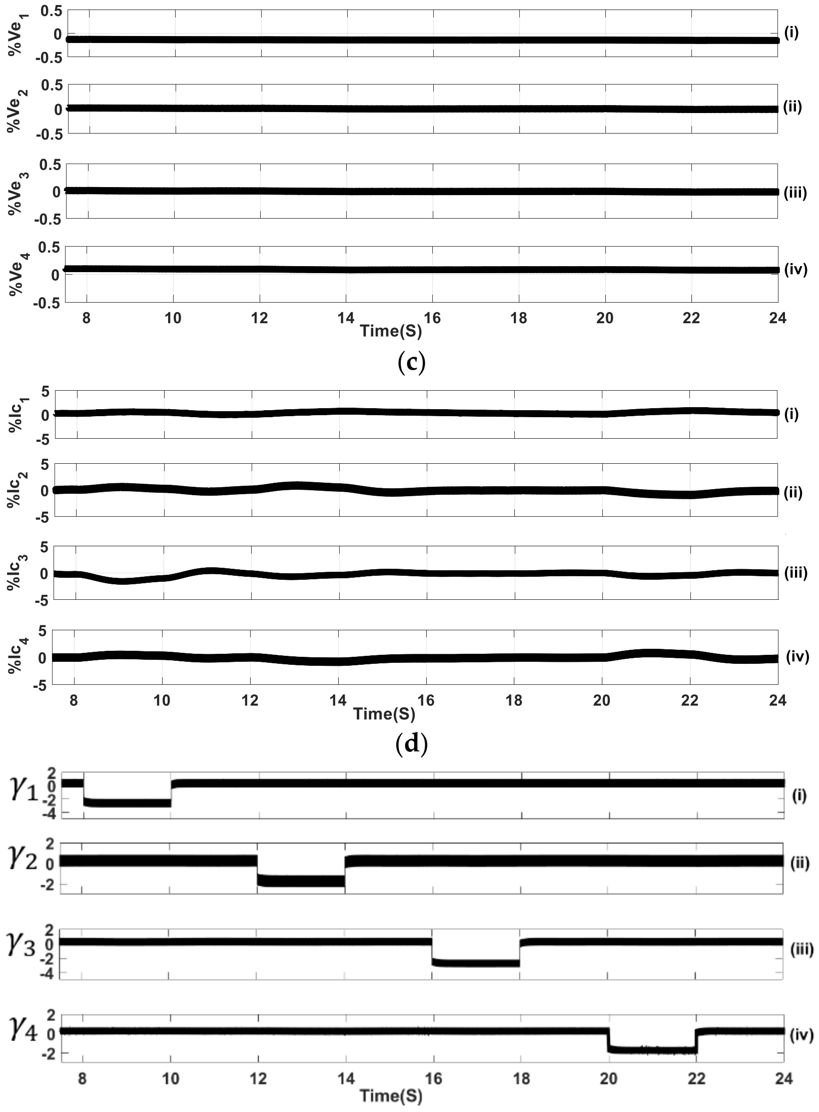
DGU *i*	FDIA Value	Attack Instant
DGU *1*	$I_{F1}\ = +3\ A$ $\alpha_1 = +5\ V$	*t* = [7–9 s]
DGU *2*	$I_{F2}\ = +3\ A$ $\alpha_2 = +10\ V$	*t* = [12–14 s]
DGU *3*	$\alpha_3 = -10\ V$	*t* = [16–18 s]
DGU *4*	$I_{F4}\ = +3\ A$	*t* = [16–18 s]



(**a**)

(**b**)

Figure 13. *Cont.*



(**c**)

(**d**)

(**e**)

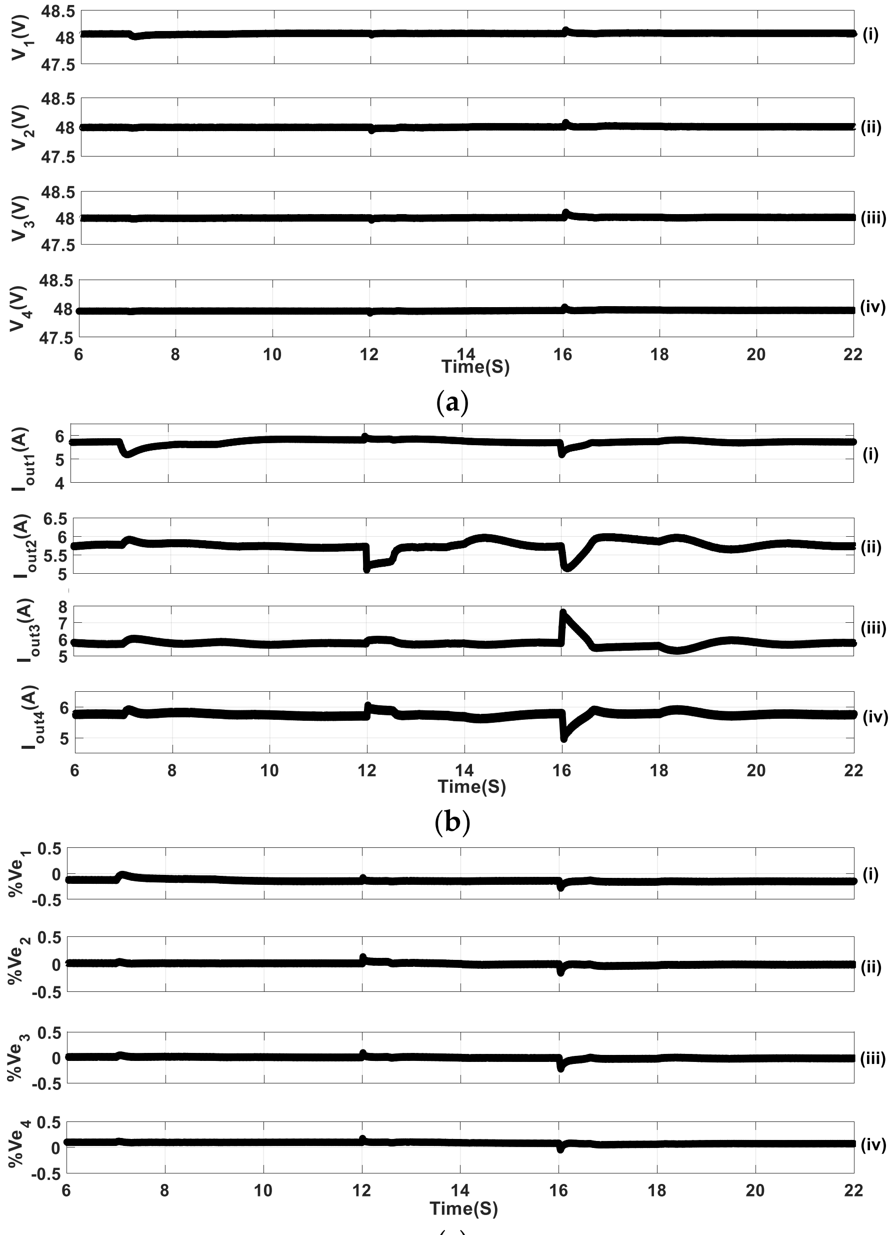
Figure 13. Fourth case study: (**a**) v_i, (**b**) $I_{out\ i}$, (**c**) $\%Ve_i$, (**d**) $\%Ic_i$, and (**e**) current cyber-attack mitigation signals for DGUs, γ_{i}.

Figure 14 indicates that, even when both attacks take place simultaneously on a single DGU or on two distinct DGUs, the voltage and current cyber-attack detection and mitigation layers work as intended. As can be observed from Figure 14a,b, voltages of all DGUs are tightly regulated regardless of the cyber-attacks and decent current sharing is maintained. DGUs voltages and currents errors are shown in Figure 14c,d, respectively. It can be revealed that there is an interaction between the voltage and current cyber-attack mitigation layers, as the percentage error of the current sharing is not totally compensated. The correction terms β_{i} and γ_{i} to mitigate the effects of voltage and current cyber-attacks are shown in Figure 14e,f, respectively. The values of these correction terms reveal that the ANNs are working appropriately, as they all generate terms that oppose the corresponding FDIA erroneous term.

The performance metrics of all case studies is summarized in Table 9, which indicates that the percentage voltage error and percentage change in current sharing is kept reasonable during cyber-attacks.

Table 9. Performance metrics for all case studies during cyber-attacks.

Case Study	Average Percentage Voltage Error $(\%Ve_i)$	Average Percentage Change in Current Sharing $(\%Ic_i)$
Sequential voltage attack	$\%Ve \approx 0.1\%$	$\%Ic \approx 10\%$
Simultaneous voltage attack	$\%Ve \approx 1\%$	$\%Ic \approx 10\%$
Simultaneous current attack	$\%Ve \approx 0\%$	$\%Ic \approx 2\%$
Sequential current attack	$\%Ve \approx 0\%$	$\%Ic \approx 0\%$
Mixed current & voltage attack	$\%Ve \approx 0.2\%$	$\%Ic \approx 5\%$

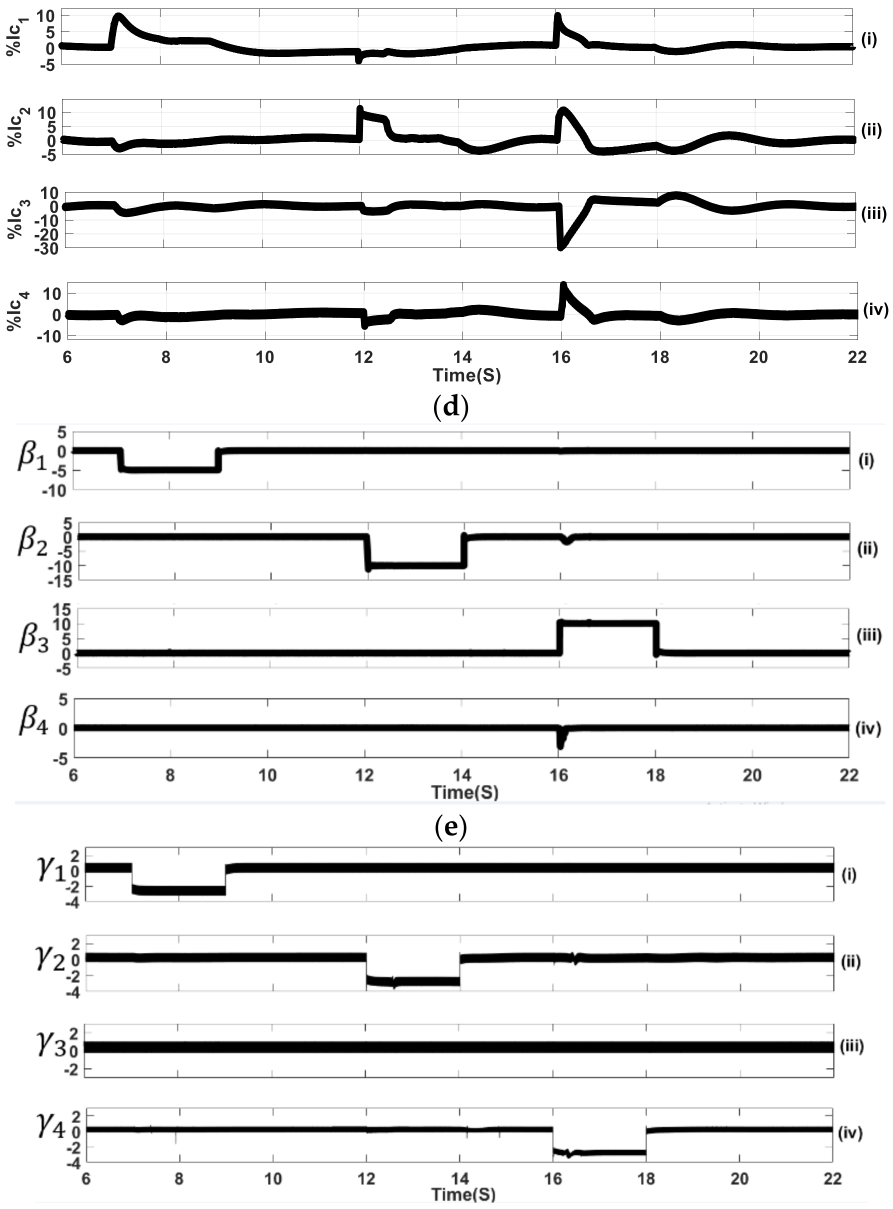


(**a**)

(**b**)

(**c**)

Figure 14. *Cont.*



(**d**)

(**e**)

(**f**)

Figure 14. Fifth case study: (**a**) v_i, (**b**) $I_{out\ i}$, (**c**) $\%Ve_i$, (**d**) $\%Ic_i$, (**e**) voltage cyber-attack mitigation signals for DGUs, β_{i}, and (**f**) current cyber-attack mitigation signals for DGUs, γ_{i}.

5. Experimental Verification

The DC microgrid system with the proposed mitigation strategy is evaluated experimentally using Typhoon Hardware in the Loop (HIL 402) with Dspace Microlab Box (RTI 1202). The test setup is shown in Figure 15. The DGUs are built on the Typhoon HIL and communications are conducted between the Typhoon HIL and Dspace to convey the measurements needed for the control strategy. The Dspace is utilized to implement the entire control strategy. The measurements are displayed using a Fluke scope, and Fluke view software is used to display the Fluke scope results where Channel 1 (Red): DGU1, Channel 2 (Blue): DGU2, Channel 3 (Black): DGU3, and finally, Channel 4 (Green): DGU4.

5.1. Sequential FDIA Voltage Attack

In this case study, a FDIA is carried out on each DGU sequentially as follows: DGU1 voltage measurement is attacked by +20 V, then a +10 V is added to DGU2 voltage, followed by an attack of + 5 V on DGU3, and finally, DGU4 is subjected to +10 V attack. The time span of each attack is 4 s.

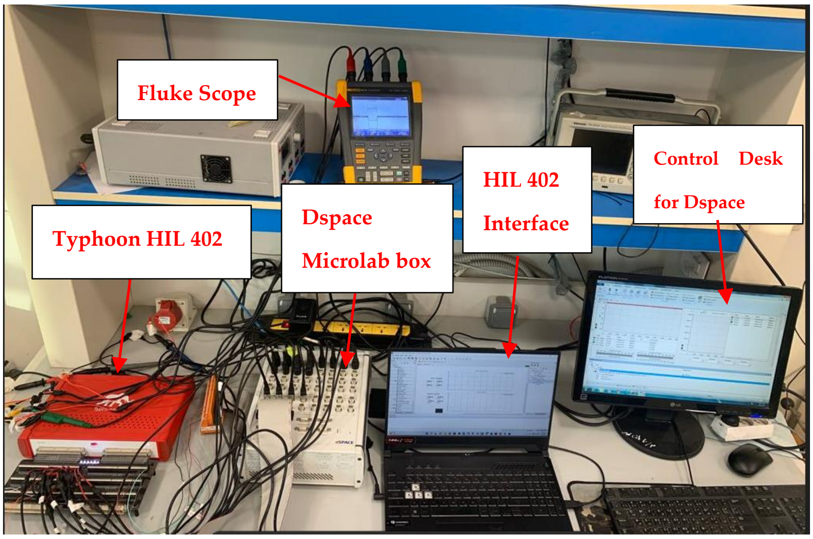


Figure 15. Experimental setup.

Figure 16 demonstrates that the voltage of each DGU is following the reference 48 V even in the presence of sequential FDIAs on the voltage measurements, which confirms that the voltage cyber-attack mitigation layer succeeded in canceling the voltage attack effect. Figure 17 shows the output currents of each DGU. The mitigation strategy managed to keep proper current sharing regardless of the attack value and instant. At the instant of applying FDIA on a DGU, its output current is disturbed and then reaches steady state eventually as indicated. The mitigation signals that cancel out the attack on DGUs are given in Figure 18. Each mitigation layer PI controller generates a correction term that matches the corresponding attack, as indicated.

5.2. Mixed FDIA Voltage Attack

In this experiment, the microgrid system is exposed to a more aggressive attack. The attacker executes both sequential and simultaneous voltage attacks, attacking DGU1 and DGU2 sequentially and DGU3 and DGU4 at the same time. DGU1 is attacked by +10 V, followed by a +15 V FDIA on DGU2; afterwards, DGU3 and DGU4 are subjected to +5 V and +10 V FDIAs, respectively, at the same instant.

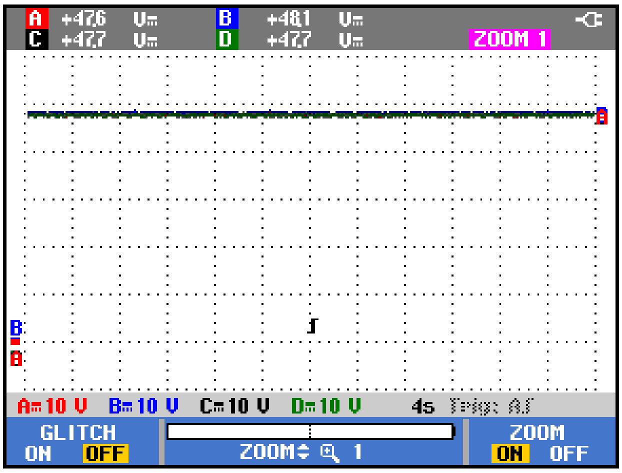


Figure 16. DGU voltages during sequential voltage attacks.

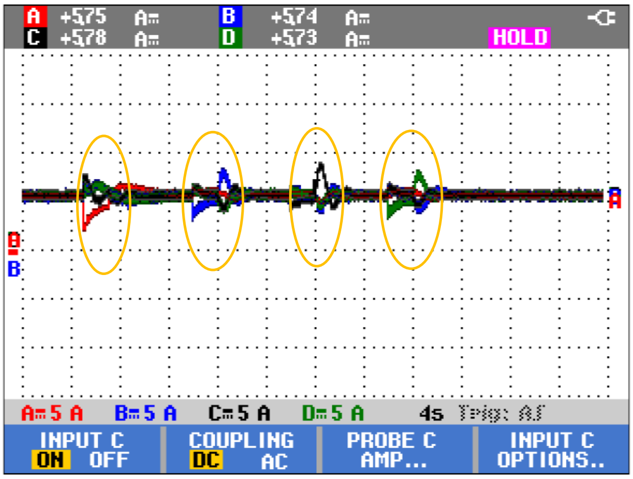


Figure 17. DGUs output currents during sequential voltage attacks.

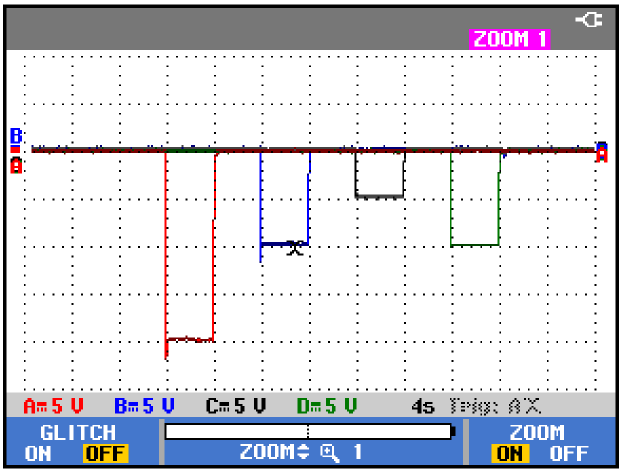


Figure 18. Mitigation signals during sequential voltage attacks.

As shown in Figure 19, the voltage is kept constant, regardless any FDIA on the system. Figure 20 presents the output currents of each DGU, where current sharing between the DGUs is still performed. Finally, the mitigation signals are given in Figure 21. It can be seen that the DGU2 mitigation layer is excited when the last attack is removed but vanishes after a short time and does not affect the DGU voltages or currents.

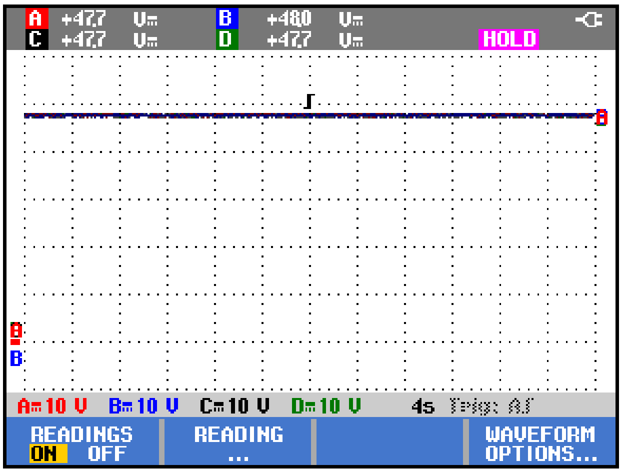


Figure 19. DGUs voltages during mixed voltage attacks.

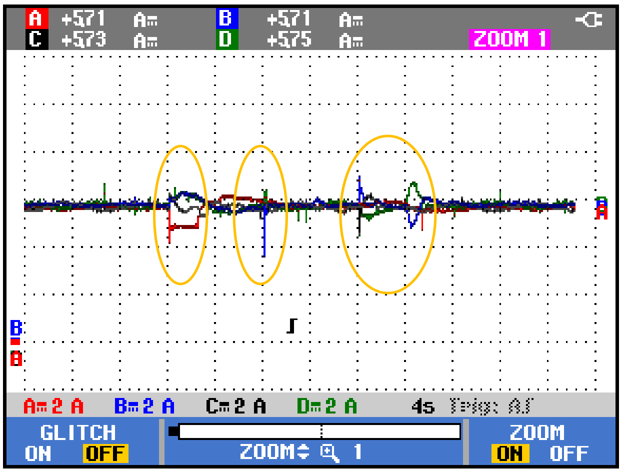


Figure 20. DGUs output currents during mixed voltage attacks.

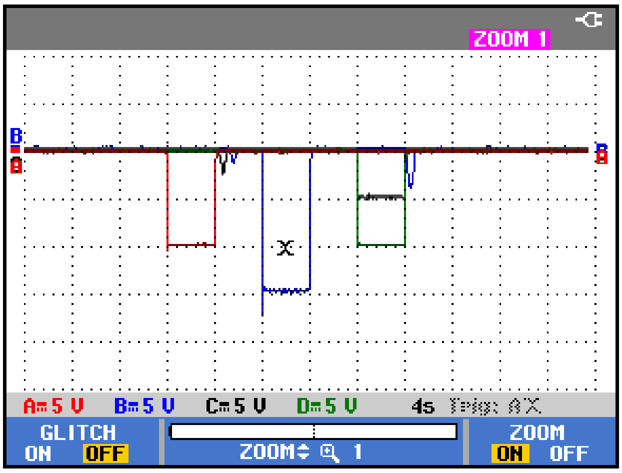


Figure 21. Mitigation signals during mixed voltage attacks.

5.3. Sequential FDIA Current Attack

In this case study, the dynamic performance of the proposed system under sequential FDIAs on current measurements is evaluated. Firstly, DGU1 is attacked by +10 A; afterwards, DGU2 with −5 A, then DGU3 with +5 A, and finally, the DGU4 current measurement is falsified by −10 A, where each attack last for four seconds. The DGU voltages are tightly regulated at their set values, as demonstrated in Figure 22. In addition, Figure 23 illustrates that the current sharing loop is still achieving equal current sharing between DGUs. Moreover, Figure 24 indicates the mitigation signals produced by the current mitigation layer, where each layer generates a value opposing the attack value on its corresponding DGU without cross-coupling.

5.4. Simultaneous FDIA Current Attack

This case study is dedicated to test the behavior of the proposed system when all DGUs' output currents measurements, which are used in the secondary controller, are attacked by +5 A at the same instant for eight seconds. The results of Figures 25 and 26 demonstrates that neither the DGUs' output currents nor voltages are impacted by the attacks. This action is due to the fast response and accurate performance of the current mitigation layers which instantaneously correct the attacked measurements by injecting −5 A during the attack interval, as demonstrated in Figure 27.

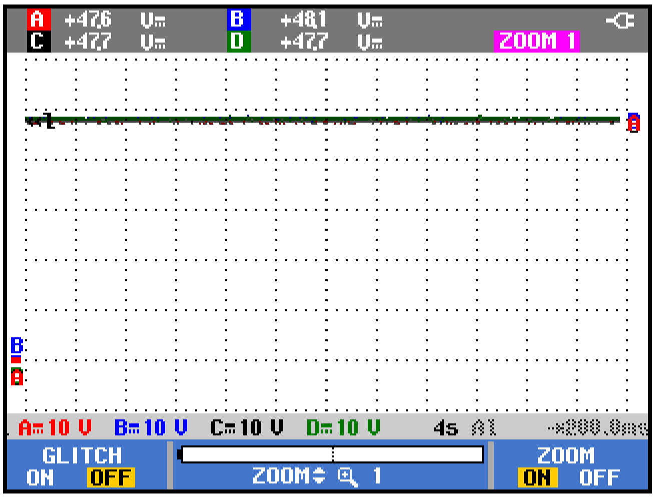


Figure 22. Voltages during sequential current attacks.

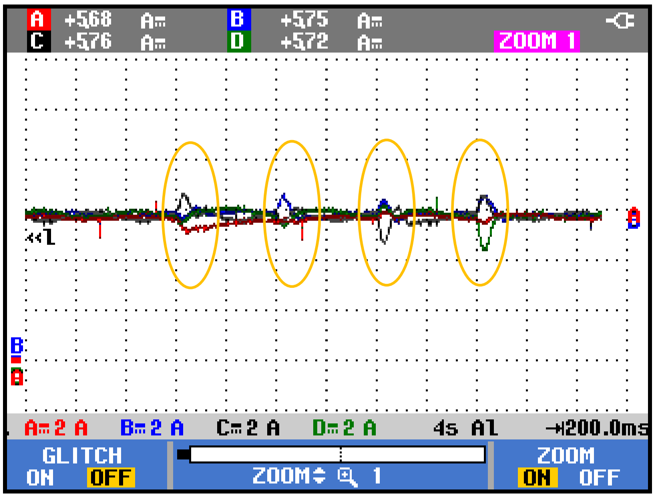


Figure 23. Output currents during sequential current attacks.

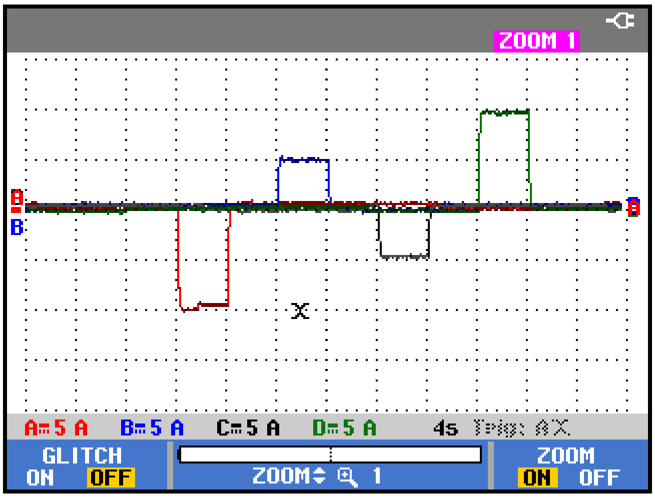
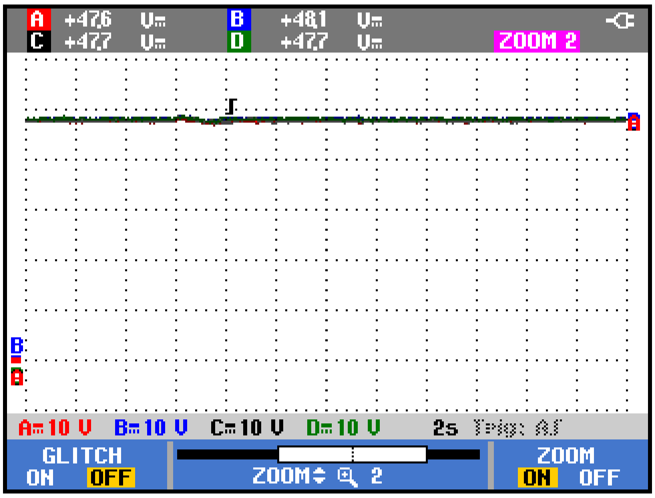


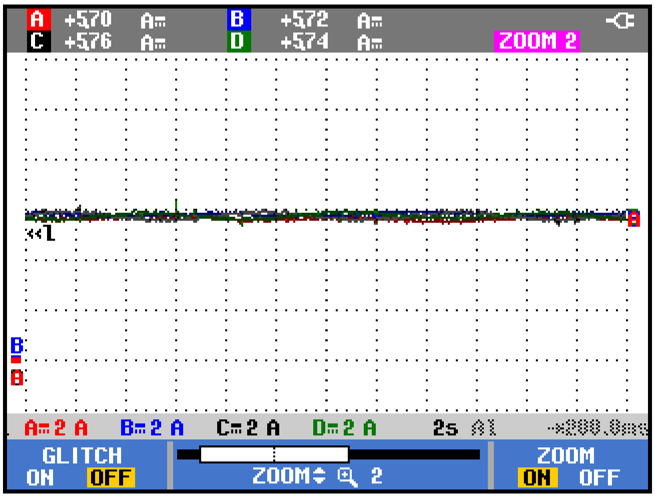
Figure 24. Mitigation signals during sequential current attacks.



A +47.6 V= B +48.1 V=
C +47.7 V= D +47.7 V=

A=10 V B=10 V C=10 V D=10 V 2s Trig: A

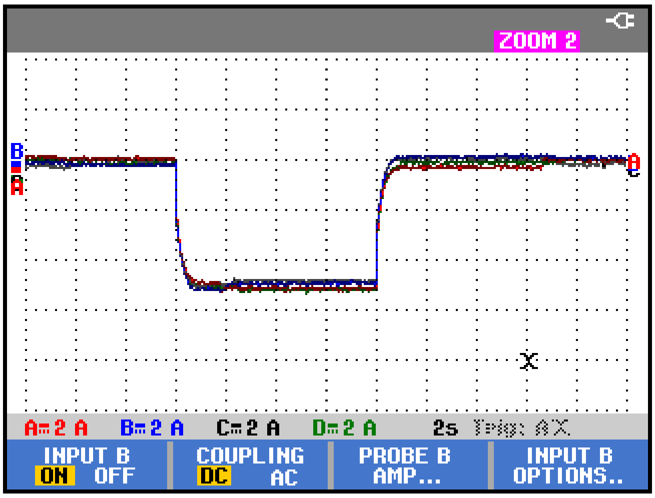
Figure 25. Voltages during simultaneous current attacks.



A +5.70 A= B +5.72 A=
C +5.76 A= D +5.74 A=

A=2 A B=2 A C=2 A D=2 A 2s A →200.0ms

Figure 26. Output currents during simultaneous current attacks.



A=2 A B=2 A C=2 A D=2 A 2s Trig: A

Figure 27. Mitigation signals during simultaneous current attacks.

6. Conclusions

This paper introduces distributed voltage and current cyber-attack detection and mitigation layers based on an ANN trained with Levenberg–Marquardt optimization as the backpropagation algorithm. The control system is updated to create an advanced power system by adding voltage and current cyber-attack detection and mitigation layers to the primary and secondary loops of each DGU in a meshed DC microgrid with a distributed control strategy. As a result, the proposed updated nonlinear control technique considers both voltage and current cyber-attacks simultaneously. Furthermore, a droop-less control method is employed to eliminate the droop control disadvantages such as subpar dynamic performance. To investigate the performance of the proposed cyber-attack layers, different case studies are conducted. The results concluded that the two layers succeeded in mitigating the effect of FDIAs on both voltage and current measurements. As a result, the proposed system managed to keep proper operation of the current sharing loop and voltage regulation loop regardless of the presence of FDIAs. In addition, there is no cross-coupling between the different voltage or current cyber-attack mitigation layers used for DGUs. Moreover, the proposed distributed scheme succeeds to secure the primary and secondary control levels of the meshed DC microgrid. The simulation and experimental findings of the proposed control approach verify the accurate operation of DC microgrids even in the presence of cyber-attacks on the measurements used for the control strategy. Additionally, the control technique is successful to diminish the maximum voltage error and maximum current sharing error between 1% and 10%, respectively. However, results show that if the voltage and current are simultaneously imposed to FDIA, the percentage error of the current sharing is not totally compensated. For future work, the proposed distributed cyber-attacks mitigation layers will be studied to enhance the current sharing accuracy when voltage and current measurements are simultaneously exposed to cyber-attacks.

Author Contributions: Conceptualization, M.I.M.; methodology, M.I.M. and M.A.A.; software, A.H.E.-E.; validation, A.H.E.-E., F.H.A. and A.M.M.; formal analysis, M.M.; investigation, M.M.; resources, M.I.M.; data curation, M.M.; writing—original draft preparation, A.H.E.-E.; writing—review and editing, M.I.M., M.A.A. and A.H.E.-E.; visualization, A.H.E.-E. and M.M.; supervision, M.I.M.; and project administration, M.I.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Nomenclature

Abbreviations

DGU	Distributed Generator Unit.
FDIA	False Data Injection Attack.
ANN	Artificial Neural Network.
RESs	Renewable Energy Sources.
ESSs	Energy Storage Systems.
EVs	Electric Vehicles.
MGs	Microgrids.
PV	Photovoltaic.
DOS	Denial of Service.
RNN	Recurrent Neural Network.
NARX	Nonlinear Autoregressive Exogenous.
MPC	Model Predictive Control.
CBs	Circuit Breakers.
LMI	Linear Matrix Inequality.
MSE	Mean Square Error.
HIL	Hardware In the Loop.

Variables and Parameters

v_i	DGU*i* terminal voltage after LC filter.
v_{ti}	DGU*i* terminal voltage before LC filter.

I_{ti}	DGU*i* inductor current.
I_{li}	DGU*i* local load current.
L_{ti}	DGU*i* LC filter inductance.
C_{ti}	DGU*i* LC filter capacitance.
R_{ti}	DGU*i* terminal resistance.
R_{ij}	Resistance of the line connecting DGUs *i* and j.
L_{ij}	Inductance of the line connecting DGUs *i* and j.
$x_{[i]}(t)$	State vector.
$u_{[i]}(t)$	Control action input to the DGU*i* system.
$d_{[i]}(t)$	External input.
$\xi_{[i]}(t)$	Vector represents the coupling of DGU*i* with each neighboring DGU*j*.
$y_{[i]}(t)$	Measured output vector.
$z_{[i]}(t)$	Controlled output variable.
v_{refi}	Reference voltage of DGU*i*.
D	Duty cycle of the buck converter.
$\mathrm{e}_{[\mathrm{i}]}(\mathrm{t})$	Steady state error of the controlled variable.
v_{i}	Dynamics of the integrator effect.
$x^{u}_{[i]}(\mathrm{t})$	Updated state vector after adding the integrator dynamics.
$d^{u}_{[i]}(\mathrm{t})$	Updated external input after adding the integrator dynamics.
$\xi^{u}_{[i]}(\mathrm{t})$	Updated vector representing the coupling of DGU*i* with each neighboring DGU*j*, after adding the integrator dynamics.
$y^{u}_{[i]}(\mathrm{t})$	Updated measured output vector after adding the integrator dynamics.
$z^{u}_{[i]}(t)$	Updated controlled output variable after adding the integrator dynamics.
V_{dc}	Input voltage of the buck converter.
k_i	Primary controller gain.
k_{Ii}	Secondary controller gain.
I_{outi}	DGU*i* injected output current.
Δv_i	Correction term generated by secondary controller.
v_i^{a}	Manipulated voltage of DGU*i*.
α_i	False injected term to voltage measurement of DGU*i*.
$v_{i\ ss}$	The final steady state value of v_i.
I^{a}_{outi}	Manipulated output current of DGU*i*.
I_{Fi}	False injected term to output current measurement of DGU*i*.
$\theta_i(t)$	Corrected voltage measurement of DGU*i*.
$\beta_i(t)$	Voltage attack mitigation signal.
$I_{In\ i}$	Input current of DGU*i*.
e_{vi}	DGU*i* voltage error.
$\overline{v}_i$	Estimated terminal voltage of DGU*i*.
$\overline{I}_{out\ i}$	Estimated output current of DGU*i*.
$\mu_i(t)$	Corrected current measurement of DGU*i*.
$\gamma_i(t)$	Current attack mitigation signal.
Y_i	Target output of the ANN.
$\hat{Y}_i$	Estimated output of the ANN.
$\%Ve_i$	Percentage voltage error DGU*i*.
$\%\ Ic_i$	Percentage change in current sharing for DGU*i*.
I_{es}	Equal current sharing value.

References

1. Dragičević, T.; Lu, X.; Vasquez, J.C.; Guerrero, J.M. DC Microgrids—Part I: A Review of Control Strategies and Stabilization Techniques. *IEEE Trans. Power Electron.* **2016**, *31*, 4876–4891.
2. Lee, H.; Kang, J.-W.; Choi, B.-Y.; Kang, K.-M.; Kim, M.-N.; An, C.-G.; Yi, J.; Won, C.-Y. Energy Management System of DC Microgrid in Grid-Connected and Stand-Alone Modes: Control, Operation and Experimental Validation. *Energies* **2021**, *14*, 581. [CrossRef]

3. Aluko, A.; Swanson, A.; Jarvis, L.; Dorrell, D. Modeling and Stability Analysis of Distributed Secondary Control Scheme for Stand-Alone DC Microgrid Applications. *Energies* **2022**, *15*, 5411. [CrossRef]
4. Lema, M.; Pavon, W.; Ortiz, L.; Asiedu-Asante, A.B.; Simani, S. Controller Coordination Strategy for DC Microgrid Using Distributed Predictive Control Improving Voltage Stability. *Energies* **2022**, *15*, 5442. [CrossRef]
5. Mokhtar, M.; Marei, M.I.; El-Sattar, A.A. A control scheme for islanded and grid-connected DC microgrids. In Proceedings of the 2017 19th International IEEE Middle East Power Systems Conference (MEPCON), Cairo, Egypt, 19–21 December 2017; pp. 176–180.
6. Meng, L.; Shafiee, Q.; Trecate, G.F.; Karimi, H.; Fulwani, D.; Lu, X.; Guerrero, J.M. Review on Control of DC Microgrids and Multiple Microgrid Clusters. *IEEE J. Emerg. Sel. Top. Power Electron.* **2017**, *5*, 928–948.
7. Kumar, R.; Pathak, M.K. Distributed droop control of dc microgrid for improved voltage regulation and current sharing. *IET Renew. Power Gener.* **2020**, *14*, 2499–2506. [CrossRef]
8. Mokhtar, M.; Marei, M.I.; El-Sattar, A.A. Improved current sharing techniques for DC microgrids. *Electr. Power Compon. Syst.* **2018**, *46*, 757–767. [CrossRef]
9. Tucci, M.; Meng, L.; Guerrero, J.M.; Trecate, G.F. Stable current sharing and voltage balancing in DC microgrids: A consensus-based secondary control layer. *Automatica* **2018**, *95*, 1–13. [CrossRef]
10. Mohamed, S.; Mokhtar, M.; Marei, M.I. An Adaptive Control of Remote Hybrid Microgrid based on the CMPN Algorithm. *Electr. Power Syst. Res.* **2022**, *213*, 108793. [CrossRef]
11. Sahoo, S.; Mishra, S.; Peng, J.C.-H.; Dragičević, T. A Stealth Cyber-Attack Detection Strategy for DC Microgrids. *IEEE Trans. Power Electron.* **2019**, *34*, 8162–8174. [CrossRef]
12. Beg, O.A.; Johnson, T.T.; Davoudi, A. Detection of False-Data Injection Attacks in Cyber-Physical DC Microgrids. *IEEE Trans. Ind. Inform.* **2017**, *13*, 2693–2703. [CrossRef]
13. Kosut, O.; Jia, L.; Thomas, R.J.; Tong, L. Malicious Data Attacks on the Smart Grid. *IEEE Trans. Smart Grid* **2011**, *2*, 645–658. [CrossRef]
14. Xie, L.; Mo, Y.; Sinopoli, B. Integrity Data Attacks in Power Market Operations. *IEEE Trans. Smart Grid* **2011**, *2*, 659–666. [CrossRef]
15. Bobba, R.B.; Rogers, K.M.; Wang, Q.; Khurana, H.; Nahrstedt, K.; Overbye, J. Detecting false data injection attacks on DC state estimation. In Proceedings of the Preprints 1st Workshop Secure Control Systems (CPSWEEK), Stockholm, Sweden, 12 April 2010; pp. 1–9.
16. Habibi, M.R.; Baghaee, H.R.; Dragičević, T.; Blaabjerg, F. False Data Injection Cyber-Attacks Mitigation in Parallel DC/DC Converters Based on Artificial Neural Networks. *IEEE Trans. Circuits Syst. II Express Briefs* **2021**, *68*, 717–721. [CrossRef]
17. Sahoo, S.; Peng, J.C.; Devakumar, A.; Mishra, S.; Dragičević, T. On Detection of False Data in Cooperative DC Microgrids—A Discordant Element Approach. *IEEE Trans. Ind. Electron.* **2020**, *67*, 6562–6571. [CrossRef]
18. Beg, O.A.; Nguyen, L.V.; Johnson, T.T.; Davoudi, A. Signal Temporal Logic-Based Attack Detection in DC Microgrids. *IEEE Trans. Smart Grid* **2019**, *10*, 3585–3595. [CrossRef]
19. Habibi, M.R.; Sahoo, S.; Rivera, S.; Dragičević, T.; Blaabjerg, F. Decentralized Coordinated Cyberattack Detection and Mitigation Strategy in DC Microgrids Based on Artificial Neural Networks. *IEEE J. Emerg. Sel. Top. Power Electron.* **2021**, *9*, 4629–4638. [CrossRef]
20. Gallo, A.J.; Turan, M.S.; Nahata, P.; Boem, F.; Parisini, T.; Ferrari-Trecate, G. Distributed Cyber-Attack Detection in the Secondary Control of DC Microgrids. In Proceedings of the 2018 European Control Conference (ECC), Limassol, Cyprus, 12–15 June 2018; pp. 344–349.
21. Gallo, A.J.; Turan, M.S.; Boem, F.; Parisini, T.; Ferrari-Trecate, G. A Distributed Cyber-Attack Detection Scheme with Application to DC Microgrids. *IEEE Trans. Autom. Control* **2020**, *65*, 3800–3815. [CrossRef]
22. Zhang, D.; Zhang, C. A NDO Based Attack Detection Observer and Isolation Strategy in Distributed DC Microgrid with FDIA. *J. Phys. Conf. Ser.* **2021**, *1754*, 012011. [CrossRef]
23. Shi, D.; Lin, P.; Wang, Y.; Chu, C.-C.; Xu, Y.; Wang, P. Deception Attack Detection of Isolated DC Microgrids Under Consensus-Based Distributed Voltage Control Architecture. *IEEE J. Emerg. Sel. Top. Circuits Syst.* **2021**, *11*, 155–167. [CrossRef]
24. Habibi, M.R.; Baghaee, H.R.; Dragičević, T.; Blaabjerg, F. Detection of False Data Injection Cyber-Attacks in DC Microgrids Based on Recurrent Neural Networks. *IEEE J. Emerg. Sel. Top. Power Electron.* **2021**, *9*, 5294–5310. [CrossRef]
25. Cecilia, A.; Sahoo, S.; Dragičević, T.; Costa-Castelló, R.; Blaabjerg, F. Detection and Mitigation of False Data in Cooperative DC Microgrids With Unknown Constant Power Loads. *IEEE Trans. Power Electron.* **2021**, *36*, 9565–9577. [CrossRef]
26. Habibi, M.R.; Baghaee, H.R.; Blaabjerg, F.; Dragicevic, T. Secure MPC/ANN-Based False Data Injection Cyber-Attack Detection and Mitigation in DC Microgrids. *IEEE Syst. J.* **2021**, *16*, 1487–1498. [CrossRef]
27. Yan, J.; Tang, B.; He, H. Detection of false data attacks in smart grid with supervised learning. In Proceedings of the International Joint Conference on Neural Networks (IJCNN), Vancouver, BC, Canada, 24–29 July 2016; pp. 1395–1402.
28. Demertzis, K.; Iliadis, L.S.; Anezakis, V.-D. An innovative soft computing system for smart energy grids cybersecurity. *Adv. Build. Energy Res.* **2018**, *12*, 3–24. [CrossRef]
29. Nejabatkhah, F.; Li, Y.W.; Liang, H.; Reza Ahrabi, R. Cyber-Security of Smart Microgrids: A Survey. *Energies* **2021**, *14*, 27. [CrossRef]
30. Ma, L.; Xu, G. Distributed Resilient Voltage and Reactive Power Control for Islanded Microgrids under False Data Injection Attacks. *Energies* **2020**, *13*, 3828. [CrossRef]

31. Mbungu, N.T.; Naidoo, R.M.; Bansal, R.C.; Vahidinasab, V. Overview of the Optimal Smart Energy Coordination for Microgrid Applications. *IEEE Access* **2019**, *7*, 163063–163084. [CrossRef]
32. Fortuna, L.; Buscarino, A. Nonlinear Technologies in Advanced Power Systems: Analysis and Control. *Energies* **2022**, *15*, 5167. [CrossRef]
33. Tucci, M.; Riverso, S.; Vasquez, J.C.; Guerrero, J.M.; Ferrari-Trecate, G. A Decentralized Scalable Approach to Voltage Control of DC Islanded Microgrids. *IEEE Trans. Control. Syst. Technol.* **2016**, *24*, 1965–1979. [CrossRef]
34. Tucci, M.; Meng, L.; Guerrero, J.M.; Ferrari-Trecate, G. *Consensus Algorithms and Plug-and-Play Control for Current Sharing in DC Microgrids*; Technical Report; IGM Institute of Mechanical Engineering: Lausanne, Switzerland, 2016.
35. El-Ebiary, A.H.; Attia, M.A.; Marei, M.I.; Sameh, M.A. An Integrated Seamless Control Strategy for Distributed Generators Based on a Deep Learning Artificial Neural Network. *Sustainability* **2022**, *14*, 13506. [CrossRef]
36. Lv, C.; Xing, Y.; Zhang, J.; Na, X.; Li, Y.; Liu, T.; Cao, D.; Wang, F. Levenberg–Marquardt Backpropagation Training of Multilayer Neural Networks for State Estimation of a Safety-Critical Cyber-Physical System. *IEEE Trans. Ind. Inform.* **2018**, *14*, 3436–3446. [CrossRef]