An Explainable Intelligent Framework for Anomaly Mitigation in Cyber-Physical Inverter-based Systems

Asad Ali Khan 1,1, Omar A Beg 2, Yufang Jin 2, and Sara Ahmed 2

1The University of Texas at San Antonio
2Affiliation not available

October 31, 2023

Abstract

An explainable intelligent framework for cyber anomaly mitigation of cyber-physical inverter-based systems is presented. Smart inverter-based microgrids essentially constitute an extensive communication layer that makes them vulnerable to cyber anomalies. The distributed cooperative controllers implemented at the secondary control level of such systems exchange information among physical nodes using the cyber layer to meet the control objectives. The cyber anomalies targeting the communication network may distort the normal operation therefore, an effective cyber anomaly mitigation technique using an artificial neural network (ANN) is proposed in this paper. The intelligent anomaly mitigation control is modeled using a dynamic recurrent neural network that employs a nonlinear autoregressive network with exogenous inputs. The effects of false data injection to the distributed cooperative controller at the secondary control level are considered. The training data for designing the neural network are generated by multiple simulations of the designed microgrid under various operating conditions using MATLAB/Simulink. The neural network is trained offline and tested online in the simulated microgrid. The proposed technique is applied as secondary voltage and frequency control of distributed cooperative control-based microgrid to regulate the voltage under various operating conditions. The performance of the proposed control technique is verified by injecting various types of false data injection-based cyber anomalies. The proposed ANN-based secondary controller maintained the normal operation of microgrid in the presence of cyber anomalies as demonstrated by real-time simulations on a real-time digital simulator OPAL-RT.
An Explainable Intelligent Framework for Anomaly Mitigation in Cyber-Physical Inverter-based Systems

Asad Ali Khan, Student Member, IEEE, Omar A Beg, Member, IEEE, Yu-Fang Jin, Member, IEEE
Sara Ahmed, Senior Member, IEEE

Abstract—Smart inverter-based microgrids essentially constitute an extensive communication layer that makes them vulnerable to cyber anomalies. The distributed cooperative controllers implemented at the secondary control level of such systems exchange information among physical nodes using the cyber layer to meet the control objectives. The cyber anomalies targeting the communication network may distort the normal operation therefore, an effective cyber anomaly mitigation technique using an artificial neural network (ANN) is proposed in this paper. The intelligent anomaly mitigation control is modeled using a dynamic recurrent neural network that employs a nonlinear autoregressive network with exogenous inputs. The effects of false data injection to the distributed cooperative controller at the secondary control level are considered. The training data for designing the neural network are generated by multiple simulations of the designed microgrid under various operating conditions using MATLAB/Simulink. The neural network is trained offline and tested online in the simulated microgrid. The proposed technique is applied as secondary voltage and frequency control of distributed cooperative control-based microgrid to regulate the voltage under various operating conditions. The performance of the proposed control technique is verified by injecting various types of false data injection-based cyber anomalies. The proposed ANN-based secondary controller maintained the normal operation of microgrid in the presence of cyber anomalies as demonstrated by real-time simulations on a real-time digital simulator OPAL-RT.

Index Terms—Artificial neural networks, cyber anomaly mitigation, distributed cooperative control, explainable neural networks, false data injection, microgrids.

I. INTRODUCTION

MICROGRIDS are cyber-physical systems (CPS) that include multiple distributed generators (DGs), loads and a communication network. Both centralized and distributed control mechanisms have been deployed in microgrids [1]–[3]. Distributed control for microgrids provides improved reliability and scalability when compared to centralized control [4]. However, due to the structure of the distributed control, it is more vulnerable to physical and cyber anomalies [5], [6]. Cyber anomalies occur when an adversary targets the communication network by false data injection (FDI) or compromising information sharing in the network [7]–[10]. These anomalies can result in system stability problems like loss of synchronization during operation [11]. Therefore, an effective mitigation strategy is required for smooth operation of microgrids under those anomalies. This paper presents an intelligent anomaly mitigation framework for cooperative distributed controlled inverter-based systems under cyber anomalies.

Most of the recent anomaly mitigation techniques in AC microgrids are model-based approaches, requiring a detailed accurate model and accurate architectural knowledge of the system [12]–[18]. However, for large-scale microgrid systems whose mathematical models are hard to derive, learning-based tools such as artificial neural network (ANNs) can be used for cyber anomalies mitigation and control design [19]–[25]. ANNs are utilized to improve power sharing, distributed generation management, and resilient control design in multi-DG microgrids. Specifically, ANNs are designed using historical voltage and current measurements to act as an estimator and an observer layer for FDI detection and mitigation in cooperative controlled DC microgrids [26]–[29]. The application of ANN-based control for AC microgrids is not common as manifested from the usage of ANN as an observer layer in [25] and in reference tracking applications for DC microgrids in [28]. In this paper, we novel use nonlinear autoregressive exogenous model (NARX ANN) as a resilient secondary control layer in a multi-DG AC microgrid.

The proposed ANN-based secondary control technique is resilient against cyber anomalies. The false data is injected to voltage and frequency communication links and the designed control technique maintained the desired operation of the system. The proposed control method is robust and that is accomplished by generating ANN training data under varied load situations and exhibiting the performance under time-varying cyber anomalies. The paper also presents an explainable framework for the proposed ANN models and controllers using partial dependence plots (PDP) to evaluate the impact of various inputs on the model’s performance. Performance comparisons with existing proportional-integral (PI)-based distributed secondary control method and real-time simulations for an AC microgrid, on the real-time digital simulator OPAL-RT are used to validate the proposed ANN-based control strategy. The results obtained from various case studies showed the effectiveness of the proposed ANN-based secondary control for AC microgrids. The mean absolute percentage error (MAPE), the voltage and frequency regulation are used as a benchmark to evaluate the performance of the trained ANNs. The resilience of the proposed ANN-based control is also tested under a noisy environment by adding white Gaussian noise to the voltage and frequency inputs of ANN.

The rest of the paper is organized as follows. Section II describes the AC microgrid used in this paper, along
with the types of cyber anomalies. The structure of ANN is given in section III. In section IV, the design of ANN-based secondary voltage and frequency control is presented. The results obtained from real-time simulations performed on the test microgrid are given in section V. Finally, this paper is concluded in section VI.

II. SYSTEM DESCRIPTION

The AC microgrid designed for this study consists of a physical layer and a cyber layer. The physical layer is composed of multiple DGs with various loads. The cyber layer contains the communication protocols for voltage and frequency information exchange in a distributed cooperative control architecture as illustrated in Fig. 1. Primary controller is implemented locally at each of the DG using conventional droop control technique that provides relationship between the frequency $\omega_i$, the reactive power $Q_i$, the active power $P_i$, and the voltages $v_o$. The voltage and frequency droop characteristics are given by:

$$
\begin{cases}
    v_o = v^* - nQ_i Q_i, \\
    w_i = w^* - mP_i P_i,
\end{cases}
$$

(1)

where $v^*$, $w^*$ are the primary voltage and frequency reference values, and $mP_i$, $nQ_i$ are the active and reactive power droop coefficients, respectively. At the secondary level, distributed cooperative control is utilized to reduce voltage and frequency deviations from nominal values generated by primary control. As demonstrated in Fig. 1, the relevant control protocols are implemented over a distributed communication network. The secondary control sets a reference for primary control such that each DG’s voltage and frequency synchronize with their respective reference values ($v^*$ and $w^*$):

$$
\begin{align*}
    \lim_{t \to \infty} ||v_o - v^*|| &= 0, \\
    \lim_{t \to \infty} ||w_i - w^*|| &= 0.
\end{align*}
$$

(2)

Based on communication protocol, the $n^{th}$ DG in the microgrid may need to share their voltage information over the communication network. Assuming that only one DG has access to the reference $v^*$, by a weight factor known as pinning gain $b_i$, the cooperative control objective in terms of local neighborhood tracking error ($v_{en}$) is as follows:

$$
v_{en} = \sum_{j \in S_n} a_{ij} (v_i - v_j) + b_i (v_i - v^*),
$$

(3)

where $S_n$ represents the set of neighboring DGs of the $n^{th}$ DG, $a_{ij}$ represents the elements of adjacency matrix, and only one DG has nonzero $b_i$. Similarly, for distributed secondary frequency control the auxiliary control input $u_i$ is as follows:

$$
\begin{align*}
    u_i &= -c_g \sum_{j \in S_n} a_{ij} (\omega_i - \omega_j) + b_i (\omega_i - \omega^*) \\
    &\quad + \sum_{j \in S_n} a_{ij} (mP_i P_i - mP_j P_j),
\end{align*}
$$

(4)

where $c_g$ is the coupling gain. In [4], more information about distributed cooperative control architecture is provided. Next, a description of the cyber anomalies investigated in this paper are given.
A. Cyber Anomalies

The cyber anomalies target the microgrid’s communication layer by feeding false data or compromising the network’s information exchange. FDI is implemented in this paper by injecting false data into the voltage and frequency information of neighboring DGs that is fed to the distributed secondary controller. A controller’s feedback signal can be characterized as:

\[ x(u_n(t)) = u_n(t) + \psi_n(t), \]

where \( x(u_n(t)) \) is the feedback signal after the attacker injects false data \( \psi_n(t) \) into the controller’s \( n^{th} \) normal feedback signal [28]. The following are five types of FDI attacks based on various \( \psi_n(t) \):

**Type 1 - Stationary attack:** A stationary attack is non-periodic in nature and it is launched by injecting a constant multiple \( \gamma \) of the desired signal \( u_n(t) \) into \( x(u_n(t)) \) at certain time \( t_o \) throughout the system’s operation, as follows:

\[ x(u_n(t)) = \begin{cases} u_n(t), & \text{where } t < t_o, \\ u_n(t) + \gamma * u_n(t), & \text{where } t > t_o. \end{cases} \]

(6)

**Type 2 - Reinforcement attack:** During a reinforcement attack, the system is compelled to follow the incorrect set of reference points by fully replacing the desired reference value with false data. The attacker replaces the intended signal \( u_n(t) \) entirely with its multiple, resulting in:

\[ x(u_n(t)) = \begin{cases} u_n(t), & \text{where } t < t_o, \\ \gamma * u_n(t), & \text{where } t > t_o. \end{cases} \]

(7)

**Type 3 - Time varying attack:** The periodic time varying attack is initiated by injecting a periodic sinusoidal signal with time period \( (\omega t) \) and amplitude \( \xi \) into the normal signal \( u_n \), as follows:

\[ \psi_n(t) = \begin{cases} 0, & \text{where } t < t_o, \\ \xi \sin(\omega t) * u_n(t), & \text{where } t > t_o. \end{cases} \]

(8)

**Type 4 - Manifold attack:** A manifold attack is composed of both stationary and time-varying attacks. This attack begins with the injection of false information, both periodic and non-periodic, as follows:

\[ \psi_n(t) = \begin{cases} 0, & \text{where } t < t_o, \\ \gamma * u_n(t) + \xi \sin(\omega t) * u_n(t), & \text{where } t > t_o. \end{cases} \]

(9)

**Type 5 - Coordinated attack:** In a coordinated attack scenario, the adversary injects false data into all of the DGs in the system to launch a large-scale attack, such that:

\[ x(u_n(t))_{4 \times 1} = \begin{cases} [u_n(t)]_{4 \times 1}, & \text{where } t < t_o, \\ [u_n(t)]_{4 \times 1} + \chi, & \text{where } t > t_o. \end{cases} \]

where \( \chi \) is the false data being injected to all the four DGs of the microgrid system when \( t > t_o \).

---

**III. NONLINEAR AUTO-REGRESSIVE EXOGENOUS ARTIFICIAL NEURAL NETWORKS**

NARX ANN (used as ANN for brevity in manuscript) are a special class of recurrent neural networks best suited for time series data prediction, input-output modeling of nonlinear dynamical systems, and cyber attack detection in microgrids [29], [30]. In this paper, we used a single layer ANN to generate the reference voltage for the primary controllers; The input layer has 13 nodes for voltage and frequency information, and the output has 4 nodes for corresponding reference output at each DG. There are 10 number of nodes for hidden layer. Mathematical model of ANN is given as follows:

\[ y(k+1) = f[x(k-n), ..., x(k-d_x-n+1), y(k), ..., y(k-d_y+1)], \]

(11)

where \( y(k) \) is the model output, \( x(k) \) is the model input at discrete time interval \( k \), \( d_x \) is input memory order, and \( d_y \) is output memory order. Assuming delay term \( k = 0 \), the model takes the form as follows:

\[ y(k+1) = f[x(k), ..., x(k-d_x+1), y(k), ..., y(k-d_y+1)], \]

(12)

which can be expressed in vector form as follows:

\[ y(k+1) = f[Y(k); X(k)], \]

(13)

where bold face letters represent vectors such as \( Y(k) \) and \( X(k) \) represent the output and input, respectively. The nonlinear mapping \( f(.) \) can be approximated by standard multilayer perceptron network. The architecture of a single layer ANN is shown in Fig. 2. and its training can be carried out in the following two configurations:

1) **Parallel Configuration:** The parallel configuration is shown in Fig. 3a such that the estimated output of the
network is fed back into the ANN input as follows:
\[
y(k+1) = \hat{f}(x(k), \ldots, x(k-d_x+1), \hat{y}(k), \ldots, \hat{y}(k-d_y+1)),
\]
(14)

2) Series Parallel Configuration: This configuration is depicted in Fig. 3b, wherein actual output values are used without feedback. The estimated output \( \hat{y} \) is given by:
\[
y(k+1) = \hat{f}(x(k), \ldots, x(k-d_x+1), y(k), \ldots, y(k-d_y+1)),
\]
(15)

Because the real output is accessible from microgrid operation, the series parallel configuration is used for the training and operation of ANN. The design of the proposed ANN-based secondary control layer is discussed in the next section.

IV. ANN-BASED DISTRIBUTED SECONDARY CONTROL DESIGN

The training of ANN models is crucial to their optimal performance. The reference for the primary control layer at each inverter is generated by the secondary distributed cooperative control [4]. As a result, each DG is constructed with ANN-based resilient secondary voltage control to generate the reference for primary controller. The control objective is to maintain the output voltage and current in predefined bounds. The proposed control structure is explained as under:

A. ANN-Based Secondary Voltage Control

Offline simulations of the test microgrid are performed to collect data for ANN training. The step load change is included in generating the training data set. The data is generated for normal operating conditions with three set reference voltages in order to complete the learning of ANNs.

B. Data Generation

For data generation, the following scenarios are considered:

1) Based on the communication graph in Fig. 5, each DG shares voltage information with the two neighboring DGs.

2) The test microgrid is operated within designed normal operating conditions and each DG’s own voltage information \( v_{n}\text{.} \) where \( n \in \{1, 2, 3, 4\} \), the voltage information from neighbors of DG1 \( v_{1i} \) and DG3 \( v_{3i} \), where \( i \in \{2, 4\} \), the voltage information from neighbors of DG2 \( v_{2j} \) and DG4 \( v_{4j} \) where \( j \in \{1, 3\} \), the reference voltage \( v^* \), and the primary control reference voltage output generated by each DG \( v_n^* \), are gathered.

3) The test microgrid in Fig. 4 is simulated with 5 load step changes and 3 different set reference voltages. This results in a total of 15 separate simulated microgrid events, each with a simulation run time of 2 s. Having a sampling rate of 1 ms for data collection, results in 15,000 data points for training the ANN model. The data sampling and simulation run times are selected such that the microgrid achieves steady-state following a load change.

The training data input \( P \) for training of ANNs is obtained from multiple simulations of the test microgrid where \( P = [v_{nn}, v_{1i}, v_{3i}, v_{2j}, v_{4j}, v^*]_{13\times1} \) and the target for training of ANNs is \( T \), where \( T = [v_n^*]_{4\times1} \). For offline training of ANN to optimize the weights, both \( P \) and \( T \), which are generated by executing various scenarios of simulations, are used. The attack vector for all DGs aimed at secondary voltage control information sharing is as follows:
\[
\mathbf{V}_{ij\text{controller}} = \mathbf{V}_{ij\text{actual}} + \chi_{\text{attack}} \mathbf{V}_{ij},
\]
(16)
such as \( \mathbf{V}_{ij\text{controller}} \) is the compromised input to the secondary voltage controller of \( DG_n \), \( \mathbf{V}_{ij\text{actual}} \) is the vector of real measurements, and \( \chi_{\text{attack}} \) represents the attack cases from section II-A. Because of the compromised information exchange, the control objectives may be disrupted, resulting in synchronization loss or divergence from the required reference voltage value. Remark 1: The FDI attack starts at time \( t_o \) and the output voltage follows the reference values before the attack at \( (t-t_o) \) but the output deviates from the desired reference after the attack at \( (t+t_o) \). The difference between \( \hat{v}_n^* \) and \( v_n^* \) is \( |\hat{v}_n - v_n^*| = \mu_v \), where, \( \hat{v}_n \) is the output voltage of the \( n^{th} \) DG under attack, \( v_n^* \) is the reference output voltage for each DG unit, and ANN-based secondary voltage control attempts to decrease this error as follows:
\[
\lim_{t \to \infty} \mu_v = 0.
\]
(17)

Remark 2: The ANN learns the system’s dynamics through offline training. The trained ANN model operates for the system having the same control mechanism used in the training phase for the online implementation [28]. Therefore, the trained ANN can now act as a distributed secondary control layer for the microgrid under investigation.

C. Training of ANN-Based Secondary Voltage Control

The architecture of the ANN model selected for secondary voltage controller is based on the following relationship:
\[
\begin{bmatrix}
0 & 1 & 1 & 0 & 1 \\
0 & 1 & 1 & 1 & 0 \\
1 & 0 & 1 & 1 & 1 \\
0 & 1 & 0 & 1 & 1
\end{bmatrix}
A \begin{bmatrix}
v_1^* \\
v_2^* \\
v_3^* \\
v_4^*
\end{bmatrix}
= \begin{bmatrix}
v_1 \\
v_2 \\
v_3 \\
v_4
\end{bmatrix}
B,
\]
(18)
where \( A \) is the microgrid’s connection matrix, \( X \) is the voltage information for all DGs at the secondary control level, and \( B \) is the reference voltages generated by each DG fed to the primary level controller at each DG. The following are the stages involved in training the ANN model:

1) To optimize the weights of the ANN during the offline training process, the feature vector for training and testing of the ANN model is taken from past data.

2) To train an ANN model efficiently, choosing the best feature vector is crucial. The supervised learning method is chosen for ANN model training in order to maximize training to accomplish the control objective with known inputs \( P \) and output \( T \).

3) The generated data is divided into training, testing, and validation with 70 %, 15 %, and 15 %, respectively.

4) The Levenberg-Marquardt training algorithm is used for training that stops when maximum generalization is achieved, indicated by the lowest mean square error (MSE) of the validation data. The maximum number of
epochs is set to 1000 and the lowest MSE of $2.32 \times 10^{-3}$ for validation data was obtained after 374 iterations.

5) After numerous training sessions, the design of the ANN, including hidden layers and the number of neurons, is determined to be optimal. This architecture has one input layer, one output layer, and one hidden layer with ten neurons, and it was found suitable for this application. The hidden layer’s activation function is tansig, while the output layer’s activation function is purelin. This architecture has been employed in time-series data prediction applications for microgrids [28].

6) During the offline training of ANN, the bias vector $b$ and the weight matrix $w$ are optimized. This trained model is then tested against an unknown test data set to ensure that it performs as expected by measuring the output voltages and currents of microgrid.

D. ANN-based Secondary Frequency Control Design

A distributed secondary frequency control layer is included in the test microgrid for coordinated operation of multiple DGs under different operational conditions as shown in Fig. 1. The operation of the microgrid is extremely sensitive to changes in frequency information, and any FDI aimed against the frequency information links between DGs may destabilize the microgrid [5]. As a result, the ANN model is applied at the microgrid’s secondary frequency control layer to mitigate the impact of FDI. For the test microgrid, DG1 and DG3 are chosen as the leading nodes, with DG2 and DG4 following behind to implement the cooperative control objectives given in (4). Therefore, ANN-based secondary frequency controller is implemented for DG2 and DG4. Following the similar process as given in sections IV-A and IV-C, the training data of the ANN-based secondary frequency controller are generated such that the training input is $P = [\omega_{nn}, \omega_{2j}, \omega_{2j}]_{6 \times 1}$, where $j \in (1, 3)$ such that, $\omega_{nn}$ is the frequency information of DG2 and DG4, $\omega_{2j}$, and $\omega_{2j}$ are frequency information from the neighbors of DG2 and DG4, respectively. The training target is $T = [\omega^*_{nn}]_{2 \times 1}$, where $n \in (2, 4)$ and $\omega^*_{nn}$ represents the first primary level reference frequency generated by DG2 and DG4. Various scenarios are implemented to measure the performance of the trained ANN model, as follows.

E. Training and Test Scenarios

The following scenarios are included in the time series simulations of the microgrid shown in Fig. 4:

Scenario 1: Step load change: $L_k$, where $k \in \{4, ..., 8\}$ kW.

Scenario 2: Target of FDI: In the cyber layer for all DGs, the voltage and frequency information exchange channels are targeted for inserting false data to cause cyber anomalies.

Scenario 3: Type of FDI: Various types of FDI are applied as described in section II-A.

Scenario 4: Reference voltage: Three different values are used for secondary level reference set voltage, i.e., $[300, 325, 350]V$.

The performance of trained ANN model is evaluated using the MAPE, given as:

$$\text{MAPE} = \frac{1}{m} \sum_{k=1}^{m} \frac{|y_p - y|}{y} \times 100,$$

where, $m$ represents total number of cases, $y$ is the actual output, and $y_p$ is the predicted output. The trained ANN model is also evaluated by adding white Gaussian noise into the measurements. To achieve the signal to noise ratio (SNR) with three distinct noise levels: i) 30 db, ii) 35 db, and iii) 40 db, the white Gaussian noise is added into the test data input [31]. The results of this case study are given in Table I. As can be observed from these data, adding noise to the input has a negligible effect on performance. Since it almost produced the same MAPE as the test data set without any distortion, the proposed technique’s resiliency against distorted measurements was confirmed. The performance of the proposed ANN-based secondary control is validated by executing real-time scenarios on the real-time digital simulator OPAL-RT under FDI cyber anomalies after training the ANN, and the results are reported in the following section.

V. SIMULATION RESULTS

The performance of the proposed ANN-based secondary control is evaluated using the test microgrid system by performing real time simulations as illustrated in Fig. 4. The four DG voltage source inverters are coupled through RL lines to provide AC power to two-three phase RL loads, denoted by $load_1$ and $load_2$ in Fig. 4. The four DGs of the test microgrid share their voltage and frequency information over the communication network as shown in Fig. 5. Table II lists the parameters of the test microgrid system and the real-time simulator setup. The cyber anomalies are introduced in the test microgrid system after the model is built up on a real-time target, as explained in the following sections.

<table>
<thead>
<tr>
<th>SNR (db)</th>
<th>DG1</th>
<th>DG2</th>
<th>DG3</th>
<th>DG4</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0.05</td>
<td>0.11</td>
<td>0.01</td>
<td>0.40</td>
</tr>
<tr>
<td>30</td>
<td>0.06</td>
<td>0.12</td>
<td>0.02</td>
<td>0.41</td>
</tr>
<tr>
<td>35</td>
<td>0.06</td>
<td>0.12</td>
<td>0.02</td>
<td>0.41</td>
</tr>
<tr>
<td>40</td>
<td>0.06</td>
<td>0.12</td>
<td>0.02</td>
<td>0.39</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>OPAL-RT Software</th>
<th>Microgrid</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version OP5600</td>
<td>Name Parameter</td>
</tr>
<tr>
<td>4 Cores, 3.0 GHz</td>
<td>Voltage (V)</td>
</tr>
<tr>
<td>RT-Lab v 2019.2.3</td>
<td>load_1</td>
</tr>
<tr>
<td>FPGA Xilinx® Artix-7 FPGA, 200T</td>
<td>load_2</td>
</tr>
</tbody>
</table>
A. Type 1 - Stationary attack

Based on (6), an adversary injects false data to the voltage communication links of DGs. In this case the target is DG1 link $v_{11}$ such as at $t = 2$ s with $\gamma = 1.5$, FDI is initiated. The microgrid is operating under normal operating conditions for $t < 2$ s. Following the FDI, the performance of the proposed ANN-based secondary voltage control is compared to the existing PI-based control and results are shown in Fig. 6. As illustrated in Fig. 6a and Fig. 6b, the proposed ANN-based secondary voltage control showed improved reference tracking capability in comparison to PI-based control that was not able to maintain the desired reference value after the FDI. Similarly, it can be seen that ANN-based voltage controller maintained the desired output voltage at the output of DG1, whereas the PI-based controller suffered the distortions in the output voltage after FDI as shown in Fig. 6c.

B. Type 2 - Reinforcement attack

This FDI is based on (7), in which false data is being injected into DGs voltage communication links. Such as for DG2 connection $v_{22}$, FDI is initiated at $t = 2$ s with $\gamma = 0.5$. Until $t = 2$ s, the microgrid is functioning under normal operational circumstances. After the FDI, the proposed ANN-based secondary voltage control is compared to the PI-based control, with the results displayed in Fig. 7. The proposed ANN-based secondary voltage control, as shown in Fig. 7a and Fig. 7b, showed improved reference tracking capabilities compared to the PI-based control. As illustrated in Fig. 7c, the ANN-based voltage controller maintained the appropriate output voltage at the output of DG2 following FDI.

C. Type 3 - Time varying attack

This FDI, based on (8), targets the voltage communication of DGs. In this case, false data is injected into the DG3 voltage communication link $v_{33}$ at $t = 2$ s with $\xi = 0.5$ and $w = 2\pi60$. The microgrid continues to operate normally for $t < 2$ s. The designed ANN-based secondary voltage control is compared to the PI-based control after the FDI, with the results shown in Fig. 8. The proposed ANN-based secondary voltage control, performed better in terms of reference tracking than the PI-based control as shown in Fig. 8a and Fig. 8b. Following FDI, the ANN-based voltage controller maintained the specified output voltage at the output of DG3 as depicted in Fig. 8c.

D. Type 4 - Manifold attack

This FDI is initiated by injecting false data into the DG4 voltage communication connection $v_{44}$ with $\gamma = 0.5$, $\xi = 0.5$, and $w = 2\pi60$ at $t = 2$ s, based on (9). The microgrid operates normally until $t = 2$ s. Following the FDI, the proposed ANN-based secondary voltage control is compared to PI-based control, with the results shown in Fig. 9. The proposed ANN-based secondary voltage control, as illustrated in Fig. 9a and Fig. 9b, showed improved performance in terms of reference tracking compared to the PI-based control. Also, the ANN-based voltage controller kept the stated output voltage at the output of DG4 after initiating FDI, as shown in Fig. 9c.

E. Type 5 - Coordinated attack

Under a coordinated attack, the adversary targets all the DGs present in the microgrid as given in (10). At $t = 2$ s, the voltage communication links of all the four DGs are compromised by injecting false data. This is a severe type of cyber anomaly due to its wide spread nature. The results of the proposed ANN-based secondary voltage control are compared to PI-based control following a FDI in terms of output voltage and current at $x_{load1}$ of test microgrid as shown in Fig. 10. The designed ANN-based controller maintained the power quality by keeping the desired phase and amplitude of three phases currents, whereas the PI-based controller did not withstand the FDI as shown in Fig. 10a. Similarly, the desired three phases voltages were maintained after FDI in case of proposed ANN-based control compared to the PI-based control that showed large deviations from the desired output voltage as depicted in Fig. 10b.

F. FDI Targeting the Frequency Communication Links

The ANN-based frequency controller is implemented for DG2 and DG4 at the secondary control level of the test microgrid. Type 3, FDI is applied targeting the frequency communication links of DG2 $w_{22}$ and DG4 $w_{44}$ with $\xi = 0.5$ and $w = 2\pi60$ based on (8). The proposed ANN-based frequency control maintained the desired frequency value following the FDI compared to the PI-based control, as shown in Fig. 11. The FDI is initiated at $t = 2$ s at DG2 and DG4 and it is evident from Fig. 11a and Fig. 11b that the designed ANN-based frequency control kept the system in normal operating condition with a little deviation following the FDI than PI-based control that showed large deviations from set reference value.

G. Variable Operating Settings

To further validate the performance of the proposed ANN-based voltage control under varying operating conditions, a step load change is applied and results are given in Fig. 12. A step down load change is applied at $t = 2$ s and a Type 2 FDI with $\gamma = 0.5$ is initiated at $t = 2$ s. It can be seen in Fig. 12a, that designed ANN-based controller follows the expected response as PI-based control with a decrease in current magnitude but following the FDI the PI-based control deviates from the desired current value. Similarly, the designed ANN-based controller sustained the desired voltage level following both a step down load change and FDI, whereas PI-based control could not sustain the effect of FDI and showed distortion in...
output voltage as evident from Fig. 12b. This showed the robust performance of proposed ANN-based control under changing operating conditions of test microgrid.

**H. Explainable ANN model**

PDP is one of the methods for global interpretability of ANN models that helps understand the model’s response over a complete data set [32], [33]. PDP are plotted for the
Fig. 12: The performance comparison of controllers under a step load change and FDI is given.

trained ANN model proposed in this paper to see the impacts on various DGs in the microgrid during cyber anomalies. Predictive response’s partial dependence is computed on a subset of predictor features by marginalizing over the other features. Based on (18), consider a subset $v_{ns}$ such that $v_{ns} = \{v_{11}, v_{12}, v_{13}\}$ and $n \in \{1,2,3,4\}$ represents the four DGs in the microgrid. Let $v_{nc}$ be the complementary set of $v_{ns}$, such that $v_{nc} = \{v_{ij} \notin v_{ns}\}$, where $v_{ij}$ represents the voltage information from neighboring DGs and $V_n$ is the set containing voltage information of all four DGs in the microgrid. The predicted output $v_n^*$ of trained ANN model $f(.)$ depends on all the features in $V_n$, given as:

$$f(V_n) = f(v_{ns}, v_{nc})$$  \hspace{1cm} (20)

The predicted output $v_n^*$ is the primary reference voltage generated by each DG in microgrid and its partial dependence on $v_{ns}$ is given by the expectation of the predicted output with respect to $v_{nc}$, as follows:

$$f_s(v_{ns}) = E[f(v_{ns}, v_{nc})] = \int f(v_{ns}, v_{nc})p_{nc}(v_{nc})d(v_{nc}),$$  \hspace{1cm} (21)

where $p_{nc}(v_{nc})$ is the marginal probability of $v_{nc}$, given as:

$$p_{nc}(v_{nc}) = \int f(v_{ns}, v_{nc})d(v_{ns}).$$  \hspace{1cm} (22)

Assuming that the correlation between $v_{ns}$ and $v_{nc}$ is not strong the partial dependence is estimated using the observed model’s responses as follows:

$$f_s(v_{ns}) = \frac{1}{m}\sum_{m}^{j=1} f(v_{ns}, v_{nc_j}),$$  \hspace{1cm} (23)

where $j$ is the number of trained model’s responses and $v_{nc_j} = (v_{ns}, v_{nc})$ is the $j^{th}$ response. The PDP for each DG is estimated with an objective of finding the impact of cyber anomaly on each DG. For this purpose, each DG’s voltage information is slanted as $v_{ns}$, individually and the results are shown in Fig. 13. It is evident that DG3 suffers the largest impact by showing maximum deviations following FDI. This finding is in line with (3) and as illustrated in Fig. 5. DG3 is the leading node based on communication graph. Next, the impact of spoofing all the communication links of DG3 on the predicted responses in terms of $v_n^*$ is shown in Fig. 13b. It can be seen that the predicted responses (in blue color) shows large deviations from the actual responses (in red color) of the system. These large deviations in $v_n^*$ lead to reduced power quality and loss of synchronism in the microgrid operation.

VI. CONCLUSION

An intelligent secondary control technique is proposed in this paper to mitigate the effect of cyber anomalies in distributed cooperative-controlled microgrids. This technique employs recurrent type neural networks as distributed secondary voltage and frequency control layer of inverter-based microgrid having multiple DGs. The training data for ANNs was generated through time-series simulation of microgrid under various operating conditions. The scalability and the resilience of the proposed ANN-based secondary control are shown by constructing a connection matrix and adding noise to the input data. The structure of trained ANN model is explained by plotting partial dependence plots. Various types of FDI are considered to verify the effectiveness of the designed ANN-based secondary control. The results are validated by comparing them to the existing distributed secondary control technique. The proposed controller outperformed PI-based secondary voltage regulation by maintaining the normal operation of the microgrid under cyber anomalies. Real-time cyber-attack scenarios are simulated in real-time digital simulator OPAL-RT to validate the proposed resilient control strategy.

REFERENCES


