Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.DOI

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

ASAD ALI KHAN[1], (Member, IEEE), OMAR A BEG[2], (Senior Member, IEEE), YU-FANG JIN[1], (Member, IEEE), and SARA AHMED [1], (Senior Member, IEEE)

[1]Department of Electrical and Computer Engineering, the University of Texas at San Antonio, One UTSA circle, TX 78249, USA (e-mails: asad.khan@my.utsa.edu; sara.ahmed@utsa.edu; yufang.jin@utsa.edu)

[2]Department of Electrical Engineering, The University of Texas, Permian Basin, 4901 E University Blvd, Odessa, TX 79762, USA (e-mail: beg_o@utpb.edu)

Corresponding author: Omar A Beg (e-mail: beg_o@utpb.edu).

ABSTRACT 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 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 neural network that employs a nonlinear autoregressive network with exogenous inputs. The effects of false data injection on 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. An explainable framework is employed to interpret the output generated by the trained neural network-based controller after the neural network has been trained offline and validated 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 the microgrid under various cyber anomalies as demonstrated on a real-time digital simulator.

INDEX TERMS Artificial neural networks, cyber anomaly mitigation, distributed cooperative control, explainable neural networks, false data injection attacks, microgrids.

I. INTRODUCTION

MICROGRIDS have evolved into 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, the challenges in designing and deploying modern distributed microgrids include uncertainties associated with loads, renewable energy resources, and communication networks that are vulnerable to cyber anomalies [5], [6]. Cyber anomalies occur when an adversary targets the communication network by False Data Injection (FDI) attack or compromising information sharing in the network [7]–[10]. These anomalies can result in system instability issues such as loss of synchronization during operation [11]. Therefore, an effective mitigation strategy is required for the smooth operation of microgrids to cater to those 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 Networks (ANNs) can be deployed for cyber anomalies mitigation, dis-

tributed generation management, and resilient control design in multi-DG microgrids [19]–[25]. In addition, ANNs can be designed using historical voltage and current measurements to act as an estimator and an observer layer for FDI attack detection and mitigation in cooperative controlled DC microgrids [26]. In [27], ANN-based resilient control design is proposed to withstand the FDI attacks that contain an anomaly detection system based on the Luenberger observer and ANN. An Extended Kalman filter is used to update the ANN learning weights online such that the input to the ANN is the difference between the actual system output and the output from the Luenberger observer. This will allow the ANN to detect an anomaly in the system and feedback data from the anomaly detection system is then used in a linear quadratic controller to compensate for the anomalies. This proposed method involves iterative calculations that pose scalability challenges as the power system becomes larger and more complex with the integration of distributed energy resources. In [28], an ANN-based reference tracking algorithm is introduced to mitigate the effect of FDI attacks in distributed consensus control-based DC microgrids. This is a two-layer control design in which ANN is applied to mitigate the discrepancies between a normal and compromised signal being fed to a proportional-integral (PI) controller. The signal latency or loss of communication between two such layers may endanger the microgrid's stable operation, which may even lead to a loss of synchronism among DGs. In [29], a model predictive control (MPC)-based ANN control strategy is proposed for the dynamic damping of DC microgrids. This proposed control approach attained the balance between demand and supply under variable operating conditions, but the robustness of the controller under cyber anomalies is not discussed. In [30], ANN is used as an estimator to detect the FDI attack by estimating the reference voltage for the secondary control layer of a DC microgrid. This is similar to a two-layer design using an estimated reference value from ANN as an input to an MPC-based controller to calculate the optimal values of the inputs to track the references by the plant outputs. This method will function properly if ANN can accurately estimate the actual voltage of the DC bus, which may be challenging if the system consists of multiple converters that experience unintended signal perturbation.

A CPS is a sophisticated system that connects physical processes and objects to the network while integrating sensing, computation, control, and networking [31]. Such CPS, including microgrids, are vulnerable to cyber-attacks due to dependence on interactions with the environment and communication networks. In [32], [33], a fuzzy-model-based approach is utilized to minimize the malicious effects of denial-of-service attacks on control networks and a truck-trailer system under cyber-attacks, respectively. The proposed approach has the potential to be applied to a wide range of networked control systems, especially those operating in harsh environments where cyber-attacks are common. The electric grid is changing from a relatively closed system to a complex highly integrated environment and the security system should evolve as threats to the electric system are inevitably diversified and multiplied. For critical infrastructure to be secure, the three most essential elements are hardware, software, and communication network [34]. Cyber-resiliency of such systems can be enhanced by incorporating modern control techniques.

Artificial intelligence (AI)-based techniques provide stable, secure, and reliable methods to address challenges with distributed control design and improve microgrid's stability [35]. However, the AI models are sometimes referred to as the black box models due to the limited understanding of their working behavior. Interpretability offers a set of techniques to overcome this black-box nature of AI models by revealing the impact of various features on the predictions of trained AI models [36], [37]. An explainable framework is needed to help users comprehend the outputs created by AI-based models. Such an explainable AI framework gives users the confidence in understanding and examining AI models in a variety of contexts, including healthcare and anomaly-based in-vehicle intrusion detection systems [38], [39]. An explainable framework based on partial dependence plots (PDP) for the neural network-based controller for power electronics converter is given in [40]. In a trained AI model, partial dependence relates to the interactions between predictor variables and predicted responses. Such explainable techniques may also help to understand feature correlations, the importance of the output of individual data points, and the feature attributions of the model outputs [41].

The application of ANN-based control for microgrids is not common as manifested from the usage of ANN as an observer layer in an AC microgrid in [27] and in reference tracking applications for DC microgrids in [28]. Also, the explainability of AI-based methods and the resilience of control designs against noise in the signals are not provided. The research motivation for this paper is based on the following observations from the literature:

- The application of ANN-based control of microgrid to take corrective actions to maintain stability under anomalies is not ubiquitous.
- The explainability of AI-based methods in the context of microgrids is not available.
- Resilience verification of the AI-based control design under a noisy signal environment in the context of microgrids is needed.

To bridge this research gap, we proposed a novel nonlinear autoregressive exogenous model (NARX ANN) as a resilient secondary control layer in a multi-DG AC microgrid. Such ANNs are nonparametric models and provide improved performance in forecasting applications based on time-series data in microgrids as evidenced in [42]. In order to evaluate the impact of different inputs on the model's performance, this paper also provides an explainable framework for the proposed ANN-based controller utilizing the partial dependence function, which displays the marginal effect of input features on the predicted output of the ANN model. There

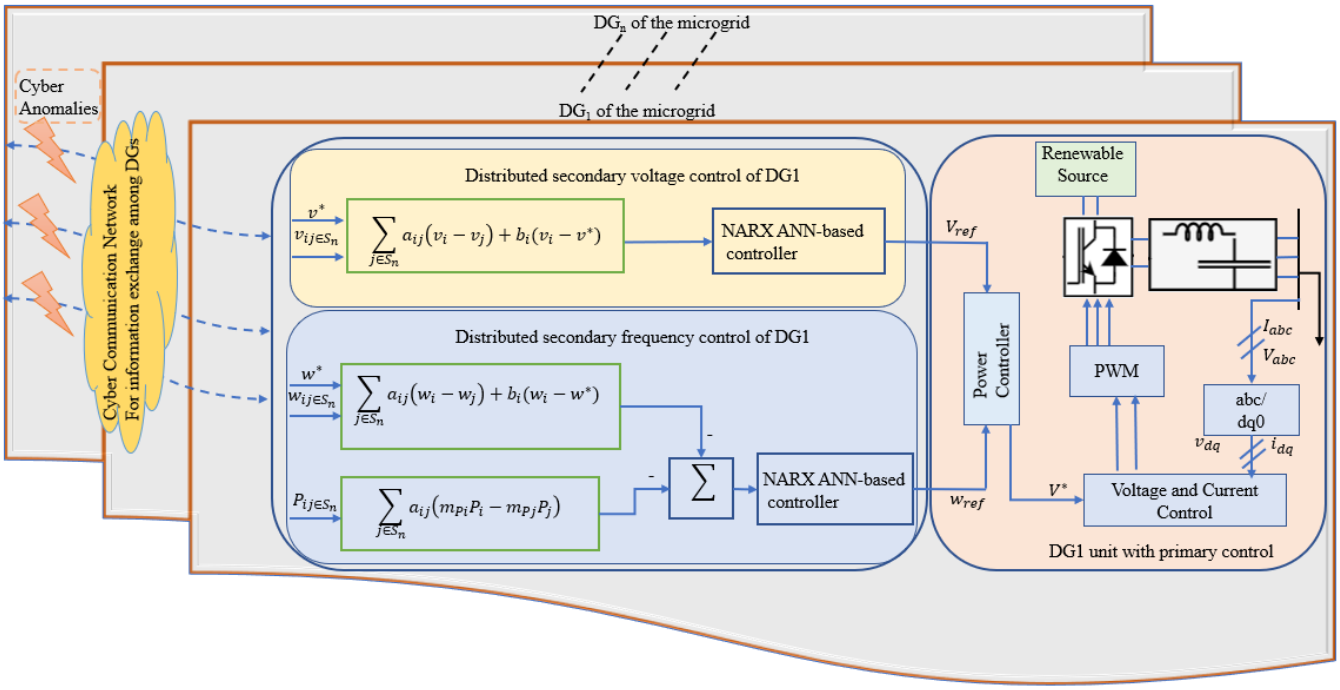


FIGURE 1: Illustration of the control mechanisms for the proposed controller in a typical microgrid setup. Cyber anomalies were injected into the communication network's voltages and frequency signals.

are several advantages of using such intelligent anomaly mitigation controls such as early detection of anomalies before they can cause significant damage or disruption to the system, less manual intervention, and enhanced understanding of the system to identify areas for improvement. The proposed control technique utilizes an advanced AI-based tool tailored to mitigate the data-driven cyber anomalies targeting the communication network of the microgrid. Also, it is scalable and depicted improved performance under complex real-time test scenarios. The main contributions of this research are summarized as follows:

- A resilient ANN-based secondary control technique is proposed to mitigate cyber anomalies. Such anomalies are introduced through the communication links to verify that the proposed control technique maintained the desired operation of the system.
- The proposed control technique does not depend on an estimator or an observer layer for cyber anomaly detection.
- The resilience of the proposed ANN-based control technique is tested under a noisy environment by adding white Gaussian noise to the voltage and frequency inputs of ANN.
- The proposed method can be expandable for a large-scale microgrid. This is accomplished by designing ANN-based control using a connection matrix allowing the integration of multiple DGs without compromising the microgrid's operation.
- An explainable framework is provided using PDP to identify the most critical node in the microgrid by evaluating the control decisions under extreme scenarios.

Performance comparisons of the proposed ANN-based control strategy with the existing PI-based distributed secondary control method are also presented in this paper. The control performance is also validated in real-time by simulating an AC microgrid, on the real-time digital simulator OPAL-RT. The results obtained in various case studies have verified the effectiveness of the proposed ANN-based secondary control for AC microgrids. The mean absolute percentage error (MAPE) and the voltage and frequency regulation are used as a benchmark to evaluate the performance of the trained ANNs.

The rest of the paper is organized as follows. Section II describes the AC microgrid used in this work 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 explainable framework for ANN is discussed in section V. In section VI, the results obtained from real-time simulations performed on the test microgrid are discussed. Finally, this paper is concluded in section VII.

II. SYSTEM DESCRIPTION

The AC microgrid used in 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. The primary controller is implemented locally at each of the DG using a conventional

droop control technique that provides a relationship between the frequency ω_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:

$$\begin{cases} v_o = v^* - n_{Q_i} Q_i, \\ w_i = w^* - m_{P_i} P_i, \end{cases} \tag{1}$$

where v^*, ω^* are the primary voltage and frequency reference values, and m_{P_i}, n_{Q_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 the voltage and frequency of each DG are synchronized with their respective reference values (v^* and w^*):

$$\begin{cases} \lim_{t\to\infty} \|v_o - v^*\| = 0, \\ \lim_{t\to\infty} \|w_i - w^*\| = 0. \end{cases} \tag{2}$$

For a given DG, the distributed cooperative secondary voltage and frequency management requires its own information as well as that of the neighboring DGs to collaboratively achieve the control objectives. The power controller implements the droop techniques and ultimately voltage and current controllers generate the reference for inverters. The communication network of a multiagent cooperative system can be modeled by a directed graph (digraph) with nodes and edges representing DGs and communication links in the microgrid, respectively. Based on the digraph 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:

$$v_{en} = \sum_{j\in S_n} a_{ij}(v_i - v_j) + b_i(v_i - v^*), \tag{3}$$

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

$$\begin{aligned} u_i = -c_g\Big(\sum_{j\in S_n} a_{ij}(\omega_i - \omega_j) + b_i(\omega_i - \omega^*) \\ + \sum_{j\in S_n} a_{ij}(m_{P_i}P_i - m_{P_j}P_j)\Big), \end{aligned} \tag{4}$$

where c_g is the coupling gain. In [4], more information about distributed cooperative control architecture is provided. Description of the cyber anomalies investigated in this paper is given in the next subsection.

A. CYBER ANOMALIES

Cyber anomalies target the microgrid's communication layer by injecting false data or compromising the network's information exchange. FDI attack targets the voltage and frequency information of neighboring DGs on the communication graph. A distributed secondary controller's feedback signal can be characterized as:

$$x(u_n(t)) = u_n(t) + \psi_n(t), \tag{5}$$

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]. Following are the 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 γ of the desired signal $u_n(t)$ into $x(u_n(t))$ at a certain time t_o throughout the system's operation, as follows:

$$x(u_n(t)) = \begin{cases} u_n(t), \ when\ t < t_o, \\ u_n(t) + \gamma * u_i(t), \ when\ t > t_o. \end{cases} \tag{6}$$

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:

$$x(u_n(t)) = \begin{cases} u_n(t), \ when\ t < t_o, \\ \gamma * u_n(t), \ when\ t > t_o. \end{cases} \tag{7}$$

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

$$\psi_n(t) = \begin{cases} 0, \ when\ t < t_o, \\ \xi sin(\omega t) * u_n(t), \ when\ t > t_o. \end{cases} \tag{8}$$

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

$$\psi_n(t) = \begin{cases} 0, \ when\ t < t_o, \\ \gamma * u_n(t) + \xi sin(\omega t) * u_n(t), \ when\ t > t_o. \end{cases} \tag{9}$$

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:

$$[x(u_n(t))]_{4\times 1} = \begin{cases} [u_n(t)]_{4\times 1}, \ when\ t < t_o, \\ [u_n(t)]_{4\times 1} + \chi, \ when\ t > t_o, \end{cases} \tag{10}$$

where χ is the false data being injected to all the four DGs of the microgrid system when $t > t_o$.

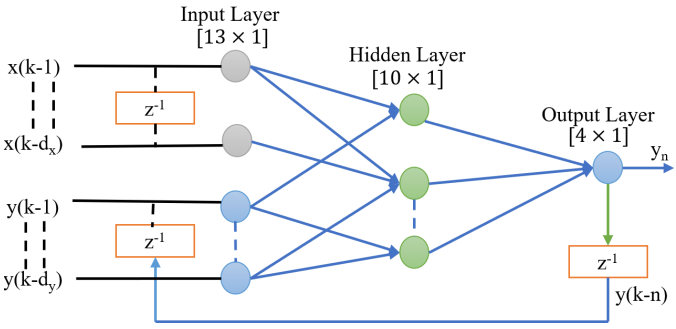


FIGURE 2: The architecture of a NARX ANN with 1 input layer with 13 nodes, 1 hidden layer with 10 nodes, and an output layer with 4 nodes is shown.

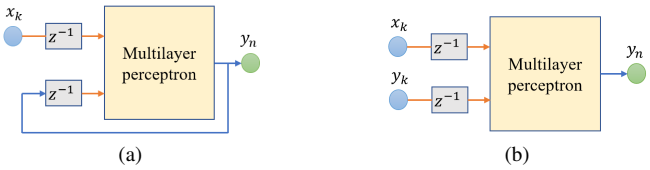


FIGURE 3: The NARX ANN configurations are shown. (a) Parallel configuration. (b) Series parallel configuration.

III. NONLINEAR AUTO-REGRESSIVE EXOGENOUS ARTIFICIAL NEURAL NETWORKS

NARX ANN (used as ANN for brevity in manuscript) is 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 [26], [42]. In this paper, we have deployed a single-layer ANN to generate the reference for the primary controllers. The embedded memory in ANN will help improve gradient descent, converge faster, and can be deployed for nonlinear systems. This ANN can model dynamic systems with arbitrary accuracy making them very suitable for time-series applications [43]. The trained ANN-based controller replaces the state-of-the-art PI-based controller in the secondary layer of distributed cooperative control as shown in Fig. 1. 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 nodes in the hidden layer. This structure is optimized after multiple trainings and found best suited for this work. The preceding batch of output and input, $y(k-i)$ and $x(k-i)$, respectively, establish the ANN's output $y(k)$ that constructs an autoregressive model to predict the current value of the dynamical system. These delayed output values act as pseudo-states to extract system dynamics from time series data. This characteristic makes NARX ANN a promising choice for nonlinear dynamical system modeling in applications like intelligent control [44]. The mathematical model of ANN is given as follows:

$$y(k+1) = f[x(k-n), ..., x(k-d_x-n+1), y(k), ..., y(k-d_y+1)], \quad (11)$$

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:

$$y(k+1) = f[x(k), ..., x(k-d_x+1), y(k), ..., y(k-d_y+1)], \quad (12)$$

which can be expressed in vector form as follows:

$$y(k+1) = f[Y(k); X(k)], \quad (13)$$

where the boldface letters represent vectors, such that, $Y(k)$ and $X(k)$ represent the output and input, respectively. The nonlinear mapping $f(.)$ can be approximated by a standard multilayer perceptron network. The architecture of a single-layer ANN is shown in Fig. 2. 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:

$$\hat{y}(k+1) = \hat{f}[x(k), ..., x(k-d_x+1), \hat{y}(k), ..., \hat{y}(k-d_y+1)], \quad (14)$$

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:

$$\hat{y}(k+1) = \hat{f}[x(k), ..., x(k-d_x+1), y(k), ..., y(k-d_y+1)]. \quad (15)$$

Since 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 level 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 the 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. 6, each DG shares voltage information with the two neighboring DGs.
2) The following data is collected under normal operating conditions: **a.** DG's own voltage information v_{nn} where $n \in (1, 2, 3, 4)$, **b.** The voltage information from neighbors of DG1 v_{1i} and DG3 v_{3i}, where $i \in (2, 4)$, **c.** The voltage information from neighbors of DG2 v_{2j} and DG4 v_{4j} where $j \in (1, 3)$, **d.** The secondary control reference voltage v^* and the primary control reference voltage output generated by each DG v_n^*.
3) The test microgrid is simulated with 5 load step changes and 3 different sets of reference voltages. This results in a total of 15 distinct 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.

Let P be the training data input for ANN. P is obtained through multiple simulations of the test microgrid, where, $P = [v_{nn}, v_{1i}, v_{3i}, v_{2j}, v_{4j}, v^*]_{13\times1}$. The target for the training of ANNs is T, where $T = [v_n^*]_{4\times1}$. To optimize the weights for offline training, both P and T are generated by executing various scenarios of simulations. The attack vector for the DGs aimed at secondary voltage control information sharing is as follows:

$$\mathbf{V}_{ij} = \mathbf{V}_{ij_{actual}} + \chi_{attack}\mathbf{V}_{ij}, \tag{16}$$

such that $\mathbf{V}_{ij}$ is the compromised information input to the secondary voltage controller of DG_n, $\mathbf{V}_{ij_{actual}}$ is the vector of real measurements, and χ_{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 is initiated 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 and v_n^* is the reference output voltage for each DG unit. ANN-based secondary voltage control attempts to decrease this error as follows:

$$\lim_{t\to\infty} \mu_v = 0. \tag{17}$$

Remark 2: 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 the secondary voltage controller is based on the following relationship:

$$\underbrace{\begin{bmatrix} 0 & 1 & 1 & 0 & 1 & . & . & a_{1j} \\ 0 & 1 & 1 & 1 & 0 & . & . & a_{2j} \\ 1 & 0 & 1 & 1 & 1 & . & . & a_{3j} \\ 0 & 1 & 0 & 1 & 1 & . & . & a_{4j} \\ . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ a_{i1} & a_{i2} & a_{i3} & a_{i4} & . & . & . & a_{ij} \end{bmatrix}}_{A} \underbrace{\begin{bmatrix} v^* \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ . \\ . \\ v_n \end{bmatrix}}_{X} = \underbrace{\begin{bmatrix} v_1^* \\ v_2^* \\ v_3^* \\ v_4^* \\ . \\ . \\ v_n^* \end{bmatrix}}_{B}, \tag{18}$$

where A is the microgrid's connection matrix and $a_{ij} \in (0, 1)$, where 1 or 0 depicts if a connection among adjacent DGs exists or not, respectively. 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. For this case study with a 4 DGs microgrid, the dimensions in (18) are $A_{4\times5} \times X_{5\times1} = B_{4\times1}$. However, the structure of A can have a higher dimension if the number of DGs increases.

As shown in Fig. 4, 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 terminates when maximum generalization is achieved, as 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 2.32×10^{-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 the microgrid.

D. ANN-BASED SECONDARY FREQUENCY CONTROL DESIGN

A distributed secondary frequency control layer is included in the test microgrid for the 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 attack 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 an FDI attack. For the test microgrid, DG1 and DG3 are chosen as the leading nodes, with DG2 and DG4 as the following nodes, to implement the cooperative control objectives given in (4). Therefore, an ANN-based secondary frequency controller is implemented for DG2 and DG4. Following a 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 $P = [\omega_{nn}, \omega_{2j}, \omega_{4j}]_{6\times 1}$, where $j \in (1, 3)$ such that, ω_{nn} is the frequency information of DG2 and DG4, ω_{2j}, ω_{2j} are frequency information from the neighbors of DG2 and DG4, respectively. The training target is $T = [\omega_n^*]_{2\times 1}$,where $n \in (2, 4)$ and ω_n^* represents the the 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. 5:

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

Scenario 2: Target of FDI attack: 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 attack: Various types of FDI attacks 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 the trained ANN model is evaluated using the mean absolute percentage error (MAPE), given as:

$$MAPE = \frac{1}{m}\sum_{k=1}^{m}\frac{|y_p - y|}{y} \times 100, \tag{19}$$

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 [45]. The results of this case study are given in Table 1. As observed from the data, adding noise to the input has a negligible effect on performance. In each case (30 dB, 35 dB, and 40 dB) the MAPE value is compared to the one at 0 dB, as shown in Table 1. This signifies that the proposed technique is resilient under distorted measurements.

TABLE 1: The MAPE performance of the trained ANN model with distorted input data is presented.

SNR	MAPE (%)			
(dB)	DG1	DG2	DG3	DG4
0	0.05	0.11	0.01	0.40
30	0.06	0.12	0.02	0.41
35	0.06	0.12	0.02	0.41
40	0.06	0.12	0.02	0.39

V. EXPLAINABLE ANN MODEL

Partial dependence plots (PDP) are one of the methods for global interpretability of ANN models that helps understand the model's response over a complete data set [46]. PDPs are plotted for the trained ANN model, proposed in this paper, to see the impacts on various DGs in the microgrid during cyber anomalies. The predictive response's partial dependence is computed on a subset of predictor features by marginalizing the other features. Based on (18), consider a subset v_{ns} such that $v_{1s} = [v_{11}, v_{12}, v_{13}]$ and $n \in (1, 2, 3, 4)$ represents the four DGs in the test microgrid. Let v_{nc} be the complementary set of v_{ns}, such that $v_{nc} = \{v_{ij} \in V_n : v_{ij} \notin v_{ns}\}$, 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:

$$f(V_n) = f(v_{ns}, v_{nc}). \tag{20}$$

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

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

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

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

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:

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

where j is the number of trained model's responses and $v_{nc_j} = (v_{ns}, v_{nc})$ is the j^{th} response. The performance of the proposed ANN-based secondary control is validated by executing real-time scenarios on the real-time digital simulator OPAL-RT under cyber anomalies after training the ANN, and the results are reported in the following section.

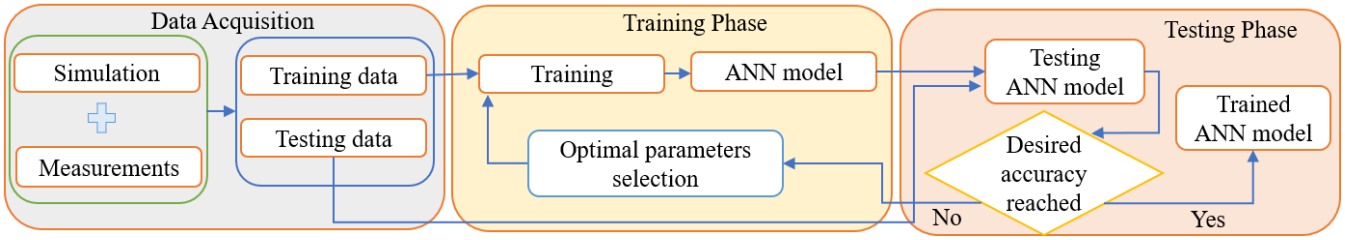


FIGURE 4: The flow chart with the steps involved in the training of the ANN model is shown.

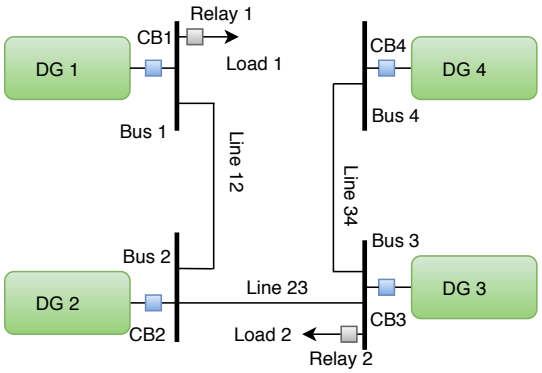


FIGURE 5: Four DGs based microgrid system.

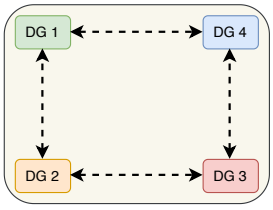


FIGURE 6: Communication graph for the four DGs.

VI. SIMULATION RESULTS

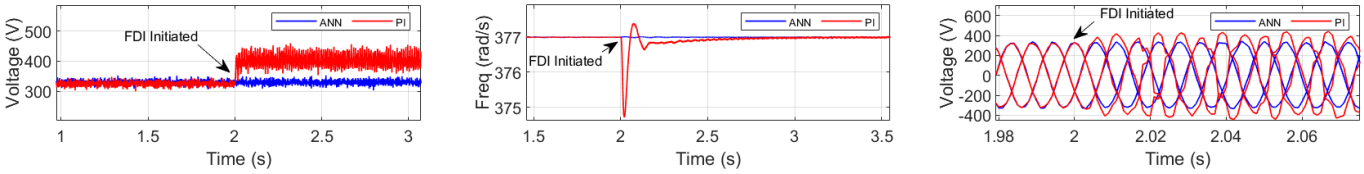
The performance of the proposed ANN-based secondary control is evaluated using the test microgrid system by performing real-time simulations as illustrated in Fig. 5. The four DG voltage source inverters are coupled through RL lines to provide AC power to two-three phase RL loads, denoted by $load_1$ and $load_2$ in Fig. 5. The four DGs of the test microgrid share their voltage and frequency information over the communication network as shown in Fig. 6. For our use case, the microgrid is designed in OPAL-RT's software simulation tool, i.e., RT-LAB. Then using MATLAB/Simulink coder, the trained ANN is implemented in RT-LAB to generate output for the designed microgrid. The trained ANN-based controller applies lessons acquired from multiple simulations to interpret anomalies and respond in real-time. Table 2, lists the parameters of the test microgrid system and the real-time simulator setup is shown in Fig. 14. Real-time digital simulator OPAL-RT facilitates the integration of real hardware into the simulation environment and consists of a communication interface, an FPGA-based input/output (I/O) subsystem, and a real-time simulation engine. OP5600 Series is a complete simulation system, that contains a powerful target computer, a reconfigurable FPGA, and signal conditioning for up to 256 I/Os. The front of the chassis provides access to the target computer's standard connectors, and monitoring interfaces and connectors, while the back of the chassis provides access to the I/O connectors, power cable, and main power switch. The lower part of the chassis contains a powerful target computer that is used to run simulations built with OPAL-RT's RT-LAB software simulation platform. The upper section contains the high-speed FPGA Xilinx Artix 7 FPGA 200T, that's programmable from the target computer. The FPGA is used to execute models designed with RT-LAB and manage the I/O lines. It can exchange data with the real-time simulations being executed on the target computer [47]. The cyber anomalies are introduced in the test microgrid system after the model is built upon a real-time target, as explained in the following sections.

A. TYPE 1 - STATIONARY ATTACK

Based on (6), an adversary injects false data into the voltage communication links of DGs. In this case, the target is DG1 link v_{11} such as at $t = 2$ s with $\gamma = 1.5$, an FDI attack is initiated. The microgrid operates under normal conditions for $t < 2$ s. After the FDI attack, the performance of the proposed ANN-based secondary voltage control is compared to the existing PI-based control and results are shown in Fig. 7. As illustrated in Fig. 7a and Fig. 7b, the proposed ANN-based secondary voltage control showed improved reference tracking capability in comparison to PI-based control which was not able to maintain the desired reference value after the FDI attack. Similarly, it can be seen that the ANN-based voltage controller maintained the desired output voltage at the output of DG1. In contrast, the PI-based controller suffered distortions in the output voltage after the FDI attack as shown in Fig. 7c.

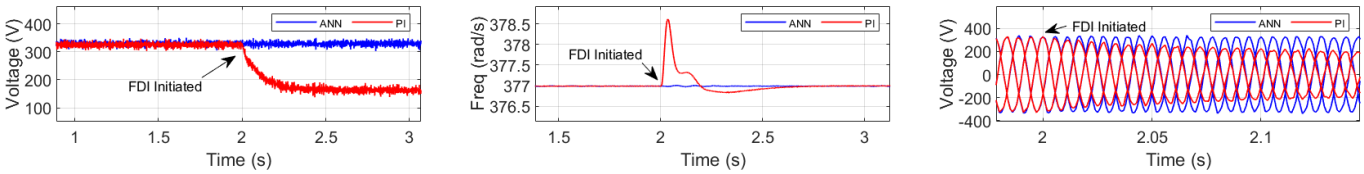
B. TYPE 2 - REINFORCEMENT ATTACK

This FDI attack is based on (7), in which false data is being injected into DGs voltage communication links. Such as for DG2's communication link v_{22}, the FDI attack is initiated at $t = 2$ s with $\gamma = 0.5$. After the FDI attack, the proposed ANN-based secondary voltage control is compared to the PI-based control, with the results displayed in Fig. 8. The



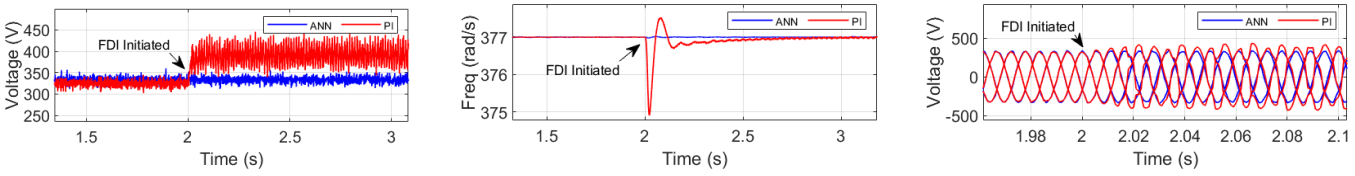
(a) Reference voltage (b) Reference frequency (c) Output voltage

FIGURE 7: Type 1: The performance comparison in terms of reference tracking and the output voltage at DG1.



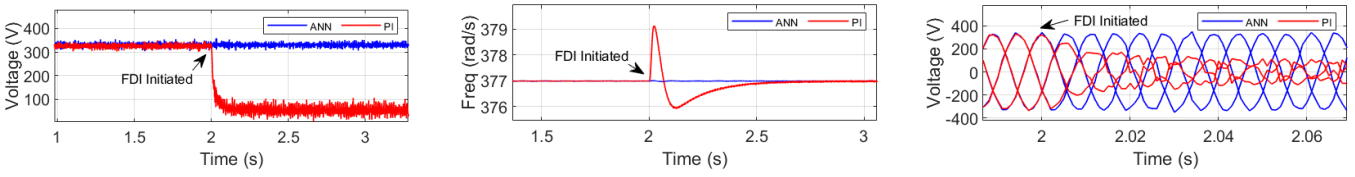
(a) Reference voltage (b) Reference frequency (c) Output voltage

FIGURE 8: Type 2: The performance comparison in terms of reference tracking and the output voltage at DG2.



(a) Reference voltage (b) Reference frequency (c) Output voltage

FIGURE 9: Type 3: The performance comparison in terms of reference tracking and the output voltage at DG3.



(a) Reference voltage (b) Reference frequency (c) Output Voltage

FIGURE 10: Type 4: The performance comparison in terms of reference tracking and the output voltage at DG4.

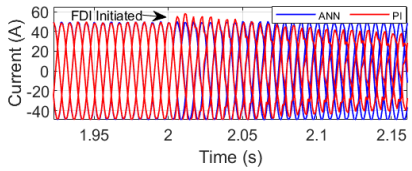
proposed ANN-based secondary voltage control, as shown in Fig. 8a and Fig. 8b, has demonstrated improved reference tracking capabilities compared to the PI-based control. As illustrated in Fig. 8c, the ANN-based voltage controller maintained the required output voltage at the output of DG2 after the FDI attack.

C. TYPE 3 - TIME-VARYING ATTACK

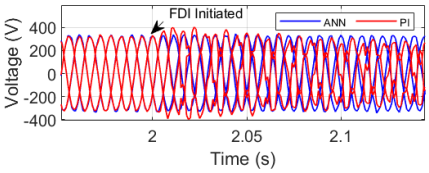
This FDI attack, based on (8), targets the voltage communication of DGs. In this case, false data is injected into the DG3 voltage communication link, v_{33}, at $t = 2$ s with $\xi = 0.5$ and $w = 2\pi 60$ rad/sec. The microgrid continues to operate normally for $t < 2$ s. The designed ANN-based secondary voltage control is compared to the PI-based control after the FDI attack is initiated, with the results shown in Fig. 9. The proposed ANN-based secondary voltage control, performed better in reference tracking than the PI-based control as shown in Fig. 9a and Fig. 9b. After the FDI attack, the ANN-based voltage controller maintained the specified output voltage at the output of DG3 as depicted in Fig. 9c.

D. TYPE 4 - MANIFOLD ATTACK

This FDI attack is initiated by injecting false data into the voltage communication connection, v_{44}, of DG4 with $\gamma = 0.5$, $\xi = 0.5$, and $w = 2\pi 60$ rad/sec at $t = 2$ s, based on (9). The microgrid operates normally until $t = 2$ s. After the FDI attack, the proposed ANN-based secondary voltage control is compared to PI-based control, with the results shown in Fig. 10. The proposed ANN-based secondary voltage control, as illustrated in Fig. 10a and Fig. 10b, 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 the FDI attack, as shown in Fig. 10c.

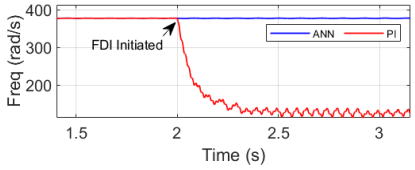


(a) Three phase currents at $load_1$

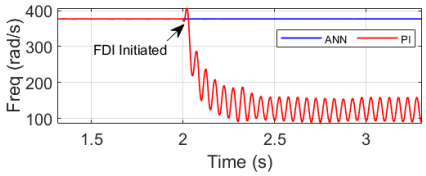


(b) Three phase voltages at $load_1$

FIGURE 11: Type 5: The performance comparison in terms of output voltage and current at $load_1$ of test microgrid system.



(a) The reference frequency at DG2

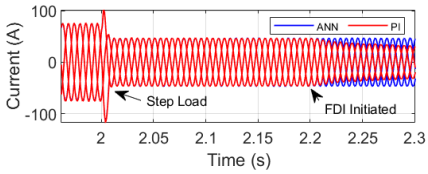


(b) The reference frequency at DG4

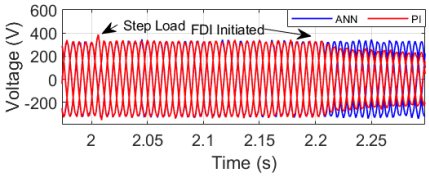
FIGURE 12: The performance comparison in terms of reference frequency under FDI attack is shown.

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 four DGs are compromised by injecting false data. This is a severe type of cyber anomaly due to its widespread nature. The results of the proposed ANN-based secondary voltage control are compared to PI-based control after an FDI attack in terms of output voltage and current at $load_1$ of test microgrid as shown in Fig. 11. The designed ANN-based controller maintained the power quality by keeping the desired phase and amplitude of three phase currents, whereas the PI-based controller did not withstand the FDI attack as shown in Fig. 11a. Similarly, the desired three phase voltages were maintained after the FDI attack in the case of the proposed ANN-based control compared to the PI-based control that showed large deviations from the desired output voltage as depicted in Fig. 11b.



(a) Output current at $load_1$



(b) Output voltage at $load_1$

FIGURE 13: The performance comparison of controllers under a step load change and FDI attack is given.

F. FDI ATTACK 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 attack is applied to target the frequency communication links of DG2 w_{22} and DG4 w_{44} with $\xi = 0.5$ and $w = 2\pi 60$ rad/sec based on (8). The proposed ANN-based frequency control maintained the desired frequency value after the FDI attack compared to the PI-based control, as shown in Fig. 12. The FDI attack is initiated at $t = 2$ s at DG2 and DG4 and it is evident from Fig. 12a and Fig. 12b that the designed ANN-based frequency control kept the system in normal operating condition with a little deviation after the FDI attack than PI-based control that showed large deviations from the reference value.

G. VARIABLE OPERATING SETTINGS

To 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. 13. A step-down load change is applied at $t = 2$ s and a Type 2 FDI attack with $\gamma = 0.5$ is initiated at $t = 2$ s. It can be observed in Fig. 13a, that the designed ANN-based controller follows the expected response as PI-based control with a decrease in current magnitude but after the FDI attack, the PI-based control deviates from the desired current value. Similarly, the designed ANN-based controller sustained the desired voltage level after both a step-down load change and FDI attack, whereas PI-based control could not sustain the effect of the FDI attack and showed distortion in output voltage as evident from Fig. 13b. This demonstrates the robust performance of the proposed ANN-based control under changing operating conditions of the test microgrid.

TABLE 2: OPAL-RT real-time digital simulator and microgrid system parameters are given.

OPAL-RT		**Microgrid**			
Name	Parameter	Name	Parameter	Name	Parameter
Version	OP5600 : 4 Cores, 3.0 GHz	L_{12}	(0.23+j318μ) Ω	V_{ref}	300 V
Software	RT-Lab v 2019.2.3	L_{23}	(0.35+j1847μ) Ω	L_{filter}	1.35 mh
FPGA	$Xilinx^{®}$ $Artix^{®}$-7 FPGA, 200T	L_{34}	(0.23+j318μ) Ω	C_{filter}	50 μF

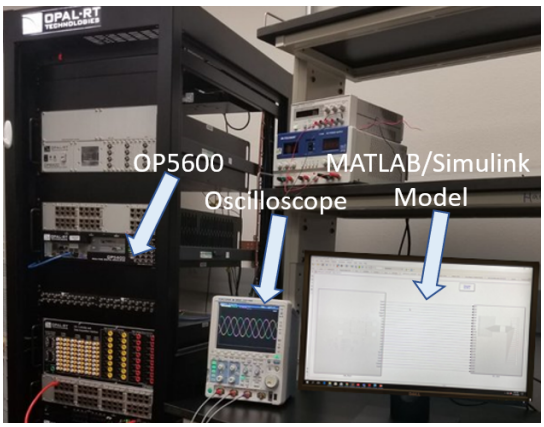
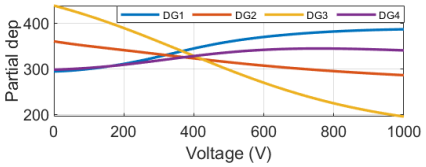
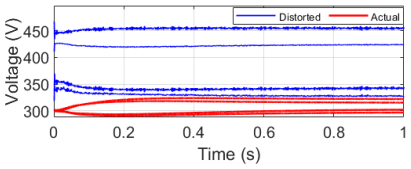


FIGURE 14: Real-time setup to evaluate the proposed resilient ANN-based control design is shown.



(a)



(b)

FIGURE 15: The results obtained from an explainable framework of ANN are shown. (a) Partial dependence plots of all the DGs. (b) The secondary reference voltage generated by all the DGs.

H. PARTIAL DEPENDENCE PLOTS

The partial dependence plots (PDP) for each DG are estimated with the objective of finding the impact of a cyber anomaly on each DG. For this purpose, an FDI attack is initiated and each DG's output voltage is selected individually as shown in Fig. 15. It is evident that DG3 suffers the largest impact by showing maximum deviations after the FDI attack. This finding is in line with (3) and as illustrated in Fig. 6, such that DG3 is the leading node based on the communication graph. Next, the impact on predicted secondary control reference voltage v_n^*, where, $n \in (1, 2, 3, 4)$ after spoofing all the communication links of DG3 is shown in Fig. 15b. It can be seen that the predicted voltages (in blue color) show large deviations from the actual voltages (in red color) of the system. These large deviations in predicted reference voltages lead to reduced power quality and loss of synchronism in the microgrid operation.

VII. CONCLUSION

An intelligent secondary cooperative control technique is proposed to mitigate the effects of cyber anomalies in distributed cooperative-controlled microgrids. This technique employs recurrent-type neural networks in the 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 resilience of the proposed ANN-based secondary cooperative control are shown by constructing a connection matrix and injecting noise to the input data. The structure of the trained ANN model is explained by plotting partial dependence plots. Various types of FDI attacks are considered to verify the effectiveness of the designed ANN-based secondary control. The results are validated by comparing it's performance with the traditional distributed secondary control technique and interpreted using an explainable framework. 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

[1] A. A. Khan, S. Ahmed, and O. A. Beg, "Intelligent anomaly mitigation in cyber-physical inverter-based systems," in IEEE Energy Conversion Congress and Exposition (ECCE), 2021, pp. 1301–1306.

[2] Q. Zhou, M. Shahidehpour, A. Paaso, S. Bahramirad, A. Alabdulwahab, and A. Abusorrah, "Distributed control and communication strategies in networked microgrids," IEEE Communications Surveys Tutorials, vol. 22, no. 4, pp. 2586–2633, 2020.

[3] A. Muhtadi, D. Pandit, N. Nguyen, and J. Mitra, "Distributed energy resources based microgrid: Review of architecture, control, and reliability," IEEE Transactions on Industry Applications, vol. 57, no. 3, pp. 2223–2235, 2021.

[4] A. Bidram, F. L. Lewis, and A. Davoudi, "Distributed control systems for small-scale power networks: Using multiagent cooperative control theory," IEEE Control Systems Magazine, vol. 34, no. 6, pp. 56–77, Dec 2014.

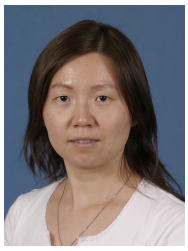
[5] M. R. Khalghani, J. Solanki, S. K. Solanki, M. H. Khooban, and A. Sargolzaei, "Resilient frequency control design for microgrids under false data injection," IEEE Transactions on Industrial Electronics, vol. 68, no. 3, pp. 2151–2162, 2021.

[6] E. Espina, J. Llanos, C. Burgos-Mellado, R. Cárdenas-Dobson, M. Martínez-Gómez, and D. Sáez, "Distributed control strategies for microgrids: An overview," IEEE Access, vol. 8, pp. 193 412–193 448, 2020.

[7] O. A. Beg, L. V. Nguyen, T. T. Johnson, and A. Davoudi, "Cyber-physical anomaly detection in microgrids using time-frequency logic formalism," IEEE Access, vol. 9, pp. 20 012–20 021, 2021.
[8] R. Moghaddass and J. Wang, "A hierarchical framework for smart grid anomaly detection using large-scale smart meter data," IEEE Transactions on Smart Grid, vol. 9, no. 6, pp. 5820–5830, 2018.
[9] H. Zhang, B. Liu, and H. Wu, "Smart grid cyber-physical attack and defense: A review," IEEE Access, vol. 9, pp. 29 641–29 659, 2021.
[10] M. A. Rahman and H. Mohsenian-Rad, "False data injection attacks against nonlinear state estimation in smart power grids," in IEEE Power Energy Society General Meeting, 2013, pp. 1–5.
[11] T. Caldognetto, P. Tenti, A. Costabeber, and P. Mattavelli, "Improving microgrid performance by cooperative control of distributed energy sources," IEEE Transactions on Industry Applications, vol. 50, no. 6, pp. 3921–3930, 2014.
[12] S. Abhinav, H. Modares, F. L. Lewis, F. Ferrese, and A. Davoudi, "Synchrony in networked microgrids under attacks," IEEE Transactions on Smart Grid, vol. 9, no. 6, pp. 6731–6741, Nov 2018.
[13] H. Zhang, W. Meng, J. Qi, X. Wang, and W. X. Zheng, "Distributed load sharing under false data injection attack in an inverter-based microgrid," IEEE Transactions on Industrial Electronics, vol. 66, no. 2, pp. 1543–1551, 2019.
[14] A. Bidram, B. Poudel, L. Damodaran, R. Fierro, and J. M. Guerrero, "Resilient and cybersecure distributed control of inverter-based islanded microgrids," IEEE Transactions on Industrial Informatics, vol. 16, no. 6, pp. 3881–3894, 2020.
[15] Q. Zhou, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, "A cyber-attack resilient distributed control strategy in islanded microgrids," IEEE Transactions on Smart Grid, vol. 11, no. 5, pp. 3690–3701, 2020.
[16] M. Shi, X. Chen, M. Shahidehpour, Q. Zhou, and J. Wen, "Observer-based resilient integrated distributed control against cyberattacks on sensors and actuators in islanded ac microgrids," IEEE Transactions on Smart Grid, vol. 12, no. 3, pp. 1953–1963, 2021.
[17] Y. Chen, D. Qi, H. Dong, C. Li, Z. Li, and J. Zhang, "A fdi attack-resilient distributed secondary control strategy for islanded microgrids," IEEE Transactions on Smart Grid, vol. 12, no. 3, pp. 1929–1938, 2021.
[18] J. Zhou, Y. Xu, L. Yang, and H. Sun, "Attack-resilient distributed control for islanded single-/three-phase microgrids based on distributed adaptive observers," Journal of Modern Power Systems and Clean Energy, pp. 1–10, 2020.
[19] S. Zhao, F. Blaabjerg, and H. Wang, "An overview of artificial intelligence applications for power electronics," IEEE Transactions on Power Electronics, vol. 36, no. 4, pp. 4633–4658, 2021.
[20] H. R. Baghaee, M. Mirsalim, and G. B. Gharehpetian, "Power calculation using rbf neural networks to improve power sharing of hierarchical control scheme in multi-der microgrids," IEEE Journal of Emerging and Selected Topics in Power Electronics, vol. 4, no. 4, pp. 1217–1225, 2016.
[21] S. Kazemlou and S. Mehraeen, "Decentralized discrete-time adaptive neural network control of interconnected dc distribution system," IEEE Transactions on Smart Grid, vol. 5, no. 5, pp. 2496–2507, 2014.
[22] A. Rosato, M. Panella, R. Araneo, and A. Andreotti, "A neural network based prediction system of distributed generation for the management of microgrids," IEEE Transactions on Industry Applications, vol. 55, no. 6, pp. 7092–7102, 2019.
[23] A. N. Akpolat, M. R. Habibi, E. Dursun, A. E. Kuzucuoğlu, Y. Yang, T. Dragičević, and F. Blaabjerg, "Sensorless control of dc microgrid based on artificial intelligence," IEEE Transactions on Energy Conversion, vol. 36, no. 3, pp. 2319–2329, 2021.
[24] S. Li, M. Fairbank, C. Johnson, D. C. Wunsch, E. Alonso, and J. L. Proao, "Artificial neural networks for control of a grid-connected rectifier/inverter under disturbance, dynamic and power converter switching conditions," IEEE Transactions on Neural Networks and Learning Systems, vol. 25, no. 4, pp. 738–750, 2014.
[25] C. J. Vega, L. Djilali, and E. N. Sanchez, "Secondary control of microgrids via neural inverse optimal distributed cooperative control," IFAC-PapersOnLine, vol. 53, no. 2, pp. 7891–7896, 2020.
[26] M. R. Habibi, S. Sahoo, S. Rivera, T. Dragičević, and F. Blaabjerg, "Decentralized coordinated cyberattack detection and mitigation strategy in dc microgrids based on artificial neural networks," IEEE Journal of Emerging and Selected Topics in Power Electronics, vol. 9, no. 4, pp. 4629–4638, 2021.
[27] A. Abbaspour, A. Sargolzaei, and K. K. Yen, "A neural network based resilient control design for distributed power systems under faults and attacks," in IEEE International Conference on Environment and Electrical Engineering and IEEE Industrial and Commercial Power Systems Europe (EEEIC / I&CPS Europe), 2018, pp. 1–6.
[28] M. R. Habibi, H. R. Baghaee, T. Dragičević, and F. Blaabjerg, "False data injection cyber-attacks mitigation in parallel dc/dc converters based on artificial neural networks," IEEE Transactions on Circuits and Systems II: Express Briefs, 2020.
[29] A. N. Akpolat, M. R. Habibi, H. R. Baghaee, E. Dursun, A. E. E. Kuzucuoglu, Y. Yang, T. Dragicevic, and F. Blaabjerg, "Dynamic stabilization of dc microgrids using ann-based model predictive control," IEEE Transactions on Energy Conversion, 2021.
[30] M. R. Habibi, H. R. Baghaee, F. Blaabjerg, and T. Dragicevic, "Secure mpc/ann-based false data injection cyber-attack detection and mitigation in dc microgrids," IEEE Systems Journal, pp. 1–12, 2021.
[31] W. Duo, M. Zhou, and A. Abusorrah, "A survey of cyber attacks on cyber physical systems: Recent advances and challenges," IEEE/CAA Journal of Automatica Sinica, vol. 9, no. 5, pp. 784–800, 2022.
[32] X. Cai, K. Shi, K. She, S. Zhong, Y. C. Soh, and Y. Yu, "Performance error estimation and elastic integral event triggering mechanism design for t–s fuzzy networked control system under dos attacks," IEEE Transactions on Fuzzy Systems, vol. 31, no. 4, pp. 1327–1339, 2023.
[33] X. Cai, K. Shi, K. She, S. Zhong, and Y. Tang, "Quantized sampled-data control tactic for t-s fuzzy ncs under stochastic cyber-attacks and its application to truck-trailer system," IEEE Transactions on Vehicular Technology, vol. 71, no. 7, pp. 7023–7032, 2022.
[34] K. Yan, X. Liu, Y. Lu, and F. Qin, "A cyber-physical power system risk assessment model against cyberattacks," IEEE Systems Journal, pp. 1–11, 2022.
[35] E. Mohammadi, M. Alizadeh, M. Asgarimoghaddam, X. Wang, and M. G. Simões, "A review on application of artificial intelligence techniques in microgrids," IEEE Journal of Emerging and Selected Topics in Industrial Electronics, vol. 3, no. 4, pp. 878–890, 2022.
[36] C. Xu, Z. Liao, C. Li, X. Zhou, and R. Xie, "Review on interpretable machine learning in smart grid," Energies, vol. 15, no. 12, p. 4427, 2022.
[37] K. Amarasinghe, K. Kenney, and M. Manic, "Toward explainable deep neural network based anomaly detection," in 11th International Conference on Human System Interaction (HSI). IEEE, 2018, pp. 311–317.
[38] D. Saraswat, P. Bhattacharya, A. Verma, V. K. Prasad, S. Tanwar, G. Sharma, P. N. Bokoro, and R. Sharma, "Explainable ai for healthcare 5.0: Opportunities and challenges," IEEE Access, 2022.
[39] H. Lundberg, N. I. Mowla, S. F. Abedin, K. Thar, A. Mahmood, M. Gidlund, and S. Raza, "Experimental analysis of trustworthy in-vehicle intrusion detection system using explainable artificial intelligence (xai)," IEEE Access, vol. 10, pp. 102 831–102 841, 2022.
[40] S. Sahoo, H. Wang, and F. Blaabjerg, "On the explainability of black box data-driven controllers for power electronic converters," in IEEE Energy Conversion Congress and Exposition (ECCE), 2021, pp. 1366–1372.
[41] R. Machlev, L. Heistrene, M. Perl, K. Levy, J. Belikov, S. Mannor, and Y. Levron, "Explainable artificial intelligence (xai) techniques for energy and power systems: Review, challenges and opportunities," Energy and AI, p. 100169, 2022.
[42] M. R. Habibi, H. R. Baghaee, T. Dragičević, and F. Blaabjerg, "Detection of false data injection cyber-attacks in dc microgrids based on recurrent neural networks," IEEE Journal of Emerging and Selected Topics in Power Electronics, vol. 9, no. 5, pp. 5294–5310, 2021.
[43] E. Diaconescu, "The use of narx neural networks to predict chaotic time series," Wseas Transactions on computer research, vol. 3, no. 3, pp. 182–191, 2008.
[44] H. Alimohammadi, B. B. Alagoz, A. Tepljakov, K. Vassiljeva, and E. Petlenkov, "A narx model reference adaptive control scheme: improved disturbance rejection fractional-order pid control of an experimental magnetic levitation system," Algorithms, vol. 13, no. 8, p. 201, 2020.
[45] J. James, Y. Hou, A. Y. Lam, and V. O. Li, "Intelligent fault detection scheme for microgrids with wavelet-based deep neural networks," IEEE Transactions on Smart Grid, vol. 10, no. 2, pp. 1694–1703, 2017.
[46] J. H. Friedman, "Greedy function approximation: a gradient boosting machine," Annals of statistics, pp. 1189–1232, 2001.
[47] Hardware products documentation, op5600v2. [Online]. Available: opal-rt.atlassian.net/wiki/spaces/PHDGD/pages/144689898/OP5600V2

ASAD ALI KHAN completed his Ph.D. degree in electrical engineering from the University of Texas at San Antonio, USA in 2022. His area of research is smart grids, integration of renewable energy into conventional power systems, fault identification, and cyber security in distributed generation systems using artificial intelligence algorithms. Before that, he received a master's in systems engineering from the Pakistan Institute of engineering and applied sciences in November 2014 and a bachelor's in electrical engineering from the university of engineering and technology Taxila, Pakistan in August 2012.

OMAR A BEG received his Ph.D. degree in electrical engineering from the University of Texas at Arlington, TX, USA in 2017. He was the recipient of the Rising STARs (Science and Technology Acquisition and Retention) grant by the UT System. He is also the recipient of the President's Research award and the Allen & Betty Edgar Faculty Fellowship. He is currently an Assistant Professor in the Department of Electrical Engineering at the College of Engineering, the University of Texas Permian Basin, TX, USA. His research interests include formal verification, cyber-attack detection, and resilient cyber-physical power systems using formal techniques and artificial intelligence.



YU-FANG JIN received her B. Sc. degree in Automation from Zhengzhou University, China in 1994, and her M.S. and Ph.D. degrees in electrical and computer engineering from the University of Central Florida, Florida, USA, in 2002 and 2004, respectively. She is a Professor in the Department of Electrical and Computer Engineering at the University of Texas at San Antonio. Her recent research interest includes modeling complex systems using both physical-driven and data-driven methods, especially the application and interpretation of different artificial intelligence algorithms.

SARA AHMED is an Associate Professor in Electrical & Computer Engineering Department in the University of Texas at San Antonio. She received her Bachelor's, Master's, and Ph.D. degrees all in Electrical Engineering with a Power Electronics concentration from Virginia Tech, Center for Power Electronics in 2006, 2007, and 2011 respectively. Dr. Ahmed has five years of prior R&D industry experience as a Senior Scientist at ABB's U.S Corporate Research Center in Raleigh, NC. Her primary research interests are in the area of modeling, simulation, and analysis of power electronics systems with a focus on control, stability, fault analysis, model prediction, integration of renewables, and hardware-in-the-loop modeling and testing. She holds 8 U.S. patents, 2 U.S. patent applications, and more than 50 referred publications.