Secure MPC/ANN-Based False Data Injection Cyber-Attack Detection and Mitigation in DC Microgrids

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

Published in:
IEEE Systems Journal

Link to article, DOI:
10.1109/JSYST.2021.3086145

Publication date:
2022

Document Version
Peer reviewed version

Secure MPC/ANN-Based False Data Injection Cyber-Attack Detection and Mitigation in DC Microgrids

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

***Abstract*—Direct current (DC) microgrids can be considered as cyber-physical systems due to implementation of measurement devices, communication network, and control layers. Consequently, dc microgrids are also vulnerable to cyber-attacks. False-data injection attacks (FDIAs) are a common type of cyber-attacks, which try to inject false data into the system in order to cause the defective behavior. This article proposes a method based on model predictive control (MPC) and artificial neural networks (ANNs) to detect and mitigate the FDIA in dc microgrids that are formed by parallel dc–dc converters. The proposed MPC/ANN-based strategy shows how MPC and ANNs can be coordinated to provide a secure control layer to detect and remove the FDIAs in the dc microgrid. In the proposed strategy, an ANN plays the role of the estimator to implement in the cyber-attack detection and mitigation strategy. The proposed method is examined under different conditions, physical events and cyber disturbances (i.e. load changing and communication delay, and time-varying attack), and the results of the MPC-based scheme is compared with conventional proportional-integral controllers. The obtained results show the effectiveness of the proposed strategy to detect and mitigate the attack in dc microgrids.**

***Index Terms*—Artificial neural network (ANN), cyber-physical dc microgrid, false-data injection attack (FDIA), model predictive control (MPC).**

I. Introduction

DIRECT current (DC) microgrids offer more advantages when compared to ac microgrids, e.g., higher reliability, more efficiency, less complex control, and also easier interface with electronic loads, energy storage systems, and renewable energy resources because of their natural dc behavior [1], [2]. Distributed generators are connected to the microgrids commonly by controllable converters [3]. To control the dc microgrids, three control layers are implemented in a hierarchical control structure, i.e., primary, secondary, and tertiary control layer [4], [5]. The primary controller aims to achieve equal current sharing between units, while the secondary control application is used to restore the voltage of the dc bus to the desired reference value [6]–[8]. Also, the tertiary controller can be implemented to manage the power flow between microgrids [9].

To implement the hierarchical control structure, it is necessary to deploy a communication network to exchange data between the primary, secondary, and tertiary controller. The existence of the measurement devices, communication networks, and also digital controllers, make the dc microgrids vulnerable to cyber-attacks. There are various types of cyber-attacks, which are able to attack dc microgrids and also smart grids, e.g., false-data injection attacks (FDIAs) [10], [11], denial of service (DoS) [12], hijacking [13], deception [14], and replay attacks [15]. FDIAs try to inject the false data into a system to alter the state of the system while the DoS attacks attempt to make the communication network completely unavailable [16]–[20]. In hijacking attacks, the attacker replaces the signals completely, while replay attacks deceive the operators of the system by first recording the data and reproducing it in the system [13], [15]. Recently, some research works have been done about FDIAs in dc microgrids. For instance, Beg *et al.* [21] have proposed a method to detect FDIAs in dc microgrids by identifying a change in candidate properties that do not change over time in cyber-physical dc microgrids. Also, Beg *et al.* [22] have introduced a strategy to detect FDIAs and DoS attacks by signal temporal logic for monitoring the output voltage and currents against the defined specifications. Furthermore, in [18], a method based on recurrent neural networks has been proposed to detect FDIAs in dc microgrids, and Sahoo *et al.* [10] have worked on FDIAs in dc microgrids based on a discordant element approach.

The above-mentioned works have tried to detect FDIAs in dc microgrids, which are controlled by distributed consensus-based algorithms. In contrast, this article studies the FDIAs in dc microgrids that are controlled hierarchically and based on the droop concept. To the best of authors' knowledge, this article is the pioneer to propose a unified secure model predictive control (MPC)/artificial neural network (ANN)-based framework to detect and mitigiate cyber-attacks in dc microgrids. By exploiting the fast operation feature of model predictive controller and nonlinear mapping capability of ANNs, we can simultaneously

Manuscript received August 21, 2020; revised January 3, 2021 and March 18, 2021; accepted May 6, 2021. *(Corresponding author: Mohammad Reza Habibi.)*

Mohammad Reza Habibi and Frede Blaabjerg are with the Department of Energy Technology, 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 15914, 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.2021.3086145

TABLE I
NOMENCLATURE

β_i^k	Output of the k^{th} neuron in the l^{th} layer.	γ_δ	Weight of the constraint violation penalty.
$f_i(.)$	Activation function.	γ_z	slack variable.
Q_{i-1}	Number of neurons in the $(i-1)^{th}$ layer.	M_z	Decision of the optimization problem.
b_i^k	Bias weight of the k^{th} neuron in the l^{th} layer.	$y_{j,min}(i)$	Minimum possible value of the of the j^{th} output for the i^{th} prediction horizon.
$w_{e,k}^i$	Weight factor from the e^{th} neuron of the $(i-1)^{th}$ layer to 0kˆth$neuron of the$lˆth$layer$.	$y_{j,max}(i)$	Maximum possible value of the of the j^{th} output for the i^{th} prediction horizon.
Z_{x-2}	Vector of the the outputs of the neurons of the $(x-2)^{th}$ layer.	$u_{j,min}(i)$	Lower bound of the j^{th} manipulated variable for the i^{th} prediction horizon.
$W_{x-1,x}$	Wieght matrix of the $(x-1)^{th}$ layer.	$u_{j,max}(i)$	Upper bound of the j^{th} manipulated variable for the i^{th} prediction horizon.
B_{x-1}	Bias vector of the $(x-1)^{th}$ layer.	$\Delta u_{j,min}(i)$	Lower bound of the j^{th} manipulated variable movement for the i^{th} prediction horizon.
$x(z)$	State of the observer.	$\Delta u_{j,max}(i)$	Upper bound of the j^{th} manipulated variable movement for the i^{th} prediction horizon.
$y(z)$	Output of the observer.	$J_{1,n}$	Matrix of ones with the size of $1 \times n$.
$u_e(z)$	Input of the observer.	v_{refj}	Voltage reference in the primary control layer of the j^{th} dc source.
$y_{meas}(z)$	Measured plant output.	ΔV_j	Output of the secondary control layer.
u^r	Real manipulated variable, which is used from $k-1$ to k.	i_j	DC current of the j^{th} dc source.
u^o	Optimal manipulated variable from $k-1$ to k.	R_{D_j}	Droop coefficient of the j^{th} dc source.
Q	Kalman gain matrix.	n	Number of power converters.
p	Prediction horizon.	x^{fd}	False injected data.
num_y	Number of variables for the plan output.	x^r	Real value of the variable.
num_u	Number of variables for the manipulated variables.	x^a	Attacked value of the variable which goes to use in the system.
$\lambda_{i,j}^y$	Tuning weight at i^{th} horizon step of the prediction for the j^{th} plant output.	V_{dc}^r	Real value of the DC bus voltage, which can be gathered by a measurement device.
$\lambda_{i,j}^u$	Tuning weight at i^{th} horizon step of the prediction for the j^{th} manipulated variable.	V_{dc}^a	Attacked and non-real value of the DC bus voltage that goes into the control application.
$\lambda_{i,j}^{\Delta u}$	Tuning weight at i^{th} horizon step of the prediction for the j^{th} manipulated variable movement.	V_{dc}^{fd}	Injected false data into the DC bus voltage.
h_j^y	Scale factor of the j^{th} output of the plant.	V_dc^{min}	Lower bound of the DC bus voltage.
h_j^u	Scale factor of the j^{th} manipulated variable.	V_dc^{max}	Upper bound of the DC bus voltage.

detect and mitigate the cyber-attack. This article focuses on detecting and removing the FDIAs in the dc microgrids to have a secure operation under this type of attack. Also, to have a more efficient evaluation, the proposed strategy is tested under cyber and physical disturbances, i.e., load changes and communication delays. Furthermore, to show the effectiveness of the proposed strategy, the proposed method is examined under a time-varying FDIA. In the case of a time-varying attack, the attacker tries to inject false data into the system, which is variable with time. In this article, a secure control layer is introduced based on MPC approach to detect and also mitigate the FDIAs. To implement the MPC, an estimator based on ANNs is used to produce the reference value for the predictive based controller. In addition, the results of the MPC-based scheme are compared with conventional PI controllers. The obtained results prove the authenticity and effectiveness of the proposed cyber-attack detection and mitigation strategy for dc microgrids.

Briefly, in this article, it will be shown that how a coordination between the ANN and the MPC can be made to provide a secure dc microgrid and improve the cyber-security of the dc microgrid. Therefore, this article introduces a method based on the ANN and also MPC to detect and mitigate FDIAs, simultaneously. It is important to note that, the implemented ANN has a feedforward-based structure, which can reduce the complexity when it is compared with other complex architectures of the ANNs. Also, the historical values of data are used in the input layer of the ANN. It is important to note that, the proposed strategy will be examined under different cyber and physical disturbances, e.g., constant FDIA, time-varying FDIA, load changes, and also the communication delay.

The rest of this article is organized as follows. Section II presents an introduction to the ANN. Section III introduces the model predictive based control approaches, and Section IV describes the dc microgrids and the effect of FDIAs on them. Section V presents the proposed method, and VI illustrates the results. In addition, Section VII provides a discussion and also future works. Finally, discussions and conclusions are stated in Section VIII. It is important to note that, the parameters which are used in this article are defined by Table I.

II. INTRODUCTION TO ANNS

ANNs as a powerful estimation and prediction tools are used in a wide range of applications, e.g., detection of stator interturn faults [23], detection of cyber-attacks in dc microgrids [18], power-sharing [24], sensorless control of dc microgrid [25], and sensorless voltage estimation for total harmonic distortion calculation [26]. Basically, ANNs have an input layer, hidden layers, and one output layer and the layers consist of neurons to help to propagate data from a layer to another layer to produce the outputs of the neural network. Fig. 1 shows the structure of a neural network. Inputs of each neuron are signals, which

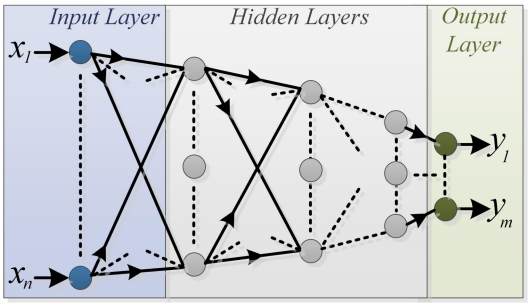

Fig. 1. Basic structure of a neural network with n inputs and m outputs. x_i and y_j are the ith input and jth output, respectively.

are calculated by multiplying a connection weight to the output of the neurons from the previews layer. The output of the kth neuron, which is placed in the ith layer is calculated as follows:

$$\beta_i^k = f_i\left(\left(\sum_{e=1}^{Q_{i-1}} w_{e,k}^i \times \beta_{i-1}^e\right) + b_i^k\right). \tag{1}$$

If the input layer and output layer of a neural network be considered as the first and last layer, and the neural network has l layers, the mathematical description of the jth output is as follows:

$$y_j = f_l(f_{l-1}(Z_{l-2}W_{l-2,l-1} + B_{l-1})W_{l-1,l} + b_l^j). \tag{2}$$

Also, $W_{x-1,x}$, B_x, and Z_x $(1 \le x \le 2)$ are defined as follows:

$$W_{x-1,x} = \begin{bmatrix} w_{1,1}^x & \cdots & w_{1,Q_x}^x \\ \vdots & \ddots & \vdots \\ w_{Q_{x-1},1}^x & \cdots & w_{Q_{x-1},Q_x}^x \end{bmatrix} \tag{3}$$

$$B_x = \begin{bmatrix} b_x^1 & \cdots & b_x^{Q_x} \end{bmatrix} \tag{4}$$

$$Z_x = \begin{bmatrix} \beta_x^1 & \cdots & \beta_x^{Q_x} \end{bmatrix}. \tag{5}$$

To use the ANN, which is built with l layers, a dataset, which is structured by the gathered inputs and outputs data should be prepared. Then, the structured dataset should be used in a training manner as an optimization problem to calculate the optimized values of weights and biases of all neurons. Finally, the neural network with optimized values of biases and weights factors can be implemented in the system.

III. Basic Concepts of MPC

MPC is a type of controller that has gained the attention of researchers in many power engineering applications, e.g., in control of power converters [27], load frequency control [28], and stabilization of dc microgrids [29]. MPC can be implemented as a reference tracking application by calculating the proper future values of the inputs for the plant. This section introduces the basic concepts and mathematical equations [30], [31] of the MPC. Fig. 2 shows the basic way to implement MPC as a reference tracking application.

The model predictive controller uses an observer to estimate the unmeasured values to help predict the future state of the system to adjust the inputs of the plant. The state of the observer

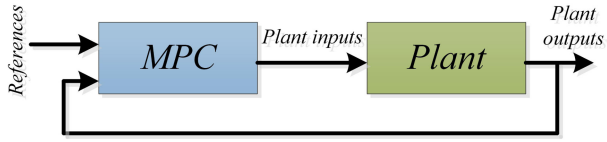

Fig. 2. Implementation of a model predictive controller in a reference tracking application.

can be written as follows:

$$\begin{cases} x(z+1) = Ax(z) + Bu_e(z) \\ y(z) = Cx(z). \end{cases} \tag{6}$$

The state of the controller will be updated based on the previews measurements of the plant as follows [30], [31]:

$$x(z|z) = x^{\text{upd}}(z|z-1) + Ne(z) \tag{7}$$

where $x^{\text{upd}}(z|z-1)$ is the updated $x(z|z-1)$ (the estimated state based on previous control interval $(k-1)$). Furthermore, N is the constant Kalman gain matrix and $e(z)$ is calculated as follows [30], [31]:

$$e(z) = y_{\text{meas}}(z) - (Cx^{\text{upd}}(z|z-1)). \tag{8}$$

In addition, in (7), $x^{\text{upd}}(z|z-1)$ is determined as follows [30], [31]:

$$x^{\text{upd}}(z|z-1) = x(z|z-1) + B(u^r(z-1) - u^o(z-1)). \tag{9}$$

After the calculation and updating the state of the controller, $x(z|z)$ is used to obtain the optimal value of the manipulated variable to be used between zth and $(z+1)$th control intervals. $x(z+1|z)$ can be predicted as follows [30], [31]:

$$x(z+1|z) = Ax^{\text{upd}}(z|z-1) + Bu^o(z) + Qe(z). \tag{10}$$

The MPC-based controller tries to predict the future values of the plant outputs by the observer and then use the predictive values in the optimization process to calculate the optimal values of the inputs to track the references by the plant outputs. So, it is essential to predict the future values of the plant outputs to have a successful control strategy. If assumed that the predicted future of the output is without noise, the observer predicts the first step of the future, and also the i step ahead of the future $(2 \le i \le p$, where p is the prediction horizon) as follows [30], [31]:

$$x(z+1|z) = Ax(z|z) + Bu(z|z) \tag{11}$$

$$x(z+i|z) = Ax(z+i-1|z) + Bu(z+i-1|z). \tag{12}$$

Also, for $1 \le j \le p$, the prediction of the future for the plant is as follows [30], [31]:

$$y(z+j|z) = Cx(z+j|z). \tag{13}$$

To calculate the manipulated variables, the MPC should solve an optimization problem based on the prediction of the future values. To define and solve an optimization problem, a cost function and the constraints should be defined. The cost function can be defined as follows:

$$J(M_z) = J_y(M_z) + J_u(M_z) + J_{\Delta u}(M_z) + J_\delta(M_z) \tag{14}$$

and [30], [31]

$$J_y(M_z) = \sum_{j=1}^{\text{num}_y} \sum_{i=1}^{p} \left(\frac{\lambda_{i,j}^y}{h_j^y} \left[\text{ref}_j(z+i|z) - y_j(z+i|z) \right] \right)^2 \tag{15}$$

$$J_u(M_z) = \sum_{j=1}^{\text{num}_u} \sum_{i=0}^{p-1} \left(\frac{\lambda_{i,j}^u}{h_j^u} \left[u_j(z+i|z) - u_{j,t}(z+i|z) \right] \right)^2 \tag{16}$$

$$J_{\Delta u}(M_z) = \sum_{j=1}^{\text{num}_u} \sum_{i=0}^{p-1} \left(\frac{\lambda_{i,j}^{\Delta u}}{h_j^u} \left[u_j(z+i|z) - u_j(z+i-1|z) \right] \right)^2 \tag{17}$$

$$J_\delta(M_z) = \gamma_\delta \delta_z^2. \tag{18}$$

It is important to note that, the decision of the optimization problem can be defined as follows:

$$M_z^T = \left[u(z|z)^T \quad \cdots \quad u(z+p-1|z)^T \quad \delta_z \right]. \tag{19}$$

As mentioned before, each optimization problem can contain some constraints. For $1 \le i \le p$ and $1 \le j \le \text{num}_y$, the constraint on the output of the plan, manipulated variables and movement of the inputs can be defined as follows [30], [31]:

$$\begin{cases} \frac{y_{j,\min}(i)}{h_j^y} - \delta_z R_{j,\min}^y(i) \le \frac{y_j(z+i|z)}{h_j^y} \\ \frac{y_{j,\max}(i)}{h_j^y} + \delta_z R_{j,\max}^y(i) \ge \frac{y_j(z+i|z)}{h_j^y} \end{cases} \tag{20}$$

where $R_{j,\min}^y(i)$ and $R_{j,\min}^y(i)$ are implemented for the constraint softening. In addition, for $1 \le i \le p$ and $1 \le j \le \text{num}_u$, the constraint on the manipulated variables and movement of the inputs can be defined as follows [30], [31]:

$$\begin{cases} \frac{u_{j,\min}(i)}{h_j^u} - \delta_z R_{j,\min}^y(i) \le \frac{u_j(z+i|z)}{h_j^u} \\ \frac{u_{j,\max}(i)}{h_j^u} + \delta_z R_{j,\max}^u(i) \ge \frac{u_j(z+i|z)}{h_j^u} \end{cases} \tag{21}$$

$$\begin{cases} \frac{\Delta u_{j,\min}(i)}{h_j^{\Delta u}} - \delta_z R_{j,\min}^y(i) \le \frac{u_j(z+i|z)}{h_j^u} \\ \frac{\Delta u_{j,\max}(i)}{h_j^{\Delta u}} + \delta_z R_{j,\max}^{\Delta u}(i) \ge \frac{\Delta u_j(z+i|z)}{h_j^{\Delta u}}. \end{cases} \tag{22}$$

For the optimization of the cost function, the values of the prediction are needed and they can calculated as follows [30], [31]:

$$Y = \Omega x(z) + \Psi u(z-1) + \Phi \Delta U \tag{23}$$

where [30], [31]

$$Y^T = \left[y(z+1) \quad y(z+2) \quad \cdots \quad y(z+p) \right] \tag{24}$$

$$\Omega^T = \left[CA \quad CA^2 \quad \cdots \quad CA^p \right] \tag{25}$$

$$\Psi^T = \left[CB \quad \cdots \quad \sum_{d=0}^{p-1} CA^d B \right] \tag{26}$$

$$\Phi = \begin{bmatrix} CB & 0 & \cdots & 0 \\ CAB + CB & CB & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ \sum_{d=0}^{p-1} CA^d B & \sum_{d=0}^{p-2} CA^d B & \cdots & CB \end{bmatrix} \tag{27}$$

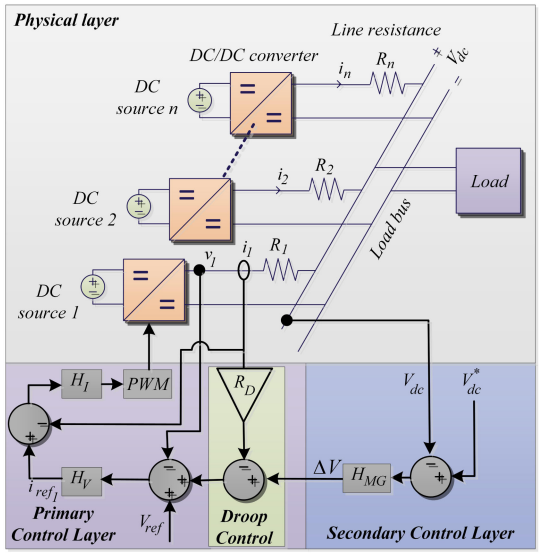

Fig. 3. Physical and control structure of a dc microgrid with n dc sources.

$$\Delta U^T = \left[\Delta u(z) \quad \Delta u(z+1) \quad \cdots \quad \Delta u(z+p-1) \quad \right]. \tag{28}$$

Finally, based on the definition of the cost function and considering the constraints, the predicted values of the future outputs can be implemented into the cost function to obtain the future values of the manipulated variables.

IV. Conventional DC Microgrids and FDIAs

Fig. 3 shows an isolated dc microgrid, which has n parallel dc–dc converters and uses primary and secondary control layers.

The voltage reference in the primary layer is obtained as follows:

$$V_{\text{REF}} = v_{\text{ref}} J_{1,n} + \Delta V - R I_{\text{dc}} \tag{29}$$

where

$$V_{\text{REF}} = \left[v_{\text{ref1}} \quad v_{\text{ref2}} \quad \cdots \quad v_{\text{ref}n} \quad \right] \tag{30}$$

$$\Delta V = \left[\Delta V_1 \quad \Delta V_2 \quad \cdots \quad \Delta V_n \quad \right] \tag{31}$$

$$I_{\text{dc}} = \begin{bmatrix} i_1 & 0 & \vdots \\ 0 & \ddots & 0 \\ \vdots & 0 & i_n \end{bmatrix} \tag{32}$$

$$R = \left[R_{D1} \quad R_{D2} \quad \cdots \quad R_{Dn} \right]. \tag{33}$$

The goal of the secondary control layer is to restore the dc-bus voltage to the desired reference value and it will be shown how FDIAs can affect the secondary control layer and destroy the dc microgrid operation. FDIAs try to inject false data into the system. The model of the FDIA is as follows:

$$x^a = x^r + x^{\text{fd}}. \tag{34}$$

As mentioned earlier, the purpose of the secondary control is to converge the voltage of the dc bus to the desired reference value

and in other hands

$$\lim_{t\to\infty} V_{\rm dc}(t) = V_{\rm ref}. \tag{35}$$

In a nonattack situation, it can be considered that $V_{\rm dc}(t) = V^r_{\rm dc}(t)$, where $V^r_{\rm dc}(t)$ is the real value of the dc-bus voltage, which can be gathered by a measurement device. Therefore

$$\lim_{t\to\infty} V^r_{\rm dc}(t) = V_{\rm ref}. \tag{36}$$

However, if the dc-bus voltage is under an FDIA, the attacked value goes through the secondary control layer and as a result

$$\begin{cases} V^a_{\rm dc}(t) = V^r_{\rm dc}(t) + V^{\rm fd}_{\rm dc}(t) \\ \lim\limits_{t\to\infty} V^a_{\rm dc}(t) = V_{\rm ref}. \end{cases} \tag{37}$$

Therefore, (37) can be converted to

$$\lim_{t\to\infty} V^r_{\rm dc}(t) = V_{\rm ref} - \lim_{t\to\infty} V^{\rm fd}_{\rm dc}(t). \tag{38}$$

If the value of the false data is considered as a constant value such as α ($V^{\rm fd}_{\rm dc}(t) = \alpha$), the following constraints should be satisfied to keep the real converged voltage of the dc bus within the allowed bounds:

$$V_{\rm ref} - \alpha \geq V^{\rm min}_{\rm dc} \tag{39}$$

$$V_{\rm ref} - \alpha \leq V^{\rm max}_{\rm dc}. \tag{40}$$

By unifying (39) and (40), the result will be

$$V_{\rm ref} - V^{\rm max}_{\rm dc} \leq \alpha \leq V_{\rm ref} - V^{\rm min}_{\rm dc}. \tag{41}$$

In other words, if the value of the false data satisfies (41), the dc-bus voltage still will converge to a value within the allowance bound. But, if α satisfies one of the following inequalities, the operation of the dc microgrid can be failed:

$$\alpha \leq V_{\rm ref} - V^{\rm max}_{\rm dc} \tag{42}$$

$$\alpha \geq V_{\rm ref} - V^{\rm min}_{\rm dc}. \tag{43}$$

For more clarification, false data will be injected into a dc microgrid. The reference of the dc-bus voltage is 125 V. To show the effect of the FDIA on a dc microgrid, which has not a secure control layer, two FDIAs start to inject false data with value of -5 and -15, respectively. Fig. 4(a) shows the value of the dc-bus voltage before and also during the first cyber-attack. In addition, Fig. 4(b) depicts the value of the dc-bus voltage before and during the second cyber-attack. Based on Fig. 4, by increasing the domain of the false data, the deviation of the dc-bus voltage from the reference value of that is increased. Also, as it is shown by Fig. 4, the dc-bus voltage is converged based on (38). Therefore, the attacker can increase or decrease the domain of the dc-bus voltage by adjusting the value of the false data.

V. Proposed Secure Control Strategy

In this article, a secure control layer based on ANNs and MPC is considered to detect and mitigate the FDIAs in dc microgrids. The purpose of using MPC is to inject data into the system to remove the effect of the FDIA. For more clarification, Fig. 5 shows the implementation of the predictive controller to mitigate the FDIA in the dc microgrid.

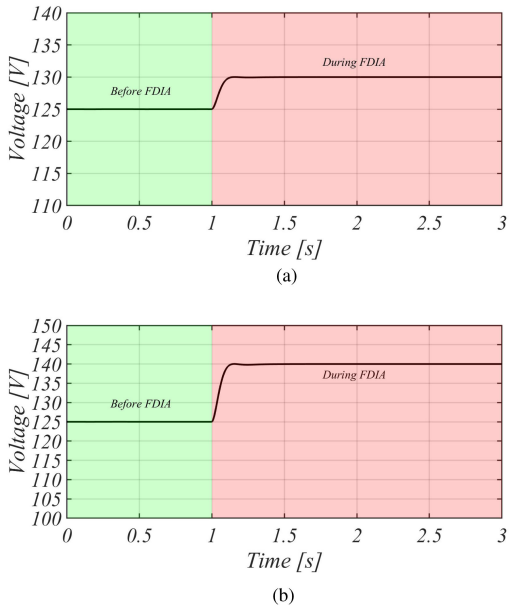

Fig. 4. Value of the dc-bus voltage before and during the FDIA: for (a) $\alpha = -5$, and (b) $\alpha = -15$. (a) Value of the DC bus voltage before and during the first FDIA (the value of the false data is -5). (b) Value of the DC bus voltage before and during the second FDIA (the value of the false data is -15).

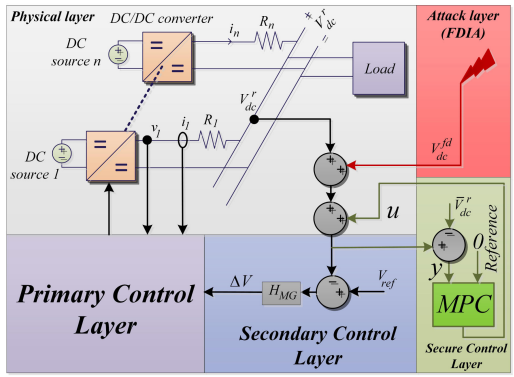

Fig. 5. Implementation of the MPC in the reference tracking application to detect and mitigate the FDIA.

Based on Fig. 5, the purpose of the MPC is to follow the reference (0) by y, which is considered as the output of the plant. By using the MPC, y will converge to 0, then

$$\lim_{t\to\infty} y(t) = 0. \tag{44}$$

In addition

$$y(t) = V^r_{\rm dc}(t) + V^{\rm fd}_{\rm dc}(t) + u(t) - \bar{V}^r_{\rm dc}(t) \tag{45}$$

and as a result

$$\lim_{t\to\infty} (V^r_{\rm dc}(t) + V^{\rm fd}_{\rm dc}(t) + u(t) - \bar{V}^r_{\rm dc}(t)) = 0. \tag{46}$$

In (45) and (46), $\bar{V}^r_{\rm dc}(t)$ is the estimated value of the real voltage of the dc bus. If the estimator works properly, it can

be assumed that $\bar{V}_{\rm dc}^{r}(t) = V_{\rm dc}^{r}(t)$ and (46) will be modified as follows:

$$\lim_{t\to\infty}(V_{\rm dc}^{\rm fd}(t) + u(t)) = 0 \tag{47}$$

and it means that the output of the MPC-based controller removes the false injected data in the system, and the real value of the dc-bus voltage goes through the secondary controller. Also, (47) can be converted as follows:

$$\lim_{t\to\infty} -u(t) = \lim_{t\to\infty} V_{\rm dc}^{\rm fd}(t). \tag{48}$$

Remark: Based on (47), the MPC-based controller produces a value to inject into the system to mitigate the FDIA and based on (48), $-u(t)$ is converged to the value of the false injected data and if $-u(t) \neq 0$, an FDIA is in the dc microgrid.

The proposed method is operated properly if the estimator can estimate the real voltage of the dc bus properly and, in other words, $\bar{V}_{\rm dc}^{r}(t) = V_{\rm dc}^{r}(t)$. To estimate the voltage of the dc bus, the ANN is implemented. The input of the neural network is considered output voltages and currents of dc–dc converters. Also, to have a more efficient and accurate ANN-based estimator, the historical values of the inputs are also considered to use in the input layer of the ANN and a cascaded architecture is considered for the ANN. For example, if the dc microgrid consists of two parallel dc–dc converters and X represents the inputs of the ANN, X can be defined as follows:

$$\begin{aligned} X(t) = [&i_1(t), i_1(t-\Delta t), \ldots, i_1(t-\lambda\Delta t) \\ &v_1(t), v_1(t-\Delta t), \ldots, v_1(t-\lambda\Delta t) \\ &i_2(t), i_2(t-\Delta t), \ldots, i_2(t-\lambda\Delta t) \\ &v_2(t), v_2(t-\Delta t), \ldots, v_2(t-\lambda\Delta t)] \end{aligned} \tag{49}$$

where λ is the input memory order. Furthermore, in the cascaded-based structure of the ANN, each layer is connected to all of the previous layers. It is important to note that the output of the neural network is the real value of the dc-bus voltage, and the estimation of that is called $\bar{V}_{\rm dc}^{r}(t)$.

Fig. 6 shows the proposed method at a glance. First, in the training phase, which happens offline, dataset of the inputs and the output of the neural network are gathered, and the neural network is trained to reach the well-tuned neural networks. After the training phase, the fine-tuned neural network and also the MPC-based controller are implemented online in the attack detection and mitigation proposed strategy.

Briefly, if the system is under the attack, the attacker tries to inject a false data into the system and as a result, the value of the dc-bus voltage, which is sent to the secondary controller, is not equal to the estimated value of that. In other words, the value of the voltage, which is sent to the secondary controller and also the output of the ANN can be different. The MPC is used to inject a faithful data to mitigate the effect of the false data and converge the appeared difference between the gathered dc voltage and also the estimated voltage to zero.

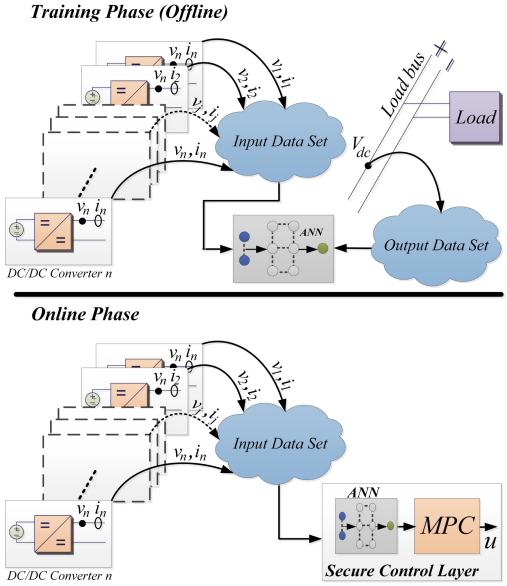

Fig. 6. Implementation of the ANN in training and online phases.

VI. Results

The proposed detection and mitigation strategy is examined under six different scenarios on a detailed simulated dc microgrid. For the Scenarios 1–5, the simulated dc microgrid is structured by two parallel dc–dc buck converters and the line resistances of the dc microgrid are as follows. $R_D = 4$, $R_1 = 0.95\ \Omega$, $R_1 = 0.9\ \Omega$. Also, the dc voltage reference is 125 V. Furthermore, R_D is considered 4. Also, for Scenario 6, the number of parallel dc–dc converters is 6. To use the neural network in the attack detection and mitigation, a neural network is considered with one input layer, one hidden layer, and one output layer. The input and hidden layers have 8 and 10 neurons, respectively. Also, the output layer has one neuron, and the output of that is the estimated value of the dc-bus voltage. The neural network is trained offline, and then, it is implemented online during the operation. To train the neural network, the simulation was run to gather data. The duration of the simulation to gather data is considered 10 s, and the sampling time is 10μs, and as a result, 10^6 samples of the inputs are gathered. It is important to note that for extracting the dynamic of the system by using the gathered data, several load changes are considered during the gathering data in the offline training phase. Also, the time delay is considered one. As will be shown later, the neural network with a time-delay of one works properly. Then, to avoid the complexity and reduce the computational burden of this application, time delay of one is used in the proposed strategy, and it is avoided to increase the time delay. Also, because the false data are arbitrary data, no inequity constraint is considered for the optimization process in the MPC application.

It is important to note that, to train the ANN, the training dataset is divided into the following three sets, i.e, training, validation, and testing. Also, the percentage of training, validation, and testing dataset are 70%, 15%, and 15%, respectively. Also, for the training phase, the number of epochs was 1000. After the

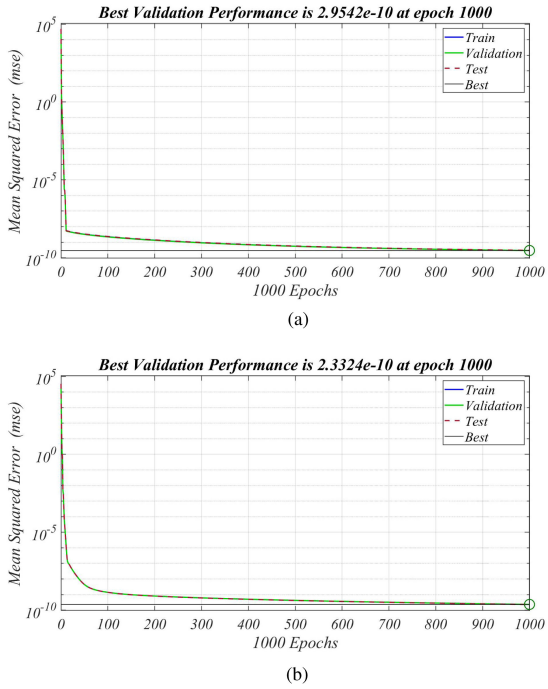

Fig. 7. MSE during the training. (a) Mean squared error (mse) of the ANN for the microgrid with two DC/DC converters. (b) Mean squared error (mse) of the ANN for the large scale DC microgrid.

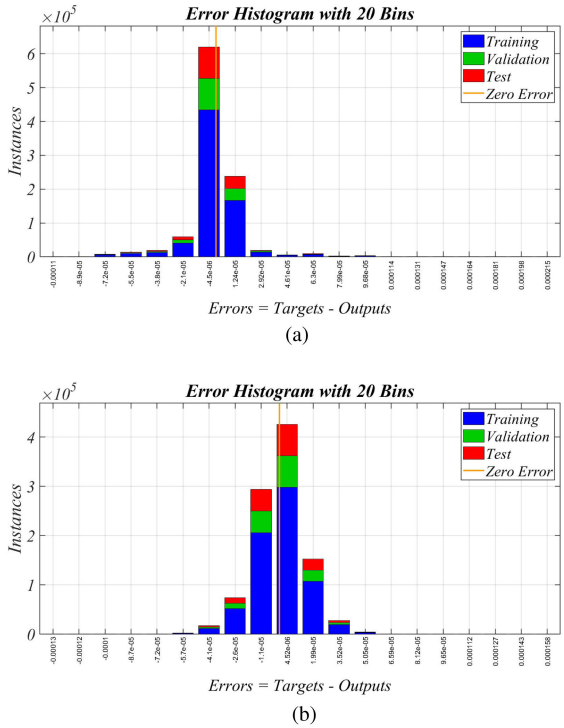

Fig. 8. Error Histogram of the ANN. (a) Error Histogram of the ANN for the DC microgid with two DC/DC converters. (b) Error Histogram of the ANN for the large scale DC microgid.

training, the trained ANNs were implemented into the secure control layer. Fig. 7 shows the mean squared error (MSE) during the training. In addition, Fig. 8 depicts the error histogram with 20 bins for the training phase. It is important to note that, in Fig. 8, the targets are the real values of the dc-bus voltage during the training phase and outputs are the output of the ANN.

It is worth mentioning that, as it will be shown later, the proposed strategy is tested under different scenarios (e.g., load changing, time-varying FDIA, communication delay, and large scale dc microgrid). As mentioned before, to use the ANNs, they have been trained and the number of epochs was 1000. Based on the mse during the training (see Fig. 7), the best validation performances were 2.9542×10^{-10} at epoch 1000 and 2.3324×10^{-10} at epoch 1000 for the dc microgrid with two and six dc–dc converters, respectively. In addition, based on the error histogram of the ANNs for the dc microgrids (see Fig. 8), it is indicated that the values of the most of the instances for the errors are very closed to zero (based on the bins).

A. *Case Study 1: Different FDIAs (Two Converters)*

This scenario evaluates the performance of the proposed strategy under FDIAs with different values of the false injected data. In this scenario, a false data with a value of -25 is injected into the system at $t = 1$ s. Then, the value of the false data is changed to 25, -50, and 50 at $t = 2$ s, $t = 3$ s and $t = 4$ s, respectively. Fig. 9(a) shows the dc-bus voltage ($V_{\rm dc}^r$) and also the estimated value of the dc-bus voltage ($\bar{V}_{\rm dc}^r$) by the neural network. As can be seen in Fig. 9(a), the false data are removed from the system after a transient time. Also, the real value and also the estimated value of the dc-bus voltage are fitted to each other. As a result, it can be concluded that the neural network and model predictive controller work properly, and they are successful to estimate the dc-bus voltage and mitigate the FDIA with different values of the false data. Furthermore, Fig. 9(b) illustrates the currents of converters and based on Fig. 9(b), the current sharing is done under the secure control proposed strategy. Also, Fig. 9(c) depicts the real value of the false injected data ($V_{\rm dc}^{\rm fd}$) and the estimated value of the false data ($-u$, where u is the output of the model predictive controller). Based on Fig. 9(c), the proposed strategy can calculate and remove the false data, properly. It is important to note that, Fig. 9(d) shows the error of estimation. Based on Fig. 9(d), the domain of the estimation error during the transient state after the injection of the first, the second, and the third false data is smaller than 0.5 mV and it is less than 1 mV during the transient state and after the injection of the last false data. In addition, based on Fig. 9(d), the estimation error during the steady state can be neglected and it is very close to zero. Therefore, in the worst case, the estimation error is less that 1 mV and as a result (if the voltage is 125 V), it can be concluded that, the domain of the percentage of the estimation error for the worst case can be less than 0.0008 and it can show the very good performance of the ANN.

B. *Case Study 2: FDIA and Laod Changing (Two Converters)*

The goal of this scenario is to test the proposed strategy under load changing. To evaluate the proposed strategy, a load is added at $t = 1$ s to the dc microgrid. Also, at $t = 2$ s, an attack starts

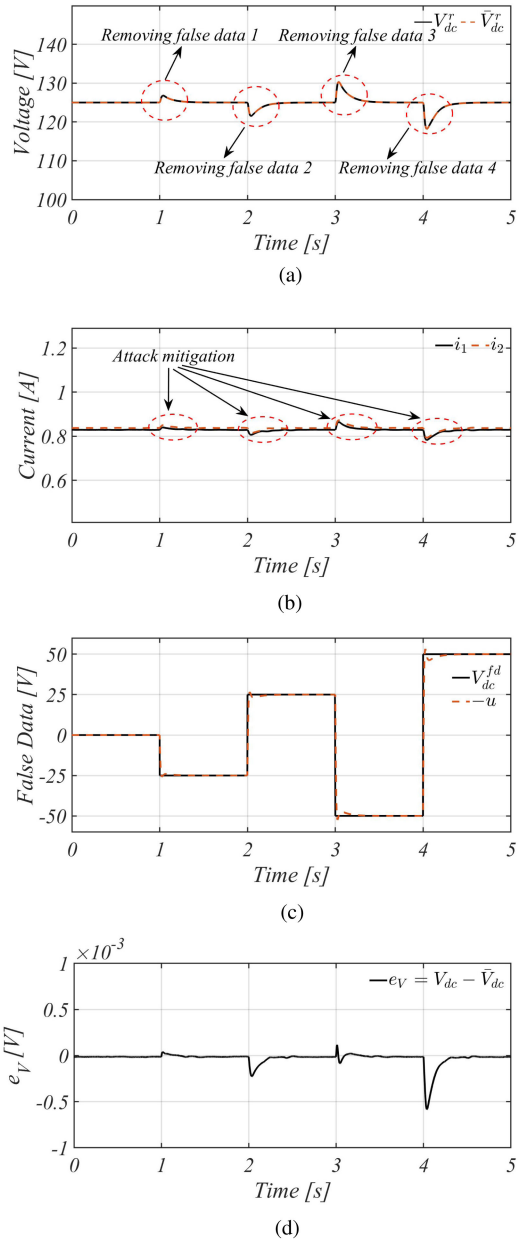

Fig. 9. Case Study 1: Values of (a) dc-bus voltage and the estimated value of that, (b) dc output currents, (c) real value and estimated value of the false data, and (d) estimation error.

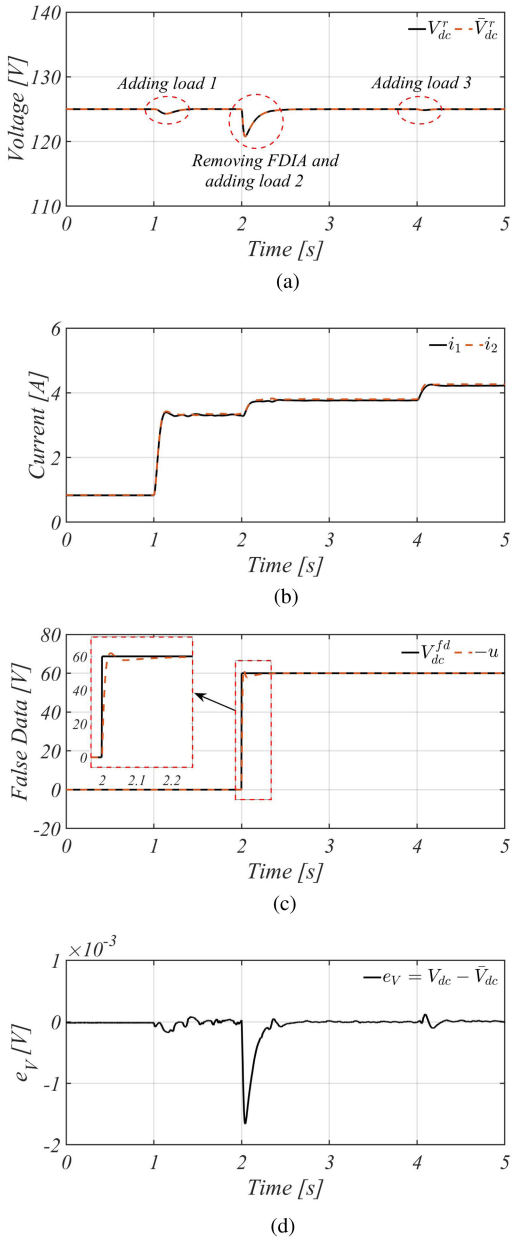

Fig. 10. Case Study 2: Values of (a) dc-bus voltage and the estimated value of that, (b) dc output currents, (c) real value and estimated value of the false data, and (d) estimation error.

to inject a false data to the system and simultaneously, a load is added to the system too. Finally, at $t = 4$ s, a load is added to the microgrid while the system is under the attack. Fig. 10(a) is related to the real and estimated values of the dc-bus voltage. Based on Fig. 10(a), the proposed method can remove false data even in the case of load changing. It is important to note that, at $t = 1$ and $t = 4$ s, a little disturbance is on the dc-bus voltage, but after a transient time, they are mitigated, and those are due to the load changing. Fig. 10(b) shows the output currents of converters. Also, Fig. 10(c) illustrates the false injected data by the FDIA and the estimated value of that by the proposed strategy. Fig. 10(c) can prove that the proposed method can estimate and mitigate the false injected data, precisely. Also, Fig. 10(d) is related to the error of estimation. Based on Fig. 10(d), the value of the estimation error is very close to zero and in the worst case (during the transient state after $t = 2$ s), the domain of the estimation error is smaller than 2 mV. So, in the worst case, the domain of the estimation error is less than 2 mV and if the dc voltage is 125 V, it can be mentioned that, the domain of the percentage of the estimation error for the worst case can be less than 0.0016 and it can prove the very good performance of the ANN during this scenario.

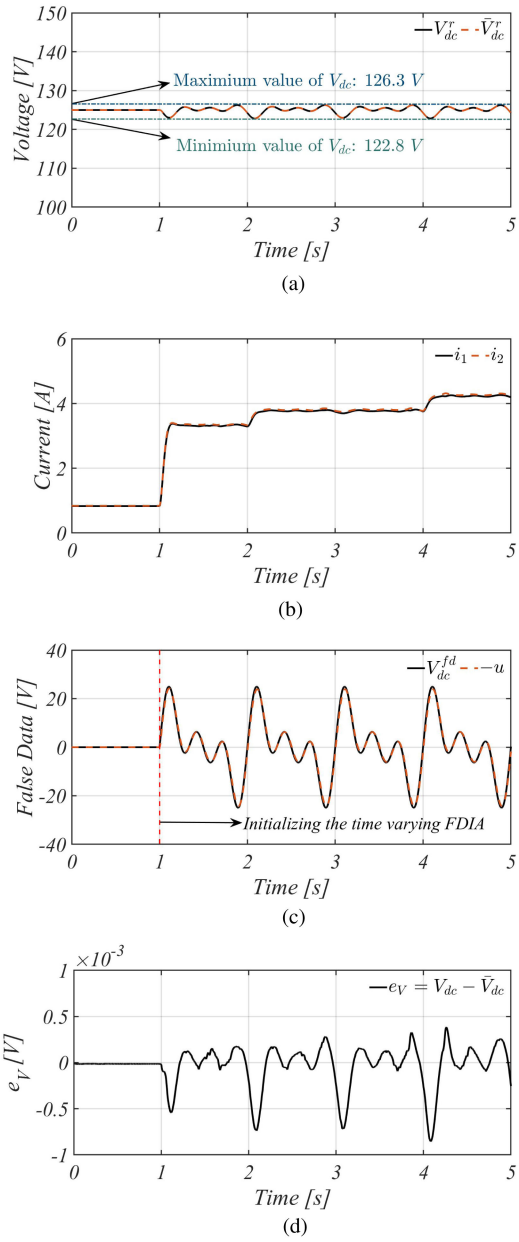

Fig. 11. Case Study 3: Values of (a) dc-bus voltage and the estimated value of that, (b) dc output currents, (c) real value and estimated value of the false data, and (d) estimation error.

C. Case Study 3: Time-Varying FDIA (Two Converters)

In this scenario, the effectiveness of the neural network-based model predictive controller under a time-varying FDIA is evaluated. In this scenario, loads are added to the dc microgrid at $t = 1\,\text{s}$, $t = 2\,\text{s}$, and $t = 4\,\text{s}$ as in the case study 2. Also, the time-varying attack is initialized in the dc microgrid at $t = 1\,\text{s}$. The time-varying false data are described as follows:

$$V_{\text{dc}}^{\text{fd}}(t) = 10\left[\sin(2\pi t) + \sin(4\pi t) + \sin(6\pi t)\right]. \tag{50}$$

Fig. 11(a) illustrates the dc-bus voltage and the estimated value of that. Based on Fig. 11(a), the dc-bus voltage has a fluctuation between 126.3 and 122.8 V because of the time-varying FDIA. Considering that the reference value of the dc-bus voltage is 125 V, it can be concluded that the dc-bus voltage deviation is between -1.76% and 1.04%, and it is an acceptable deviation. Furthermore, Fig. 11(b) shows the currents of the converters, and it illustrates the successful current sharing in the dc microgrid. Also, Fig. 11(c) depicts the injected false data and the estimated value of that. As can be seen in Fig. 11(c), the proposed method can estimate the false data properly, even in the case of the time-varying FDIA. Furthermore, Fig. 11(d) illustrates the error of estimation. Based on Fig. 11(d), the domain of the estimation error is smaller than 1 mV and during the injection of the false data, the values of the upper and the lower bounds for the dc-bus voltage are 126.3 and 122.8 V. Therefore, in the worst case, the domain of the percentage of the estimation error can be less than 0.0008144 and it can prove the effectiveness of the ANN even it is under a time-varying FDIA.

D. Case Study 4: FDIA and Communication Delay (Two Converters)

In this scenario, the proposed strategy is examined under a communication delay. A delay of 3 ms is considered to send the data from the secondary controller to the primary controller of both units. Fig. 12(a) is related to the real and estimated values of the dc-bus voltage and Fig. 12(b) depicts the output currents of the converters. Fig. 12(a) shows that the ANN can estimate the dc-bus voltage properly under the time delay. It is important to note that in Fig. 12(a) and (b) fluctuations exists because of the delay effect. Also, Fig. 12(c) illustrates the real and estimated values of the false injected data. Based on Fig. 12(c), the proposed strategy can calculate the value of the false data, properly. In addition, Fig. 12(d) shows the error of estimation. Based on Fig. 12(d), during the transient state and steady state, the domain of the estimation error is smaller than 0.5 mV. If the reference of the voltage is 125 V and the worst value of the estimation error is less than 0.5 mV, the domain of the percentage of the estimation error can be less than 0.0004 and it can show the proper performance of the ANN even it is under a communication delay.

E. Case Study 5: Comparison of the Proposed Strategy and PI Controller (Two Converters)

In this scenario, the performance of the MPC based proposed method is compared with a PI-based strategy. The model predictive based controller is completely replaced by a tuned PI controller. A false data with value of +100 is injected into the system at $t = 1\,\text{s}$. Fig. 13(a) shows the dc-bus voltage by the proposed strategy and PI-based application, i.e., $V_{\text{dc}}^{\text{mpc}}$ and $V_{\text{dc}}^{\text{pi}}$, respectively. Based on Fig. 13(a), the minimum values of $V_{\text{dc}}^{\text{mpc}}$ and $V_{\text{dc}}^{\text{pi}}$ are 118.1723 and 77.2855 V, respectively. Therefore, because the reference for the dc-bus voltage is 125 V, the maximum deviation by the proposed MPC based method and the PI-based application are 5.46% and 38.17%, respectively. In addition, Fig. 13(b) illustrates the estimated values of the false data by the MPC- and PI-based methods. As it is shown by Fig. 13(b), the PI-based approach can estimate the value of the

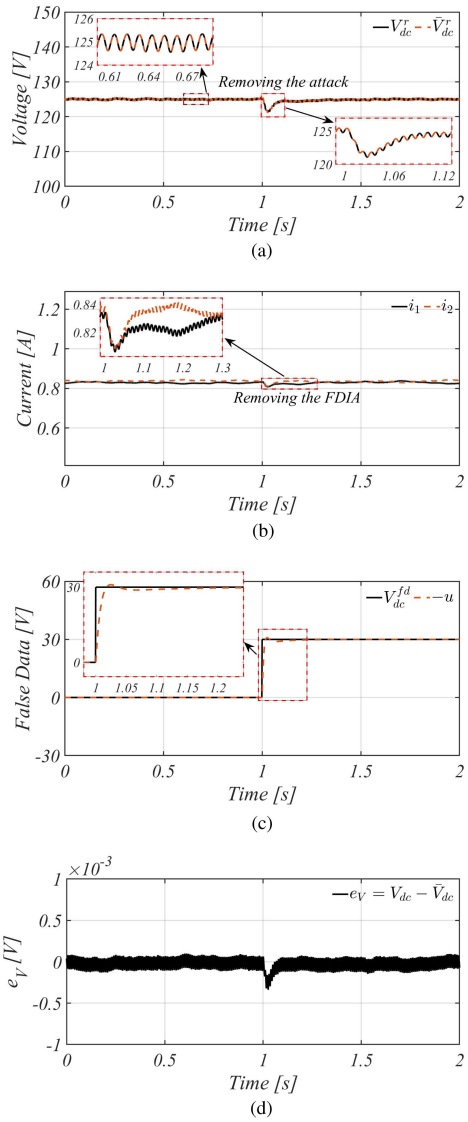

Fig. 12. Case Study 4: Values of (a) dc-bus voltage and the estimated value of that, (b) dc output currents, (c) real value and estimated value of the false data, and (d) estimation error.

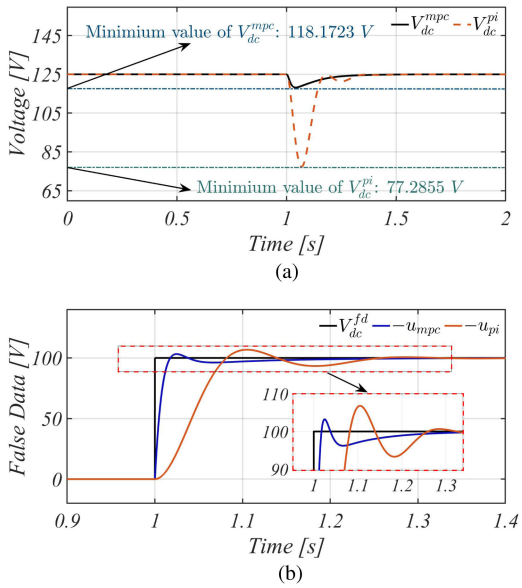

Fig. 13. Case Study 5: The values of (a) dc-bus voltage, and (b) estimated values of the false injected data by the MPC and the PI controller.

false data, but the MPC-based application is more successful because of smaller overshoot and also faster response. Briefly, the maximum deviation of the dc-bus voltage by the PI-based application is very larger than MPC-based strategy. Also, because of the less overshoot and faster response time of the MPC-based method, the MPC is more successful rather than the PI controller.

F. Case Study 6: Large Scale DC Microgrid (Six Converters)

In this scenario, the performance of the proposed method is evaluated in a more complex dc microgrid with six dc–dc converters. In this scenario, a false data with a value of +30 at $t = 1$ s is injected into the system. Fig. 14(a) shows the real and estimated values of the dc-bus voltage, and it is shown that the neural network estimates the dc-bus voltage, precisely. In addition, Fig. 14(b) illustrates the output currents of converters. Based on Fig. 14(a) and (b), the attack is removed successfully. Furthermore, Fig. 14(c) depicts the value of the false injected data and the estimated value of that. As it is shown, the proposed strategy can estimate the value of the false data. Furthermore, Fig. 14(d) is related to the error of estimation. Based on Fig. 14(d), in the worst case and during the transient state after $t = 1$ s, the domain of the estimation error is smaller than 0.5 mV. So, if the dc-bus voltage is 125 V and the worst value of the estimation error is less than 0.5 mV, the domain of the percentage of the estimation error can be less than 0.0004. Therefore, Fig. 14(d) can show the effectiveness of the ANN even it is implemented in a large scale dc microgrid.

VII. Discussion and Future Work

This article introduced a method to detect and mitigate FDIAs in dc microgrids. The proposed strategy tried to show that how a positive and constructive cooperation between artificial intelligence (AI) and the MPC can be made to increase the cyber-security of the dc microgrid. In this article, the ANN as a type of AI-based application was used to be implemented in the proposed strategy. To have a more dynamic ANN, a historical value of the input was considered to be implemented into the ANN. In addition, a comparison between MPC and a traditional PI controller was done. Based on the obtained results, the MPC-based strategy was more successful due to faster response and also smaller overshoot. So, the MPC was more successful in transient and also steady state. It is important to note that, MPC-based approach needs to solve an optimization problem and it can increase the computational burden. It is worth mentioning that, if the system has not a cyber-attack mitigation strategy, as it has been shown before, by injecting the false data into the system, the attacker can change the value of the voltage of the dc bus. So, if the attacker is able to inject the false data into the system, the attacker can change the value of the dc-bus voltage to a value, which is out of the allowance bounds. Therefore, the outage of the dc bus can be happen and

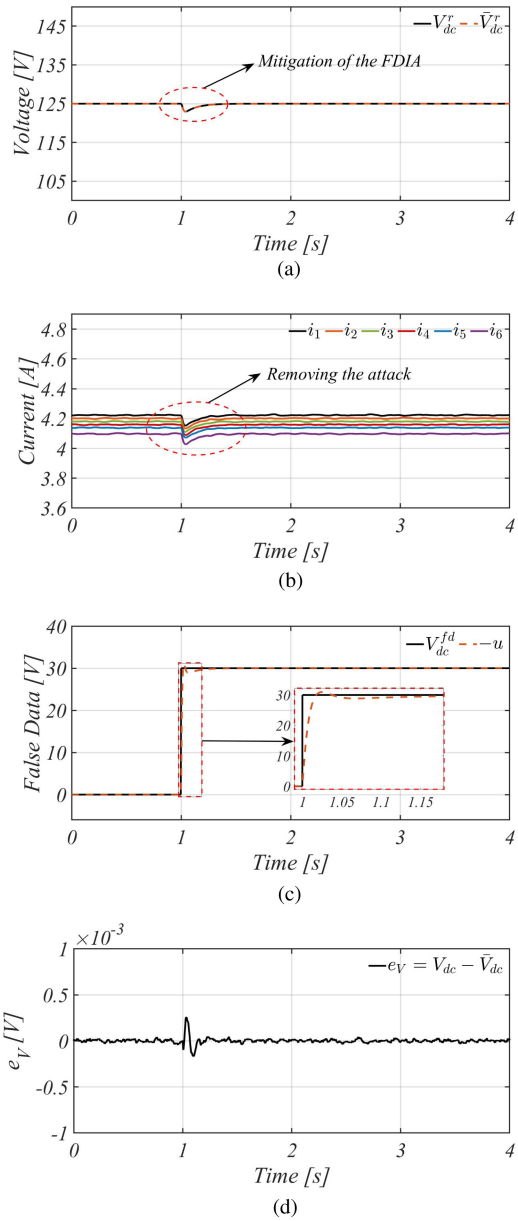

Fig. 14. Case Study 6: Values of (a) dc-bus voltage and the estimated value of that, (b) dc output currents, (c) real value and estimated value of the false data, and (d) estimation error.

consequently, it may result to the outages of the dc sources, which are connected to the attacked dc bus. Briefly, the attacker can make a plan to inject a false data into the system to make the dc microgrid shutdown and as a result, it is important to have a strategy to detect and mitigate cyber-attacks for the dc microgrids. In the future work, a method based on AI can be introduced to mitigate other types of cyber-attacks.

VIII. Conclusion

In this article, a new method was proposed based on MPC to detect and mitigate FDIAs in dc microgrids, which uses the ANN to implement to produce the reference for the model predictive based controller. The goal of this article is to show that how the ANN and MPC can be coordinated to detect and mitigate FDIAs in dc microgrids. To reduce the complexity of the proposed strategy, a simple structure of the ANNs was used. Therefore, the implemented ANN had a feedforward-based architecture. Also, to improve the performance of the ANN, the historical value of the data was considered as the inputs of the ANN. The function of the model predictive based controller is to inject the proper data to counteract the effect of the cyber-attacks in the system. Finally, the performance of the proposed strategy was evaluated under the normal operation, the load changing events, the communication delay, as well as under the time-varying attack by performing simulations in MATLAB/Simulink software environment. The obtained results show the effectiveness of the proposed strategy for secure cyber-attack detection and mitigation. By using the proposed MPC/ANN-based strategy, successful cooperation between MPC and ANN is achieved to detect and remove FDIAs in dc microgrids. To conclude this article, it is important to note that, by adjusting and modifying the proposed framework, it can be applied to provide a secure operation for other types of cyber-physical systems.

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] M. A. Bianchi, I. G. Zurbriggen, F. Paz, and M. Ordonez, "Improving DC microgrid dynamic performance using a fast state-plane-based source-end controller," *IEEE Trans. Power Electron*, vol. 34, no. 8, pp. 8062–8078, Aug. 2019.

[3] 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.

[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] S. K. Sahoo, A. K. Sinha, and N. K. Kishore, "Control techniques in AC, DC, and hybrid AC-DC microgrid: A review," *IEEE J. Emerg. Sel. Topics Power Electron*, vol. 6, no. 2, pp. 738–759, Jun. 2018.

[6] L. Che, M. Shahidehpour, A. Alabdulwahab, and Y. Al-Turki, "Hierarchical coordination of a community microgrid with AC and DC microgrids," *IEEE Trans. Smart Grid*, vol. 6, no. 6, pp. 3042–3051, Nov. 2015.

[7] A. Tah and D. Das, "An enhanced droop control method for accurate load sharing and voltage improvement of isolated and interconnected DC microgrids," *IEEE Trans. Sustain. Energy*, vol. 7, no. 3, pp. 1194–1204, Jul. 2016.

[8] J. Ma, L. Yuan, Z. Zhao, and F. He, "Transmission loss optimization-based optimal power flow strategy by hierarchical control for DC microgrids," *IEEE Trans. Power Electron.*, vol. 32, no. 3, pp. 1952–1963, Mar. 2017.

[9] Q. Shafiee, T. Dragičević, J. C. Vasquez, and J. M. Guerrero, "Hierarchical control for multiple DC-microgrids clusters," *IEEE Trans. Energy Convers.*, vol. 29, no. 4, pp. 922–933, Dec. 2014.

[10] S. Sahoo, J. C. Peng, D. Annavaram, 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.

[11] 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.*, to be published, doi: 10.1109/JESTPE.2021.3050851.

[12] J. Liu, X. Lu, and J. Wang, "Resilience analysis of DC microgrids under denial of service threats," *IEEE Trans. Power Syst.*, vol. 34, no. 4, pp. 3199–3208, Jul. 2019.

[13] S. Sahoo, J. C. 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.

[14] A. Afshari, M. Karrari, H. R. Baghaee, and G. B. Gharehpetian, "Resilient synchronization of voltage/frequency in AC microgrids under deception attacks," *IEEE Syst. J.*, vol. 15, no. 2, pp. 2125–2136, Jun. 2021

[15] T. Tran, O. Shin, and J. Lee, "Detection of replay attacks in smart grid systems," in *Proc. Int. Conf. Comput., Manage. Telecommun.*, 2013, pp. 298–302.

[16] 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.

[17] 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: Express Briefs*, vol. 68, no. 2, pp. 717–721, Feb. 2021.

[18] M. R. Habibi, H. R. Baghaee, T. Dragičević, and F. Blaabjerg, "Detection of false data injection cyber-attacks in DC microgrids based on recurrent neural networks," *IEEE Trans. Emerg. Sel. Topics Power Electron.*, pp. 1–1, 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. Inf.*, vol. 15, no. 7, pp. 4066–4075, Jul. 2019.

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

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

[22] 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.

[23] L. S. Maraaba, Z. M. Al-Hamouz, A. S. Milhem, and M. A. Abido, "Neural network-based diagnostic tool for detecting stator inter-turn faults in line start permanent magnet synchronous motors," *IEEE Access*, vol. 7, pp. 89014–89025, 2019.

[24] H. R. Baghaee, M. Mirsalim, G. B. Gharehpetian, and H. A. Talebi, "Unbalanced harmonic power sharing and voltage compensation of microgrids using radial basis function neural network-based harmonic power-flow calculations for distributed and decentralised control structures," *IET Gener., Transmiss. Distribution*, vol. 12, no. 7, pp. 1518–1530, 2018.

[25] A. N. Akpolat *et al.*, "Sensorless control of DC microgrid based on artificial intelligence," *IEEE Trans. Energy Convers.*, pp. 1–1, 2020.

[26] B. Adineh, M. R. Habibi, A. N. Akpolat, and F. Blaabjerg, "Sensorless voltage estimation for total harmonic distortion calculation using artificial neural networks in microgrids," *IEEE Trans. Circuits Syst. II: Express Briefs*, to be published, doi: 10.1109/TCSII.2021.3059410.

[27] T. Dragičević, "Model predictive control of power converters for robust and fast operation of AC microgrids," *IEEE Trans. Power Electron.*, vol. 33, no. 7, pp. 6304–6317, Jul. 2018.

[28] F. Banis, D. Guericke, H. Madsen, and N. K. Poulsen, "Load-frequency control in microgrids using target-adjusted MPC," *IET Renewable Power Gener.*, vol. 14, no. 1, pp. 118–124, 2020.

[29] T. Dragičević, "Dynamic stabilization of DC microgrids with predictive control of point-of-load converters," *IEEE Trans. Power Electron*, vol. 33, no. 12, pp. 10872–10884, Dec. 2018.

[30] E. F. Camacho and C. Bordons, *Model Predictive Control*. London, U.K.: Springer-Verlag, 2007.

[31] [Online]. Available: https://se.mathworks.com/products/mpc.html