Electrical Power and Energy Systems 145 (2023) 108586

Contents lists available at ScienceDirect

International Journal of Electrical Power and Energy Systems

journal homepage: www.elsevier.com/locate/ijepes

Resilient operation of DC microgrid against FDI attack: A GRU based framework☆

Qiaohui He, Priyank Shah, Xiaowei Zhao *

Intelligent Control & Smart Energy(ICSE) Research Group, School of Engineering, University of Warwick, Coventry CV4 7AL, United Kingdom

ARTICLE INFO

Keywords:
Distributed generation
Power converter
Power electronics
Smartgrid
Solar energy conversion system

ABSTRACT

DC microgrid is the most susceptible to cyber-attacks as the communication channel is involved for the implementation of the secondary controller. Accordingly, the false data are injected into the transmitted data (i.e., DC bus voltage) and it may lead to deteriorating the system performance. To address these issues, the gated recurrent unit (GRU) based mechanism is presented to eliminate the false data injection (FDI) attack for the resilient operation of the DC microgrid. The presented GRU-based framework is divided into two parts: 1) estimation strategy: an offline-trained GRU based network is employed herein for online evaluation of the actual DC bus voltage, and 2) mitigation strategy: GRU based trained network is exploited herein with an amalgamation of the proportional-integral (PI) controller to counteract the malicious cyber-attack. The presented GRU-based framework has several advantages such as ease of implementation and computationally efficient, unlike state-of-art methods. The sensitivity analysis is investigated herein to validate the effectiveness of the presented GRU-based framework over state-of-art techniques. Simulation results show satisfactory performance under manifold operating scenarios such as bias injection attack and time-varying attack. In addition, the quantitative and qualitative comparative performances are performed herein to demonstrate the efficacy of the presented framework.

1. Introduction

Nowadays, renewable energy sources (e.g. solar, wind, biomass, geothermal, etc.) are booming into the distribution energy sector as the traditional forms of power generation (e.g. coal-based thermal power generation) increase the concern over greenhouse gas, acid rain, climate change, and global warming, etc. To address these issues, several researchers have investigated the AC and DC microgrid in the literature [1–3] for the reliable operation of the centralized network. Nonetheless, the DC microgrid has several advantages [2–5] over the AC microgrid such as low cost, low complexity, high reliability, energy efficient, etc. Several configurations of the power electronic converters are described in [6–8] for an application of the DC microgrid. This DC microgrid network [6–8] is susceptible to cyber-attacks as the centralized and hierarchical controllers require a communication channel for its reliable operation. The attack model in a cyber-physical system [9,10] is divided into three categories: disclosure attacks, deception attacks, and disruption attacks. The disclosure attacks try to steal and collect vital information from the system and it may be used for the next attack in the future. The false-data injection (FDI) and the replay attacks are categorized as the deception attacks [9,10], where the attacker destroys the real data of the system to compel the destabilization of the overall system. The disruption attack is popularly known as a denial of service (DoS) attack [9,10], where the attacker prevents the data and makes it inaccessible to the controller

Several researchers [11–14] have investigated resilient strategies to alleviate the FDI attack as it is the most common attack in the cyber-physical system (CPS). In the DC microgrid, a hierarchical control is investigated in [11] for flexible regulation of the output voltage and current, however, this control strategy fails to provide stable operation under cyber-attack. To address this issue, the FDI counteract framework is analyzed in [12] to identify the attack signal using the Daikon dynamic invariant detector. Likewise, Sahoo *et. al.* [13] have analyzed a cooperative vulnerability factor-based framework to identify the attack for each agent of the DC microgrid. However, these controllers [12,13] fail to provide resilient operation under the presence of disturbances in the current components. A discordant element-based approach is described in [14] to detect destabilization and deception attacks by

☆ This work has received funding from the UK Engineering and Physical Sciences Research Council under grant EP/S001905/1.
* Corresponding author.
E-mail address: Xiaowei.Zhao@warwick.ac.uk (X. Zhao).

https://doi.org/10.1016/j.ijepes.2022.108586
Received 4 January 2022; Received in revised form 17 July 2022; Accepted 30 August 2022
Available online 8 October 2022

Table 1
State-of-Art Resilient Techniques Against Attack.

Ref.	Technique	Type of application	Reconstruct False data	Complexity	Limitation
[26]	Sliding mode observer	Buck converter	Feasible	High	Chattering problem
[27]	Sliding mode observer-based resilient approach	AC microgrid	Not feasible	High	Chattering problem
[28]	Adaptive control	Bidirectional interleaved converter	Not Feasible	High	Only consider impulsive FDI attack
[8]	Trust-based cooperative controller	Buck converter	Not Feasible	Medium	More than half of the neighbours should be healthy.
[29]	Adaptive control	Nonlinear cyber-physical systems	Not feasible	Medium	Not applied to the actual model
[30]	Luenberger observer and artificial neural network	Load frequency control system	Feasible	High	Not consider the communication delay
[31]	Sliding mode observer-based	F-404 aircraft engine system	Not feasible	High	The transition rates of the considered Markovian jump system are assumed to be known
[32]	Artificial neural network	Buck converter	Feasible	Low	Fails Performance with disturbance of input of a neural network
[33]	LSTM and adaptive neuro-fuzzy inference system	Energy management system	Not Feasible	High	Accuracy is conceded to the calculation ratio

analyzing the consensus-based cooperative control network. Nonetheless, the value of the discordant element in [14] abruptly changes as the cyber-attack is occured in the DC microgrid.

The model-based FDI attack frameworks [15–23] are the most common approach to ensure the resilient operation of the microgrid. An event-driven resilient control mechanism is analyzed in [18] to suppress the impact of attack signal from both voltage and current measurements of the DC microgrid. Accordingly, the event signal is actuated as one of the agents is attacked, thereafter, the trusted neighbor agents rebuild the estimated value, which is used in the consensus controller. In literature [19,20], a model-based command authentication strategy to detect and mitigate attacks for multi-agent power system is put forward. The stealthy attacks targeting the economic dispatch control signal from centralized control centre to generating units is modelled. The proposed mitigation method can restore system from the attacks and make the system perform in optimal operation. In case of poor coordination between these agents [21], the performance of the system can be deteriorated under cyber-attack. Researchers [22,23] have addressed these issues with help of an adaptive control strategy to compensate the impacts of malicious cyber-attacks (e.g., at the output of the secondary controller) in the distributed power generation system. Cecilia *et. al.* [23] have analyzed the reconstruction approach to obtain the original data from the measured signal, however, this strategy is restricted to constant power loads. In addition, the nonlinear sliding mode observer is incorporated in [23] to estimate the states of the system, which leads to chattering phenomena in the converter and yields to the high heat losses in the power circuits. In essence, the model-based technique has several disadvanatges, which can be summarized as follows:

- Highly dependent on the precision of the modelling
- Performance is affected by the uncertainty in the parameters
- Most of the model-based method linearizes the nonlinear system which reduces the effectiveness of the approach
- It may be invalid when the hacker knows the information of the whole system

Therefore, continuous development of resilient techniques is necessary for the reliable operation of DC microgrid systems.

Data-driven techniques [24,25,32] are booming in power electronics system as it needs to build the relationship between variables of a system, which is easier to be applied in the real-time CPS. The cons of the model-free based techniques can be concluded as:

- Implemented without having knowledge of the system model
- High precision
- Easy application in nonlinear system

Several researchers have designed data-driven techniques [24,32] for resilient operation under deception attacks. A nonlinear neural network method is realized in [24] to detect the FDI attack in the voltage and current measurement of the DC microgrid. The deep-learning-based strategy is analyzed in [25] for satisfactory operation of the DC microgrid, which combines a deep-learning-based identification scheme with a state vector estimator to capture behavior features of the attack signal. The summary of state of art resilient techniques against attack is shown in Table 1.

The artificial neural network (ANN) based controller is employed in [32] to mitigate the FDI attack on parallel-connected buck converters in the DC microgrid. However, ANN is the simplest structure of the neural network. In order to learn more complicated and nonlinear relationships between the data, especially the time series data, the deep learning method is popular as it consists of multiple layers of neural network. Nonetheless, accumulating the ANN for a deeper layer cannot get the desired result in certain scenarios [34]. It may suffer from the overfitting issues, where estimated error decreases at first, thereafter, it will rise because of having multiple layers in ANN. To solve these problems, the recurrent neural network (RNN) is designed in the literature [34]. Despite that, RNN has the drawback of remembering long time sequences [34], which leads the long short-term memory (LSTM). The LSTM is widely adopted in the prediction of the power and energy sector [35]. Nevertheless, it suffers from a large computational burden. Therefore, the gated recurrent unit (GRU) is developed in [36], which is an advanced version of the recurrent neural network and it solves the vanishing gradient problem of the RNN. In addition, it is capable to analyze the intrinsic relationship of sequence like LSTM does but it is more concise than LSTM [37]. The estimation of DC bus voltage is highly related to the precision of input variants of the neural network (i.e., if there is a disturbance of the input variants and the estimation of the attack signal is not precise enough, the effectiveness of the mitigation method is reduced). To solve this problem, the GRU-based framework in this paper is proposed for DC microgrid system. It performs lower sensitivity against the disturbance of the input signal. The main contributions of this article are explained as follows:

- A GRU-based resilient framework is presented herein to mitigate the impact of the FDI attack on the DC microgrid. The presented

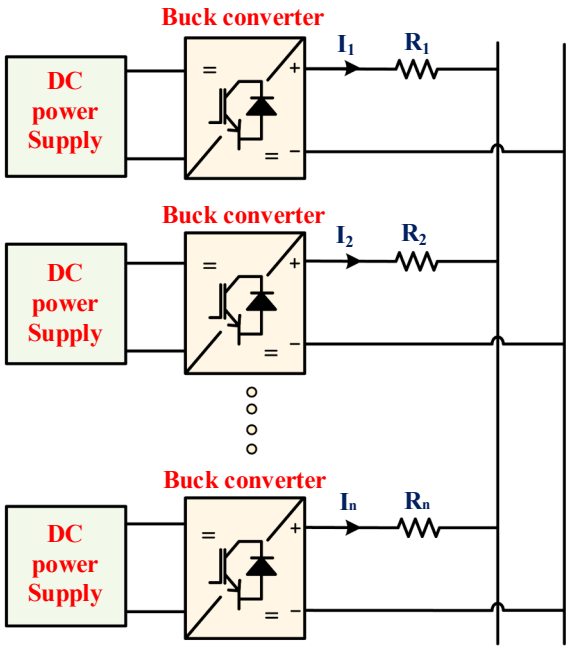

Fig. 1. Schematics of DC-DC buck converter coupled DC microgrid.

framework is a model-free approach, which helps to overcome the modeling inaccuracy and eliminates the vanishing gradient problem, unlike classical neural network, and improves the system dynamics under various FDI attacks.

- In contrast with the state-of-art strategies [17,24,38,39], the presented GRU-based framework ensures satisfactory performance even under various kinds of FDI attacks (i.e., constant DC bias, time-varying attack). In addition, detailed qualitative and quantitative comparative performances are carried out to exhibit the effectiveness of the presented GRU-based framework.
- A detailed sensitivity analysis is carried out to demonstrate the strength of the presented GRU-based approach against the input disturbances, unlike classical neural network-based technique. The numerical results illustrate the effectiveness of the presented approach over the classical method.

The rest of this article is organized as follows. Section 2 describes the basic structure of the DC microgrid. Section 3 introduces the GRU-based control strategy to mitigate the FDI attack. In Section 4, simulation results are demonstrated to validate the effectiveness of the presented framework. A qualitative and quantitative comparative analysis between the GRU-based framework and the classical method, are performed in Section 5. The research findings and conclusions are summarized in Section 6.

2. Schematic diagram

Fig. 1 shows the schematic diagram of the DC microgrid [40]. The renewable energy sources are coupled with DC microgrid through a DC-DC buck converter. These converters are connected at a common coupling point through a transfer line. The resistances (R_1-R_n) represent the equivalent resistance of transfer line for DC-DC converters (i.e., 1, 2, …, n). Fig. 2 illustrates the basic structure of primary and secondary controllers based droop control for DC microgrid [41]. The droop controller is implemented herein for the reliable operation of the DC microgrid. The main objective of the secondary control is to adjust the output of the DC-DC converter to ensure the reference value, which is obtained from the master controller. In order to regulate the current sharing, the output of the secondary controller is processed further into the droop controller. The primary control layer plays a vital role as it is consisted of an outer voltage controller and an inner current controller to regulate the output voltage and current of each converter. As it can be

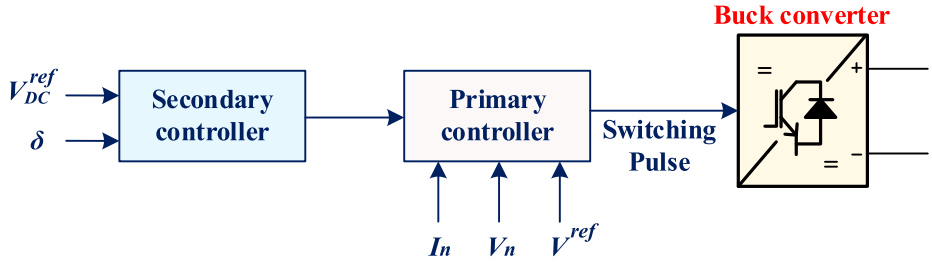

Fig. 2. Schematics of control structure for DC microgrid.

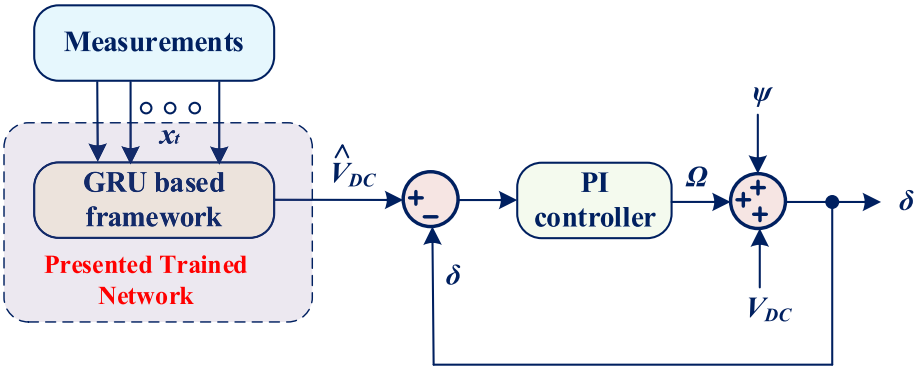

Fig. 3. Neural network-based FDI attack mitigation method.

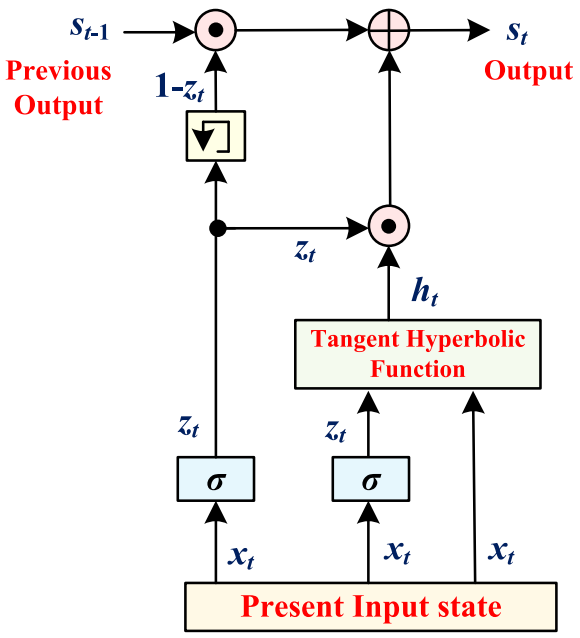

Fig. 4. Working principles of GRU block at time..*t*

observed from Fig. 2, when the attack (Ψ(t)) happens in the bus voltage V_{dc}, that is, $\delta(t) = V_{dc}(t) + \Psi(t)$, becomes the bus voltage transferred to the control layer. Then, the whole system could be destabilized and it may damage the DC microgrid. To cope with these malicious cyber-attacks, the gated recurrent unit based control strategy is designed to estimate the attack signal and provides a resilient operation to the DC microgrid. The detailed modeling parameters of the DC microgrid is given in Appendix.

3. Presented control strategy

Fig. 2 and Fig. 3 illustrates the schematics of the presented control strategy to eliminate the FDI attack on DC microgrid. The problem statement of the presented work can be expressed as follows:

Input signal: DC bus voltage (with inclusion of malicious attack signal ($V_{dc} + \Psi$)).

Target: Accurate estimation of an attack signal (Ω) (i.e., $\lim_{t\to\infty}\Psi(t) + \Omega(t) = 0$).

End goal: To provide resilient operation of the DC microgrid under malicious attack

The whole control structure is composed of two sections: (1) The basic control structure part includes the primary controller and secondary controller, and (2) The gated recurrent unit-based neural network, which is trained in such a way that it estimates the DC bus voltage with help of the converter output voltage and current measurements, and provides resiliency to the DC microgrid under malicious cyber-attack. The detailed implementation of the gated recurrent unit-based mitigation strategy is explained below.

3.1. Introduction of GRU

In order to estimate the time-series signals like voltage and current, the data-driven techniques are widely adopted because of having certain advantages [36] over classical model-based methods [8,26–31]. Nonetheless, the classical neural network has several drawbacks, for example, it faces the random gradient explosion for deeper network while considering the long-term signal, which may lead to trapping in a locally optimal solution rather than offering a global optimum solution. To solve the vanishing gradient problem and to learn longer-term relationships, a long short-term memory (LSTM) method is described in the literature [37]. However, the computation process of LSTM algorithm is quite complicated, thereby, it requires a lot of training time. Therefore, the gated recurrent unit (GRU) is analyzed in [36] to simplify the structure of the LSTM and overcome its shortcomings. The single-time step working principle of GRU is demonstrated in Fig. 4. The output value (s_t) is computed as follows:

$$\begin{aligned} z_t &= \sigma(U_z x_t + W_z s_{t-1} + b_z) \\ r_t &= \sigma(U_r x_t + W_r s_{t-1} + b_r)\# \\ h_t &= \tanh(U_h x_t + W_h(s_{t-1} \odot r_t) + b_h) \\ s_t &= (1 - z_t) \odot s_{t-1} + z_t \odot h_t \#\#\# \end{aligned} \tag{1}$$

where, z_t is the updated gate, r_t is reset gate, x_t is the current input state, h_t is the candidate activation, σ is the sigmoid function, and $\odot$ represents an element-wise multiplication; U_z, U_r, and U_h represent the input weight matrixs; W_z, W_r, and W_h are the recurrent weights; b_z, b_r, and b_h are biases. From the output function, it is easy to notice that if the updated gate approaches to 1, then, information from previous memory would be forgotten and the current state would be remembered and vice versa. Because of having this inherent characteristic, the GRU has the ability to remember long-term information and discards some unimportant information to extract the intrinsic relationship of a model, which makes it the best candidate amongst the other data-driven techniques in order to develop the mitigation strategy.

3.2. GRU-Based mitigation strategy

Fig. 3 shows the overall control structure of the GRU-based mitigation method to alleviate the FDI attack on the DC microgrid. The GRU-based neural network plays a vital role to estimate the DC bus voltage data in an event of a malicious FDI attack. The detailed implementation of the control structure is depicted in Fig. 3.

Supposing that the revised value of the DC bus voltage (δ) under FDI and mitigation method is expressed as [23–25]:

$$\delta(t) = V_{dc}(t) + \Psi(t) + \Omega(t) \tag{2}$$

where, $\Psi(t)$ is the attack signal and $\Omega(t)$ is the output of the proportional

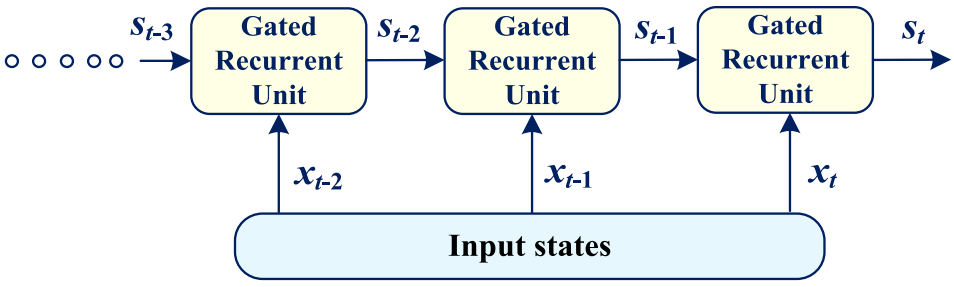

Fig. 5. Unrolled architecture of GRU considering present and past input values.

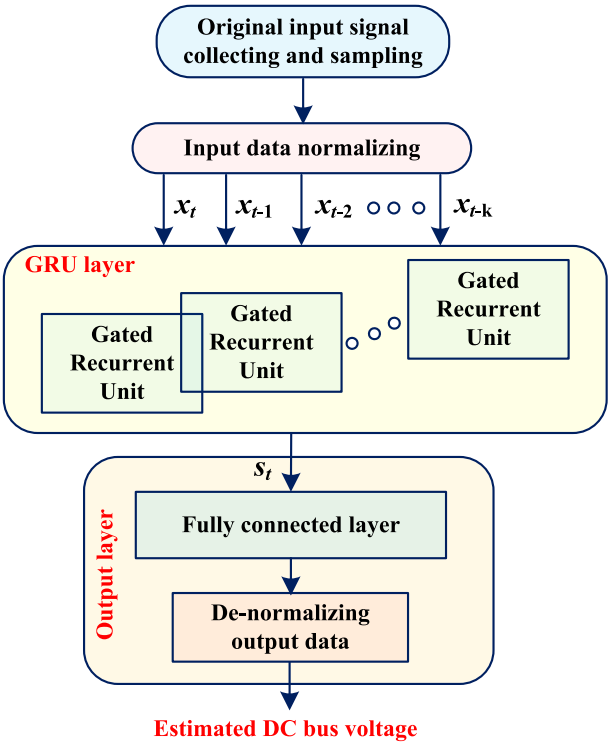

Fig. 6. The whole structure of the GRU-based neural network.

integral (PI) controller and $V_{dc}(t)$ is actual value of DC bus voltage. As the PI parameters are properly designed, it yields that input of the secondary controller (δ) converge to $\widehat{V}_{dc}$, i.e.,:

$$\lim_{t\to\infty} \widehat{V}_{dc}(t) = \delta(t) \tag{3}$$

It can be analyzed that the GRU-based neural network precisely estimates the DC bus voltage at event of the malicious cyber-attack, thereafter the output of the PI controller counteracts the attack signal from the measured DC bus voltage data. It yields an accurate estimation of the attack signal.

$$\lim_{t\to\infty} \Psi(t) + \Omega(t) = 0 \tag{4}$$

In case of the absence of the FDI attack, it can be observed that the input of the secondary controller is equal to the actual DC bus voltage (V_{dc}).

3.3. Detailed implementation of GRU-Based neural network framework

Fig. 5 shows an unrolled architecture of the gated recurrent unit network. The inputs and output of the GRU network are the output currents and voltages of the converters, and the estimated DC bus voltage, respectively. The present input state (x_t) and the output of the previous block (s_{t-1}), are fed to the current time step GRU block as illustrated in Fig. 5. By parity of reasoning, the output of the previous block maintains the information from the previous input state. The updated gate determines the retained information. In the case of a deep neural network [34], the mathematical formulation of weight, state, and bias, may give trivial value and leads to a vanishingly small gradient. In contrast with the classical neural network, the GRU overcomes these issues by introducing the gated structure in the network as explained in (1). Because of having this mechanism, the long-term state is easily retained and passed to its end, regardless of the length of the subsequence. Henceforth, the structure of the neural network plays a vital role to train the data set. The input data of GRU-based neural network is expressed as follows:

Table 2
Offline training process.

Initialization:
1. Sample and collect output voltage $v_1, v_2, .., v_n$ and current $i_1, i_2, .., i_n$ of converters, and bus voltage V_{dc}, and, thereafter, it is categorized into training data and tested data.
2. Normalize the collected data.

Process:
3. Measurement data of x_t in (5) is assigned as the input of the GRU and the DC bus voltage (V_{dc}) is assigned as the target value.
4. Apply the data to the built GRU-based network with initial parameters in (1).
5. Train the network.
6. If the training value of loss and RMSE are low enough, the trained network is obtained, if not, turn to Step-1 to collect more data and adjust the parameter of the network.

Output:
7. Using test data to verify the effectiveness of the network.
8. If it works perfectly, the parameter of a well-trained network in Eq. (1) is gained. If not, go back to Step-1.

$$x_t = \begin{bmatrix} i_1(t) \\ \vdots \\ i_n(t) \\ v_1(t) \\ \vdots \\ v_n(t) \end{bmatrix} \tag{5}$$

where, i_n, v_n are the output current and voltage of the n^{th} converters, respectively.

The whole GRU-based estimated framework is illustrated in Fig. 6. It consists of the input layer, GRU layer, and output layer. The time-series signals are sampled, normalized, and processed to the GRU block. The normalizing process plays a pivot role herein because there are two benefits of applying the normalization in the GRU-based neural network. The first one is accelerating the convergence speed, the second one is eliminating the disunity of the units. Subsequently, the GRU layer is implemented to attain the final time-step output. For each timesteps t, it calculates an output (s_t). Here, k represents the timesteps, which is related to the hidden number of the GRU. Then the outputs of the last timestep are imported to the fully connected layer. To obtain the desired output size, the fully connected layer is exploited herein to map the output of GRU layer, thereafter, it multiplies the input by a weight matrix and a bias vector to obtain an output of the GRU-based framework. Significantly, the output of the data should be denormalized to get the estimated value of the bus voltage ($\widehat{V}_{dc}$) using the same optimized parameters of the weights and bias to compel the estimated value close to the actual value.

The detailed description of the training process is manifested in Table 2. Accordingly, the training process is described for n parallel DC-DC converters coupled DC microgrid. The first step is sampling and collecting the data from the system under nominal case with different operating conditions. In order to prevent the divergence of the network training, the second step plays a pivot role to obtain the standardize data with help of its mean value and standard deviation. It is computed by taking the difference between the input value and mean value of the whole data, thereafter, it is processed with the standard deviation. The initial learning rate is set as 0.05 and it would be lessened by factor 0.2 after reaching 125 epochs. The maximum epoch is set as 250, which is

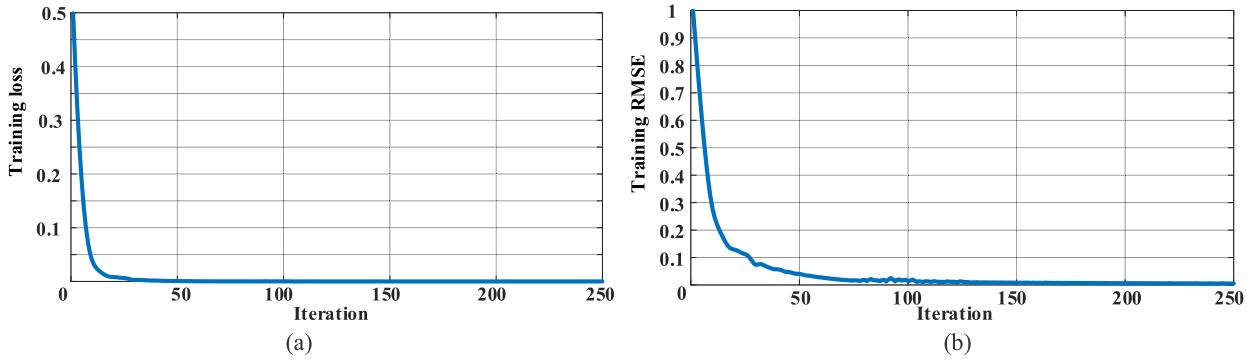

Fig. 7. Training process (a) Training loss (b) Training RMSE.

the number of times passing through the full data. The values of weights and biases are altered through the learning rate to get the minimum difference value between the target value and the estimated value. In this work, the Adam optimizer is chosen as the gradient descent optimization algorithms. If the training process curve is smooth and the loss and root-mean-square error (RMSE) are quite small enough, the network is well-trained. Thereafter, the effectiveness of the network is verified by using test data. More data should be re-collected and reset the initial values of the network in case of a mismatch between the estimated output and actual output of the system. The loss and RMSE of training process are shown in Fig. 7. One can observe that the loss and RMSE are small enough (1.4×10^{-5}, 0.0049, respectively), which indicates that the network is well trained. Finally, the well-trained network is used in the online application for the resilient operation of the DC microgrid.

3.4. Sensitivity analysis of GRU with respect to classical neural network

The partial derivatives sensitivity analysis method is used to demonstrate the superiority of the GRU-based framework compared with the classical neural network with the presence of disturbance in the network inputs.

3.4.1. Sensitivity analysis of classical neural network

In classical neural network, multi-layer perceptron (MLP) is a well-known structure to learn nonlinear realtionship between inputs and outputs. The MLP is consisted of three or more layers. The three layers MLP (i.e., one input layer, one hidden layer, and one output layer) is considered in [40] to build the classical neural network. The basics design and implementation of classical neural network with MLP framework is described in Appendix. Supposed that the input of the k^{th} neuron in the $l^{th}(1 \le l \le 3)$ layer is z_k^l, and the i^{th} neuron of the output of the last layer is y_i^{l-1}. Thus, the partial derivate regards to last layer's output are [42]:

$$\partial z_k^l / \partial y_i^{l-1} = \omega_{ki}^l \tag{6}$$

where, ω_{ki}^l is the weights between the connection neuron of l^{th} and $(l-1)^{th}$.

The derivative of the output of the neuron regards to the input of the neuron is expressed as:

$$\partial y_k^l / \partial z_i^l = \partial f_k^l / \partial z_i^l \tag{7}$$

In order to reduce the calculation burden, it is expressed in the matrix form as [42]:

$$\frac{\partial z^l_{[1\times n^l]}}{\partial y^{l-1}_{1\times n^{l-1}}} = \begin{bmatrix} \frac{\partial z_1^l}{\partial y_1^{l-1}} & \frac{\partial z_1^l}{\partial y_2^{l-1}} & \cdots & \frac{\partial z_1^l}{\partial y_{n^{l-1}}^{l-1}} \\ \frac{\partial z_2^l}{\partial y_1^{l-1}} & \frac{\partial z_2^l}{\partial y_2^{l-1}} & \cdots & \frac{\partial z_2^l}{\partial y_{n^{l-1}}^{l-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\partial z_{n^l}^l}{\partial y_1^{l-1}} & \frac{\partial z_{n^l}^l}{\partial y_{n^{l-1}}^{l-1}} & \cdots & \frac{\partial z_{n^l}^l}{\partial y_{n^{l-1}}^{l-1}} \end{bmatrix} = \begin{bmatrix} \omega_{11}^l & \omega_{12}^l & \cdots & \omega_{1n^{l-1}}^l \\ \omega_{21}^l & \omega_{22}^l & \cdots & \omega_{2n^{l-1}}^l \\ \vdots & \vdots & \ddots & \vdots \\ \omega_{n^l1}^l & \omega_{n^l2}^l & \cdots & \omega_{n^l1n^{l-1}}^l \end{bmatrix} = W^l_{[n^l\times n^{l-1}]} \tag{8}$$

$$\frac{\partial y^l_{[1\times n^l]}}{\partial z^l_{[1\times n^l]}} = \begin{bmatrix} \frac{\partial y_1^l}{\partial z_1^l} & \frac{\partial y_2^l}{\partial z_1^l} & \cdots & \frac{\partial y_{n^l}^l}{\partial z_1^l} \\ \frac{\partial y_1^l}{\partial z_2^l} & \frac{\partial y_2^l}{\partial z_2^l} & \cdots & \frac{\partial y_{n^l}^l}{\partial z_2^l} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\partial y_1^l}{\partial z_{n^l}^l} & \frac{\partial y_2^l}{\partial z_{n^l}^l} & \cdots & \frac{\partial y_{n^l}^l}{\partial z_{n^l}^l} \end{bmatrix} = \begin{bmatrix} \frac{\partial f_1^l}{\partial z_1^l}(z_1^l) & \frac{\partial f_2^l}{\partial z_1^l}(z_1^l) & \cdots & \frac{\partial f_{n^l}^l}{\partial z_1^l}(z_1^l) \\ \frac{\partial f_1^l}{\partial z_2^l}(z_2^l) & \frac{\partial f_2^l}{\partial z_2^l}(z_2^l) & \cdots & \frac{\partial f_{n^l}^l}{\partial z_2^l}(z_2^l) \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\partial f_1^l}{\partial z_{n^l}^l}(z_{n^l}^l) & \frac{\partial f_2^l}{\partial z_{n^l}^l}(z_{n^l}^l) & \cdots & \frac{\partial f_{n^l}^l}{\partial z_{n^l}^l}(z_{n^l}^l) \end{bmatrix} = J^l_{[n^l\times n^l]} \tag{9}$$

Thus, the Jacobian matrix of the output in the l^{th} layer with regard to the input $(l-j)^{th}$ layer is calculated by:

$$J^l_{l-j} = J^l_l \bullet \prod_{h=l-1}^{l-j} \left(W^{h+1} \bullet J^h_h\right) \tag{10}$$

After applying all the measurement data, the mean value of the quantitative result for classical neural network is:

$$[\,0.8814757 \quad -3.9321402 \quad -6.8684759 \quad 13.9050731\,]$$

3.4.2. Sensitivity analysis of gated recurrent unit integrated neural network

The output of the GRU-based neural network is shown as follows:

$$y = W_F s_t + b_F \tag{11}$$

where, W_F is the weight factor matrix of the fully-connected layer, and b_F is a bias factor.

In order to calculate the sensitivity of output value (y) of GRU based network regards to the input variables, the partial derivative of the output regards to the input signals for each time step should be computed and it is formulated as:

$$\begin{aligned}\frac{\partial y}{\partial x_1}+\frac{\partial y}{\partial x_2}+\frac{\partial y}{\partial x_3}+\cdots+\frac{\partial y}{\partial x_{10}} &= \left(\frac{\partial s_{10}}{\partial s_9}\frac{\partial s_9}{\partial s_8}\cdots\frac{\partial s_2}{\partial s_1}\frac{\partial s_1}{\partial x_1}\right)^T\frac{\partial y}{\partial s_{10}}+\left(\frac{\partial s_{10}}{\partial s_9}\frac{\partial s_9}{\partial s_8}\cdots\frac{\partial s_3}{\partial s_2}\frac{\partial s_2}{\partial x_2}\right)^T\frac{\partial y}{\partial s_{10}}+\cdots+\left(\frac{\partial s_{10}}{\partial x_{10}}\right)^T\frac{\partial y}{\partial s_{10}}\\ &= \sum_{i=1}^{9}\left(\left(\prod_{j=i}^{9}\frac{\partial s_{j+1}}{\partial s_j}\right)\frac{\partial s_i}{\partial x_i}\right)^T W_F^T+\left(\frac{\partial s_{10}}{\partial x_{10}}\right)^T W_F^T\#\end{aligned} \tag{12}$$

For convenience, x_1 and x_{10} stands for x_{t-9} and x_t, respectively. The gradient of output of GRU block (s_i) with respect to input state (x_i) is represented by $\left(\frac{\partial s_i}{\partial x_i}\right)$ and it is computed as:

$$\begin{aligned}\frac{\partial s_i}{\partial x_i} &= \frac{\partial s_i}{\partial z_i}\frac{\partial z_i}{\partial x_i}+\frac{\partial s_i}{\partial h_i}\frac{\partial h_i}{\partial x_i}\\ &= \frac{\partial s_i}{\partial z_i}\frac{\partial z_i}{\partial x_i}+\frac{\partial s_i}{\partial h_i}\left(\frac{\partial h_i}{\partial r_i}\frac{\partial r_i}{\partial x_i}+\frac{\partial \overline{h}_i}{\partial x_i}\right) = diag(s_{i-1}-h_i)diag(z_i\odot(1-z_i))U_Z+diag(z_i)\begin{pmatrix}diag(1-h_i\odot h_i)W_h diag(s_{i-1})diag(r_i\odot(1-r_i))U_r\\ +diag(1-h_i\odot h_i)U_h\end{pmatrix}\#\\ &\#\end{aligned} \tag{13}$$

where, $\frac{\partial \overline{h}_i}{\partial x_i}$ is the gradient of h_i with respect to x_i with considering r_i as a constant. It should be noted that the numerator layout is applied in this work.

$$\begin{aligned}\frac{\partial s_i}{\partial s_{i-1}} &= \frac{\partial s_i}{\partial h_i}\frac{\partial h_i}{\partial s_{i-1}}+\frac{\partial s_i}{\partial z_i}\frac{\partial z_i}{\partial s_{i-1}}+\frac{\partial \overline{s}_i}{\partial s_{i-1}} = \frac{\partial s_i}{\partial h_i}\left(\frac{\partial h_i}{\partial r_i}\frac{\partial r_i}{\partial s_{i-1}}+\frac{\partial \overline{h}_i}{\partial s_{i-1}}\right)+\frac{\partial s_i}{\partial z_i}\frac{\partial z_i}{\partial s_{i-1}}+\frac{\partial \overline{s}_i}{\partial s_{i-1}}\\ &= diag(z_i)\times\begin{pmatrix}diag(1-h_i\odot h_i)W_h diag(s_{i-1})diag(r_i\odot(1-r_i))W_r\\ +diag(1-h_i\odot h_i)diag(r_i)W_h\end{pmatrix}+diag(h_i-s_{i-1})diag(z_i\odot(1-z_i))W_z+diag(z_i)\end{aligned} \tag{14}$$

where, $\left(\frac{\partial \overline{s}_i}{\partial s_{i-1}}\right)$ is the gradient of present output (s_i) with respect to previous output (s_{i-1}) of GRU block, whereas, the variables candidate activation (h_i) and updated gate (z_i) are considered as constant. After applying the same data-set of classical neural network, the obtained mean value of quantitative result for a GRU-based framework is:

$$[\,-0.0743262 \quad -0.0566587 \quad 0.0486835 \quad 0.0851134\,]^T$$

The result indicates that the GRU has less sensitivity than the classical neural network, which means that it has better stable performance even when the input of the network is disturbed.

4. Simulation result

The DC-DC converter interfaced DC microgrid is modeled in MATLAB®/Simulink using the Simpower toolbox. The proposed algorithm applied on the MATLAB version 9.9.0.1467703 (R2020b) /Simulink of a laptop with Windows 10, Intel(R) Core (TM) i7-10750H CPU @ 2.60 GHz. The installed memory (RAM) is 16 GB and the system type is a 64-bit operating system with X-64 based processor. As for the software environment, the Neural Network Time Series app which belongs to the Deep Learning Toolbox (version 14.1) is used. Besides, the MATLAB Coder interface for Deep learning Libraries, and Intel Math Kernel Library for Deep Neural Networks (V0.14) is required. In this simulation study, the DC microgrid with two converters ($n = 2$) is modeled in Case 1 and Case 2 to verify the effectiveness of the presented GRU-based framework. In order to prove the scalability of the presented work, three converters ($n = 3$) are also considered. The designed parameters of the system configuration are given in Appendix. The initial setting parameters of the GRU and classical neural network for training are described in Appendix. In order to train the data, the system measurement data is collected from the nominal case with different operating scenarios. Moreover, the load and target values are varied with the purpose to capture additional measurement data. The system runs for 10s in normal operating scenario. Total 1×10^6 sets of measurement data are obtained and utilized in network training progress. The GRU-based framework is applied to these data to train the network, thereafter, the well-trained network is applied to the DC microgrid system to alleviate the impact of malicious cyber-attack.

4.1. Case1: Constant FDI attack with two converters

Fig. 8 (a-b) show the performance of the DC microgrid system with

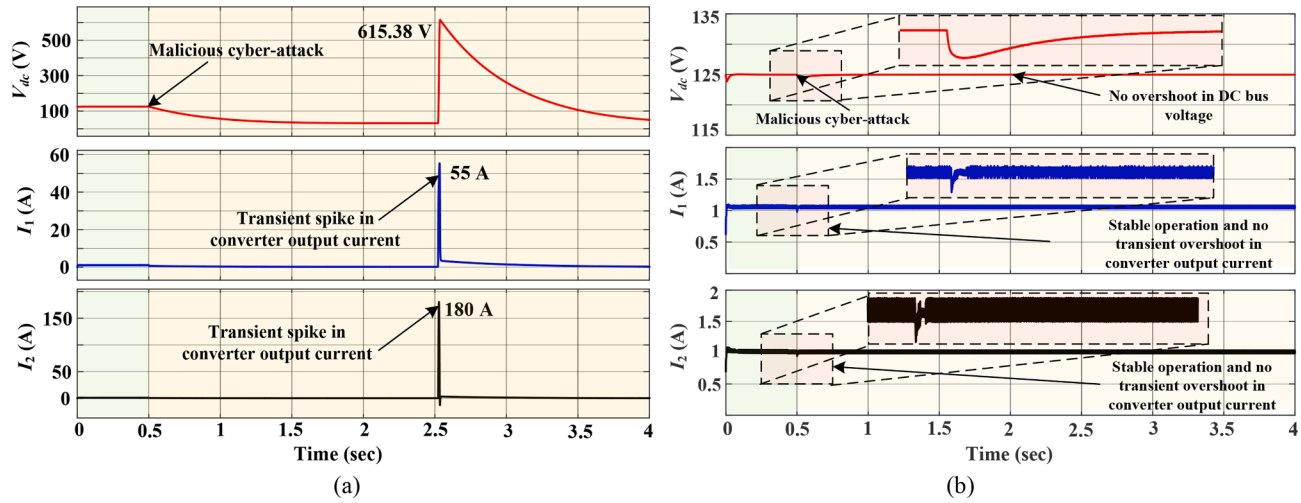

Fig. 8. The bus voltage and output current of converters (a) System under 60V step FDI attack without mitigation method (b) System under 60V step FDI attack with mitigation method.

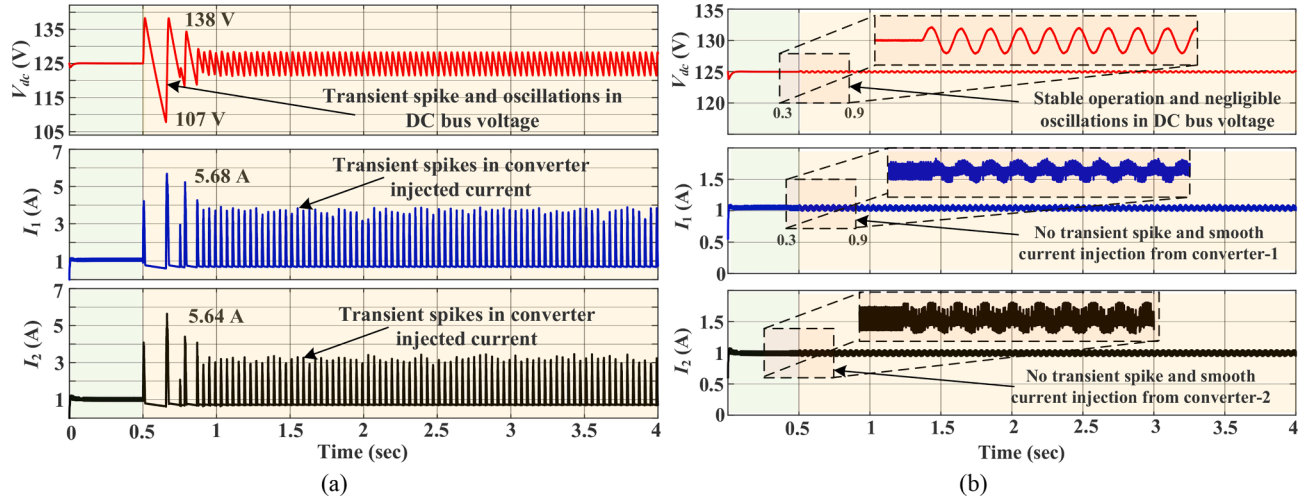

Fig. 9. The bus voltage and output current (a) System under $\omega = 157rad/s$ sinusoidal wave FDI attack without mitigation method (b) System under $\omega = 157rad/s$ sinusoidal wave FDI attack with mitigation method.

the presence of an FDI attack. At 0.5*s*, the step input of false data with a typical value of 60V, is injected to the sensor of DC bus voltage sensor. Fig. 8(a) shows the dynamics of DC microgrid without having any mitigation method. It is easy to notice that the system may collapse as the converter DC bus voltage reaches over 600V. Furthermore, the inverter output current is noticeably increased over 55A, which may damage the converter switches. Fig. 8(b) shows the response of the system with the presented mitigation framework under FDI attack. It is easy to observe that DC bus voltage is regulated within restricted limits even under large malicious FDI attack. Furthermore, the peak value of the DC bus voltage is attained at around 124.6V. It takes typically 0.4*s* to recover from the attack, which means that the bus voltage reaches to 125V. The oscillation in the DC bus voltage is quite low as depicted in Fig. 8(b). In contrast to Fig. 8 (a), the GRU-based mitigation approach nullifies the negative impact of FDI attacks on the DC microgrid.

4.2. Case2: Time-varying FDI attack with two converters

Fig. 9 (a-b) and Fig. 10 (a-b) illustrate the dynamics of the DC microgrid at an event of a time-varying FDI attack. Fig. 9 (a-b) show the performance of the system with considering attack signal of a sinusoidal wave with an amplitude of 20V and $\omega = 157\text{rad/s}$. As the attack starts at $t = 0.5s$, It is easy to notice that the DC bus voltage is suddenly increased over 138V with a steady-state bound of 125 ± 20V and this may lead to damage to the switches of the converter. The DC bus dynamics are.

harmonically polluted as exhibited in Fig. 9 (a), which leads to injection of harmonics in the converter output current. The peak value of the current is attained in-range of 5.7A, which brings awful consequence compared with the rated value 1A. Fig. 9 (b) shows the effectiveness of the presented approach under time-varying FDI attack. It shows that DC bus voltage is effectively sustained as per reference DC bus voltage as illustrated in Fig. 9 (b). The zoom-view demonstrates that the fluctuation of the DC bus voltage is achieved within ± 0.1V.

Likewise, a sinusoidal wave with an amplitude of 20V and $\omega = 3.14\text{rad/s}$ is voluntarily injected into the DC bus voltage and dynamics of the system are exhibited in Fig. 10 (a-b). Fig. 10 (a) shows the performance of the system without any resilient controller strategy. As the attack happens at $t = 0.5s$, the fluctuation of the DC bus voltage reaches up to 83V and it affects the system performances as illustrated in Fig. 10 (a). The performance of the system is not satisfactyory as the voltage has a disturbance of ± 20V with $\omega = 3.14rad/s$ as illustrated in Fig. 10 (a). Fig. 10 (b) shows the dynamics of the system as the mitigation method is

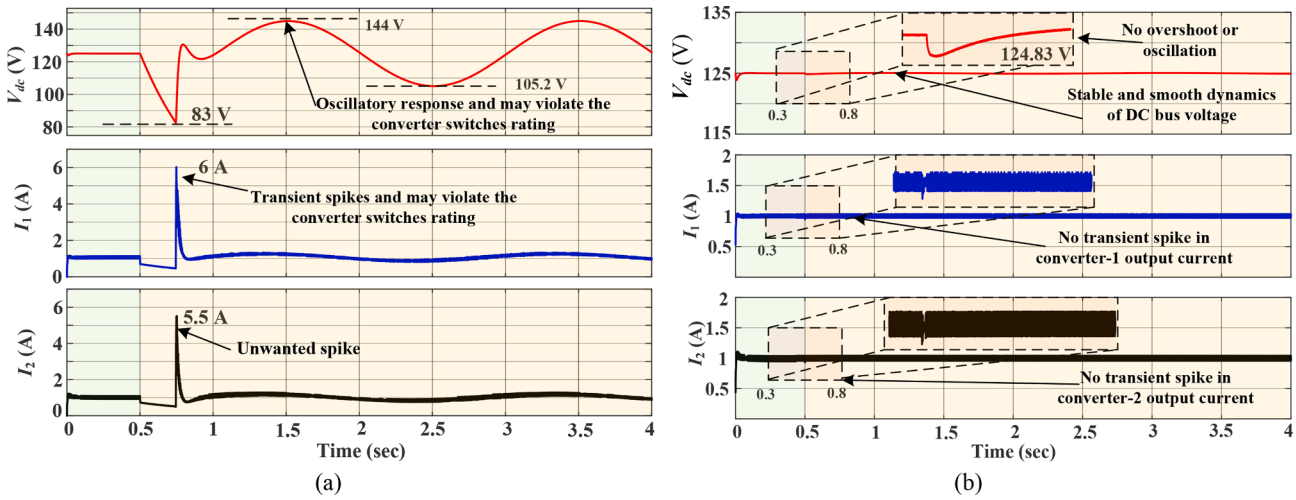

Fig. 10. The DC bus voltage and output current (a) System under $\omega = 3.14 rad/s$ sinusoidal wave FDI attack without mitigation method (b) System under $\omega = 3.14 rad/s$ sinusoidal wave FDI attack with mitigation method.

engaged with the control strategy. One can easily notice that the deviation of the voltage is cut down to the 125 ± 0.05V. The transient oscillation in the output of converter current is alleviated using the presented GRU-based mitigation framework.

4.3. Case3: Time-varying FDI attack with three converters

Fig. 11 (a) shows the system performance of the three converters with the presence of the malicious cyber-attack of having typical value of $\omega = 157$ rad/s sinusoidal wave false data injection attack characteristics. The presented framework effectively identifies the attack signal and provide resiliency as depicted in Fig. 11 (a). The converter output currents are also not affected as the network is effectively trained with datasets. It is worth to notice that no oscillations or no magnitude variations are observed in any of the converter even with the presence of cyber-attack. Likewise, the performance of the system (with consideration of three converters) is analyzed in Fig. 11 (b). The typical frequency of the sinusoidal attack signal is 3.14 rad/s with having false data injection characteristics. As one can observe that the little transient is observed in the DC bus voltage dynamics, which is significantly low and it will not affect the system performance. The dynamics of the converter output currents are smooth as depicted in Fig. 11(b).

5. Comparative performance

The comparative performances between the presented GRU-based

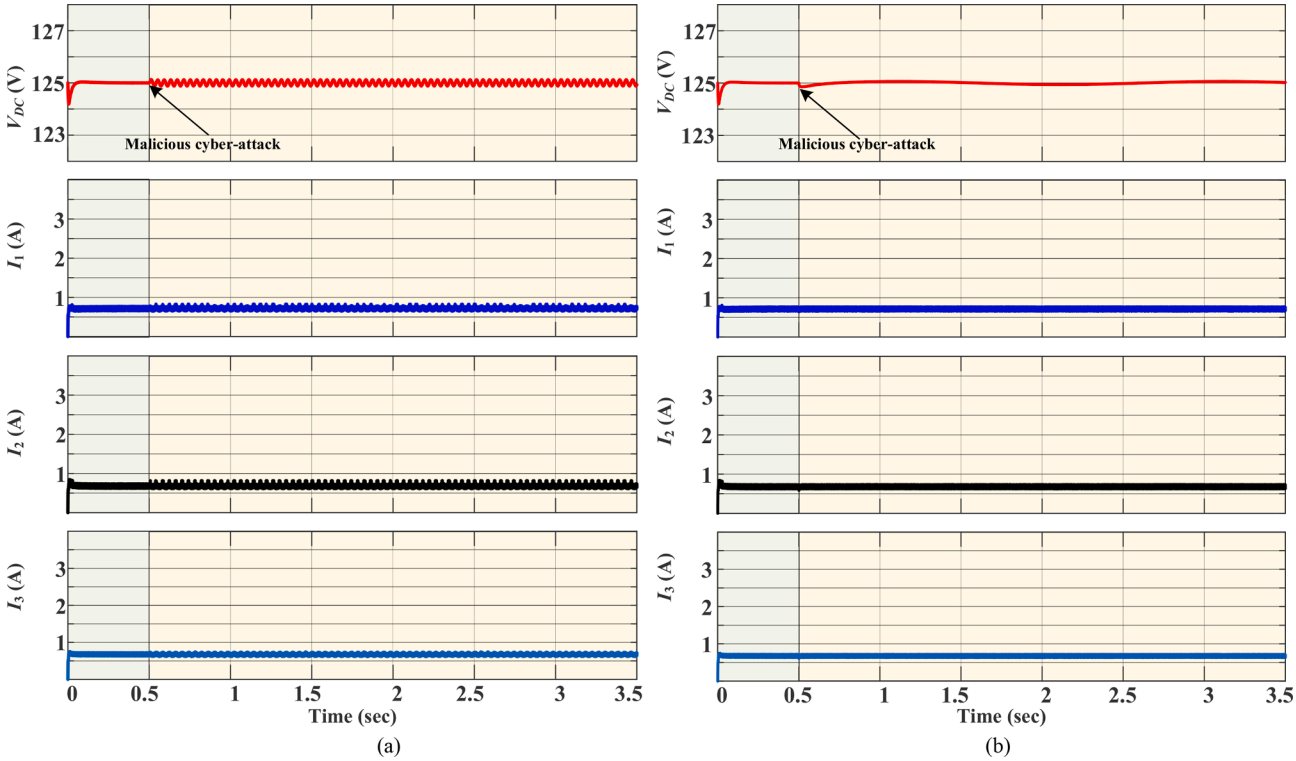

Fig. 11. The DC bus voltage and output current (a) System under $\omega = 157 rad/s$ sinusoidal wave FDI attack with mitigation method (b) System under $\omega = 3.14 rad/s$ sinusoidal wave FDI attack with mitigation method.

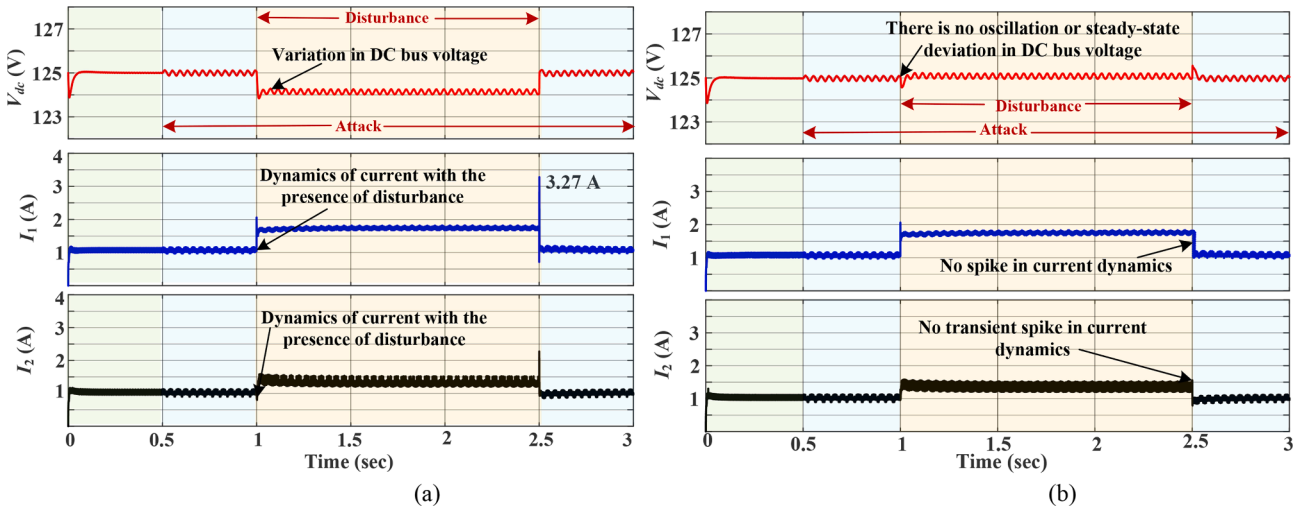

Fig. 12. Dynamics of bus voltage and output current with the presence of 1A disturbance to the sensor of output current (i_1) (a) Classical neural network based mitigation method (b) GRU-based mitigation method.

Table 3
RMSE under different measurement disturbances.

Disturbance in Current Measurements	RMSE of GRU-Based Method	RMSE of Classical Neural Network-Based Method [32]
Step signal(1 A)	0.0513482	0.6099651
Step signal(0.1 A)	0.0280360	0.0641471
Sinusoidal (0.5 A, 314 rad/s)	0.0449013	0.2177374
Sinusoidal (0.5 A, 3.14 rad/s)	0.0554365	0.2177380

Table 4
Comparative Analysis Between Presented Controller and State-of-Art Technique.

Parameters	[38]	[32]	[39]	Presented Work
Type of algorithm	Kalman and H-infinity controller	Classical neural network	Hybrid observer	Gated Recurrent unit
Type of application	Buck-Boost converter	Buck converter	Buck converter	Buck converter
Performance under time-varying attack	Fails	Adapts	Fails	Adapts
Performance under constant bias attack	Fails	Adapts	Adapts	Adapts
Performance with disturbance in current data	Fails	Fails	Fails	Adapts
Computation burden	NA	186.126 *s*	NA	257.409 *s*
Sensitivity under cyber-attack	Poor	Medium	Medium	Better
Complexity	Low	High	Low	High

mitigation framework and classical neural network-based method [32] are analyzed for DC microgrid with the presence of disturbance in a current sensor measurement under variation of loads. In addition, the qualitative and quantitative analyses under different attacks and output current measurement noise are considered to validate the effectiveness of the presented approach. The detailed analysis of the comparative performance is explained as follows.

Fig. 12 shows the comparative performance with the consideration of the noise and disturbance in the output of the current sensor. It shows that the disturbance signal of 1A is voluntarily injected from $t = 1s$ to $t = 2.5s$. In addition, the FDI attack happens in DC bus voltage at $t = 0.5s$ with its typical value of 10V, $\omega = 314\text{rad/s}$. For a fair comparison, the same measurement data set is used to train both GRU and classical neural network. Fig. 12 (a) shows that the DC bus voltage deviates from the steady-state value with a bias of 1V in the case of the classical neural network-based method. In contrast with the classical neural network, Fig. 12 (b) demonstrates that the disturbance of the current causes an insignificant steady-state error or bias in the DC bus voltage (i.e., 0.08V) using the GRU-based mitigation approach. The presented algorithm provides a better response as compared to the classical neural network-based method. Thereby, it is verified that the sensitivity of the GRU-based framework is better than the classical neural network.

Additionally, the RMSE analysis under different measurement error and noise in current measurement (i_1) are also carried out in Table 3. As the disturbance signal of 1A is injected into the current sensor measurement (i_1), the RMSE of GRU-based method is restricted up to one-tenth as compared to the classical neural network-based method. It demonstrates that the GRU-based framework provides a superior response when inputs of the network are disturbed. For different measurement disturbances in the current sensor, the GRU-based framework attained lower RMSE as compared to the classical method. To validate this claim, the time-varying disturbance is injected into the sensor measurements, the RMSE of GRU based method is significantly low with respect to the classical method. That is, if one of the inputs of the network is disturbed, the GRU-based framework has the capability to accomplish better accuracy and stability of the DC microgrid system. Table 3 and Table 4 summarizes the qualitative and quantitative analysis of the presented approach and state-of-art controllers.

6. Conclusion

The GRU-based mitigation framework has been presented to alleviate the various kinds of FDI attacks in the parallel DC-DC converters interfaced hierarchical DC microgrid. In comparison with the state-of-art methods, the presented strategy has several distinct benefits, which are mentioned as follows. (1) The GRU based mitigation method is a model-free framework, thereby, it eliminates an modeling inaccuracy while estimating the attack signal as compared with the model-based approaches, (2) The presented framework provides satisfactory performance and ensures the resiliency for the system even under various kinds of FDI attacks (i.e., DC bias attack, time-varying attack), (3) In comparison with the state-of-art method, the presented GRU-based framework accomplishes better tracking performance under

distinct cyber-attacks. In addition, the root mean square error analysis also demonstrates the effectiveness of the presented work over conventional neural network-based method, and (4) A comparative sensitivity analysis has been analyzed and it shows that the presented GRU-based framework has better disturbance rejection capability as compared with the classical neural network-based mitigation technique. To validate the scalability of the presented work, the three converters based DC microgrid systems is analyzed and shows the satisfactory performance under dynamic operating scenarios. In addition, the presented framework effectively mitigates the impact on DC bus voltage with the presence of disturbance in the output current sensor of converters. In contrast with the classical neural network, the numerical comparative results of sensitivity analysis demonstrate the strength of the GRU-based approach under the presence of disturbances in the measurements. Furthermore, the numerical results show that RMSE value obtained through the presented approach is one-tenth of the value attained by the traditional method, which demonstrates the effectiveness of the presented framework.

7. Future work

The future work can be planned to consider more complicated DC microgrid control structure. In that case, the attack would affect the reference value of the secondary control which is a constant value in our case. The distinguish between fault and cyber attack could be investigated in the DC microgrid. In addition, the proposed mitigation frame work will be improved to implemented on different type of attack such as DoS attack and replay attack. The calculation burden of the proposed method can also be improved.

CRediT authorship contribution statement

Qiaohui He: Conceptualization, Data curation, Formal analysis, Investigation, Methodology, Project administration, Software, Validation, Visualization, Writing – original draft. **Priyank Shah:** Conceptualization, Formal analysis, Investigation, Methodology, Project administration, Software, Validation, Visualization, Writing – review & editing. **Xiaowei Zhao:** Conceptualization, Funding acquisition, Formal analysis, Investigation, Methodology, Project administration, Resources, Supervision, Writing – review & editing.

Declaration of Competing Interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests.

Data availability

Data will be made available on request.

Appendix

A.1. Simulation parameters

DC power supply=350V, Equivalent resistance of transfer line: R_1= 0.6Ω and R_2= 0.5Ω, V_{dc}^{ref} = 125V; Secondary controller parameters: $k_p = 1$, $k_i = 100$; Drop constant: $k = 1$; Outer voltage loop controller parameters: $k_p = 1$, $k_i = 10$; Inner current loop controller parameters: $k_p = 1$, $k_i = 10$; Sampling time: 10μs.

A.2. Network parameters

GRU initial setting parameters: number of input features = 4; Number of hidden units = 10; Max epochs = 250; Initial learning rate = 0.005; Classical neural network initial setting parameters: number of hidden neurons = 10; Delay order = 3.

A.3. Prelimanries for senstivity analysis of classical neural network

For the classical feedforward neural network, Fig. 13 shows, there are only three layers. The input layer, the hidden layer, and the output layer. Supposing that the number of the converters are n, the inputs data (X_t) are as follow, where D is the memory order [24,25,32]:

$$X_t = \begin{matrix} [i_1(t-1), & \cdots, & i_1(t-D), \\ \cdots, & i_n(t-1), & \cdots, & i_n(t-D), \\ v_1(t-1), & \cdots, & v_1(t-D), \\ \cdots, & v_n(t-1), & \cdots, & v_n(t-D)] \end{matrix} \tag{15}$$

The neuron is formulated by weights (ω_{ij}) and bias (b_j), and these will be multiplied with the input vector (z_j). These input vector comes from the input of the system or the previous layer by the weights array and bias, then the output value of the neuron (y_i) is obtained through the activation function like sigmoid or the hyperbolic tangent function. It is expressed as:

$$y_i = f\left(\sum_{j=1}^{n} z_j \omega_{ij} + b_j\right) \tag{16}$$

The output of the neural network ($\overline{y}$) is the estimated value of the DC bus voltage and it is expressed as [24,25,32]:

$$\overline{y} = f_2(f_1(X_t W_1 + B_1)W_2 + B_2) \tag{17}$$

where, f_1, f_2 are the activation function of the hidden layer and output layer, respectively. W_1, W_2 are the weights and B_1, B_2 are the biases. To obtain the value of these parameters, the trained data is collected and implemented to the network offline. Then the weights and bias are accommodated to make the output value of the network tend to the target value that is bus voltage in this case.

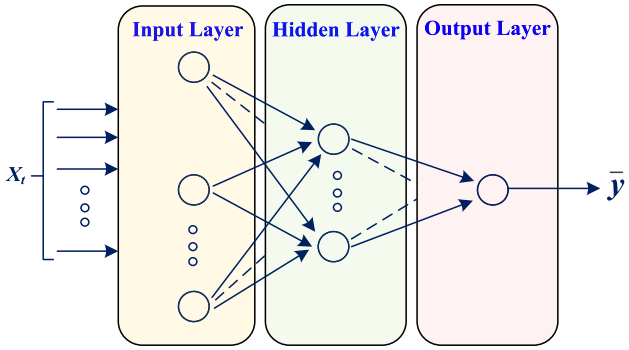

Fig. 13. Structure of a three layers classical feedforward neural network.

A.4. Prelimanries for senstivity analysis of gated recurrent unit

In order to explain the derivation of the GRU, some basic formulations like the derivation of sigmoid and hyperbolic functions are explained as follows. The sigmoid function is expressed as:

$$\sigma(x) = \frac{1}{1+e^{-x}} \tag{18}$$

The derivation of it in matrix form is expressed as [42,43]:

$$\sigma^{'}(x) = diag(\sigma(x) \odot (1-\sigma(x))) \tag{19}$$

The hyperbolic function is expressed as:

$$\tanh(x) = \frac{e^{x}-e^{-x}}{e^{x}+e^{-x}} \tag{20}$$

The derivation of (20) in matrix form is expressed as:

$$\tanh^{'}(x) = \mathrm{diag}(1-\tanh(x) \odot \tanh(x)) \tag{21}$$

Thus, according to the above formulation, the equation deducing process of the (13) is shown as follows:

$$\begin{aligned}\frac{\partial s_i}{\partial x_i} &= \frac{\partial s_i}{\partial z_i}\frac{\partial z_i}{\partial x_i} + \frac{\partial s_i}{\partial h_i}\frac{\partial h_i}{\partial x_i} = \frac{\partial s_i}{\partial z_i}\frac{\partial z_i}{\partial x_i} + \frac{\partial s_i}{\partial h_i}\left(\frac{\partial h_i}{\partial r_i}\frac{\partial r_i}{\partial x_i} + \frac{\partial \bar{h}_i}{\partial x_i}\right) = diag(s_{i-1}-h_i)\sigma'(f_z(x_i))\frac{\partial f(x_i)}{\partial x_i} + diag(z_i)\left(tanh'(f_h(r_i))\frac{\partial r_i}{\partial x_i} + \frac{\partial \bar{h}_i}{\partial x_i}\right) \\ &= diag(s_{i-1}-h_i)diag(z_i \odot (1-z_i))U_Z + (diag(z_i)) \times \begin{pmatrix} diag(1-h_i \odot h_i)W_h diag(s_{i-1})diag(r_i \odot (1-r_i))U_r \\ +diag(1-h_i \odot h_i)U_h \end{pmatrix}\end{aligned} \tag{22}$$

The gradient of present output (s_i) with respect to previous output (s_{i-1}) of GRU block is expressed as [42,43]:

$$\begin{aligned}\frac{\partial s_i}{\partial s_{i-1}} &= \frac{\partial s_i}{\partial h_i}\frac{\partial h_i}{\partial s_{i-1}} + \frac{\partial s_i}{\partial z_i}\frac{\partial z_i}{\partial s_{i-1}} + \frac{\partial \bar{s}_i}{\partial s_{i-1}} = \frac{\partial s_i}{\partial h_i}\left(\frac{\partial h_i}{\partial r_i}\frac{\partial r_i}{\partial s_{i-1}} + \frac{\partial \bar{h}_i}{\partial s_{i-1}}\right) + \frac{\partial s_i}{\partial z_i}\frac{\partial z_i}{\partial s_{i-1}} + \frac{\partial \bar{s}_i}{\partial s_{i-1}} \\ &= diag(z_i)\left(tanh'(f_h(r_i))\left(\sigma'(f_r(s_{i-1}))\frac{\partial f_r(s_{i-1})}{\partial s_{i-1}}\right) + \frac{\partial \bar{h}_i}{\partial s_{i-1}}\right) + diag(h_i - s_{i-1})\left(\sigma'(f_z(s_{i-1}))\frac{\partial f_z(s_{i-1})}{\partial s_{i-1}}\right) + diag(z_i) = diag(z_i) \\ &\times \begin{pmatrix} diag(1-h_i \odot h_i)W_h diag(s_{i-1}) \\ diag(r_i \odot (1-r_i))W_r + diag(1-h_i \odot h_i)diag(r_i)W_h \end{pmatrix} + diag(h_i - s_{i-1})diag(z_i \odot (1-z_i))W_z + diag(z_i)\end{aligned} \tag{23}$$

A.5. Detailed calculation of quantitative result of sensitivity

For better clarity to the readers, the flow chart is introduced in Fig. 14 in order to demonstrate the process of calculating quantitative results for both neural network and GRU-based frameworks. In Fig. 14 (a), the sensitivity quantitative result calculation of the classic neural network is described. All the data sets of input states, weights, and biases from the well-trained neural network are processed/fed into the calculation program. Each of the datasets is calculated by applying Eqs. (8)–(10) and adding them together by iteration and its output is the sum of the sensitivity value of each dataset. Thereafter, the mean value of sensitivity should be divided by the number of datasets. As for the GRU-based framework, the datasets of input states, weights, and biases from the well-trained GRU framework are fed into the calculation program. At first, the forward process of the GRU framework is calculated by applying Eq. (1) to prepare for the value of the following steps. Then, the sensitivity of a timestep is calculated by Eqs. (13)–(14). Then, considering the hidden units, the Eq. (12) is applied. The sensitivity of each dataset is added and divided by the applied dataset to get the mean value.

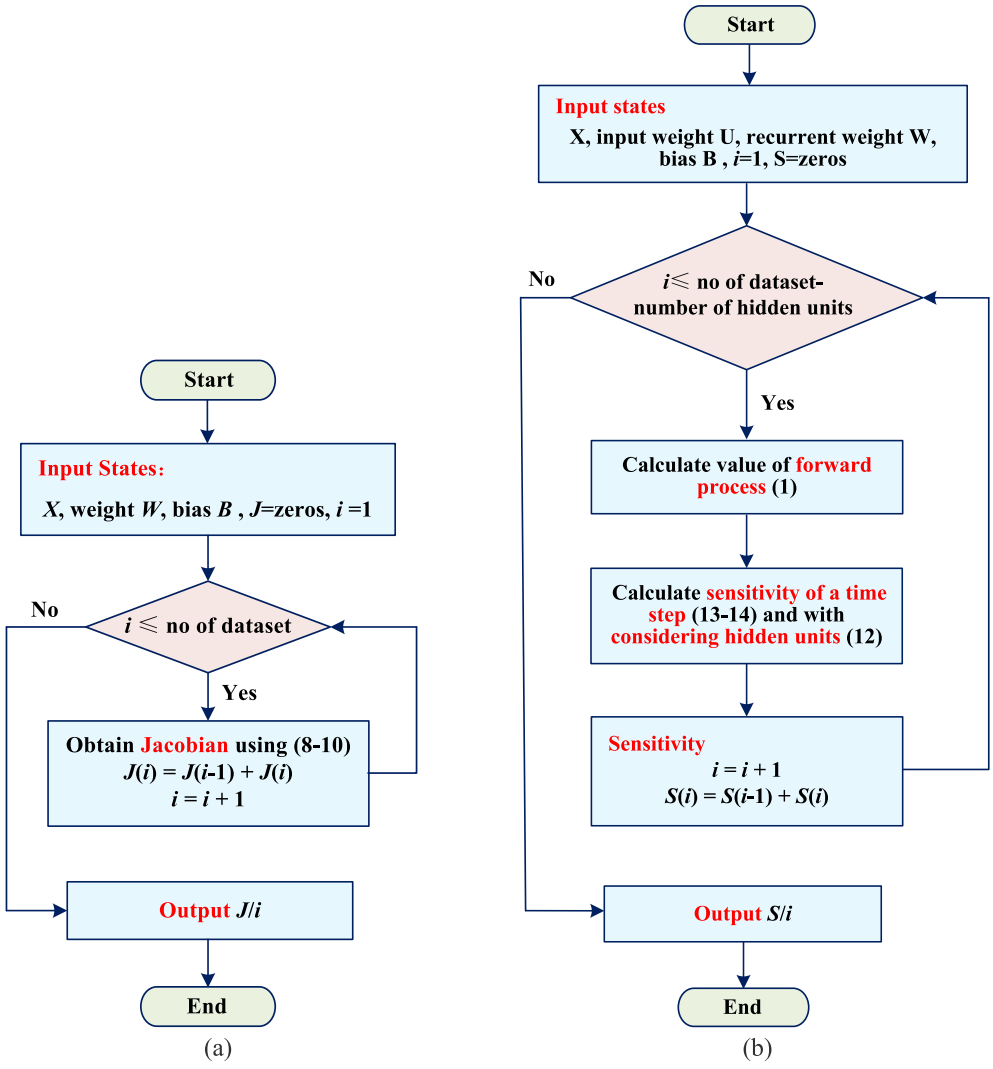

Fig. 14. Flow chart of sensitivity calculation (a) For neural network (b) For GRU based framework.

References

[1] Mohammadi F, Mohammadi-Ivatloo B, Gharehpetian G, et al. Robust control strategies for microgrids: a review. IEEE Syst J 2022;16(2):2401–12.
[2] Zolfaghari M, Gharehpetian GB, Shafie-khah M, et al. Comprehensive review on the strategies for controlling the interconnection of AC and DC microgrids. Int J Electr Power Energy Syst 2022;136:107742.
[3] Saxena V, Kumar N, Singh B, Panigrahi BK. A voltage support control strategy for grid integrated solar PV system during abnormal grid conditions utilizing interweaved GI. IEEE Trans Ind Electron 2021;68(9):8149–57.
[4] Han Y, Ning X, Li L, Yang P, et al. Droop coefficient correction control for power sharing and voltage restoration in hierarchical controlled DC microgrids. Int J Electr Power Energy Syst 2021;133:107277.
[5] Liu Y, Zhuang X, Zhang Q, Arslan M, et al. A novel droop control method based on virtual frequency in DC microgrid. Int J Electr Power Energy Syst 2020;119:105946.
[6] Weaver WW, Robinett IIIRD, et al. Energy storage requirements of dc microgrids with high penetration renewables under droop control. Int J Electr Power Energy Syst 2015;68:203–9.
[7] Shahid MU, Khan MM, Hashmi K, et al. Renewable energy source (RES) based islanded DC microgrid with enhanced resilient control. Int J Electr Power Energy Syst 2019;113:461–71.
[8] Abhinav S, Modares H, Lewis FL, Davoudi A. Resilient cooperative control of DC microgrids. IEEE Trans Smart Grid 2019;10(1):1083–5.
[9] Poudel BP, Mustafa A, Bidram A, et al. Detection and mitigation of cyber-threats in the DC microgrid distributed control system. Int J Electr Power Energy Syst 2020;120:105968.
[10] Tan S, Guerrero JM, Xie P, Han R, Vasquez JC. Brief survey on attack detection methods for cyber-physical systems. IEEE Syst J 2020;14(4):5329–39.
[11] Meng L, Dragicevic T, Vasquez J, Guerrero J. Tertiary and secondary control levels for efficiency optimization and system damping in droop controlled DC–DC converters. IEEE Trans Smart Grid 2015;6(6):2615–26.
[12] Beg O, Johnson T, Davoudi A. Detection of false-data injection attacks in cyber-physical DC microgrids. IEEE Trans Ind Inf 2017;13(5):2693–703.
[13] Sahoo S, Mishra S, Peng J, Dragičević T. A stealth cyber-attack detection strategy for DC microgrids. IEEE Trans Power Electron 2019;34(8):8162–74.
[14] Sahoo S, Peng J, Devakumar A, Mishra S, Dragičević T. On detection of false data in cooperative DC microgrids: a discordant element approach. IEEE Trans Ind Electr 2020;67(8):6562–71.
[15] Saha S, Roy TK, Mahmud MA, et al. Sensor fault and cyber attack resilient operation of DC microgrids. Int J Electr Power Energy Syst 2018;99:540–54.
[16] Jena S, Padhy NP, Guerrero JM. Cyber-resilient cooperative control of DC microgrid clusters. IEEE Syst J 2022;16(2):1996–2007.
[17] Saha S, Haque ME, Tan CP, Mahmud MA. Sensor fault resilient operation of permanent magnet synchronous generator based wind energy conversion system. IEEE Trans Ind Appl 2019;55(4):4298–308.
[18] Peng J, Fan B, Yang Q, Liu W. Distributed event-triggered control of DC microgrids. IEEE Syst J 2021;15(2):2504–14.
[19] Siu JY, Kumar N, Panda SK. Command authentication using multi-agent system for attacks on the economic dispatch problem. IEEE Trans Ind Appl Early Access. (DOI: 10.1109/TIA.2022.3172240).
[20] Siu JY, Kumar N, Panda SK. Attack detection and mitigation using multi-agent system in the deregulated market. In: 2021 IEEE 12th Energy Conversion Congress & Exposition - Asia (ECCE-Asia); 2021. p. 821-826.
[21] Sahoo S, Dragičević T, Blaabjerg F. An event-driven resilient control strategy for DC microgrids. IEEE Trans Power Electron 2020;35(12):13714–24.
[22] Deng C, Wang Y, Wen C, Yan X, Lin P. Distributed resilient control for energy storage systems in cyber–physical microgrids. IEEE Trans Ind Inf 2021;17(2):1331–41.

[23] Cecilia A, Sahoo S, Dragičević T, Costa-Castelló R, Blaabjerg F. Detection and mitigation of false data in cooperative DC microgrids with unknown constant power load. IEEE Trans Power Electron 2021;36(8):9565–77.
[24] Habibi M, Baghaee H, Dragicevic T, Blaabjerg F. Detection of false data injection cyber-attacks in DC microgrids based on recurrent neural networks. IEEE J Emerg Selected Topics Power Electron 2021;9(5):5294–310.
[25] He Y, Mendis G, Wei J. Real-time detection of false data injection attacks in smart grid: a deep learning-based intelligent mechanism. IEEE Trans Smart Grid 2017;8 (5):2505–16.
[26] Rath S, Pal D, Sharma PS, Panigrahi BK. A cyber-secure distributed control architecture for autonomous AC microgrid. IEEE Sys J 2021;15(3):3324–35.
[27] Abianeh AJ, Mardani MM, Ferdowsi F, Gottumukkala R, Dragičević T. Cyber-resilient sliding-mode consensus secondary control scheme for islanded AC microgrids. IEEE Trans Power Electron 2022;37(5):6074–89.
[28] Liu XK, Wen C, Xu Q, Wang YW. Resilient control and analysis for dc microgrid system under dos and impulsive FDI attacks. IEEE Trans Smart Grid 2021;12(5): 3742–54.
[29] Ren XX, Guang HY. Adaptive control for nonlinear cyber-physical systems under false data injection attacks through sensor networks. Int J Robust Nonlinear Control 2020;1(30):65–79.
[30] Abbaspour A, Sargolzaei A, Forouzannezhad P, Yen KK, Sarwat AI. Resilient control design for load frequency control system under false data injection attacks. IEEE Trans Ind Electron 2020;67(9):7951–62.
[31] Yang H, Han H, Yin S, et al. Sliding mode-based adaptive resilient control for Markovian jump cyber–physical systems in face of simultaneous actuator and sensor attacks. Automatica 2022;142:110345.
[32] Habibi MR, Baghaee HR, Dragičević T, Blaabjerg F. False data injection cyber-attacks mitigation in parallel DC/DC converters based on artificial neural networks. IEEE Trans Circuits Syst II 2021;68(2):717–21.
[33] Kamal MB, Mendis GJ, Wei J. Intelligent soft computing-based security control for energy management architecture of hybrid emergency power system for more-electric aircrafts. IEEE J Sel Top Signal Process 2018;12(4):806–16.
[34] Shi H, Xu M, Li R. Deep learning for household load forecasting—A novel pooling deep RNN. IEEE Trans Smart Grid 2018;9(5):5271–80.
[35] Alavi SA, Mehran K, Vahidinasab V, Catalão JPS. Forecast-based consensus control for DC microgrids using distributed long short-term memory deep learning models. IEEE Trans Smart Grid 2021;12(5):3718–30.
[36] Chung J, Gulcehre C, Cho K, Bengio Y. Empirical evaluation of gated recurrent neural networks on sequence modeling. 2014, arXiv:1412.3555 [cs.NE].
[37] Hochreiter S, Schmidhuber J. Long short-term memory. Neural Comput 1997;9(8): 1735–80.
[38] Salimi A, Batmani Y, Bevrani H. Model-based fault detection in DC microgrids. In: IEEE Smart Grid Conference (SGC), Tehran, Iran; 2019. p. 1-6, 2019.
[39] Dali A, Diaf S, Tadjine M. Sensor fault tolerant control of a photovoltaic DC-DC buck converter: HDS approach. In: IEEE 2016 8th International Conference on Modelling, Identification and Control (ICMIC), Algiers, Algeria; 2016. p. 786-791.
[40] Habibi MR, Baghaee HR, Blaabjerg F, Dragičević T. Secure MPC/ANN-based false data injection cyber-attack detection and mitigation in DC microgrids. IEEE Syst J 2022;16(1):1487–98.
[41] Habibi MR, Baghaee HR, Blaabjerg F, Dragičević T. Secure control of DC microgrids for instant detection and mitigation of cyber-attacks based on artificial intelligence. IEEE Syst J 2022;16(2):2580–91.
[42] Pizarroso J, Portela J, Muñoz A, Neuralsens: sensitivity analysis of neural networks.2020, arXiv:2002.11423.
[43] Petersen K, Pedersen M. Derivatives The matrix cookbook. 11th ed. M.A: Technical University of Denmark; 2012.