Secure Control of DC Microgrids for Instant Detection and Mitigation of Cyber-Attacks Based on Artificial Intelligence

Habibi, Mohammad Reza; Baghaee, Hamid Reza; Blåbjerg, Frede; Dragicevic, Tomislav

Published in:
IEEE Systems Journal

Link to article, DOI:
10.1109/JSYST.2021.3119355

Publication date:
2022

Document Version
Peer reviewed version

Secure Control of DC Microgrids for Instant Detection and Mitigation of Cyber-Attacks Based on Artificial Intelligence

Mohammad Reza Habibi, *Student Member, IEEE*, Hamid Reza Baghaee, *Member, IEEE*, Frede Blaabjerg, *Fellow, IEEE*, and Tomislav Dragičević, *Senior Member, IEEE*

***Abstract*—DC microgrids can be operated under a hierarchical control strategy, and it needs a communication-based layer. The implementation of digital controllers and the communication infrastructure can make a dc microgrid vulnerable to cyber-attacks. This article introduces an approach based on Artificial Intelligence (AI) to detect and mitigate cyber-attacks in a dc microgrid. The proposed method is based on the artificial neural network (ANN), which can be categorized as an AI-based method. The proposed application implements an ANN to detect and mitigate false data injection attacks (FDIAs). FDIAs try to inject false data into the system to affect the control application of the dc microgrid, and it can shut down the dc microgrid. The proposed method can calculate the value of the false data, and it can detect and remove the attack simultaneously. The proposed method is tested in a MATLAB/Simulink environment. Also, to have more accurate results, the introduced approach is examined under different conditions and cyber/physical disturbances (e.g., communication delay, noise, plug-and-play of additional units, and time-varying FDIAs). Besides, a comparison is considered to evaluate the effectiveness of the proposed strategy. The obtained results can conclusively prove the effectiveness, accuracy, and authenticity of the proposed method to successfully detect the FDIAs and remove the cyber-attack.**

***Index Terms*—Artificial neural network (ANN), cyber-attack, cyber-physical systems (CPSs), dc–dc converters, dc microgrid, false data injection attack (FDIA).**

I. Introduction

DC MICROGRIDS consist of power devices and structures such as dc bus, dc–dc converters, dc sources, and loads [1]–[3]. In order to make an effective coordination between power components, dc microgrids are controlled by a hierarchical control strategy to satisfy certain control objectives, i.e., current sharing and voltage regulation [4]. The hierarchical control layer is made by three control levels, i.e., primary, secondary, and tertiary controllers, and because of the use of controllers, voltage and current sensors are implemented to gather input data of the controllers and send gathered data to the controllers [5], [6]. The implementation of a cyber network and digital controllers causes that dc microgrids are under a risk to be vulnerable to cyber-attacks. Because of the vulnerability of dc microgrids to cyber-attacks, it is highly recommended to have a plan to detect cyber-attacks as well as mitigate them in dc microgrids. There are some types of cyber-attacks, e.g., false data injection attacks (FDIAs) [7], man-in-the-middle (MITM) attacks [8], replay attacks [9], hijacking attacks [10], and denial-of-service (DoS) attacks [11]–[15]. In the case of FDIAs, the attackers try to inject false data into the system, and the injected false data go to be added to the real data, and consequently, wrong data are used in the system [16]. For the MITM attack, the attacker tries to target data, which are transmitted between two units, which are connected directly, and data transmission between them exists [17]. In the replay attacks, data are gathered and recorded for a given time, and the recorded data will be used to deceive the operator of the system [18]. Also, in the hijacking attacks, the real data are replaced with the false data by the attacker [19]. Also, in the DoS attack, the goal of the attacker is to make the communication network unavailable [20]. In addition, some works have been done related to the distributed-DoS attacks, e.g., [21]. The goal of this article is to detect and remove FDIAs in dc microgrids, which are made by parallel dc–dc converters.

The increasing complexity of cyber-physical systems (CPSs) can lead to motivation for introducing new methods to increase the security of the systems [22]. Coupling the power and cyber layers can improve the functionality of the system, but it can increase the vulnerability of the power-based CPSs to cyber-attacks [23]. The concept of CPSs can be used for microgrids [24]. Also, a dc microgrid is a type of microgrid, and as a result, a dc microgrid can be classified as a type of cyber-physical microgrid. Security threats and issues can be emerged in CPSs [25]. Recently, some works have been done about FDIAs in power-based CPSs (e.g., dc microgrids). For example, in [26], an FDIA detection method is proposed based on identifying a change in a set of candidates, which called invariant, and they do not change. The FDIA, which

Manuscript received October 23, 2020; revised April 27, 2021; accepted June 8, 2021. *(Corresponding author: Mohammad Reza Habibi.)*

Mohammad Reza Habibi and Frede Blaabjerg are with the AAU Energy, Faculty of Engineering and Science, Aalborg University, 9220 Aalborg, Denmark (e-mail: mre@et.aau.dk; fbl@et.aau.dk).

Hamid Reza Baghaee is with the Department of Electrical Engineering, Amirkabir University of Technology, Tehran 1591634311, Iran (e-mail: hrbaghaee@aut.ac.ir).

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

Digital Object Identifier 10.1109/JSYST.2021.3119355

is considered in [26], tries to destroy the consensus protocol in dc microgrids, which are controlled based on a distributed control scheme. Also, the method proposed in [26] has tried to mitigate the attack in three different ways, i.e., making the attacked converter offline, disconnecting the communication link of the attacked unit, and the control-based approach to suppress the false data. In [27], an approach has been introduced to detect two types of FDIAs and DoS in dc microgrids, which are controlled in a distributed manner. To detect the attack, the voltage and current are monitored against certain specifications, which are defined (e.g., operational bounds). Also, Beg *et al.* [27] suppress the FDIA using a strategy by adjusting a parameter in a low-pass filter. Also, a method based on a recurrent neural network (RNN) is introduced by Habibi *et al.* [28] to detect the FDIAs in dc microgrids. Based on the proposed method in [28], RNNs are trained to be used to estimate the output dc voltage and current of converters. Then, the error of estimation is considered as a parameter to detect the existence of the FDIA in the dc microgrid. In [29], another method has been proposed to detect FDIAs on current measurements in dc microgrids. The proposed method in [29] is modeling the attack considering the consensus protocol, and based on a discordant element strategy, the attack in cooperative dc microgrids is detected. Furthermore, a decentralized method has been introduced in [30] to remove FDIAs, which try to inject false data on current measurement. The strategy proposed by Habibi *et al.* [30] introduced a secure control layer, which is based on a reference tracking application, and it has a controller and an RNN. Besides, in [31], an attack-resilient intelligent-soft-computing-based method has been proposed to have a secure control strategy for more-electric aircraft applications. In [31], the proposed strategy has been implemented adaptive neuro-fuzzy inference system and RNNs. In addition, a secure control strategy has been proposed by Habibi *et al.* [32] to remove cyber-attacks in a dc microgrid. In [32], the proposed strategy has implemented a controller and an artificial neural network (ANN) to make a collaboration between them to mitigate cyber-attacks. In addition, in [33], a decentralized ANN-based approach has been developed to detect and mitigate FDIAs on current measurements of a dc microgrid. It is important to note that the strategy proposed by Habibi *et al.* [33] has been examined on a dc microgrid, which has been made by distributed dc sources, which are controlled based on a consensus approach.

Some previous works have attempted to detect the FDIAs, and they did not work on both detection and mitigation of attacks. In addition, some of them have generally focused on dc microgrids, which are controlled in a distributed manner and based on a consensus-based protocol. Furthermore, the majority of them need to know enough information about the system, the relations in the model, and complex mathematical equations and concepts of the cyber-physical dc microgrid. This article proposes a strategy to detect and mitigate FDIAs in dc microgrids, simultaneously. Also, in this article, dc microgrids are structured by parallel dc–dc converters, and they are controlled based on a droop-based strategy. Furthermore, this article implements an ANN to detect and remove the FDIAs. ANNs can be considered as a data-based technique, and by using them, there is no need to have information about all parts of the system, the mathematical equations, and relations in the system, and this can reduce the complexity of the proposed method. In this article, the attack is on the dc-bus voltage, and the attacker tries to inject false data to the value of the dc-bus voltage. As a result, a wrong value of the dc-bus voltage goes to the secondary controller. By adjusting the domain of the false data by the attacker, the real value of the dc-bus voltage can exceed the allowed bounds, and it can shut down the dc microgrid. To implement the proposed ANN-based method, an ANN is trained and used to estimate the exact value of the false data to detect that, and based on the output of the ANN, data are injected into the system to remove the false injected data.

Briefly, the proposed method introduces a fully ANN-based secure layer to detect and remove the FDIAs at the same time. It is important to note that the proposed application is a data-based technique, and it does not need mathematical-based information of the system. The introduced method is implemented in a dc microgrid, which is structured by parallel dc–dc converters. Also, in this article, the FDIAs try to change the value of the dc-bus voltage to shut down the dc microgrid. In addition, the proposed strategy can estimate the value of the false data. Furthermore, the proposed strategy can work under different cyber and physical disturbances, e.g., communication delay, noise, load changing, and time-varying FDIAs.

The rest of this article is organized as follows. Section II elaborates on the basic concepts of ANNs. Section III describes the structure of dc microgrids, their control application, and the effect of FDIAs on them. Section IV explains the proposed cyber-attack detection and mitigation strategy. Section V presents the simulation results and comparison. Finally, Section VII concludes this article.

II. Basic Concepts of ANNs

ANNs can be considered as a part of artificial intelligence (AI). They are well-known and powerful data-based techniques to be used in different types of applications, such as model-predictive control of a three-phase inverter [34], design of weighting factors for a model-predictive controller to control power converters [35], detection of cyber-attacks in dc microgrids [28], and application of power calculations to improve power sharing in microgrids [36]. Fig. 1 illustrates the basic architecture of an ANN with n inputs and one output. An ANN has input, hidden, and output layers, and the input and output layers of the ANN can be considered as its first and last layers, respectively. The output signal of the kth neuron in the mth layer ($2 \leq m$) of the ANN can be calculated as follows:

$$\gamma_{k,m} = f_m \left(b_{k,m} + \sum_{j=1}^{N_{m-1}} \gamma_{j,m-1} \times w_{j_{m-1},k_m} \right) \quad (1)$$

where $\gamma_{k,m}$ is the output signal of the kth neuron in the mth layer, $f_m(.)$ is the activation function of the mth layer, $b_{k,m}$ is the bias weight of the kth neuron in the mth layer, N_{m-1} is the number of neurons in the $(m-1)$th layer, and w_{j_{m-1},k_m} is the

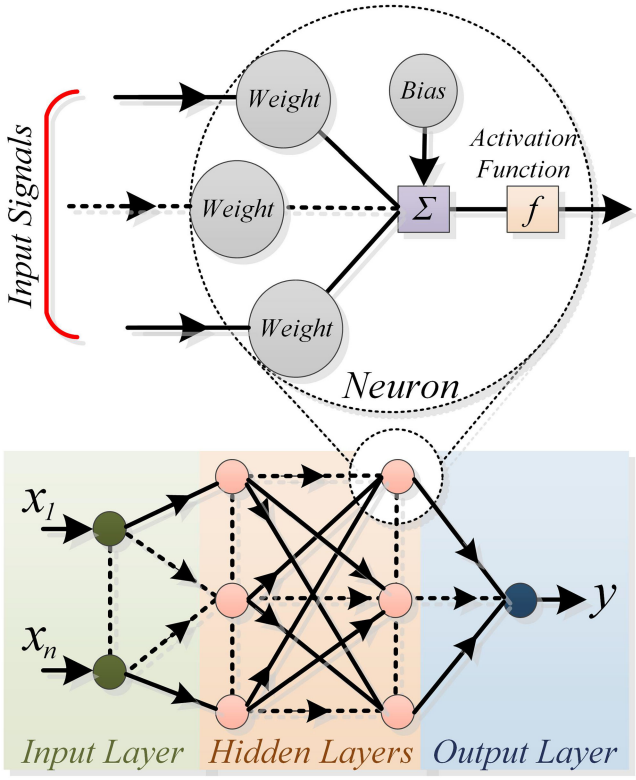

Fig. 1. Architecture of an ANN with input, hidden, and output layers, as well as the structure of neurons. Here, x_i $(1 \leq i \leq n)$ and y are the input and the output of the ANN, respectively.

connection weight between jth neurons of the $(m-1)$th and kth neurons of the mth layer.

In addition, matrices of W_m and B_m represent the connection weights between $(m-1)$th and mth layers and the bias factor of neurons in the mth layer, respectively. Matrices of W_m and B_m can be defined as follows:

$$W_m = \begin{bmatrix} w_{1_{m-1},1_m} & \cdots & w_{N_{m-1},1_m} \\ \vdots & \ddots & \vdots \\ w_{1_{m-1},N_m} & \cdots & w_{N_{m-1},N_m} \end{bmatrix} \tag{2}$$

$$B_m = \begin{bmatrix} b_{1,m} & b_{2,m} & \cdots & b_{N_m,m} \end{bmatrix}. \tag{3}$$

To use the ANN, the training phase should be done. The goal of the training is to calculate proper values of W_m and B_m $(2 \leq m \leq n)$. To train the ANN, the dataset, which has the inputs and the output, are gathered. Then, the gathered dataset is used in an optimization problem to find the optimized values of the connection and bias weights (W_m and B_m for $2 \leq m \leq n$) to have a well-tuned ANN. Finally, the tuned ANN can be used to estimate the output.

III. FDIAs in Conventional DC Microgrids

In Fig. 2, the physical architecture and the control layer of a dc microgrid with n parallel dc–dc converters are shown. The secondary controller sends a value to the primary controller to regulate the dc-bus voltage. If the output of the secondary

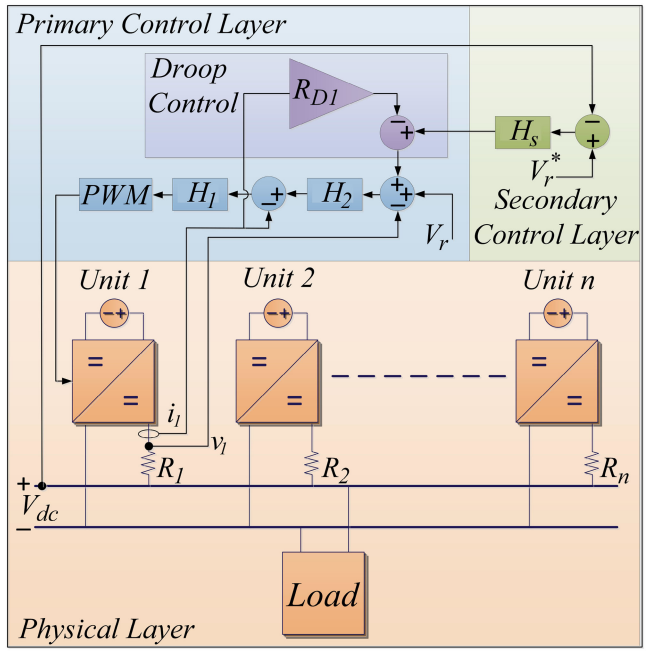

Fig. 2. Control layer and physical architecture of a dc microgrid with n units.

controller is ΔV, the reference voltage of the primary controller for the jth unit is adjusted as follows:

$$V_{rj}(t) = V_r + R_{Dj} i_j(t) + \Delta V(t) \tag{4}$$

where V_{rj} is the adjusted reference voltage for the jth unit. Also, V_r, R_{Dj}, and i_j are the reference dc-bus voltage, droop coefficient, and the output current of the jth unit, respectively.

The secondary controller is a proportional–integral (PI) controller, and its task is to keep the dc-bus voltage ($V_{\rm dc}$) to its reference value. In other words, we have

$$\lim_{t\to\infty} V_{\rm dc}(t) = V_r. \tag{5}$$

Also, an FDIA may inject false data into the system. In this article, the FDIA is considered on the secondary control layer to take the dc-bus voltage out of the allowance bounds, which can shut down the dc microgrid. If the system is under the attack, the model of the FDIA can be considered as follows:

$$V_a(t) = V_{\rm dc}(t) + V_f(t). \tag{6}$$

In (6), V_f represents the false data, which are injected by the attacker to the system, and V_a is the nonreal value of the dc-bus voltage, which goes to the secondary controller. If the dc microgrid is not under the FDIA, then we have

$$V_f(t) = 0 \tag{7}$$

and

$$V_a(t) = V_{\rm dc}(t). \tag{8}$$

If the FDIA exists in the dc microgrid, $V_{\rm dc}$ is replaced by V_a. So, in the case of attack, (6) can be converted into (9) as follows:

$$\lim_{t\to\infty} V_a(t) = V_r. \tag{9}$$

As a result, we have

$$\lim_{t\to\infty}\left(V_{\text{dc}}(t)+V_f(t)\right)=V_r \tag{10}$$

and consequently

$$\lim_{t\to\infty}V_{\text{dc}}(t)=V_r-\lim_{t\to\infty}V_f(t). \tag{11}$$

If the false injected data have a constant value of α ($V_f(t)=\alpha$), (11) can be altered as follows:

$$\lim_{t\to\infty}V_{\text{dc}}(t)=V_r-\alpha. \tag{12}$$

Therefore, based on (12), by adjusting α, the dc-bus voltage can converge to a value, which is out of the allowed bounds, and it can shut down the system.

IV. Proposed Secure Control Strategy

In this article, the FDIA is considered on the secondary controller, and the attacker tries to inject false data (V_f) into the dc-bus voltage. The goal of this article is to show how ANNs can be used to detect and remove the FDIA in the system very fast. The ANN is used to calculate the false data, which are injected by the attacker. Then, the output of the ANN is implemented to remove the attack. To implement the ANN, the inputs and output of the ANN should be selected, and after that, input and output data should be gathered to train the ANN to reach a well-tuned ANN. Finally, the tuned ANN can be used in the dc microgrid to detect and mitigate the FDIA. To avoid more measurements, the inputs of the ANN use the existing measured values, i.e., dc-bus voltage, output dc voltages, and currents of units.

Furthermore, the current as well as the historical value of the data is considered as the input of the ANN, and as will be shown later, it improves the behavior of the ANN. Also, as mentioned earlier, the task of the ANN is the calculation of the false injected data. As a result, the output of the ANN is the estimated value of the false injected data. Therefore, the input data (X) set and the output (Y) of the ANN are defined as follows:

$$\begin{aligned}lX(t)=\{&v_j(t-k\Delta t),i_j(t-k\Delta t),\dots\\&V_{dc}(t-k\Delta t)|1\le j\le n\quad\text{and}\quad 0\le k\le D\}\end{aligned} \tag{13}$$

$$Y(t)=\left\{\bar{V}_f(t)\right\} \tag{14}$$

where v_j and i_j are the output voltage and current of the jth dc–dc converter. Also, $\bar{V}_f$ is the estimated value of the false injected data by the ANN. Furthermore, D is the memory, which is considered for the input, and Δt is the sampling time width. It is important to note that, in this article, the ANN has one input layer, one hidden layer, and an output layer. As will be shown later, the ANN with one hidden layer works properly, and as a result, to avoid more complexity, the number of hidden layers is not increased. Therefore, considering that the number of hidden layers is one, the ANN has three layers. So, $\bar{V}_f$ will be calculated by the ANN as follows:

$$\bar{V}_f(t)=f_3\left(B_3+f_2\left(B_2+X(t)W_2^T\right)W_3^T\right). \tag{15}$$

To use the ANN, it should be trained to calculate the optimized values of B_2, B_3, W_2, and W_3. To train the ANN, the dataset of the inputs and the output should be gathered. To gather the dataset for the training, the required data should be produced. For producing the dataset of the training, several load changes and attacks with different values are simulated and considered in the system. Then, while the system is operated under different conditions (i.e., load changes and FDIAs), the required data for collecting the training dataset are gathered. After the training, the ANN can be implemented in the system online to detect and remove the FDIA. It is important to note that the training is done offline, and then, the trained ANN can be implemented online to detect and mitigate FDIA. Fig. 3 shows how the ANN can be trained offline and also how it can be implemented online to calculate the value of false injected data in the dc microgrid.

The output of the ANN is the estimated value of the false injected data, which is called $\bar{V}_f$. After the calculation of $\bar{V}_f$, authentic data, called V_{auth}, are injected into the system to mitigate the FDIA. V_{auth} is calculated as follows:

$$V_{\text{auth}}(t)=-\bar{V}_f(t). \tag{16}$$

The value of V_{auth} is added to the input of the secondary controller. If the dc microgrid is under the FDIA, the input of H_s, which is called V_s, is as follows:

$$V_s(t)=V_{\text{auth}}(t)+V_a(t). \tag{17}$$

The PI controller tries to converge the input of the controller to the reference value. Then, we have

$$\lim_{t\to\infty}V_s(t)=V_r. \tag{18}$$

Based on (6), (17), and (18), it can be concluded that

$$\lim_{t\to\infty}\left(V_{\text{auth}}(t)+V_{\text{dc}}(t)+V_f(t)\right)=V_r. \tag{19}$$

If the ANN works properly, the estimated value of the false injected data ($\bar{V}_f$) is very close to the real value of the false injected data (V_f). Therefore, based on (16), it can be obtained that $V_{\text{auth}}(t)=-V_f(t)$.

Remark 1: V_{auth} can be used as an index to detect the existence of the FDIA in the dc microgrid. If the dc microgrid is not under the attack, it can be considered that $V_f(t)=0$, and consequently, $V_{\text{auth}}(t)=0$. Therefore, if $V_{\text{auth}}(t)\neq 0$, it can be stated that there is FDIA in the system.

In addition, (19) can be converted as follows:

$$\lim_{t\to\infty}\left(-V_f(t)+V_{\text{dc}}(t)+V_f(t)\right)=V_r. \tag{20}$$

By simplifying, (20) can be changed to (5), and it means that the voltage of the dc bus is converging to the reference voltage. In other words, the dc microgrid is operated normally with a normal dc-bus voltage even when the system is under FDIA by the attacker.

Remark 2: If the dc microgrid is under the attack, $-V_f$ is injected into the system to remove the FDIA. Therefore, the dc-bus voltage will converge to the reference value.

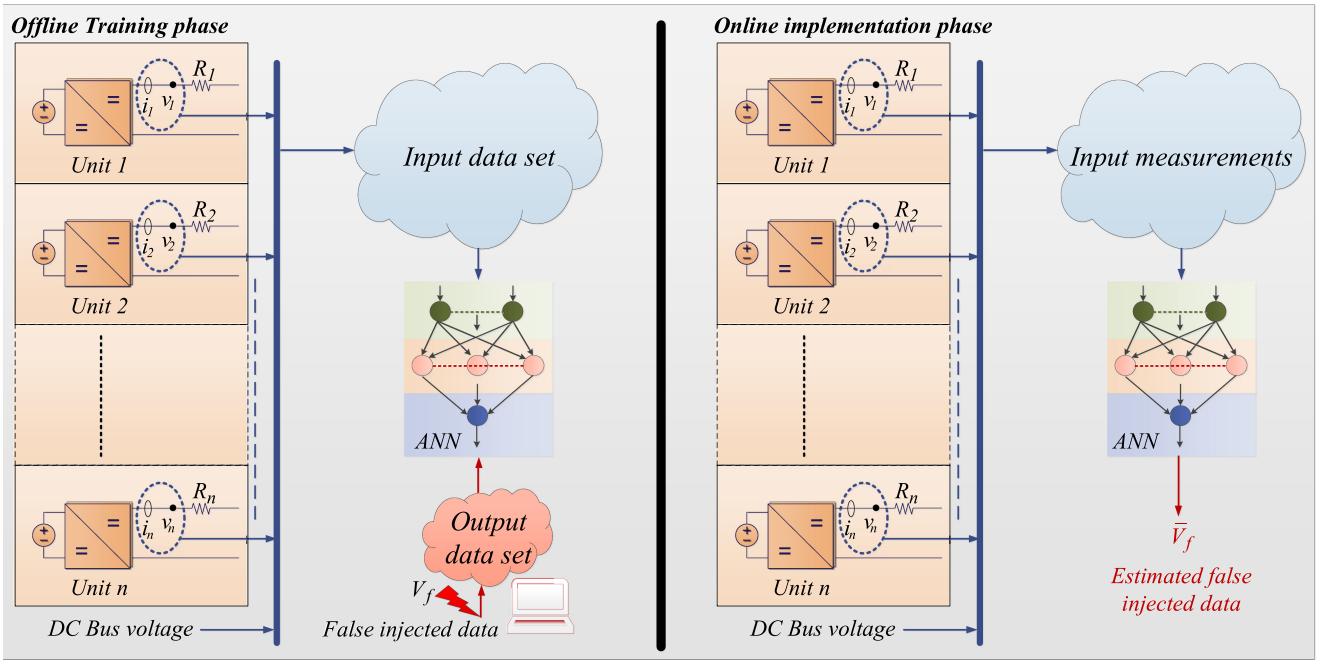

Fig. 3. Offline and online phases to use the ANN to estimate the false injected data in a dc microgrid. The offline phase is for the training of the ANN, and the online phase is related to the implementation of the ANN to estimate the value of the false injected data. The value of the false injected data is represented by V_f, and the estimated value of the false injected data, which is calculated by the ANN, is $\bar{V}_f$.

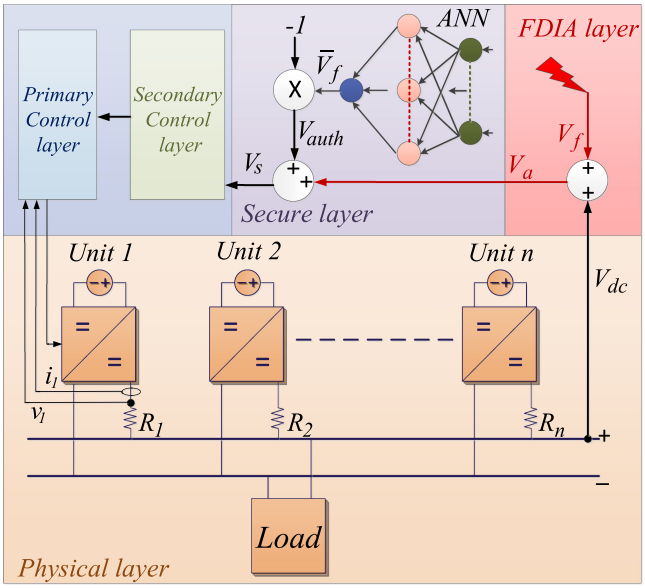

Fig. 4. Implementation of the proposed ANN-based FDIA mitigation strategy.

For more clarification, Fig. 4 shows the proposed mitigation method to detect and mitigate the FDIA in the system.

V. Results

The proposed method is examined on a modeled dc microgrid in a MATLAB/Simulink environment. The dc microgrid is structured by six units, which are connected to the main dc bus by resistive lines. In addition, each unit consists of a dc source (120 V) and one buck dc–dc converter that connects the dc source to the dc microgrid by connecting to the resistive line. The reference voltage for the dc bus is 48 V. In addition, the values of the resistive lines are as follows: $R_1 = 1.5\ \Omega, R_2 = 1.4\ \Omega$, $R_3 = 1.65\ \Omega$, $R_4 = 1.55\ \Omega$, $R_5 = 65\ \Omega$, and $R_6 = 1.70\ \Omega$. Before the exploitation of the ANN, it should be trained. To train the ANN, the simulated dc microgrid was run for 20 s with a sampling time of 20 μs. Then, 10^6 samples of inputs and the output were gathered to train the neural network. To gather data related to the inputs and the output, the dc microgrid was operated under different conditions, i.e., different load changes and also FDIA with variable values. In addition, during the operation of the dc microgrid, the number of dc sources and connected dc–dc converters to the dc microgrid also varied. All elements of the set A ($A = \{1, 2, 3, 4, 5, 6\}$) were considered as the number of connected dc–dc converters to the dc microgrid. So, the number of connected dc–dc converters to the dc microgrid was a variable number to have a more dynamic gathering data for the training phase. To evaluate the proposed strategy, eight case studies are considered. It is important to note that the memory for the input (D) is considered 2.

In case studies 1–5 and 7, the number of connected dc sources is three, and for case studies 6 and 8, it is six. Table I gives a preview of the case studies.

It is important to note that, for better evaluation of the proposed method, the index e, which is related to the domain of the error of estimation by the ANN, is shown in the simulated scenarios to have more effective evaluation. Also, e is calculated

TABLE I
PREVIEW OF THE CASE STUDIES

Case Study Number	Planned scenario	Number of units
1	Constant FDIA	3
2	Load changing and FDIA	3
3	Injection a time-varying false data	3
4	Outage of an unit under FDIA	3
5	FDIA and a communication delay	3
6	FDIA, outage of an unit, and load changing in a complex DC microgrid	6
7	Operation of the DC microgrid, while: 1- The proposed strategy does not used. 2- The proposed strategy is implemented. 3- The proposed strategy is implemented with non-historical value of data.	3
8	Evaluation of the proposed ANN-based strategy under noise.	6

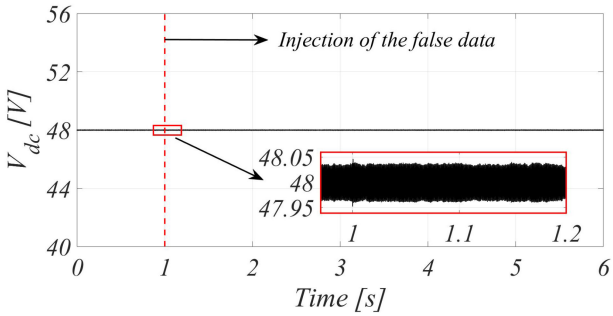

Fig. 5. Voltage of the dc bus in case study 1.

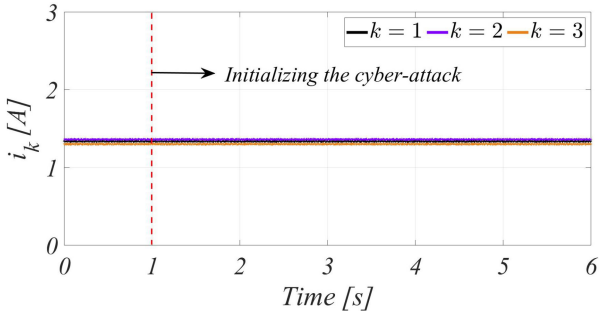

Fig. 6. Currents of the dc–dc converters in case study 1.

as follows:

$$e[\%] = \frac{|\bar{V}_f - V_f|}{V_f} \times 100. \quad (21)$$

A. Case Study 1: Constant FDIAs

In this scenario, the performance of the proposed strategy is examined under an FDIA with constant false data. The false data (V_f) with the value of $+10$ are injected into the system at $t = 1$ s. Figs. 5 and 6 show the dc-bus voltage and currents of the converters. As can be seen from Figs. 5 and 6, the FDIA is removed immediately, and the FDIA cannot have a destructive effect on the dc-bus voltage and also currents of dc–dc converters. Also, Fig. 7 illustrates the real value of the false data (V_f)

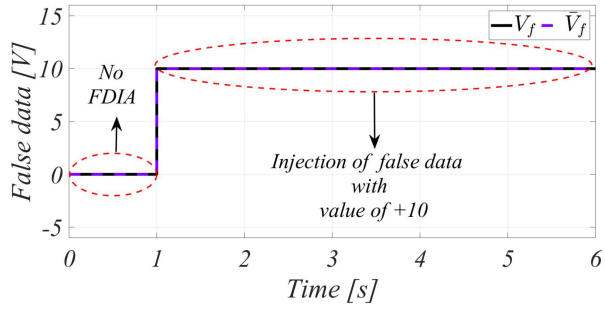

Fig. 7. Real and estimated values of the false data (i.e., V_f and $\bar{V}_f$, respectively) in case study 1.

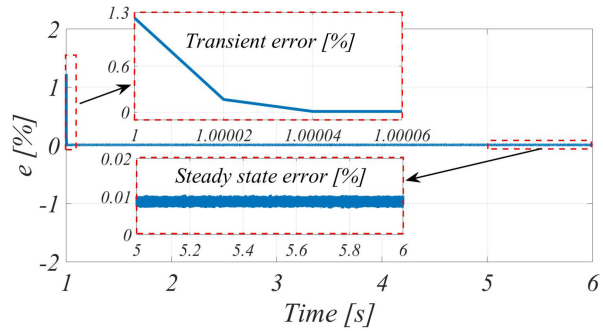

Fig. 8. Percentage of the error of estimation (e) by the ANN during the FDIA in case study 1.

and the output of the ANN ($\bar{V}_f$). Based on Fig. 7, the ANN can calculate the injected false data successfully. Furthermore, Fig. 8 shows the error of the estimation by the ANN, and it shows the percentage of the error of estimation for the ANN. Based on Fig. 8, the domain of the error is about 0.01% in the steady state and less than 1.3% for the transient time. Besides, the duration of the transient time is 40 μs, which is twice the sampling time. Briefly, the proposed method can estimate the value of the false data properly, and the FDIA can be removed by the proposed strategy with an excellent and proper performance.

B. Case Study 2: Nonsimultaneous as well as Simultaneous FDIA and Load Changing

The goal of this scenario is to show the effectiveness of the proposed method under an FDIA and also load changing. In this scenario, first, a load is added to the dc microgrid at $t = 1$ s. Then, at $t = 3$ s, another load is added to the system, and an FDIA is initialized simultaneously to have a more complex FDIA. Fig. 9 illustrates the dc-bus voltage, and it shows that the dc-bus voltage is converged to the reference value. Also, Fig. 10 depicts the output currents of the dc–dc converters. When the loads are added to the dc microgrid, the currents are increased. Furthermore, Fig. 11 shows the real and estimated false data. Based on Fig. 11, the ANN is operated properly to estimate the value of the false data. Also, Fig. 12 shows the value of e during the attack, and as it is illustrated, the domain of the error is less than 6% in the transient time and around 0.01% during the

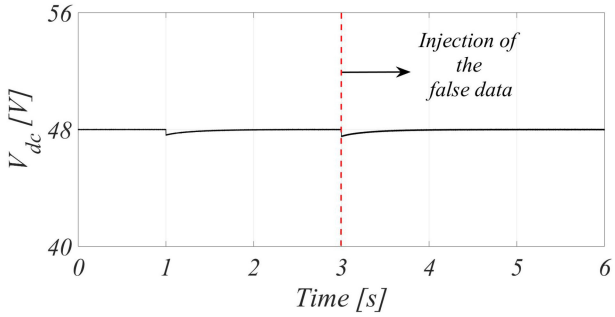

Fig. 9. Voltage of the dc bus in case study 2.

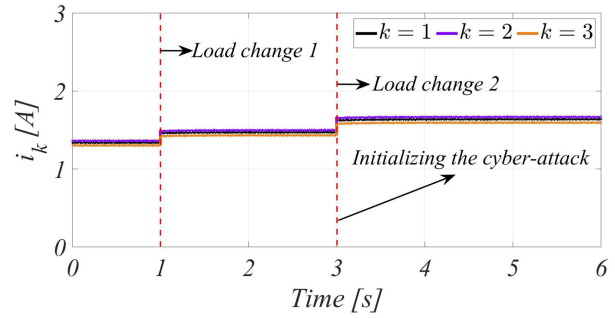

Fig. 10. Currents of the dc–dc converters in case study 2.

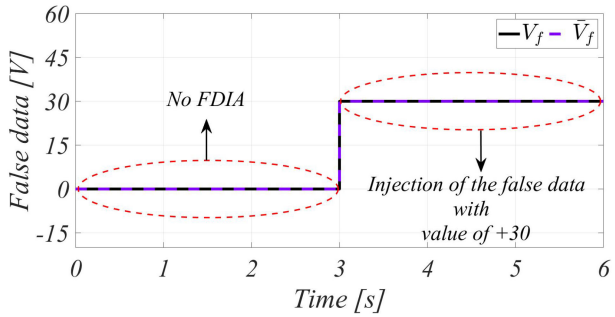

Fig. 11. Real and estimated values of the false data (i.e., V_f and $\bar{V}_f$, respectively) in case study 2.

steady state. Also, the duration of the transient time is twice the sampling time, and thereby, it is 40 μs.

C. Case Study 3: Time-Varying FDIA

In this case, the proposed strategy is examined under a time-varying cyber-attack. The model of the injected false data is as follows:

$$V_f(t) = 3\left(\cos(\pi t + \pi) + \cos(2\pi t) + \cos(4\pi t)\right) + 10. \quad (22)$$

Figs. 13 and 14 show the dc-bus voltage and currents of converters. Figs. 13 and 14 illustrate that the time-varying FDIA can be removed easily without disruptive effect. Furthermore, Fig. 15 depicts V_f and $\bar{V}_f$. Based on Fig. 15, the ANN can estimate the time-varying false data properly. Also, Fig. 16 is related to the error of estimation. Fig. 16 shows that the error of the transient time is less than 4% and less than 0.02% in the steady state.

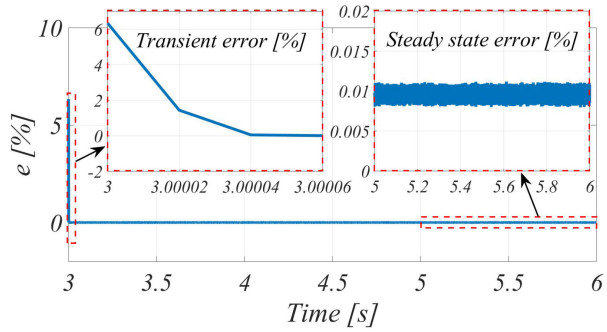

Fig. 12. Percentage of the error of estimation (e) by the ANN during the FDIA in case study 2.

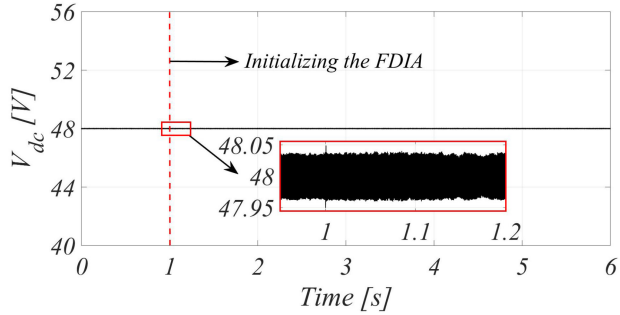

Fig. 13. Voltage of the dc bus in case study 3.

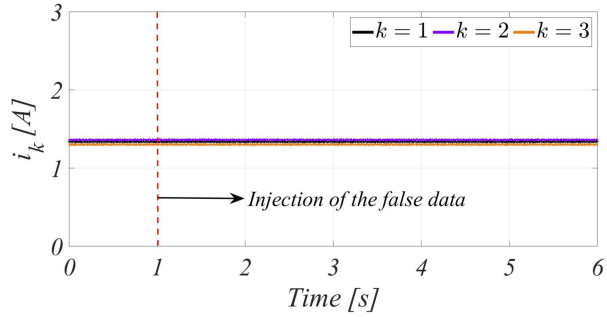

Fig. 14. Currents of the dc–dc converters in case study 3.

D. Case Study 4: Plug-and-Play of Additional Unit

In this scenario, the proposed strategy is tested under the plug-and-play of an additional unit (dc–dc converter). For this purpose, false data with the value of +20 are injected into the system at $t = 1$ s. Then, at $t = 3$ s, the outage of unit 2 happens. Figs. 17 and 18 depict the dc-bus voltage and the currents of units, respectively. Also, Fig. 19 illustrates the real and estimated values of the false data, and it shows that the ANN can calculate the value of the false data successfully. Furthermore, Fig. 20 describes the error of the estimation. Based on Fig. 20, e is approximately less than 0.003 in the steady state.

E. Case Study 5: FDIA and Communication Delay

In this scenario, the dc microgrid is operated under a delay with value of 10 ms, which is considered for the output of the secondary controller. So, the output of the secondary controller

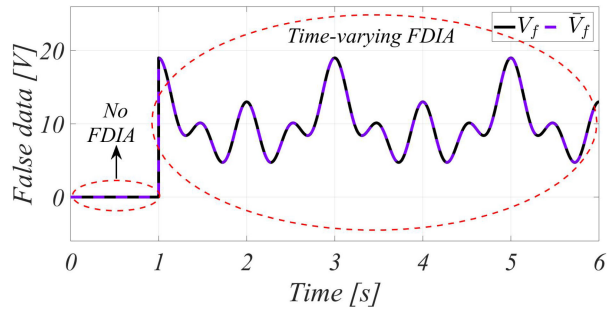

Fig. 15. Real and estimated values of the false data (i.e., V_f and $\bar{V}_f$, respectively) in case study 3.

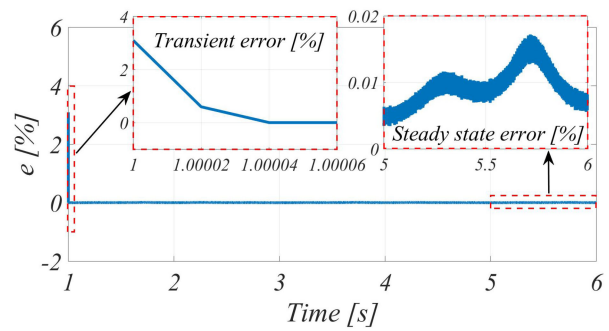

Fig. 16. Percentage of the error of estimation (e) by the ANN during the FDIA in case study 3.

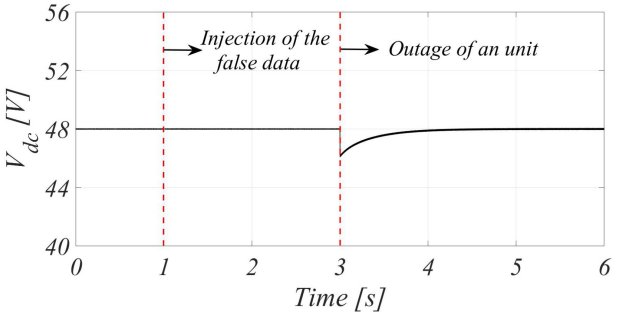

Fig. 17. Voltage of the dc bus in case study 4.

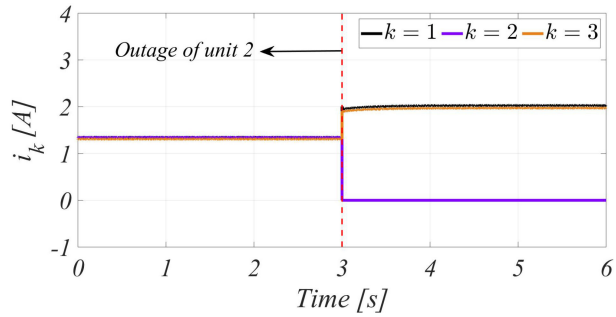

Fig. 18. Currents of the dc–dc converters in case study 4.

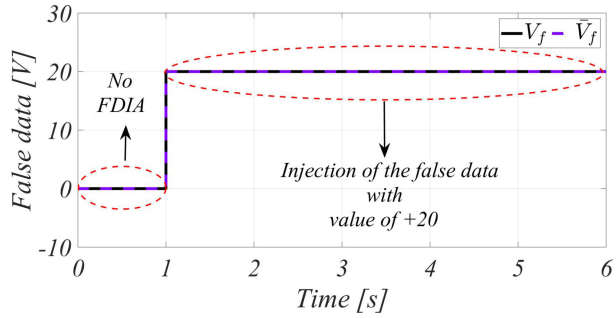

Fig. 19. Real and estimated values of the false data (i.e., V_f and $\bar{V}_f$, respectively) in case study 4.

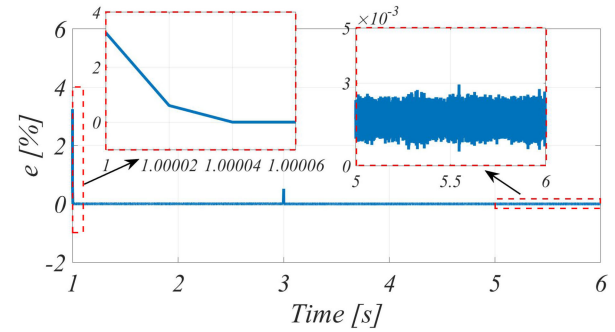

Fig. 20. Percentage of the error of estimation (e) by the ANN during the FDIA in case study 4.

is sent to the primary controllers with a delay of 10 ms. The false data are injected into the system at $t = 1$ s with the value of $+25$. Fig. 21 shows the dc-bus voltage. In the steady state, the dc-bus voltage is between 47.75 and 48.25 V. Furthermore, Fig. 22 illustrates the output currents of the converters. Also, Fig. 23 shows that the ANN has a proper performance to calculate the value of the false data. Fig. 24 illustrates the estimation error, and it is less than 0.006% in the steady state. Based on the achieved results, the proposed approach can remove the FDIA under the time delay.

F. Case Study 6: FDIA and Complex DC Microgrid

In this scenario, the performance of the proposed ANN-based method is tested in a more complex dc microgrid. In this scenario, the dc microgrid has six dc sources. At $t = 1$ s, false data with the value of $+10$ are injected into the system. Then, the outage of unit 6 is happening at $t = 3$ s, and a load is added to the dc microgrid at $t = 5$ s. Fig. 25 illustrates the voltage of the dc bus, and Fig. 26 shows the output currents of the dc–dc converters. As shown in Figs. 25 and 26, when the dc microgrid is operated under the proposed strategy, the FDIA could not have a destructive effect in the dc microgrid even the system is under the load changing or an outage of the unit. Also, Fig. 27 depicts the real and estimated values of the false data, and as it is depicted, the ANN is successful in estimating the value of the false data. Also, Fig. 28 illustrates the estimation error, and it is less than 0.014% in the steady state.

G. Case Study 7: Comparison of Nonhistorical and Historical-Based ANNs

In this article, the goal is to show the importance of the existence of a proper strategy to remove the cyber-attack and

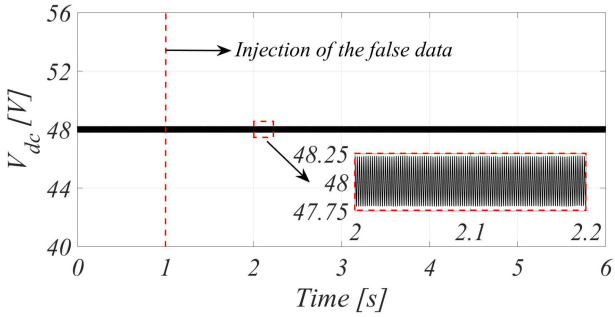

Fig. 21. Voltage of the dc bus in case study 5.

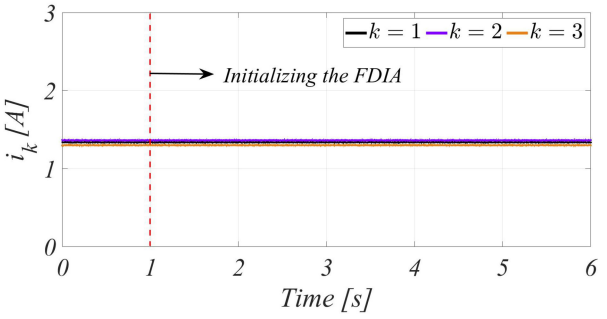

Fig. 22. Currents of the dc–dc converters in case study 5.

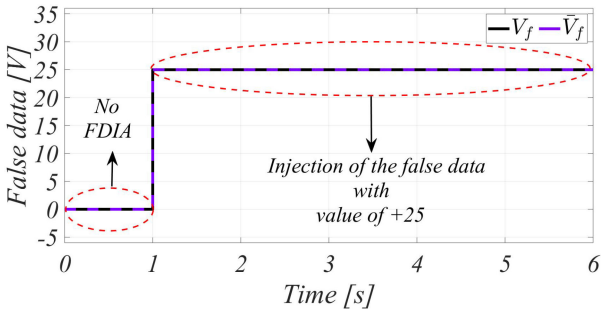

Fig. 23. Real and estimated values of the false data (i.e., V_f and $\bar{V}_f$, respectively) in case study 5.

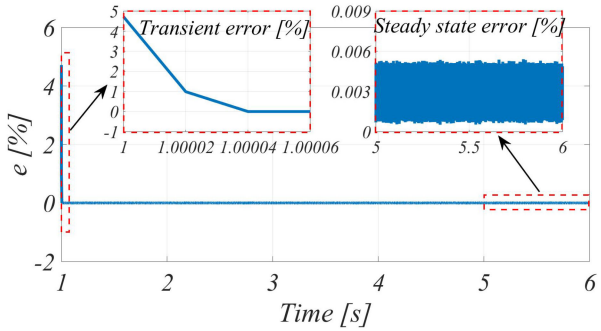

Fig. 24. Percentage of the error of estimation (e) by the ANN during the FDIA in case study 5.

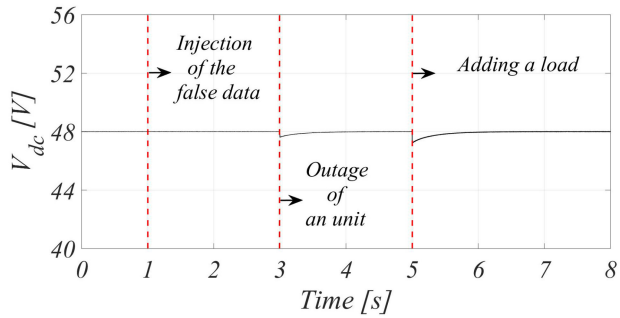

Fig. 25. DC-bus voltage in case study 6.

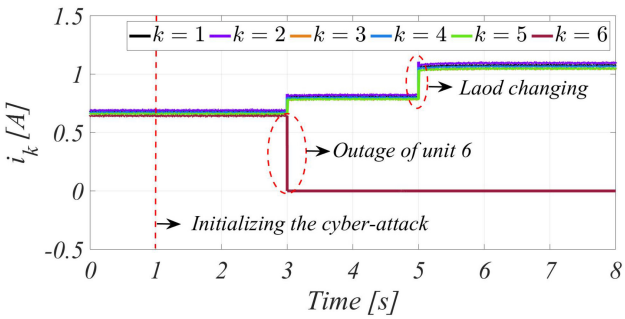

Fig. 26. Currents of the dc–dc converters in case study 6.

also to show the advantage of using the historical values of data in the input of the ANN. In this scenario, false data with a value of $+12$ are injected into the system at $t = 1$ s. This scenario is operated under three different conditions, i.e., Plans 1, 2, and 3, as follows.

Plan 1: The dc microgrid is controlled hierarchically [6] like shown in Fig. 2 and without the proposed FDIA mitigation strategy.

Plan 2: The same method as Plan 1 but operated under the proposed cyber-attack strategy.

Plan 3: The same method related to Plan 2 is used, but the parameter D is set to zero. In other words, the historical values of data are not used in the input of the ANN. So, the input of the ANN in this method is changed as follows:

$$X(t) = \{v_1(t), \ldots, v_n(t), i_1(t), \ldots, i_n(t), V_{\text{dc}}(t)\}\,. \qquad (23)$$

Fig. 29 shows the dc-bus voltage during the operation of the dc microgrid under the mentioned methods. Based on Fig. 29, after initializing the cyber-attack, in Plan 1, the dc-bus voltage starts to change, and it converges to 36 V that is expectable based on (12). However, for Plans 2 and 3, the dc-bus voltage still is converging to a reference value, which is 48 V. Furthermore, for a better comparison of Plans 2 and 3, the domain of errors for the ANN is compared based on the implemented index DE, which is as follows:

$$DE = \frac{e_{\text{Plan3}}}{e_{\text{Plan2}}} \qquad (24)$$

where e_{Plan2} and e_{Plan3} are the percentage of error in the estimation using ANNs in Plans 2 and 3, respectively, which is calculated based on (21). If DE is less than 1, the domain of the error of estimation by Plan 2 is less than that by Plan 3. Also, if DE is more than 1, the domain of the estimation error by Plan 2

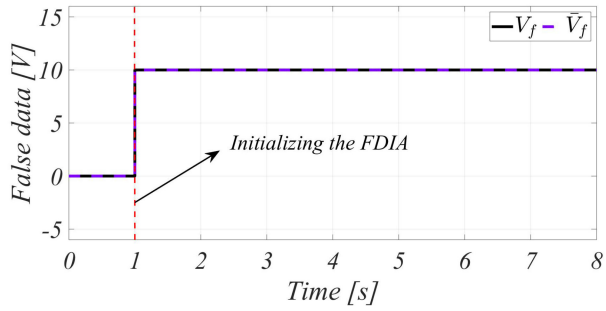

Fig. 27. Real and estimated values of the false data (i.e., V_f and $\bar{V}_f$, respectively) in case study 6.

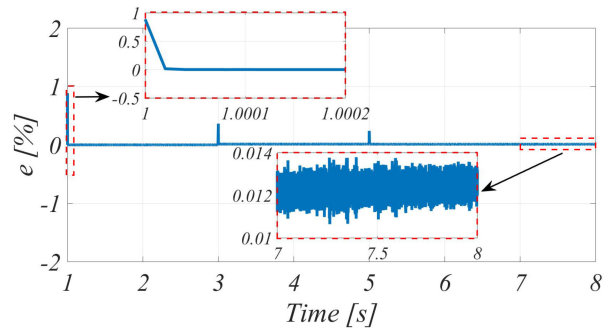

Fig. 28. Percentage of the error of estimation (e) by the ANN during the FDIA in case study 6.

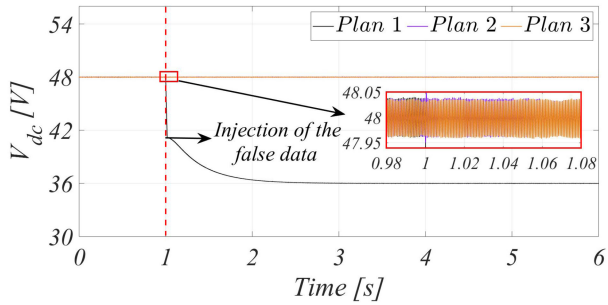

Fig. 29. Voltage of the dc bus in case study 7 for Plans 1–3.

is more than that by Plan 3. Fig. 30 shows DE. Based on Fig. 30, by injecting the false data, the DE starts closely from zero, and it reaches to a value around 4, approximately. Therefore, based on Fig. 30, it can be concluded that in the transient state, if the ANN does not use the historical value of the data in the input, the error of estimation is very small but, in the steady state, it has more errors compared to the proposed method.

H. Case Study 8: Evaluation of the Trained ANN Under Noise

In this part, the accuracy and performance of the trained ANN are evaluated. To train the ANN, as mentioned before, the simulated dc microgrid is operated for 20 s with a sampling time of 20 μs. Therefore, a dataset with 10^6 samples of the inputs and the output is made. In addition, different load changes are considered during the simulation to gather the training dataset. Besides, the outage of different units is simulated during the operation of

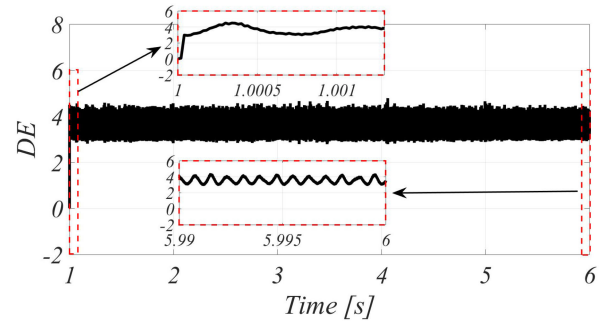

Fig. 30. Value of DE in case study 7.

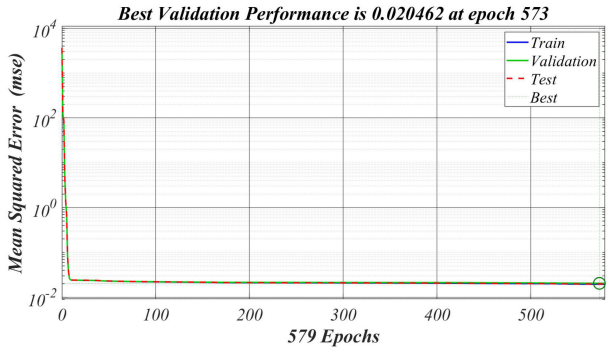

Fig. 31. Mean squared error (mse) of the ANN for the microgrid under noise in case study 8.

the dc microgrid to prepare the dataset. In addition, to make the situations closer to the real world and make the results more accurate, white noise is considered on the measurement of the dc-bus voltage. Therefore, in case study 8, a new ANN is trained under the noise to have more accurate results.

Briefly, the goal of case study 8 is to evaluate the performance of the trained ANN. In addition, to make the results more accurate, white noise is implemented on the value of the dc-bus voltage.

To train the ANN, 10^6 samples of the voltages and currents of the dc–dc converters and the dc-bus voltage are gathered to create the input dataset for the training. The dc microgrid has six dc–dc converters, and the voltages and currents of the converters are needed to create the input dataset (12 elements). In addition, the value of the dc-bus voltage is needed. So, 13 elements are needed to create the input dataset. But, the memory (D) is two, and as a result, the number of elements is increased to 39 ($13\times(2+1)$). To create the input dataset, a matrix with 10^6 samples of 39 elements is created. Also, the output dataset is made based on 10^6 samples of false data, which is injected into the system during the operation of the dc microgrid. To train the ANN, the Levenberg–Marquardt algorithm is implemented. Furthermore, 70% of the samples are implemented for training, 15% of them are used for validation, and 15% of them are implemented for testing.

In Fig. 31, the mean squared error (mse) during the training is illustrated. In addition, the error histogram of the ANN is shown in Fig. 32. The error histogram includes 20 bins. Also, in Fig. 32, the Targets represent the real values of the false data and Outputs

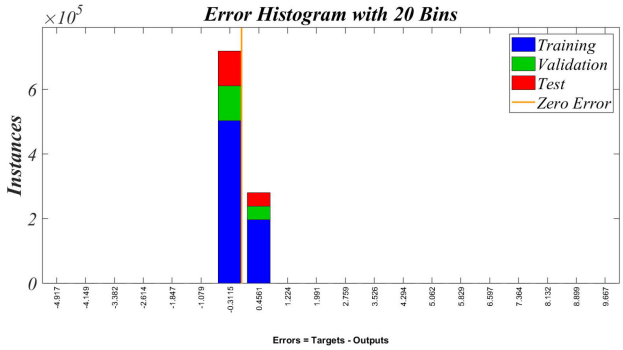

Fig. 32. Error histogram of the ANN for the dc microgrid under noise in case study 8.

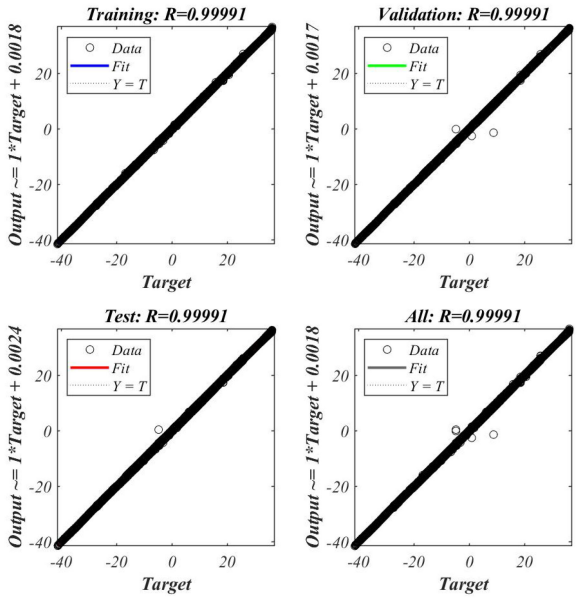

Fig. 33. Regression of the ANN for the dc microgrid under noise in case study 8.

are the output of the ANN. Besides, Fig. 33 shows the regression diagram of the ANN.

VI. Discussions and Future Works

This article proposed a method based on the ANN to increase the cyber-security of dc microgrids by the detection and mitigation of cyber-attacks. The type of studied cyber-attack in this article is considered FDIA. The ANN is used to estimate the value of the false data, which is injected into the system when the system is under FDIA. Based on the output of the ANN, an authentic value is produced to inject into the system to remove the false injected data. Due to the implementation of the ANN, the system can be considered as a black box, and there is no need to have mathematical-based information about the system to identify and mitigate the cyber-attack. In addition, the proposed strategy can mitigate the FDIA with constant and time-varying false data. In future works, the proposed method can be extended to more improvement of the cyber-security of dc microgrids by identifying and removing other types of cyber-attacks. In addition, an AI-based application can be introduced to detect and mitigate FDIAs in dc microgrids, which are made by distributed dc sources with multiple dc buses.

VII. Conclusion

This article introduces an ANN-based method to detect and mitigate FDIA in a dc microgrid. The proposed method is based on the ANN, and the ANN is implemented to calculate the value of the false data, which are injected to the system by the attacker. Then, the calculated value of false data is used to remove the cyber-attack. The proposed method can remove the attack quickly, and it has very fast performance to mitigate the attack. In this article, no additional controllers (e.g., PI and model-predictive controllers) are used, and because of that, it has reduced complexity. Furthermore, the proposed strategy was examined under different cyber and physical disturbances and events (i.e., load changing, communication delay, and plug-and-play of additional units). Besides, both constant and time-varying FDIAs were considered to evaluate the proposed approach. In addition, the performance of the ANN was evaluated under white noise in a separate case study. The obtained results show that the proposed strategy can calculate the value of the false injected data and remove the FDIA very fast and properly.

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] Z. Fan, B. Fan, J. Peng, and W. Liu, "Operation loss minimization targeted distributed optimal control of DC microgrids," *IEEE Syst. J.*, to be published, doi: 10.1109/JSYST.2020.3035059.

[3] T. K. Roy and M. A. Mahmud, "Dynamic stability analysis of hybrid islanded DC microgrids using a nonlinear backstepping approach," *IEEE Syst. J.*, vol. 12, no. 4, pp. 3120–3130, Dec. 2018.

[4] Y. Han, X. Ning, P. Yang, and L. Xu, "Review of power sharing, voltage restoration and stabilization techniques in hierarchical controlled DC microgrids," *IEEE Access*, vol. 7, pp. 149202–149223, 2019.

[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] J. M. Guerrero, J. C. Vasquez, J. Matas, L. G. de Vicuna, and M. Castilla, "Hierarchical control of droop-controlled AC and DC microgrids—A general approach toward standardization," *IEEE Trans. Ind. Electron.*, vol. 58, no. 1, pp. 158–172, Jan. 2011.

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

[8] M. Conti, N. Dragoni, and V. Lesyk, "A survey of man in the middle attacks," *IEEE Commun. Surv. Tut.*, vol. 18, no. 3, pp. 2027–2051, Jul.–Sep. 2016.

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

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

[11] S. Liu, P. Siano, and X. Wang, "Intrusion-detector-dependent frequency regulation for microgrids under denial-of-service attacks," *IEEE Syst. J.*, vol. 14, no. 2, pp. 2593–2596, Jun. 2020.

[12] Q. He *et al.*, "A game-theoretical approach for mitigating edge DDoS attack," *IEEE Trans. Dependable Secure Comput.*, to be published, doi: 10.1109/TDSC.2021.3055559.

[13] K. Doshi, Y. Yilmaz, and S. Uludag, "Timely detection and mitigation of stealthy DDoS attacks via IoT networks," *IEEE Trans. Dependable Secure Comput.*, vol. 18, no. 5, pp. 2164–2176, Sept./Oct. 2021.

[14] J. Li, Z. Xue, C. Li, and M. Liu, "RTED-SD: A real-time edge detection scheme for Sybil DDoS in the Internet of vehicles," *IEEE Access*, vol. 9, pp. 11296–11305, 2021.

[15] B. Hussain, Q. Du, B. Sun, and Z. Han, "Deep learning-based DDoS-attack detection for cyber-physical system over 5G network," *IEEE Trans. Ind. Inform.*, vol. 17, no. 2, pp. 860–870, Feb. 2021.

[16] D. Xue, X. Jing, and H. Liu, "Detection of false data injection attacks in smart grid utilizing ELM-based OCON framework," *IEEE Access*, vol. 7, pp. 31762–31773, 2019.

[17] F. Fayyaz and H. Rasheed, "Using JPCAP to prevent man-in-the-middle attacks in a local area network environment," *IEEE Potentials*, vol. 31, no. 4, pp. 35–37, Jul./Aug. 2012.

[18] S. Yoon, M. Koh, J. Park, and H. Yu, "A new replay attack against automatic speaker verification systems," *IEEE Access*, vol. 8, pp. 36080–36088, 2020.

[19] 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.

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

[21] N.-N. Dao *et al.*, "Securing heterogeneous IoT with intelligent DDoS attack behavior learning," *IEEE Syst. J.*, to be published, doi: 10.1109/JSYST.2021.3084199.

[22] S. Mili, N. Nguyen, and R. Chelouah, "Transformation-based approach to security verification for cyber-physical systems," *IEEE Syst. J.*, vol. 13, no. 4, pp. 3989–4000, Dec. 2019.

[23] D. Liu, C. K. Tse, and X. Zhang, "Tradeoff between robustness and functionality in cyber-coupled power systems," *IEEE Syst. J.*, to be published, doi: 10.1109/JSYST.2020.3045597.

[24] B.Zhang, C. Dou, D. Yue, and Z. Zhang, "Response hierarchical control strategy of communication data disturbance in micro-grid under the concept of cyber physical system," *IET Gener., Transmiss. Distrib.*, vol. 12, no. 21, pp. 5867–5878, Nov. 2018.

[25] M. M. Rana, R. Bo, and A. Abdelhadi, "Distributed grid state estimation under cyber attacks using optimal filter and Bayesian approach," *IEEE Syst. J.*, vol. 15, no. 2, pp. 1970–1978, Jun. 2021.

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

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

[28] 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.*, vol. 9, no. 5, pp. 5294–5310, Oct. 2021.

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

[30] M. R. Habibi, T. Dragicevic, and F. Blaabjerg, "Secure control of DC microgrids under cyber-attacks based on recurrent neural networks," in *Proc. IEEE 11th Int. Symp. Power Electron. Distrib. Gener. Syst.*, 2020, pp. 517–521.

[31] M. B. Kamal, G. J. Mendis, and J. Wei, "Intelligent soft computing-based security control for energy management architecture of hybrid emergency power system for more-electric aircrafts," *IEEE J. Sel. Topics Signal Process.*, vol. 12, no. 4, pp. 806–816, Aug. 2018.

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

[33] M. R. Habibi, S. Sahoo, S. Rivera, T. Dragičević, and F. Blaabjerg, "Decentralized coordinated cyber-attack detection and mitigation strategy in DC microgrids based on artificial neural networks," *IEEE Trans. Emerg. Sel. Topics Power Electron.*, vol. 9, no. 4, pp. 4629–4638, Aug. 2021.

[34] I. S. Mohamed, S. Rovetta, T. D. Do, T. Dragicević, and A. A. Z. Diab, "A neural-network-based model predictive control of three-phase inverter with an output *lc* filter," *IEEE Access*, vol. 7, pp. 124737–124749, 2019.

[35] T. Dragičević and M. Novak, "Weighting factor design in model predictive control of power electronic converters: An artificial neural network approach," *IEEE Trans. Ind. Electron.*, vol. 66, no. 11, pp. 8870–8880, Nov. 2019.

[36] H. R. Baghaee, M. Mirsalim, and G. B. Gharehpetian, "Power calculation using RBF neural networks to improve power sharing of hierarchical control scheme in multi-DER microgrids," *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 4, no. 4, pp. 1217–1225, Dec. 2016.