Decentralized Coordinated Cyberattack Detection and Mitigation Strategy in DC Microgrids Based on Artificial Neural Networks

Mohammad Reza Habibi, *Student Member, IEEE*, Subham Sahoo, *Member, IEEE*, Sebastián Rivera, *Senior Member, IEEE*, Tomislav Dragičević, *Senior Member, IEEE*, and Frede Blaabjerg, *Fellow, IEEE*

***Abstract*— DC microgrids can be considered as cyber-physical systems (CPSs) and they are vulnerable to cyberattacks. Therefore, it is highly recommended to have effective plans to detect and remove cyberattacks in dc microgrids. This article shows how artificial neural networks can help to detect and mitigate coordinated false data injection attacks (FDIAs) on current measurements as a type of cyberattacks in dc microgrids. FDIAs try to inject the false data into the system to disrupt the control application, which can make the dc microgrid shutdown. The proposed method to mitigate FDIAs is a decentralized approach and it has the capability to estimate the value of the false injected data. In addition, the proposed strategy can remove the FDIAs even for unfair attacks with high domains on all units at the same time. The proposed method is tested on a detailed simulated dc microgrid using the MATLAB/Simulink environment. Finally, real-time simulations by OPAL-RT on the simulated dc microgrid are implemented to evaluate the proposed strategy.**

***Index Terms*— Artificial neural networks, cyberattack mitigation, dc microgrid, false data injection attack (FDIA).**

I. Introduction

DC MICROGRIDS are more efficient with less control complexity compared with ac microgrids [1]–[4] and its operation can be further improved by coordination between the sources using communication. Based on the communication networks, two typical communication topologies exist in dc microgrids, i.e., centralized and distributed [5]. Although centralized methods are simple to implement, their performance impedes due to single point of failure [6]. As a result, the reliability of operation becomes very poor for centralized systems. On the other hand, distributed control enhances the reliability and flexibility of operation since the information is being shared only between the neighbors. As a result, it becomes robust to limited communication delays and link failure. Also, it can be flexible to plug-and-play capability. However, since global information is inadequate, it is highly vulnerable to cyberattacks. This has been a primary concern for autonomous systems used in mission-critical applications, such as electric ships, aircrafts, and telecommunication centers [7]–[10].

Recently, cooperative and consensus-based distributed control strategies are applied in dc microgrids applications [7], [11]–[13]. The objectives of cooperative control in dc microgrids are to regulate the average voltage and also proportional sharing of the currents by using local and neighbor's data [13], [14]. In cooperative control strategies, since dc microgrids only exchange information between the neighbors, the global information is missing. As a result, cooperative dc microgrids are highly vulnerable to cyberattacks [15]. There are various kinds of cyberattacks, such as denial-of-service (DoS) attacks, replay attacks, and false data injection attacks (FDIAs). DoS attacks attempt for unavailability of the communication network, whereas FDIAs inject the false data into the system to change the state of the system and replay attacks record the reading of sensors for a given time, and then, it repeats those readings to defraud the operator of the system [14], [16]–[20]. This article investigates the most prominent attack, i.e., FDIAs. The generalized FDIAs usually are recognized as stealth attacks can inject the false data into the system without any disturbances by deceiving the control application leaving the operator uninformed about the online attack in this case [14], [21]. After penetration into the control system, the attacker can cause the dc microgrid shutdown by increasing the magnitude of attacked elements in an unfair manner. To protect the system from such events, it is vital to design a resilient strategy to remove the FDIA elements in dc microgrids.

This article introduces a method to determine the value of the false data in cooperative dc microgrids and remove the FDIA from the dc microgrid. The goal is to show how artificial neural networks can be implemented as a powerful tool to mitigate the false data into cooperative dc microgrids easily with very high accuracy. First, an artificial neural network-based estimator is designed to monitor the output

Manuscript received April 15, 2020; revised September 27, 2020; accepted October 20, 2020. Date of publication January 11, 2021; date of current version July 30, 2021. The work of Sebastián Rivera was supported in part by the Advanced Center in Electrical and Electronic Engineering (AC3E) Project under Grant ANID/Basal/FB0008 and in part by the Solar Energy Research Center (SERC) Project under Grant ANID/FONDAP/15110019. Recommended for publication by Associate Editor Hao Ma. *(Corresponding author: Mohammad Reza Habibi.)*

Mohammad Reza Habibi, Subham Sahoo, and Frede Blaabjerg are with the Department of Energy Technology, Aalborg University, 9220 Aalborg, Denmark (e-mail: mre@et.aau.dk; sssa@et.aau.dk; fbl@et.aau.dk).

Sebastián Rivera is with the Faculty of Engineering and Applied Sciences, Universidad de los Andes, Santiago 7620086, Chile (e-mail: s.rivera.i@ieee.org).

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

Color versions of one or more figures in this article are available at https://doi.org/10.1109/JESTPE.2021.3050851.

Digital Object Identifier 10.1109/JESTPE.2021.3050851

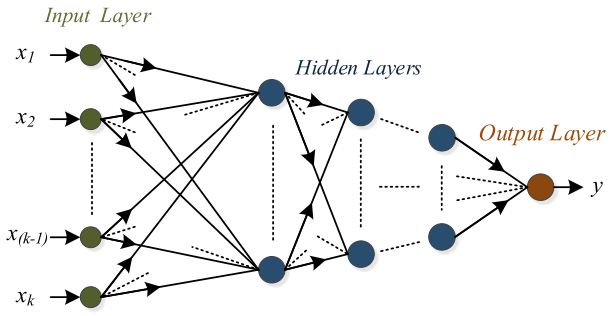


Fig. 1. General architecture of a feedforward neural network with k inputs and one output.

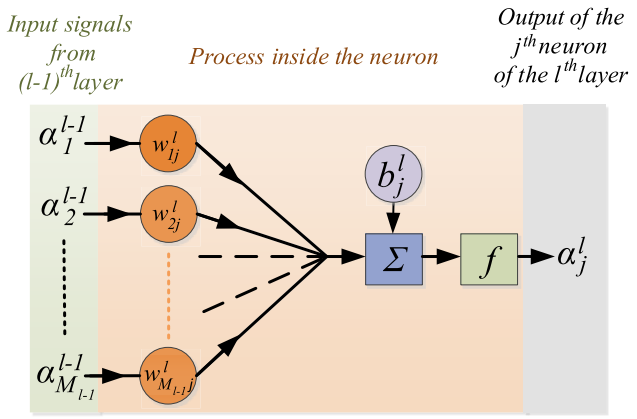


Fig. 2. Structure of the jth neuron in the lth layer of the feedforward neural network, which is shown in Fig. 1.

current of converters that connect the distributed energy resources (DERs) to the dc microgrid and based on the output of the estimator, FDIAs; also, the value of the false data can be calculated. In the next step, in regard to the calculated value of the false data, a reference tracking approach using a PI controller is introduced to mitigate the false data in the attacked converter.

The organization of the rest of this article is as follows. Section II introduces the basics of the feedforward neural networks. Section III discusses the fundamental concepts of cooperative control of dc microgrids based on the consensus theory and also the effect of FDIAs on the cooperative dc microgrids. In addition, the proposed strategy is explained in Section IV. Sections V and VI show the performance of the proposed method under offline and real-time simulations, respectively. In Section VII, a discussion about the proposed method and future work are prepared. Finally, the conclusion of this article is proposed in Section VIII.

II. Introduction to Feedforward Neural Networks

A feedforward neural network consists of an input layer with multiple inputs, one or more hidden layers, and an output layer. In the feedforward structure, each layer is built by a number of neurons, and data will propagate from neurons in one layer to another. Fig. 1 shows the general structure of a feedforward neural network.

In Fig. 1, x_i and y are the ith input and the output of the neural network, respectively. Considering the input and output layer as the first and last layers, respectively, in the neural network, Fig. 2 shows the structure of the jth neuron in the lth ($l > 1$) layer of the neural network and Table I shows the corresponding parameters of the neural network shown in Fig. 2.

The mathematical formulation mentioned in Fig. 2 is as follows:

$$\alpha_j^l = f\left(\left(\sum_{i=1}^{M_{l-1}} \alpha_i^{l-1} \times w_{rj}^l\right) + b_j^l\right). \tag{1}$$

In this article, a feedforward neural network is implemented to estimate the output dc current of converters that connect DERs to the dc microgrid. For the implementation of a feedforward neural network, two steps are considered. In the first step, the neural network is trained offline to prepare a fine-tuned neural network, and in the second step, the well-trained feedforward neural network is used to monitor and estimate the output dc current of converters. First, a feedforward neural network with one hidden layer is trained offline and then examined to estimate the output currents for several scenarios. Based on the seen proper results and avoiding complexity, a neural network with one hidden layer is considered. The mathematical description of a feedforward neural network with one hidden layer and one output is as follows:

$$\bar{y} = f_{\text{out}}\left(f_{\text{hid}}\left(XW^{\text{hid}} + b^{\text{hid}}\right)W^{\text{out}} + b^{\text{out}}\right) \tag{2}$$

where f_{hid} and f_{out} are activation functions of neurons in the hidden layer and output layer, respectively. In addition, $\bar{y}$ is the estimated output by the feedforward neural network and X is the input vector of the neural network with k inputs, which is defined as follows:

$$X = (x_1, x_2, \ldots, x_{k-1}, x_k). \tag{3}$$

Furthermore, b^{out} is the bias weight of the neuron in the output layer. Moreover, W^{hid}, W^{out}, and b^{hid} are a weight matrix of the hidden layer, weight vector of the output layer, and bias vector of the hidden layer, respectively. The aim of the offline training of the feedforward neural network is to find the optimized value of W^{hid}, W^{out}, b^{hid}, and b^{out} to have a fine-tuned neural network for estimating the output properly. To train the neural network offline, a set of input data and corresponding outputs should be prepared to be used in the training process to optimize the parameters of the feedforward neural network.

TABLE I
Parameters of Fig. 2

Parameter	Description
M_{l-1}	Number of neurons in the $(l-1)^{th}$ layer
α_j^l	Output of the j^{th} neuron from the l^{th} layer
b_j^l	Bias weight of the j^{th} neuron of the l^{th} layer
$f(.)$	Activation function of the neuron
w_{rj}^l	Connection weight between r^{th} neuron in $(l-1)^{th}$ layer and j^{th} neuron in l^{th} layer

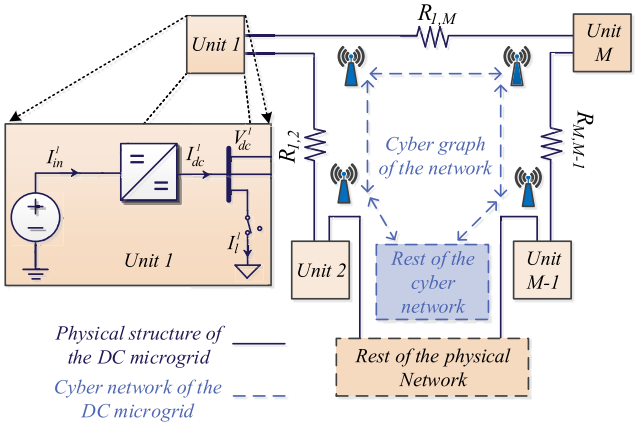


Fig. 3. Cyber-physical model of the dc microgrid with M units.

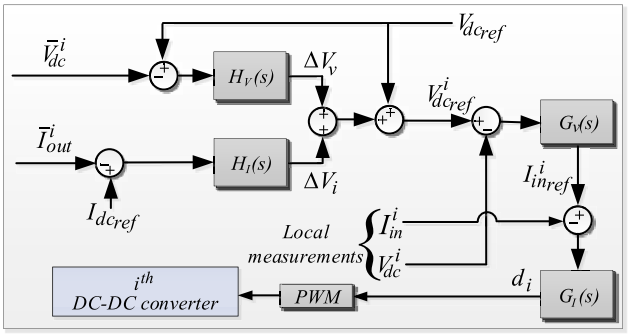


Fig. 4. Cooperative control of the dc microgrid.

III. FDIA on Cooperative Control-Based DC Microgrids

In this section, a traditional cooperative control scheme used for dc microgrids will be introduced. Furthermore, the effect of FDIAs in cooperative dc microgrids will be discussed.

A. Cooperative Control of a DC Microgrid

Fig. 3 shows a general cyber-physical model of a dc microgrid, which is studied in this article. The illustrated dc microgrid consists of M units, and each unit is a dc source that is connected to the dc microgrid by a dc–dc converter with equal power rating for all of the converters. Each converter works to restore the voltage as per the reference voltage, which is prepared by the local primary and the secondary controllers. In addition, an undirected cyber graph is employed to transmit the local information only between the neighbors.

Also, Fig. 4 shows the cooperative control application of the dc microgrids. As it can be seen in Fig. 4, two voltage terms are added to the global voltage reference to deal with the local voltage reference and maintain the output voltage of each converter as follows:

$$V^i_{\mathrm{dc_{ref}}} = V_{\mathrm{dc_{ref}}} + \Delta V_v + \Delta V_i. \tag{4}$$

In Fig. 4, $V_{\mathrm{dc_{ref}}}$ and $I_{\mathrm{dc_{ref}}}$ represent the global reference of voltage and current for all units, respectively. It is important to note that $I_{\mathrm{dc_{ref}}} = 0$ for the load current sharing proportionally between units [18]. $\bar{V}^i_{\mathrm{dc}}$ is the average voltage estimated for the ith unit and it is updated based on the following protocol, which is named dynamic consensus [22]:

$$\bar{V}^i_{\mathrm{dc}}(t) = V^i_{\mathrm{dc}}(t) + \int_0^t \sum_{j\in M_i} a_{ij}\left(\bar{V}^j_{\mathrm{dc}}(\tau) - \bar{V}^i_{\mathrm{dc}}(\tau)\right)d\tau \tag{5}$$

and M_i is the set of neighbors of the ith unit. In addition, $\bar{I}^i_{\mathrm{out}}$ is updated as follows:

$$\bar{I}^i_{\mathrm{out}}(k) = \sum_{j\in M_i} c_i a_{ij}\left(\frac{I^j_{\mathrm{dc}}(k)}{I^j_{\max}} - \frac{I^i_{\mathrm{dc}}(k)}{I^i_{\max}}\right). \tag{6}$$

In (6), c_i and I^i_{dc} are the coupling gain in the ith unit and measured output current of the ith converter, respectively. In addition, $I^i_{\max}$ denotes the maximum output current allowed for the ith converter. By the distributed consensus algorithm, the objectives of the dc microgrids for a well-connected cyber graph will converge as follows [23]:

$$\lim_{k\to\infty} \bar{V}^i_{\mathrm{dc}}(k) = V_{\mathrm{dc_{ref}}}, \quad \lim_{k\to\infty} \bar{I}^i_{\mathrm{out}}(k) = 0 \ \forall i \in M. \tag{7}$$

B. Effect of FDIAs on Cooperative DC Microgrids

In the case of attacks in the dc microgrid, the objectives of the dc microgrids will not follow (7). However, some attacks can be programmed with more complexity to deceive the operators by obeying (7). Also, detection of Stealth attacks using voltage measurements is studied in [14], and therefore, this article focuses on detection and mitigation of coordinated attacks on the current measurements. The attack on the current sensors in the ith agent can be conducted using

$$I^i_a = I^i_{\mathrm{dc}} + \kappa_i I^i_f \tag{8}$$

where I^i_a is the value of the output current of the ith unit, which is reported to the controller, and I^i_{dc} is the real value of the output current of the ith unit. In addition, I^i_f is the false data that are injected to the system by attackers. It is important to note that κ_i is a binary parameter and $\kappa_i = 1$ means the presence of attack element and vice versa. Furthermore, the model of the FDIAs on cyber link is as follows:

$$I^{ij}_a = I^j_{\mathrm{dc}} + \kappa_i I^i_f \quad \forall j \in M_i. \tag{9}$$

In (9), I^{ij}_a is the value of the output current of the ith unit that is sent to the jth units. Coordinated attacks inject the false data both into sensor and cyber link. The coordinated attack seems such a load change in the dc microgrid and it satisfies the objectives of coordinated control, i.e., current sharing and average voltage regulation.

IV. Proposed Method

The objective of this article is to detect and mitigate the coordinated FDIAs on output current measurements of converters. As it was mentioned earlier, these kinds of smart attacks satisfy (7), which makes it difficult to identify the existence of attacks just by monitoring the cooperative control signals. As a result, it is important to have an appropriate control strategy to mitigate those attacks in cooperative dc

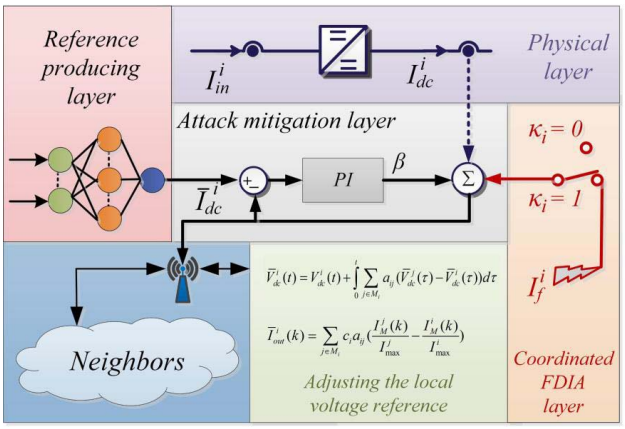


Fig. 5. Implementation of the PI-based reference tracking method to remove the attack in cooperative dc microgrids in the ith unit.

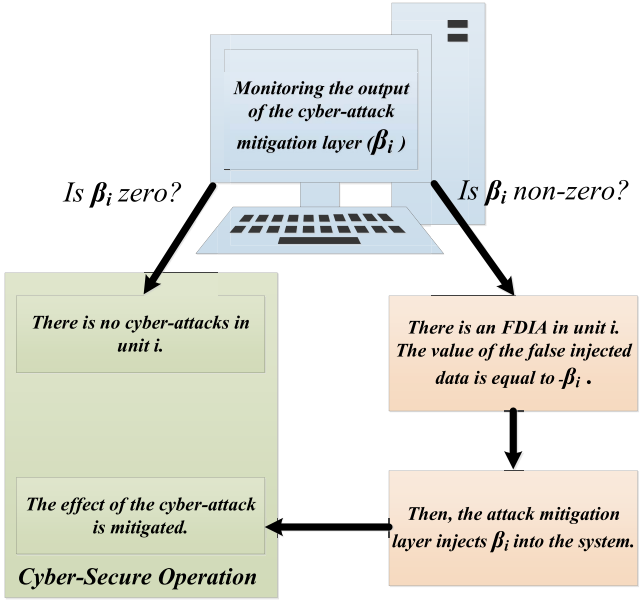


Fig. 6. Monitoring and implementing β_i to detect and also to mitigate the existence of the false data in the ith unit.

microgrids. The introduced strategy is based on the reference tracking application for the output dc current of each converter, to mitigate the false data. The proposed method is based on a PI controller-based reference tracking application in which the reference is prepared by an artificial neural network. In this work, a local estimator is designed for each unit to estimate the output current of the converter using an artificial neural network. The output of this neural network is then used as a reference to a PI controller, and the output of the PI controller is then added to the output current of the converter. In continuous, the implementation of the PI controller and also artificial neural network as the estimator are discussed in more detail.

Fig. 5 shows the implementation of the local PI controller in the ith unit. Based on Fig. 5, if there is no the attack mitigation layer and the PI controller in the ith unit, the gathered value of the output current of the converter to use

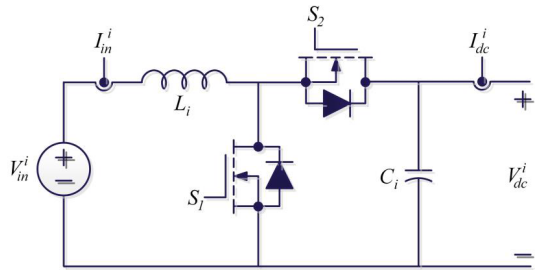


Fig. 7. Structure of the bidirectional boost dc–dc converter in the ith unit of the cooperative dc microgrid.

in the local controller and send to neighbors is as follows:

$$I_M^i(k) = I_a^i(k) = I_{\rm dc}^i(k) + \kappa_i I_f^i \tag{10}$$

where I_M^i is the gathered value of the output current of the converter in the ith unit. In the presence of the attack mitigation layer in the ith unit, I_M^i is determined as follows:

$$I_M^i(k) = I_{\rm dc}^i(k) + \kappa_i I_f^i + \beta_i. \tag{11}$$

In (11), β_i is the output of the PI controller in the ith unit. The PI controller is employed to follow $I_{\rm dc}^i$ by I_M^i even in the presence of attacks. The reference, which is used in the attack mitigation layer, is the estimated value of the output current of the ith unit and it is represented by $\bar{I}_{\rm dc}^i$. If $\bar{I}_{\rm dc}^i$ is to be estimated exactly with an ideal estimator and without any errors, $\bar{I}_{\rm dc}^i = I_{\rm dc}^i$ happens. Alternatively, β_i can be written as

$$\beta_i = -\kappa_i I_f^i. \tag{12}$$

Based on (12), the PI controller tries to produce a value as the output to add to the gathered value of the output current to remove the effect of the coordinated FDIAs from the unit. Based on (12), β_i is a proper index to monitor the ith unit locally. If the value of β_i is not zero, it means that the ith unit is under attack. If the ith unit is not under attack, κ_i is zero, and therefore, based on (12), β_i is zero. However, if the ith unit is under attack, κ_i is one, and based on (12), β_i and the injected false data have the same domain with different signs. Therefore, by monitoring β_i in each unit, the exact value of the false data can be determined if the unit is under attack. Briefly, the following holds.

Remark 1: By monitoring $-\beta_i$, the existence of the attack in the ith unit can be detected. Based on (12), it can be concluded that if the value of $-\beta_i$ is not zero, the ith unit is under an FDIA, but if the ith unit is not under the attack, the value of $-\beta_i$ is zero.

Remark 2: Based on (12), if the ith unit is under an FDIA, the value of the false injected data (I_f^i) is equal to the value of $-\beta_i$. Therefore, by injecting the output of the PI controller (β_i) into the system, the attack will be mitigated.

Fig. 6 shows that how the decentralized proposed method can detect and mitigate the cyberattack in the system. Also, in the attack mitigation layer, $\bar{I}_{\rm dc}^i$ has an important role and the reference producing layer should be a reliable layer and it should produce $\bar{I}_{\rm dc}^i$ as close as $I_{\rm dc}^i$ with high accuracy and small error. In this work, based on the abilities of artificial neural networks to extract the map between inputs and the output of a system with a high degree of nonlinearity and complexity,

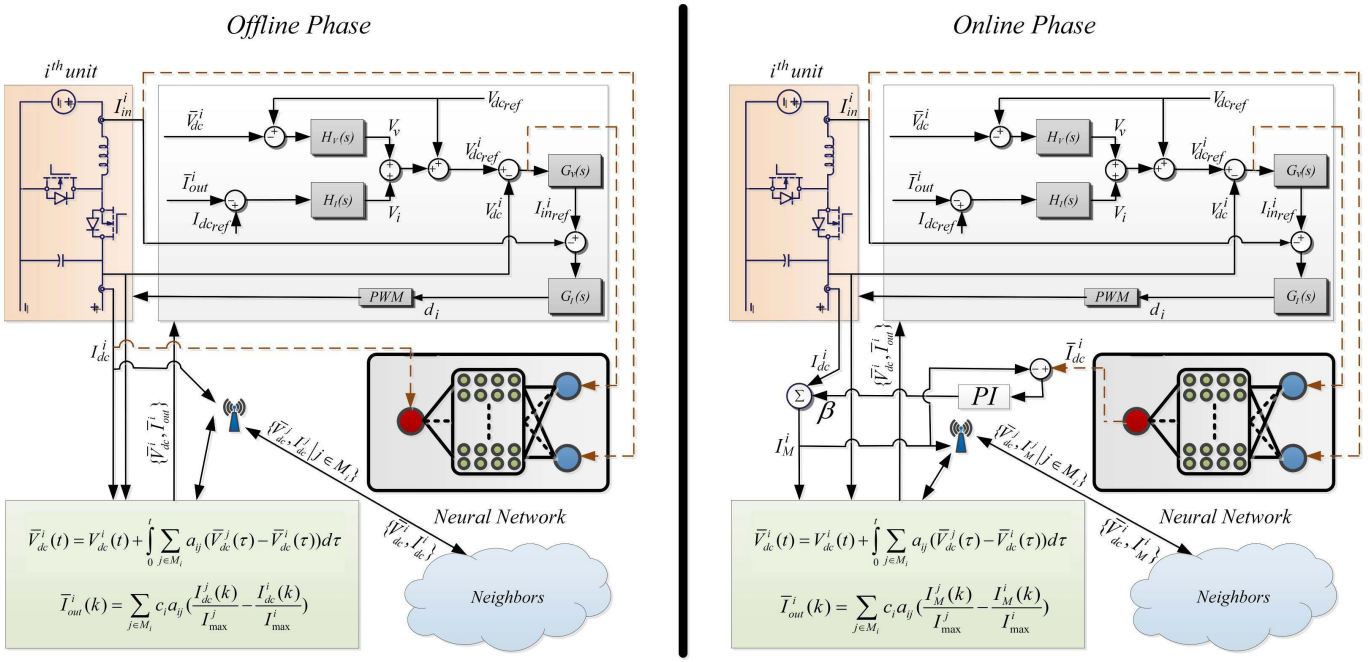


Fig. 8. Implementation of the neural network in offline and online modes in the ith unit in the dc microgrid.

artificial neural network is implemented to estimate the output current of the converter in each unit. A feedforward neural network is used as the estimator and as it will be shown later; in this work, the feedforward neural network has a good ability to estimate and predict the output current of the converter. Therefore, because of acceptance results and also preventing complexity in the reference predicting layer, the feedforward neural network is selected as a proper candidate and solution to be used in this work.

The implementation of the neural network consists of two phases. The first phase that is done offline is related to the training of the neural network to reach a fine-tuned network to have the ability of estimation properly, and the second phase is about implementation of the trained neural network to estimate the output current of the converter and make the reference for the PI controller online. The cooperative dc microgrid consists of DERs, and each DER as a dc source is connected to the main dc bus by a bidirectional buck–boost converter that is modeled based on Fig. 7.

In this study, I^i_{in} and $(V^i_{\text{dc}_{\text{ref}}} - V^i_{\text{dc}})$ are selected as the input of the neural network to be used for the estimation of I^i_{dc}. Before the implementation of the neural network online, it should be trained to determine the optimized value of the connection weight between neurons of the consecutive layers and also bias weights of neurons to reach a well-trained neural network. For the training, a set of data inputs and data output of the neural network should be gathered to be used in the training phase. It is important to note that the training is implemented offline before the online implementation of the neural network. Fig. 8 shows how the neural network is trained offline to be ready to implement in each unit online to estimate the output current of that unit.

V. Simulation Results

A cyber-physical microgrid with $M = 4$ units is considered here, as shown in Fig. 3. The simulated parameters are

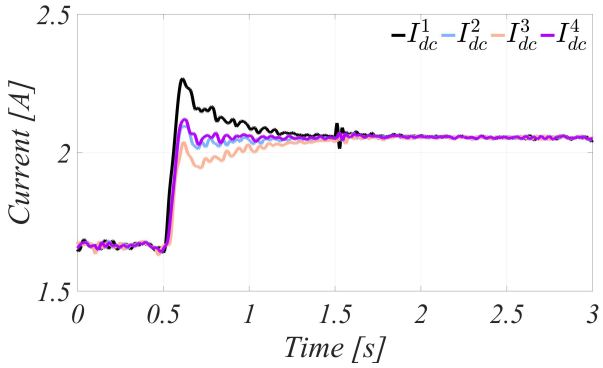


Fig. 9. DC output currents of all units during a coordinated attack in scenario 1.

included in the Appendix. At first, a neural network with one hidden layer, which has ten neurons, is considered to be implemented for estimation of the output current of the converter. As it will be shown later, the results with one hidden neural network are proper and the neural network can estimate the output current of each converter precisely; therefore, in order to avoid more complexity of the neural network, this work avoids to use a neural network with more hidden layers and the neural network with one hidden layer is implemented. In this work, the neural network has two inputs, and as a result, the number of neurons in the input layer is two. Also, the number of neurons in the output layer is equal to the number of outputs of the neural network. In this study, the output of the neural network is the estimated value of the output current. Therefore, the neural network has just one output and the number of the neurons in the output layer is one. Also, by default, the number of neurons in the hidden layer is ten. The obtained results based on ten hidden neurons were satisfactory because of that, the number of neurons in the hidden layer was not changed. In addition, because the structure and parameters of the converters in all

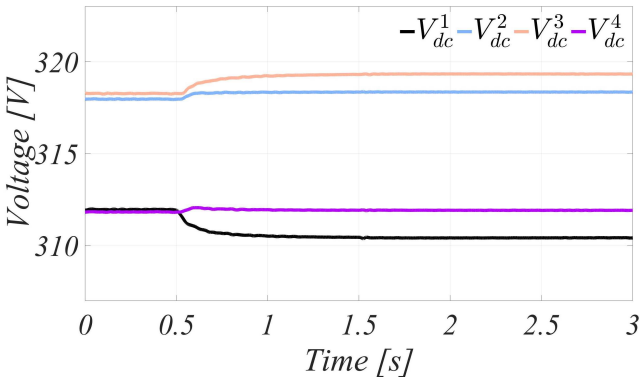


Fig. 10. DC voltages of all units during a coordinated attack in scenario 1.

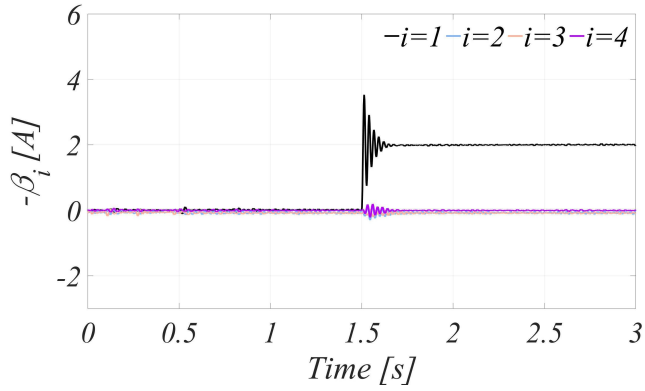


Fig. 11. Estimation of the false injected data into all units in scenario 1.

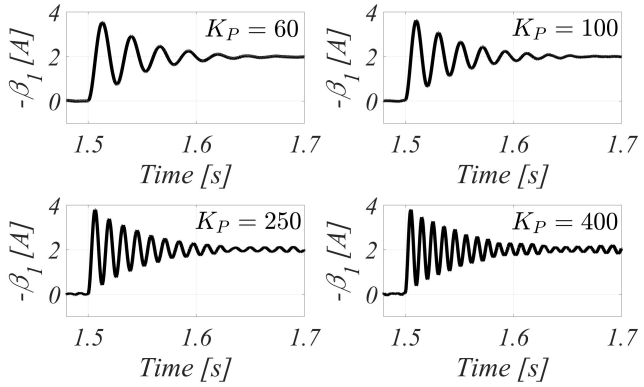


Fig. 12. Estimated value of the false injected data in the attacked unit for different values of K_p in scenario 1.

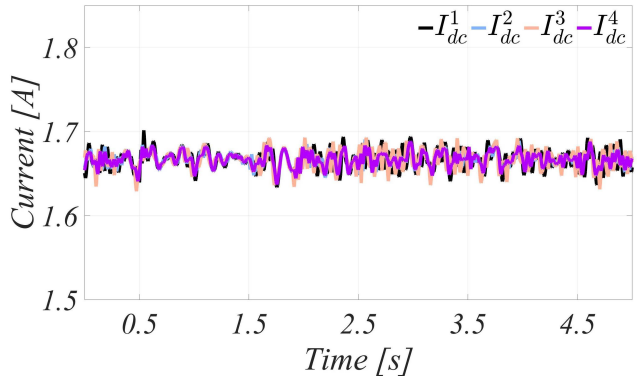


Fig. 13. DC output currents of all units during wide coordinated attacks in scenario 2.

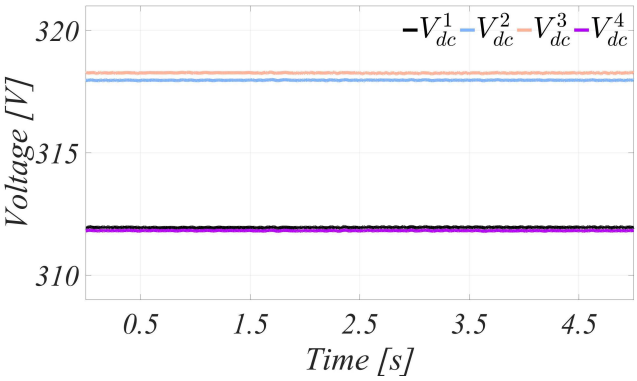


Fig. 14. DC voltages of all units during wide coordinated attacks in scenario 2.

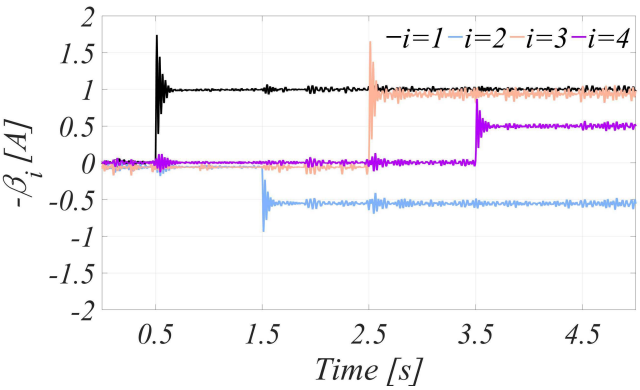


Fig. 15. Estimation of the false injected data into all units in scenario 2.

units are the same, a neural network was trained for one unit and the trained neural network was implemented in other units. To gather data to train the neural network, when the simulation model was running, for a given duration (20 s), data were gathered every 0.1 ms, so a set of data consists of 200 000 samples of $\{I_{\text{in}}^1, (V_{\text{dc}_{\text{ref}}}^1 - V_{\text{dc}}^1)\}$ as the input of the neural network, and 200 000 samples of $\{I_{\text{dc}}^1\}$ as the output of the neural network were selected to be used in the training phase. It is important to note that during the selected time to gather the data, 14 load changes were considered in the simulation and 11 of them happened in unit 1. Those load changes were considered to map the dynamics of the converter when the data were gathered to have a more accurate neural network-based estimator. In addition, the activation functions of the neural network in the hidden layer and the output layer, namely f_1 and f_2, are tan-sigmoid and linear activation functions, respectively, and they are considered as follows:

$$f_1(x) = \frac{2}{1 + e^{-2x}} - 1 \tag{13}$$

$$f_2(x) = x. \tag{14}$$

It is important to note that the global reference voltage in this work is 315 V. In addition, to gather data to train the neural

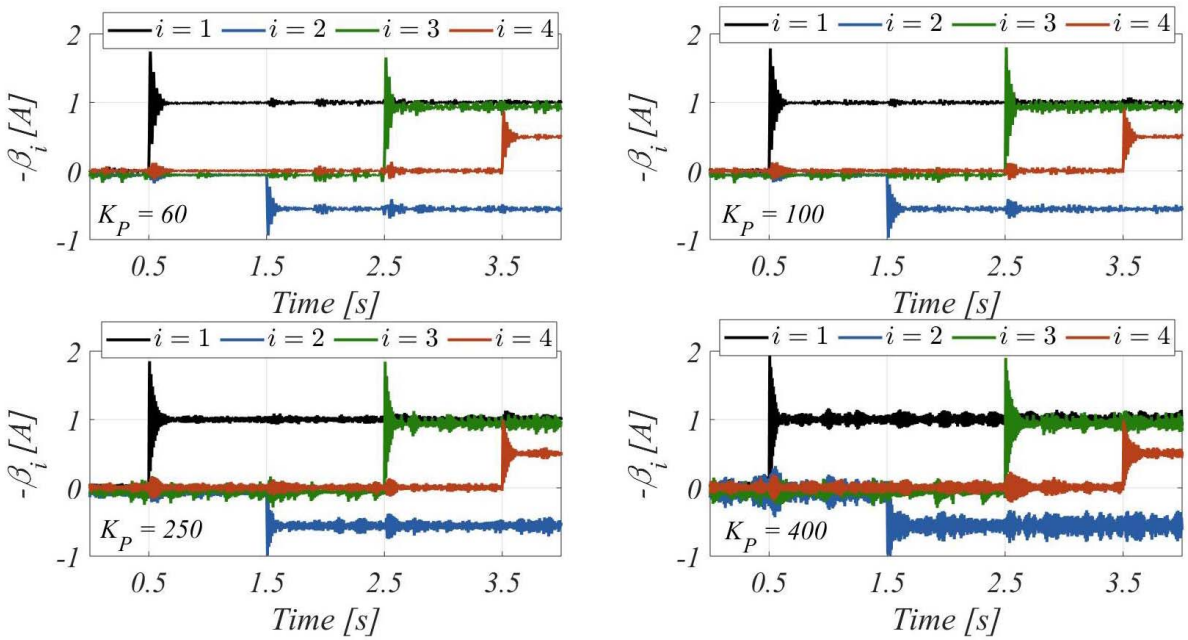


Fig. 16. Estimated value of the false injected data to all units for different values of K_p in scenario 2.

network, the dc microgrid model was simulated without any attack on the model. The rest of this section is to show the results of different scenarios based on the proposed method.

A. Scenario 1: Injecting a False Data by a Coordinated Attack

In this scenario, the dc microgrid is in a steady state before the time $t = 0$ s and a load change happens on unit 1 at $t = 0.5$ s, and after 1 s, a false data with value of 2 starts to be injected into unit one as a coordinated attack. Fig. 9 shows the output currents and converters. Also, Fig. 10 shows the dc voltages of all units. Based on Fig. 9, the attack is removed from the attacked unit quickly. Furthermore, based on (12), $-\beta_i$ represents the estimated value of the false data, which is injected to the ith unit coordinately; thus, Fig. 11 shows the estimated value of the false data in all units, and based on the results, the proposed method estimates the false data value in all units precisely. As it can be seen in Fig. 11, $-\beta_i$ for $i = 2, 3$, and 4 is zero, but at $t = 1.5$ s, $-\beta_i$ for $i = 1$ starts to be increased to reach to 2 and it means that the attacked unit is unit 1 by a false data with value of 2. In addition, Fig. 12 shows the estimated value of the false data for the attacked unit for different values of K_p.

B. Scenario 2: Wide FDIAs on All Units

In this scenario, all units at different times are targets of the attacker to implement coordinated FDIAs on them. Based on the planned scenario, at $t = 0.5$ s, $t = 1.5$ s, $t = 2.5$ s, and $t = 3.5$ s, the false data with value of $+1$, -0.5, $+1$, and $+0.5$ are injected to units 1, 2, 3, and 4, respectively. Fig. 13 shows the output currents of the dc–dc converters in the dc microgrid. It can clearly be seen in Fig. 13 that the introduced strategy in this work is so efficient to remove the coordinated FDIA even when all units are under attack. Also, Fig. 14 shows the output voltages of all units. Furthermore, Fig. 15 shows the estimated values of the false data by the proposed strategy. Based on Fig. 15, the proposed method is successful to detect the attacked units, and also, it is reliable to estimate the value of the false data. Finally, Fig. 16 shows the estimated value of false data for different values of K_p.

VI. Real-Time Simulation Results

This work is verified on real-time simulation using OPAL-RT on a detailed simulated cooperative dc microgrid to evaluate the computational burden of the proposed method. The setup consists of OPAL-RT, a laptop, and a router, which connects devices to each other. The software of the OPAL-RT is RT-LAB that is integrated by MATLAB, and the MATLAB/Simulink environment is opened by RT-LAB; then, RT-LAB generates the C code of the model, which can be run on a real-time target. It is important to note that the sample time in MATLAB configuration parameters of the model is 5×10^{-5} s. The real-time system has three subsystems, i.e., master, slave, and console subsystems. The plant model is implemented in the master subsystem, and the slave subsystem is used to separate the computational section. In addition, scopes are located in the console subsystem. The information of the target is illustrated in the Appendix. Fig. 17 shows the real-time setup based on OPAL-RT, and Fig. 18 shows the implementation of the subsystems. In this section, all units are considered under coordinated attacks simultaneously with unfair values of false data. The values of $+80$, $+60$, $+40$, and $+20$ are injected to be added to units 1, 2, 3, and 4, respectively. Fig. 19(a) and (b) shows the currents and voltages in the dc microgrid, respectively. As it can be seen from Fig. 19(a) and (b), the effect of the unfair coordinated attacks

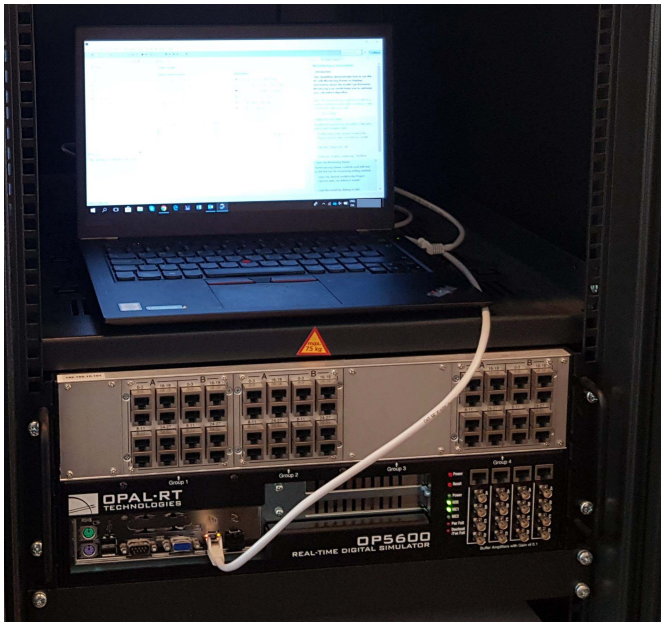


Fig. 17. Real-time setup to evaluate the proposed attack detection and mitigation strategy.

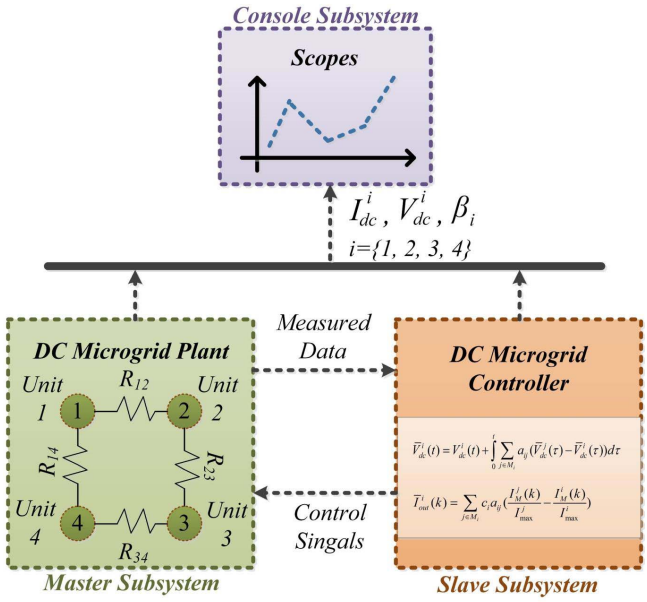
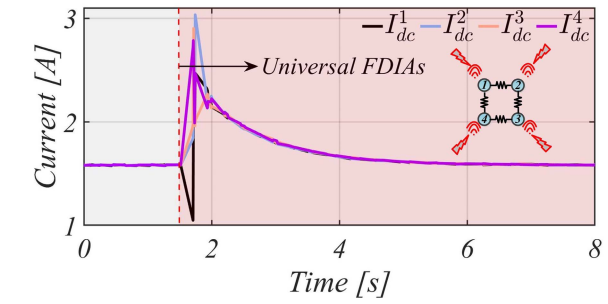


Fig. 18. Implementation of the master, slave, and console subsystems for real-time simulation.

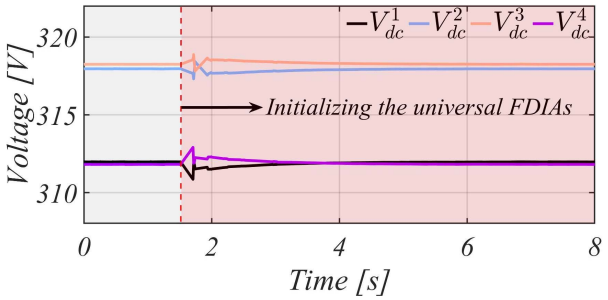
is removed from the dc microgrid. In addition, Fig. 20 shows the value of $-\beta_i$ for $i = 1, 2, 3$, and 4.

VII. Discussion and Future Work

In this study, a method based on artificial neural networks is introduced to detect and mitigate FDIAs in dc microgrids. The proposed strategy has advantages. For example, it is a decentralized approach, and as a result, it does not need extra data transmission between units and just uses the local data. Furthermore, the proposed method can calculate the value of the false injected data. Also, the neural network was trained based on nonattacked data and it does not need the data of



(a)



(b)

Fig. 19. Values of (a) dc currents and (b) dc voltages for all units during the real-time simulation.

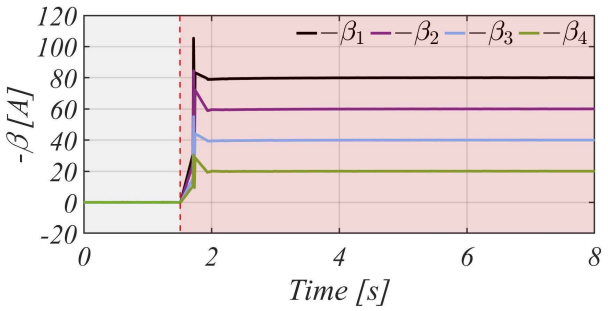


Fig. 20. Estimation of the false injected data for all units during the real-time simulation.

the system when the system is under attack. In other words, the neural network is trained based on the nonattacked system without any attacked data, and despite other methods, there is no need to model the attack in the training phase to detect and mitigate the FDIAs. Based on the proposed strategy, the FDIAs can be detected and also mitigated and there is no need to disconnect the attacked converter from the dc microgrid, and the dc microgrid can be operated successfully without any stress even it is under the FDIAs. The proposed work is successful even all units are under unfair attacks. In the planned future works, the proposed application will be developed to detect and remove other types of attacks. Also, the proposed strategy will be developed to implement in more complex dc microgrids.

VIII. Conclusion

This work introduced a method based on artificial neural networks to detect and remove the coordinated FDIAs on current measurements to have a secure cooperative control

TABLE II
PARAMETERS OF THE SIMULATED DC MICROGRID

$R_{12} = 1.8\ \Omega$	$V_{dc_{ref}} = 315\ V$ and $\Delta t = 0.1\ ms$
$R_{23} = 2.3\ \Omega$	$V_{in}^1 = V_{in}^2 = V_{in}^3 = V_{in}^4 = 270\ V$
$R_{34} = 2.1\ \Omega$	$L_1 = L_2 = L_3 = L_4 = 5\ mH$
$R_{14} = 1.3\ \Omega$	$C_1 = C_2 = C_3 = C_4 = 50\ mF$

TABLE III
PARAMETERS OF THE TARGET

$Version$	$2.6.29.6 - opalrt - 6.1$
$Number\ of\ CPUs$	12
$CPU\ speed$	$3466\ [MHz]$
$Artitecture$	$i686$

strategy in dc microgrids. Based on the proposed method, first, a neural network is used in each unit to estimate the output dc current of each converter, and based on the estimated value, a PI controller is implemented to remove the attack from the attacked unit. The proposed method is a decentralized method and there is no need to have exchange of any extra data between neighbors. The proposed strategy can determine the value of the false data when any of the units are under attack. Furthermore, as the results show, this work can successfully detect and remove attacks in dc microgrids when all units are under attack, even when the attacker tries to inject the false data to all units simultaneously with high domains and unfairly.

APPENDIX

The dc microgrid parameters used in the simulation are shown in Table II. In addition, Table III shows the information of the target for the real-time simulation.

REFERENCES

[1] T. Dragičević, X. Lu, J. C. Vasquez, and J. M. Guerrero, "DC microgrids—Part II: A review of power architectures, applications, and standardization issues," *IEEE Trans. Power Electron.*, vol. 31, no. 5, pp. 3528–3549, May 2016.

[2] D. Chen, L. Xu, and J. Yu, "Adaptive DC stabilizer with reduced DC fault current for active distribution power system application," *IEEE Trans. Power Syst.*, vol. 32, no. 2, pp. 1430–1439, Mar. 2017.

[3] Z. Liu, M. Su, Y. Sun, W. Yuan, H. Han, and J. Feng, "Existence and stability of equilibrium of DC microgrid with constant power loads," *IEEE Trans. Power Syst.*, vol. 33, no. 6, pp. 6999–7010, Nov. 2018.

[4] Y. Gu, W. Li, and X. He, "Passivity-based control of DC microgrid for self-disciplined stabilization," *IEEE Trans. Power Syst.*, vol. 30, no. 5, pp. 2623–2632, Sep. 2015.

[5] 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.

[6] C. Wang, J. Duan, B. Fan, Q. Yang, and W. Liu, "Decentralized high-performance control of DC microgrids," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 3355–3363, May 2019.

[7] 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.

[8] L. Meng *et al.*, "Review on control of DC microgrids and multiple microgrid clusters," *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 5, no. 3, pp. 928–948, Sep. 2017.

[9] T. Morstyn, B. Hredzak, G. D. Demetriades, and V. G. Agelidis, "Unified distributed control for DC microgrid operating modes," *IEEE Trans. Power Syst.*, vol. 31, no. 1, pp. 802–812, Jan. 2016.

[10] T. Wang, D. O'Neill, and H. Kamath, "Dynamic control and optimization of distributed energy resources in a microgrid," *IEEE Trans. Smart Grid*, vol. 6, no. 6, pp. 2884–2894, Nov. 2015.

[11] X. Chen *et al.*, "Consensus-based distributed control for photovoltaic-battery units in a DC microgrid," *IEEE Trans. Ind. Electron.*, vol. 66, no. 10, pp. 7778–7787, Oct. 2019.

[12] L. Meng, T. Dragicevic, J. Roldan-Perez, J. C. Vasquez, and J. M. Guerrero, "Modeling and sensitivity study of consensus algorithm-based distributed hierarchical control for DC microgrids," *IEEE Trans. Smart Grid*, vol. 7, no. 3, pp. 1504–1515, May 2016.

[13] Y. Li, P. Dong, M. Liu, and G. Yang, "A distributed coordination control based on finite-time consensus algorithm for a cluster of DC microgrids," *IEEE Trans. Power Syst.*, vol. 34, no. 3, pp. 2205–2215, May 2019.

[14] S. Sahoo, S. Mishra, J. C.-H. Peng, and T. Dragicevic, "A stealth cyber-attack detection strategy for DC microgrids," *IEEE Trans. Power Electron.*, vol. 34, no. 8, pp. 8162–8174, Aug. 2019.

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

[16] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inform. Syst. Secur.*, vol. 14, no. 1, p. 13, 2011.

[17] M. R. Habibi, H. R. Baghaee, T. Dragicevic, and F. Blaabjerg, "Detection of false data injection cyber-attacks in DC microgrids based on recurrent neural networks," *IEEE J. Emerg. Sel. Topics Power Electron.*, early access, Jan. 20, 2020, doi: 10.1109/JESTPE.2020.2968243.

[18] S. Sahoo, J. C.-H. Peng, A. Devakumar, S. Mishra, and T. Dragicevic, "On detection of false data in cooperative DC microgrids—A discordant element approach," *IEEE Trans. Ind. Electron.*, vol. 67, no. 8, pp. 6562–6571, Aug. 2020.

[19] S. Liu, Z. Hu, X. Wang, and L. Wu, "Stochastic stability analysis and control of secondary frequency regulation for islanded microgrids under random denial of service attacks," *IEEE Trans. Ind. Informat.*, vol. 15, no. 7, pp. 4066–4075, Jul. 2019.

[20] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *Proc. 47th Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Sep. 2009, pp. 911–918.

[21] J. Zhao, L. Mili, and M. Wang, "A generalized false data injection attacks against power system nonlinear state estimator and countermeasures," *IEEE Trans. Power Syst.*, vol. 33, no. 5, pp. 4868–4877, Sep. 2018.

[22] M. Zhu and S. Martínez, "Discrete-time dynamic average consensus," *Automatica*, vol. 46, no. 2, pp. 322–329, Feb. 2010.

[23] S. Sahoo, J. C.-H. Peng, S. Mishra, and T. Dragicevic, "Distributed screening of hijacking attacks in DC microgrids," *IEEE Trans. Power Electron.*, vol. 35, no. 7, pp. 7574–7582, Jul. 2020.

Mohammad Reza Habibi (Student Member, IEEE) was born in Tehran, Iran. He is currently pursuing the Ph.D. degree with the Department of Energy Technology, Aalborg University, Aalborg, Denmark.

He is a Visiting Research Scholar with the Department of Electrical Power Engineering and Mechatronics, Tallinn University of Technology, Tallinn, Estonia. His current research interests include intelligent energy systems, application of artificial intelligence in power electronics and power systems, advanced control of power converters, modeling and control of energy storage systems, modeling and secure control of dc distribution systems and microgrids, and cyber-physical systems.

Subham Sahoo (Member, IEEE) received the B.Tech. degree in electrical and electronics engineering from the VSS University of Technology, Burla, India, in 2014, and the Ph.D. degree in electrical engineering from IIT Delhi, New Delhi, India, in 2018.

He has worked as a Visiting Student with the Department of Electrical and Electronics Engineering, Cardiff University, Cardiff, U.K., in 2017. Prior to completion of his Ph.D. degree, he worked as a Research Fellow with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore. He has made a significant contribution toward the development of advanced resilient control strategies in cyber-physical dc microgrids. He is currently working as a Post-Doctoral Researcher with the Department of Energy Technology, Aalborg University, Aalborg, Denmark. His research interests include control and stability of microgrids, renewable energy integration, cyber-physical power electronic systems, and cybersecurity in power electronic systems.

Dr. Sahoo was a recipient of the Indian National Academy of Engineering (INAE) Innovative Students Project Award for his Ph.D. thesis across all the institutes in India for the year 2019. He received the IRD Student Startup Award in 2017 to incorporate a company named Silov Solutions Pvt. Ltd. commercialized and based on his contributions during his doctoral studies. This company is based and incubated by IIT Delhi. He is also active in many expert talks as the Secretary of IEEE Young Professionals Affinity Group, Denmark. He was also one of the outstanding reviewers for the IEEE TRANSACTIONS ON SMART GRID in 2020.

Sebastián Rivera (Senior Member, IEEE) received the M.Sc. degree in electronics engineering from Universidad Tecnica Federico Santa Maria (UTFSM), Valparaíso, Chile, in 2011, and the Ph.D. degree in electrical and computer engineering from Ryerson University, Toronto, ON, Canada, in 2015.

He was a Post-Doctoral Fellow with the University of Toronto, Toronto, and the Advanced Center of Electrical and Electronic Engineering (AC3E), UTFSM, in 2016 and 2017, respectively. Since 2018, he has been an Assistant Professor with the Faculty of Engineering and Applied Sciences, Universidad de los Andes, Santiago, Chile. He is also an Associate Researcher wth the AC3E and the Solar Energy Research Center (SERC-Chile), both centers of excellence in Chile. His research focuses on dc distribution systems, electric vehicle charging infrastructure, high-efficiency dc–dc conversion, multilevel converters, and renewable energy systems.

Dr. Rivera was a recipient of the Academic Gold Medal of the Governor General of Canada in 2016.

Tomislav Dragičević (Senior Member, IEEE) received the M.Sc. and industrial Ph.D. degrees in electrical engineering from the Faculty of Electrical Engineering, Zagreb, Croatia, in 2009 and 2013, respectively.

From 2013 until 2016, he has been a Post-Doctoral Research Associate with Aalborg University, Aalborg, Denmark, where he has been an Associate Professor from March 2016 until 2020. Since April 2020, he has been a Professor with the Technical University of Denmark, Copenhagen, Denmark. He made a guest professor stay at Nottingham University, Nottingham, U.K., during spring/summer of 2018. His principal field of interest is the design and control of dc distributions systems and microgrids and the application of advanced modeling and control concepts to power electronic systems. He has authored or coauthored more than 200 technical publications (more than 100 of them are published in international journals, mostly in IEEE) in his domain of interest, eight book chapters, and a book in the field.

Dr. Dragičević has been an Alexander von Humboldt fellow since 2019. He was a recipient of the Končar Prize for the Best Industrial Ph.D. Thesis in Croatia and the Robert Mayer Energy Conservation Award. He serves as Associate Editor for the IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, IEEE TRANSACTIONS ON POWER ELECTRONICS, IEEE JOURNAL OF EMERGING AND SELECTED TOPICS IN POWER ELECTRONICS, and *IEEE Industrial Electronics Magazine*.

Frede Blaabjerg (Fellow, IEEE) received the Ph.D. degree in electrical engineering from Aalborg University, Aalborg, Denmark, in 1995, and the Honoris Causa degree from the University Politehnica Timisoara (UPT), Timişoara, Romania, and Tallinn Technical University (TTU), Tallinn, Estonia.

From 1987 to 1988, he was with ABB-Scandia, Randers, Denmark, where he became an Assistant Professor in 1992, an Associate Professor in 1996, and a Full Professor of power electronics and drives in 1998. In 2017, he became a Villum Investigator. He has published more than 600 journal articles in the field of power electronics and its applications. He is the coauthor of four monographs and an editor of ten books in power electronics and its applications. His current research interests include power electronics and its applications, such as in wind turbines, photovoltaic (PV) systems, reliability, harmonics, and adjustable speed drives.

Dr. Blaabjerg received the 32 IEEE Prize Paper Awards, the IEEE PELS Distinguished Service Award in 2009, the EPE-PEMC Council Award in 2010, the IEEE William E. Newell Power Electronics Award 2014, the Villum Kann Rasmussen Research Award in 2014, the Global Energy Prize in 2019, and the 2020 IEEE Edison Medal. From 2019 to 2020, he served as the President for the IEEE Power Electronics Society. He is also the Vice-President of the Danish Academy of Technical Sciences. He is nominated for the term 2014–2019 by Thomson Reuters to be among the most 250 cited researchers in Engineering in the world. He was the Editor-in-Chief of the IEEE TRANSACTIONS ON POWER ELECTRONICS from 2006 to 2012. He has been a Distinguished Lecturer of the IEEE Power Electronics Society from 2005 to 2007 and the IEEE Industry Applications Society from 2010 to 2011 and from 2017 to 2018.